Working Paper Series
of the Institute of
Business Management

Diskussionspapiere
des Betriebswirtschaftlichen
Instituts

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

2022/8

Axel Winkelmann,
Christian Janiesch (Eds.)

Plattform für das integrierte Management von Kollaborationen in Wertschöpfungsnetzwerken (PIMKoWe)

Working Paper Series of the Institute of Business Management

This working paper series is issued by the Institute of Business Management of the University of Würzburg. It aims for quick dissemination of new research results and publishes research papers in all areas of business management.

Diskussionspapiere des Betriebswirtschaftlichen Instituts

Die vorliegenden Diskussionspapiere werden vom betriebswirtschaftlichen Institut der Universität Würzburg mit dem Ziel herausgegeben, neue Forschungserkenntnisse schnell zu veröffentlichen. Die Themen entstammen dem gesamten Spektrum der Betriebswirtschaftslehre.

Betriebswirtschaftliches Institut
Sanderring 2
D-97070 Würzburg
Tel.: +49 (0) 931 / 31-82901
Fax: +49 (0) 931 / 31-87274
http://www.bwl.uni-wuerzburg.de

Würzburg 2022.

Dieses Dokument wird bereitgestellt durch den Publikationsservice der Universität Würzburg.

Universitätsbibliothek Würzburg
Am Hubland
D-97074 Würzburg
Tel.: +49 (0) 931 / 31-85906
opus@bibliothek.uni-wuerzburg.de
https://opus.bibliothek.uni-wuerzburg.de
Titelblattgestaltung / Fotos: Kristina Hanig

ISSN: 2199-0328

Citation / Zitation dieser Publikation:

Winkelmann, A.; Janiesch, C. (Eds.) (2022): Plattform für das integrierte Management von Kollaborationen in Wertschöpfungsnetzwerken (PIMKoWe). Working Paper Series of the Institute of Business Management, 2022/8. Würzburg: University of Würzburg. DOI: 10.25972/OPUS-29335

Plattform für das integrierte Management von Kollaborationen in Wertschöpfungsnetzwerken (PIMKoWe)

Das Verbundprojekt „Plattform für das integrierte Management von Kollaborationen in Wertschöpfungsnetzwerken“ (PIMKoWe – Förderkennzeichen „02P17D160“) ist ein Forschungsvorhaben im Rahmen des Forschungsprogramms „Innovationen für die Produktion, Dienstleistung und Arbeit von morgen“ der Bekanntmachung „Industrie 4.0 – Intelligente Kollaborationen in dynamischen Wertschöpfungsnetzwerken“ (InKoWe). Das Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) gefördert und durch den Projektträger des Karlsruher Instituts für Technologie (PTKA) betreut.

Ziel des Forschungsprojekts PIMKoWe ist die Entwicklung und Bereitstellung einer Plattformlösung zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors.

Konsortialpartner

Julius-Maximilians-Universität Würzburg

infosim®

actiware® DEVELOPMENT

ROBUR AUTOMATION – YOUR INDUSTRIAL AUTOMATION SPECIALIST

MAUL-THEET – Vibration Test & Analysis

SAP Signavio

Gefördert vom:

Bundesministerium für Bildung und Forschung

Bereut vom:

Projektträger Forschungszentrum Karlsruhe (PTKA)

Vorwort

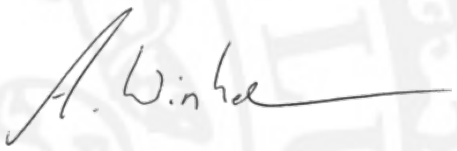
Zwar scheinen die jüngsten Krisen die Errungenschaften der Globalisierung der letzten Jahrzehnte zurückzudrängen, doch nach wie vor ermöglicht die internationale, kleinteilige Spezialisierung den Unternehmen das Handeln auf internationalen Märkten. Dies führt gleichzeitig zu einem hohen Konkurrenzdruck, um gegenüber Konkurrenz z.B. aus Niedriglohnländern zu überleben. Viele Unternehmen haben deswegen enorme Wertschöpfungsnetzwerke und sind daher gezwungen, mit vielen Partnern im internationalen Austausch zu stehen. Diese hohe Reaktivität, die einhergeht mit einer benötigten Flexibilität im Lieferantennetzwerk, bedeutet aber auch, sich permanent auf neue, teilweise unbekannte Partner einzulassen. Während sich die Notwendigkeit der datentechnischen Integration und deren Vorteil bereits seit Jahrzehnten herumgesprochen hat und in vielen Wertschöpfungsnetzwerken auch gelebt wird, stellt sich nach wie vor die Frage, wie digitale und insbesondere sensible Informationen fälschungssicher so ausgetauscht werden können, dass alle Kooperationspartner auf verifizierte Informationen zurückgreifen können. Hier greifen die derzeitigen, sehr heterogen ausgelegten betriebswirtschaftlichen Unternehmenssoftwaresysteme noch deutlich zu kurz. Es fehlt insgesamt an einer technischen Lösung, um mit den besagten unbekannten Partnern kooperieren zu können und die Prozesse aus der Welt der Unternehmenssoftware abzubilden. Auf diese Weise lässt sich im Sinne der datentechnischen Integration kein gemeinsames vertrauenswürdiges Datenfundament aufbauen.

Das Innovationsthema Blockchain verspricht hier die Möglichkeit, insbesondere ein verteiltes Datenfundament auch bei miteinander kooperierenden Partnern aufzubauen. Bekannt wurde dieser Ansatz vor allem durch den Fintech-Hype zur Abbildung von virtuellen Währungen wie dem Bitcoin und zugehörigen Transaktionen. Die Technologie hat aber darüber hinausgehend sehr viele disruptive Potenziale, z.B. für den Austausch von Daten im Bereich der Unternehmenssoftware. Gleichzeitig zeigte sich, dass in diesem Bereich der Ausbau der Forschung vertieft werden muss, um einen Einsatz in vertrauenswürdigen und internationalen Kooperationsnetzwerken zu ermöglichen.

Mit dieser Zielsetzung, einen fälschungssicheren Austausch digitaler und sensibler Informationen zu erreichen, traten wir an das Bundesministerium für Bildung und Forschung (BMBF) heran, welches uns mit dem Verbundprojekt „Plattform für das integrierte Management von Kollaborationen in Wertschöpfungsnetzwerken“ – (PIMKoWe – Förderkennzeichen „02P17D160“ - https://projekt-pimkowe.de) von Oktober 2018 bis Ende März 2022 beauftragte. Hierin adressieren wir die Problematik durch die Entwicklung einer entsprechenden Austauschplattform, welche sich als wichtiger Bestandteil in die Förderlinie „Industrie 4.0 – Intelligente Kollaborationen in dynamischen Wertschöpfungsnetzwerken“ (InKoWe) einreiht und durch den Projektträger Karlsruhe (PTKA) betreut wurde. Ziel war es, einen Plattformansatz zu entwickeln, um anhand mehrerer Anwendungsszenarien zu eruieren, inwieweit die Blockchain-Technologie geeignet ist, den Datenaustausch über das Wertschöpfungsnetzwerk zu ermöglichen und damit den hiesigen Wirtschaftsstandort zu stärken. Das Projekt konnte insbesondere viele neue Erkenntnisse gewinnen, wie z.B. die Anwendbarkeit der Blockchain in kritischen Bereichen wie der Echtzeitdatenauswertung in der Produktion, der Entwicklung von Datenstandards für Blockchain-basierte Unternehmenssoftware oder der Definition einer Blockchain-basierten Wertschöpfungsplattform. Damit schafft PIMKoWe wichtige Grundlagen, um internationale Wertschöpfungsnetzwerke in der betrieblichen Praxis zu fördern. Gleichzeitig zeigt sich aber auch, dass die Konzepte innerhalb des Blockchain-Umfelds jung und unerforscht sind und die technologische Reife der dahinterstehenden Ansätze noch in ihren Kinderschuhen steckt. Namhafte Pleiten und Crashs bei den virtuellen Währungen, in letzter Zeit aber auch rechtliche Bedenken im praktischen Einsatz in Wertschöpfungsnetzwerken zeigen, dass trotz unserer Forschung das Thema noch deutlich ausgebaut werden muss. Wir sind jedoch auch mit Blick auf verwandte Technologieentwicklung, wie z.B. der relationalen oder hierarchischen Datenbanken,

überzeugt, dass an den Konzepten der Blockchain kein Weg vorbeiführt und wir mit unserer Forschung und Umsetzung einen wichtigen Beitrag leisten konnten.

Bedanken möchten wir uns insbesondere bei dem Bundesministerium für Bildung und Forschung (BMBF) und dem PTKA. Zu erwähnen sind hier insbesondere Frau Dr. Danuta Seredynska und Herr Thomas Rosenbusch, die uns während der Verbundlaufzeit intensiv betreut haben und auch darüber hinaus stets für unsere Fragen zur Verfügung standen sowie wertvolle Anregungen gegeben haben. Die Ergebnisse des Verbundprojektes sind den zahlreichen Projektpartnern zu verdanken, bei denen wir uns ebenfalls sehr herzlich bedanken dürfen: Actiware Development GmbH, Infosim GmbH & Co. KG, ROBUR Automation GmbH, Maul-Theet GmbH und SAP Signavio. Uns hat die unkomplizierte, ideenreiche und nicht selten mit intensiven Diskussionen begleitete Zusammenarbeit auch während der COVID-19 Pandemie mit entsprechend virtuellen Arbeitstreffen sehr viel Freude bereitet. An der Julius-Maximilians-Universität Würzburg waren neben dem Lehrstuhl für BWL und Wirtschaftsinformatik auch die Juniorprofessur für Informationsmanagement von Prof. Dr. Christian Janiesch an der Forschung an diesem Verbundprojekt beteiligt. Auch hier ebenso wie an alle anderen Projektmitarbeiter ein herzliches Dankeschön für das unkomplizierte Zusammenarbeiten.



Prof. Dr. Axel Winkelmann
Lehrstuhl für BWL und Wirtschaftsinformatik
Julius-Maximilians-Universität Würzburg

Die Autoren

Prof. Axel Winkelmann ist Lehrstuhlinhaber für BWL und Wirtschaftsinformatik an der Julius-Maximilians-Universität in Würzburg. Er beschäftigt sich mit dem Management und der Gestaltung von betriebswirtschaftlicher Anwendungssoftware, insbesondere Enterprise-Resource-Planning-Systemen, sowie damit verbunden mit der Ablaufgestaltung von Unternehmen. Labore für Unternehmenssoftware, KI und Sensorik schaffen die Basis für grundlegende und angewandte Forschung. Ebenso schaffen bereits abgeschlossene Verbundsprojekte wie „DeepScan - Maschinelles Lernen zur automatisierten Erkennung von IKT-Sicherheitsvorfällen und Manipulationsversuchen“ und „DiHP - Dienstleistung für den integrierten Handel mit Produktionskapazitäten“ die entsprechenden wissenschaftlichen Grundlagen. Er ist Autor zahlreicher internationaler Artikel und Fachbücher, die sich thematisch an den genannten Bereichen orientieren. Im Rahmen des Verbundprojektes PIMKoWe übernahm er die Rolle des Projektkoordinators und beaufsichtigte die akademische Forschung und Koordination im Bereich der Prozessintegration in neuartigen Blockchain-Lösungen.

Prof. Dr. Christian Janiesch ist seit Oktober 2021 Inhaber des Lehrstuhls für Enterprise Computing in der Fakultät für Informatik an der Technischen Universität Dortmund. Zuvor leitete er die Juniorprofessur für Information Management an der Julius-Maximilians-Universität Würzburg. Sein Forschungsschwerpunkt liegt auf der Entwicklung von intelligenten, prozessorientierten Informationssystemen sowie deren Einbettung im organisationalen Kontext der Unternehmung. Seine gestaltungsorientierte Forschung verbindet dabei insbesondere die Themenfelder Geschäftsprozessmanagement, Business Analytics und Künstliche Intelligenz. Sie zielt darauf ab, neue Design-Theorien zu entwickeln. Während die konzeptuelle und modellhafte Gestaltung von Systemen stets ein Fokus seiner Forschung war, stehen heute die Chancen und Herausforderungen der Digitalisierung und insbesondere des maschinellen Lernens für die Informationssystementwicklung und den Einsatz in der unternehmerischen Praxis im Vordergrund. Anwendung findet diese Forschung vornehmlich im Umfeld des Industrial Internet of Things und der Robotic Process Automation. Im Rahmen des Projekts PIMKoWe verantwortete er die Erhebung der Anforderungsanalyse sowie die Ableitung und Implementierung der Eventarchitektur.

Norman Pytel ist wissenschaftlicher Mitarbeiter an der Universität Würzburg. Nach seinem Studium arbeitete er in mehreren Unternehmen der Automobilbranche und Zulieferindustrie, um werksinterne und -übergreifende Materialflüsse zu organisieren. Seine Forschung konzentriert sich auf die Einführung von Distributed-Ledger-Technologien in den Bereichen Logistik und Produktion in Kombination mit Enterprise Systemen. In diesem Zusammenhang untersucht er die Herausforderungen der konzeptionellen Gestaltung und Standardisierung von Anwendungsfällen in Supply Chains.

Myriam Schaschek ist wissenschaftliche Mitarbeiterin am Lehrstuhl für BWL und Wirtschaftsinformatik an der Julius-Maximilians-Universität Würzburg tätig. Ihre Forschungsschwerpunkte umfassen das Geschäftsprozessmanagement, die Daten- und Prozessanalyse sowie die datengetriebene Entscheidungsunterstützung von Unternehmen. Vor ihrer Tätigkeit als wissenschaftliche Mitarbeiterin studierte sie Wirtschaftswissenschaften (B.Sc.) und International Economic Policy (M.Sc.) an der Universität Würzburg. Zusätzlich absolvierte Myriam Schaschek ein Begleitstudium im Europäischen Recht.

Christian Zeiß ist wissenschaftlicher Mitarbeiter am Lehrstuhl für BWL und Wirtschaftsinformatik der Universität Würzburg. Im Rahmen seiner Forschung beschäftigt er sich mit verschiedenen Anwendungen der Distributed Ledger Technologie in der Supply Chain. Christian Zeiß wirkte im Projekt PIMKoWe bei der Simulation eines Blockchain-basierten Tracking und Tracing Systems und der Gestaltung der Datenaustauschstruktur mit. Besonders die Konzeption und Gestaltung von Token und Smart Contracts, aber auch von Datenflüssen in automatisierten Prozessen im Sinne des Tracing Systems, stand dabei im Vordergrund.

Lukas-Valentin Herm ist wissenschaftlicher Mitarbeiter am Lehrstuhl für BWL und Wirtschaftsinformatik an der Universität Würzburg. Seine Forschungsschwerpunkte umfassen die Wahrnehmung, Gestaltung und Umsetzung von explainable AI-Verfahren sowie den Bereich Hyperautomation. Innerhalb des Projektes PIMKoWe hat sich Lukas-Valentin Herm mit der Erhebung der Anforderungsanalyse, der Blockchain-Implementierung sowie der Ableitung und Implementierung der Eventarchitektur befasst.

Dr. Julian Kolb promovierte am Lehrstuhl für BWL und Wirtschaftsinformatik zum Thema Referenzarchitekturen für Blockchain-Anwendungen in Wertschöpfungsnetzwerken. Im Rahmen seiner Dissertation hat Dr. Kolb den Einsatz von Blockchain-Technologie in der interorganisatorischen Zusammenarbeit zwischen Unternehmen untersucht und dabei insbesondere betriebswirtschaftliche IT-Systeminfrastrukturen von Unternehmen berücksichtigt. Herr Kolb unterstützte das Projekt PIMKoWe fast über die gesamte Projektlaufzeit von der Antragsstellung bis zu den letzten Arbeiten im Projektkonsortium und übernahm in der Anfangsphase zudem die Rolle des Projektleiters und koordinierte insbesondere die Zusammenarbeit mit dem Projektträger. Nach Abschluss seiner Promotion widmet sich Herr Dr. Kolb dem Wissenstransfer und unterstützt Unternehmen beim Aufbau ihrer Digitalisierungsstrategie.

Dr. Adrian Hofmann war wissenschaftlicher Mitarbeiter am Lehrstuhl für BWL und Wirtschaftsinformatik der Universität Würzburg. In seiner Forschung beschäftigte er sich mit datengetriebenen Lösungen zu Problemen in den Bereichen Geschäftsprozessmanagement und Unternehmenssoftware. Zudem untersuchte er, wie sich Unternehmen durch neue Technologien wie maschinelles Lernen und Blockchain verändern. In diesem Zuge widmete er sich innerhalb des Projektes PIMKoWe der Implementierung der Blockchain sowie der Forschung innerhalb dieses Gebietes. Inzwischen ist Herr Dr. Hofmann Gründer und CTO der Firma Paxray GmbH.

Michael Baumgart ist Senior R&D Engineer bei Infosim®, einem internationalen IT-Unternehmen mit Hauptsitz in Würzburg. Als M.Sc. in Informatik mit dem Schwerpunkt Intelligente Systeme liegt sein primärer Fokus in der Forschung auf Maschinellem Lernen, anderen Teilbereichen der Künstlichen Intelligenz und Systemen der Industrie 4.0. Seine entwicklungsseitigen Schwerpunkte sind das Implementieren von Schnittstellen, die Kommunikation zwischen Anwendungen und die Entwicklung von (Web-)Plattformen. Im Rahmen des PIMKoWe-Projekts hat Michael Baumgart als Experte für die Infosim-Software StableNet® Blockchainsysteme und die Anbindung von Komponenten fungiert und in dieser Rolle unter anderem eine Anbindung von Blockchainplattformen an StableNet® und weitere Komponenten der PIMKoWe-Plattform ermöglicht.

Oliver Stübs leitet das Circular Innovation Lab von Infosim®, aus dem Kompetenzen und Ergebnisse aus Innovationsprojekten in neuartige Softwarelösungen für die Kreislaufwirtschaft in der verarbeitenden Industrie überführt werden. Er studierte Volkswirtschaft am Karlsruher Institut für Technologie (KIT) und war anschließend in der Kunststoffindustrie tätig. Dort hat er ein auf Nachhaltigkeit in der Kunststoffverarbeitung fokussiertes Geschäftsfeld aufgebaut und zahlreiche Innovationsprojekte auf diesem Gebiet durchgeführt. Im Projekt PIMKoWe befasste er sich neben der Projektleitung seitens Infosim mit den Themen dezentrale Plattformen und Datenaustausch.

Dr. David Hock ist Director of Research der Infosim® Gruppe und koordiniert die Forschungsaktivitäten unternehmensübergreifend. Zuvor studierte er Informatik und Mathematik an der Universität Würzburg und an der BTH in Karlskrona, Schweden, und war als wissenschaftlicher Mitarbeiter am Lehrstuhl für Kommunikations-netze am Institut für Informatik in Würzburg tätig. Seine aktuellen Forschungsschwerpunkte liegen auf dem Automated Network und Service Management in Kombination mit vielen angrenzenden Themenfeldern wie (Industrial) IoT, 5G & 6G, Machine Learning/Artificial Intelligence sowie neuartigen Technologien wie Quantenkommunikation und Quantum Key Distribution (QKD). Im Projekt PIMKoWe beteiligte sich David Hock neben der anfänglichen Projektleitung seitens Infosim inhaltlich an mehreren Arbeitspaketen, insbesondere auch im Kontext der Einbindung von Ansätzen aus dem Network Management.

Dr. Michael Kröhn ist Leiter Forschung und Entwicklung bei ROBUR Automation GmbH. In dieser Funktion befasst er sich mit Themen des maschinellen Lernens und dem industriellen Internet der Dinge. Letzteres ist zunehmend auch geprägt von Aspekten der Transparenz und Manipulationssicherheit. Im Projekt PIMKoWe übernimmt ROBUR Automation daher die Rolle des Anwendungspartners, der Branchenwissen einbringt und erarbeitete Lösungen testet, kritisch überprüft und Optimierungen mitgestaltet.

Timotheus Kampik ist Principal Scienctist in Residence bei der SAP Signavio. Timotheus Kampik beschäftigt sich in enger Zusammenarbeit mit akademischen Partnern, mit forschungsgetriebenen Innovationen. Im Zuge der Zusammenarbeit am PIMKoWe-Projekt hat sich Timotheus mit Signavio um die prozessorientierte Perspektive gekümmert. Beispiele von Innovationen, die von SAP Signavio teils als Prototypen und teils als skalierbare Erweiterungen der SAP Signavio Business Transformation Suite entwickelt wurden, sind die SiGNAL Query Language für die prozessgetriebene Analyse von Daten, ein Tool zur testgetriebenen und prozessorientierten Entwicklung von sogenannten "Smart Contracts", die organisationsübergreifende Geschäftsregelausführung ermöglichen, und eine Entwicklungs-pipeline, die das Deployment von Prototypen organisations-übergreifend in Prozessanalyseumgebungen ermöglicht.

Matthias Keil studierte an der Technischen Universität Berlin Maschinenbau mit der Fachrichtung Konstruktionstechnik. Nach seiner Zeit als wissenschaftlicher Mitarbeiter am damaligen Institut für Schwingungslehre und Maschinendynamik der TU Berlin, sammelte er bei der Maul-Theet GmbH, einem Ingenieurbüro für Schwingungs-technik, Erfahrungen im Bereich der Soft- und Hardwareentwicklung auf allen Gebieten der Strukturdynamik. Bis heute ist er als leitender Ingenieur für die Maul-Theet GmbH im Bereich Entwicklung, Design und Konstruktion von Messsystemkomponeten tätig und verantwortlich für das Prototyping sowie für die Beschaffung von Zukaufteilen. Herr Keil war im Rahmen des PIMKoWe-Projektes beratend tätig und führte Qualitätstests an der entwickelnden Plattform durch.

Leif Ole Jankowski ist Junior Solution Architect bei der ACTIWARE Development GmbH. Er besitzt einen B.Sc. in Softwaretechnik. Seine Bachelorarbeit behandelte das Thema der Vertrauensbildung mithilfe der Blockchain in teilautomatisierten Prozessen. Sein Projektfokus war die Integration der gewählten Blockchain in die ACTIWARE.io Plattform und die Anpassung der Plattform zur Abbildung der Supply-Chain off- und onchain.

Dr. Patrick Bredebach ist Produktmanager bei der ACTIWARE Development GmbH. Er hält einen M.A. in Ökonomie und Management und hat u.a. zu Qualitätsmanagement und zur Integration sowie Anwendung von Qualitätsmanagement im Kontext von Industrie 4.0 veröffentlicht. Seit 2020 hat er u.a. zwei Teilprojekte zur Integration von Blockchain und insbesondere von Smart Contracts zur Sicherung von Lieferketten und zur Rückverfolgbarkeit in Unternehmen geleitet.

Kurzbeschreibung PIMKoWe

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Einerseits führen Skaleneffekte und leistungsfähigere Informations- und Kommunikationstechnologie zu einer zunehmenden Spezialisierung der Wertschöpfung. Andererseits begünstigt die Verfügbarkeit unterschiedlicher Systeme, Standards und Protokolle die Entstehung fragmentierter und heterogener IT-Infrastrukturen, sodass der automatisierte Austausch relevanter Informationen erschwert wird und häufig bilateral verhandelte Vereinbarungen voraussetzt. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen. Zur Realisierung dieser Potenziale bedarf es ganzheitlicher Lösungen, die dezentrale Aktivitäten innerhalb von Wertschöpfungsnetzwerken koordinieren und Mechanismen für die überbetriebliche Kommunikation, Kollaboration und Optimierung bereitstellen.

Das Verbundprojekt „Plattform für das integrierte Management von Kollaborationen in Wertschöpfungsnetzwerken“ (PIMKoWe) adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet wird. Die dabei entstehende Plattform ermöglicht die zentrale Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU. Ausgehend vom State of the Art in den Bereichen Wirtschaft, Technologie und Forschung erfolgten die Konzeption und Implementierung der Plattform entlang verschiedener Anwendungsszenarien, die typische Problemstellungen des deutschen Mittelstandes abbilden. Hierbei wurden die Realisierbarkeit und der wirtschaftliche Nutzen der Lösung demonstriert und ein optimaler Ausgangspunkt für den Transfer auf andere Branchen und Wirtschaftszweige hergestellt.

Möglich wurde die Umsetzung durch die Kombination wissenschaftlicher Methoden und technischer Lösungsansätze in bisher unbekannter Form. Auf wissenschaftlicher Ebene folgten die Konzeption und Entwicklung der Methode des Service Engineering, die alle Aktivitäten zur Bestimmung und Realisierung von Funktionen, Merkmalen und Qualitätsanforderungen von Dienstleistung unterstützt. Ein besonderer Fokus lag dabei auf der Optimierung von Strukturen und Abläufen, um eine größtmögliche Servicequalität bei geringstmöglichen Kosten zu gewährleisten. Dies förderte die Adoption der Plattform durch potenzielle Anwenderunternehmen, stärkte deren wirtschaftlichen Mehrwert und resultierte in einer langfristigen Weiterentwicklung und Bereitstellung. Auf technischer Ebene wurde eine Blockchain implementiert, die eine vertrauensvolle Datenhaltung und -verarbeitung ermöglicht und dabei Skalierbarkeit, Leistungsfähigkeit und Transparenz sicherstellt. Weitere technische Lösungskomponenten umfassen adaptive Schnittstellen zu etablierter Unternehmenssoftware sowie eine Cloud-basierte Plattform, die alle Funktionalitäten und Merkmale unter Einhaltung höchster Anforderungen an Datenschutz und Datensicherheit bündelten und für KMU bereitstellt. Zur Abwicklung von Transaktionen über Blockchain-basierte Smart Contracts wurden betriebswirtschaftliche Anforderungen von Marktteilnehmern erfasst und in eine einheitliche Referenzdatenstruktur übertragen. Innovative Analysemethoden aus den Bereichen Operational Business Intelligence und Advanced Analytics ermöglichten es zudem, historische Transaktionen und Echtzeitereignisse auszuwerten und zur Identifikation von Optimierungspotenzialen zu nutzen. Diversifizierte und kontinuierlich in das Projekt integrierte Praxispartner begleiteten die Entwicklung der Plattformlösung und evaluierten die entsprechenden Funktionalitäten mit den eigenen Anforderungen.

Verzeichnis der Arbeitspakete

Projektmanagement (Arbeitspaket A)

Im nachfolgenden Abschnitt wird das Arbeitspaket Projekt-management dargestellt. Ebenso erfolgt eine Darstellung der damit verbundenen Arbeitspakete, um eine holistische Betrachtung des Projekts zu ermöglichen.

1 Vorgehen innerhalb des Projektes

Ziel des Forschungsprojektes PIMKoWe ist die Entwicklung und Bereitstellung einer Plattformlösung zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in internationalen Wertschöpfungsnetzwerken. Um dies zu erreichen, wurde ein iteratives Vorgehen angewendet, welches durch ein konstantes Projektmanagement (AP A) umgesetzt wurde. Dies umfasst die Anforderungsanalyse (AP B), die Konzeption der Plattform (AP C), die Realisierung der Plattform (AP D), die Evaluierung der Ergebnisse (AP E) sowie die konstant durchgeführte Dissemination (AP F). Diese Umsetzung wird der Abbildung A.1 dargestellt und im Folgenden beschrieben.

2 Anforderungsanalyse (AP B)

Die Anforderungsanalyse besteht aus insgesamt sechs Teilarbeitspaketen.

In *Teilarbeitspaket B1: Identifikation von Anspruchsgruppen* wurden alle Akteure und Stakeholder identifiziert, die sich im Einflussbereich der durch die Plattform bereitgestellten Dienstleistung befinden. Neben staatlichen Institutionen, denen insbesondere eine regulierende Rolle zukommt, sind dies potenzielle Betreiber und Anwender der Plattform.

Anschließend wird die Anforderungsanalyse in *Teilarbeitspaket B2: Empirische Studien zur Anforderungserhebung* initiiert. Diese folgte durch ein dreistufiges Vorgehen. Zuerst wurden detaillierte Vorstudien bei den Praxispartnern des Projektkonsortiums durchgeführt. Die dabei erhobenen Anforderungen wurden im Rahmen von Anwendungsszenarien verarbeitet und dienen im weiteren Verlauf der Evaluation der Projektergebnisse. Im zweiten Schritt wurde der diversifizierte Projektbeirat durch mehrere semi-strukturelle Interviews integriert. Hierbei wurden insbesondere Anforderungen aus weiteren Branchen erhoben. Abschließend wurden in Kooperation mit den Multiplikatoren des Verbundprojekts weitere potenzielle Unternehmen identifiziert und befragt.

Im Rahmen des dritten *Teilarbeitspakets B3: Klassifikation von Muss-, Wunsch- und Abgrenzungskriterien* wurden die erhobenen Anforderungen hinsichtlich ihrer Bedeutung für den nachhaltigen Erfolg der Plattform analysiert. Hierbei verwendete das Projektkonsortium wissenschaftliche Methoden zur Analyse qualitativer und quantitativer Daten, um eine möglichst rigorose und nachvollziehbare Klassifikation zu gewährleisten. Daraus resultierende Musskriterien waren von primärer Bedeutung und wurden durch den entwickelten Plattformdemonstrator adressiert. Abschließend konstituierten Abgrenzungskriterien Eigenschaften und Problemstellungen, die durch die Plattform vermieden werden mussten.

Eine Integration und formale Festsetzung von Anforderungen erfolgte im *Teilarbeitspaket B4: Erstellung des Pflichtenhefts*. Hierbei handelte es sich um eine Dokumentation und Systematisierung der Gesamtheit der Anforderungen aller Anspruchsgruppen an die Lieferungen und Leistungen des Projektkonsortiums. Diese wurden dabei so allgemein wie möglich und so einschränkend wie nötig formuliert, sodass die Projektpartner über genügend Freiheitsgrade verfügen, um optimale Lösungen für die einzelnen Problemstellungen zu erarbeiten, ohne durch zu konkrete Anforderungen in ihrer Lösungskompetenz eingeschränkt zu werden.

Zur Sicherstellung der langfristigen Wirtschaftlichkeit der Plattform wurde die Entwicklung nachhaltiger Betreiber- und Gebührenmodelle im *Teilarbeitspaket B5: Analyse von Betreiber- und Gebührenmodellen* fokussiert. Im Rahmen eines integrierten Geschäftsmodells sollten Einnahmequellen, Kostentreiber, strategische Partner, adressierte Kundensegmente und weitere Aspekte identifiziert werden. Gleichzeitig müssen die festgesetzten Rahmenbedingungen kontinuierlich mit den erhobenen Anforderungen der Anspruchsgruppen abgeglichen werden, um die Verwendung der Plattform zu fördern.

Abschließend wurden Aspekte des Datenschutzes und der Datensicherheit im *Teilarbeitspaket B6: Analyse von Anforderungen hinsichtlich Datenschutzes und -sicherheit* besonders fokussiert. Hierbei wurden die Implikationen des theoretischen Privacy-Calculus-Modells instrumentalisiert, welches eine Korrelation zwischen Bereitschaft zur Bereitstellung sensibler Daten durch Nutzer und dem wahrgenommenen Mehrwert einer Dienst-

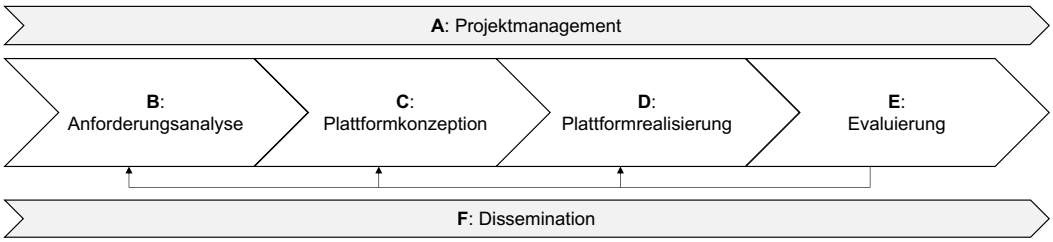


Abbildung A.1: Projektübersicht der Arbeitspakete A bis F

leistung herstellt. Vor der Initiierung der Plattformkonzeption war es folglich notwendig, etwaige Anforderungen hinsichtlich Datenschutzes und Datensicherheit zu erheben, um die Mindestanforderungen der Plattformlösung zu determinieren.

3 Plattformkonzeption (AP C)

Das Arbeitspaket umfasst insgesamt sechs Teilarbeitspakete.
Im Rahmen von *Teilarbeitspaket C1: Konzeption der Plattformarchitektur* wurden die Grundkomponenten der anvisierten Plattformlösung durch ein Mehrschichtenmodell skizziert. Die Architektur setzt sich allgemein aus einer Daten-, Applikations-, Business- und Anwenderschicht zusammen. Auf Basis der Architektur konnte die Komplexität der Problemstellung reduziert und etwaige funktionale und nicht-funktionale Anforderungen sowie technische und organisatorische Einflussfaktoren berücksichtigt werden. Weiterhin dient die Plattformarchitektur der Organisation von Lösungsideen und technischen Konzepten, unterstützt Entwurfsentscheidungen und erlaubt eine frühzeitige Integration von Qualitätsanforderungen wie Ausfallsicherheit, Zusammenspiel verteilter Systemkomponenten, Richtigkeit, Effizienz und Flexibilität.
Die Konzeption der Blockchain-Lösung wurde in *Teilarbeitspaket C2: Konzeption der Blockchain* fokussiert. Hierbei wurden sowohl technische Modelle als auch Datenmodelle abgeleitet und in eine Entwicklungsumgebung transferiert. Technische Aspekte dienten insbesondere der Gewährleistung einer ausreichenden Datensicherheit durch die Selektion eines asymmetrischen kryptographischen Verfahrens. Das Datenmodell musste weiterhin die effiziente Strukturierung betriebswirtschaftlicher Informationen erlauben und diese für Transaktionen nutzbar machen.
In *Teilarbeitspaket C3: Klassifikation betriebswirtschaftlicher Informationen* erfolgte die Analyse handelsüblicher Informationssysteme. Hierbei wurden die Datenstrukturen von ERP-Systemen untersucht, die bei der Mehrzahl deutscher KMU zum Einsatz kommen. Durch die Erstellung von Mapping-Tabellen konnten unterschiedliche Datenanforderungen abgeglichen und zu einem Meta-Standard zusammengeführt werden. Der Meta-Standard diente anschließend der Entwicklung adaptiver Plattformschnittstellen, die einen bidirektionalen Austausch von Daten zwischen ERP-Systemen und Plattform ermöglichen.
Zur Automatisierung von Transaktionen wurde die Entwicklung von Smart Contracts in *Teilarbeitspaket C4: Konzeption von Smart Contracts* fokussiert. In Abstimmung mit den Aktivitäten der Teilarbeitspakete C2 und C3 wurden hierbei programmierbare Vereinbarungen konzipiert, die eine Prüfung betriebswirtschaftlicher Daten ermöglichen und auf der Blockchain gespeichert werden. Hierbei können z. B. produktspezifische Anforderungen eines Marktakteurs mit den Eigenschaften von Produkten eines Produzenten automatisiert abgeglichen werden. Bei Übereinstimmung erlaubten Smart Contracts weiterhin die automatische Durchführung darauf aufbauender Transkationen.
Die Aktivitäten des *Teilarbeitspakets C5: Konzeption der Architektur für Echtzeitverarbeitung* adressierte die Bereitstellung von Plattformfunktionalitäten zur Echtzeitverarbeitung von Informationen. Hierbei wurden sowohl potenzielle Datenquellen wie Datenbanksysteme, Enterprise Service Bus, Log-Daten oder Prozessdaten, identifiziert, als auch Mechanismen zur Filterung, Korrelation und Aggregation dieser entwickelt werden. Die Complex-Event-Processing-Architektur ermöglichte es der Plattform, voneinander abhängige Ereignisse kontinuierlich und zeitnah zu erkennen, analysieren, gruppieren und verarbeiten sowie damit verbundene Aktivitäten zu initiieren.
Abschließend dient das *Teilarbeitspaket C6: Simulator als Proof of Concept* der Überprüfung der Machbarkeit, Kompatibilität und Anforderungskonformität der Plattformkomponenten. Hierbei wurden die Komponenten im Rahmen eines Simulators implementiert sowie die daraus entstehenden Ergebnisse evaluiert.

4 Plattformimplementierung (AP D)

Das Arbeitspaket setzt sich aus insgesamt sieben Teilarbeitspaketen zusammen.
Die Teilarbeitspakete D1 bis D5 verlaufen weitestgehend parallel und bauen auf den Ergebnissen des Arbeitspakets C auf. So wurden die in der Simulation verarbeiteten Komponenten in einen integrierten Plattformdemonstrator überführt. Dies erforderte die *Implementierung der Blockchain (D1)* sowie die *Implementierung von Smart Contracts (D2)*. Darauf aufbauend konnten die entwickelten Smart Contracts auf der Blockchain umgesetzt werden, die eine *Automatisierung von Transaktionen* ermöglichen (D3).
Darüber hinaus galt es, die konzipierte ereignisgesteuerte Architektur auf der Plattform zu implementieren, um die *Echtzeitverarbeitung von Informationen* zu gewährleisten (D4). Weiterhin erfolgte die *Realisierung des Front-Ends,* um die User Experience zu optimieren (D5). Daraus resultierte ein integrierter und vollständig *funktionsfähiger Plattformdemonstrator* zur Koordination und Unterstützung von Kollaborationen in Wertschöpfungsnetzwerken (D6).
Während die Machbarkeit durch die Proof-of-Concept-Lösung bereits initial überprüft wurde, induzierte der Transfer in eine Produktivumgebung

neue Anforderungen. Exemplarisch bedarf es der Selektion eines adäquaten Zugangskanals, über welchen die Plattform für KMU bereitgestellt werden sollte. Die Entscheidung wurde durch zahlreiche Parameter, wie z. B. Datenschutz und Datensicherheit, beeinflusst. Aufgrund der hohen Skalierbarkeit und des geringen nutzerseitigen Implementierungsaufwands wurde eine Lösung fokussiert, die über handelsübliche Webbrowser aufgerufen werden kann. Die Spezifikation nutzerseitiger Zugangspunkte war notwendig, um die Peer-to-Peer-Struktur und Dezentralität der Plattform zu untermauern. Abschließend galt es, die nahtlose Integration der Teilkomponenten sicherzustellen, sodass der Plattformdemonstrator in seiner Gesamtheit produktiv einsetzbar ist.

Neben der Implementierung und Integration der Teilkomponenten wurde die Umsetzung anforderungsgerechter Mechanismen für Datenschutz und Datensicherheit in *Teilarbeitspaket D7: Datenschutz, Datensicherheit und Zertifizierung* fokussiert. Durch die Integration überbetrieblicher Prozesse und Datenfundamente kam es zum unternehmensübergreifenden Austausch sensibler Informationen über betriebswirtschaftliche Kennzahlen und Produkte. Diese Informationen konnten als Indikatoren für den wirtschaftlichen Erfolg eines anderen Unternehmens instrumentalisiert werden, sodass potenziell weitreichende Risiken hätten entstehen können. Dementsprechend galt es, klare Richtlinien für die Datenverarbeitung zu definieren, die während der Abwicklung von Smart Contracts beachtet werden müssen. Weiterhin war die Umsetzung kryptographischer Verfahren notwendig, die eine Verschlüsselung von Daten und Ergebnissen gewährleisteten und vor unbefugtem Zugriff sowie weiterführenden Analysen schützen sollten. Mit dem Ziel, böswillige Akteure von der Partizipation auszuschließen, mussten klare Kriterien festgelegt werden, die den Zugang zur Plattform einschränken und Unternehmen eindeutig und rechtlich bindend identifizieren und zertifizieren. Neben der Festlegung von Regularien hinsichtlich des Erhalts und der Verwendung auf der Plattform verarbeiteter Informationen galt es insbesondere, notwendige Beschränkungen für den Datenaustausch zu definieren. Der Austausch transaktionaler Daten erfolgte hierbei gemäß dem Schlüssel-Schloss-Prinzip.

Da die Plattform einen neuartigen Lösungsansatz für eine bedeutende Problemstellung darstellt, konnten innovative und disruptive Geschäftsmodelle entstehen, die auf ihren Funktionalitäten aufbauen. Diese sind sowohl für die Diffusion der Plattform als auch für die Digitalisierung des Industriestandorts Deutschland von hoher Bedeutung und erforderten die Entwicklung effektiver Methoden für das Management von Geschäftsmodellen in *Teilarbeitspaket D8: Geschäftsmodellanalyse- und Management*. Dies beinhaltete neben der Identifikation und Analyse, vor allem die Förderung innovativer Geschäftsmodellideen.

5 Evaluation (AP E)

Zur Integration der KMU-Praxispartner in das Gesamtprojekt wurden in *Teilarbeitspaket E1: Use-Case-Umsetzung und Evaluation* für den deutschen Mittelstand typische Anwendungsszenarien entwickelt, die ein möglichst breites Spektrum praxisrelevanter Anforderungen, Nutzungsszenarien und Herausforderungen abdecken sollten. Mit Hilfe der Anwendungsszenarien wurden die einzelnen Bausteine der Plattform praxisorientiert evaluiert, um Aufschluss über notwendige Anpassungen zu geben.

Hierbei erfolgte die Evaluation des Plattformdemonstrators unter Berücksichtigung der unternehmensspezifischen Zielsysteme, sodass eine realistische Einschätzung über dessen Mehrwert und Leistungsfähigkeit generiert werden konnte. Die Untersuchung verlief entlang verschiedener, standardisierter Evaluationskriterien, die unter Zuhilfenahme wissenschaftlicher Methoden konzipiert wurde. Dadurch konnten die Vergleichbarkeit der Ergebnisse gewährleistet und zielführende Schlussfolgerungen getroffen werden. Die Evaluationskriterien umfassten den Grad der Zielerfüllung in Bezug auf die durch den jeweiligen Use Case skizzierte Problemstellung. Abschließend galt es festzustellen, inwieweit die Performance der Plattform mit den Anforderungen der Praxisunternehmen übereinstimmt.

Neben diesen funktionalen Eigenschaften lag ein spezieller Fokus auf der wahrgenommenen Datensicherheit sowie der Angemessenheit der Zertifizierungsmechanismen. Hierbei wurde festgestellt, inwieweit die bereitgestellten Mechanismen einen positiven Einfluss auf die wahrgenommene Sicherheit der Plattform haben oder ob zu restriktive Verfahren ihre Nützlichkeit reduzieren. Dementsprechend wurde es als zielführend angesehen, die erarbeiteten Betreiber- und Gebührenmodelle erst nach initialer Nutzung zu evaluieren. Weiterhin wurde die Usability der Plattform durch verschiedene Methoden, wie Interviews und Fragebögen, mit verschiedenen Mitarbeitern der Praxispartner überprüft.

Zusätzlich zur Evaluation mit den Praxispartnern des Projektkonsortiums wurde die Generalisierbarkeit der Dienstleistung auf andere Unternehmen und Branchen in *Teilarbeitspakete E2: Evaluation der Übertragbarkeit* evaluiert. Zu diesem Zweck wurden mehrere Studien und Workshops mit den Unternehmen durchgeführt. Weiterhin

wurden die Projektergebnisse bereits früh auf Informationsveranstaltungen der zahlreichen Multiplikatoren beworben, sodass weitere interessierte Anwenderunternehmen identifiziert werden konnten, die anschließend in die Studie integriert wurden. Dies erfolgte unter der Zielsetzung, notwendige Adaptionen für unterschiedliche Branchen zu identifizieren und in Bezug auf ihre Komplexität zu klassifizieren.

6 Dissemination (AP F)

Um die Ergebnisse wissenschaftlich-orientierter Aktivitäten für die entsprechende Community zugänglich zu machen, wurden wissenschaftliche Publikationen veröffentlicht und in Fachkreisen präsentiert. Zur Bekanntmachung der Plattform wurden potenzielle Nutzer im Rahmen von praxisorientierten Workshops und Multiplikatoren-Events über den gesamten Projektverlauf hinweg informiert. Zur Sicherstellung der Wissensdiffusion sowie zur Generierung von Netzwerkeffekten wurde zu Projektbeginn eine Projektwebseite entwickelt (https://projekt-pimkowe.de) und kontinuierlich mit Ergebnissen abgeschlossener Arbeitspakete aktualisiert. Daraus resultierend konnten Interessenten und Anwenderunternehmen Informationen in Bezug auf die Plattform finden und den aktuellen Stand des Projekts verfolgen. Schlussendlich haben Projektpartner die erarbeiteten Ergebnisse kontinuierlich auf Messen und Branchentreffen vorgestellt und praxisnah demonstriert, um die Anforderungskonformität der Lösung zu überprüfen.

– Inhaltsverzeichnis Arbeitspaket B –

Das Arbeitspaket (AP) B umfasst die Anforderungsanalyse der verschiedenen Anspruchsgruppen, um eine direkte Förderung der überbetrieblichen Integration zu ermöglichen. Die summative Betrachtung stellt hierbei die wissenschaftliche Ausgangsbasis für die Plattformkonzeption (AP C) dar. Dies teilt sich folgende auf:

B1 & B2 Empirische Studie zur Anforderungserhebung. Diese Teilarbeitspakete (TAP) umfassen zum einen eine Vorabidentifikation der Anspruchsgruppen (B1) an eine Blockchain-basierte Plattform und zum anderen die Erhebung konkreter Anforderungen für die Anspruchsgruppen (B2).

B3 & B4 Pflichtenheft: Klassifikation in Muss-, Wunsch- und Abgrenzungskriterien. Die erhobenen Anforderungen werden anschließend klassifiziert sowie in Muss-, Wunsch-, und Abgrenzungskriterien und in ein Pflichtenheft überführt. Das Pflichtheft dient als Datengrundlage der verschiedenen Konsortialspartner.

B5 Analyse von Betreiber- und Gebührenmodellen für Blockchain-basierte Plattformen. Dieses AP leitet ein Betreiber- und Gebührenmodell ab, um eine langfristige Wirtschaftlichkeit der Plattform zu ermöglichen. Hierdurch wird die Transferierbarkeit in die betriebliche Praxis gewährleistet.

B6 Analyse von Anforderungen hinsichtlich Datenschutz und -sicherheit. Dieses AP teilt sich in drei Bereiche auf: *1)* Die Betrachtung der Vereinbarkeit zwischen der Blockchain-Technologie und dem Datenschutz (B6.1). *2)* Der Herleitung eines Privacy-Calculus-Modells (B6.2) zur Kosten-Nutzen-Rechnung der Blockchain-Technologie. *3)* Erweiterung der Anforderungsanalyse zur Abbildung aktueller Entwicklungen durch eine gezielte Betrachtung der Aspekte Datenschutz, Datensicherheit und Zertifikate (B6.3).

B1 & B2: Empirische Studien zur Anforderungserhebung

Im folgenden Arbeitsbericht werden die Vorgehensweise und die Ergebnisse der Anforderungsanalyse vorgestellt. Aufgrund einer vorhergegangenen Literaturanalyse wurden bereits erste Anforderungen definiert, die nun anhand von einer Interviewstudie mit Partnern aus dem Projektkonsortium und dem Projektbeirat konkretisiert und ergänzt wurden. Das Ergebnis sind 45 Anforderungen, die die Stakeholder an eine Blockchain-basierte Kollaborationsplattform in einem Supply-Network haben.

1 Darstellung der Interviewstudie

Das folgende Kapitel beschreibt zunächst die Entwicklung der Experteninterviews. Um eine Entwicklung durchführen zu können, ist es zuerst notwendig, relevante Anspruchsgruppen ausfindig zu machen. Anhand dieser Anspruchsgruppen werden anschließend in dem Kapitel 3.1 die Experteninterviews erhoben.

Vorgehen anhand der Forschungsmethodik

Auf Grund der hohen praktischen Relevanz für Unternehmen, eine Blockchain-basierte Kollaborationsplattform in ihrem Wertschöpfungsnetzwerk zu integrieren, sollen diese Unternehmen ebenso zu dieser Thematik befragt werden. Diese Befragung soll mittels einer qualitativen Querschnittsanalyse erfolgen. Bei dieser Methodik werden verschiedene Personen zu einer Thematik befragt und anschließend ein Querschnittsbild der ausgewerteten Daten erstellt (Wilde und Hess 2007, 282).

Anhand dieses Verfahrens können mehrere Untersuchungsfälle zur Erkennung eines Gesamtkonzeptes, der Kollaborationsplattform, entstehen. Als anzuwendende Methodik können verschiedene Techniken angewandt werden. Nach Wilde und Hess (2007, 282) sind dies z.B. Fragebögen oder Experteninterviews. Auf Grund der Komplexität der Forschungsfrage werden Experteninterviews angewendet. Ebenso werden die erstellten Fragen für diese Interviewstudie auf Basis von Vorüberlegungen, welche im Zuge einer Literaturanalyse entstanden sind, entwickelt. Ausgangsbasis bilden die erhobenen Dimensionen aus der Literaturanalyse. Nach Paré (2004, 247f.) wird diese Expertenbefragung daher nach einem semi-strukturierten Interview durchgeführt. Bei diesem Interviewtyp sind die Fragen zu einer bestimmten Thematik gestellt, ermöglichen jedoch genug Freiraum in den Antwortmöglichkeiten der befragten Personen, um keinerlei Gedankengänge auszuschließen. Die Identifikation von Kausalitäten und damit Reduktion auf Kernaspekte innerhalb der Ergebnisse der Befragungen erfolgt erst bei der Datenauswertung (Gläser und Laudel 2010, 26f.).

Unterteilung der Interviews in Anspruchsgruppen

Relevanz von Anspruchsgruppen. Die Definition von Anspruchsgruppen bzw. Interessengruppen leitet sich aus dem englischen Begriff „Stakeholder“ ab und wird meist von Edward Freeman unter folgender Definition verwendet:

„[..] any group or individual who can affect or is affected by the achievement of the organization's objectives“ (Freeman 2010, 46)

Dabei definiert Freeman eine Anspruchsgruppe als einen aktiven Beeinflusser bzw. ein Individuum oder eine Gruppe, welche unmittelbar beeinflusst wird. Durch diese direkte Beeinflussung der Anspruchsgruppen zu operierenden Unternehmen, sind diese Unternehmen von verschiedenen Anspruchsgruppen abhängig. Die Anpassungsfähigkeit an die Anforderungen der Anspruchsgruppen trägt damit maßgeblich zu dem Erfolg eines Unternehmens bei (Elias et al. 2002, 303). Dies gilt ebenso für die Implementierung von Informationssystemen, da der Erfolg einer Implementierung nicht mehr nur von technischen, sondern auch von unternehmerischen Aspekten abhängig ist (Scott et al. 2004, 101; Pouloudi 1999, 1). Nach Paul Nutt, scheiterten bis zum Jahre 2002 ca. 50 Prozent aller Informationssystem-Projekte u.a. aufgrund der fehlenden Erfüllung der Erwartungen der betroffenen Anspruchsgruppen (Nutt 2002, 41ff.). Demnach scheint es essentiell, alle notwendigen Anspruchsgruppen und deren Individuen zu erkennen. Potentielle Anspruchsgruppen sollen im Folgenden durch eine wissenschaftliche Literaturrecherche ausfindig gemacht werden.

Identifizierung von möglichen Anspruchsgruppen. Wie im vorherigen Kapitel beschrieben ist es notwendig, die verschiedenen Anspruchsgruppen bei einer Informationssystems-Implementierung ausfindig zu machen. Um dies für die Anforderungsentwicklung für eine Kollaborationsplattform bei Wertschöpfungsnetzwerken vorzunehmen, wird eine mehrstufige Vorgehensweise eingesetzt. Da es sich bei der Blockchain um eine disruptive Technologie handelt, welche durch ihre Struktur auf verschiedene Intermediäre verzichten kann, müssen bestehende Forschungsbeiträge zur Implementierung von Dienstleistungsplattformen kritisch betrachtet werden. Ausgangsbasis ist zu Beginn der Forschungsbeitrag von Riedl et al. (2009, 6f.). In diesem Beitrag werden vier verschiedene Anspruchsgruppen an eine Dienstleistungsplattform bzw. Dienstleistungsumgebung herausgearbeitet. Diese sind Kunde, Plattform-Provider, Dienstleistungs-Provider sowie ein Vermittler. Der Kunde nutzt verschiedene Dienstleistungen, welche durch den Dienstleistungs-Provider auf der Plattform zur Verfügung gestellt werden. Die Entwicklung der Plattform sowie Bereitstellung der Infrastruktur erfolgt durch den Plattform-Provider. Der Vermittler bringt den Kunden sowie die Dienstleistungsplattform zusammen. Diese Anspruchsgruppen sind bei Dienstleistungs-plattformen im SCM ebenfalls vorhanden. So beschreiben die Autoren Barros und Kylau (2011, 49ff.) ein Framework, welches Anspruchsgruppen wie Kunden, Dienstleistungs-Provider sowie einen

Im Bereich von Blockchain-Anwendungen beschreibt der Forschungsbeitrag von Riasanow et al. (2018, 4–7) die möglichen Rollen, welche sich durch den Einsatz einer Blockchain in verschiedenen Anwendungsszenarien ergeben. Diese wurden anhand einer Untersuchung von 479 Blockchain-Unternehmen erhoben. Hierbei wurden elf verschiedene Anspruchsgruppen festgestellt. Diese Anspruchsgruppen beziehen sich auf die verschiedenen Entwicklungsstufen Blockchain 1.0 bis 3.0. Bei den erfassten Anspruchsgruppen handelt es sich um: Anwender, Blockchain Infrastruktur-Provider, Blockchain Plattform Provider, verschiedene Blockchain Applikations-Provider, Token-basierter Gemeinschaftsplattform-Provider, Schürfer, Schürfer-Equipment-Provider, Blockchain-Entwickler, Blockchain-Anwendergemeinschaft und die verschiedenen Blockchain Beratungen. Jedoch kann eine Person oder ein Knoten innerhalb einer Blockchain mehreren Anspruchsgruppen zugeordnet werden. So können z.B. Anwender auch gleichzeitig Schürfer sein (Riasanow et al. 2018, 7). Ebenso sind manche Anspruchsgruppen je nach Wahl der Blockchain-Umsetzung, wie z. B. Token-basierter Gemeinschaftsplattform-Provider, bei Implementierungen ohne den Einsatz einer Kryptowährung oder Tokens nicht notwendig. Daher werden auf Basis der genannten Forschungsbeiträge weitere Beiträge untersucht. Zusätzlich wird der Forschungsbeitrag von Tönnissen und Teuteberg (2019, 4) herangezogen, welcher bereits verschiedene Anspruchsgruppen anhand von evaluierten Anwendungsszenarien betrachtet.

Auf Basis dessen werden weitere Forschungsbeiträge untersucht und die Anspruchsgruppen angepasst. Um gezielte Forschungsbeiträge im Anwendungsfeld der Blockchain in Wertschöpfungsnetzwerken zu finden, wurden unter anderem Datenbanken wie AISeL oder ScienceDirect dahingehend untersucht. Die herausgearbeiteten Beiträge sind in der Tabelle 1 zu sehen und beschreiben sowohl bereits umgesetzte als auch konzeptionelle Blockchain-Lösungen in Wertschöpfungsnetzwerken. Die Forschungsbeiträge werden im Folgenden prägnant beschrieben und dienen als Grundlage für die Unterteilung der Experten für die Interviewstudie in verschiedene Anspruchsgruppen. Die übergeordneten Anspruchsgruppen wurden zu Beginn durch Beiträge von Riedl et al. (2009, 6f.) unter Einbezug der von Riasanow et al. (2018, 7) Blockchain spezifischen Rollenbezeichnung sowie Einbezug von Voranalysen durch Tönnissen und Teuteberg (2019, 4) erhoben und bei der Betrachtung der in Tabelle B.1-2.1 dargestellten Forschungsbeiträgen angepasst. Durch diese Verknüpfung sollen Anspruchsgruppen identifiziert werden, welche sich an etablierten Rollenmodellen von Dienstleistungsgeschäftsfeldern orientieren und gleichzeitig innerhalb disruptiver

		Anspruchsgruppen											
		Anwender					Plattform-Provider			Dienstleistungs-Provider			Zertifizierungs-Provider
		Kunde	Materiallieferant	Logistik	Produzenten	Verkäufer	Technischer Entwickler	Blockchain-Entwickler	Standard-Entwickler	Blockchain-Administration	Registrierungsverwaltung	Applikations-Provider	Zertifizierungs-Provider
Forschungsbeiträge	*Abeyratne und Monfared 2016*	•		•	•	•		•	•				(•)
	Angrish et al. 2018	•			•		•	•			•	•	•
	Baruffaldi und Sternberg 2018			•			•			•			
	Hancock und Vaizey 2016	•			•			•			•	•	
	Lacity 2018	•	•		•		•	•	•				
	Leng et al. 2018	•	•	•	•	•		•	•			•	
	Wang et al. 2017	•		•	•			•		•	(•)	(•)	•
	Toyoda et al. 2017	•	•	•	•	•		•	•	•	(•)	(•)	
	Saberi et al. 2019	•	•	•	•	•		•	•		•	•	•
	Xu et al. 2019b	•	•		•	•	•	•		•	•	•	•

Tabelle B.1-2.1: Einteilung von Anspruchsgruppen anhand verschiedener Forschungsbeiträge

Wertschöpfungsnetzwerken angewendet werden können.

Die Forschungsbeiträge aus Tabelle B.1-2.1 werden im Folgenden beschrieben. Die Autoren Abeyratne und Monfared (2016, 4–6) präsentieren in ihrem Forschungsbeitrag einen bereits umgesetzten Einsatz der Blockchain im SCM. Verschiedene Anwender nutzen die Blockchain zum Speichern und Aufrufen von Transaktionen sowie gespeicherten IoT-Sensorwerten aus verschiedenen Produktionsstufen. Bei dieser Implementierung handelt es sich um eine öffentliche Blockchain, welche durch einen Blockchain-Entwickler sowie einer Rolle, welche für die Definition von Datenaustausch-Standards zuständig ist, umgesetzt wird. Auf Grund der öffentlichen Blockchain wird kein Dienstleistungs-Provider benötigt, da die Erstellung von Smart Contracts dezentral erfolgt und damit keine Notwendigkeit einer Rechteverwaltung wie bei einer privaten oder Konsortial-Blockchain besteht. Laut Abeyratne und Monfared (2016, 6) ist bisher keine Schnittstelle für Zertifizierungs-Provider implementiert, soll aber zukünftig erfolgen. Ebenso stellen Leng et al. (2018, 642–646) eine öffentliche Blockchain vor, welche zur Überwachung von Lebensmitteln dient. Bei dieser Blockchain müssen alle Beteiligten innerhalb der Lieferantenkette ihre Prozessdaten speichern. Durch unabhängige Dienstleistungs-Provider werden Smart Contracts und Applikationen für die Plattform und Kunden entwickelt. Die Entwicklung der Kollaborationsplattform sowie von notwendigen Datenstandards erfolgt durch einen Blockchain-Entwickler. Die Autorin Lacity (2018, 209–211) beschreibt eine Blockchain für Hersteller im Bereich additiver Fertigung, welche für verschiedene Anwender gedacht ist. Die Implementierung, also die Bereitstellung der Plattform, erfolgt durch ein Unternehmen, welches ebenso die notwendigen Schnittstellen und in Zusammenarbeit mit verschiedenen Organisationen Standards im Bereich additiver Fertigung zur Speicherung in der Blockchain entwickelt. Nach erfolgreicher Implementierung soll dieses Szenario in eine Konsortial-Blockchain umgewandelt werden. Hancock und Vaizey (2016, 56ff.) beschreiben eine private Blockchain-Implementierung auf Basis von Ethereum. Diese Blockchain soll genutzt werden, um die Fälschungssicherheit von Diamanten über eine Blockchain sicherzustellen.
Die Entwicklung wird durch die Firma Everledger durchgeführt, welche auch als Dienstleistungs-Provider z.B. zur Verwaltung von Zugriffsrechten und Entwicklung von Smart Contracts fungiert. Die Plattform dient der Überwachung und damit Rückverfolgbarkeit der Produzenten. Angrish et al. (2018, 1182ff.) beschreiben eine konzeptionelle private Blockchain „FabReg“ auf Basis von Hyperledger Fabric oder Ethereum, welche zur Sicherung von Produktionsdaten genutzt wird. Durch einen Zertifizierungs-Provider wird sichergestellt, dass die Daten der Produzenten vor der Speicherung in der Blockchain korrekt sind. Dadurch kann ein Kunde sich auf die Qualität des Produktes verlassen bzw. diese zurückverfolgen. Ein Dienstleistungs-Provider übernimmt die Entwicklung von Applikationen sowie die Rechteverwaltung. Die Plattform wird durch einen Plattform-Provider zur Verfügung gestellt. Baruffaldi und Sternberg (2018, 3940ff.) beschreiben ein aktuelles Blockchain-Projekt zur transparenten Überwachung von Logistik-Prozessen. In diesem Beitrag werden keine expliziten Rollen genannt, sondern nur auf verschiedene Logistik-Unternehmen, die Blockchain-Entwickler sowie ein Blockchain-Administrator eingegangen. Wang et al. (2017, 72f.) beschreiben eine private Blockchain-Lösung auf Basis der Hyperledger Fabric, die zur Rückverfolgbarkeit in der Anlagenwirtschaft eingesetzt wird. Diese wird verschiedenen Anwendern durch einen Entwickler zur Verfügung gestellt. Die Verwaltung der Plattform soll durch eine Blockchain-Administration erfolgen, welche auch als Registrierungsverwaltung und als Smart-Contracts-Provider verstanden wird. Durch einen Inspekteur (Zertifizierungs-Provider), werden gemietete Kunden durch den Kunden im Nachgang überprüft. Die Autoren Toyoda et al. (2017, 17471f.) beschreiben eine auf Ethereum-basierte private Blockchain zur Speicherung von RFID-Daten eines Supply-Chain-Networks. Auf diese haben verschiedene Anwender Zugriff. Diese Blockchain wird durch einen Plattform-Anbieter entwickelt, welcher auch die Definition von RFID-Austauschformaten vornimmt.
Eine Blockchain-Administration nimmt die Verwaltung der Anwender sowie die Entwicklung von Smart Contracts vor. Saberi et al. (2019, 2121–2125) beschreiben eine private Kollaborationsplattform, auf der verschiedene Anwender am Wertschöpfungsprozess teilnehmen. Durch Rollen wie Registrierungsverwaltung, Standard-Entwickler, Plattform-Entwickler und Zertifizierungs-Provider wird die Verwaltung und Entwicklung der Plattform vorgenommen. Der letzte Forschungsbeitrag aus Tabelle B.1-2.1 stammt von den Autoren Xu et al. (2019b, 284). Bei diesem wird eine Konsortial-Blockchain auf Basis von Ethereum implementiert. Entwickelt werden die Blockchain sowie die zugehörige Plattform durch ein Unternehmen. Die Rolle der Blockchain-Administration dient zur Verwaltung der Blockchain, der Rechteverwaltung sowie der

Entwicklung und Verwaltung von Dienstleistungen wie Smart Contracts. Mehrere verschiedene Anwender wie Kunden, Lieferanten, Produzenten oder Verkäufer nutzen die Plattform. Durch den Einsatz von Zertifizierungs-Providern werden neben der Speicherung von Produktions-kennzahlen auch Produktqualitätsprüfungen vorgenommen und in der Blockchain gespeichert.

Definition der Anspruchsgruppen. Wie die Auswertung zeigt, zeichnet sich kein einheitliches Bild der notwendigen Anspruchsgruppen ab. Dies liegt u.a. an den verschiedenen eingesetzten Blockchain-Formen. So setzen Abeyratne und Monfared (2016) und Leng et al. (2018) auf eine öffentliche Blockchain, während hingegen Wang et al. (2017), Toyoda et al. (2017), Saberi et al. (2019) und Hancock und Vaizey (2016) auf eine private bzw. Xu et al. (2019b) und Lacity (2018) auf eine Konsortial-Blockchain setzen. Die Wahl beeinflusst die Notwendigkeit von Rollen wie der Registrierungsverwaltung oder eine zentrale Blockchain-Administration. Ebenso wird in drei der sechs beleuchteten Beiträge ein Zertifizierungs-Provider zur Prüfung von Produktion oder Prozessen, bevor die dazugehörigen Daten in die Blockchain geschrieben werden, eingesetzt. Um keinerlei Anspruchsgruppen für die Anforderungsanalyse auszuschließen, werden daher alle übergeordneten Anspruchsgruppen berücksichtigt. Dies erlaubt den befragten Experten uneingeschränkte Auswahl. Falls sich ein Experte in mehreren Anspruchsgruppen sieht, wird dies durch eine Mehrfachauswahl im Experteninterview berücksichtigt. Nach Leng et al. (2018, 642) wird in einer Blockchain-basierten Dienstleistungs-Plattform auf zusätzliche regulatorische Instanzen wie staatliche Organisationen verzichtet. Vielmehr ist es Aufgabe von staatlichen Organisationen, rechtliche Vorausetzungen für den generellen Einsatz der Blockchain-Technologie (Blockchain 1.0 bis 3.0), wie z.B. die Handhabung der unwiderruflichen Speicherung von Informationen im Sinne der Datenschutz-Grundverordnung, zu definieren (Saberi et al. 2019, 2127; Hein et al. 2019, 21f.). Da diese Anspruchsgruppe nicht spezifisch mit der Kollaborationsplattform in Verbindung steht, sondern eine grundsätzliche Problematik der Blockchain-Technologie darstellt, wird diese Rolle für die Anforderungserhebung nicht weiter betrachtet, aber eine Einschätzung durch die weiteren Rollen gefordert. Die konkrete Rolle können die befragten Experten anschließend innerhalb des Experteninterviews selbst bestimmen. Im Folgenden werden die Anspruchsgruppen sowie eine verallgemeinerte Beschreibung der Anspruchsgruppe dargestellt. Dies zum Beantworten der *Forschungsfrage F1.*

- *Anwender* – Jeglicher Nutzer der Plattform, der Daten aus der Blockchain lesen bzw. nutzen möchte oder Daten in dieser abspeichert.
- *Plattform-Provider* – Der Plattform-Provider ist für die Entwicklung der Infrastruktur und damit der Blockchain, der zusätzlichen Verwaltungsinstanzen sowie der User-Interfaces (UI) der verschiedenen Anspruchsgruppen zuständig. Ebenso soll dieser für die Definition von Datenaustauschstandards verantwortlich sein. Weitere Aufgabenfelder können sich im Rahmen der Anforderungsanalyse ergeben.
- *Dienstleistungs-Provider* – Der Dienstleistungs-Provider übernimmt die Verwaltung der implementierten Plattform und regelt z.B. die Zugriffsrechte der Nutzer, die Entwicklung von weiteren Analyseverfahren für die Anwender oder die Verwaltung von Smart Contracts. Weitere Aufgabenfelder können sich im Rahmen der Anforderungsanalyse ergeben und hängen von der ausgewählten Blockchain-Form ab.
- *Zertifizierungs-Provider* – Der Zertifizierung-Provider ist eine externe Anspruchs-gruppe, welche die Überprüfung von z.B. Produktionsmaschinen oder Produkten übernimmt, um sicherzustellen, dass Informationen, welche in der Blockchain persistent gespeichert werden, korrekt sind.

Aufbauend auf diesen Anspruchsgruppen, werden verschiedene semistrukturierte Fragebögen für die Experteninterviews entwickelt.

Entwicklung von Interviewfragen anhand der Anspruchsgruppen

Formaler Aufbau. Die formale Gestaltung der Experteninterviews erfolgt anhand Moosbrugger und Kelava (2012). Es handelt es sich bei den im Folgenden beschriebenen Experteninterviews um semi-strukturierte Interviewbögen. Die Fragestellungen geben im Vergleich zu Ankreuzungsmöglichkeiten keine vordefinierte Lösung vor, sondern sind durch Freitext offen beantwortbar. Jedoch kann eine Antwort der befragten Person nicht völlig unstrukturiert sein, da die Aufgabenstellung eine Struktur vorgibt (Moosbrugger und Kelava 2012, 40). Der Aufbau des Fragebogens erfolgt in drei Teilen und weißt eine kontinuierliche Steigerung in der Komplexität bezüglich der Forschungsthematik auf (Moosbrugger und Kelava 2012, 68f.; Gläser und

Personen für die Thematik und ihre Komplexität zu sensibilisieren. Die auszuwertenden Fragen aus Teil drei werden jedoch nicht vorab zugeschickt, um eine neutrale Erhebungsperspektive seitens der befragten Personen zu ermöglichen. Ebenso wird eine Erprobung der erstellten Fragen durch eine vorläufige Testversion nach Moosbrugger und Kelava (2012, 70) vorgenommen. Der Fragebogen wird in einer Testversion durch drei wissenschaftliche Mitarbeiter der Juniorprofessur für Information Management sowie des Lehrstuhls für Betriebswirtschaftslehre und Wirtschaftsinformatik der Universität Würzburg evaluiert. Hierfür werden nach Moosbrugger und Kelava (2012, 70f.) zwei Ansätze genutzt. Zum einen wird die Methodik des kognitiven Vortestens eingesetzt. Bei dieser Methode werden die Testprobanden gebeten, die Gedanken sowie Überlegungen während der Bearbeitung der Aufgabenstellung dem Prüfer offenzulegen. Hierdurch kann frühzeitig eine Differenz in der Absicht und dem Verständnis der Fragestellung durch den Probanden erkannt werden. Zum anderen wird eine retroperspektive Befragung angewendet. Nach der Beendigung des Testes werden die Probanden zu Problemen und Missverständnissen durch die Aufgabenstellungen befragt. Alle genannten Problematiken werden im Anschluss adressiert.

Inhaltlicher Aufbau. Im dem ersten Teil (A) werden der inhaltliche Rahmen der Interviewstudie beschrieben sowie die Handhabung der erhobenen Daten erläutert. Dieses umfasst die Anonymisierung sowie Speicherung der Daten. Ebenso wird um eine Verständniserklärung über die Aufzeichnung des Gespräches gebeten.

Im zweiten Teil (B) werden Kennzahlen wie Umsatz und Unternehmensgröße sowie Eckdaten zu der befragten Person (Berufsbezeichnung und Dauer der Anstellung) erhoben und damit die demographische Erschließung nach Moosbrugger und Kelava (2012, 68f.) ermöglicht. Anschließend folgen eine Selbsteinschätzung der Personen zum Wissensstand der Thematik sowie einleitende Fragen zu der Thematik. Auf Grund der Aktualität sowie der Entwicklung der Thematik wird der zweite Teil genutzt, um neben der Einschätzung den befragten Personen ein generalisiertes Framework über eine Blockchain-basierte Kollaborationsplattform vorzustellen und damit ein gemeinsamer Konsens für die Erhebung von Anforderungen für diese Plattform präsentiert.

Wie sich zeigt, sind mehrere Anspruchsgruppen für die Umsetzung und Beitreibung einer Blockchain-basierten Kollaborationsplattform relevant. Ebenso zeigen Beiträge wie Nutt (2002, 41ff.), dass die Berücksichtigung der Ansichtsweisen sowie Anforderung dieser Anspruchsgruppen ausschlaggebend für den langfristigen Erfolg einer solchen Plattform sind.

Daher werden für die Interviewstudie für jede Anspruchsgruppe separate Fragen entwickelt (Teil C). Sieht sich eine Person durch mehrere Anspruchsgruppen vertreten, wird diese Person für jede Anspruchsgruppe befragt. Die Fragen sind teilweise deckungsgleich mit weiteren Fragen aus den verschiedenen Anspruchsgruppen formuliert, um eine gegenseitige Validierung zu ermöglichen.

Umfang und Verteilung der Befragung

Umfang. Bei dieser Befragung wurden insgesamt 10 Interviewstudien mit einem Gesamtumfang von 12 Stunden und 24 Minuten durchgeführt. Die Verteilung der Interviewstudien wird in Tabelle B.1-2.2 dargestellt. Sollte eine Person zu mehreren Anspruchsgruppen befragt werden, wird jede Befragung als separates Interview gewertet. Durch dieses Vorgehen wurden sieben Personen aus sechs verschiedenen Unternehmen befragt. Hierbei sahen sich vier Personen in der Rolle des Anwenders, drei in der Rolle des Plattform-Providers und drei Personen in der Rolle des Dienstleistungs-Providers. Die durchschnittliche Dauer der Befragung für den Anwender liegt bei 57 Minuten, bei dem

Nr.	*Kürzel*	*Interviewte Person*	*Rolle*	*Ungefähre Dauer*	*Durchschnittsdauer pro Rolle*	*Durchschnittsdauer*
1	I1	Person C	Anwender	35min	57min	1h 14min
2	I2	Person B	Anwender	53min		
3	I3	Person D	Anwender	1h 8min		
4	I4	Person E	Anwender	1h 10min		
5	I5	Person G	Plattform-Provider	1h 33min	1h 44min	
6	I6	Person A	Plattform-Provider	1h 38min		
7	I7	Person F	Plattform-Provider	2h 2min		
8	I8	Person B	Dienstleistungs-Provider	41min	1h 8min	
9	I9	Person G	Dienstleistungs-Provider	1h 14min		
10	I10	Person A	Dienstleistungs-Provider	1h 30min		
		∑ 12 Stunden und 24min				

Tabelle B.1-2.2: Umfang der Interviews

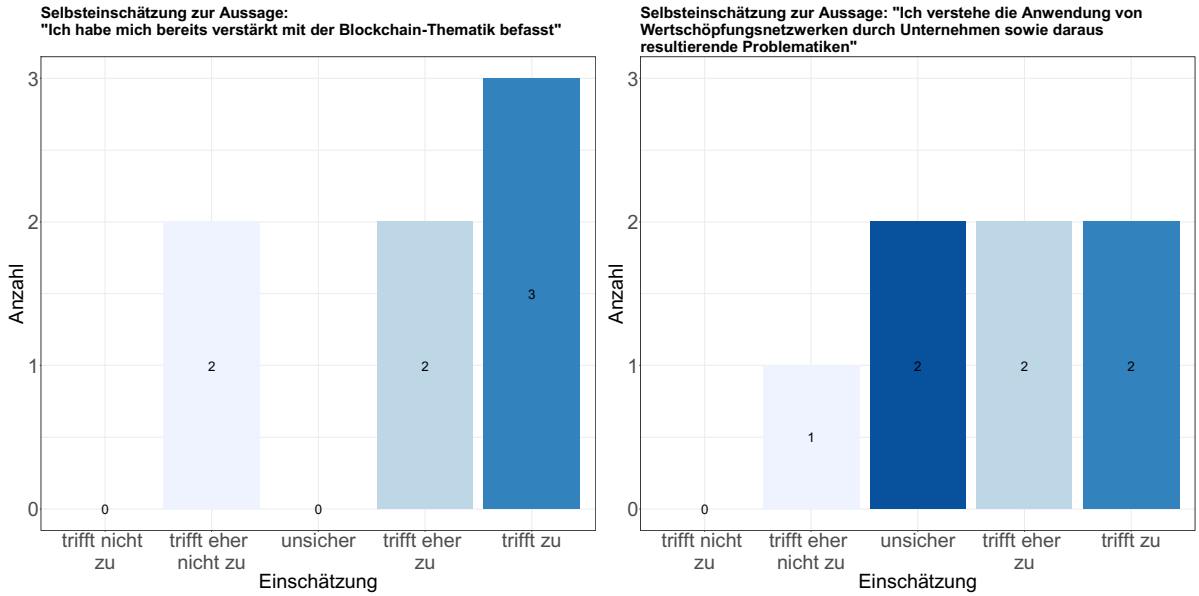


Abbildung B.1-2.1: Verteilung der befragten Personen zur Selbsteinschätzung des Wissenstandes zur Blockchain-Thematik sowie zu Wertschöpfungsnetzwerken

Plattform-Provider bei 1 Stunde und 44 Minuten sowie 1 Stunde und 8 Minuten bei dem Dienstleistungs-Provider. Der gerundete Durchschnitt aller Interviews liegt bei einer 1 Stunde und 14 Minuten.

Die Durchführung der Interviewstudien fand zwischen dem 02.06.2019 und dem 12.07.2019 statt. Als Austauschmedium wurden die Programme Microsoft Skype oder Zoom der Firma Zoom Video Communications Inc. genutzt. Die Interviewstudie mit der Person E wurde persönlich durchgeführt und mit einem Aufnahmegerät aufgezeichnet. Bei Aufzeichnung des Interviews I5 kam es zu technischen Störungen. Daher wurde bei diesem Interview keine Aufzeichnung durchgeführt, sondern nach der Studie ein Gedächtnisprotokoll erstellt. Dieses Protokoll wurde der befragten Person übermittelt und durch diese validiert. Ebenso wurden mehrere Zertifizierungs-Provider, Unternehmen und wissenschaftliche Einrichtungen, welche in diesem Bereich tätig sind, für eine Interviewstudie angefragt. Jedoch gab es hierbei keine Bereitschaft, bei einer Interviewstudie teilzunehmen oder die kontaktierten Personen sahen sich nicht in der Rolle eines Zertifizierungs-Providers.

Verteilung. Im Folgenden wird eine Übersicht über die befragten Personen und Unternehmen dargestellt.

Innerhalb der Interviewstudie wurde neben den Eckdaten zu der befragten Person auch eine Selbsteinschätzung zum Wissensstand der Thematiken Blockchain sowie Wertschöpfungsnetzwerken erfragt. Die Einschätzung erfolgte ebenfalls anhand einer fünfteiligen Liket-Skala und wird in Abbildung 1 dargestellt. Die Abbildung zeigt die Anzahl der jeweilig gewählten Möglichkeiten der präsentierten Liket-Skala.

2 Darstellung der Anforderungsanalyse

Methodik der Anforderungsanalyse

Im Folgenden wird das Vorgehen bei der Anforderungsanalyse beschrieben. Der gewählte Ansatz orientiert sich an einem „requirements engineering"-Ansatz von der IEEE Computer Society (Abran 2004, 2:1-2:12). Das methodische Vorgehen wird in Abbildung B.1-2.2 dargestellt und folgend beschrieben.

Der Ablauf aus Abbildung B.1-2.1 lässt sich in mehrere Abschnitte unterteilen. Auf Basis der konkretisierten Idee aus der ersten Phase des Service-Engineering-Ansatzes werden Anforderungen

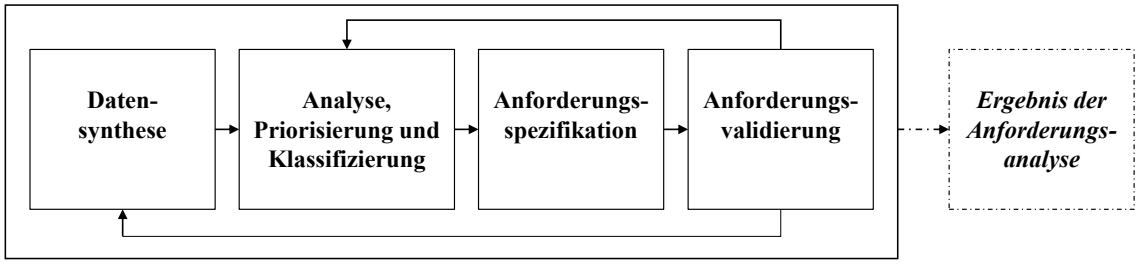


Abbildung B.1-2.2: Vorgehen bei der Anforderungsanalyse (eigene Darstellung in Anlehnung an (Abran 2004)

validiert. Die einzelnen Komponenten innerhalb der Vorgehensweise werden in den folgenden Kapiteln beschrieben.

Datensynthese. Da Anforderungen aus verschiedenen Quellen entstehen können, ist es notwendig, bei der Datensynthese mehrere Informationsquellen zu betrachten. Nach Abran (2004, 2:5) sowie Rupp (2009, 86ff.) wird zum einen eine Dokumentenanalyse in Form einer Literaturanalyse vorgenommen, zum anderen kann nach Abran (2004, 2:5) eine Befragung von Anspruchsgruppen oder Experten mit Wissen innerhalb der Domäne durchgeführt werden. Ebenso schlägt der Autor als mögliche Quellen die Erhebung auf Basis von definierten Zielen oder Untersuchung der betroffenen Prozessumgebung vor.

Analyse, Priorisierung und Klassifizierung. Die Analyse dient der Erkennung und Beseitigung von Unstimmigkeiten und Konflikten innerhalb der erstellten Anforderungen. Die Gestaltung der Anforderungen richtet sich nach den Richtlinien von Pohl (2010, 300):

- *Korrektheit* – Alle erhobenen Anforderungen entsprechen den genannten Aspekten der befragen Personen sowie den Anforderungen, die durch die Literaturanalyse erhoben wurden.
- *Eindeutigkeit* – Jede Anforderung muss eindeutig formuliert sein und erlaubt somit keinen Interpretationsspielraum.
- *Prüfbarkeit* – Jede Anforderung muss anhand der umgesetzten Kollaborationsplattform überprüfbar sein.
- *Rückverfolgbarkeit* – Die Definition jeder Anforderung muss durch eine benötigte Quelle überprüfbar sein.

Die Priorisierung der Anforderungen erfolgt in Anlehnung der von Meiren und Barth (2002, 25) genannten Prioritäten „Muss“, „Wunsch“ und „Abgrenzung“. Bei dieser Vorgehensweise wurde die von Meiren und Barth (2002, 25) vorgeschlagene Priorität „should have“ mit in die Priorität „muss“ integriert, um in der Planungsphase eine eindeutige Abgrenzung zwischen den Prioritäten zu ermöglichen. Die Beschreibung der drei Prioritäten in Anlehnung an Meiren und Barth (2002, 25) wird im Folgenden aufgeführt:

1. ***Muss*** – Die Anforderung muss zwingend in die Kollaborationsplattform, für deren Betrieb oder Nutzung, integriert werden.
2. ***Wunsch*** – Die Anforderung sollte in die Kollaborationsplattform integriert werden, um die Effektivität sowie Effizienz der Plattform zu steigen.
3. ***Abgrenzung*** – Die Anforderung ist für die Kollaborationsplattform nicht von Relevanz.

Die Unterscheidung in Produkt- sowie Prozess-Anforderungen kann bei der Gestaltung einer Kollaborationsplattform nur schwer bemessen werden, da Produkteigenschaften der Plattform häufig mit technischen Prozessaspekten zusammenhängen. Ebenso beschreibt der vorliegende Bericht die Erhebung von Anforderungen vor Umsetzungsbeginn; daher kann eine Bemessung der Stabilität einer Anforderung nur an der erhobenen Anzahl der Nennungen festgemacht werden. Relevante Kriterien wie die Anzahl der Nennungen und Weiterentwicklung der Anforderung über mehrere Iterationsschritte können jedoch noch nicht erfolgen (siehe Abran 2004, 2:6f.). Nach Paetsch et al. (2003, 310) erfolgt die Einordnung der Anforderungen durch die Anspruchsgruppen. Anhand dieses Vorgehens können Konflikte zwischen mehreren Anspruchsgruppen erkannt werden.

Anforderungsspezifikation. Die Phase der Anforderungsspezifikation wird genutzt, um die erhobenen Anforderungen in ein standardisiertes Format zu übertragen. Nach Abran (2004, 2:8) kann dies durch den Einsatz von natürlicher Sprache erfolgen, welche, falls notwendig, durch verschiedene formale Beschreibungssprachen unterstützt werden kann. Die Gestaltung kann nach Rupp (2009, 161f.) anhand von Vorlagen standardisiert werden. Der vorliegende Bericht konzentriert sich bei der Definition von Anforderungen auf die fehlerfreie Definition durch natürliche Sprache sowie Einsatz der in der Datenerhebung genannten Richtlinien. Nach Abran (2004, 2:8) ist die Spezifikation notwendig, um zum einen die Ausgangsbasis für die spätere Planung von Softwarekonzepten sowie Anwendungsszenarien für die Anwender der Software zu entwickeln. Zum anderen dient eine transparente Spezifikation dazu, mit zusätzlichem Domänenwissen eine Einschätzung über Entwicklungskosten und -risiken sowie eine zeitliche Planung vorzunehmen.

Anforderungsvalidierung. Die Anforderungsvalidierung dient zur abschließenden Überprüfung von Anforderungen. Dieses Vorgehen stellt sicher, dass sowohl die Modellierer als auch Anwender der Kollaborationsplattform die verschiedenen Anforderungen korrekt verstanden und entsprechend den Prioritäten der befragten Personen richtig und konfliktfrei zugeordnet haben. Ziel dieser Phase ist es, Probleme zu erkennen, bevor verschiedene Ressourcen für die Umsetzung aufgebraucht werden (Abran 2004, 2:8f.). Nach Abran (2004, 2:9f.) können für die Validierung verschiedene

Vorgehensweisen wie Anforderungsbetrachtung, Entwicklung eines Prototyps, Modellvalidierung oder Akzeptanztests sein.
Ergebnis der Anforderungsanalyse. Das Ergebnis der Anforderungsanalyse stellt alle Anforderungen sowie deren Klassifizierung übersichtlich dar.
.

Anwendung innerhalb des Arbeitsberichtes

Die Herleitung der Ergebnisse aus der Anforderungsanalyse nach Abran (2004, 2:1-2:12) wird im Folgenden beschrieben:
Durchführung der Anforderungsdefinition. Die Anforderungsdefinition umfasst die Prozessschritte Anforderungs-Analyse, -Spezifikation, -Validierung sowie -Klassifikation. Der erste Teil der Definition umfasst die Darstellung der Ergebnisse aus dem iterativen Prozess der Anforderungsanalyse, -Spezifikation sowie –Validierung. Diese Ergebnisse werden in Kapitel 3.2.2 dargestellt.
Anhand dieser Analyse wird die Spezifikation in Form einer natürlichen Sprache vorgenommen. Um eine hohe Transparenz bei der Erstellung der Anforderungen zu erreichen, werden alle relevanten Aspekte für die Definition aus den zwei durchgeführten Synthesen prägnant aufgeführt und kombiniert. Die Nomenklatur der Anforderungen besteht aus zwei Bestandteilen. Der erste Teil beschreibt durch den Ausdruck „REQ“, dass es sich um eine Anforderung handelt. Der zweite Teil stellt durch eine iterative Nummerierung der Anforderung eine eindeutige Zuordnung dar. Auf Basis dieser Spezifikation werden diese Anforderungen validiert und gegebenenfalls korrigiert. Die Validierung erfolgt anhand eines Fragebogens, welcher an verschiedene Personen u.a. aus der Interviewstudie versendet wird. Die Darstellung des Fragebogens erfolgt in Kapitel 3.2.1. Durch dieses Vorgehen sollen Konflikte durch zusätzliche Informationen gelöst und für alle befragten Interviewpartner konforme Anforderungen erhoben werden. Dieses Vorgehen verknüpft den Schritt des Akzeptanztestes sowie der Anforderungsbetrachtung nach Abran (2004, 2:9f.) durch potentielle Anwender der Kollaborationsplattform. Ebenso dient der Fragebogen zur Priorisierung der Anforderungen anhand einer quantitativen Umfrage. Die Ergebnisse sowie die numerische Auswertung der Umfrage werden in Kapitel 3.2.3 dargestellt.
Ergebnis der Anforderungsanalyse. Abschließend erfolgt die Darstellung des Vorgehens der Anforderungsanalyse. Innerhalb dieser Darstellung werden die verschiedenen Anforderungen anhand der Dimensionen bzw. Subdimensionen, welche durch eine Literaturanalyse identifiziert wurden, sortiert. Zusätzlich wird zu jeder erhobenen Anforderung die Klassifizierung in Form der Priorisierung sowie Einstufung in funktionale und nichtfunktionale Anforderungen dargestellt. Um eine übersichtliche Präsentation zu gewährleisten, erfolgt die Darstellung durch eine tabellarische Form.

2.1 Verwandte Forschungsarbeiten

Forschungsbeiträge wie Koteska et al. (2017) und Zhang und Jacobsen (2018) zeigen die aktuelle Problematik auf, dass weitere und gezieltere Untersuchungen zu der Thematik Blockchain in Wertschöpfungsnetzwerken erforderlich sind. Die Literaturanalyse sowie die Auswertung von Yuan et al. (2019) bestätigen anhand einer Verteilung, dass die Anzahl an wissenschaftlichen Publikationen in diesem Bereich sehr gering ist. Die Autoren Moin et al. (2019) konkretisieren diese Wissenslücke und präsentieren die Notwendigkeit der weiteren und gezielten Forschung bei der Implementierung von Blockchain-Plattformen in Wertschöpfungs-netzwerken. Auf dieser Basis erörtern Beiträge wie Lu et al. (2018), Behnke und Janssen (2019), Lin et al. (2019) sowie Weber et al. (2019) erste Anforderungen für die Umsetzungen einer Blockchain-Plattform. Diese Anforderungen basieren jedoch nur auf einer literarischen Analyse und sind nicht durch den Einbezug von Praktikern und damit der eigentlichen Zielgruppe evaluiert. Ähnlich der genannten Forschungsbeiträge lässt sich der Beitrag von Xu et al. (2019a) einordnen, welcher ein nicht evaluiertes Framework für die Umsetzung von Blockchain-Plattformen in Wertschöpfungsnetzwerken vorstellt. Der Beitrag von Sund und Lööf (2019) zeigt eine Evaluierung der postulierten Anforderungen durch prototypische Realisierung einer Blockchain-Plattform innerhalb der Wertschöpfungsnetzwerke des Unternehmens IKEA. Die genannten Anforderungen beschreiben aber primär die Speicherung und Handhabung von Transaktionen auf der implementierten Blockchain.
Abseits der reinen Betrachtung von wissenschaftlichen Publikationen ist zu erkennen, dass in der Praxis bereits erste Blockchain-basierte Kollaborationsplattformen für Wertschöpfungs-netzwerke durch Plattformen wie originChain und AgriDigital existieren (Xu et al. 2019b). Daher scheint es notwendig, Wissen von Praktikern durch wissenschaftliche Methoden zu erheben. Beiträge wie von Korpela et al. (2017) verfolgen bereits diesen Ansatz, aber beschäftigen sich mit Einflussfaktoren und Akzeptanzmodellen für die erfolgreiche Umsetzung. Autoren wie Wang et al. (2019c) hingegen konzentrieren sich primär auf die Durchführung von Interviewstudien zur Erkennung von potentiellen Verbesserungspotentialen. Bei dieser Untersuchung kann nur der Beitrag von Lu (2018) identifiziert werden, welcher anhand der

Befragung von sechs Anwendern innerhalb des Unternehmens Walmart sowie einer Literaturanalyse, Funktionen sowie eine protypische Umsetzung einer Blockchain-basierten Kollaborationsplattform präsentiert. Eine Darstellung der dadurch erhobenen Anforderungen bleibt jedoch ebenfalls aus. Das Vorgehen ähnelt dem Ansatz von Lu (2018), da sowohl durch eine Interviewstudie sowie eine Literaturanalyse eine Entwicklung einer Blockchain-basierten Kollaborationsplattform angestrebt wird. Der Arbeitsbericht konzentriert sich jedoch auf der transparenten Erhebung von Anforderungen, der Entwicklung eines Plattformkonzeptes sowie der Darstellung eines praxisrelevanten Anwendungsszenarios.

3 Definition von Anforderungen

3.1 Analyse der Dimensionen anhand Interviewstudie-Synthese

Im Folgenden werden die erhobenen Interviews analysiert. Hierzu werden die Interviews durch eine qualitative Querschnittsanalyse nach Wilde und Hess (2007, 280–286) erhoben und mithilfe der Software MAXQDA systematisch nach den vorgestellten Dimensionen sowie aus den Interview-Studien erhobenen Unterdimensionen ausgewertet.

Dimension Plattform-Implementierung

Blockchain-Typ. I5 und I6 beschreiben den Einsatz einer privaten oder Konsortial-Blockchain als Notwendigkeit für eine Blockchain-basierte Kollaborationsplattform auf Grund der Sensibilität von unternehmenskritischen Daten. Nach I7 müssen für Wertschöpfungsnetzwerkszenarien ebenso die verschiedenen Anwendungspartner bekannt sein und können nicht wie in einer öffentlichen Blockchain anonym, durch ihren öffentlichen und privaten Schlüssel auf der Blockchain interagieren. Ebenso stellt I7 die erhöhte Verarbeitungsgeschwindigkeit einer zulassungsbeschränkten Blockchain heraus. In den Interviews I1-4 werden verschiedene mögliche Anwendungsszenarien für eine solche Blockchain beschrieben, welche ebenfalls eine private oder Konsortial-Blockchain voraussetzen. Langfristig sieht I7 die Potentiale einer öffentlichen Blockchain, welche eine Authentifizierung benötigt und bei der Lese- und Schreibrecht-Stufen für die Anwender existieren, jedoch bietet nach I7 eine Konsortial-Blockchain die einfachere Ausgangsbasis.

Blockchain-Implementierung. Auf Basis der Konsortial-Blockchain beschreibt I7 den Einsatz der Hyperledger Fabric als eine mögliche Blockchain-Implementierung. Nach I7 hat diese Implementierungsform Skalierungsprobleme, zeichnet sich jedoch durch den Einsatz von bewährten Programmiersprachen wie JavaScript und Java sowie der Festlegung von Abhängigkeiten in Smart Contracts aus. I6 beschreibt zusätzlich, dass die Akzeptanz der Plattform durch den Einsatz einer Blockchain-Implementierung abhängig ist, welche von einem renommierten Entwickler stammt. Da hinter der Hyperledger Fabric u. a. die Linux Fundation sowie das Unternehmen IBM steht, sieht I6 die Hyperledger Fabric als notwendige Implementierung. Diese These wird auch von I7 beschrieben. I5 und I7 erwähnen bei der Ethereum-Blockchain den Einsatz der Gas-Kosten als nicht relevant und für Wertschöpfungsnetzwerke als hinderlich. Auf Grund der schlechten Skalierbarkeit wird die VeChain-Blockchain sowie die Bitcoin-Blockchain auf Grund ihrer nicht Turing-vollständigen Smart Contracts ebenfalls ausgeschlossen (I5).

Konsens-Algorithmus. I5-I7 beschreiben, dass der Einsatz von Konsens-Algorithmen, welche monetäre Anreize bei der Generierung von Blöcken in Wertschöpfungsnetzwerken bieten, nicht sinnvoll ist. Daher scheiden Konsens-Algorithmen wie PoW und PoS aus. I7 stellt heraus, dass in einem Wertschöpfungsnetzwerk alle Beteiligten ein Interesse an dem Fortbestehen der Plattform haben sollten; daher sollten alle Beteiligten durch ein faires Verfahren eine Generierung von Blöcken vornehmen. I7 spricht hierbei von einem möglichen „Round-Robin"-Ansatz. I6 sieht bei der Wahl der Konsens-Algorithmen als besonders wichtig an, dass die Anwendung für die beteiligten Unternehmen einfach und leicht durchführbar sein muss:

„Es sind so viele Innovationen in jeder Hinsicht, [..] dass dies bei den Unternehmen eine breite Umsetzung verhindert, weil es diese überfordert. Deshalb muss es reibungslos funktionieren so wie sich Privatleute bei der Anwendung von Bezahlsystemen wie PayPal keine Gedanken machen, sondern einfach anwenden wollen" (I6)

Als mögliche Konsens-Algorithmen kann, nach I5, die Byzantinische Fehlertoleranz oder eine der zahlreichen Ableger wie pBFT dienen.

Blockdefinition. I1-I3 beschreiben im Punkt der Dauer bei der Entstehung einer Transaktion bis zur persistenten Speicherung in der Blockchain durch die Validierung des zugehörigen Blockes keine Anforderung im Millisekundenbereich. I1 und I3 beschreiben, dass die Daten jedoch innerhalb weniger Stunden für alle Teilnehmer verfügbar sein sollten, u.a. auf Grund von rechtlichen Restriktionen. Eine maximale Blockgröße auf Grund der Datei-größe von Transaktionen sowie der Frequenz dieser Transaktionen kann durch die Personen, welche sich in der Rolle der Anwender

sehen, nicht beantwortet werden. I2 spricht jedoch von ca. einer Transaktion pro Tag und Knoten.

Knotenstruktur. Nach I5 muss die Entwicklung zwei verschiedener Knotentypen erfolgen. Zum einen soll es einen Knoten geben, welcher durch den Dienstleistungs-Provider zur Verfügung gestellt wird und Operationen wie das Generieren und Validieren von Blöcken übernimmt. Zum anderen soll ein leichtgewichtiger Knoten entwickelt werden. Dieser Knoten speichert nur ein Abbild der Blockchain, um Redundanz und damit Vertrauen innerhalb der Plattform zu entwickeln. Dieser Knoten soll nach I5 jedem Anwender zur Verfügung stehen. I6 erweitert dieses Vorgehen und stellt heraus, dass auch Anwender die Möglichkeit haben sollten, die Generierung und Validierung von neuen Blöcken vorzunehmen, um durch eine Involvierung die Kontrolle sowie Vertrauen in die Blockchain aufbauen zu können. Jedoch sollten diese Anwender auch jederzeit die Möglichkeit besitzen, diese Aufgabe an den Dienstleistungs-Provider abgeben zu können.

Dimension Datenspeicherung

On- und Off-Chain. Nach I5-I7 ist es von dem eingesetzten Anwendungsszenario abhängig, welche Daten nach dem On-Chain/Off-Chain-Prinzip gespeichert werden sollen. I5 beschreibt jedoch die Notwendigkeit, dass Datensätze, welche für die unmittelbare Überwachung von Wertschöpfungsnetzwerken erforderlich sind und keine hochsensiblen Daten darstellen, auf der Blockchain gespeichert werden müssen. Dabei kann es sich z.B. um Produktionsmesswerte handeln. Große Dateien, welche nicht für die unmittelbare Rückverfolgung notwendig sind, sollen außerhalb der Blockchain gespeichert und nur deren Prüfsumme in die Blockchain geschrieben werden (I5-I6). Die Benennung einer kritischen Dateigröße, ab welcher diese im Ursprungsformat nicht mehr auf der Blockchain gespeichert werden soll, findet nicht statt. I7 stellt die Möglichkeit der Speicherung von aggregierten Daten vor. So können bestimmte Daten einmal pro Tag und in aggregierter Form in die Blockchain geschrieben werden. Daten, die in feingranularer Form vorliegen müssen, können jedoch nicht durch diese Aggregationsfunktion abgespeichert werden.

Cloud-Speicherung. Die Off-Chain gespeicherten Daten müssen permanent für alle betroffenen Anwender oder Unternehmen verfügbar sein, was durch die Kollaborationsplattform erfolgen soll (I6). I7 differenziert den Einsatz von Cloud-Speicherungen anhand verschiedener Cloud-Lösungen. Hierbei muss auf die lokalen Gesetzgebungen, in denen diese Lösungen aufgebaut sind, geachtet werden.

„*Wir wissen von einigen deutschen Kunden, dass diese [..] Amazon [AWS] unter den aktuellen Bedingungen nicht verwenden würden [..], es gibt deutsche Provider, die Anforderungen der deutschen Kunden abdecken*“ (I7)

I6 bestätigt diese These von I7 und verweist auf gesetzliche Vorgaben im Vergleich von Cloud-Lösungen, die in den USA aufgebaut sind, im Vergleich zu Cloud-Lösungen aus Deutschland. Der Anwender I3 beschreibt, dass bei einem Auftrag in China die notwendigen Dateien nicht auf Cloud-Diensten wie von Google oder Amazon gespeichert werden dürfen, da auf Grund von lokalen Beschränkungen kein Zugriff auf solche Cloud-Dienste möglich ist.

Dimension Datenaustausch

ERP. Für die Abwicklung von Transaktionen der verschiedenen ERP-Lösungen der Kooperationspartner über die Blockchain ist es notwendig, einen standardisierten Datenaustausch zu ermöglichen. I5 beschreibt die Situation der Kunden im deutschsprachigen Raum. Nach I5 arbeitet ein Großteil der Unternehmen mit einem selbstentwickelten ERP-System. Auf Grund der hohen Varianz und der damit meist fehlenden Interoperabilität zwischen verschiedenen ERP-Systemen, soll der Datenaustausch anhand von Metadaten erfolgen, welche durch das JSON-Format übertragen werden. I7 spricht in diesem Kontext ebenfalls von einem leichtgewichtigen Standard wie JSON oder XML. Eine Definition eines Dateiformates sowie des Datenaustausch-Formates ist in diesem Fall notwendig. Sowohl I4 und I1 zeigen die Bereitschaft, definierte ERP-Datenstandards (eStandards) adaptieren zu wollen. Beide Unternehmen nutzen bisher selbstentwickelte Datenaustauschformate. I1 zeigt die Bereitschaft für das selbstentwickelte ERP-System, eine Schnittstelle zur Integration eines Blockchain-Knotens zu ermöglichen. I4, welches Microsoft Dynamics Nav nutzt, sieht hingegen den Softwareentwickler in der Pflicht, vordefinierte Schnittstellen für verbreitete Blockchain-Implementierungen wie Hyperledger Fabric oder Ethereum zur Verfügung zu stellen.

Sensorik. Die Anwender I1 und I4 schlagen u.a. als Datenaustausch-Format für eingesetzte Sensorik ebenfalls das JSON-Format vor. I1 stellt die Notwendigkeit, dass das eingesetzte Format eine native Serialisierung aufweisen muss, fest. Dies trifft nach I1 ebenfalls auf das XML-Format zu. I2 und I3 können hierzu keinerlei Aussagen treffen. Der Plattform-Provider I5 stellt ebenfalls die Transformation von Sensordaten in das JSON-Format für die Datenübertragung in die Blockchain vor. I5 und I6 beschreiben, dass viele

Unternehmen ihre Sensordaten über eine Open Platform Communications Unified Architecture (OPC UA) -Schnittstelle aus einer speicherprogrammierbaren Steuerung (SPS) abfragen und auswerten. Daher soll eine Transformation von Daten aus der OPC UA-Schnittstelle in das JSON-Format erfolgen. I6 und I7 definieren in diesem Kontext die Notwendigkeit, dass neue Verbands- oder Industrienormen geprüft und gegebenenfalls adaptiert werden sollen. I7 erwähnt als Möglichkeit den O-M/O-DF-Standard, welcher sich noch in der Beta-Phase befindet.

Dimension Datenschutz

Durch die Befragung der Interviewpartner können zwei verschiedene Aspekte zum Thema Datenschutz identifiziert werden: Zum einen die rechtliche Handhabung von Daten und zum anderen die Geheimhaltung bzw. Wahrung der Datensicherheit. Diese werden im Folgenden beschrieben.

Rechtliche Handhabung. I1 und I4 stellen heraus, dass keine personenbezogenen Daten, welche in Konflikt mit der DSGVO stehen könnten, auf der Blockchain gespeichert werden dürfen. I4 zeigt ebenso aktuelle rechtliche Unklarheiten bei der Speicherung von Prüfsummen von personenbezogenen Daten und der Handhabung innerhalb des Unternehmens mit den dazugehörigen Klardaten. I1 ergänzt, dass selbst Prüfsummen von personenbezogenen Daten durch ein logisches Ausschlussprinzip das Herleiten der Klardaten ermöglichen könnten. Hierbei müssen Richtlinien entwickelt werden, um eine solche Problematik zu verhindern. Verschiedene Interviewpartner wie I4 und I9 sehen in diesem Kontext die Notwendigkeit von rechtlichen Regelungen solcher Problematiken z.B. durch die Bundesregierung.

Geheimhaltung von Daten. Die Geheimhaltung von bestimmten Daten ist für alle Anwender (I1-I4) ein relevanter Faktor in einer Kollaborationsplattform. Hierbei ist es nach I2 und I3 wichtig, dass nicht jeder Teilnehmer alle Daten auf der Blockchain auslesen darf. Daher muss ein mehrstufiges Rechtesystem entwickelt werden, das die Lese- und Schreib-Rechte verschiedener Anwender auf die in der Blockchain gespeicherten Transaktionen klar definiert. Nach I1 muss es möglich sein, dass konkurrierende Unternehmen nicht nur nicht alle Daten auf der Blockchain lesen können, sondern ebenso keinerlei Informationen über die Existenz mancher Transaktionen zwischen verschiedenen Kooperationspartnern haben. Diese Anforderung orientiert sich an der Channel-Funktion der Hyperledger Fabric.

Dimension Verwaltung

Integration von Anwendern in die Plattform. I7 setzt für die Umsetzung von verschiedenen Zugriffsrechten ein User-Management-System voraus, welches von einem Superadministrator verwaltet wird. I5 beschreibt die Umsetzung eines solchen Systems anhand des „Certification Authority"-Moduls von Hyperledger Fabric, setzt im Gegensatz zu I7 aber mehrere Superadministratoren, welche in der Rolle als Dienstleistungs-Provider interagieren, voraus. Hierdurch soll ein single point of failure verhindert werden. Ebenso kann mittels eines Mehrheits-Votums die Objektivität bei der Zulassung oder dem Ausschluss von Anwendern durch verschiedene Dienstleistungs-Provider bewahrt werden (I6). Um eine Zulassung bzw. eine Einstufung der Anwender in die verschiedenen Zugriffsrechtstufen (siehe Dimension Datenschutz) vorzunehmen, ist eine Überprüfung der Unternehmen notwendig. I10 und I9 schlagen eine Adaption des Verfahrens „Know Your Customer" vor. Nach I10 soll hierfür eine Orientierung anhand der Finanzbranche erfolgen. Eine Überprüfung dieses Verfahrens kann durch verschiedene Wirtschafts-auskünfte erfolgen, welche durch diese Vorgehensweise Unternehmen zertifizieren können, für diese Kollaborationsplattform geeignet zu sein. Ebenso müssen nach I8 und I10 technische Anforderungen für die Bereitstellung der Infrastruktur des Knoten durch den Anwender überprüft werden. I6 und I9 beschreiben die zusätzliche Definition von Regelwerken, wie Personen innerhalb eines Unternehmens auf die Plattform für einen kontrollierten Zugriff zugreifen dürfen.

Verwaltung des Public/Private-Schlüsselpaares. Für die Nutzung der Blockchain-basierten Kollaborationsplattform ist es notwendig, dass alle Anwender permanent handlungsfähig auf dieser Blockchain sind (I6). Ein Verlust des Public/Private-Schlüsselpaares würde einen automatischen Selbstausschluss aus der Plattform bedeuten. I5, I6 und I9 verdeutlichen diesen Sachverhalt und argumentieren damit, dass der Anwender durch definierte Handlungsrichtlinien unterstützt werden soll, um einem Verlust entgegenzuwirken. I5 und I6 schlagen als mögliche Lösung die Ausgabe mehrerer Public/Private-Schlüsselpaare pro Unternehmen vor, welche redundant benutzt werden können. Der Verlust von Schlüsselpaaren würde keinen Ausschluss auf der Plattform bedeuten, solange der Anwender noch ein Schlüsselpaar zur Verfügung hätte. I7 sieht diesen Vorschlag kritisch, da dies in der Praxis dazu führen würde, dass Unternehmen mehrere Schlüsselpaare auf einer zen-tralen Einheit speichern würden, welche ein single point of failure erzeugen könnte. Die Sicherung von Schlüsselpaaren für Unternehmen durch die

Dienstleistungs-Provider ist nach I8 keine plausible Lösung, da diese sonst die Schlüsselpaare theoretisch ebenso missbrauchen könnten. Daher sollen die Dienstleistungs-Provider nur für die Generierung der Schlüsselpaare für die Plattform und den Anwender zuständig sein.

Integration von staatlichen Organisationen. Bei der Befragung der Dienstleistungs-Provider I8-I10 sowie den Plattformprovidern I5-I7 zeigt sich kein einheitliches Bild, wie staatliche Organisationen in die Plattform integriert werden können. I5 und I7 schlagen einen permanenten Zugriff für staatliche Organisationen vor. Ebenso sollen Schnittstellen bereitgestellt werden, welche eine automatische Analyse in Form von Audits durch die Organisationen ermöglichen. I8 stellt heraus, dass staatliche Organisationen keinen Zugriff auf die Blockchain haben sollten, jedoch sollte die Plattform für staatliche Organisationen zertifiziert werden, dass die Durchführung von Kartellen oder illegalen Transaktionen durch Smart Contracts automatisch überprüft und verhindert werden kann. I10 schließt jegliche Interaktion zwischen staatlichen Organisationen und der Kollaborationsplattform aus.

Entwicklungsunterstützung bei Smart Contracts. Die befragten Anwender innerhalb dieser Interviewstudie würden die Entwicklung von eigenen Smart Contracts selbst vornehmen (I1) oder diese Entwicklung auf Grund von fehlendem Wissen an Dienstleistungs-Provider auslagern (I2 und I4). Für die Entwicklung der Smart Contracts, sowohl durch Anwender oder Dienstleistungs-Provider, sollen konfigurierbare branchenspezifische Vorlagen zur Verfügung gestellt werden. Diese Vorlagen sollen durch Web-basierte Schnittstellen sowie Anleitungen innerhalb dieser Schnittstelle eine einfache und schnelle Konfiguration von Smart Contracts ermöglichen. Zusätzlich ist die Unterstützung von weniger technischen Entwicklern wie Juristen durch Darstellung von Pseudocode oder einer programmcodefreien Eingabe von Parametern notwendig (I5, I6, I9 und I10). Da es in Wertschöpfungsnetzwerken, nach I10, viele Standardprozesse gibt, kann ein Großteil der zu entwickelnden Smart Contracts durch Vorlagen unterstützt und effizient gestaltet werden. Ebenso sollen diese Templates für Branchen mit mehreren Anwendern in Zusammenarbeit entwickelt werden (I10). Auch beschreiben I7 und I9 den Einsatz von Modellierungswerkzeugen, welche auf grafischer Basis eine Entwicklung von Prozessabläufen z. B. anhand des Standards Business Process Model and Notation (BPMN) ermöglicht. Diese Abläufe sollen automatisiert in einen parametrisierbaren Smart Contract übertragen werden. Mittels externer Variablentabellen sollen Smart Contracts wiederverwendbar gestaltet werden. Ebenso ermöglicht dies die dynamische Gestaltung von Gültigkeitsbereichen. Diese Variablentabellen befinden sich außerhalb der Blockchain und können durch zugehörige Anwender angepasst werden. Vor der Ausführung von Smart Contracts fragt dieser diese Tabellen ab und führt auf Basis dieser Variablen sowie dem Programmcode Befehle aus (I7, I5).

Verwaltung von Smart Contracts sowie Oracles. Um eine Verwaltung bzw. Übersicht über die aktiven Smart Contracts auf der Plattform zu ermöglichen ist es notwendig, eine transparente und nachvollziehbare Darstellung zu implementieren. Es muss möglich sein, die aktiven Smart Contracts sowie die Beziehungen zu den verschiedenen Anwendern zu überwachen und filtern zu können (I5, I7). Nach I5, I7 und I9 kann dies anhand einer Prozesskarte erfolgen, welche die aktiven Smart Contracts, deren Beziehung sowie den dazugehörigen Quellcode und eine Darstellung in Pseudocode bietet. Zum einen soll nach I7 eine Echtzeitüberwachung der aktiven Smart Contracts erfolgen, zum anderen ermöglicht dies den Einsatz von Analyseverfahren (I10). Nach I5 sollen diese Funktionalitäten sowohl für die Dienstleistungs-Provider als auch für die Anwender zur Verfügung gestellt werden. I5 sieht hierdurch das Erzeugen von Vertrauen der Anwender in die Plattform. Für die Implementierung von Oracles soll ein nach I7 ein zertifikatsbasierter Ansatz gewählt werden. Zertifizierte Schnittstellen und Dienstleister können hierfür eingesetzt werden. Ebenso besteht nach I7 die Problematik, dass staatliche Organisationen in internationalen Wertschöpfungsnetzwerken nicht als vertrauliche Informationsquelle betrachtet werden können, da nicht jedes Unternehmen fremden staatlichen Organisationen vertraut. Als Beispiel für einen Oracle zeigt I6 die Integration von Wechselkursen, um aktuelle Warenwertschwankungen in der Blockchain abbilden zu können.

Dimension Anwendungsmöglichkeiten

Die Befragung der Anspruchsgruppen ergab für die Anwender vier verschiedene Szenarien. Diese werden im Punkt „Anwendung“ beschrieben. Ebenso wird hier die Konzeption eines Marktplatzes, welche durch verschiedene Dienstleistungs-Provider erwähnt wurde, beschrieben.

Anwendung. I1 und I2 beschreiben als mögliche Einsatzpotentiale die unwiderrufliche Speicherung von Dokumenten und Transaktionen. I1 würde eine solche Kollaborationsplattform nutzen, um eine Dokumentation von Komponenten und Geräten wie Messgeräte zu ermöglichen. Die Dokumentation soll in Form eines Steckbriefes in jedem Produktionsschritt durch definierte

Kennzahlen des Prozesses sowie durchgeführte Prüfungen in Form von Zertifikaten erweitert werden. Hier soll sich eine lückenlose Rückverfolgung aller Schritte bei der Produktion bei Zulieferern als auch bei I1 ergeben. I2 würde die Blockchain-basierte Kollaborationsplattform nutzen, um abgeschlossene Verträge mit Kunden und Vertriebspartnern zu speichern. Hierdurch soll ein Vertrag, der dazugehörige Vertragstext sowie die Signaturen aller Partner gesichert werden. Durch diese Bestandteile sind spätere Rückverfolgungen möglich. Durch diese Speicherung sollen spätere Konfliktpunkte über Vertragsbestandteile vermieden werden und damit allen Kooperationspartnern eine transparente Argumentationsbasis für weitere Vertragsverhandlungen liefern. I3 beschreibt die Dokumentation des Lebenszyklus von produzierten Prüfständen. Für jeden Prüfstand sollen Eckdaten, wie die installierte Software inkl. Versionsnummern, Hardware sowie historische Daten wie Vorbesitzer und Standort gespeichert werden. Diese Daten sollen erhoben werden, um bei Kundenanfragen eine Nachvollziehbarkeit über die Prüfstände zu haben. I4 beschreibt zwei thematisch nahe Anwendungsszenarien. Im ersten Szenario soll durch die Blockchain eine Rückverfolgbarkeit im Containerverleih erzielt werden. Das Unternehmen von I4 verleiht Container mit bestimmten Qualitätsanforderungen. Diese sind z.B. die Garantie der Einhaltung von Kühlketten in einem festgelegten Zeitumfang. Um eine Beweisbarkeit der Einhaltung notwendiger Maßnahmen zu ermöglichen, sollen verschiedene Montagezustände bei Containeraufbereitung überwacht und persistent gespeichert werden und als Beweisgrundlage dienen. Das zweite Szenario beschreibt die Rückverfolgbarkeit von verliehenen Containern hinweg über die Lieferkette zu verschiedenen Kunden, welche durch Speditionen durchgeführt wird.

Marktplatzentwicklung. Die Interviewpartner I9 und I10 beschreiben in der Rolle als Dienstleistungs-Provider die Adaption eines elektronischen Marktplatzes, welcher ebenfalls in die Kollaborationsplattform integriert werden soll. Nach I10 soll dieser Marktplatz in Anlehnung an bestehende Online-Handelsplattformen angelegt werden. I9 sieht den Marktplatz als Möglichkeit, dass verschiedene Dienstleistungs-Provider transparent verschiedene Applikationen, Smart Contracts sowie Servicebündle für die Anwender auf der Kollaborationsplattform anbieten können. Ein Anwender soll die Möglichkeit haben, über Suchfunktionen verschiedene Dienstleistungen zu suchen und anschließend durch individuelle Abstimmung mit den zugehörigen Dienstleistungs-Providern eine Leistung entwickeln zu lassen. Ebenso sollen den Anwendern Vorschläge über weitere mögliche Dienstleistungen angeboten werden. Die Bezahlung der Dienstleistungen muss sowohl über ein Token-System, aber auch über traditionelle Bezahlsysteme möglich sein.

Dimension Kryptowährung

I2, I3 und I4 sehen den Einsatz von elektronischen Bezahlmöglichkeiten auf der Kollaborationsplattform als eine gute Möglichkeit, verschiedene Abläufe zu automatisieren. I1 hingegen hält zwar den Einsatz von Kryptowährungen für sinnvoll, ist jedoch der Überzeugung, dass die vertretene Firma keine Akzeptanz für eine solche Währung zeigen wird. Sowohl I2 als auch I4 präferieren den Einsatz von Tokens auf der Blockchain gegenüber bekannten Kryptowährungen. Die befragten Personen sehen durch Tokens die Möglichkeit, im Vergleich zu Kryptowährungen ein wertstabiles Handeln vorzunehmen. I3 sieht die Notwendigkeit, mehrere Bezahlarten anzubieten, damit auch konservative Kooperationspartner durch einen Smart Contract angestoßene Banktransaktionen ebenso von Prozessautomatisierungen profitieren können.

Dimension Externe Parteien

Weitere externe Parteien kann keiner der vier befragten Anwender nennen. I1 nutzt bisher keinen Zertifizierungs-Provider in verschiedenen Wertschöpfungsnetzwerken. Vielmehr werden durch vertragliche Rahmenbedingungen Qualitätsanforderungen festgelegt, an die sich die Kooperationspartner halten. Wird durch das Unternehmen von I1 festgestellt, dass es zu Verstößen kommt, drohen Strafen für die entsprechenden Unternehmen. Im Hinblick auf neue Kooperationspartner sieht I1 jedoch die Notwendigkeit der Integration von Zertifizierungs-Providern. I2 bestätigt diesen Sachverhalt, erwähnt jedoch, dass der Einsatz solcher Provider für die geprüften Unternehmen nur notwendig ist, wenn für diese dadurch ein Mehrwert entsteht oder es für manche Unternehmen als Voraussetzung zur Kooperation definiert ist. I3 nutzt keine dezidierten Zertifizierungs-Provider, da die Kunden selbst eine Prüfung der eingekauften Produkte bzw. Messanlagen vornehmen. I9 ergänzt die zusätzliche Notwendigkeit einer externen Prüfstelle oder einen Zertifizierungs-Provider, welche Smart Contracts und Oracles auf Fehleranfälligkeit oder unautorisierte Anforderungen prüfen müssen.

Dimension User-Interfaces

Gestaltungsrichtlinien. Mehrere befragte Personen (I1-I3) sehen es als notwendig an, auch über mobile Endgeräte auf diese Schnittstellen

zugreifen zu können. Ein Ansatz für diese Personen stellt die Entwicklung von Web-Oberflächen z.B. durch eine HTML-Entwicklung dar. Ebenso müssen die Oberflächen zusätzliche Informationen und Felder enthalten, welche Nutzer zur Orientierung sowie als schrittweise Anleitung bei der Prozessabwicklung nutzen können. Diese Schnittstellen sollen nach I3 sowie I7 zu mindestens 95 bzw. 99 Prozent der Zeit verfügbar sein und angestoßene Abfragen bzw. Aktivitäten innerhalb von maximal 10 Sekunden bzw. zwei bis drei Minuten bei internationalen Zugriffen abarbeiten können. Der Anmeldeprozess auf dieser Plattform für den Zugriff auf die Schnittstellen soll nach I2 durch die unternehmens-internen Anmeldedaten erfolgen.
Validierung bei Falscheingaben. Mögliche Einsatzszenarien wie die von I2 und I3 genannten, zeigen die Anforderung, dass auch manuelle Eingaben in die Plattform möglich sein müssen. Sowohl I6 als auch I7 schlagen die Implementierung eines Vier-Augen-Prinzips für Bestellungen und Transaktionen mit höherem Ausmaß vor, bei dem z.B. ein Vorgesetzter einer Transaktion zuvor zustimmen muss. Eine quantitative Bemessung des höheren Ausmaßes findet nicht statt. Für kleinere Bestellungen soll nach I7 eine Eingabevalidierung anhand einer bestimmten Logik und Plausibilitätsprüfungen erfolgen. Dies kann nach I6 über maschinelle Lernverfahren erfolgen. I6 beschreibt diesen Einsatz, da das Vier-Augen-Prinzip die unmittelbare Speicherung auf der Blockchain verzögert, weshalb primär automatisierte Verfahren genutzt werden sollen. Nach I6 können ebenso verzögerte Eingaben auf die Blockchain gespeichert werden. Der Nutzer hat somit die Möglichkeit, Transaktionen innerhalb eines bestimmten zeitlichen Intervalls korrigieren können, bevor diese Transaktionen auf der Plattform gespeichert werden.

Dimension weitere Aspekte

Abschließend wurden die Personen befragt, welche sich in der Rolle des Dienstleistungs- sowie Plattform-Providers sehen, ob diese noch weitere notwendige Aspekte für die Kollaborationsplattform sehen. Hierbei können zwei Aspekte ausfindig gemacht werden. Zum einen Schulungen und zum anderen Nutzungskosten der Plattform.
Schulungen. I6 verdeutlicht die Aktualität der Blockchain-Thematik und der damit einhergehenden Notwendigkeit, Schulungen für Anwender der verschiedenen Kooperations-partner im Zuge einer Plattformrealisierung anzubieten. Ebenso müssen Rollen wie der Plattform- oder der Dienstleistungs-Provider Schulungen zu rechtlichen Aspekten innerhalb der Blockchain-Thematik belegen.
Kosten. Die Benutzung der Kollaborationsplattform darf nach I6 keine wesentlich höheren Kosten verursachen als bestehende Systeme in Wertschöpfungsnetzwerken.

3.2 Durchführung der Anforderungsanalyse

3.2.1 Darstellung des Fragebogens für die Validierung und Priorisierung

Das Ziel der Studie ist es, anhand eines multidimensionalen Tests mehrere verschiedene Kriterien zu erfassen und zu überprüfen (Moosbrugger und Kelava 2012, 34). Diese sind die Priorisierung und Validierung der definierten Anforderungen. Die Gestaltung des Fragebogens orientiert sich an Moosbrugger und Kelava (2012). Der Aufbau des Fragebogens unterteilt sich in zwei Bereiche. Im ersten Bereich werden Rahmeninformationen sowie die weitere Handhabung mit den erhobenen Daten der befragten Person zur Verfügung gestellt. Das Vorgehen erfolgt in Anlehnung an der durchgeführten semi-strukturierten Interviewstudie aus Kapitel 1. Zusätzlich werden in dem ersten Bereich Eckdaten zu der befragten Person erhoben. Diese sind neben dem Namen, die Selbsteinschätzung zu der Blockchain-Thematik sowie Wertschöpfungsnetzwerken. Diese Eckdaten sind auf Grund der zeitlichen Differenz zwischen der ersten Interviewstudie und der Durchführung des Fragebogens notwendig. Im zweiten Bereich erfolgten die Validierung sowie die Priorisierung der Anforderungen. Hierfür wird pro erhobene Anforderung folgende Beispielstabelle integriert und durch diskret gestufte Ratingskalen dargestellt.

Die Teilnehmer haben vier Auswahlmöglichkeiten zur Einordnung.

1. ***Muss*** – Die Anforderung muss zwingend in die Kollaborationsplattform für deren Betrieb oder Nutzung integriert werden.
2. ***Wunsch*** – Die Anforderung sollte in die Kollaborationsplattform integriert werden, um die Effektivität sowie Effizienz der Plattform zu steigen.
3. ***Abgrenzung*** – Die Anforderung ist für die Kollaborationsplattform nicht von Relevanz.
4. ***Keine Einordnung*** – Die Anforderung ist für die Kollaborationsplattform nicht von Relevanz.

Zum einen können die befragten Personen durch anklickbare Felder „Muss“, „Wunsch“, „Abgrenzung“ und „Keine Einordnung“ eine Einordnung zur Anforderung innerhalb der Spalte „Anforderung“ vornehmen. Das Vorgehen richtet

sich nach einer diskret gestuften Ratingskala (Moosbrugger und Kelava 2012, 51). Zum anderen können die befragten Personen durch die Spalte „Änderungsvorschlag“ Korrekturvorschläge für die jeweiligen Anforderungen durch ein Freitextfeld vornehmen. Der komplette Fragebogen wird in Anhang C dargestellt.

Die Umfrage wurde durch eine editierbare Datei im PDF-Format an Interviewpartner aus der semi-strukturierten Interview-Studie sowie weiteren Mitarbeitern innerhalb der Unternehmen geschickt. Zusätzlich wurde die Studie, um die Betrachtung aus wissenschaftlicher Sicht zu ermöglichen, an wissenschaftliche Mitarbeiter des Lehrstuhls BWL und Wirtschaftsinformatik der Universität Würzburg gesendet. Die Umfrage fand im Zeitraum zwischen August und September 2019 statt.

Insgesamt nahmen neun Personen an der Umfrage teil. Neben den befragten Interviewteilnehmern (Person A-G) aus der semi-strukturierten Interviewstudie beantworteten die folgenden zwei Personen die Fragebögen.

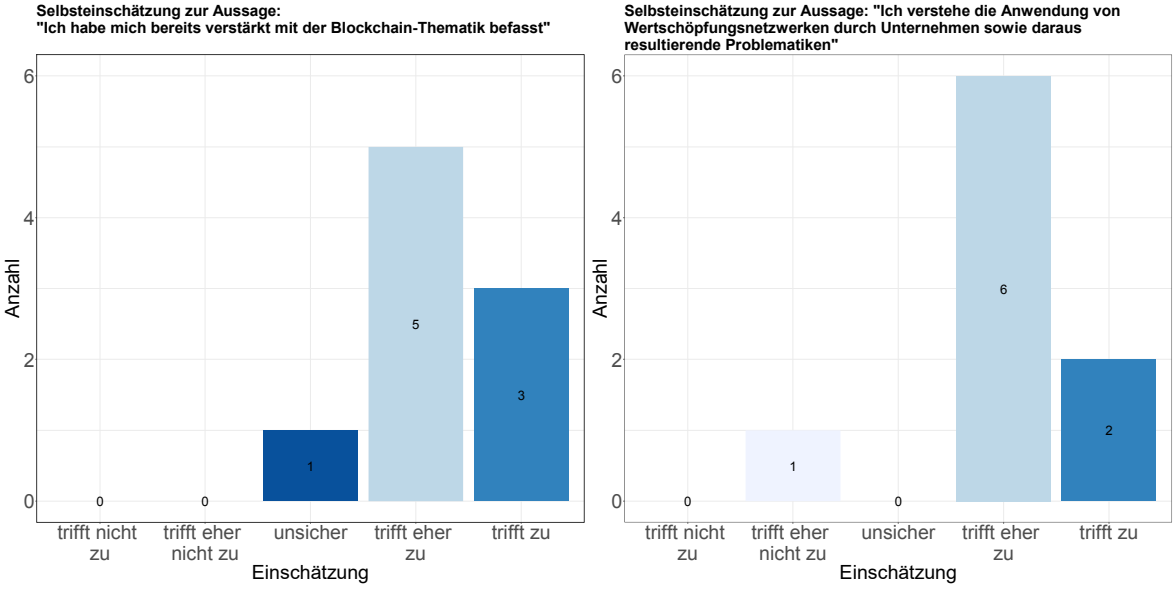


Abbildung B.1-2.3: Verteilung der Selbsteinschätzungen innerhalb der befragten Personen bei der Anforderungs-Priorisierung und Validierung

Die Ergebnisse der Selbsteinschätzung zu den Thematiken Blockchain sowie Wertschöpfungsnetzwerken werden durch Abbildung B.1-2.3 dargestellt. Sie verdeutlicht die thematische Weiterentwicklung der befragten Personen im Vergleich zu den erhobenen Daten der semi-strukturierten Interviewstudie und verdeutlicht somit die aktuellen Tendenzen der Thematik.

Die Ergebnisse der Fragebögen werden in folgenden Kapiteln dargestellt. Um nach Pohl (2010, 300) die Transparenz bei der Erstellung von Anforderungen herzustellen, werden die Änderungsvorschläge der befragten Personen zusammen mit dem Ergebnis der Literaturanalyse sowie der semi-strukturierten Interviewstudie in Kapitel 3.2.2 dargestellt. Die Verteilung und Ergebnisse der Anforderungspriorisierung werden in Kapitel 3.2.3 dargestellt.

3.2.2 Ergebnis der Anforderungsdefinition

Dimension Plattformimplementierung

Blockchain-Typ. Bei der Literaturanalyse beschreiben mehrere Quellen den Einsatz einer Konsortiums-Blockchain auf Grund von gesetzlichen Be-stimmungen sowie der höheren Verarbeitungsgeschwindigkeit im Vergleich zu öffentlichen Plattformen (siehe Albrecht et al. 2018, 3529; Chang et al. 2019, 2; Mandolla et al. 2019, 138). Die Interviewpartner in der Rolle der Plattform-Provider I5 bis I7 bestätigten diesen Sachverhalt.

REQ1: Für die Kollaborationsplattform muss eine Implementierung in Form einer Konsortial-Blockchain erfolgen.

Blockchain-Implementierung. In der Literatur werden verschiedene Softwareplattformen für die Umsetzung einer Blockchain im SCM beschrieben. Die Hyperledger Fabric, welche bei der Literaturanalyse am häufigsten Erwähnung findet, zeichnet sich nach Nasir et al. (2018, 5) sowie Kuhi et al. (2018, 259) besonders durch ihre geringe Latenz, Validierungszeit sowie hohe Skalierbarkeit von Transaktionen in Wertschöpfungsnetzwerken aus. I7 sieht primär die Entwicklung durch bewährte Programmiersprachen als Grund für den Einsatz von Hyperledger Fabric. I5 und I6 erwähnen das zusätzliche Vertrauen von Anwendern in das Unternehmen IBM, welche die Hyperledger Fabric mitentwickelt. Nach I5 und I7

kommt der Einsatz der Ethereum-Plattform auf Grund der Gas-Kosten bei Smart Contracts nicht in Frage.

REQ2: Die Softwareimplementierung der Blockchain muss anhand von Hyperledger Fabric erfolgen.

Konsens-Algorithmus. Die Validierung der Blöcke kann durch verschiedene Konsens-Algorithmen erfolgen (Konsensbildung). Bei der Literaturanalyse können verschiedene Verfahren identifiziert werden. Nach Hulea et al. (2018, 5) ist es für den Einsatz einer Blockchain im SCM Bereich relevant, einen leichtgewichtigen und trotzdem sicheren Konsens-Algorithmus einzusetzen. I5 und I7 bestätigen dies und sehen es als notwendig an, dass der gewählte Konsens-Algorithmus keinerlei monetäre Anreize für die Validierung von Blöcken, sondern ein faires und gleichverteiltes Verfahren bietet. Alle Beteiligten sollen mit gleichem Anteil an diesem Prozess teilhaben. Person I und G zeigen innerhalb der Anforderungsvalidierung, dass in REQ4 die Anzahl der notwendigen Parteien für die Konsens-Bildung integriert werden muss, da sonst die Anforderung missverstanden werden kann.

REQ3: Bei der Wahl des Konsens-Algorithmus muss ein Verfahren gewählt werden, welches eine gleichmäßige Verteilung der Konsensbildung auf alle Anwender der Kollaborationsplattform ermöglicht.

REQ4: Alle Anwender müssen nach Bedarf des Konsens-Algorithmus an dem Prozess der Blockvalidierung teilnehmen. Die Anzahl der notwendigen Parteien für die Konsens-Bildung wird durch den Konsens-Algorithmus bestimmt.

Knotenstruktur. Die Validierung von Blöcken soll nach I5 und I6 durch die beteiligten Unternehmen in dem Wertschöpfungsnetzwerk durchgeführt werden. Ebenso muss es nach I6 möglich sein, dass Unternehmen diesen Prozess in Form einer Dienstleistung bei einem Dienstleistungs-Provider einkaufen können. Der Dienstleistungs-Provider nimmt stellvertretend die Generierung und Validierung für die Anwender der Plattform vor.

REQ5: Beteiligte Unternehmen in der Kollaborationsplattform müssen die Möglichkeit haben, die Konsensbildung auf der Blockchain in Form einer kontinuierlichen Dienstleistung an Dienstleistungs-Provider auszulagern.

Dimension Datenspeicherung

On- und Off-Chain. Sowohl in der Literatur durch Autoren wie Chang et al. (2019, 4) oder Mandolla et al. (2019, 139), aber auch durch die befragten Personen wird erwähnt, dass nicht alle Daten auf Grund von Skalierbarkeit und der hohen Datenmenge auf der Blockchain gespeichert werden sollen. I5 beschreibt die Notwendigkeit, dass alle relevanten Informationen zur unmittelbaren Rückverfolgbarkeit auf der Blockchain gespeichert werden müssen. Die Definition, welche Daten notwendig sind, muss nach Chang et al. (2019, 4) und Xu et al. (2019a, 403ff.) sowie I5 und I6 pro eingesetztem Anwendungsszenario mit den Anwendern auf der Kollaborationsplattform abgestimmt werden. Die restlichen Daten sollen außerhalb der Plattform gespeichert werden. Die Prüfsummen dieser Daten werden jedoch auf der Blockchain gespeichert und basieren auf kryptografischen Hash-Funktionen (Person H).

REQ6: Es dürfen nur Datensätze auf der Blockchain gespeichert werden, die für die unmittelbare Rückverfolgbarkeit von Ergebnissen innerhalb von Wertschöpfungsnetzwerken notwendig sind. Die Definition der betroffenen Daten wird pro angewendetem Anwendungsszenario in Zusammenarbeit mit den zugehörigen Anwendern bestimmt.

REQ7: Daten, welche nicht auf der Blockchain gespeichert werden, sollen durch die Generierung von Prüfsummen auf Basis kryptografischer Hash-Funktionen auf ihre Unveränderlichkeit überprüft werden können. Die Speicherung der Prüfsumme erfolgt auf der Blockchain.

Cloud-Speicherung. Prozessdaten oder Transaktionen, welche für das Wertschöpfungs-netzwerk relevant sind, aber nicht auf der Blockchain gespei-chert werden sollen, müssen nach u.a. Lacity (2018, 221) oder Perboli et al. (2018, 62025) sowie I6 durch verschiedene Cloud-Lösungen permanent für alle Anwender verfügbar sein. I7 zeigt die Problematik, dass Cloud-Dienste wie Amazon Web Service nicht allen Ansprüchen z.B. in Punkten des Datenschutzes erfüllen können. Der Anwender I3 bestätigt diese Problematik. Daher muss für die Kollaborationsplattform eine Cloud-Lösung implementiert werden, welche allen Ansprüchen der Anwender entspricht. Person H ergänzt innerhalb der Validierung, dass diese Cloud-Lösungen ebenfalls dezentral sein müssen. Die Personen I und G definieren ebenso die Notwendigkeit von On-Premise-Lösungen für unternehmensinterne Daten, welche auf der Kollaborationsplattform, aber nicht auf der Blockchain gespeichert werden sollen.

REQ8: Für die Speicherung von Daten außerhalb der Blockchain müssen dezentrale Cloud-Lösungen eingesetzt werden, welche eine permanente Verfügbarkeit der Daten für die Anwender ermöglichen. Für unternehmensinterne Daten können On-Premise-Lösungen genutzt werden.

REQ9: Für die Speicherung von Daten außerhalb der Blockchain müssen dezentrale Cloud-Lösungen eingesetzt werden, die den Datenschutzansprüchen der Anwender genügen. Die Ansprüche müssen individuell mit allen Anwendern abgeglichen werden.

Dimension Datenaustausch

ERP. Für den automatisierten Austausch von Transaktionen zwischen mehreren ERP-Systemen von verschiedenen Unternehmen muss ein eStandard geschaffen werden. Diese Notwendigkeit wird in der Literatur durch u.a. Korpela et al. (2017, 4183) oder Westerkamp et al. (2018, 1) sowie durch die befragten Personen I5 und I7 beschrieben. Nur I7 spricht beispielhaft von dem Austausch von Metadaten mittels eines leichtgewichtigen Standards wie JSON oder XML. Bei der Befragung zeigt sich, dass alle Personen in der Rolle des Anwenders einen vorgeschlagenen Standard adaptieren würden. Diese Anwender nutzen zumeist ein eigens entwickeltes Dateiformat oder können darüber keine Aussage treffen. Daher ergibt sich folgende Anforderung:

REQ10: Für den Austausch von Transaktionsdaten zwischen verschiedenen ERP-Systemen sowie Unternehmen muss ein gemeinsames Datenformat festgelegt werden.

REQ11: Eine Adaption des Datenformates muss durch die Anwender erfolgen, um Transaktionen mittels der Blockchain zwischen den verschiedenen ERP-Systemen austauschen zu können.

Sensorik. Um eine standardisierte und automatisierte Auswertung von Sensordaten vornehmen zu können, muss für die eingesetzte Sensorik ebenfalls eine Dateistruktur festgelegt werden. Angrish et al. (2018, 1190f.), Hulea et al. (2018, 5) sowie Pustišek et al. (2019, 3) stellen das JSON- sowie das XML-Format vor. Diese Formate werden auch von den Personen I1 und I4 genannt. Die Person F schlägt zusätzlich die Betrachtung des IoT-Standards O-MI/O-DF vor.

REQ12: Für einen standardisierten und automatisierten Austausch von Daten muss die Plattform die Dateistruktur von JSON sowie XML unterstützen können.

Als Standard für den Datenaustausch muss nach I5 sowie I6 eine automatisierte und standardisierte Abfrage von Produktionsanlagen erfolgen. I5 und I6 beschreiben, dass viele Unternehmen hierfür bisher eine OPC-UA-Schnittstelle für die Abfrage der installierten SPS nutzen.

REQ13: Für die standardisierte und automatisierte Speicherung von Produktionsdaten auf der Blockchain muss die Kollaborationsplattform eine Schnittstelle zur Verfügung stellen, die den Datenaustauschstandard OPC-UA unterstützt.

Dimension Datenschutz

Rechtliche Handhabung. In einem Konsortium dürfen Anwender bzw. Unternehmen anonym auf der Blockchain interagieren (Moin et al. 2019, 333). Anhand der Schlüsselpaare sind Anwender oder die involvierten Unternehmen eindeutig identifizierbar (Leng et al. 2018, 643ff.). Jedoch dürfen keine personenbezogenen Daten in der Blockchain gespeichert werden, um die DSGVO nicht zu verletzen. Dies betrifft nicht nur Knoten, welche in Europa aktiv sind, sondern auch alle personenbezogenen Daten von EU Bürgern (Reyna et al. 2018, 174; George et al. 2019, 19). Dieser Sachverhalt wird ebenso von I1 und I4 bestätigt, welche zusätzlich die Speicherung von Prüfsummen von personenbezogenen Daten, auf Grund von fehlenden Gesetzen, als rechtlich bedenklich einstufen.

REQ14: Es dürfen keine personenbezogenen Daten sowie die Prüfsummen von diesen personenbezogenen Daten auf der Blockchain gespeichert werden.

Geheimhaltung von Daten. Bei der Geheimhaltung von Daten auf der Blockchain zeigen verschiedene Autoren wie Weber et al. (2019, 103) oder van Engelenburg et al. (2019, 606), dass es notwendig ist, verschiedene Zugriffsrechte für definierte Daten-sätze auf der Blockchain einzurichten. Diesem Sachverhalt stimmen alle befragten Personen in der Rolle des Anwenders zu (I1-I4). I1 beschreibt zusätzlich, dass konkurrierende Unternehmen auf der Plattform keinerlei Transaktionsverlauf mit Kunden oder anderen Unternehmen sehen dürfen. Dieser Sachverhalt ähnelt der Channel-Funktion der Hyperledger Fabric.

REQ15: Auf der Plattform muss ein mehrstufiges Rechtesystem für die Blockchain implementiert werden. Anhand dieses Rechtesystems werden die Lese- und Schreib-Rechte verschiedener Anwender festgelegt. Die Anzahl der Stufen sowie deren Abgrenzung muss durch eine weitere Evaluierung, mit den Anwendern, vorgenommen werden.

REQ16: Das implementierte Rechtesystem muss die Möglichkeit bieten, dass definierte Transaktionen sowie Daten nur für bestimmte Plattformteilnehmer sichtbar sind.

Staatliche Organisationen. Nach Moin et al. (2019, 333), Albrecht et al. (2018, 3532), I5 und I7 dürfen auf Grund von notwendigen Überprüfungen keinerlei Transaktionen vor staatlichen Organisationen vorborgen werden. Dies ist notwendig, um Steuerbetrug oder manipulierte Kontoführungen durch den Abgleich mit durchgeführten Prozessen innerhalb des Wertschöpfungsnetzwerkes ausfindig zu machen. Durch die Anforderungsvalidierung erhebt Person G und Person I, dass dies nur in Verdachtsfällen geschehen darf.

REQ17: Die Kollaborationsplattform muss staatlichen Organisationen in Verdachtsfällen zur Betrugsüberprüfung Lesezugriff auf alle in der Blockchain gespeicherten Daten bieten.

Dimension Verwaltung

Integration von Anwendern auf die Kollaborationsplattform. In der Literatur wird

durch verschiedene Autoren wie Glaser (2017, 1547) und Leng et al. (2018, 643) der Sachverhalt beschrieben, dass die Rechteverwaltung durch einen Super-Anwender geschehen soll, der dies anhand eines Benutzerverwaltungs-Services umsetzen kann. Dieser Sachverhalt wird durch die befragten Personen I5 und I7 ebenfalls bestätigt. Zusätzlich sieht I7 die Vor-aussetzung, mehrere dieser Administratoren in die Plattform zu integrieren. Anhand eines Mehrheits-Votums wird die Objektivität gesichert sowie ein single point of failure verhindert. Diese Adminis-trationsrolle wird durch einen Dienstleistungs-Provider durchgeführt (I7).

REQ18: Die Zulassung sowie das Entfernen von Anwendern innerhalb der Kollaborationsplattform muss durch Administratoren durchgeführt werden. Diese Aufgabe wird durch Dienstleistungs-Provider wahrgenommen.

REQ19: Die Zulassung oder der Ausschluss darf nicht nur durch einen Administrator durchgeführt werden. Alle Administratoren auf der Plattform müssen durch ein Mehrheits-Votum dem Vorgang zustimmen.

Die Zulassung von Unternehmen auf der Kollaborationsplattform darf nicht uneingeschränkt erfolgen, sondern muss anhand verschiedener Kriterien, wie z.B. die Geschäftslizenz oder die Liquidität bei Unternehmen, geprüft werden (Hua et al. 2018, 25650f.; Mao et al. 2018, 5). I9 und I10 empfehlen die Adaption des „Know-Your-Customer"-Prinzips, welches anhand von verschiedenen Wirt-schaftsauskünften erfolgen kann[1]. Ebenso beschreibt I8 und I10 die Überprüfung von technischen Anforderungen an das Unternehmen für die Betreibung eines Knoten.

REQ20: Vor der Zulassung eines Anwenders auf die Plattform muss eine Überprüfung erfolgen. Dies soll zum einen auf Basis von betriebswirtschaftlichen Faktoren nach dem „Know-Your-Customer"-Prinzip und zum anderen durch Überprüfungen auf Erfüllung von technischen Anforderungen für die Kollaborationsplattform erfolgen.

Verwaltung des Public/Private-Schlüsselpaares. Die Signierung und Validierung von Transaktionen sowie Smart Contracts erfolgen durch ein Public/Private-Schlüsselpaar, welches nach der Zulassung an den Anwender ausgehändigt wird. Verliert ein Anwender sein Schlüsselpaar, bedeutet dies einen Selbstausschluss aus der Kollaborationsplattform. I5, I6 und I9 schlagen die Entwicklung von Handlungsrichtlinien für die Anwender vor, um dem Verlust von Schlüsselpaaren entgegenzuwirken. Die Speicherung der Schlüsselpaare durch Dienstleistungs-Provider stellt nach I8 auf Grund von Missbrauchspotentialen keine Lösung dar.

REQ21: Um den Verlust von Public/Private-Schlüsselpaaren durch Anwender zu entgegenzuwirken, ist es notwendig, Handlungsempfehlungen für die-se zu entwickeln.

Entwicklungsunterstützung bei Smart Contracts. Die Befragung von Anwender und Dienstleistungs-Provider zeigt, dass die Plattform die Möglichkeit bieten muss, Smart Contracts zum einen durch Anwender selbst entwickeln zu lassen (I1), aber auch die Entwicklung in Abstimmung mit einem Dienstleistungs-Provider vornehmen zu können (I2 und I4).

REQ22: Die Entwicklung von Smart Contracts muss sowohl durch die Anwender als auch durch Dienstleistungs-Provider möglich sein.

REQ23: Die Dienstleistungs-Provider können die Entwicklung von Smart Contracts für die Anwender als Dienstleistung anbieten.

Zur Unterstützung sollen branchenspezifische und konfigurierbare Vorlagen entwickelt werden. Diese Vorlagen sollen durch eine Web-Schnittstelle adressierbar sein und durch eine Anleitung den Entwickler führen (Obour Agyekum et al. 2018, 1321). Zusätzlich soll der geschriebene Programmcode auch für nicht technische Anwender lesbar sein. Dies kann durch Pseudocode ermöglicht werden (I5, I6, I9 und I10). Durch grafische Modellierungswerkzeuge wie BPMN sollen zusätzlich Smart Contracts modularisierbar sein (I7 und I9).

REQ24: Für die Entwicklung von Smart Contracts müssen konfigurierbare und branchenspezifische Vorlagen angeboten werden. Diese Vorlagen sollen den Entwickler durch Tipps und Anleitungen, interaktiv eingebettet in die Vorlage, unterstützen.

REQ25: Anhand von grafischen Modellierungswerkzeugen müssen Smart Contracts modular und sequentiell entwickelt werden können.

REQ26: Die Smart-Contracts-Vorlagen müssen regulatorische und branchen-spezifische Anforderungen erfüllen.

REQ27: Die Smart-Contracts-Vorlagen müssen durch Web-Schnittstellen auf der Plattform adressierbar sein.

REQ28: Jeder Smart Contract muss durch die Darstellung des Quellcodes sowie des zugehörigen Pseudocodes nachvollziehbar sein.

Auf Grund der autonomen Ausführung von Smart Contracts auf der Blockchain müssen durch die Angabe von Zeitstempeln Gültigkeitsbereiche

[1] Das Know-Your-Customer-Prinzip beschreibt die Überprüfung von Neukunden anhand von Legitimationsprüfungen im Finanzbereich (Byrne 2000, 347ff.).

definiert werden (Bartoletti und Pompianu 2017, 228).

REQ29: Für jeden Smart Contract müssen zeitliche Gültigkeitsbereiche für dessen Ausführung definiert werden.

Verwaltung von Smart Contracts sowie Oracles. Um eine Verwaltung sowie Übersicht über die Blockchain-Implementierung auf der Kollaborationsplattform zu haben, ist es erforderlich, dass auf der Plattform eine nachvollziehbare und transparente Darstellung von aktiven Smart Contracts implementiert ist. Dies kann anhand einer Prozesskarte erfolgen (I5, I7 und I9) und soll eine Echtzeitüberwachung der Smart Contracts und deren Beziehungen ermöglichen (I9 und I10).

REQ30: Zur Anzeige von aktuell aktiven Smart Contracts muss eine Implementierung einer nachvollziehbaren und transparenten Darstellung erfolgen. Die Darstellung muss einen Überblick über unmittelbare Aktivitäten von Smart Contracts sowie deren Beziehungen zu weiteren Smart Contracts und Teilnehmern der Kollaborations-plattform bieten.

Sollten für die Ausführung von Smart Contracts Informationen, welche sich nicht auf der Plattform befinden, notwendig sein, muss der Einsatz von Oracles erfolgen (I6). Um die Integration von gefälschten oder manipulierten Informationen in die Plattform zu verhindern, sollen nach I7 nur zertifizierte Quellen in die Blockchain speichern dürfen. Person I und G ergänzen durch die Anforderungsvalidierung die Notwendigkeit, dass Oracles nur nach Bedarf innerhalb der eingesetzten Anwendungsszenarien implementiert werden sollen.

REQ31: Quellen, welche Informationen für Oracles auf der Kollaborationsplattform zur Verfügung stellen, müssen zertifiziert sein. Die Implementierung der Oracles erfolgt abhängig des eingesetzten Anwendungsszenarios.

Dimension Anwendungsmöglichkeiten. Die Kollaborationsplattform muss nach I9 und I10 zusätzlich eine Marktplatzkomponente enthalten, welche sich an bestehenden digitalen Handelsplattformen orientiert. Auf diesem Marktplatz sollen nach den beiden Interviewpartnern die Entwicklung von Smart Contracts oder Servicebündel z.B. durch weitere Analyseverfahren angeboten werden. Anhand von Suchfunktionen und Vorschlägen sollen Anwender gezielt nach Smart Contracts verschiedener Dienstleistungs-Provider suchen bzw. informiert werden. Gezielte Anpassungen sollen durch eine individuelle Absprache ermöglicht werden (I10).

REQ32: Die Kollaborationsplattform muss einen digitalen Marktplatz für Smart Contracts, Servicebündel oder weitere Dienstleistungen für die Anwender zur Verfügung stellen. Die Entwicklung der Leistungen erfolgt durch die Dienstleistungs-Provider.

REQ33: Anhand von Suchfunktionen sollen Anwender nach Dienstleistungen und Anbieter auf dem digitalen Marktplatz gezielt suchen können.

REQ34: Die Anwender sollen branchenspezifische Dienstleistungen über den digitalen Marktplatz der Kollaborationsplattform vorgeschlagen bekommen.

REQ35: Mittels einer Kommunikationsschnittstelle sollen Anwender und Dienstleistungs-Provider eine individuelle Anpassung von bestehenden Dienst-leistungen oder die Beauftragung von neuen Dienstleistungen vornehmen können.

Dimension Kryptowährung

Die Blockchain-Technologie ermöglicht den Einsatz von Kryptowährungen oder Tokens, um beispielsweise Güter automatisiert bezahlen zu können (Westerkamp et al. 2018, 7). Ebenso kann der Einsatz von Kryptowährung für die Realisierung von Marktplätzen genutzt werden (Yanovich et al. 2018, 3). Die Personen I und G definieren in der Anforderungsvalidierung als mögliche Alternative die Integration einer Schnittstelle zu einem bestehenden Token-System. Nach Glaser (2017, 1545f.) muss eine preisstabile Kryptowährung gewählt werden. Ebenso muss bei dem Einsatz von Tokens die Möglichkeit gegeben sein, diese wieder in eine traditionelle Währung umwandeln zu können. Auf Grund der Preisstabilität von Tokens im Vergleich zu Kryptowährungen sehen I2 und I4 primär den Einsatz von Tokens auf der Kollaborationsplattform. Auf Grund der fehlenden Preisstabilität von Kryptowährung ist nach I1 die Akzeptanz zu gering. I3 stellt heraus, dass neben Tokens auch traditionelle Bezahlmethoden wie z.B. Banküberwei-sungen oder Schecks weiterhin eingesetzt werden müssen.

REQ36: Die Kollaborationsplattform muss eine Bezahlung von Dienstleistungen sowie zur Abwicklung von automatisierten Transaktionen durch ein integriertes Token-System oder einer Schnittstelle zu einem Token-System ermöglichen.

REQ37: Die Kollaborationsplattform muss, bei einem integrierten Token-System, die Möglichkeit bieten, Tokens wieder in traditionelle Währungen wie Euro und Dollar umzutauschen.

REQ38: Neben dem Einsatz von Tokens sollen auch traditionelle Bezahlmethoden wie Banküberweisung und Schecks zum Bezahlen auf der Kollaborationsplattform bestehen.

Dimension externe Parteien

In der Literatur wird der Einsatz von Zertifizierungsstellen genutzt, um eine Validierung von Produkten oder Produktchargen vorzunehmen. Prüfpunkte können neben der

vertraglich vereinbarten Menge auch die Qualitätssicherung sein (Seebacher und Maleshkova 2018, 3494; Mandolla et al. 2019, 147). I1 und I2 bestätigten die Notwendigkeit des Einsatzes von Zertifizierungsstellen auf der Kollaborationsplattform. Die Autoren Moin et al. (2019, 334) ergänzen die zusätzliche Überprüfung von eingesetzter Sensorik in dem Wertschöpfungsnetzwerk.

REQ39: Auf der Kollaborationsplattform müssen Zertifizierungsstellen eingesetzt werden, welche die Überprüfung von Produkten, Produktchargen sowie eingesetzter Sensorik vornehmen.

Ebenso ist es nach George et al. (2019, 19) sowie I9 notwendig, eine Überprüfung von Smart Contracts sowie eine regelmäßige Zertifizierung von Oracles vorzunehmen. Durch Zertifizierungsstellen sollen diese auf Fehleranfälligkeit geprüft werden.

REQ40: Zertifizierungsstellen können die Überprüfung von Smart Contracts und Oracles auf Basis von Zertifikaten durchführen.

Dimension User-Interfaces

Die Dimension User-Interfaces beschreibt Anforderungen an die Anwender-Schnittstellen zu der Kollaborationsplattform.

Gestaltungsrichtlinien. Die Implementierung von User-Interfaces sollen nach Kim und Laskowski (2018, 234) anhand von leichtgewichtigen Frameworks erfolgen und auf verschiedenen Anwendungsgeräten abrufbar sein. Nach I1 bis I3 sollen auch mobile Endgeräte eingesetzt werden können. Die befragten Personen erwähnen hierbei die Entwicklung mittels HTML.

REQ41: Die User-Interfaces sollen durch eine Web-basierte Beschreibungssprache entwickelt werden, um verschiedenen Anwendungsgeräten wie PC, Smartphone oder Tablet einen Zugriff zu ermöglichen.

Alle implementierten User-Interfaces sollen nach I3 sowie I7 mindestens 99 Prozent der Zeit verfügbar sein. Ebenso darf eine Abfrage von Informationen nicht länger als 10 Sekunden dauern, bei internationalen Abfragen maximal zwei Minuten. Die Person B ergänzt innerhalb der Validierung die Einschränkung nur für Abfragen von Datenmengen aus der Blockchain.

REQ42: Alle implementierten User-Interfaces sollen zu mindestens 99 Prozent der Zeit verfügbar sein.

REQ43: Eine Abfrage von Daten aus der Blockchain, über ein User-Interface, darf nicht länger als 10 Sekunden dauern, bei internationalen Abfragen hingegen maximal 2 Minuten.

Handhabung von Falscheingaben. Autoren wie Zachariadis et al. (2019, 114) beschreiben die Problematik von manuellen Falscheingaben auf einer Blockchain-Plattform. Auf Grund der Datenstrukturen werden solche Daten unwiderruflich gespeichert. I6 und I7 bestätigen diese Problematik und stellen verschiedene Möglichkeiten vor. I7 stellt eine automatisierte Eingabevalidierung anhand von Plausibilitätsprüfungen dar, I6 sieht den Einsatz des 4-Augen-Prinzipes durch z.B. Vorgesetzte auf Grund der Verzögerung kritisch.

REQ44: Um manuelle Falscheingaben durch Anwender zu reduzieren, müssen automatisierte Plausibilitätsprüfungen der Eingaben in den User-Interfaces erfolgen. Die Definition der Plausibilitätsprüfungen erfolgt in Zusammenarbeit mit den Anwendern der Kollaborationsplattform.

Dimension weitere Aspekte

Sowohl Tian (2017, 3) als auch I6 verdeutlichen den Sachverhalt, dass viele Anwender mit der Blockchain-Thematik noch nicht vertraut sind. Um die Akzeptanz sowie eine reibungslose Handhabung der Plattform zu ermöglichen, ist es notwendig, für die verschiedenen Rollen der Kollaborationsplattform verschiedene Schulungen anzubieten. Person I und Person G ergänzen in der Validierungsphase zusätzlich die Notwendigkeit der Entwicklung von Schulungsvideos und Frequently Asked Questions (FAQ).

REQ45: Es müssen Schulungen, Schulungsvideos sowie FAQ zu der Blockchain-Thematik sowie der Benutzung der Kollaborationsplattform angeboten werden.

3.2.3 Ergebnis der Anforderungspriorisierung und -Klassifizierung

Die Studienteilnehmer werden durch die Umfrage gebeten, die vorgestellten Anforderungen zusätzlich zu priorisieren. Die Teilnehmer sollen für jede Anforderung eine Einschätzung geben. Anhand der Einschätzungen der Befragten werden die Anforderungen klassifiziert. Sollte bei einer Anforderung bei mehreren Antwortmöglichkeiten dieselbe Anzahl vorkommen, kann keine Entscheidung zur Einordnung getroffen werden. Daher wird zur eindeutigen Bestimmung eine numerische Priorisierung nach Berander und Andrews (2005, 67f.) vorgenommen. Jeder Antwortmöglichkeit wird daher ein folgender numerischer Wert zugewiesen:

- Muss = 1,00
- Wunsch = 0,00
- Abgrenzung = -1,00

Für jede $Anforderung_i$ mit der Menge $i = \{1, .., I\}$ wird die Summe aller $Entscheidungen_{i,j}$ durch die befragten $Personen_j$ $j = \{1, .., J\}$ addiert und durch die Gesamtanzahl aller Einordnungen pro Anforderungen geteilt. Dies erfolgt anhand folgender Formel:

$$Ergebnis_i = \frac{\sum_{j=1}^{J=9} Muss_{i,j} + \sum_{j=1}^{J=9} Wunsch_{i,j} + \sum_{j=1}^{J=9} Abgrenzung_{i,j}}{\sum_{j=1}^{J=9} Entscheidung_{i,j}} \quad \forall i$$

$$Entscheidung_{i,j} \neq Keine\ Einordnung \quad \forall i, j$$

Anhand der dargestellten Formel ist ein Wertebereich zwischen 1,0 und -1,0 möglich, wobei die Zahl 1,0 dafürsteht, dass alle Befragten der Anforderung die Priorisierung „Muss“ zugeordnet haben. Ist das Ergebnis -1,0, haben alle Befragten für die Anforderung die Priorisierung „Abgrenzung" gewählt. Ab dem Wert $Ergebnis_i \geq 0{,}34$ wird die Priorisierung „Muss“ ausgewählt. Sollte das $Ergebnis_i \leq -0{,}34$ dann wird die Priorisierung „Abgrenzung“ angenommen. Innerhalb dieses Zahlenbereiches wird die Priorisierung „Wunsch“ gewählt.
Dieses Vorgehen wird angewendet, um eine gleichmäßige Verteilung des Zahlenraumes -1 bis 1 für die drei Prioritäten zu ermöglichen. Um eine praktikable Anwendung zu ermöglichen, wird der Grenzwert von $\overline{0{,}3}$ bzw. $-\overline{0{,}3}$ auf 0,34 bzw. -0,34 gerundet. Der Sachverhalt wird durch folgende Abbildung verdeutlicht.

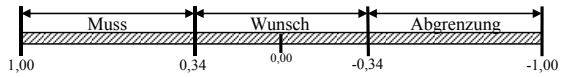


Abbildung B.1-2.4: Skala für die Einordnung der Priorisierung

Die Einschätzung „keine Einordnung“ wird nicht betrachtet und fliest nicht in die Summe aller Entscheidungen mit ein. Sollte eine befragte Person pro Anforderung mehr als eine Priorisierung ausgewählt haben, werden die Entscheidungen der Person der jeweiligen Anforderungen nicht weiter betrachtet. Das errechnete Ergebnis wird später anhand des Skalenraumes aus Abbildung B.1-2.4 wieder in die Klassifizierung „Muss“, „Wunsch“ und „Abgrenzung“ übertragen.
Im folgenden Kapitel wird durch eine tabellarische Darstellung die Anforderungsklassifikation dargestellt. Die Tabelle 11 stellt zum einen die Einordnung in funktionale bzw. nicht funktionale Anforderungen dar, zum anderen wird die Anzahl der Einschätzungen zu jeder Priorisierung sowie Anforderung dargestellt. Abschließend wird das $Ergebnis_i$ der jeweiligen $Anforderung_i$ dargestellt.

3.3 Ergebnis der Anforderungsanalyse

Folgende Tabellen stellen die Ergebnisse noch einmal kompakt zusammen:

Nr.	Anforderungsbeschreibung	Priorität
Plattformimplementierung		
Blockchain-Typ		
REQ1	Für die Kollaborationsplattform muss eine Implementierung in Form einer Konsortial-Blockchain erfolgen.	Muss
Blockchain-Implementierung		
REQ2	Die Softwareimplementierung der Blockchain muss anhand von Hyperledger Fabric erfolgen.	Muss
Konsens-Algorithmus		
REQ3	Bei der Wahl des Konsens-Algorithmus muss ein Verfahren gewählt werden, welches eine gleichmäßige Verteilung der Konsensbildung auf alle Anwender der Kollaborationsplattform ermöglicht.	Wunsch
REQ4	Alle Anwender müssen, nach Bedarf des Konsens-Algorithmus, an dem Prozess der Blockvalidierung teilnehmen. Die Anzahl der notwendigen Parteien für die Konsens-Bildung wird durch den Konsens-Algorithmus bestimmt.	Wunsch
Knotenstruktur		
REQ5	Beteiligte Unternehmen in der Kollaborationsplattform müssen die Möglichkeit haben, die Konsensbildung auf der Blockchain in Form einer kontinuierlichen Dienstleistung an Dienstleistungs-Provider auszulagern.	Muss
Datenspeicherung		
On- und Off-Chain		
REQ6	Es dürfen nur Datensätze auf der Blockchain gespeichert werden, die für die unmittelbare Rückverfolgbarkeit von Ergebnissen innerhalb von Wertschöpfungsnetzwerken notwendig sind. Die Definition der betroffenen Daten wird pro angewendetem Anwendungsszenario in Zusammenarbeit mit den zugehörigen Anwendern bestimmt.	Wunsch
REQ7	Daten, welche nicht auf der Blockchain gespeichert werden, sollen durch die Generierung von Prüfsummen auf Basis kryptografischer Hash-Funktionen auf ihre Unveränderlichkeit überprüft werden können. Die Speicherung der Prüfsumme erfolgt auf der Blockchain.	Muss
Cloud-Speicherung		
REQ8	Für die Speicherung von Daten außerhalb der Blockchain müssen dezentrale Cloud-Lösungen eingesetzt werden, welche eine permanente Verfügbarkeit der Daten für die Anwender ermöglichen. Für unternehmensinterne Daten können On-Premise-Lösungen genutzt werden.	Wunsch
REQ9	Für die Speicherung von Daten außerhalb der Blockchain müssen dezentrale Cloud-Lösungen eingesetzt werden, die den Datenschutzansprüchen der Anwender genügen. Die Ansprüche müssen individuell mit allen Anwendern abgeglichen werden.	Muss

Nr.	Anforderungsbeschreibung	Priorität
Datenaustausch		
ERP		
REQ10	Für den Austausch von Transaktionsdaten zwischen verschiedenen ERP-Systemen sowie Unternehmen muss ein gemeinsames Daten-Format festgelegt werden	Muss
REQ11	Eine Adaption des Daten-Formates muss durch die Anwender erfolgen, um Transaktionen mittels der Blockchain zwischen den verschiedenen ERP-Systemen austauschen zu können.	Muss
Sensorik		
REQ12	Für einen standardisierten und automatisierten Austausch von Daten muss die Plattform die Dateistruktur von JSON sowie XML unterstützen können.	Muss
REQ13	Für die standardisierte und automatisierte Speicherung von Produktionsdaten auf der Blockchain muss die Kollaborationsplattform eine Schnittstelle zur Verfügung stellen, die den Datenaustauschstandard OPC-UA unterstützt.	Wunsch
Datenschutz		
Rechtliche Handhabung		
REQ14	Es dürfen keine personenbezogenen Daten sowie die Prüfsummen von diesen personenbezogenen Daten auf der Blockchain gespeichert werden.	Muss
Geheimhaltung von Daten		
REQ15	Auf der Plattform muss ein mehrstufiges Rechtesystem für die Blockchain implementiert werden. Anhand dieses Rechtesystems werden die Lese- und Schreib-Rechte verschiedener Anwender festgelegt. Die Anzahl der Stufen sowie deren Abgrenzung müssen durch eine weitere Evaluierung mit den Anwendern vorgenommen werden.	Wunsch
REQ16	Das implementierte Rechtesystem muss die Möglichkeit bieten, dass definierte Transaktionen sowie Daten nur für bestimmte Plattformteilnehmer sichtbar sind.	Muss
Staatliche Organisationen		
REQ17	Die Kollaborationsplattform muss staatlichen Organisationen in Verdachtsfällen zur Betrugsüberprüfung Lesezugriff auf alle in der Blockchain gespeicherten Daten bieten.	Wunsch

Nr.	Anforderungsbeschreibung	Priorität
Verwaltung (1/2)		
Integration von Anwendern auf die Kollaborationsplattform		
REQ18	Die Zulassung sowie das Entfernen von Anwendern innerhalb der Kollaborationsplattform muss durch Administratoren durchgeführt werden. Diese Aufgabe wird durch Dienstleistungs-Provider wahrgenommen.	Wunsch
REQ19	Die Zulassung oder der Ausschluss darf nicht nur durch einen Administrator durchgeführt werden. Alle Administratoren auf der Plattform müssen durch ein Mehrheits-Votum dem Vorgang zustimmen.	Muss
REQ20	Vor der Zulassung eines Anwenders auf die Plattform muss eine Überprüfung erfolgen. Dies soll zum einen auf Basis von betriebswirtschaftlichen Faktoren nach dem „Know-Your-Customer"-Prinzip und zum anderen durch Überprüfungen auf Erfüllung von technischen Anforderungen für die Kollaborationsplattform erfolgen.	Muss
Verwaltung des Public/Private-Schlüsselpaares		
REQ21	Um dem Verlust von Public/Private-Schlüsselpaaren durch Anwender entgegenzuwirken, ist es notwendig, Handlungsempfehlungen für diese zu entwickeln.	Muss
Entwicklungsunterstützung bei Smart Contracts		
REQ22	Die Entwicklung von Smart Contracts muss sowohl durch die Anwender als auch durch Dienstleistungs-Provider möglich sein.	Muss
REQ23	Die Dienstleistungs-Provider können die Entwicklung von Smart Contracts für die Anwender als Dienstleistung anbieten.	Muss
REQ24	Für die Entwicklung von Smart Contracts müssen konfigurierbare und branchenspezifische Vorlagen angeboten werden. Diese Vorlagen sollen den Entwickler durch Tipps und Anleitungen, interaktiv eingebettet in die Vorlage, unterstützen.	Wunsch
REQ25	Anhand von grafischen Modellierungswerkzeugen müssen Smart Contracts modular und sequentiell entwickelt werden können.	Wunsch
REQ26	Die Smart-Contracts-Vorlagen müssen regulatorische und branchenspezifische Anforderungen erfüllen.	Muss
REQ27	Die Smart-Contracts-Vorlagen müssen durch Web-Schnittstellen auf der Plattform adressierbar sein.	Wunsch
REQ28	Jeder Smart Contract muss durch die Darstellung des Quellcodes sowie des zugehörigen Pseudocodes nachvollziehbar sein.	Muss
REQ29	Für jeden Smart Contract müssen zeitliche Gültigkeitsbereiche für dessen Ausführung definiert werden.	Wunsch

Nr.	Anforderungsbeschreibung	Priorität
Verwaltung (2/2)		
Verwaltung von Smart Contracts sowie Oracles		
REQ30	Zur Anzeige von aktuell aktiven Smart Contracts muss eine Implementierung einer nachvollziehbaren und transparenten Darstellung erfolgen. Die Darstellung muss einen Überblick über unmittelbare Aktivitäten von Smart Contracts sowie deren Beziehungen zu weiteren Smart Contracts und Teilnehmern der Kollaborationsplattform bieten.	Muss
REQ31	Quellen, welche Informationen für Oracles auf der Kollaborationsplattform zur Verfügung stellen, müssen zertifiziert sein. Die Implementierung der Oracles erfolgt abhängig des eingesetzten Anwendungsszenarios.	Muss
Anwendungsmöglichkeiten		
REQ32	Die Kollaborationsplattform muss einen digitalen Marktplatz für Smart Contracts, Servicebündel oder weitere Dienstleistungen für die Anwender zur Verfügung stellen. Die Entwicklung der Leistungen erfolgt durch die Dienstleistungs-Provider.	Wunsch
REQ33	Anhand von Suchfunktionen sollen Anwender nach Dienstleistungen und Anbieter auf dem digitalen Marktplatz gezielt suchen können.	Muss
REQ34	Die Anwender sollen branchenspezifische Dienstleistungen über den digitalen Marktplatz der Kollaborationsplattform vorgeschlagen bekommen.	Wunsch
REQ35	Mittels einer Kommunikationsschnittstelle sollen Anwender und Dienstleistungs-Provider eine individuelle Anpassung von bestehenden Dienstleistungen oder der Beauftragung von neuen Dienstleistungen vornehmen können.	Wunsch
Kryptowährung		
REQ36	Die Kollaborationsplattform muss eine Bezahlung von Dienstleistungen sowie zur Abwicklung von automatisierten Transaktionen durch ein integriertes Token-System oder eine Schnittstelle zu einem Token-System ermöglichen.	Wunsch
REQ37	Die Kollaborationsplattform muss, bei einem integrierten Token-System, die Möglichkeit bieten, Tokens wieder in traditionelle Währungen wie Euro und Dollar umzutauschen.	Muss
REQ38	Neben dem Einsatz von Tokens sollen auch traditionelle Bezahlmethoden wie Banküberweisung und Schecks zum Bezahlen auf der Kollaborationsplattform bestehen.	Muss
Externe Parteien		
REQ39	Auf der Kollaborationsplattform müssen Zertifizierungsstellen eingesetzt werden, welche die Überprüfung von Produkten, Produktchargen sowie eingesetzter Sensorik vornehmen.	Wunsch
REQ40	Zertifizierungsstellen können die Überprüfung von Smart Contracts und Oracles, auf Basis von Zertifikaten, durchführen.	Wunsch

Nr.	Anforderungsbeschreibung	Priorität
	User-Interfaces	
	Gestaltungsrichtlinien	
REQ41	Die entwickelten User-Interfaces sollen auf der Beschreibungssprache HTML basieren, um verschiedenen Anwendungsgeräten wie PC, Smartphone oder Tablet einen Zugriff zu ermöglichen.	Muss
REQ42	Alle implementierten User-Interfaces sollen zu mindestens 99 Prozent der Zeit verfügbar sein.	Muss
REQ43	Eine Abfrage von Daten aus der Blockchain über ein User-Interface darf nicht länger als 10 Sekunden dauern, bei internationalen Abfragen hingegen maximal 2 Minuten.	Muss
	Handhabung von Falscheingaben	
REQ44	Um manuelle Falscheingaben durch Anwender zu reduzieren, müssen automatisierte Plausibilitätsprüfungen der Eingaben in den User-Interfaces erfolgen. Die Definition der Plausibilitätsprüfungen erfolgt in Zusammenarbeit mit den Anwendern der Kollaborationsplattform.	Wunsch
	Weitere Aspekte	
REQ45	Es müssen Schulungen, Schulungsvideos sowie FAQ zu der Blockchain-Thematik sowie der Benutzung der Kollaborationsplattform angeboten werden.	Muss

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Juniorprofessur für Information Management
Prof. Dr. Christian Janiesch
Stephanstraße 1
97070 Würzburg
https://www.wiwi.uni-wuerzburg.de/lehrstuhl/bwljp1/startseite/

Autoren und Ansprechpartner

Lukas-Valentin Herm, M.Sc.

Wissenschaftlicher Mitarbeiter
lukas-valentin.herm@uni-wuerzburg.de
+49 931 31-81730

Prof. Dr. Christian Janiesch

Juniorprofessur für Information Management
christian.janiesch@uni-wuerzburg.de
+49 931 31-84930

B3 & B4: Pflichtenheft

Aus den Anforderungen an die Plattform wurden Maßnahmen erarbeitet und Zuständigkeiten für die Umsetzung zugeordnet. Daraus wurde ein Pflichtenheft entwickelt, um den weiteren Projektverlauf strukturiert zu gestalten.

Pflichtenheft für das Verbundprojekt PIMKoWe

Nr.	Anforderungsbeschreibung / Maßnahme	Priorität
	Thematik Plattformimplementierung	
REQ1	Für die Kollaborationsplattform muss eine Implementierung in Form einer Konsortial-Blockchain erfolgen.	Muss
REQ2	Die Softwareimplementierung der Blockchain muss anhand von Hyperledger Fabric erfolgen. Aus REQ1 und REQ2 ergibt sich, dass eine Hyperledger Fabric Konsortial-Blockchain zum Einsatz kommen soll. Zunächst muss dazu ein Testnetz aufgesetzt werden. Zuständigkeit: Universität Würzburg	Muss
REQ3	Bei der Wahl des Konsens-Algorithmus muss ein Verfahren gewählt werden, welches eine gleichmäßige Verteilung der Konsensbildung auf alle Anwender der Kollaborationsplattform ermöglicht. Es müssen verschiedene Konsensalgorithmen überprüft werden. Die gleichmäßige Verteilung der Konsensbildung darf dabei nicht zu Lasten der Skalierbarkeit der Blockchainlösung gehen. Zuständigkeit: Universität Würzburg	Wunsch
REQ4	Alle Anwender müssen nach Bedarf des Konsens-Algorithmus an dem Prozess der Blockvalidierung teilnehmen. Die Anzahl der notwendigen Parteien für die Konsens-Bildung wird durch den Konsens-Algorithmus bestimmt.	Wunsch
REQ5	Beteiligte Unternehmen in der Kollaborationsplattform müssen die Möglichkeit haben, die Konsensbildung auf der Blockchain in Form einer kontinuierlichen Dienstleistung an Dienstleistungsprovider auszulagern. Es muss geprüft werden, ob es ausreichend ist, die beteiligten Unternehmen über Light-Nodes anzubinden, die am Konsens-Verfahren nicht teilnehmen. Zuständigkeit: Actiware	Muss
	Thematik Datenspeicherung	
REQ6	Es dürfen nur Datensätze auf der Blockchain gespeichert werden, die für die unmittelbare Rückverfolgbarkeit von Ergebnissen innerhalb von Wertschöpfungsnetzwerken notwendig sind. Die Definition der betroffenen Daten wird pro angewendetem Anwendungsszenario in Zusammenarbeit mit den zugehörigen Anwendern bestimmt. Je nach Anwendungsszenario sind unterschiedliche Datenpakete notwendig. Diese werden je nach Modul vor Beginn der Entwicklung festgelegt, sollen jedoch auch nachträglich flexibel gestaltet werden können. Bei der Definition der Datenpakete wird auf die Einhaltung gängiger elektronischer Austauschstandards geachtet. Zuständigkeit: Universität Würzburg	Wunsch
REQ7	Daten, welche nicht auf der Blockchain gespeichert werden, sollen durch die Generierung von Prüfsummen auf Basis kryptografischer Hash-Funktionen auf ihre Unveränderlichkeit überprüft werden können. Die Speicherung der Prüfsumme erfolgt auf der Blockchain.	Muss

	Es wird die Anbindung an Dokumentenverwaltungssysteme gewährleistet. Zur Generierung von Prüfsummen werden Hash-Funktionen auf Basis des secure hash algorithm (SHA-3) mit Schnittstellen zu unterschiedlichen dezentralen Speicher- und Dokumentenverwaltungssystemen implementiert. Die Prüfsummen können anschließend auf der Blockchain revisionistischer abgelegt werden. **Zuständigkeit**: Actiware	
REQ8	Für die Speicherung von Daten außerhalb der Blockchain müssen dezentrale Cloud-Lösungen eingesetzt werden, welche eine permanente Verfügbarkeit der Daten für die Anwender ermöglichen. Für unternehmensinterne Daten können On-Premise-Lösungen genutzt werden. Für Daten, welche nicht auf einem lokalen Datenspeichersystem abgelegt werden können, wird die Integration des InterPlanetary File System (IPFS) implementiert. **Zuständigkeit**: Actiware	Wunsch
REQ9	Für die Speicherung von Daten außerhalb der Blockchain müssen dezentrale Cloud-Lösungen eingesetzt werden, welche den Datenschutzansprüchen der Anwender genügen. Die Ansprüche müssen individuell mit allen Anwendern abgeglichen werden. Für Daten, welche nicht auf einem lokalen Datenspeichersystem abgelegt werden können, wird die Integration des InterPlanetary File System (IPFS) implementiert. **Zuständigkeit**: Universität Würzburg	Muss
	Thematik Datenaustausch	
REQ10	Für den Austausch von Transaktionsdaten zwischen verschiedenen ERP-Systemen sowie Unternehmen muss ein gemeinsames Datenformat festgelegt werden. Zum Austausch zwischen ERP-Systemen wird ein einheitliches Datenformat festgelegt, welches gängigen elektronischen Austauschstandards folgt. Dabei wird jedoch auch eine flexible Anpassung für künftige Änderungen berücksichtigt. **Zuständigkeit**: Universität Würzburg & Infosim	Muss
REQ11	Eine Adaption des Datenformates muss durch die Anwender erfolgen, um Transaktionen mittels der Blockchain zwischen den verschiedenen ERP-Systemen austauschen zu können. Zum Austausch zwischen ERP-Systemen wird ein einheitliches Datenformat festgelegt, welches gängigen elektronischen Austauschstandards folgt. Dabei wird jedoch auch eine flexible Anpassung für künftige Änderungen berücksichtigt. **Zuständigkeit**: APE & Maul-Theet.	Muss
REQ12	Für einen standardisierten und automatisierten Austausch von Daten muss die Plattform die Dateistruktur von JSON sowie XML unterstützen können.	Muss
REQ13	Für die standardisierte und automatisierte Speicherung von Produktionsdaten auf der Blockchain muss die Kollaborationsplattform eine Schnittstelle zur Verfügung stellen, die den Datenaustauschstandard OPC-UA unterstützt. Zum Austausch zwischen ERP-Systemen wird ein einheitliches Datenformat festgelegt, welches gängigen elektronischen Austauschstandards folgt. Eine Umsetzung erfolgt als REST-API, welche u. a. die gängigen Datenformate XML, JSON und OPC-UA unterstützt. **Zuständigkeit**: Signavio.	Wunsch

	Thematik Datenschutz	
REQ14	Es dürfen keine personenbezogenen Daten sowie die Prüfsummen von diesen personenbezogenen Daten auf der Blockchain gespeichert werden. Je nach Anwendungsfall kann auch eine Speicherung von personenbezogenen Daten auf der Blockchain notwendig sein. Nach den Regeln der DSGVO wird die Blockchain jedoch nach dem Grundsatz „privacy by design“ grundsätzlich ohne personenbezogene Daten verwendet. **Zuständigkeit**: Universität Würzburg	Muss
REQ15	Auf der Plattform muss ein mehrstufiges Rechtesystem für die Blockchain implementiert werden. Anhand dieses Rechtesystems werden die Lese- und Schreib-Rechte verschiedener Anwender festgelegt. Die Anzahl der Stufen sowie deren Abgrenzung müssen durch eine weitere Evaluierung mit den Anwendern vorgenommen werden.	Wunsch
REQ16	Das implementierte Rechtesystem muss die Möglichkeit bieten, dass definierte Transaktionen sowie Daten nur für bestimmte Plattformteilnehmer sichtbar sind.	Muss
REQ17	Die Kollaborationsplattform muss staatlichen Organisationen in Verdachtsfällen zur Betrugsüberprüfung Lesezugriff auf alle in der Blockchain gespeicherten Daten bieten. Zur Implementierung eines mehrstufigen Rechtesystems bietet Hyperledger eine Konfiguration der einzelnen Nutzer. So lässt sich ein Rechtesystem je nach Anforderung der einzelnen Anwendung umsetzen. **Zuständigkeit**: Signavio	Wunsch
	Thematik Plattformverwaltung	
REQ18	Die Zulassung sowie das Entfernen von Anwendern innerhalb der Kollaborationsplattform muss durch Administratoren durchgeführt werden. Diese Aufgabe wird durch Dienstleistungsprovider wahrgenommen. Die Hyperledger Instanz muss so konfiguriert werden, dass von vorneherein privilegierte Benutzer angelegt sind. **Zuständigkeit**: Signavio	Wunsch
REQ19	Die Zulassung oder der Ausschluss darf nicht nur durch einen Administrator durchgeführt werden. Alle Administratoren auf der Plattform müssen durch ein Mehrheits-Votum dem Vorgang zustimmen. Es muss ein Smart-Contract erstellt werden, der eine Voting-Funktion abbildet. Dieser Smart-Contract soll nur Stimmen von Administratoren berücksichtigen und bei Erfolg automatisch neue Nutzer zulassen oder bestehende Nutzer ausschließen. **Zuständigkeit**: Infosim	Muss
REQ20	Vor der Zulassung eines Anwenders auf die Plattform muss eine Überprüfung erfolgen. Dies soll zum einen auf Basis von betriebswirtschaftlichen Faktoren nach dem „Know-Your-Customer“-Prinzip und zum anderen durch Überprüfungen auf Erfüllung von technischen Anforderungen für die Kollaborationsplattform erfolgen. Es müssen Faktoren definiert werden, aufgrund deren eine Zulassung zur Plattform ermöglicht wird. Die Überprüfung der Voraussetzungen sollte möglichst automatisiert ablaufen. Durch Vorarbeiten der Universität Würzburg können diese eventuell auch dezentral geprüft werden und der Zulassungsprozess vollständig automatisiert werden. **Zuständigkeit**: Universität Würzburg	Muss

REQ21	Um dem Verlust von Public/Private-Schlüsselpaaren durch Anwender zu entgegenzuwirken, ist es notwendig, Handlungsempfehlungen für diese zu entwickeln. Es müssen “Best Practices” für den Umgang mit Private Keys ermittelt, evaluiert und geteilt werden. Hierzu werden Erfahrungen für die Private Key Verwaltung aus verwandten Bereichen wie Server-Wartung und Schlüsselverwaltung bei Crypto-Börsen herangezogen. **Zuständigkeit**: Universität Würzburg	Muss
REQ22	Die Entwicklung von smart contracts muss sowohl durch die Anwender als auch durch Dienstleistungsprovider möglich sein. Das Berechtigungssystem wird darauf konfiguriert, dass jeder Teilnehmer Smart-Contracts erstellen und verteilen kann. Ein Leitfaden für die sichere Erstellung von Smart Contracts sowie technische Hilfsmittel werden zur Verfügung gestellt. (bspw. BPMN Compiler) **Zuständigkeit**: Signavio	Muss
REQ23	Die Dienstleistungsprovider können die Entwicklung von smart contracts für die Anwender als Dienstleistung anbieten. Dienstleistungsprovider müssen eine Plattform bieten, die bei der Erstellung der Smart-Contracts unterstützt oder im Austausch mit den Nutzern maßgeschneiderte Smart-Contracts erstellt. Hierzu müssen rechtliche und technische Rahmenbedingungen geprüft werden. **Zuständigkeit**: Infosim	Muss
REQ24	Für die Entwicklung von smart contracts müssen konfigurierbare und branchenspezifische Vorlagen angeboten werden. Diese Vorlagen sollen den Entwickler durch Tipps und Anleitungen, interaktiv eingebettet in die Vorlage, unterstützen. Neben der Erstellung des Leitfadens und der technischen Hilfsmittel müssen häufig verwendete oder besonders sicherheitskritische Funktionen identifiziert und als vorkompilierte Smart-Contracts zur Verfügung gestellt werden. **Zuständigkeit**: Universität Würzburg	Wunsch
REQ25	Anhand von grafischen Modellierungswerkzeugen müssen smart contracts modular und sequenziell entwickelt werden können. Siehe REQ 22	Wunsch
REQ26	Die smart-contracts-Vorlagen müssen regulatorische und branchenspezifische Anforderungen erfüllen. Es muss während der Entwicklung eine fortlaufende Kontrolle durchgeführt werden, ob die Anforderungen erfüllt sind. Bei Nichterfüllung müssen entsprechende Gegenmaßnahmen getroffen werden. **Zuständigkeit**: Infosim	Muss
REQ27	Die smart-contracts-Vorlagen müssen durch Web-Schnittstellen auf der Plattform adressierbar sein. Dieser Punkt muss noch einmal überarbeitet werden. Eine Adressierung über Webschnittstellen ist nicht immer zielführend, da Smart-Contracts sich gegenseitig ohne Web-Schnittstellen aufrufen können. Anforderung neu prüfen. **Zuständigkeit**: Universität Würzburg	Wunsch

REQ28	Jeder smart contract muss durch die Darstellung des Quellcodes sowie des zugehörigen Pseudocodes nachvollziehbar sein. Bei der Entwicklung der Smart-Contracts ist eine umfassende Dokumentation Pflicht. Smart-Contracts dürfen nur zusammen mit einer Dokumentation veröffentlicht werden. **Zuständigkeit**: alle	Muss
REQ29	Für jeden smart contract müssen zeitliche Gültigkeitsbereiche für dessen Ausführung definiert werden. Smart-Contracts dürfen nur mit zeitlichem Gültigkeitsbereich veröffentlicht werden. Sollte der Gültigkeitsbereich zeitlich unbestimmt sein, so muss dies explizit in der Dokumentation erwähnt werden. **Zuständigkeit**: alle	Wunsch
REQ30	Zur Anzeige von aktuell aktiven smart contracts muss eine Implementierung einer nachvollziehbaren und transparenten Darstellung erfolgen. Die Darstellung muss einen Überblick über unmittelbare Aktivitäten von smart contracts sowie deren Beziehungen zu weiteren smart contracts und Teilnehmern der Kollaborationsplattform bieten. Die Plattform erhält ein Tracking-Feature, das neue Smart-Contracts automatisch inclusive Dokumentation in eine Datenbank aufnimmt. Die Datenbank steht allen Teilnehmern zur Verfügung. **Zuständigkeit**: Universität Würzburg	Muss
REQ31	Quellen, welche Informationen für oracles auf der Kollaborationsplattform zur Verfügung stellen, müssen zertifiziert sein. Die Implementierung der oracles erfolgt abhängig des eingesetzten Anwendungsszenarios. Wie bei der Zertifizierung der Teilnehmer wird auch eine automatische Zertifizierung der oracles angestrebt. Zertifizierung nicht zielführend --> Teilnehmern müssen Konsens finden, welches Oracle vertrauenswürdig ist durch internes Voting der Nutzer **Zuständigkeit**: Universität Würzburg	Muss
	Thematik Marktplatz/ Dienstleistungen	
REQ32	Die Kollaborationsplattform muss einen digitalen Marktplatz für smart contracts, Servicebündel oder weitere Dienstleistungen für die Anwender zur Verfügung stellen. Die Entwicklung der Leistungen erfolgt durch die Dienstleistungsprovider. In die Plattform, welche durch Hyperledger Fabric umgesetzt wird, wird durch ein zusätzliches Modell ein Marktplatz zur Verfügung gestellt. Das Marktplatz-Modul wird durch einen Webserver umgesetzt und basiert auf einem bestehenden CMS von Actiware. **Zuständigkeit**: Actiware	Wunsch
REQ33	Anhand von Suchfunktionen sollen Anwender nach Dienstleistungen und Anbieter auf dem digitalen Marktplatz gezielt suchen können. Suchfunktionen innerhalb des Marktplatz-Moduls ermöglichen eine gezielte Abfrage von Services, welche durch ein Content-Management-System verwaltet werden. **Zuständigkeit**: Actiware & Infosim.	Muss
REQ34	Die Anwender sollen branchenspezifische Dienstleistungen über den digitalen Marktplatz der Kollaborationsplattform vorgeschlagen bekommen.	Wunsch

	Durch das Netzwerkanalysemanagement-Tool StableNet von Infosim werden bestehende und aktive Dienstleistungen wie z.B. Smart Contracs und den Besitzern dieser zugehörigen Dienstleistungselemente vorgeschlagen. **Zuständigkeit**: Infosim	
REQ35	Mittels einer Kommunikationsschnittstelle sollen Anwender und Dienstleistungsprovider eine individuelle Anpassung von bestehenden Dienstleistungen oder der Beauftragung von neuen Dienstleistungen vornehmen können. Im Zuge der Entwicklung des Marktplatzes soll eine Kommunikationsschnittstelle integriert werden. **Zuständigkeit**: Actiware	Wunsch
	Thematik Kryptowährung bzw. Token	
REQ36	Die Kollaborationsplattform muss eine Bezahlung von Dienstleistungen sowie die Abwicklung von automatisierten Transaktionen durch ein integriertes Token-System oder eine Schnittstelle zu einem Token-System ermöglichen. Es werden Smart-Contracts vorbereitet, die grundlegende Token-Funktionalitäten abbilden (vgl. ERC20). **Zuständigkeit**: Infosim	Wunsch
REQ37	Die Kollaborationsplattform muss bei einem integrierten Token-System die Möglichkeit bieten, Tokens wieder in traditionelle Währungen wie Euro und Dollar umzutauschen. Es werden Smart-Contracts vorbereitet, die einen Handelsmechanismus abbilden. So sollen sowohl Token gegen andere Token handelbar, als auch Token gegen Fiatgeld handelbar werden. **Zuständigkeit**: Infosim	Muss
REQ38	Neben dem Einsatz von Tokens sollen auch traditionelle Bezahlmethoden wie Banküberweisung und Schecks zum Bezahlen auf der Kollaborationsplattform bestehen. Es werden Orakel entwickelt, die Daten von vertrauenswürdigen Bank-APIs abgreifen und für Smart-Contracts nutzbar machen. **Zuständigkeit**: Infosim	Muss
	Externe Parteien	
REQ39	Auf der Kollaborationsplattform müssen Zertifizierungsstellen eingesetzt werden, welche die Überprüfung von Produkten, Produktchargen sowie eingesetzter Sensorik vornehmen. Bei der Implementierung der Blockchain werden Nutzer für externe Parteien angelegt. **Zuständigkeit**: Signavio	Wunsch
REQ40	Zertifizierungsstellen können die Überprüfung von smart contracts und oracles auf Basis von Zertifikaten durchführen. Für sicherheitskritische Smart-Contracts werden Zertifizierungsbestimmungen erarbeitet und evaluiert. **Zuständigkeit**: Universität Würzburg	Wunsch

	Thematik User-Interface	
REQ41	Die entwickelten User-Interfaces sollen auf der Beschreibungssprache HTML basieren, um verschiedenen Anwendungsgeräten wie PC, Smartphone oder Tablet einen Zugriff zu ermöglichen. Die User-Interfaces werden mit Standard Web-Frameworks entwickelt. Dabei wird auf eine Unterstützung von responsive Design geachtet. **Zuständigkeit**: alle	Muss
REQ42	Alle implementierten User-Interfaces sollen zu mindestens 99 Prozent der Zeit verfügbar sein. Die User-Interfaces werden so entwickelt, dass sie ohne zentrales Backend funktionieren können. Somit kann auf jedem Knoten die Nutzeroberfläche bereitgestellt werden. **Zuständigkeit**: alle	Muss
REQ43	Eine Abfrage von Daten aus der Blockchain über ein User-Interface darf nicht länger als 10 Sekunden dauern. Bei internationalen Abfragen hingegen maximal 2 Minuten. Die Nutzeroberfläche liegt direkt bei den Blockchain-Knoten, um Latenzen zu vermeiden. Sonstige Verzögerungen, die durch die Blockgenerierung entstehen, werden durch eine möglichst kurze Blockzeit so gering wie möglich gehalten. **Zuständigkeit**: Signavio	Muss
REQ44	Um manuelle Falscheingaben durch Anwender zu reduzieren, müssen automatisierte Plausibilitätsprüfungen der Eingaben in den User-Interfaces erfolgen. Die Definition der Plausibilitätsprüfungen erfolgt in Zusammenarbeit mit den Anwendern der Kollaborationsplattform. Bei der Implementierung des Frontends muss eine clientseitige Validierung mittels HTML5 und JavaScript verwendet werden, bevor Daten an die Blockchain gesendet werden. **Zuständigkeit**: alle	Wunsch
	Weitere Aspekte	
REQ45	Es müssen Schulungen, Schulungsvideos sowie FAQ zu der Blockchain-Thematik sowie der Benutzung der Kollaborationsplattform angeboten werden. Während der Projektlaufzeit werden fortlaufend die Konzepte mit den Evaluationspartnern getestet und typische Fragestellungen festgehalten. Aus den Erkenntnissen werden Schulungsunterlagen und Erklärvideos erstellt. **Zuständigkeit**: Universität Würzburg	Muss

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION

actiware®
DEVELOPMENT

MAUL-THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Juniorprofessur für Information Management
Prof. Dr. Christian Janiesch
Stephanstraße 1
97070 Würzburg
https://www.wiwi.uni-wuerzburg.de/lehrstuhl/bwljp1/startseite/

Autoren und Ansprechpartner

Lukas-Valentin Herm, M.Sc.

Wissenschaftlicher Mitarbeiter
lukas-valentin.herm@uni-wuerzburg.de
+49 931 31-81730

Prof. Dr. Christian Janiesch

Juniorprofessur für Information Management
christian.janiesch@uni-wuerzburg.de
+49 931 31-84930

B5: Analyse von Betreiber- und Gebührenmodellen für Blockchain-basierte Plattformen

Digitale Plattformen haben in den letzten Jahren durch den Einsatz neuer Technologien den Innovationsdruck auf Unternehmen mit klassischen Geschäftsmodellen verstärkt. Historisch basiert die Architektur digitaler Plattformen auf einem zentralisierten Ansatz, bei welchem der Betreiber der Plattform als Intermediär fungiert. Mit dem disruptiven Potential der Blockchain-Technologie können Plattformen dezentral gestaltet werden und eröffnen zahlreiche Anwendungsmöglichkeiten in der Praxis. Zur Sicherstellung der langfristigen Wirtschaftlichkeit des Forschungsprojekts „PIMKoWe“ werden in diesem Arbeitspaket nachhaltige Betreiber und Gebührenmodelle Blockchain-basierter Plattformen untersucht. Als Benchmarking werden bestehende Geschäftsmodelle Blockchain-basierter Plattformen analysiert und geeignete Frameworks für die Geschäftsmodelle identifiziert.

1 Betreiber- und Gebührenmodelle dezentraler Plattformen

Die Blockchain-Technologie bietet mit ihrem Konzept der dezentralen Datenspeicherung und Konsensfindung vielfältige und branchenunabhängige Anwendungsmöglichkeiten. Längst sind es nicht mehr nur die Start-ups, welche sich mit der Blockchain-Technologie auseinandersetzen, sondern seit einigen Jahren auch große und traditionelle Unternehmen wie IBM Watson, Microsoft oder Wal-mart. Um das volle Potential der Dezentralität der Blockchain-Technologie zu nutzen, ist die Adaption der Blockchain-Technologie in die Geschäftsmodelle notwendig (Morabito 2017).

Insbesondere mit dem Fokus auf Transparenz und effiziente Nutzung von Informationen (Kouhizadeh, Saberi, und Sarkis 2021) hat die Blockchain-Technologie Auswirkungen auf die Geschäftsmodelle digitaler Plattformen. Typische Beispiele für Serviceanbieter digitaler zweiseitiger Plattformarchitekturen sind beispielweise Uber, Airbnb oder eBay. Plattformanbieter, die als Intermediäre für einen zweiseitigen Markt fungieren, besitzen häufig ein Monopol auf das Angebot ihrer Services. Folglich können sie hohe Gebühren für Transaktionen auf ihren Plattformen verlangen. Inzwischen existieren zunehmend Stimmen, die eine kostengünstigere und sicherere Lösung fordern (Hadi, Dmitry, und Azamat 2018).

Mit dem Konzept der dezentralen Plattformtechnologie kann die traditionell zweiseitige Architektur einer Plattform aufgebrochen werden. Als Folge kann dem Abhängigkeitsverhältnis der Teilnehmer der Plattform gegenüber dem Betreiber entgegengewirkt werden. Zudem eignet sich die Blockchain-Technologie aufgrund ihrer diversen Einsatzmöglichkeiten. Trotz der vielfältigen potentiellen Anwendungsfelder und Vorteile dezentraler Plattformen, werden von Unternehmen Barrieren, wie bspw. mangelnde Skalierbarkeit, mangelnde Interoperabilität (Onik und Miraz 2019) wahrgenommen.

Das Angebot einer Plattform für das integrierte Management von Kollaborationen in Wertschöpfungsnetzwerken kann die Einstiegsbarrieren zur Anwendung der Blockchain-Technologie in Wertschöpfungsnetzwerken senken. Im Rahmen des Forschungsprojekts „PiMKoWe“ wird die Bereitstellung einer Koordinationsplattform in Wertschöpfungsnetzwerken fokussiert, welche langfristig weiterentwickelt werden soll. Zur Sicherstellung der langfristigen und nachhaltigen Wirtschaftlichkeit der Plattform werden in diesem Arbeitspaket Betreiber- und Gebührenmodelle für Blockchain-basierte Plattformen identifiziert. Insbesondere sollen Einnahmequellen, Kostentreiber, strategische Partner, adressierte Kundensegmente und weitere Aspekte ausfindig gemacht werden.

Ziel dieses Ergebnisberichts ist es, mittels einer strukturierten Literaturrecherche nach vom Brocke et al. (2009), einen Überblick über den aktuellen Stand der Forschung zu Blockchain-basierten und dezentralen Geschäftsmodellen zu geben. Konkreter fokussiert sich der Ergebnisbericht auf die Identifizierung eines integrierten Geschäftsmodells für Blockchain-basierte Plattformen für die Kollaboration in Wertschöpfungsnetzwerken. Als Benchmarking werden die mittels Literaturrecherche identifizierten Geschäftsmodelle Blockchain-basierter Plattformen herangezogen.

2 Eine konzeptuelle Übersicht über digitale Geschäftsmodelle

Die kontinuierlichen technologischen Fortschritte zwingen Unternehmen branchenübergreifend zur Aufnahme neuer Geschäftsmodellstrategien. Vor allem im Bereich des Supply Chain Managements sind Veränderungen der traditionellen Märkte spürbar. Digitale Geschäftsmodelle revolutionieren die Art und Weise wie Geschäfte durchgeführt werden und wie Unternehmen miteinander konkurrieren (Bharadwaj u. a. 2013). Treiber dieser Transformation sind vor allem digitale Technologien wie Big Data, IoT oder die Blockchain. Um mit der einhergehenden Unsicherheit der neuen Technologien umzugehen, ist eine strategische Ausrichtung des Geschäftsfelds unerlässlich für die Aufrechterhaltung der Wettbewerbskraft (Hamel 2001).

Digitale Geschäftsmodelle ermöglichen es Unternehmen, ihre digitalen wertschöpfenden Aktivitäten zu erfassen und zu formulieren (Al-Debei und Avison 2010). Somit bilden sie die Ebene zwischen der Geschäftsstrategie und den Geschäftsprozessen (Kazan, Tan und Lim 2015). Zur Entwicklung eines digitalen Geschäftsmodell gibt es in der Literatur zwei Hauptforschungsströme, welche unterschiedliche Ansätze zur Wertschöpfung von Geschäftswert verfolgen (Chong u. a. 2019). In der ersten Strömung wird untersucht, wie Kerngeschäftsprozesse wertschöpfend konfiguriert werden können (Bharadwaj u. a. 2013; Pitelis Dr. 2009), wohingegen in der zweiten Strömung der Fokus auf wertschöpfenden Aktivitäten in digitalen Umgebungen liegt (Al-

Eigenschaft	Ausprägung			
(1) Fokus	Ergebnisse	Methoden	Theorien	Anwendung
(2) Ziel	Integration	Kritisieren		zentrale Fragestellungen
(3) Organisation	Historisch	Konzeptuell		Methodisch
(4) Perspektive	Neutrale Darstellung		Subjektive Darstellung	
(5) Zielgruppe	Fachleute	Wissenschaft	Praxis/Politik	Öffentlichkeit
(6) Abdeckung	Erschöpfend	Erschöpfend selektiv	Repräsentativ	Zentral

Abbildung B.5.1: Taxonomie der Literaturrecherche nach Cooper (1988)

Debei und Avison 2010; Pagani 2013). Um die konzeptuellen Eigenschaften digitaler und Blockchain-basierter Geschäftsmodelle abzubilden, wird im Folgenden das Konzept von Al-Debei und Avison (2010) aufgegriffen, bei welchem das digitale Geschäftsmodell zwischen betrieblichen Aktivitäten und der allgemeinen Branchenpositionierung des Unternehmens eingeordnet wird.

Mit der Blockchain-Technologie als eine der vielversprechendsten Technologien werden signifikante Veränderungen der Geschäftsmodelle im Bereich des Supply Chain Managements vorhergesagt. Dabei verändern sich Wertquellen als auch Wertdimensionen bestehender Geschäftsmodelle und erweitern sich um die wertschöpfenden Aktivitäten und Eigenschaften der Blockchain Technologie. Beispielsweise erlaubt die Verwendung von Smart Contracts in der Wertschöpfungskette die Neukonfiguration von Geschäftsmodellen, da Hersteller und Verbraucher keinen weiteren Intermediär für den Handel benötigen (Queiroz und Fosso Wamba 2019).

3 Forschungsdesign: Strukturierte Literaturrecherche

Zur Analyse eines geeigneten Betreiber- und Gebührenmodells für die Plattform „PiMKoWe“ wird eine strukturierte Literaturrecherche durchgeführt. Diese folgt dem Ansatz nach vom Brocke et al. (2009), welcher Transparenz hinsichtlich der verschiedenen Entscheidungen im Rechercheprozess verschafft. Insgesamt werden dabei fünf verschiedene Phasen durchlaufen: Umfang der Recherche, Konzeptualisierung, Literaturrecherche, Analyse und Synthese sowie Forschungsagenda. In Phase I der Agenda wird der Umfang der Literaturrecherche klar anhand einer Taxonomie nach Cooper (1988) abgesteckt. Anschließend wird sich in der Konzeptualisierungsphase mittels relevanter Basisliteratur ein Überblick über das Thema verschafft. Phase III beinhaltet die eigentliche Literatursuche. Diese umfasst die Auswahl passender Journale und Datenbanken sowie die Entwicklung eines Suchstrings. Die ermittelten Quellen werden anschließend auf ihre Relevanz überprüft. In Phase IV wird die ermittelte Literatur quantitativ und qualitativ analysiert. Abschließend wird eine Forschungsagenda erstellt, die als Grundlage für zukünftige Forschung zu sehen ist (Vom Brocke u. a. 2009). Durch die detaillierte Dokumentation des Rechercheprozesses kann dessen Replizierbarkeit sowie die Nachvollziehbarkeit des Vorgehens sichergestellt werden. Im Folgenden werden die fünf Phasen schrittweise durchlaufen.

3.1 Phase I: Umfang der Recherche

Die erste Phase der strukturierten Literaturrecherche nach vom Brocke et al. (2009) sieht zunächst vor, den Umfang der Recherche klar abzustecken. Abbildung B.5.1 zeigt zusammenfassend die Einordnung der Arbeit nach Cooper (1988).

Im Fokus der Literaturrecherche steht die Identifikation bestehender Betreiber- und Gebührenmodelle sowie integrierter Geschäftsmodelle für Blockchain-basierte Anwendungen und Plattformen. Insbesondere stehen dabei einerseits Forschungsergebnisse im Mittelpunkt sowie die verschiedenen praxisorientierten Anwendungsszenarien. Ziel der Recherche ist es, einen strukturierten Überblick über die unterschiedlichen Blockchain-basierten Geschäftsmodelle zu schaffen und zentrale Aspekte dieser zu identifizieren. Die Organisation der Arbeit ist konzeptuell. Um zu klären, welche Betreiber- und Gebührenmodelle für Blockchain-basierte Anwendungen und Plattformen bereits existieren, werden diese gruppiert und analysiert. Es wird eine sachliche und neutrale Darstellung der Ergebnisse gewählt. Als Zielgruppe sollen in erster Linie ein ausgewähltes Fachpublikum und Praktiker angesprochen werden. In Bezug auf den Abdeckungsgrad wird auf eine repräsentative Auswahl an Beiträgen gesetzt.

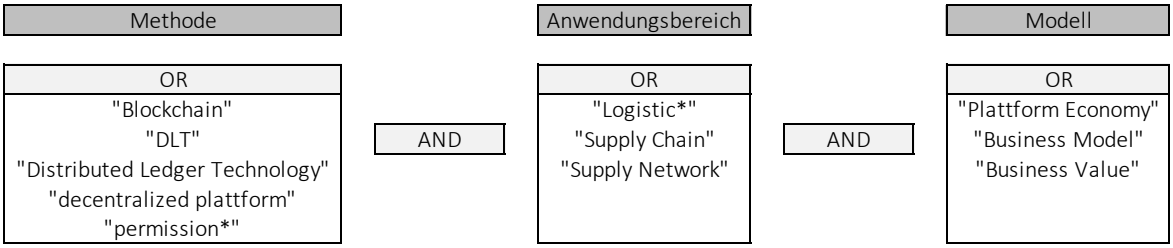


Abbildung B.5.2: Verwendete Suchbegriffe in der Literaturrecherche

Durch die Konzeptualisierungsphase wurde deutlich, dass der Fokus des Blockchain Forschungsgebiets hauptsächlich auf die technologischen Aspekte gerichtet ist sowie deren Potentiale (Cho u. a. 2021; Ochoa u. a. 2020; Zhang u. a. 2021).

3.3 Phase III: Literatursuche

Im nächsten Schritt (Phase III) wird die strukturierte Literatursuche und Auswahl der Ergebnisse durchgeführt. Aufgrund des hoch-innovativen Themengebiets wird der Suchumfang auf einen Erscheinungszeitpunkt nach 2016 beschränkt. Die Aktualität des untersuchten Forschungsgebiets beschränkt die Literaturverfügbarkeit hinsichtlich qualitativ hochwertiger Literatur, weshalb auch Konferenzbeiträge oder Bücher inkludiert werden. Darüber hinaus werden geeignete Datenbanken identifiziert. Ausgewählt wurden die drei Datenbanken EBSCOhost/ Business Source Premier, Web of Science und IEEE Xplore.

Anschließend wurde auf Basis der in der Konzeptualisierungsphase identifizierten Schlüsselbegriffe ein Suchstring ermittelt, mit dem die ausgewählten Datenbanken gleichermaßen durchsucht wurden. Der finale Suchstring wurde mit Hilfe von Clustering-Techniken anhand von Schlüsselbegriffen verwandter Arbeiten zusammengestellt. Die identifizierten Schlüsselbegriffe wurden anschließend mit Synonymen und verwandten Begriffen angereichert. Zusätzlich wurden die bestimmten Schlüsselwörter anhand ihrer Gemeinsamkeiten gruppiert. Suchbegriffe innerhalb einer Gruppe wurden mit dem „OR“ Operator verknüpft, während die Gruppen untereinander mit dem Operator „AND“ verbunden wurden. Die erste Gruppe adressiert die grundlegende Technologie, für welche verschiedene Geschäftsmodelle identifiziert werden sollen. Gruppe zwei umfasst das Anwendungsfeld, in welchem die Technologie eingesetzt werden soll. Abschließend beinhaltet Gruppe drei verschiedene Ausprägungen und Bezeichnungen für Geschäftsmodelle. Abbildung B.5.2 bildet die Zusammensetzung des final erstellten Such-strings ab.

Die resultierende Literaturauswahl beinhaltete über alle Datenbanken hinweg 168 Veröffentlichungen, welche im nächsten Schritt auf Duplikate untersucht wurde. Insgesamt konnten zehn Doppelungen von Artikeln aus unterschiedlichen Datenbanken registriert werden, welche anschließend entfernt wurden. Nachfolgend wurden jeweils Titel und Abstract auf Relevanz untersucht, um eine Entscheidung für oder gegen eine detaillierte Volltextanalyse zu treffen. Da die Suchbegriffe bewusst recht allgemein gehalten wurden, reduzierte sich die Literaturauswahl auf dreiundvierzig thematisch passende Artikel. Nach der Volltextanalyse verblieben elf für relevant befundene Artikel.

Abschließend wurde eine Vorwärts- und Rückwärtssuche für jeden der aus der Volltextanalyse hervorgehenden Artikel durchgeführt. So konnten weitere themenrelevante Artikel ermittelt werden, die durch die Stichwortsuche nicht identifiziert werden konnten. Insgesamt ergab die Vorwärts- und Rückwärtssuche sechs weitere Publikationen. Eine vollständige Übersicht über das durchgeführte Suchverfahren kann Abbildung B.5.3 entnommen werden.

4 Ergebnisse der Literatursuche

Nachdem in den vorherigen Phasen der strukturierten Literaturrecherche nach vom Brocke et al. (2009) relevante Literatur zum Thema Blockchain-basierter Plattformen und deren Geschäftsmodelle gesammelt wurde, wird diese nun analysiert und synthetisiert. Dafür wird diese qualitativ mit Hilfe einer Konzeptmatrix (Webster und Watson 2002) eingeordnet und analysiert. Dieses Vorgehen ermöglicht es, die bisherige Forschung auf

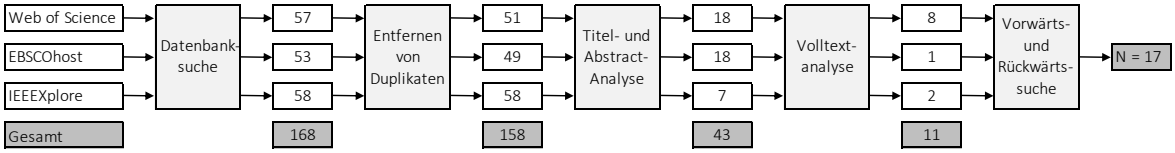


Abbildung B.5.3: Ergebnisse des Suchprozesses

dem zu untersuchenden Forschungsgebiet zu ordnen und zu synthetisieren. Aus den gesammelten Beiträgen konnten Funktionalitäten, Betriebsmodi und Einflussfaktoren auf Blockchain-basierte Geschäftsmodelle identifiziert werden. Darüber hinaus sollen folgende Fragen beantwortet werden: *Die Blockchain-Anwendungen haben eine Reihe von Wertversprechen. Welchen Nutzen erzeugt dieses Wertversprechen für Agenten eines Wertschöpfungsnetzwerks? Wie können die Agenten eines Wertschöpfungsnetzwerks in eine Blockchain-Anwendung integriert werden? Wie wird das Werteversprechen erreicht? Welche Kosten entstehen durch eine Blockchain-Anwendung und wer trägt diese Kosten? Welche Erträge können erwirtschaftet werden, um die Kosten einer Blockchain-Anwendung zu decken?*

Zur Beantwortung dieser Fragen wurde die relevante Literatur in Klassen eingeteilt. Insgesamt konnte die Literatur sechs übergeordneten Klassen zugeordnet werden, welche sich jeweils in weitere Ausprägungen unterteilen. Alle Artikel und deren Einordnung in die jeweiligen Klassen und deren Ausprägungen werden in eine Konzeptmatrix (Webster und Watson 2002) eingeordnet (siehe Tabelle B.5.1).

Um einen Überblick über die Anwendungsszenarien der untersuchten relevanten Literatur zu erhalten, wurden diese nach der **Funktionalität** ihrer Blockchain-basierten Anwendung untergliedert. Dabei kann die Funktionalität einer Blockchain-basierten Anwendung in die Kategorien Geldtransfer und Dienstleistung unterschieden werden. Dabei beinhaltet die erste Kategorie relevante Literatur, welche im Anwendungsbereich Finanzen (Chen und Bellavitis 2020; Upadhyay 2020; Wenngren u. a. 2020) platziert ist. Alle Beiträge, die der Kategorie Dienstleistung zugeordnet sind, bieten einen gewissen Service an, welcher nicht-monetär ist und Anwendungsbereiche wie die Wertschöpfungskette (Hackius und Petersen 2020; Tönnissen und Teuteberg 2020; Wang, Chen, und Zghari-Sales 2021; Wenngren u. a. 2020), den Gesundheitsbereich (Palas und Bunduchi 2021) oder die Lebensmittelindustrie (Kramer, Bitsch, und Hanf 2021a) umfassen. Durch die gezielte Stichwortsuche nach Anwendungsszenarien im Dienstleistungsbereich (insbesondere im Wertschöpfungskettenmanagement) sind Anwendungen im Finanzbereich gering vertreten.

In der gesammelten Literatur befinden sich mehrere Beiträge, welche bestehende Blockchain-Anwendungen analysieren und diese anhand ihrer Betriebsmodi oder zugrundeliegenden digitalen Geschäftsmodelle unterscheiden (Tönnissen, Beinke, und Teuteberg 2020; Weking u. a. 2020). Nach Abgleich der relevanten Literatur konnten vier Betriebsmodi der Anwendungen festgestellt werden. Zu den **Betriebsmodi** Blockchain-basierter Anwendungen (siehe Tabelle 1) gehören: Plattformanbieter (Kramer u. a. 2021a; Lu u. a. 2019; Onik und Miraz 2019; Zheng u. a. 2019), Applikationsanbieter (Hadi u. a. 2018; Rückeshäuser, Brenig, und Müller 2017; Weking u. a. 2020), Dienstleistungsanbieter (Rückeshäuser u. a. 2017) und Infrastrukturanbieter (Chong u. a. 2019; Weking u. a. 2020). Welche Dienstleistungen und Werteversprechen die jeweiligen Modelle an ihre Zielgruppe versprechen, unterscheidet sich jedoch fallabhängig. Zusätzlich hängen die Ausprägungen der Betriebsmodi und der spezifischen Merkmale von der Gestaltung Blockchain-Architektur und des angebotenen Service ab. Es können auch verschiedene Betriebsmodi miteinander kombiniert werden.

Ein typisches **Geschäftsmodellmuster** als Ausprägung der Betriebsmodi sind im Bereich des Managements von Wertschöpfungsketten die gezielte *Integration* mehrerer Unternehmen über die

	Funktionalität		Betriebsmodus				Zugang		Gebührenmodell				Betreibermodell			Wertschöpfungsnetzwerk				
Referenz	Währung/ Geldtransfer/ Zahlungsservice	Dienstleistung	Plattform-anbieter	Applikations -anbieter	Dienstleistungs-anbieter	Infrastruktur -anbieter	Ohne Genehmigung	Mit Genehmigung	Kostenfrei	Kosten pro Transaktion	Regelmäßige Gebühr	Einrichtungs -kosten	Nutzen -versprechen	Wertlieferung	Plattform Peripherie	B2B	B2C	C2C	B2G	Vertikale Koordination
Hackius und Petersen (2020)		●	●		●			●					●	●		●	●		●	●
Wenngren et al. 2020	●	●			●		●	●					●	●	●	●	●	●	●	●
Tseng und Shang (2021)		●		●	●			●					●			●	●			●
Kramer et al. (2021)		●	●		●		●	●					●	●	●					●
Trabucchi et al. (2020)			●		●								●	●	●	●	●	●	●	
Upadhyay (2020)	●	●	●	●		●							●			●	●		●	
Wang et al. (2021)		●	●		●			●					●	●						
Palas, M.J.U. und Bunduchi, R. (2021)		●	●		●			●		●	●	●	●	●	●	●	●			●
Tönnissen und Teuteberg (2019)		●	●	●	●	●							●			●				
Weking et al. (2020)	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●				
Esmaeilian et al. (2020)		●	●							●		●	●	●	●	●	●		●	●
Chen und Bellavitis (2019)	●		●	●	●	●	●	●					●	●						
Chong et al. (2019)	●	●	●								●	●	●	●	●	●	●		●	●
Frizzo-Barker et al. (2019)													●							
Morkunas et al. (2019)	●	●	●		●		●	●					●			●	●			
Lu et al. (2019)		●	●		●	●							●	●	●					
Sáez (2020)			●				●	●					●	●	●					

Tabelle B.5.1: Konzeptmatrix der Literaturrecherche (nach Webster und Watson (2002))

2019; Onik und Miraz 2019; Zheng u. a. 2019), Applikationsanbieter (Hadi u. a. 2018; Rückeshäuser, Brenig, und Müller 2017; Weking u. a. 2020), Dienstleistungsanbieter (Rückeshäuser u. a. 2017) und Infrastrukturanbieter (Chong u. a. 2019; Weking u. a. 2020). Welche Dienstleistungen und Werteversprechen die jeweiligen Modelle an ihre Zielgruppe versprechen, unterscheidet sich jedoch fallabhängig. Zusätzlich hängen die Ausprägungen der Betriebsmodi und der spezifischen Merkmale von der Gestaltung Blockchain-Architektur und des angebotenen Service ab. Es können auch verschiedene Betriebsmodi miteinander kombiniert werden.

Ein typisches **Geschäftsmodellmuster** als Ausprägung der Betriebsmodi sind im Bereich des Managements von Wertschöpfungsketten die gezielte *Integration* mehrerer Unternehmen über die Blockchain-Anwendung (Weking u. a. 2020). Dabei nimmt die Blockchain-Anwendung die Rolle eines *Disintermediärs* ein (Chong u. a. 2019) und es werden bestehende Strukturen von Wertschöpfungsketten integriert. Es kann sich hier auch um die Erweiterung eines bestehenden digitalen Geschäftsmodells, wie beispielsweise eines *digitalen Plattformangebots* für einen mehrseitigen Markt, handeln. Dabei wirkt die Blockchain-Anwendung wie eine zentraler Verwaltungsinstanz einer klassischen Plattform. Darüber hinaus kann die Rolle der Blockchain-basierten Anwendung auch als *Mediator* oder *Transformer* verstanden werden (Chong u. a. 2019). Als *Mediator* liegt der Fokus in der Lösung von Ineffizienzen innerhalb des Wertschöpfungsnetzwerks mit Hilfe der Blockchain, wohingegen das Geschäftsmuster des *Transformers* auf die ganzheitliche Entwicklung Architektur des Peer-to-Peer Netzwerkes anbietet und des Geschäftsmodellmusters einer klassischen Plattform, die mehrseitige Märkte miteinander verbindet.

Sobald die Betriebsmodi als auch die Geschäftsmodellmuster ausgewählt sind, ist über den **Zugang** zur Blockchain-basierten Anwendung zu entscheiden. Dies hat direkten Einfluss auf die Peer-to-Peer-Architektur der zugrundeliegenden Blockchain-basierten Anwendung. Somit ist die ganzheitliche Ausgestaltung eines Blockchain-basierten Geschäftsmodells von der Notwendigkeit einer Instanz zur Verwaltung von Zugriffsberechtigungen und Applikationen einer genehmigungspflichtigen Blockchain abhängig. Dabei kann der Zugang zu einer Anwendung ohne Genehmigung oder mit Genehmigung gestaltet werden. Typischerweise sind öffentliche Netzwerke, welche keine Genehmigung für einen Zugang zur Plattform oder Anwendung einer Applikation benötigen, eher im Finanzbereich zu finden (Chen und Bellavitis 2020). Genehmigungspflichtige Blockchain-Architekturen sind dahingegen Grundlage für die Schaffung gemeinsamer Ökosysteme auf Basis von Konsortien, welche einen gemeinsamen organisatorischen Rahmen teilen (Hackius und Petersen 2020; Kumar, Liu, und Shan 2020; Meyer, Kuhn, und Hartmann 2019). Genehmigungen sind in diesem Rahmen insbesondere Zugriffsberechtigungen auf bestimmte Dienste. Aufgrund des architektonischen Aufbaus sind genehmigungspflichtige Peer-to-Peer Netzwerke häufig für den Anwendungsfall der Kollaboration innerhalb von Wertschöpfungsnetzwerken verbreitet (Moon, Wei und Miao 2019).

Eine dezentral organisierte Blockchain-Anwendung benötigt trotz dezentraler Ausführung

Tabelle B.5.1: Konzeptmatrix der Literaturrecherche (nach Webster und Watson (2002))

von Blockchain-Anwendungen abzielt, die explizit auf die bestehenden Geschäftsaktivitäten der Kunden angepasst sind. Für die Bereitstellung individualisierter Blockchain-Anwendung können Unternehmen auch mit Unternehmen mit Blockchain-Knowhow als *Co-Innovatoren* zusammenarbeiten. Diese bieten den Unternehmen individualisierte Blockchain-Applikationen auf einer eigenen Plattform inklusive Infrastruktur an. Häufig werden jedoch Blockchain-Plattformen inklusive Infrastruktur angeboten, um Unternehmen den Aufbau individueller Applikationen zu ermöglichen, ohne eigene Infrastruktur zu besitzen. Dieses Geschäftsmodellmuster wird häufig auch als *Blockchain-as-a-Service* (Kernahan, Bernskov, und Beck 2021; Li u. a. 2020; Lu u. a. 2019; Zheng u. a. 2019) betitelt. Wichtig ist hier die Unterscheidung des Blockchain-Plattform-Anbieters, welcher die eine initiale Aufstellung der benötigten Infrastruktur und Initiierung des Vorhabens. Darüber hinaus müssen Infrastruktur und laufende Kosten des Netzwerks gedeckt werden. Deshalb benötigt das Geschäftsmodell einer Blockchain-Anwendung ein spezielles **Gebührenmodell**. In der betrachteten Literatur konnten verschiedene Ausgestaltungsmöglichkeiten identifiziert werden. Es besteht die Möglichkeit, dass das Konsortium die Einrichtungskosten der Blockchain-basierten Anwendung aufteilt und anschließend das Netzwerk kostenfrei zu Verfügung stellt (Weking u. a. 2020). Hier ist jedoch fraglich, wie dieses Gebührenmodell bei einer Erweiterung des Konsortiums mit den Neueinsteigern verfährt. Ein nachhaltiges Gebührenmodell ist es, entweder Kosten pro getätigte Transaktion zu erheben oder eine fixe regelmäßige Gebühr von jedem Teilnehmer des Netzwerks zu verlangen (Chong

u. a. 2019; Esmaeilian u. a. 2020; Palas und Bunduchi 2021; Tönnissen und Teuteberg 2020). Hier ist abzuwägen, welche Variante rentabler ist oder ob sogar eine Kombination beider Komponenten nachhaltig ist.

Für ein nachhaltiges Geschäftsmodell für Blockchain-basierte Anwendungen ist die Ausarbeitung eines **Betreibermodells** ein essenzieller Bestandteil. Die Auswertung der relevanten Literatur zeigt hier bei der Analyse von Betreibermodellen Blockchain-basierter Anwendungen eine starke Parallelität zu Analysen allgemeiner digitaler Geschäftsmodelle auf. Häufig werden digitale Betreibermodelle nur um die Blockchain-spezifischen Aspekte erweitert. Im Fokus des Betreibermodells stehen in Bezug auf Blockchain-basierte Anwendungen vor allem das Nutzenversprechen, die Wertlieferung und die Ausgestaltung der Plattform Peripherie im Fokus. Typische Nutzenversprechen für Blockchain-basierte Anwendungen für Kollaborationen in Wertschöpfungsnetzwerken sind die Verringerung von Transaktionskosten und aufgewendeter Zeit für die Erhaltung von Kontakten durch das Fehlen von Zwischenhändlern in der Blockchain-Technologie (Mercuri, della Corte und Ricci 2021). Darüber hinaus besteht der Kern der Wertlieferung für den Anwender bzw. den Kunden aus einer erhöhten Transparenz über die Transaktionen innerhalb des Wertschöpfungsnetzwerks, welche eine gewisse Prozesssicherheit induziert. Durch die erhöhte Transparenz der Transaktionen kann eine Rückverfolgung der Wertströme im Wertschöpfungs-netzwerk angestoßen werden (Wang u. a. 2021). Dem Anwender werden durch eine Echtzeit-Verarbeitung der Transaktionsdaten Prozessverbesserungen ermöglicht, welche wiederum nachgelagert einen zusätzlichen Wertlieferant darstellen (Tönnissen und Teuteberg 2020). Aufgrund der inhärenten Sicherheitsaspekte der Blockchain-Technologie können unternehmensübergreifende Prozesse zusätzlich im Maße der Prozesssicherheit verbessert werden. Beispielsweise können Sicherheitsanforderungen und -standards aus den staatlichen Regularien abgebildet werden (Lähdeaho und Hilmola 2020). Ein hervorzuhebender Aspekt der Ausgestaltung eines Betreibermodells explizit für Blockchain-basierte Anwendungen ist der Aufbau der Plattform Peripherie, da dieser maßgebliche Einfluss auf die Ausgestaltung des Betreibermodells hat. Die Plattform Peripherie umfasst zusätzliche Technologien wie beispielsweise IoT, Cloud, Dapps, oder Big Data Analytics (Weking u. a. 2020). Ein weiteres relevantes Konzept für Blockchain-basierte Geschäftsmodelle konnte in der relevanten Literatur identifiziert werden, welches insbesondere für die strategische Ausrichtung eines Konsortiums innerhalb von Wertschöpfungsnetzwerken bedeutungsvoll ist. Genauer gesagt ist vor Aufbau des Konsortiums festzulegen, welche Arten von Geschäftsbeziehungen innerhalb des **Wertschöpfungsnetzwerks** in die Anwendung integriert werden sollen. Durch die Recherche der relevanten Literatur konnten bestehende Blockchain-basierte Anwendungen im Bereich B2B (z.B. Kramer, Bitsch, und Hanf 2021b; Tönnissen und Teuteberg 2020), B2C (z.B. Palas und Bunduchi 2021; Tseng und Shang 2021), C2C (z.B. Moon u. a. 2019; Trabucchi u. a. 2020; Wenngren u. a. 2020) und B2G (Chong u. a. 2019; Esmaeilian u. a. 2020; Upadhyay 2020) gefunden werden. Hier sind insbesondere die Eigenschaften einer vertikalen Integration innerhalb einer Wertschöpfungskette zu beachten, welche häufig besondere Herausforderungen hinsichtlich des Informationsaustauschs mit sich bringen (Chong u. a. 2019; Kramer u. a. 2021b; Tseng und Shang 2021).

5 Klassifikation bestehender Blockchain-basierter Geschäftsmodelle

Die Einordnung und Identifikation von Geschäftsmodellmustern, Funktionalitäten, Betriebsmodi und Einflussfaktoren auf Blockchain-basierte Geschäftsmodelle in der relevanten Literatur kann nur teilweise Aufschluss über den praktischen Nutzen geben. Deshalb werden in diesem Kapitel vor allem bestehende Geschäftsmodelle aufgezeigt, welche in der Praxis existieren und als Anwendungsfälle für das Wertschöpfungsmanagement geeignet sind.

Das Geschäftsmodell *Blockchain as a Service* bietet Kunden eine Plattform-Lösung inklusive Infrastruktur an, um Blockchain-basierte Applikationen ausführen, überwachen und steuern zu können, ohne dabei selbst die nötige Infrastruktur besitzen zu müssen (Li u. a. 2020; Ochoa u. a. 2020). Somit kann *Blockchain as a Service* auch als Fusion der neuartigen Blockchain-Technologie mit Cloud Computing angesehen werden (Asheralieva und Niyato 2020). Deshalb ist das Geschäftsmodell bei Anbietern wie Amazon, IBM, Microsoft Azure beliebt, da das Produktportfolio bereits die Bereitstellung von Cloud-Lösungen umfasst und dieses nur noch um das Angebot von Blockchain-Plattformen erweitert werden muss (Lu u. a. 2019). Letztendlich ermöglicht dieses Geschäftsmodell einen einfachen und schnellen Zugang zu notwendiger Infrastruktur und Plattform zum Aufbau individualisierter und Blockchain-basierter Anwendungen für Kollaborationen innerhalb

Wertschöpfungsnetzwerken. Darüber hinaus fördert der schnelle Zugang zur essenziellen Infrastruktur die schnellere Entwicklung eigener und individualisierter Blockchain-Applikationen.
Um Kundengruppen zu adressieren, die nicht in der Lage sind, selbst Blockchain-basierte Anwendungen zu entwickeln oder zu implementieren, zielt das Geschäftsmodell *Blockchain-based Software* direkt auf diese Bedürfnisse ab (Blanco u. a. 2020; Sharma o. J.). Im Wertschöpfungsnetzwerk-Management ist beispielsweise ein Lösungsansatz das Angebot eines Blockchain-basierten Softwareprodukts, das das Tracking eines Produkts in der Lieferkette ermöglicht, die Verifikation von Mitarbeitern sicherstellt oder rein als verteilte Datenbasis fungiert (Salviotti, de Rossi, und Abbatemarco 2018). Dabei wird die Softwarelösung in die bestehenden Unternehmensstrukturen integriert.
Ein weiteres Geschäftsmodell ist von den vorherigen abzugrenzen – das *Utility Token Business Model* in der *Token Economy* (Martin 2021). Hier können Geschäftsmodelle auf Plattform-, Netzwerk- und Anwendungslevel geschaffen werden; dabei werden Netzwerke auf Plattformen aufgebaut und Anwendungen wiederum in den verschiedenen Netzwerken (Martin 2021). Das Ziel ist es, die Grenzen der Netzwerke auf Dauer verschwimmen zu lassen und branchenübergreifende Netzwerke entstehen zu lassen, welche mithilfe von *Utility Tokens* das Geschäftsmodell der *Token Economy* aufbauen.

6 Fazit

Dieser Ergebnisbericht bietet einen Überblick über den aktuellen Stand der Forschung zu Blockchain-basierten und dezentralen Geschäftsmodellen in der Literatur. Im Anwendungsbereich der Kollaboration von Teilnehmern in Wertschöpfungsnetzwerken gibt es verschiedene Geschäftsmodellmuster, wonach Blockchain-basierte Geschäftsmodelle abgeleitet werden können. In der Praxis und Literatur sind bereits Geschäftsmodelle wie *Blockchain as a Service* oder *Blockchain-based Software Products* etabliert. Die Integration der Blockchain-Technologie kann Unternehmen zu Effizienzsteigerungen führen und Anbieter von Blockchain-Geschäftsmodellen können Unternehmen schnellen Zugang zu dieser Technologie bieten. Die vielfältigen Ausgestaltungsmöglichkeiten der Geschäftsmodellmuster ermöglichen den Aufbau eines nachhaltigen Geschäftsmodells für Anbieter Blockchain-basierter Anwendungen.

Literaturverzeichnis

Al-Debei, Mutaz M., und David Avison. 2010. „Developing a unified framework of the business model concept“. *European Journal of Information Systems* 19(3):359–76.

Asheralieva, Alia, und Dusit Niyato. 2020. „Distributed Dynamic Resource Management and Pricing in the IoT Systems with Blockchain-as-a-Service and UAV-Enabled Mobile Edge Computing“. *IEEE Internet of Things Journal* 7(3):1974–93.

Bharadwaj, Anandhi, Omar A. El Sawy, Paul A. Pavlou, und N. Venkatraman. 2013. „Digital Business Strategy: Toward a Next Generation of Insights“. *MIS Quarterly* 37(2):471–82.

Blanco, Pablo, Andi Maroge, Joe Porter, Avery Leider, und Charles C. Tappert. 2020. „Adopting Blockchain In The Digital Music Industry“. S. 1–8 in *Proceedings of Student-Faculty Research Day, CSIS*.

Vom Brocke, Jan, Alexander Simons, Björn Niehaves, Kai Riemer, Ralf Plattfaut, und Anne Cleven. 2009. „Reconstructing the giant: On the importance of rigour in documenting the literature search process“. S. 161 in *17th European Conference on Information Systems, ECIS 2009*.

Chen, Yan, und Cristiano Bellavitis. 2020. „Blockchain disruption and decentralized finance: The rise of decentralized business models“. *Journal of Business Venturing Insights* 13:e00151.

Cho, Soohyun, Kyungha Lee, Arion Cheong, Won Gyun No, und Miklos A. Vasarhelyi. 2021. „Chain of Values: Examining the Economic Impacts of Blockchain on the Value-Added Tax System“. *Journal of Management Information Systems* 38(2):288–313.

Chong, Alain Yee Loong, Eric T. K. Lim, Xiuping Hua, Shuning Zheng, und Chee Wee Tan. 2019. „Business on Chain: A Comparative Case Study of Five Blockchain-Inspired Business Models“. *Journal of the Association for Information Systems* 20(9):9.

Cooper, Harris M. 1988. „Organizing knowledge syntheses: A taxonomy of literature reviews“. *Knowledge in Society 1988 1:1* 1(1):104–26.

Esmaeilian, Behzad, Joe Sarkis, Kemper Lewis, und Sara Behdad. 2020. „Blockchain for the future of sustainable supply chain management in Industry 4.0.“ *Resources, Conservation & Recycling* 163: 105064.

Hackius, Niels, und Moritz Petersen. 2020. „Translating High Hopes into Tangible Benefits: How Incumbents in Supply Chain and Logistics Approach Blockchain“. *IEEE Access* 8:34993–3.

Hadi, Saleh, Alexandrov Dmitry, und Dzhonov Azamat. 2018. „Uberisation Business Model Based on Blockchain for Implementation Decentralized Application for Lease/Rent Lodging“. *Smart Innovation, Systems and Technologies* 111:225–32.

Hamel, Gary. 2001. „Leading the revolution: An interview with Gary Hamel“. *Strategy & Leadership* 29(1):4–10.

Kazan, Erol, Chee Wee Tan, und Eric T. K. Lim. 2015. „Value creation in cryptocurrency networks: Towards a taxonomy of digital business models for bitcoin companies“. in *Pacific Asia Conference on Information Systems, PACIS 2015 - Proceedings*.

Kernahan, Alan, Ulrik Bernskov, und Roman Beck. 2021. „Blockchain out of the box - Where is the blockchain in blockchain-as-a-service?“ *Proceedings of the Annual Hawaii International Conference on System Sciences* 2020-January:4281.

Kouhizadeh, Mahtab, Sara Saberi, und Joseph Sarkis. 2021. „Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers“. *International Journal of Production Economics* 231:107831.

Kramer, Michael Paul, Linda Bitsch, und Jon Hanf. 2021a. „Blockchain and Its Impacts on Agri-Food Supply Chain Network Management“. *Sustainability 2021, Vol. 13, Page 2168* 13(4):2168.

Kramer, Michael Paul, Linda Bitsch, und Jon Hanf. 2021b. „Blockchain and Its Impacts on Agri-Food Supply Chain Network Management“. *Sustainability 2021, Vol. 13, Page 2168* 13(4):2168.

Kumar, Akhil, Rong Liu, und Zhe Shan. 2020. „Is Blockchain a Silver Bullet for Supply Chain Management? Technical Challenges and Research Opportunities.“ *Decision Sciences* 51(1):8–37.

Lähdeaho, Oskari, und Olli Pekka Hilmola. 2020. „Business Models Amid Changes in Regulation and Environment: The Case of Finland–Russia“. *Sustainability 2020, Vol. 12, Page 3393* 12(8):3393.

Li, Daming, Lianbing Deng, Zhiming Cai, und Alireza Souri. 2020. „Blockchain as a service models in the Internet of Things management: Systematic review“. *Transactions on Emerging Telecommunications Technologies* e4139.

Lu, Qinghua, X. Xu, Yue Liu, Ingo Weber, Liming Zhu, und Weishan Zhang. 2019. „uBaaS: A unified blockchain as a service platform“.

Future Generation Computer Systems 101:564–75.

Martin, Andy. 2021. „The Token Economy“. *SSRN Electronic Journal*.

Mercuri, Francesco, Gaetano della Corte, und Federica Ricci. 2021. „Blockchain Technology and Sustainable Business Models: A Case Study of Devoleum“. *Sustainability 2021, Vol. 13, Page 5619* 13(10):5619.

Meyer, Tobias, Marlene Kuhn, und Evi Hartmann. 2019. „Blockchain technology enabling the Physical Internet: A synergetic application framework.“ *Computers & Industrial Engineering* 136:5–17.

Moon, Hyoungeun, Wei Wei, und Li Miao. 2019. „Complaints and resolutions in a peer-to-peer business model“. *International Journal of Hospitality Management* 81:239–48.

Morabito, Vincenzo. 2017. „Business Innovation Through Blockchain“. *Cham: Springer International Publishing*.

Ochoa, Justin J., Gomanth Bere, Indrasena R. Aenugu, Taesic Kim, und Kim Kwang Raymond Choo. 2020. „Blockchain-as-a-service (BaaS) for battery energy storage systems“. *2020 IEEE Texas Power and Energy Conference, TPEC 2020*.

Onik, Md Mehedi Hassan, und Mahdi H. Miraz. 2019. „Performance Analytical Comparison of Blockchain-as-a-Service (BaaS) Platforms“. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST* 285:3–18.

Pagani, Margherita. 2013. „Digital Business Strategy and Value Creation: Framing the Dynamic Cycle of Control Points“. *Source: MIS Quarterly* 37(2):617–32.

Palas, Md. Jahir Uddin, und Raluca Bunduchi. 2021. „Exploring interpretations of blockchain's value in healthcare: a multi-stakeholder approach.“ *Information Technology & People* 34(2):453–95.

Perscheid, Guido, Nadine Ostern, und Jürgen Moormann. 2020. „TOWARDS A TAXONOMY OF DECENTRALIZED PLATFORM-BASED BUSINESS MODELS“. *European Conference on Information Systems*.

Pitelis Dr., Christos N. 2009. „The Co-Evolution of Organizational Value Capture, Value Creation and Sustainable Advantage“: *http://dx.doi.org/10.1177/0170840609346977* 30(10):1115–39.

Queiroz, Maciel M., und Samuel Fosso Wamba. 2019. „Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA.“ *International Journal of Information Management* 46:70–82.

Rückeshäuser, Nadine, Christian Brenig, und Günter Müller. 2017. „Blockchains als Grundlage digitaler Geschäftsmodelle“. *Datenschutz und Datensicherheit - DuD 2017 41:8* 41(8):492–96.

Salviotti, Gianluca, Leonardo Maria de Rossi, und Nico Abbatemarco. 2018. „A structured framework to assess the business application landscape of blockchain technologies“. *Proceedings of the Annual Hawaii International Conference on System Sciences* 2018-January:3467–76.

Sharma, T. K. o. J. „The best Blockchain Business Models“. Abgerufen (https://www.blockchain-council.org/blockchain/the-best-blockchain-business-models/).

Tönnissen, Stefan, Jan Heinrich Beinke, und Frank Teuteberg. 2020. „Understanding token-based ecosystems – a taxonomy of blockchain-based business models of start-ups“. *Electronic Markets* 30(2):307–23.

Tönnissen, Stefan, und Frank Teuteberg. 2020. „Analysing the impact of blockchain-technology for operations and supply chain management: An explanatory model drawn from multiple case studies“. *International Journal of Information Management* 52:101953.

Trabucchi, Daniel, Antonella Moretto, Tommaso Buganza, und Alan MacCormack. 2020. „Disrupting the Disruptors or Enhancing Them? How Blockchain Reshapes Two-Sided Platforms“. *Journal of Product Innovation Management* 37(6):552–74.

Tseng, Cheng Te, und Shari S. C. Shang. 2021. „Exploring the Sustainability of the Intermediary Role in Blockchain“. *Sustainability 2021, Vol. 13, Page 1936* 13(4):1936.

Tumasjan, Andranik, und Theodor Beutel. 2019. *Blockchain-Based Decentralized Business Models in the Sharing Economy: A Technology Adoption Perspective*. Bd. Business Transforma…. herausgegeben von H. . B. R. Treiblmaier. Springer International Publishing.

Upadhyay, Nitin. 2020. „Demystifying blockchain: A critical analysis of challenges, applications and opportunities“. *International Journal of Information Management* 54:102120.

Wang, Yingli, Catherine Huirong Chen, und Ahmed Zghari-Sales. 2021. „Designing a blockchain enabled supply chain.“ *International Journal of Production Research* 59(5):1450–75.

Webster, Jane;, und Richard T. Watson. 2002. „Analyzing the Past to Prepare for the Future: Writing a Literature Review“. *MIS Quarterly* 26(2):13–23.

Weking, Jörg, Michael Mandalenakis, Andreas Hein, Sebastian Hermes, Markus Böhm, und Helmut Krcmar. 2020. „The impact of blockchain technology on business models – a taxonomy and archetypal patterns“. *Electronic Markets* 30(2):285–305.

Wenngren, Johan, Martin Lundgren, Asa Ericson, und Johan Lugnet. 2020. „Distributed ledger technologies building trust in value chains?“ *2020 3rd International Symposium on Small-Scale Intelligent Manufacturing Systems, SIMS 2020*.

Zhang, Wenping, Chih Ping Wei, Qiqi Jiang, Chih Hung Peng, und J. Leon Zhao. 2021. „Beyond the Block: A Novel Blockchain-Based Technical Model for Long-Term Care Insurance“. *Journal of Management Information Systems* 38(2):374–400.

Zheng, Weilin, Zibin Zheng, Xiangping Chen, Kemian Dai, Peishan Li, und Renfei Chen. 2019. „NutBaaS: A Blockchain-As-A-Service Platform“. *IEEE Access* 7:134422.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL-THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt "PIMKoWe"

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PiMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Lehrstuhl für BWL und Wirtschaftsinformatik
Prof. Dr. Axel Winkelmann
Sanderring 2
97070 Würzburg

Autoren und Ansprechpartner

Myriam Schaschek, M.Sc.

Wissenschaftliche Mitarbeiterin
myriam.schaschek@uni-wuerzburg.de
+49 931 31-87662

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 931 31-89640

B6.1: Bedeutung von Privatsphäre auf Blockchains

Das Teilarbeitspaket „Analyse von Anforderungen hinsichtlich Datenschutzes und -sicherheit“ befasst sich mit der Blockchain-Technologie, speziell mit der Frage des Datenschutzes und der Datensicherheit auf Blockchains. Dazu wird zunächst auf den Datenschutz und die Datensicherheit, insbesondere unter dem Aspekt der Privatsphäre der Nutzer beim Private Voting sowie den Kryptowährungen Monero und Zcash eingegangen. In diesem Kapitel wird die Forschungsfrage, ob und wie in öffentlich verteilten Netzwerken wie der Blockchain trotzdem Privatsphäre für die Nutzer gewährleistet werden kann, erarbeitet. Anhand dreier Anwendungsfälle soll dies aufgezeigt werden. Die Arbeit dient dem Verständnis für die Funktionsweise der Blockchain-Technologie, aber auch der Betrachtung dieser Technologie unter dem Aspekt des Datenschutzes und der Sicherheit für den Nutzer.

1 Privatsphäre und rechtliche Rahmenbedingungen

Bei vielen Blockchain-Anwendungen steht der Datenschutz an erster Stelle der wichtigsten Eigenschaften. Nutzer wollen ihre Identität schützen und bei Zahlungen auch die Höhe der getätigten Transaktionen. Die Privatsphäre stellt sich jedoch als eine der größten Herausforderungen dar, denn standardmäßig ist die Blockchain ein öffentliches Buch. Jeder Teilnehmer kann die Einträge einsehen. Daher ist es wichtig, Regulierungen einzuführen, die sich mit der Anonymität bzw. Pseudonymisierung bei Kryptowährungen und der Privatsphäre von Blockchain-basierten Systemen auseinandersetzen (Li et al. 2019).
Das Recht auf Privatsphäre sowie auf die Unauffindbarkeit von Finanztransaktionen hat dazu geführt, dass seit der Einführung von Bitcoin immer mehr Kryptowährungen entwickelt wurden, die Anonymität gewährleisten sollen (Lee 2019). Eine verbesserte Privatsphäre und Anonymität der Nutzer haben jedoch auch Schattenseiten. Teilnehmer einer öffentlichen Blockchain können zwar teilweise durch einen öffentlichen Schlüssel identifiziert werden, dahinter verbirgt sich jedoch nicht immer eine Person mit Adresse. Dies kann sich als Problem für die Strafverfolgung bei Finanzdelikten herausstellen. Derartige Delikte anonymer Nutzer zu verfolgen, kann schwierig und in manchen Fällen unmöglich sein. Auf der Gegenseite haben Nutzer, denen Unrecht widerfahren ist, oft keine Möglichkeit, die an der Transaktion beteiligte, schuldige Person auffindbar zu machen. Für Regulierungsbehörden wird die Anonymität der Nutzer, die für viele Blockchain-Teilnehmer einen großen Vorteil darstellt, zu einem Problem. Straftäter können sich im Netzwerk teilweise völlig anonym bewegen. Deswegen müssen Vorschriften erarbeitet werden, die illegale Aktivitäten überwachen können und auf Grundlage von Gesetzen Strafen herbeiführen (Fulmer 2019). Wohingegen es in anderen Ländern wie Pakistan und China bereits ein Verbot von Bitcoin bzw. von einigen Kryptowährungen gibt, ist die Technologie in Deutschland keinem Verbot ausgesetzt (Ruoti et al. 2020). In Europa fehlen spezifische Gesetze zum Umgang mit Kryptowährungen. Bitcoin wird in Deutsch-land als privates und nicht als gesetzliches Zahlungsmittel aufgefasst (Read und Gräslund 2018). Die Tatsache, dass es inzwischen über 1600 verschiedene Kryptowährungen gibt, erschwert die Entwicklung eines Regulierungssystems. Es existieren unterschiedliche Interpretationen darüber, was eine Kryptowährung ausmacht. Sie kann zum Beispiel als Wertpapier, als Ware oder als Eigentum interpretiert werden (Kfir 2020). Zahlreiche Fälle werden einzeln entschieden, weil es keine eindeutigen Vorschriften gibt.
Hinzu kommt, dass sich einige der Fälle in Grauzonen befinden. Besonders herausfordernd ist die Tatsache, dass die Grundsätze der Blockchain-Technologie, die Dezentralität sowie die Unveränderlichkeit öffentlicher Blockchains in einem Konflikt mit der EU-Datenschutzgrundverordnung (DSGVO) stehen. Bisher wurde keine Änderung der Rechtsgrundlagen veranlasst (Reetz 2019). Regierungen stehen den mangelnden Regulierungen und Vorschriften für anonyme Kryptowährungen kritisch gegenüber (Li et al. 2019). Die Datenschutzgrundverordnung gilt in ganz Europa seit dem 25. Mai 2018 (Hein et al. 2019). Sie beinhaltet Verpflichtungen gegenüber den Personen, die Daten verarbeiten. Außerdem wird darin der Umgang mit der Verarbeitung persönlicher Daten geregelt. Drei zentrale Punkte in Bezug auf die Anwendbarkeit der Verordnung auf die Blockchain-Technologie sind die Verarbeitung personenbezogener Daten, die für den Datenschutz verantwortlichen Akteure sowie das Recht des Einzelnen (Eichler at al. 2018).

Personenbezogene Daten

Inwieweit die Blockchain personenbezogene Daten enthält, ist fraglich. Es muss zwischen anonymen Informationen und personenbezogenen Daten unterschieden werden. Bei anonymen Informationen lässt sich kein Bezug zu einer identifizierten oder einer identifizierbaren, natürlichen Person herstellen. Es besteht auch die Möglichkeit, dass derartige Informationen so anonymisiert wurden, dass keine Person mehr dahinter ausgemacht werden kann. Durch die Verwendung von Pseudonymen in Blockchain-Netzwerken stellt sich die Frage, inwieweit über diese dennoch eine Identifikation erfolgen kann (Hein et al. 2019). Hier entsteht ein Konflikt mit dem Datenschutz. Die Transaktionen eines Netzwerks sind öffentlich einsehbar, was zwar einerseits der Sicherheit dient, jedoch bei sensiblen Daten auf Hindernisse stößt. So ist es beispielsweise in einem Netzwerk aus mehreren Teilnehmern möglich, die Identität eines Teilnehmers herauszufinden. Um für mehr Datenschutz zu sorgen, wurden bereits zahlreiche Methoden und Technologien vorgeschlagen. Dazu gehören vertrauliche Ringtransaktionen, Ringsignaturmischungen oder auch private Netzwerke (Ismail und Matewala 2019). Laut Eichler et al. (2018) können potenziell alle auf Blockchains gespeicherten Daten personenbezogen sein. Um Konflikte mit der DSGVO in diesem Bereich zu verringern, muss die Menge dieser Daten begrenzt, neue Möglichkeiten zur Anonymisierung sowie Speicheroptionen außerhalb der Blockchain entwickelt werden.

Recht auf Löschung

Ein weiterer Konflikt zur DSGVO stellt die Unveränderlichkeit der Blockchain dar. Es ist fraglich, inwieweit hier das Recht auf Löschung aus Artikel 17 der DSGVO Anwendung findet. Der Artikel bezieht sich auf personenbezogene Daten. Sollte Artikel 17 auf die Blockchain-Technologie anwendbar sein, dürften demnach keine personenbezogenen Daten in der Blockchain gespeichert sein (Engelschall 2019). Grundsätzlich ist es sowohl in privaten als auch in öffentlichen Blockchains möglich, einen Personenbezug mit Hilfe von Analysetools herzustellen und die Hashwerte Personen zuzuordnen. Deshalb können hier Artikel 16 und 17 der DSGVO zu den Veränderungsansprüchen auch für die Blockchain Anwendung finden. Es ergibt sich hier allerdings der Konflikt, wer als Verantwortlicher herangezogen werden kann (Saive 2018).

Verantwortlichkeit

Laut Eichler et al. (2018) gibt es innerhalb von Blockchain-Systemen verschiedene Akteure, wie die Knoten oder die Entwickler, welche als Verantwortliche herangezogen werden könnten. Die DSGVO unterteilt die Verantwortlichen im Bereich der Datenverarbeitung in Verantwortliche für die Datenverarbeitung, Prozessoren und gemeinsame Kontrolleure. Die Blockchain-Technologie passt jedoch auf Grund ihrer Dezentralität nicht in diesen aufgestellten Rahmen, weshalb auch hier keine klare Einordnung durchgeführt werden kann. Mögliche Entitäten, welche in Zukunft in der Verordnung als Verantwortliche herangezogen werden könnten, sind die Knoten, die digitalen Geldbeutel, Dienste und Anwendungen sowie die Entwickler von Protokollen.

Smart Contracts

Im Bereich der Smart Contracts steht die Gesetzgebung ebenfalls vor großen Herausforderungen. Aktuell ist das traditionelle Vertragsrecht nicht auf intelligente Verträge anzuwenden. Die Tatsache, dass die Vertragsabwicklung in Computercode in der Blockchain gespeichert ist, erschwert die Regulierungen. Anwälte verfügen meist nicht über ausreichende Programmierkenntnisse. Es sind neue Regulierungen notwendig, denn immer mehr Unternehmen finden an der Verwendung von Smart Contracts Gefallen, um Zeit und Kosten bei Vertragsabwicklungen zu sparen. Es stellt sich außerdem die Frage nach dem Ort des Vertragsabschlusses. Durch die Dezentralität sind viele Computer über die ganze Welt verteilt in einem Netzwerk miteinander verbunden. Um Gesetze im Zusammenhang mit intelligenten Verträgen anzuwenden, müsste festgestellt werden, welches Recht länderabhängig anzuwenden ist. Auch hier ist unklar, wer als Verantwortlicher herangezogen werden kann, wenn es zu Fehlfunktionen von Verträgen kommt. Bisher sind diese Fragen auf Grund der Neuheit und der schwachen Umsetzung der Technologie noch ungelöst, werden jedoch sicher in Zukunft noch Gegenstand einiger Diskussionen zu diesem Thema sein (Fulmer 2019). Es muss eine Lösung dafür gefunden werden, wenn die eingegebenen Daten falsch sind, der Vertrag jedoch automatisch ausgeführt und auf der Blockchain hochgeladen wird. Darüber hinaus stellt sich die Frage, wie man Vertragsbedingungen in einer unveränderlichen Blockchain ändern kann. Hierfür müssen die Rechts- und Regulierungsbehörden Lösungen finden, um mit dem Vertragsrecht nicht in Konflikt zu kommen (Santos 2020).

Rücktritt und Widerruf

Im Zivilrecht ist des Weiteren der Grundsatz verankert, dass eine Rückabwicklung von Schuldverhältnissen möglich ist. Außerdem ist dort der Rücktritt (§ 346 BGB) und der Wider-ruf (§ 355 BGB) geregelt, aus denen eine Nichtigkeit folgt. Eine prägende Eigenschaft der Blockchain besteht allerdings in der unveränderlichen Speicherung von Daten. Erfolgt ein Vertragsangebot und eine Annahme über eine Blockchain-Anwendung, ist die Möglichkeit einer Rückabwicklung des Schuldverhältnisses hier ebenfalls erforderlich (Saive 2018). Da die derzeitigen Gesetze bezüglich der Datenschutzbestimmungen sich hauptsächlich auf zentralisierte Datenverwaltung beziehen, sind genaue Überlegungen zur Einhaltung der Datenschutzbestimmungen bei der Einführung von Blockchain-Anwendungen notwendig (Acerbi 2019).

Neben den hier aufgeführten Artikeln und Gesetzen gibt es zahlreiche gesetzliche Konfliktpunkte mit Blockchain-Anwendungen. Um den Umfang dieser Arbeit zu limitieren, wurden einige ausgewählt, die besonders häufig Fragen in Bezug auf die Datensicherheit und den Datenschutz auf Blockchains aufwerfen.

Mögliche Lösungen

In ihrem Paper haben Zang et al. (2019) verschiedene Techniken vorgestellt, die zur Verbesserung von Sicherheit und Datenschutz auf Blockchain-Systemen beitragen können. Eine Möglichkeit ist das Vermischen von Münzen. Dadurch können Adressen nicht mit der Identität des Nutzers verknüpft werden. Die Nutzer mischen ihre Münzen untereinander zufällig. Zwei derartige Mischdienste sind Mixcoin und CoinJoin. Beim CoinJoin-Protokoll besteht jedoch die Gefahr, dass Benutzer dennoch identifiziert werden können, da alle Transaktionen und Teilnehmer aufgezeichnet werden. Eine weitere Möglichkeit sind anonyme Signaturen. Bei einer Gruppensignatur signiert ein Teilnehmer seine Transaktion mit einem persönlichen

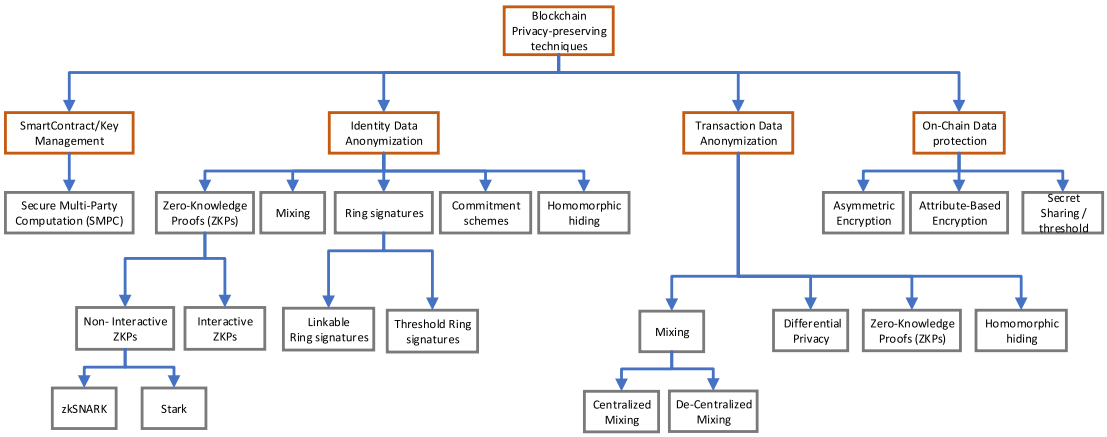


Figure 6.1.1: Taxonomie für Privatsphäre auf der Blockchain (Bernabe et al. 2019)

anonymen Schlüssel, die restlichen Mitglieder verifizieren die Transaktion mit dem öffentlichen Schlüssel der Gruppe. Ein Mitglied kann lediglich seiner Gruppe, aber keiner spezifischen Transaktion zugeordnet werden. Der Gruppenleiter verwaltet die Mitgliedschaft. Die Ringsignatur hingegen besitzt keinen Gruppenleiter und ist auf öffentlichen Blockchains anwendbar. Darüber hinaus lassen sich mit Hilfe homomorpher Verschlüsselung bestimmte Berechnungen direkt auf einem verschlüsselten Text durchführen. Außerdem kann ein Zero-Knowledge-Proof verwendet werden, welcher im Verlauf der Arbeit genauer erläutert wird. Er ermöglicht die Verifizierung von Transaktionen, ohne dass ein Knoten Informationen über diese benötigt.

Dies ist nur eine Reihe von Vorschlägen, die zur Verbesserung des Datenschutzes und der Sicherheit von Blockchain-Anwendungen beitragen können. Man könnte darüber hinaus vorhandene Regularien des technischen Datenschutzes in die Blockchain-Technologie einbinden oder das Datenschutzrecht an die neue Technologie anpassen und weiterentwickeln (Pesch und Böhme 2017b).

2 Privatsphäre auf Blockchains – Anwendung

Im Folgenden werden drei Anwendungsfälle zum Thema Privatsphäre auf Blockchains untersucht. Monero und Zcash stellen zwei Kryptowährungen dar, die besonders für ihre hohe Anonymität bekannt sind. Auch im Bereich des Private Voting

Name	Technology Features	Anonymity	Advantages	Disadvantages	Typical Application
Centralized coin mixing	Trusted third-party	Weak	Short Mixing time	High handling fee, theft of funds, and denial of service attack	Mixcoin, Blindcoin, Dash
Decentralized coin mixing	Multi-signature transaction	Medium	security, and no transaction fee	Leakage coin mixing information, and sybil attack	CoinShuffle, TumbleBit
Zero knowledge proof	Completeness, reliability, and zero knowledge	Strong	Hide transaction details and resist transaction graph analysis	High cost of computing and storage	Zerocoin, Zerocash
Ring signature	Unconditional anonymity, unforgeability, and correctness	Medium	Internal unlinkability	High cost and poor scalability	CryptoNote, Monero
Homomorphic encryption	Encrypted data can be operated without decryption	Strong	Resist transaction graph analysis	High cost of computing and storage	Confidential transaction (CT), Paillier encryption [47]
Hidden address	One-time middle address	Weak	Recipient anonymity	Sender is not anonymous	CryptoNote, Monero
Pedersen commitment	Preventing message leakage by random blinding factor	Strong	The transaction itself is anonymous	Sender and receiver are not anonymous	Confidential transaction (CT), RingCT, Monero
Secure multi-party computation	Input privacy, calculation correctness, and decentralization	Strong	Confidential input message	Message not verifiable	Millionaire Problem (MP)
Trusted execution environment	Have a trusted and secure independent environment	Strong	Ensure data security and integrity	High hardware cost and difficult development of trusted applications	IntelSGX

Figure 6.1.2: Technologien für Schutz der Privatsphäre (Wang et al. 2020)

spielt die Privatsphäre eine bedeutende Rolle. Wo diese hier Anwendung findet und ob Nutzern trotz eines öffentlichen verteilten Netzwerkes Privatsphäre gewährleistet werden kann, wird im Folgenden untersucht.

2.1 Monero

Seit der Entstehung von Bitcoin werden Kryptowährungen mit verbesserten Datenschutzfunktionen entwickelt, die auf der Protokollebene eingebaut werden. Hierzu gehören auch Monero und Zcash. Die Nutzer von Monero verwenden eine Liste an öffentlichen Schlüsseln, bilden damit eine Ringsignatur und können somit verbergen, welche der Adressen ihnen gehört (Fauzi et al. 2019).
Monero wurde im Jahr 2014 unter dem Aspekt der starken Wahrung von Privatsphäre und Anonymität vorgestellt. Als Protokoll wurde bei Monero ursprünglich das CryptoNote-Protokoll genutzt, um so die Privat-sphäre des Teilnehmers, der eine Zahlung empfängt, zu schützen. Um die Identität der Sender zu bewahren, werden verknüpfte Ringsignaturen verwendet. Die wahre Identität des Senders kann so in einem Ring verborgen werden (Li et al. 2019). Monero gilt als eine datenschutzzentrierte Kryptowährung. Das Ziel ist es, das Auffinden von Zahlungen unmöglich zu machen (Hinteregger und Haslhofer 2019). Es wird ein Proof-of-Work-Algorithmus verwendet. Das ursprüngliche CryptoNote-Protokoll wurde erweitert. Da die Anwendung auf vertraulichen Transaktionen basiert, die Ringsignaturen erlauben, werden die Transaktionen vertrauliche Ring-Transaktionen (engl. Ring Confidential Transactions), kurz Ring-CT, genannt. Zu den Eigenschaften des Ring-CT- Protokolls gehört die Dezentralität. Sowohl die Identität des Empfängers als auch die des Senders einer Transaktion bleibt verborgen. Außerdem wird der Betrag der Transaktion geheim gehalten, was bei CryptoNote ursprünglich nicht möglich war. Mit Hilfe eines hash-basierten Mining-Prozesses und der Dezentralisierung wird für eine vertrauenslose Münzgenerierung gesorgt. Einmalschlüssel verstecken die Identität der Empfänger (Noether und Mackenzie 2016).

Ringsignatur

Die Ringsignatur gehört neben der Gruppensignatur zu den anonymen Signaturen. Den Namen verdankt sie ihrer ringähnlichen Struktur (Zhang et al. 2019). Der Sender verwendet bei Monero eine spezielle Ringsignatur für eine Transaktion. Dadurch können doppelte Ausgaben vermieden werden. Diese Signatur kann lediglich einer Gruppe, jedoch keinem einzelnen Mitglied aus dieser Gruppe, zugeordnet werden. Eine Identifikation des wahren Absenders ist damit nicht möglich (Kolb et al. 2020, 28). Ringsignaturen ermöglichen eine Transaktionsmischung ohne zentralen Knoten, um den Betrag von Transaktionen zu verbergen. Eine Gruppe von Teilnehmern erhält eine Signatur. Ein Teilnehmer aus dieser Gruppe verwendet dann für seine Transaktion die öffentlichen Schlüssel der Teilnehmer sowie seinen eigenen privaten Schlüssel. Signiert er seine Transaktion, ist nicht zu erkennen, wer aus dieser Gruppe die Transaktion unterzeichnet hat. So können mehrere Ausgaben getätigt werden, ohne zu unterscheiden, wer die öffentlichen und wer die privaten Schlüssel verwendet hat (Biryukov et al. 2019). Damit wird die Rückverfolgbarkeit von Zahlungen verhindert. Der Betrag, der versendet werden soll, wird mit einer Art Köder-Betrag (engl. Mixin) zur Verschleierung vermischt (Amarasinghe et al. 2019). Die Auswahl der Mixins erfolgt nach einem Zufallsprinzip. Sie werden aus allen Schlüsseln früherer Transaktionen von Teilnehmern des Netzwerkes generiert (Lee und Miller 2018). Die Mixins werden gemeinsam mit der realen Ausgabe verwendet. Dadurch entsteht die Ringsignatur. Mixins sind öffentliche Schlüssel, die bereits in der Blockchain zu finden sind. Sie sind vorhandene Ausgaben von anderen Transaktionen und besitzen die gleiche Anzahl an Münzen. Diese Münzen werden zu einer Eingabe kombiniert. Ein Außenstehender kann so aus allen Ausgaben nicht die wahre Ausgabe erraten. Die öffentlichen Schlüssel enthalten die versteckte wirkliche Anzahl an Münzen einer Transaktion (Wijaya et al. 2018).

Stealth-Adresse

Eine einmalig verwendete Stealth-Adresse, abgeleitet von der richtigen Adresse des Empfängers, bestimmt den Ort einer Transaktion. Somit hat kein externer Beobachter die Möglichkeit, eine Adresse zurückzuverfolgen (Kolb et al. 2020). Die Stealth-Adressen dienen zur Verhinderung der Identifikation von Transaktionen durch die Generierung eines Einmalschlüssels. Dieser Schlüssel wird aus einem Zufallswert sowie aus der Adresse des Empfängers generiert. Die Stealth-Adresse gewährleistet, dass keine Verbindung zwischen Transaktionen hergestellt werden kann (Hinteregger und Haslhofer 2019). Sie ist eine einmalige Adresse, die den Empfänger von Transaktionen verbirgt (Amarasinghe et al. 2019).

Ring-CT

Im Jahr 2017 wurde Monero um vertrauliche Ring-Transaktionen ergänzt. Diese dienen der Verbergung von Zahlungsbeträgen bei gleichzeitiger Möglichkeit der Überprüfung auf deren Gültigkeit. Um den Nutzern diese Privatsphäre und Überprüfbarkeit bieten zu können, wird viel Speicherplatz benötigt. Deswegen wird bereits daran gearbeitet, die benötigte Speicherkapazität für Transaktionen zu reduzieren (Kolb et al. 2020). Ring-CTs

ermöglichen das Verbergen der Zahlungsbeträge und eine gleichzeitige Überprüfung der Transaktionen durch die Teilnehmer (Amarasinghe et al. 2019).

Herausforderungen

Inzwischen hat sich herausgestellt, dass es Möglichkeiten geben könnte, die Anonymität von Transaktionen bei Monero aufzudecken. Die für die Mixin-Inputs verwendete Mixin- Sampling-Strategie ermöglicht die Verknüpfung von Transaktionen, wodurch diese rückverfolgbar werden könnten (Amarasinghe et al. 2019). Die in der Signatur verwendeten Mi- xins dienen zwar dem Schutz der Identität des Senders, die Unauffindbarkeit des Senders kann jedoch inzwischen durch Analysen aufgehoben werden (Wijaya et al. 2019). Nach Amarasinghe et al. (2019) ist außerdem eine Verknüpfung der Stealth-Adressen mit den IP- Adressen auf der Netzwerkebene möglich. Die Monero-Entwickler arbeiten bereits an einem anonymen Zahlungsnetzwerk, Kovri genannt. Es soll dafür sorgen, die IP-Adressen bei Transaktionen über Monero zu verbergen.
Abschließend kann festgehalten werden, dass Monero trotz der anonymen Eigenschaften nicht die ultimative Lösung zur Gewährleistung vollständiger Privatsphäre auf einer Blockchain bietet.

2.2 Zcash

Im Oktober 2016 wurde die Kryptowährung Zcash offiziell eingeführt (Biryukov und Feher 2019). Sie ermöglicht das Schützen des öffentlichen Schlüssels und der Höhe der Transaktion. In diesem System wird eine homomorphe Verschlüsselung genutzt. Knoten können ohne die Seriennummer, Adressen oder die Höhe der Transaktion zu kennen, eine Transaktion validieren (Li et al. 2019, 113). Die Verbindung zwischen Sender und Empfänger soll hier im Gegensatz zu Bitcoin unterbrochen werden (Kappos et al. 2018). Genauso wie Monero basiert das Zcash-System auf den grundlegenden Eigenschaften von Bitcoin, jedoch wurden einige Funktionen ergänzt. Zcash soll die Anonymität der Nutzer optimal wahren. Private Transaktionen sind abgeschirmt, sodass sowohl Sender als auch Empfänger anonym bleiben (Lee 2019).
Bei Zcash lassen sich zwei Transaktionsarten unterscheiden. Es gibt transparente Transaktionen wie bei Bitcoin, bei denen eine Zahlung zwischen öffentlichen, transparenten Adressen ausgetauscht wird. Diese Adressen werden als t-Adressen bezeichnet, und die Transaktionen als t-to-t-Transaktionen. Neben den t-Adressen gibt es die z-Adressen. Bei der zweiten Art von Transaktionen sind Sender und Empfänger der Zahlung geheim. Es gibt lediglich einen Beweis in der Blockchain, dass die z-Adresse gültig ist (Biryukov und Feher 2019). Die z-Adressen befinden sich in einem abgeschirmten Pool (Kappos et al. 2018). Die Hauptnutzer von Zcash sind die Gründer, die Knoten und die von einigen Knoten gebildeten sogenannten Mining-Pools. Für die Erzeugung von Blöcken erhalten die Knoten oder Pools eine Belohnung. Die Anonymität von Zcash wird verstärkt, da neue Münzen, bevor private Transaktionen ausgeführt werden, erst in den abgeschirmten Pool gelegt werden müssen (Zhang et al. 2020).

Shielded Pool

Die Nutzer können ihre Münzen in den abgeschirmten Pool (engl. Shielded Pool) legen. Bei einer Transaktion werden Münzen aus diesem Pool verwendet, ohne dabei aufzudecken, wem diese gehören. Während bei Monero die Adresse eines Teilnehmers auch ohne dessen Zustimmung in einem Ring verwendet werden kann, können Nutzer von Zcash dagegen nicht bestreiten, unfreiwillig Teil einer Transaktion gewesen zu sein. Sie legen ihre Münzen bewusst in den abgeschirmten Pool (Fauzi et al. 2019).

Zero-Knowledge-Proof

Um das Datenschutzproblem, von dem Bitcoin und weitere Kryptowährungen betroffen sind, zu lösen, verwendet Zcash einen Zero-Knowledge-Proof. Dadurch lässt sich sowohl der Ursprung und das Ziel als auch der Betrag der Zahlung verbergen (Wüst et al. 2019). Diese kryptographische Technologie ermöglicht die Verifizierung von Transaktionen in anonymen, dezentralisierten Zahlungssystemen. Die Existenz bestimmter Informationen sowie der Besitz dieser können nachgewiesen werden, ohne die Informationen preiszugeben oder mit den Knoten kommunizieren zu müssen. Somit kann die Privatsphäre der Nutzer gewahrt werden (Amarasinghe et al. 2019). Die Zero-Knowledge-Proofs werden auch zk-SNARKs genannt. Diese Beweise werden für private, abgeschirmte Transaktionen verwendet (Biryukov und Feher 2019). Zk-SNARK steht für Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (Biryukov et al. 2019). Damit können alle Informationen über die Identität von Sender und Empfänger, Beträge sowie Verknüpfungen verborgen werden. Zwischen Sender und Empfänger ist keine direkte Kommunikation notwendig (Wüst et al. 2019).

Herausforderungen

Wüst et al. (2019) haben sich in ihrem Paper mit ressourcenbeschränkten Teilnehmern beschäftigt und ein System entwickelt, um solchen Teilnehmern bei Zcash Privatsphäre zu ermöglichen. Auch wenn Zcash eine Verbesserung in Sachen Anonymität und Wahrung der Privatsphäre hervorbringt, ergeben sich hier anhaltende Herausforderungen. Eine Zcash- Transaktion beinhaltet einen

verschlüsselten Text, Chiffretext genannt. Um zu erkennen, dass eine Zahlung für einen Nutzer bestimmt ist, muss eine Probeentschlüsselung des Chiffretextes stattfinden. Diese Entschlüsselung muss für jede Zahlung durchgeführt werden, um die Transaktionen zu überwachen. Hier stößt das Zcash-System auf ein Ressourcenproblem. Im Gegensatz zu Standard-PCs ist die Entschlüsselung über mobile Geräte oftmals nicht ausführbar.
Darüber hinaus betrug in den ersten Versionen die Dauer für die Erstellung eines Beweises mit der zk-SNARK Technologie 40 Sekunden und benötigte 1,5 GB Speicher. Deshalb wird stets an der Einsparung von Speicherplatz und der Schnelligkeit von Beweisen gearbeitet. Seit Oktober 2018 konnte mit Hilfe eines neuen zk-SNARK-Protokolls die Dauer auf 3 Sekunden und der Speicherplatz auf 40 MB reduziert werden. Das Protokoll nennt sich Sapling (Biryu- kov et al. 2019). Da Zcash sowohl öffentliche, transparente als auch private, abgeschirmte Transaktionen ermöglicht, ist davon auszugehen, dass Transaktionen dennoch bis zu einem gewissen Punkt verknüpft werden können. Zwar bietet Zcash für die Nutzer einen relativ hohen Grad an Anonymität, jedoch ist die Mehrheit der Transaktionen dennoch transparent (Amarasinghe et al. 2019). Es lässt sich demnach auch hier eine Schwachstelle in Bezug auf die Privatsphäre der Nutzer erkennen, welche es in Zukunft zu beheben gilt.

2.3 Private Voting

Blockchain-Anwendungen im Bereich des Online-Voting können das Vertrauen bei elektronischen Wahlen erhöhen. Es gibt verschiedene Möglichkeiten, Blockchain-basierte Wahlsysteme zu verwirklichen. Hierzu gehören auf Kryptowährungen basierte Abstimmungssysteme. Ein Kandidat erhält eine Zahlung vom Wähler, die die Stimmabgabe darstellt. Problematisch ist hier, wenn ein böswilliger Wähler keine Zahlung abgibt und das Geld behält. Außerdem muss eine zentrale vertrauliche Person die Zahlungen kontrollieren. Darüber hinaus gibt es die Möglichkeit, dass das Wahlsystem auf einem intelligenten Vertrag basiert. Hier kann jedoch nur zwischen zwei Kandidaten gewählt werden und die Teilnehmerzahl ist begrenzt. Die dritte Möglichkeit ist die Verwendung einer Blockchain als Wahlurne. So kann die Integrität der Stimmabgaben geschützt werden. Ein derartiges System sollte plattformunabhängig verwendbar sein. Änderungen der Protokolle sollten sich nicht auf das System auswirken. Es sollte sicher und skalierbar sein, sodass eine große Anzahl an Stimmabgaben in einer angemessenen Zeit abgewickelt werden kann (Yu et al. 2018)

Anforderungen

Racsko (2019) hat in seiner Arbeit verschiedene Konsensprotokolle auf ihre Verwend-barkeit für Online-Abstimmungen untersucht. Er kam zu dem Schluss, dass keiner der aktuell existierenden Algorithmen den Anforderungen für Online-Wahlsysteme genügt. Um die Blockchain-Technologie für derartige Systeme dezentral einsetzen zu können, muss ein neues Konsensprotokoll entwickelt werden. Damit können Manipulationen verhindert werden. Nachträglich abgegebene oder verlorene Stimmen sind für alle Teilnehmer sichtbar. Eine Verifizierung des Wahlergebnisses ist notwendig, damit nachvollzogen werden kann, ob eine Abstimmung illegal war oder ob es nachträgliche Änderungen gab. Häufig auftretende Probleme bei Wahlen wie Stimmneuzählungen könnten mit Hilfe der Blockchain-Technologie vermieden werden, was wiederum zu mehr Fairness beiträgt. Die Stimmabgaben können auf Manipulation geprüft werden. Außerdem erhalten die Wähler das Ergebnis unmittelbar. Um eine faire und sichere Wahl mit Hilfe der Blockchain-Technologie zu ermöglichen, ist eine pragmatische Umsetzung notwendig. Bevor die Blockchain für Online-Abstimmungen inklusive eines Konsensprotokolls eingesetzt werden kann, sind zahlreiche technische und theoretische Probleme zu lösen.

Kryptographische Techniken

Es gibt verschiedene kryptographische Techniken, um derartige Wahlsysteme zu realisieren. Eine davon ist die homomorphe Verschlüsselung. Es kann mit verschlüsselten Texten gearbeitet werden, ohne diese dafür zu entschlüsseln. Typische Beispiele hierfür sind die Paillier- und die ElGamal-Verschlüsselung. Des Weiteren kann ein Mischnetz (engl. Mix-Net) verwendet werden. Eine Menge von Chiffriertexten wird miteinander vermischt. Die Stimmenzähler können so die Stimmzettel nicht mit einem Wähler in Verbindung bringen. Eine weitere Option ist die Verwendung des Zero-Knowledge-Proofs. Hier kann die Gültigkeit des Stimmzettels überprüft werden, ohne die Aussage des Zettels preisgeben zu müssen. Darüber hinaus können verknüpfbare Ringsignaturen genutzt werden, um die Privatsphäre der Wähler zu schützen (Yu et al. 2018).

Mögliche Realisierungen

Kshetri und Voas (2018) stellen in ihrer Arbeit eine Idee zur Online-Wahl vor. Blockchain-basierte Wahlen können sich mit dem Austausch digitaler Währungen vergleichen lassen. Jeder Teilnehmer besitzt eine Art Geldbeutel mit einem Ausweis sowie eine einzelne Münze, die für seine Stimme steht. Um einen Kandidaten zu wählen, wird diese Münze vom eigenen Geldbeutel in den des gewünschten Kandidaten übertragen. Sie kann nur einmal ausgegeben werden und vor der

festgelegten Frist wieder zurückgezogen und geändert werden. Per Smartphone oder Computer lässt sich eine Stimme anonym abgeben. Im öffentlichen Stimmbuch sind alle Aktivitäten ersichtlich. Durch den Prüfpfad der Blockchain kann sichergestellt werden, dass keine Änderungen oder das Entfernen von Stimmen stattfinden. Außerdem hält es Betrüger von der Abgabe unrechtmäßiger Stimmen ab.

Ayed (2017) hat in seinem Paper eine E-Voting-Lösung vorgestellt, die vier wichtige An-forderungen erfüllen soll. Hierzu gehört die Anonymität der Wähler, die Genauigkeit der Stimmzählung, die Überprüfbarkeit und die Authentifizierung der Wähler. Der erste Block und die erste Transaktion sollen den Namen des Kandidaten enthalten. Jede Stimme für den Kandidaten wird auf diesem Block platziert. Es soll die Möglichkeit einer Proteststimme, also einer leeren Stimmabgabe, geben. Im System wird geprüft, ob der Wähler stimmberechtigt ist. Die Stimmen sind verschlüsselt und das System generiert die Identifikationsnummer des Wählers, seinen Namen sowie den Hashwert der vorherigen Abstimmung als Eingabe. Die Hashfunktion SHA-256 soll die Informationen verschlüsseln, um das Wahlgeheimnis zu garantieren. Danach wird die Stimme zur Blockchain hinzugefügt und jeder Block mit den vorherigen Stimmen verknüpft. Ein Manko bei dieser Lösung ist, dass keine Möglichkeit besteht, seine Stimmabgabe nochmal zu ändern. Außerdem ist ein Hackerangriff auf das Gerät eines Wählers trotz des sicheren Wahlsystems nicht auszuschließen.

Ouyang et al. (2019) haben in ihrem Paper ein anonymes Online-Abstimmungssystem erarbeitet, das zum Schutz der Privatsphäre sowie zur Glaubwürdigkeit der Abstimmungsdaten beitragen soll. Grundlage ist ein Ethereum-System. Es ist möglich, die ID des Eingangskontos zu ermitteln. Außerdem können die Abstimmungsdaten zurückverfolgt werden. In einer Brieftasche können öffentliche und private Schlüssel beantragt und gespeichert werden. Somit wird die Privatsphäre der Wähler garantiert. In Zukunft sollen die Funktionen des hier erarbeiteten Systems verbessert werden. Es soll robuster und benutzerfreundlicher werden.

Ein Beispiel für ein öffentliches Blockchain-Wahlsystem ist Follow my Vote. In diesem Sys-tem sind Behörden und Wähler miteinander verbunden, wodurch der Wahlprozess nachvollziehbar und transparent wird (Ismail und Materwala 2019). Neben Follow my Vote gibt es weitere Protokolle für Fernabstimmungen wie BitCongress und TIVI. Die Follow my Vote- und TIVI-Protokolle erfüllen zwar einige der oben genannten Anforderungen, jedoch können sie keine Fairness gewährleisten. BitCongress kann neben der Fairness auch keine Gewährleistung dafür geben, dass nur wahlberechtigte Teilnehmer ihre Stimme abgeben (Hardwick et al. 2018). TIVI und Follow my Vote verwenden die Blockchain als eine Wahlurne (Yu et al. 2018). Hardwick et al. (2018) haben in ihrer Arbeit ein Schema für elektronische Wahlen basierend auf der Blockchain-Technologie entwickelt, welches den Anforderungen an ein Online-Abstimmungssystem entsprechen soll. Sie haben herausgearbeitet, dass noch hohes Entwicklungspotenzial in der Kernforschung dieser Technologie von Nöten ist, um komplexe Anwendungen zu unterstützen und zu verbessern.

Herausforderungen

Die bisherigen Lösungen und Ideen, die im Bereich des Private Voting basierend auf Blockchains entwickelt wurden, zeigen Grenzen auf. Dennoch besitzen Online-Wahlen großes Potenzial. Es lassen sich erhebliche Kosten einsparen und die Verantwortung liegt nicht mehr allein in der Hand einer kleinen Gruppe von Beamten, deren Lösungen sich oft als unsicher und diskriminierend herausstellen. Hinzu kommt die mangelnde Transparenz bei traditionellen Wahlen. Neuzählungen beanspruchen Zeit und Kosten, wenn sie überhaupt durchgeführt werden (Orman 2019). Online-Wahlen können ein kostengünstiges, effizientes und sicheres Mittel zur Stimmabgabe in Echtzeit darstellen. Durch kryptographische Verschlüsselung kann Anonymität allein jedoch nicht erreicht werden. Es muss gewährleistet werden, dass die Abstimmung nicht rückverfolgbar ist, denn bei einer Online-Wahl sind Computer, Smartphones und das Internet im Einsatz. Es ist eine Technik notwendig, mit der die Blockchain für derartige Abstimmungen genutzt werden kann, die gleichzeitig die Anonymität und Privatsphäre der Wähler schützt (Yi 2019).

3 Zusammenfassung und Fazit

Die Arbeit hat gezeigt, dass die Entwickler neuer Blockchain-Anwendungen vor einigen Herausforderungen stehen. Die Gesetzgebung ist noch unklar und es fehlen angemessene rechtliche Rahmenbedingungen. Die wohl größte Herausforderung wird sein, die Interessen der Nutzer in Bezug auf die Wahrung ihrer Privatsphäre und das Schützen ihrer Daten mit den Datenschutzgesetzen und der Strafverfolgung in Einklang zu bringen. Die Dezentralität als eine der attraktivsten Eigenschaften der Blockchain-Technologie sollte für ihre Nutzer gewahrt bleiben, ohne Strafverfolgern hier ein Bein zu stellen und ihre Arbeit bei illegalen Aktivitäten zu erschweren.

Als Anwendungsbeispiele wurden Monero, Zcash und das Private Voting herangezogen, um die Bedeutung des Aspektes der Privatsphäre auf Blockchain-Anwendungen aufzuzeigen. Es gibt zahlreiche weitere Anwendungen, in denen der

Datenschutz und die Datensicherheit auf Blockchains eine wichtige Rolle spielen. Diese hier aufzuführen, hätte jedoch den Rahmen dieser Arbeit gesprengt. Den Lesern konnte durch die Beispiele aufgezeigt werden, dass bereits an Lösungen und Techniken gearbeitet wird, um Blockchain-Nutzern Anonymität und Sicherheit bieten zu können. Seit der Entstehung von Bitcoin vor über 10 Jahren hat sich einiges getan. Die Technologie wird ständig weiterentwickelt und ihre Funktionen werden optimiert. Es bleibt spannend zu sehen, wie die Gesetzgebung in Zukunft auf die aufkommenden Blockchain-Anwendungen eingehen wird und inwieweit sie in die Gesetze zum Datenschutz miteinbezogen werden. Aktuell ist klar, dass die Rahmenbedingungen zu diesem Thema noch nicht gefestigt sind. Die bisher entwickelten Techniken zur Verbesserung von Sicherheit und Datenschutz auf Blockchains wie das Mischen von Münzen, digitale Signaturen oder der Zero-Knowledge-Proof allein reichen nicht aus, um alle rechtlichen und persönlichen Anforderungen an diese Technologie zu erfüllen. Hier muss ein Kompromiss zwischen den Wünschen der Nutzer nach Sicherheit, Anonymität und Datenschutz und den Bestrebungen der Gesetzgeber nach festen Regulierungen und eindeutigen Gesetzen zur Verfolgung von Straftaten gefunden werden. Allen voran darf hierbei die Funktionalität und Effizienz der Blockchain-Technologie nicht darunter leiden.

Das Potenzial für künftige Anwendungen ist riesig. Um das Vertrauen in die Blockchain- Technologie zu fördern, müssen sowohl die rechtlichen Akteure als auch die Entwickler neuer verteilter Plattformen Schritte in eine gemeinsame Richtung gehen. Zusammen könnten damit Einschränkungen der rechtlichen Durchsetzung durch und für Blockchain-Lösungen beseitigt werden (Werbach 2018).

Literaturverzeichnis

Acerbi, P. (2019): Is blockchain technology a challenge for antitrust law? In: Competition Law & Policy Debate, 5(3), 63-66.

Achenbach, D.; Baumgart, I.; Rill, J. (2017): Die Blockchain im Rampenlicht. In: DuD – Datenschutz und Datensicherheit, 41(11), 673-677.

Amarasinghe, N.; Boyen, X.; McKague, M. (2019): A survey of anonymity of cryptocurren- cies. In: Proceedings of the Australasian Computer Science Week Multiconference, 2, 1-10.

Andriole, S. J. (2020): Blockchain, cryptocurrency, and cybersecurity. In: IEEE Computer Society, IT Professional, 22(1), 13-16.

Ayed, A. B. (2017): A conceptual secure blockchain-based electronic voting system. In: International Journal of Network Security & Its Applications, 9(3), 1-9.

Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. IEEE Access, 7, 164908-164940.

Biryukov, A.; Feher, D. (2019): Privacy and linkability of mining in Zcash. In: IEEE Conference on Communications and Network Security, 118-123.

Biryukov, A.; Feher, D.; Vitto, G. (2019): Privacy aspects and subliminal channels in Zcash. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 1813-1830.

Bosch, R.; Baumann, K.; Gussmann, A. (2018): Transparenz, Datensicherheit und Automatisierung. In: IM+io, 2, 38-41.

Buhl, H. U.; Schweizer, A.; Urbach, N. (2017): Blockchain-Technologie als Schlüssel für die Zukunft? In: Zeitschrift für das gesamte Kreditwesen, 596-599.

Dai, H. N.; Zheng, Z.; Zhang, Y. (2019): Blockchain for internet of things: A survey. In: IEEE Internet of Things Journal, 6(5), 8076-8094.

Eichler, N.; Jongerius, S.; McMullen, G.; Naegele, O.; Steininger, L.; Wagner, K. (2018): Blockchain, data protection, and the GDPR. In: Blockchain Bundesverband, https://www.bundesblock.de/wp-content/uploads/2019/01/GDPR_Position_Paper_v1.0.pdf, zugegriffen am 08.04.2020.

Engelschall, R. S. (2019): Blockchain – Suchen wir nur das Problem zur Lösung? In: Informatik Spektrum, 42(3), 205-210.

Fanning, K.; Centers, D. P. (2016): Blockchain and its coming Impact on financial services. In: The Journal of Corporate Accounting and Finance, 27(5), 53-57.

Fauzi, P.; Meiklejohn, S.; Mercer, R.; Orlandi, C. (2019): Quisquis: A new design for anonymous cryptocurrencies. In: Galbraith, S. D.; Moriai, S. (Hrsg.): Advances in Cryptology – ASIACRYPT 2019, Springer, Cham, 649-678.

Fill, H. G.; Meier, A. (2020): Blockchain kompakt – Grundlagen, Anwendungsoptionen und kritische Bewertung. Springer Vieweg, Wiesbaden.

Fulmer, N. (2019): Exploring the legal issues of blockchain applications. In: Akron Law R view, 52(1), 161-192.

Genkin, D.; Papadopoulos, D.; Papamanthou, C. (2018): Privacy in decentralized cryptocurrencies. In: Communications of the ACM, 61(6), 78-88.

Hardwick, F. S.; Gioulis, A.; Akram, R. N.; Markantonakis, K. (2018): E-voting with blockchain: An e-voting protocol with

decentralisation and voter privacy. In: IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 1561-1567.

Hein, C.; Wellbrock, W.; Hein, C. (2019): Rechtliche Herausforderungen von Blockchain- Anwendungen: Straf-, Datenschutz- und Zivilrecht. Springer Verlag, Wiesbaden.

Himmer, K. (2019): Blockchain-basiertes Fundraising als innovative Alternative der Unternehmensfinanzierung. Springer Gabler, Wiesbaden.

Hinteregger, A.; Haslhofer, B. (2019): Short paper: An empirical analysis of Monero crosschain traceability. In: Goldberg, I.; Moore, T. (Hrsg.): Financial Cryptography and Data Security, Springer, Cham, 150-157.

Ismail, L.; Materwala, H. (2019): A review of blockchain architecture and consensus proto- cols: Use cases, challenges, and solutions. In: Symmetry, 11(10), 1198.

Joshi, A. P.; Han, M.; Wang, Y. (2018): A survey on security and privacy issues of blockchain technology. In: Mathematical Foundations of Computing, 1(2), 121-147.

Kappos, G.; Yousaf, H.; Maller, M.; Meiklejohn, S. (2018): An empirical analysis of anonymity in Zcash. In: 27th USENIX Security Symposium, 463-477.

Kfir, I. (2020): Cryptocurrencies, national security, crime and terrorism. In: Comparative Strategy, 39(2), 113-127.

Kolb, J; Abdelbaky, M.; Katz, R. H.; Culler, D. E. (2020): Core concepts, challenges, and future directions in blockchain: A centralized tutorial. In: ACM Computing Surveys, 53(1), 1-39.

Kshetri, N.; Voas, J. (2018): Blockchainnenabled e-voting. In: IEEE Software, 35(4), 95-99.

Lee, J. H. (2019): Rise of anonymous cryptocurrencies: Brief introduction. In: IEEE Consumer Electronics Magazine, 8(5), 20-25.

Lee, K.; Miller, A. (2018): Authenticated data structures for privacy-preserving Monero light clients. In: IEEE European Symposium on Security and Privacy Workshops, 20-28.

Li, Y.; Susilo, W.; Yang, G.; Yu, Y.; Du, X.; Liu, D.; Guizani, N. (2019): Toward privacy and regulation in blockchain-based cryptocurrencies. In: IEEE Network, 33(5), 111- 117.

Meiriño, M. J.; Méxas, M. P.; do Valle Faria, A.; Méxas, R. P.; Meirelles, G. D. (2019): Blockchain technology applications: A literature review. In: Brazilian Journal of Operations & Production Management, 16(4), 672-684.

Noether, S.; Mackenzie, A. (2016): Ring confidential transactions. In: Ledger Journal, 1, 1- 18.

Orman, H. (2019): Online voting: We can do it! (We have to). In: Communications of the ACM, 62(9), 25-27.

Ouyang, J.; Deng, Y.; Tang, H. (2019): Blockchain electronic voting system for preventing one vote and multiple investment. In: Zheng, Z.; Dai, H. N.; Tang, M.; Chen, X. (Hrsg.): Blockchain and Trustworthy Systems, Springer, Singapur, 752-757.

Pesch, P.; Böhme, R. (2017a): Datenschutz trotz öffentlicher Blockchain? In: DuD – Datenschutz und Datensicherheit, (41)2, 93-98.

Pesch, P.; Böhme, R. (2017b): Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie. In: DuD – Datenschutz und Datensicherheit, 41(8), 473-481.

Prinz, Prof. Dr. W.; Rose, Prof. Dr. T.; Osterland, T.; Putschli, C. (2018): Blockchain – Verlässliche Transaktionen. In: Neugebauer, R. (Hrsg.): Digitalisierung – Schlüsseltechnologien für Wirtschaft und Gesellschaft, Springer Vieweg, Heidelberg, 311-319.

Pur, S. (2018): Blockchain in der Praxis – Funktionsweise und Anwendungsfälle. ibi research an der Universität Regensburg GmbH, Regensburg.

Racsko, P. (2019): Blockchain and democracy. In: Society & Economy, 41(3), 353-369.

Read, O.; Gräslund, K. (2018): EU-Regulierung von Bitcoin und anderen virtuellen Währungen: erste Schritte. In: Wirtschaftsdienst, 98(7), 504-511.

Reetz, F. (2019): Herausforderungen und Förderstrategien für die Blockchain-Technologie. Studien zum deutschen Innovationssystem, Expertenkommission Forschung und Innovation, 10-2019, Berlin.

Rosenberger, P. (2018): Bitcoin und Blockchain – Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. Springer Vieweg, Berlin.

Ruoti, S.; Kaiser, B.; Yerukhimovich, A.; Clark, J.; Cunningham, R. (2020): Blockchain technology: What is it good for? In: Communications of the ACM, 63(1), 46-53.

Saive, D. (2018): Rückabwicklung von Blockchain-Technologien. In: DuD – Datenschutz und Datensicherheit, 12, 764-767.

Santos, A. A. (2020): What's the big deal about blockchain? In: The Florida Bar Journal,

94(2), 42-46.
Schlatt, V.; Schweizer, A.; Urbach, Prof. Dr. N.; Fridgen, Prof. Dr. G. (2019): Blockchain: Grundlagen, Anwendungen und Potenziale – White Paper. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT.
Schuh, G.; Ryschka, S.; Holtkemper, D.; Wieninger, S.; Kampa, M. (2020): Herausforderungen und Potenziale der Blockchain-Technologie. In: Industrie 4.0 Management, 36(1), 7-10.
Süme, O.; Sens, D. (2019): Blockchain – Rechtsrahmen und Governance. In: IT-Governance, 30, 23-25.
Sunyaev, Prof. Dr. A. (2019): Eine Einführung in die Distributed Ledger Technology (Block-chain – "Like A Locked Train"). In: SSRN Electronic Journal, 16-27.
Tredinnick, L. (2019): Cryptocurrencies and the blockchain. In: Business Information Review, 36(1), 39-44.
Wang, D., Zhao, J., & Wang, Y. (2020). A survey on privacy protection of blockchain: the technology and application. IEEE Access, 8, 108766-108781.
Wang, Q.; Huang, J.; Wang, S.; Chen, Y.; Zhang, P.; He, L. (2020): A comparative study of blockchain consensus algorithms. In: Journal of Physics: Conference Series, 1437, 012007.
Werbach, K. (2018): Trust, but verify: Why the blockchain needs the law. In: Berkeley Technology Law Journal, 33(2), 487-550.
Wijaya, D. A.; Liu, J.; Steinfeld, R.; Liu, D. (2018): Monero ring attack: Recreating zero mix- in transaction effect. In: 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering, 1196-1201.
Wijaya, D. A.; Liu, D.; Liu, J. K.; Yu, J.; Steinfeld, R. (2019): On the unforkability of Monero. In: Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (Asia CSS '19), Association for Computing Machinery, 621-632.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Lehrstuhl für BWL und Wirtschaftsinformatik
Prof. Dr. Axel Winkelmann
Sanderring 2
97070 Würzburg

Autoren und Ansprechpartner

Julian Kolb, M.Sc.

Wissenschaftlicher Mitarbeiter
julian.kolb@uni-wuerzburg.de
+49 931 31-86166

Sophie Kopala

Universität Würzburg

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 931 31-89640

B6.2: Ein erweitertes Privacy-Calculus-Modell für Anwendungen der Blockchain-Technologie

Technologische Entwicklungen wie z. B. die Blockchain haben das Potential, in der Zukunft ganze Industriezweige zu verändern und bieten dabei unter anderem Transparenz, Automatisierung und niedrige Transaktionskosten in vielen Prozessen. Da viele Anwendungen, welche eine Blockchain als technische Komponente nutzen, personenbezogene oder unternehmensinterne Transaktionsdaten verarbeiten, muss der Schutz dieser Daten bereits bei der Anwendungsentwicklung eine zentrale Rolle einnehmen, um Blockchain-Anwendungen produktiv im Massenmarkt einsetzen zu können. Verbraucher und Unternehmen neigen dabei oftmals dazu, ihre Daten nur weiterzugeben, wenn der gefühlte Nutzen mögliche Risiken überwiegt und führen unterbewusst oder bewusst eine Kosten-Nutzen-Rechnung durch. In der vorliegenden Arbeit wird daher ein erweitertes Privacy-Calculus-Modell für Anwendungen der Blockchain-Technologie vorgestellt und untersucht. Dabei spielen vor allem die Affinität zur Blockchain-Technologie generell und die zu erwartenden finanziellen Vorteile eine signifikante Rolle.

1 Blockchain – Privatsphäre in Gefahr?

Die Blockchain-Technologie (BCT) bietet mit ihrem Konzept der dezentralen Datenspeicherung und Konsensfindung, welche mit modernen kryptografischen Methoden verbunden ist, in der Zukunft großes Potential für Transparenz, Automatisierung und niedrige Transaktionskosten in vielen Bereichen. Gerade bei Kryptowährungen gehen viele Nutzer von einer hohen Anonymität aus und sehen dies als positiven Einfluss auf ihre Bereitschaft zur Weitergabe personenbezogener Daten wie z. B. Finanzbewegungen und Konsumverhalten [1]. In den meisten Fällen (auch bei Bitcoin) sind Blockchain-Anwendungen jedoch nicht anonym und die Daten werden nur in pseudonymisierter Form gespeichert und verarbeitet [2]. Daher muss sowohl bei Anwendungen mit personenbezogenen Daten als auch unternehmensinternen Transaktionsdaten der Schutz dieser Daten eine zentrale Rolle einnehmen, um Blockchain-Anwendungen produktiv im Massenmarkt einsetzen zu können. Verbraucher und Unternehmen neigen dazu, ihre Daten nur dann weiterzugeben, wenn der gefühlte Nutzen mögliche Risiken überwiegt [3]. In den letzten Jahren haben zahlreiche Studien versucht, dieses Verhalten in einem Privacy-Calculus-Modell zu erklären, dabei jedoch die BCT bisher unzureichend integriert. In der vorliegenden Arbeit wird daher ein erweitertes Privacy-Calculus-Modell für Anwendungen der BCT vorgestellt und untersucht. Folgende Forschungsfragen sollen dabei beantwortet werden:

FF1: Wie ist der aktuelle Stand der Forschung zur Theorie des Privacy Calculus im Umfeld der Blockchain-Technologie?
FF2: Welche erweiterten Faktoren beeinflussen den Privacy Calculus von Individuen bei Blockchain-Anwendungen?
FF3: Wie kann die Beeinflussung einzelner Faktoren in einem Strukturgleichungsmodell quantifiziert werden?

2 Stand der Forschung

Zur Beantwortung der einleitend gestellten Forschungsfragen FF1 wurde auf etablierte Methoden der IS-Forschung zurückgegriffen. In einem ersten Schritt wurde eine erschöpfende Literaturanalyse nach vom Brocke et al. (2009) und Webster und Watson (2002) durchgeführt, um bestehende Veröffentlichungen im Bereich Privacy Calculus & BCT zu identifizieren [4], [5]. Der Ablauf der Literaturanalyse ist in Abbildung B.6.2.1 dargestellt. Insgesamt konnten mit den Suchbegriffen „Blockchain“ + „privacy calculus“; „dinev“; „culnan“ 155 Treffer im AIS Basket of Eight und den Datenbanken Web of Science, EBSCOHOST, AISeL, Wiley, ScienceDirect, Springer Link und Google Scholar erzielt werden. Nach der Analyse von Titel, Abstract und ggf. Volltext konnten sechs relevante Arbeiten identifiziert werden, welche in diesem Kapitel vorgestellt werden. Durch eine nachfolgende Vorwärts- und Rückwärtssuche konnten vor allem zusätzliche Standardwerke in den Forschungsfeldern Technologieakzeptanz und Privacy Calculus wie z. B. Laufer und Wolfe (1997), Culnan und Bies (2003) und Dinev und Hart (2006) identifiziert werden. Die geringe Anzahl an relevanten Arbeiten bestätigt noch einmal die bestehende Forschungslücke.
Die Theorie des Privacy Calculus geht davon aus, dass Individuen über zukünftige Folgen ihrer Verhaltensreaktionen nachdenken und dabei permanent eine Abwägung von Kosten und Nutzen durchführen. Als Grundlage für viele unterschiedliche Auslegungen und Modelle des Privacy Calculus dienen Referenztheorien oder andere theoretische Erweiterungen wie z. B. Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAU), Social Exchange

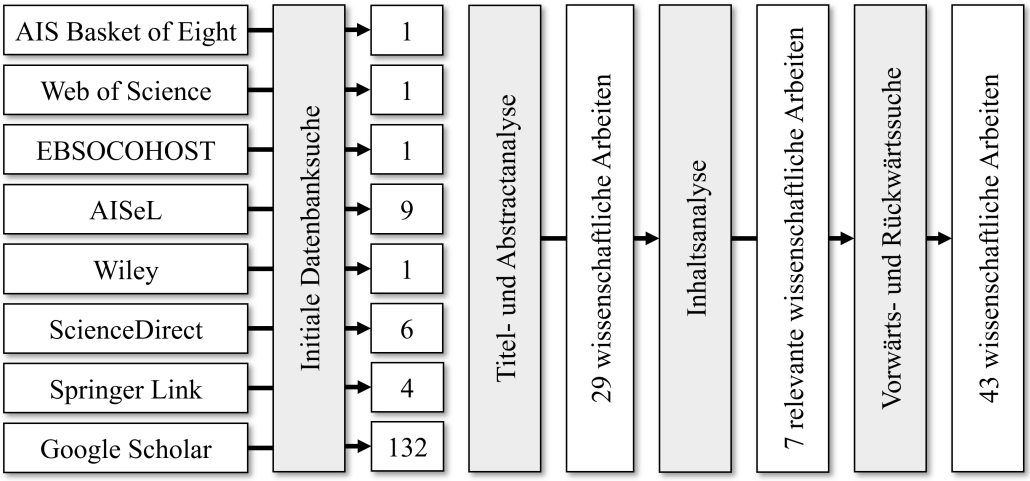


Abbildung B.6.2.1: Verlauf der Literaturanalyse

Theory (SET), Theory of Reasoned Action (TRA) oder Theory of Planned Behavior (TPB).

In ökonomischen Transaktionen und Prozessen und dem damit verbundenen Austausch von personenbezogenen Daten werden die „Kosten" und „Nutzen" durch die beteiligten Individuen abgewogen. Diese Kosten werden dabei oft mit bestimmten Risiken verbunden, die sich aus der Weitergabe von Informationen ergeben. Wenn Individuen mit der Offenlegung ihrer persönlichen Daten konfrontiert werden, begeben sie sich dabei in eine unabhängige Risiko-Nutzen-Analyse oder in einen Kompromiss. Dinev und Hart (2006) beschreiben das wahrgenommene Datenschutzrisiko als das potenzielle opportunistische Verhalten des Empfängers, welches zu einem Kontrollverlust über die personenbezogenen Daten führt. Dies kann beispielsweise durch eine Weitergabe der Daten an Dritte oder einen unbefugten Zugriff geschehen. Allerdings können neben den Risiken auch positive Effekte in Form finanzieller Anreize, einfacher Interaktion in sozialen Netzen oder auch eher technisch orientierter Leistungen wie z. B. Location-Based-Services erfolgen. Die Abwägung von Risiko und Nutzen impliziert also einen Privacy Calculus, der zeigt, dass Individuen eher dazu neigen, personenbezogene Daten weiterzugeben, wenn der Nutzen die Risiken überwiegt [3], [7]. Auch die Art und der Prozess der Datenerhebung, -speicherung und -verarbeitung haben dabei einen Einfluss auf den Privacy Calculus [16].

Obwohl im Umfeld der BCT bereits eine Vielzahl von wissenschaftlichen Arbeiten die Technologieakzeptanz, vor allem in den USA und im asiatischen Raum, beleuchten [17]–[22], ist weitere Forschung dringend notwendig, um eine vollständige Etablierung dieser disruptiven Technologie zu ermöglichen [19], [23]. Die Theorie des Privacy Calculus wurde dabei bisher nur sehr rudimentär betrachtet. Fabian et al. (2016) haben in einer Befragung unter 125 Teilnehmern die Erwartungen an Anonymität im Bitcoin-Netzwerk untersucht und dabei festgestellt, dass ein Großteil der Nutzer dem Netzwerk eine hohe Anonymität unterstellt und daher unbefangen in der Nutzung ist [1], obwohl das Bitcoin-Netzwerk tatsächlich nur eine sehr beschränkte Anonymität aufweist und bereits vielfach de-anonymisiert wurde [2], [24]–[26].

Cabinakova et al. (2019) haben in einer Studie zur Akzeptanz von Decentralized Identity Management Systemen die Privacy Calculus Theorie aufgegriffen und diese in ihr Modell integriert [27]. Dabei hat sich gezeigt, dass die Nutzer durchaus eine starke Kosten-Nutzen-Rechnung durchführen und dass die subjektiv wahrgenommene Kontrolle über die persönlichen Daten einen großen Einfluss auf die Akzeptanz der untersuchten Systeme hat [27]. Auch Frey et al. (2017) haben bereits den Einfluss von technischen und organisatorischen Maßnahmen zum Datenschutz auf die Bereitschaft zur Weitergabe personenbezogener Daten belegt [28]. Dabei wird der BCT jedoch kein signifikanter Einfluss nachgewiesen [28], was in dem schlechten Knowhow über die Technologie der befragten Studienteilnehmer begründet sein könnte.

Alaeddin et al. (2018) haben in einer Studie die Akzeptanz, das Vertrauen sowie die Nutzungsabsicht junger Menschen zum Thema Kryptowährung, also einem Subset des Themengebiets Blockchain, untersucht [29]. Hierbei wurden Studenten in Kuala Lumpur befragt. Der Fokus hierbei lag auf dem Zusammenhang des technischen Interesses der befragten mit der Akzeptanz der Technologie. Hierbei wurde ein positiver Zusammenhang nachgewiesen [29].

Ermakova et al. (2017) haben sich mit den Faktoren beschäftigt, welche das zukünftige Wachstum einer ausgewählten Blockchain-Technologie, dem Bitcoin, beeinflussen und haben hierzu 100 Experten befragt [30]. Hierbei stellte sich heraus, dass die befragten Experten den Einfluss von Anonymität und Informationssicherheit sowohl als größte Wachstumschance als auch als größtes Risiko identifizeren und somit der Frage nach dem Einfluss

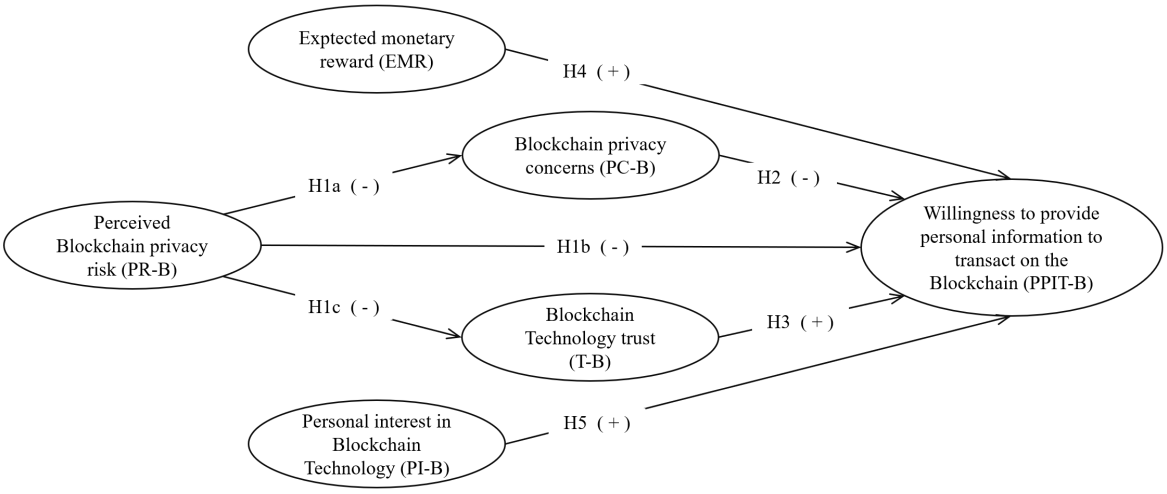


Abbildung B.6.2.2: Forschungsmodell

der persönlichen Informationssicherheit weiter Gewicht verleiht [30].

3 Entwicklung eines Forschungsmodells

Um zu untersuchen, wie sich die BCT auf die Bereitschaft zur Offenlegung von persönlichen Daten auswirkt (FF2), wurde durch einen iterativen Prozess ein Forschungsmodell entwickelt, welches in Abbildung B.6.2.2 schematisch dargestellt ist. Derartige Modelle wurden bereits in vielen Studien erfolgreich eingesetzt und bieten die Möglichkeit, Zusammenhänge und Hypothesen visuell zu erfassen und durch Variablen darzustellen [27], [31].
Zur Erstellung des Forschungsmodells wurde auf die Delphi-Methode zurückgegriffen [32], [33]. Dazu wurden mehrere Experten aus dem Gebiet der Blockchain-Technologie in einem Panel zusammengebracht und nach ihren Grundsatzpositionen zu den eingangs gestellten Forschungsfragen befragt. Dabei wurden auch etablierte Modelle wie z. B. Dinev und Hart (2006) und Cabinakova et al. (2019) vorgestellt und bereits nachgewiesene Abhängigkeiten in den Delphi-Prozess integriert, jedoch auf den Zusammenhang zur BCT adaptiert [3], [27]. In einem nachfolgenden iterativen Prozess wurden die von den Teilnehmern dargelegten Meinungen und Sachverhalte strukturiert und bewertet. Die jeweiligen Ergebnisse wurden durch einen Moderator festgehalten und zusammengefasst. Insgesamt wurde so das Modell von Dinev und Hart (2006) grundsätzlich bestätigt, jedoch neben den bereits teilweise erforschten Faktoren PR-B, PC-B und PI-B insbesondere bei EMR und T-B noch großes Potential in der Forschung erkannt. So wird angenommen, dass der EMR einen großen Einfluss auf die PPIT-B hat, da Nutzer der BCT aktuell starke Assoziationen zu den Gewinnen an Kryptobörsen und ICO's herstellen. Ebenso ist das eigene Interesse an der BCT ein starker Motivator, eine Anwendung mit dieser technologischen Komponente zu nutzen.
Folgende Hypothesen wurden im Verlauf des Delphi-Prozesses aufgestellt und sollen anschließend überprüft werden:
H1a: Das wahrgenommene Privatsphärenrisiko hat einen positiven Einfluss auf die Privatsphärenbedenken.
Die erste Hypothese geht davon aus, dass das wahrgenommene Risiko der Privatsphäre durch Blockchain die Privatsphärenbedenken eines Nutzers negativ beeinträchtigt. Es erscheint logisch, dass mit einem höheren Risiko auch die Bedenken steigen.
H1b: Das wahrgenommene Privatsphärenrisiko hat einen negativen Einfluss auf die Bereitschaft zur Informationspreisgabe in der Blockchain.
Ebenfalls ist davon auszugehen, dass ein höheres wahrgenommenes Risiko der Privatsphäre durch die Nutzung von Blockchain sich negativ auf die Nutzungsbereitschaft auswirkt.
H1c: Das wahrgenommene Privatsphärenrisiko hat einen negativen Einfluss auf das Vertrauen in die Blockchain-Technologie.
Diese Hypothese vermutet, dass ein höheres wahrgenommenes Privatsphärenrisiko durch Nutzung der Blockchain-Technologie das Vertrauen in die Technik schmälert.
H2: Die Privatsphärenbedenken haben einen negativen Einfluss auf die Bereitschaft zur Informationspreisgabe in der Blockchain
Auch wird vermutet, dass ein Befragter mit hohen Privatsphärenbedenken weniger gewillt zur Nutzung eines auf Blockchain aufbauenden Dienstes ist als ein Nutzer mit weniger Bedenken.
H3: Das Vertrauen in die Blockchain-Technologie hat einen positiven Einfluss auf die Bereitschaft zur Informationspreisgabe in der Blockchain.
Eine weitere Vermutung ist die Annahme, dass ein höheres Vertrauen in die Technologie Blockchain zu einer höheren Nutzungsbereitschaft und demzufolge auch zu einer höheren Bereitschaft zur Preisgabe von Nutzerdaten in der Blockchain führt.
H4: Der erwartete, finanzielle Nutzungsanreiz hat einen positiven Einfluss auf die Bereitschaft zur Informationspreisgabe in der Blockchain.
In Hypothese 4 wird angenommen, dass ein höherer erwarteter finanzieller Anreiz bei der Nutzung (z. B. Spekulationsgewinne an Börsen, niedrigere Transaktionskosten oder Belohnungen für die Teilnahme am Miniprozess) zu einer höheren Nutzungs- und Datenpreisgabebereitschaft führt.
H5: Das persönliche Interesse an der Blockchain-Technologie hat einen positiven Einfluss auf die Bereitschaft zur Informationspreisgabe in der Blockchain.
Abschließend wird auch der Einfluss des persönlichen Interesses in die Technologie abgebildet. Ein höheres persönliches Interesse an der Blockchain-Technologie führt zu einer vermutlich höheren Bereitschaft zur Datenpreisgabe.

4 Datenerhebung

Zur empirischen Untersuchung des beschriebenen Forschungsmodells wurde eine standardisierte Umfrage erstellt, welche spezifische Fragen für die unterschiedlichen Variablen und zu untersuchenden Hypothesen enthält. Um den Befragten ein grundlegendes Verständnis über die Blockchain-Technologie zu geben, wird der Befragung ein kurzes Informationsvideo vorangestellt. Inhalt dieses Videos sind ein kurzer Abriss über die Funktionsweise der Technologie und mögliche Anwendungsfälle in einer leicht verständlichen Form. Das Video

ist über folgenden Link frei zugänglich: https://youtu.be/4FU3tc-foaI.
Mit Hilfe von Likert-Skalen ist eine Quantifizierung der Antworten möglich und erlaubt schließlich deren Überführung in ein Strukturgleichungsmodell [3]. Für die Befragung wurden Likert-Skalen mit fünf Antwortmöglichkeiten gewählt, welche im Vergleich zu einer Skala mit einer geraden Anzahl an Antwortmöglichkeiten dem Befragten auch die Wahl lässt, bei einer Frage eine unschlüssige Antwort zu geben [34]. Dies ist sinnvoll, da auch Menschen ohne technisches Vorwissen befragt werden, die möglicherweise einige Fragen nicht vollständig beantworten können.
Bei der Auswahl der Untersuchungsteilnehmer ist insbesondere darauf zu achten, eine breite Streuung in Alter, Geschlecht, Bildungsgrad und Technologieinteresse zu erreichen, um die Tauglichkeit der Massendurchdringung nachzuweisen [1]. Daher werden zu Beginn der Befragung unterschiedliche demographische Daten abgefragt (Alter, Geschlecht, Bildungsgrad) und durch eine Einschätzung des eigenen Blockchain-Know-hows ergänzt. In Tabelle B6.2.1 (Anhang) wird der erstellte Fragebogen dargestellt.
Nach einem Pretest mit zehn Teilnehmer*innen wurde die Studie im November 2019 als digitale Umfrage über das Portal Unipark veröffentlicht und von 366 Teilnehmer*innen vollständig bearbeitet.

5 Auswertung der Ergebnisse

Im ausgewerteten Datensatz konnte eine homogene Verteilung nach Geschlecht und Bildungsstand angetroffen werden. Die Altersstruktur ist ebenfalls grundsätzlich homogen, hat jedoch einen deutlichen Peak zwischen 22 und 32 Jahren, was auf die Nutzung von Portalen zur Vermarktung der Umfrage zurückzuführen ist. Auffallend ist jedoch, dass die Mehrheit der Nutzer (ca. 85 % der Teilnehmer*innen) nur über mäßige, schlechte oder keine Kenntnisse im Bereich Blockchain verfügen, wobei davon ausgegangen werden kann, dass dies nur einen geringen Einfluss auf die Ergebnisse hat.
Henseler et al. (2009) erklären, dass die Pfadmodellierung in einem frühen Stadium der theoretischen Entwicklung empfohlen wird, um explorative Modelle zu testen und zu validieren. Da durch das vorliegende Modell eine neue Theorie eingeführt werden soll, wird das „partial least squares"-Verfahren (PLS) für die Analyse des theoretischen Modells nach Abschluss der Datenerhebung genutzt (Chin, 1998). Nach Chin (2010) sollen dazu zunächst die Zuverlässigkeit und Validität der verwendeten Variablen untersucht und anschließend die Bewertungsergebnisse in einem Strukturgleichungsmodell präsentiert werden (FF3). Für die anschließende Analyse des Modells wurde auf SmartPLS in der neuesten Version zurückgegriffen. Die Zahlen in den jeweiligen Verbindungen zwischen den Konstrukten in Abbildung 54 zei-gen den errechneten Regressionskoeffizienten an. Der Wert 0 steht dabei für keinen erkennbaren Zusammenhang, während eine 1 eine vollständige Korrelation der Parameter signalisiert. Bei einem Wert unter 0 wird dementsprechend eine negative Korrelation angezeigt. Laut Chin liegt bereits ein bedeutsamer Zusammenhang zwischen zwei Konstrukten vor, wenn der Pfadkoeffizient größer/gleich -0,2 bzw. kleiner/gleich 0,2 ist (Chin, 1998). Die Überprüfung der Hypothesen führt daher zu folgenden Ergebnissen:
H1a, die den Zusammenhang zwischen dem wahrgenommenen Privatsphärenrisiko und den Privatsphärenbedenken beschreibt, hat sich mit einem Regressionskoeffizienten von 0,598 deutlich bestätigt und zeigt, dass ein höheres wahrgenommenes Privatsphärenrisiko einen positiven Einfluss auf die Privatsphärenbedenken hat.
H1b, die den Zusammenhang zwischen dem wahrgenommenen Privatsphärenrisiko und der

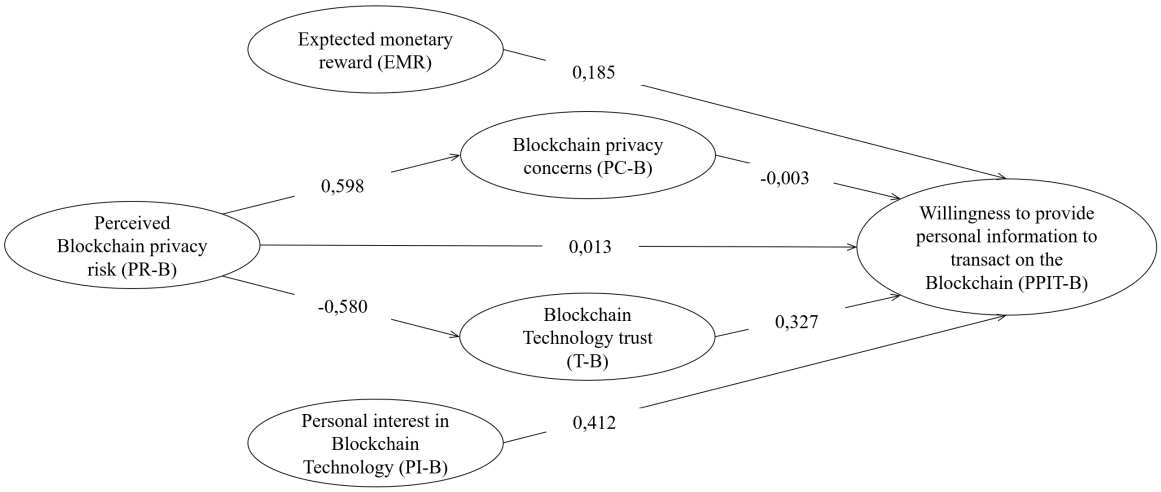


Abbildung B6.2.3: Ergebnisse des Strukturgleichungsmodells nach der Analyse in SmartPLS

Bereitschaft zur Informationspreisgabe in der Blockchain beschreibt, hat sich in unserem Modell bei den Teilnehmern nicht bewahrheitet. Der Koeffizient ist mit 0,013 sehr nahe bei Null und ein Zusammenhang ist somit nicht nachweisbar.

H1c, die den negativen Einfluss des wahrgenommenen Privatsphärenrisikos auf das Vertrauen in die Blockchain-Technologie widerspiegelt, ist mit -0,58 sehr deutlich bestätigt worden.

H2 wiederum, die das Verhältnis von PC-B auf PPIT-B beschreibt, lässt sich in der durchgeführten Umfrage nicht bestätigen. Mit -0,003 ist der Regressionskoeffizient sehr nah bei Null und demzufolge ist ein Einfluss nicht nachzuweisen.

H3, welche die Verbindung zwischen T-B und PPIT-B thematisiert, hat sich im Gegensatz dazu bestätigt. Mit 0,327 als Koeffizient hat sich gezeigt, dass es einen mit über 0,2 bedeutsamen positiven Zusammenhang zwischen T-B und PPIT-B gibt, der sich aus den Antworten der 366 Beteiligten errechnen lässt.

H4 befasst sich mit dem Einfluss einer möglichen finanziellen Entlohnung für die Blockchain-Nutzung auf die Bereitschaft zur Nutzung der Technologie. Der Koeffizient dieses Zusammenhangs zeigt mit 0,185 einen vorhandenen Einfluss an. Allerdings ist dieser mit einem Wert von kleiner 0,2 als nicht bedeutsam einzuschätzen.

H5 als letzte postulierte Hypothese thematisiert den Einfluss des persönlichen Interesses in Technologie und Blockchain auf die Nutzung und Bereitschaft zur Preisgabe von Informationen. Hier hat sich mit einem Wert von 0,412 gezeigt, dass es einen bedeutsamen Einfluss dieses Faktors gibt.

Abschließend lässt sich aus den oben genannten Ausführungen festhalten, dass sich die Hypothesen H1a, H1c, H3 und H5 bestätigen lassen, wobei H4 in seiner Auswirkung als unterhalb eines relevanten Signifikanzniveaus einzuschätzen ist. H1b und H2 sind in der vorhandenen Studie zurückzuweisen.

6 Zusammenfassung

Es hat sich gezeigt, dass die Technologieakzeptanzforschung und insbesondere auch die Theorie des Privacy Calculus etablierte Forschungsgebiete der Wirtschaftsinformatik sind, aber im Umfeld der BCT noch unzureichend untersucht wurden (FF1). Um den Einfluss verschiedener Faktoren wie z. B. der zu erwartende monetäre Nutzen oder die Affinität zur BCT auf die Bereitschaft zur Offenlegung von persönlichen Daten in dezentralen Anwendungen zu untersuchen, wurde ein Forschungsmodell mit insgesamt sieben Hypothesen in einem Delphi-Prozess entwickelt (FF2). Dabei wurde auch auf bereits etablierte Modelle wie z. B. von Dinev und Hart (2006) zurückgegriffen und diese auf den Kontext der Blockchain-Technologie adaptiert. Anschließend wurde eine standardisierte Umfrage erstellt und die Ergebnisse nach dem PLS-Verfahren in ein Strukturgleichungsmodell überführt. Dabei konnten vier der sieben Hypothesen bestätigt werden, zwei Hypothesen werden als nichtzutreffend zurückgewiesen und eine Hypothese liegt knapp unterhalb der Annahmeschwelle und kann daher nicht automatisch als falsch eingestuft werden (FF3). Insgesamt konnte ein deutlicher Zusammenhang zwischen dem Privatsphärenverhalten und dem Verhalten der Nutzer von Blockchain-Technologie nachgewiesen werden, wobei monetäre Aspekte überraschenderweise nicht im Vordergrund stehen.

LATENTE VARIABLE	Item	Skala
METADATEN	Bitte beantworten Sie folgende Fragen:	
	META 1: Bitte geben Sie Ihr Alter an.	Diskreter Wert
	META 2: Bitte geben Sie Ihr Geschlecht an.	Männlich, Weiblich, Divers, Keine Angabe
	META 3 Welches ist der höchste akademische Abschluss, über den Sie derzeit verfügen?	Kein Schulabschluss, Grund-/Hauptschulabschluss, Mittlere Reife, Abitur, Abgeschlossene Ausbildung, Fachhochschulabschluss, Hochschulabschluss, Promotion
	META 4: Wie schätzen Sie Ihre Kenntnis über die Blockchain-Technologie ein?	Keine Kenntnisse – Sehr gute Kenntnisse
PPIT-B	Wie schätzen Sie Ihre Bereitschaft ein, Blockchain-Technologie in folgenden Situationen in Ihrem Alltag zu verwenden:	Nicht vorhanden – Sehr wahrscheinlich
	PPIT-B 1: Bezahlen mit Kryptowährung (z. B: Bitcoin).	
	PPIT-B 2: Spekulation am Kapitalmarkt.	
	PPIT-B 3: Nachverfolgung der Lieferkette von Lebensmitteln.	
	PPIT-B 4: Dezentrale Speicherung von Gesundheitsdaten.	
	PPIT-B 5: Blockchain in mit dem Internet verbundener Haushaltsgeräte.	
	PPIT-B 6: Blockchain in der Kommunikation mit öffentlichen Einrichtungen (z. B. Behörden).	
	PPIT-B 7: Blockchain in Videospielen	
PR-B	Wie hoch schätzen Sie ihr Risiko bei der Nutzung von BC ein, dass folgende Situationen eintreffen:	Sehr niedriges Risiko – Sehr hohes Risiko
	PR-B 1: Ihre privaten Daten werden missbraucht.	
	PR-B 2: Ihre persönlichen Informationen werden unerlaubt an Dritte weitergegeben oder veröffentlicht.	
	PR-B 3: Sie werden durch staatliche Einrichtungen offen oder verdeckt überwacht.	
	PR-B 4: Es werden Nutzungsprofile (z. B. für gezielte Werbung) über Sie erstellt.	
PC-B	Wie hoch schätzen Sie die Auswirkungen folgender Situationen auf Sie ein?	Sehr geringe Auswirkung – sehr hohe Auswirkung
	PC-B 1: Ihre privaten Daten werden missbraucht.	
	PC-B 2: Ihre persönlichen Informationen werden unerlaubt an Dritte weitergegeben oder veröffentlicht.	
	PC-B 3: Sie werden durch staatliche Einrichtungen offen oder verdeckt überwacht.	
	PC-B 4: Es werden Nutzungsprofile (z. B. für gezielte Werbung) über Sie erstellt.	

T-B	Stimmen sie folgenden Aussagen zum Vertrauen in die Blockchain-Technologie zu?	Keine Zustimmung – volle Zustimmung
	T-B 1: Blockchaindienste sind sichere Umgebungen für Informationsaustausch.	
	T-B 2: Blockchaindienste sind sichere Umgebungen für Geschäftstransaktionen.	
	T-B 3: Blockchaindienste gehen vertrauensvoll mit Userdaten um.	
	T-B 4: Blockchaindienste versuchen ihr Äußerstes, um sich gegen technische Schwachstellen abzusichern, die zum Datenverlust verwendet werden können.	
PI-B	Wie groß ist Ihr Interesse an Blockchain und Technologie?	Keine Zustimmung - volle Zustimmung
	PI-B 1: Mein persönliches Interesse an der Nutzung von Blockchaindiensten übersteigt mögliche Bedenken.	
	PI-B 2: Je größer mein Interesse an der Nutzung ist, desto unwichtiger werden die Bedenken.	
	PI-B 3: Im Allgemeinen ist mein Nutzungsinteresse größer als meine Bedenken.	
	PI-B 4: Ich bin grundsätzlich neuer Technologie gegenüber aufgeschlossen.	
	PI-B 4: Ich gehöre gerne zu den Ersten, die eine neue Technologie im Alltag nutzen.	
EMR	Stimmen Sie folgenden Aussagen bezüglich des Einflusses einer finanziellen Vergütung (z. B. geringere Transaktionskosten oder Gewinnausschüttung) auf die Nutzung von Blockchain-Technologie zu?	Keine Zustimmung – volle Zustimmung
	EMR 1: Finanzielle Anreize sind der einzige Grund für mich, Blockchaindienste zu nutzen.	
	EMR 2: Finanzielle Anreize sind der wichtigste Grund für mich, Blockchaindienste zu nutzen.	
	EMR 3: Je höher der finanzielle Anreiz ist, desto gewillter bin ich, Blockchaindienste zu nutzen.	

Tabelle B6.2.1: Darstellung des Fragebogens

Literaturverzeichnis

1. Fabian, B., T. Ermakova, and U. Sander, "Anonymity in Bitcoin – The Users' Perspective," in *37th International Conference on Information Systems (ICIS) 2016*, 2016.
2. Lischke, M. and B. Fabian, "Analyzing the Bitcoin Network: The First Four Years," *Future Internet*, vol. 8, no. 4, p. 7, Mar. 2016.
3. Dinev, T. and P. Hart, "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research*, vol. 17, no. 1, pp. 61–80, Mar. 2006.
4. vom Brocke, J., A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, and A. Cleven, "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process," *17th European Conference on Information Systems*, vol. 9, pp. 2206–2217, 2009.
5. Webster, J. and R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review.," *MIS Quarterly*, vol. 26, no. 2, pp. xiii–xxiii, 2002.
6. Laufer, R. S. and M. Wolfe, "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues*, vol. 33, no. 3, pp. 22–42, Jul. 1977.
7. Culnan, M. J. and R. J. Bies, "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues*, vol. 59, no. 2, pp. 323–342, Jun. 2003.
8. Smith, Dinev, and Xu, "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly*, vol. 35, no. 4, p. 989, 2011.
9. Ajzen, I., "From Intentions to Actions: A Theory of Planned Behavior," in *Action Control*, Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 11–39.
10. Ajzen, I. and M. Fishbein, *Understanding attitudes and predicting social behavior*. Prentice-Hall, 1980.
11. Weinhard, A., M. Hauser, and F. Thiesse, "Explaining Adoption of Pervasive Retail Systems with a Model based on UTAUT2 and the Extended Privacy Calculus," *PACIS 2017 Proceedings*, Jul. 2017.
12. Berg, B. L., *Qualitative Research Methods for the Social Sciences*. Needham Heights: Allyn & Bacon, 2001.
13. Crossler, R. and C. Posey, "Robbing Peter to Pay Paul: Surrendering Privacy for Security's Sake in an Identity Ecosystem," *Journal of the Association for Information Systems*, vol. 18, no. 7, pp. 487–515, Jul. 2017.
14. Xu, H., H.-H. Teo, B. C. Y. Tan, and R. Agarwal, "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems*, vol. 26, no. 3, pp. 135–174, Dec. 2009.
15. Cabinakova, J., N. Kathrin Ostern, and J. Krönung, "Understanding Preprototype User Acceptance of Centralised and Decentralised Identity Management Systems," in *Proceedings of the 27th European Conference on Information Systems (ECIS)*, 2019.
16. Beke, F. T., F. Eggers, and P. C. Verhoef, "Consumer Informational Privacy: Current Knowledge and Research Directions," *Foundations and Trends® in Marketing*, vol. 11, no. 1, pp. 1–71, 2018.
17. Queiroz, M. M. and S. Fosso Wamba, "Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA," *International Journal of Information Management*, vol. 46, pp. 70–82, 2019.
18. Kamble, S., A. Gunasekaran, and H. Arha, "Understanding the Blockchain technology adoption in supply chains-Indian context," *International Journal of Production Research*, vol. 57, no. 7, pp. 2009–2033, 2019.
19. Li, Y., T. Marier-Bienvenue, A. Perron-Brault, X. Wang, and G. Paré, "Blockchain Technology in Business Organizations: A Scoping Review," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.
20. Esmaeilzadeh, P., S. Hemang, and K. Cousins, "Individuals' Cryptocurrency Adoption: A Proposed Moderated-Mediation Model," in *Proceesings of Americas Conference on Information Systems (AMCIS) 2019*, 2019.
21. Mendoza-Tello, J. C., H. Mora, F. A. Pujol-López, and M. D. Lytras, "Disruptive innovation of cryptocurrencies in consumer acceptance and trust," *Information Systems and e-Business Management*, pp. 1–28, Jul. 2019.
22. Sadhya, V. and H. Sadhya, "Barriers to Adoption of Blockchain Technology," *AMCIS 2018 Proceedings*, Aug. 2018.
23. Lowry, P. B., T. Dinev, and R. Willison, "Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda," *European Journal of Information Systems*, vol. 26, no. 6, pp. 546–563, 2017.
24. Reid, F. and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," in *IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing*, 2011, pp.

1318–1326.
25. Mastan, I. D. and S. Paul, “A new approach to deanonymization of unreachable bitcoin nodes,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018.
26. Fanti, G. and P. Viswanath, “Deanonymization in the Bitcoin P2P Network,” *Advances in Neural Information Processing Systems 30*, 2017.
27. Cabinakova, J., N. Kathrin Ostern, and J. Krönung, “Understanding Preprototype User Acceptance of Centralised and Decentralised Identity Management Systems,” in *Proceedings of the 27th European Conference on Information Systems*, 2019.
28. Frey, R. M., P. Buhler, A. Gerdes, T. Hardjono, K. L. Fuchs, and A. Ilic, “The effect of a blockchain-supported, privacy-preserving system on disclosure of personal data,” in *IEEE 16th International Symposium on Network Computing and Applications (NCA)*, 2017, pp. 1–5.
29. Alaeddin, O., O. Alaeddin, and R. Altounjy, “Trust, Technology Awareness and Satisfaction Effect into the Intention to Use Cryptocurrency among Generation Z in Malaysia,” *International Journal of Engineering & Technology*, vol. 7, no. 4.29, pp. 8–10, Nov. 2018.
30. Ermakova, T., B. Fabian, A. Baumann, M. Izmailov, and H. Krasnova, “Bitcoin: Drivers and Impediments,” *SSRN Electronic Journal*, Aug. 2017.
31. Eagly, A. H. and S. Chaiken, *The psychology of attitudes*. Harcourt Brace Jovanovich College Publishers, 1993.
32. Heinzl, A., W. König, J. H.-Wirtschaftsinformatik, and undefined 2001, “Erkenntnisziele der Wirtschaftsinformatik in den nächsten drei und zehn Jahren,” *Springer*.
33. Dalkey, N. and O. Helmer, “An Experimental Application of the DELPHI Method to the Use of Experts,” *Management Science*, vol. 9, no. 3, pp. 458–467, Apr. 1963.
34. Franzen, A., “Antwortskalen in standardisierten Befragungen,” in *Handbuch Methoden der empirischen Sozialforschung*, Wiesbaden: Springer Fachmedien Wiesbaden, 2014, pp. 701–711.
35. Henseler, J., C. M. Ringle, and R. R. Sinkovics, “The use of partial least squares path modeling in international marketing,” Emerald Group Publishing Limited, 2009, pp. 277–319.
36. Chin, W. W., “The partial least squares approach for structural equation modeling.,” in *Modern methods for business research*, 1998, pp. 295–336.
37. Chin, W. W., “How to Write Up and Report PLS Analyses,” in *Handbook of Partial Least Squares*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 655–690.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Lehrstuhl für BWL und Wirtschaftsinformatik
Prof. Dr. Axel Winkelmann
Sanderring 2
97070 Würzburg

Autoren und Ansprechpartner

Julian Kolb, M.Sc.

Wissenschaftlicher Mitarbeiter
julian.kolb@uni-wuerzburg.de
+49 931 31-86166

Adrian Hofmann, M.Sc.

Wissenschaftlicher Mitarbeiter
adrian.hofmann@uni-wuerzburg.de
+49 931 31-84537

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 931 31-89640

B6.3: Anforderungen an Datenschutz, Datensicherheit und Zertifikate

Zur Erhebung der Anforderungen an Datenschutz, Datensicherheit und Zertifikate wurde zunächst eine Literaturanalyse gemäß dem Vorgehen von vom Brocke et al. (2009) durchgeführt. Dabei wurden unterschiedliche Arbeiten mit dem Fokus auf die genannten Problemfelder identifiziert, deren Ergebnisse hier zusammengefasst und in eine Anforderungsdefinition für das Projekt PIMKoWe überführt werden.

1 Anforderungen aus der Literatur

Zur Erhebung der Anforderungen an Datenschutz, Datensicherheit und Zertifikate wurde zunächst eine Literaturanalyse gemäß dem Vorgehen von vom Brocke et al. (2009) durchgeführt. Dabei wurden unterschiedliche Arbeiten mit dem Fokus auf die genannten Problemfelder identifiziert, deren Ergebnisse hier zusammengefasst und in eine Anforderungsdefinition für das Projekt PIMKoWe überführt werden.

Datenschutz

Konzepte rund um das Thema Datenschutz spielen in der Blockchain traditionell eine große Rolle, da bereits Nakamoto (2008) dem Thema Privacy eine besondere Bedeutung zugeordnet hat (J. Kolb et al., 2020). Demnach arbeiten bestehende Informationssysteme mit einer Limitierung des Zugriffs auf personenbezogene Daten, wohingegen die Blockchain durch eine Trennung von Identitäten und Transaktionen versucht, Anonymität und somit einen Schutz der personenbezogenen Daten zu wahren (Nakamoto, 2008). Im Rahmen einer Literaturanalyse ist insbesondere die im MISQE erschienene Arbeit von Rieger et al. (2019) zu erwähnen. Die Autoren untersuchen die Vereinbarkeit der Europäischen Datenschutzgrundverordnung (DSGVO) mit den Funktionsweisen und technischen Komponenten der Blockchain-Technologie. Sie stellen drei Empfehlungen auf, welche bei der Konzeption von datenschutzkonformen Systemen eingehalten werden sollen (Rieger et al., 2019):

(1): Keine Speicherung von personenbezogenen Daten in einer Blockchain:
Blockchain-Anwendungen sollten so konzipiert werden, dass es nicht notwendig ist, personenbezogene Daten auf der Blockchain selbst zu speichern. Stattdessen sollten personenbezogene Daten in Systemen verbleiben, die eine Veränderung und Löschung ermöglichen und damit den Anforderungen der DSGVO entsprechen. Dies gilt auch für Daten, welche die Identifizierung einer Person durch die Analyse von Nutzungsmustern ermöglichen könnten (Rieger et al., 2019).

(2): Wenn personenbezogene Daten verarbeitet werden müssen, sollte eine private und permissioned Blockchain mit Pseudonymisierung kombiniert werden:
Wenn eine Blockkettenlösung Personendaten verarbeiten soll, ist ein Pseudonymisierungsansatz zu verfolgen, um eine Zuordnung der Daten zu genau einer Person zu regulieren, da ein zentraler Intermediär in den meisten Fällen nicht praktikabel ist und dem Grundsatz der Dezentralisierung entgegensteht. Die Autoren empfehlen ferner die Nutzung einer privaten und permissioned Blockchain, welche die Einrichtung und Verwaltung von Vereinbarungen vereinfacht, die für die gemeinsame Verarbeitung personenbezogener Daten erforderlich sind. Insbesondere ermöglicht ein privates Netzwerk die Einrichtung eines kontrollierten Einführungsprozesses, in dessen Verlauf neue Teilnehmer in die Vereinbarungen aufgenommen werden können. Ein privates Netzwerk erleichtert die Schaffung eines flexiblen und rollenbasierten Modells für die Zuweisung von Zuständigkeiten, wobei sich auch pseudonymisierte Daten auf ein absolutes Minimum beschränken sollten, um unbeabsichtigte Zuweisungen zu vermeiden (Rieger et al., 2019).

(3): Wenn Blockchain-Anwendungen mit organisationsübergreifenden Prozessen arbeiten, sollte eine private und permissioned Blockchain mit Pseudonymisierung und einem Identifier Mapping kombiniert werden:
Bei organisationsübergreifenden Prozessen bietet sich ebenfalls der Pseudonymisierungsansatz, erweitert um ein Identifier-Mapping, an. Jeder Teilnehmer im Netzwerk erhält dabei separate Mapping-Datenbanken mit den für ihn notwendigen Informationen, was die Sicherheit zusätzlich erhöht. Obwohl die Speicherung ausschließlich gehashter Ereignisprotokolle in der Blockkette sicherer wäre, würde dieser Ansatz einen redundanten Austausch der nicht gehashten Daten erfordern und die Verwendung der Blockchain auf eine einfache Validierung beschränken.

Datensicherheit

Neben dem Schutz personenbezogener Daten im Bereich Data Privacy sind unterschiedliche Sicherheitsaspekte seit jeher ein Kernelement der Blockchain-Technologie. In der untersuchten Literatur bearbeiten viele Autoren das Thema Sicherheit in einer sehr oberflächlichen und unkonkreten Art und Weise. Sie sprechen beispielsweise von „security mechanisms“ (Ølnes und Jansen, 2018) der Blockchain-Technologie, der Notwendigkeit von Sicherheitsproblemen bei der Entwicklung von Smart Contracts (Lu et al., 2019), einem unspezifischen „security layer“ (Lima, 2018) oder ganz allgemein über die Sicherheit der Blockchain-Technologie (Balani, 2020; Homoliak et al., 2019; Jacobs, 2016; Korpela et al., 2017; López und Farooq, 2020; Tang et al., 2019). Insbesondere in den jüngeren Forschungsarbeiten nehmen jedoch die konkreten Umsetzungen technischer Sicherheit von Blockchain-Anwendungen zu. Song et al.

(2021) untersuchen beispielsweise unterschiedliche Architekturen von Blockchain-as-a-Service (kurz BaaS) und identifizieren dabei Schichten und Prozesse zur Sicherheitsüberwachung. Kon-kret schlagen sie definierte Services vor, um die Sicherheit der Anwendungen zu erhöhen (Song et al., 2021). Auch Belchior et al. (2020) sehen für ihre Anwendung Sicherheitsaspekte als kritisch und stellen ihre Mechanismen zur Einhaltung der Sicherheitsmerkmale Konsistenz, Integrität und Zuverlässigkeit vor.

Zertifikate

In der gängigen Literatur zu Blockchain-Anwendungen werden Zertifikate in unserem Verständnis bisher kaum thematisiert. Publikationen nutzen die Blockchain eher zur Verwaltung und zur Generierung von Zertifikaten, bieten jedoch keine Konzepte zur Zertifizierung von Komponenten auf der Plattform.

2 Anforderungen aus dem Pflichtenheft

Im Rahmen der Anforderungsanalyse wurden im Pflichtenheft der Kollaborationsplattform (QQQ) verschiedene Anforderungen festgehalten, welche Einfluss auf Datenschutz und -sicherheit sowie Zertifikate haben:

Datenschutz

REQ14: Es dürfen keine personenbezogenen Daten sowie die Prüfsummen von diesen personenbezogenen Daten auf der Blockchain gespeichert werden.
Je nach Anwendungsfall kann auch eine Speicherung von personenbezogenen Daten auf der Blockchain notwendig sein. Nach den Regeln der DSGVO wird die Blockchain jedoch nach dem Grundsatz „privacy by design“ grundsätzlich ohne personenbezogene Daten verwendet.
REQ15: Auf der Plattform muss ein mehrstufiges Rechtesystem für die Blockchain implementiert werden. Anhand dieses Rechtesystems werden die Lese- und Schreib-Rechte verschiedener Anwender festgelegt. Die Anzahl der Stufen sowie deren Abgrenzung muss durch eine weitere Evaluierung, mit den Anwendern, vorgenommen werden.
REQ16: Das implementierte Rechtesystem muss die Möglichkeit bieten, dass definierte Transaktionen sowie Daten nur für bestimmte Plattformteilnehmer sichtbar sind.
REQ17: Die Kollaborationsplattform muss staatlichen Organisationen in Verdachtsfällen, zur Betrugsüberprüfung Lesezugriff auf alle in der Blockchain gespeicherten Daten bieten.

Datensicherheit

REQ6: Es dürfen nur Datensätze auf der Blockchain gespeichert werden, die für die unmittelbare Rückverfolgbarkeit von Ergebnissen innerhalb von Wertschöpfungsnetzwerken notwendig sind. Die Definition der betroffenen Daten wird pro angewendetem Anwendungsszenario in Zusammenarbeit mit den zugehörigen Anwendern bestimmt.
REQ7: Daten, welche nicht auf der Blockchain gespeichert werden, sollen durch die Generierung von Prüfsummen auf Basis kryptografischer Hash-Funktionen auf ihre Unveränderlichkeit überprüft werden können. Die Speicherung der Prüfsumme erfolgt auf der Blockchain.
REQ8: Für die Speicherung von Daten außerhalb der Blockchain müssen dezentrale Cloud-Lösungen eingesetzt werden, welche eine permanente Verfügbarkeit der Daten für die Anwender ermöglichen. Für unternehmensinterne Daten können On-Premise-Lösungen genutzt werden.
Für Daten, welche nicht auf einem lokalen Datenspeichersystem abgelegt werden können, wird die Integration des InterPlanetary File System (IPFS) implementiert.
REQ9: Für die Speicherung von Daten außerhalb der Blockchain müssen dezentrale Cloud-Lösungen eingesetzt werden, welche den Datenschutzansprüchen der Anwender genügen. Die Ansprüche müssen individuell mit allen Anwendern abgeglichen werden.
Für Daten, welche nicht auf einem lokalen Datenspeichersystem abgelegt werden können, wird die Integration des InterPlanetary File System (IPFS) implementiert. Neben den genannten konkreten Anforderungen sind die Grundsätze ordentlicher Software-Architektur zu beachten, welche unter anderem die Aspekte Sicherheit der entwickelten Anwendung, Fehlerbehandlung und Server-Sicherheit berücksichtigen.

Zertifikate

REQ39: Auf der Kollaborationsplattform müssen Zertifizierungsstellen eingesetzt werden, welche die Überprüfung von Produkten, Produktchargen sowie eingesetzter Sensorik vornehmen.
REQ40: Zertifizierungsstellen können die Überprüfung von smart contracts und oracles, auf Basis von Zertifikaten, durchführen.

3 Zusammenfassung und Fazit

Basierend auf den Erkenntnissen aus Literatur und Praxis können daher folgende Anforderungen an Datenschutz, Datensicherheit und Zertifizierung zusammengefasst werden:

Datenschutz
Keine Speicherung von personenbezogenen Daten in einer Blockchain
Falls personenbezogene Daten verarbeitet werden müssen, soll eine private permissioned Blockchain mit Pseudonymisierung verwendet werden
Mehrstufiges Rechtesystem
Datensicherheit
Datensparsamkeit auch für nicht personenbezogene Daten.
Unveränderbarkeit von externen Daten sicherstellen
Externe Daten auf dezentralen Cloud-Lösungen ablegen
Externe Anbieter müssen die DS-GVO umsetzen
Anwendungssicherheit
Fehlerbehandlung
Server-Sicherheit
Zertifikate
Einbindung externer Zertifizierungsstellen
Zertifizierung von Produkten und Dienstleistungen der Plattform

Literaturverzeichnis

Balani, N. (2020). *Blockchain Reference Architecture*. Abgerufen 26. Februar 2020, von https://dzone.com/articles/blockchain-reference-architecture

Belchior, R., Correia, M., und Vasconcelos, A. (2020). *Towards Secure, Decentralized, and Automatic Audits With Blockchain*. *Twenty-Eigth European Conference on Information Systems (ECIS2020)*. Marrakesh, Morocco.

Homoliak, I., Venugopalan, S., Hum, Q., und Szalachowski, P. (2019). *The Security Reference Architecture for Blockchains: Towards a Standardized Model for Studying Vulnerabilities, Threats, and Defenses*. *2nd IEEE International Conference on Blockchain (2019)*, 390–397. Institute of Electrical and Electronics Engineers Inc.

Jacobs, M. (2016). *A Proposed Blockchain Reference Architecture*. Abgerufen 20. Juni 2020, von https://www.linkedin.com/pulse/proposed-blockchain-reference-architecture-mike-jacobs/

Kolb_JOSH, J., Kolb, J., und Winkelmann, A. (2020). *Ein erweitertes Privacy-Calculus-Modell für Anwendungen der Blockchain-Technologie*. *15th International Conference on Wirtschaftsinformatik (WI 2020)*, 1789–1801. Potsdam.

Lima, C. (2018). *DLT/Blockchain Architectures and Reference Frameworks - A System-of-System Model*. Abgerufen 20. Juni 2020, von IEEE Global Blockchain Summit (2018) website: https://blockchain.ieee.org/images/files/pdf/20180917-blockchain-architecture-and-reference-frameworks_-_c-lima.pdf

López, D., und Farooq, B. (2020). *A multi-layered blockchain framework for smart mobility data-markets*. Transportation Research Part C: Emerging Technologies, *111*, 588–615.

Lu, Q., Xu, X., Liu, Y., Weber, I., Zhu, L., und Zhang, W. (2019). *uBaaS: A unified blockchain as a service platform*. Future Generation Computer Systems, *101*, 564–575.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Ølnes, S., und Jansen, A. (2018). *Blockchain technology as infrastructure in public sector -An analytical framework*. *19th Annual International Conference on Digital Government Research (2018)*, 1–10. New York, New York, USA: Association for Computing Machinery.

Rieger, A., Lockl, J., Urbach, N., Guggenmos, F., und Fridgen, G. (2019). *Building a blockchain application that complies with the EU general data protection regulation*. MIS Quarterly Executive, *18*(4), 263–279.

Song, J., Zhang, P., Alkubati, M., Bao, Y., und Yu, G. (2021). *Research advances on blockchain-as-a-service: architectures, applications and challenges*. Digital Communications and Networks.

Tang, B., Kang, H., Fan, J., Li, Q., und Sandhu, R. (2019). *IoT passport: A blockchain-based trust framework for collaborative internet-of-things*. *24th ACM Symposium on Access Control Models and Technologies (2019)*, 83–92. New York, NY, USA: Association for Computing Machinery.

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., und Cleven, A. (2009). *Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process*. 17th European Conference on Information Systems, *9*, 2206–2217.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Lehrstuhl für BWL und Wirtschaftsinformatik
Prof. Dr. Axel Winkelmann
Sanderring 2
97070 Würzburg

Autoren und Ansprechpartner

Julian Kolb, M.Sc.

Wissenschaftlicher Mitarbeiter
julian.kolb@uni-wuerzburg.de
+49 931 31-86166

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 931 31-89640

– Inhaltsverzeichnis Arbeitspaket C –

Das Arbeitspaket (AP) C zielt auf die Konzeption der Kernkomponenten der Plattform ab. Neben der Ausgestaltung Blockchainarchitektur umfasst dies die Konzeption der Plattformarchitektur, die Kategorisierung betriebswirtschaftlicher Daten aus handelsüblichen Informationssystemen sowie die Erstellung von Smart Contracts und die Konzeption einer Complex-Event-Processing Architektur. Alle Aktivitäten des Arbeitspakets dienen der Adressierung der in AP B identifizierten Anforderungen Das AP C umfasst sechs Teilarbeitspakete:

C1 & C2 Konzeption Kollaborationsplattform und Anwendungsszenario. Diese Teilarbeitspakete (TAP) setzen sich mit den Grundkomponenten der anvisierten Plattformlösung auseinander. Dabei werden Daten-, Applikations-, Business-, und Anwenderschicht betrachtet und eine passende Blockchain-Lösung konzipiert.

C3 Klassifikation betriebswirtschaftlicher Daten. Das TAP C3 analysiert die Datenstrukturen der ERP-Systeme im hauseigenen ERP-Labor.

C4 Konzeption von Smart Contracts. Zur Automatisierung der Transaktionen auf der Plattform werden Smart Contrakts in Abstimmung mit den TAP C2 und C3 konzipiert.

C5 Konzeption der Architektur für Eventverarbeitung. Hierbei wird Bereitstellung von Plattformfunktionalitäten zur Echtzeitverarbeitung analysiert. Potentielle Datenquellen, Verarbeitungsmechanismen und Auswertungswerkzeuge werden eruiert.

C6 Proof of Concept. Abschließend dient die Erstellung eines Simulators als Proof of Concept der Überprüfung der Machbarkeit, Kompatibilityt und Anforderungskonformität der Plattformkomponenten.

C1 & C2: Konzeption Kollaborationsplattform und Anwendungsszenario

Aus der umfangreichen Anforderungsanalyse und den aktuellen Plattformkonzepten aus Forschung und Praxis wurde ein Konzept für die Plattformarchitektur entwickelt. Im folgenden Ergebnisbericht wird die Architektur vorgestellt. Mit einem Szenario, das mithilfe eines Partners aus dem Projektbeirat erarbeitet wurde, wird die Anwendbarkeit in der Praxis demonstriert.

1 Aufbau der Kollaborationsplattform

Die folgende Abbildung zeigt den generalisierten Aufbau einer Blockchain-basierten Kollaborationsplattform, welche von zwei verschiedenen Wertschöpfungsnetzwerken genutzt wird. Die Plattform ist angelehnt an die von Xu et al. (2019b, 283) beschriebene Plattform und wurde an die Anforderungen aus Ergebnisbericht 1 angepasst.
Die in Abbildung C1-2.1 dargestellte Kollaborationsplattform besteht aus drei verschiedenen Schichten (Anwender-, Logik-, und Daten-Schicht). Die Anwendung der Plattform auf ein Wertschöpfungsnetzwerk wird in der Abbildung C1-2.1 durch die zweite Schicht von oben beginnend sowie die zugehörige Darstellung der Knoten der Unternehmen in der ersten Schicht dargestellt. Die genannten Schichten werden im Folgenden kurz beschrieben und durch eine Implementierung von Hyperledger Fabric vorgenommen (REQ2).

Wertschöpfungsnetzwerk-Schicht

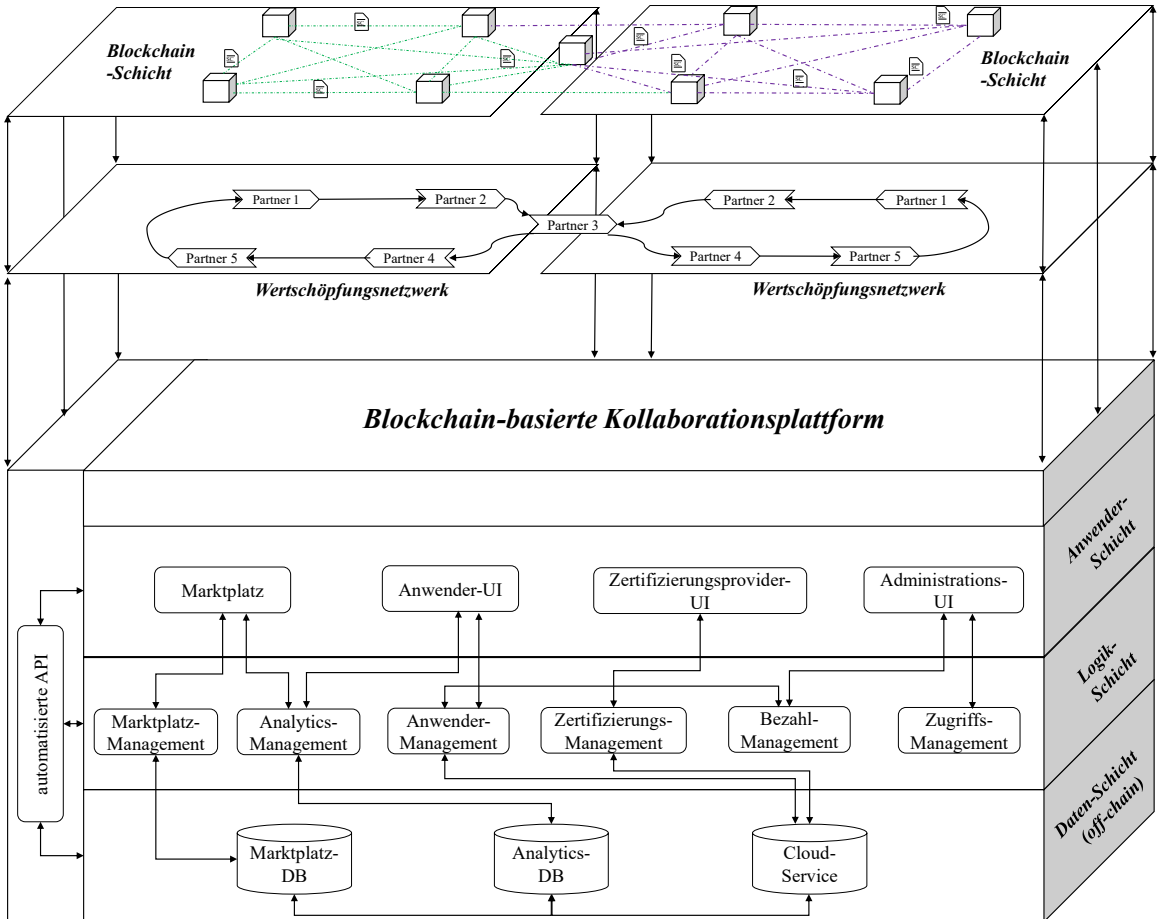
Die Wertschöpfungsnetzwerk-Schicht repräsentiert die Wertschöpfungsnetzwerke, welche die Kollaborationsplattform nutzen. Die Prozesse sowie dadurch anfallende Daten werden je nach Definition des Speicherungsortes entweder auf der Blockchain-Schicht oder anhand von manueller Eingabe durch die Anwenderschicht sowie durch eine automatisierte Eingabe auf der Kollaborationsplattform gespeichert.

Blockchain-Schicht

Jedes Wertschöpfungsnetzwerk, das die Kollaborationsplattform nutzt, besitzt neben der Wertschöpfungsnetzwerk-Schicht eine Blockchain-Schicht. In der Blockchain-Schicht wird ein Unternehmen durch einen Knoten dargestellt. Diese Blockchain-Schicht wird mittels einer Konsortial-Blockchain umgesetzt (REQ1). Die Blockchain-Schicht enthält ein mehrstufiges Rechtesystem, welches die Lese- und Schreibe-Rechte der Anwender einschränkt (REQ15). Wie in Abbildung C1-2.1 zu sehen, sind definierte Transaktionen (grün und lila dargestellt) nur für bestimmte Anwender sichtbar (REQ16). Zusätzlich dürfen keine personenbezogenen Daten oder deren Prüfsummen auf der Blockchain-Schicht gespeichert werden (REQ14). Staatliche Organisationen erhalten durch die Dienstleistungs-Provider ebenfalls Lesezugriff auf die dort gespeicherten Daten zur Überprüfung von z.B. betrügerischen Handlungen (REQ17). Die Umsetzung erfolgt ebenfalls durch eine separate Anwender-Schnittstelle.

Automatisierte API

Diese Schnittstelle dient zum automatisierten Datenaustausch zwischen den Unternehmen im



AbbildungC1-2.1: Darstellung der konzeptionierten Kollaborationsplattform

Wertschöpfungsnetzwerk und der Blockchain-Schicht sowie für den automatisierten Datenaustausch zwischen Daten, welche auf der Kollaborationsplattform, aber nicht auf der Blockchain-Schicht gespeichert werden sollen. Die Speicherung & Verteilung der Anwender-Daten auf die Blockchain erfolgt über die Kollaborationsplattform hinweg. Der Datenaustausch zwischen ERP-Systemen verschiedener Unternehmen über die Blockchain erfolgt anhand eines gemeinsam festgelegten Daten-Formats (REQ10). Dieses Datenformat wird von allen Anwendern adaptiert und implementiert (REQ11). Für den Datenaustausch zwischen Produktionsanlagen und der Blockchain-Schicht unterstützt die Plattform den OPC-UA-Standard (REQ13). Als Dateiformate müssen Sensordaten im JSON oder XML-Format in die Blockchain eingelesen werden (REQ12). Die oben genannten Requirements werden durch die ACTIWARE Plattform und Processengine erfüllt. Hier ist es möglich, unterschiedliche ERP Systeme sowie Drittanwendungen anzubinden. Ebenso ist die Ansteuerung durch Schnittstellen, beispielsweise REST, möglich. Prozessoren für die Verarbeitung von JSON und XML Files stehen hier ebenso zur Verfügung wie die Anbindung mittels OPC-UA Standard. Das von der ACTIWARE verfolgte Objektmodell wurde hierzu für die verschiedenen Anwendungsfälle aus dem PiMKoWe-Projekt angepasst.

Anwender-Schicht

Die Anwender-Schicht dient als Schnittstelle, die erhobenen Rollen in die Plattform einbinden zu können. Die Abbildung zeigt eine generalisierte Darstellung der verschiedenen Schnittstellen. Zum einen besitzt jede Rolle durch eine Schnittstelle die Möglichkeit auf die Plattform zugreifen zu können, zum anderen wird ein Marktplatzmodul der Plattform zur Verfügung gestellt, welches einen Einkauf von Leistungen durch die Anwender ermöglicht (REQ32). Diese Schnittstelle sowie die weiter beschriebenen Schnittstellen werden durch die Beschreibungssprache HTML umgesetzt, um verschiedenen Anwendungsgeräten wie PC, Smartphone oder Tablet einen Zugriff zu ermöglichen (REQ41), sind zu mindestens 99 Prozent verfügbar (REQ42) und haben ebenso eine maximale Abfragedauer von zehn Sekunden bzw. internationalen Abfragen von zwei Minuten (REQ43). Die verschiedenen Schnittstellen beinhalten Handlungsempfehlungen für verschiedene Rollen wie für die Verwaltung von ausgehändigten Public/Private-Schlüsselpaaren für die Anwender (REQ21) sowie interaktive Schulungen für die verschiedenen Rollen zu der Blockchain-Thematik (REQ45). Um den unterschiedlichen Nutzern den Zugriff auf die Blockchain zu ermöglichen, wurde im Rahmen des Projektes ein Formulargenerator entwickelt, der es ermöglicht, Daten anzuzeigen und auch verändern zu können. Damit wird die Interaktion zwischen Anwender und der Kollaborationsplattform ermöglicht. Durch Umsetzung als webfähige Komponente ist dabei die Darstellung auf unterschiedlichen Endgeräten langfristig gegeben.

Logik-Schicht

Die Logik-Schicht bildet alle notwendigen Logiken für die Verwaltung der Plattform ab. Das Marktplatz-Management verwaltet alle notwendigen Komponenten für das Marktplatz-Modul, auf das die Anwender sowie Dienstleistungs-Provider zugreifen können. Das Modul Analytics-Management beinhaltet die Verwaltung von Applikationen, welche auf Grund von erhöhtem Rechenaufwand nicht auf der Blockchain-Schicht durch Smart Contracts umgesetzt, sondern in Verbindung mit der Daten-Schicht (off-chain) durch Dienstleistungs-Provider auf der Plattform verschiedenen Anwendern zur Verfügung gestellt werden. Das Anwender-Management dient der Verwaltung von Anwenderdaten sowie Verarbeitung. Das Zertifizierungsmanagement verwaltet die durch die Zertifizierungs-Provider generierten Zertifikate für die Wertschöpfungsprozesse. Das Bezahl-Management wird genutzt, um zum einen automatischen monetären Austausch durch Smart Contracts und zum anderen die Bezahlung von Dienstleistungen innerhalb des Marktplatz-Moduls zu ermöglichen. Das Zugriffs-Management wird von den Dienstleistungs-Providern genutzt, um neue oder bestehende Anwender auf der Plattform zu verwalten.
Die Logik umzusetzender Smart Contracts wird in der Plattform von ACTIWARE durch zu modellierende Prozesse ermöglicht. Der Vorteil dieser Umsetzung besteht darin, damit die Generierung von Smart Contracts auf Low- bzw. No Code Basis umzusetzen. Im Rahmen des Projektes wurde ein Modul zum Schreiben und Lesen auf der Hyperledger Fabric entwickelt, das sich auch auf andere Blockchain-Netzwerke anpassen lässt Dadurch, dass Prozesse, die zusammen mit den bereits angesprochenen Formularen Bestandteil von Projekten in der Plattform sind, durch Export der Projekte kopier- und damit reproduzierbar sind, ist ein Austausch der modellierten Bedingungen für die Smart Contracts möglich. Diese können wiederum als Templates für neue Smart Contracts dienen, womit eine Voraussetzung für das Handeln oder den Austausch von Smart-Contracts gegeben ist. Dadurch, dass die Plattform selbstdokumentierend ist, kann die Erstellung und mögliche Veränderung der Prozesse und der darauf aufbauenden Smart-Contracts lückenlos nachvollzogen werden.

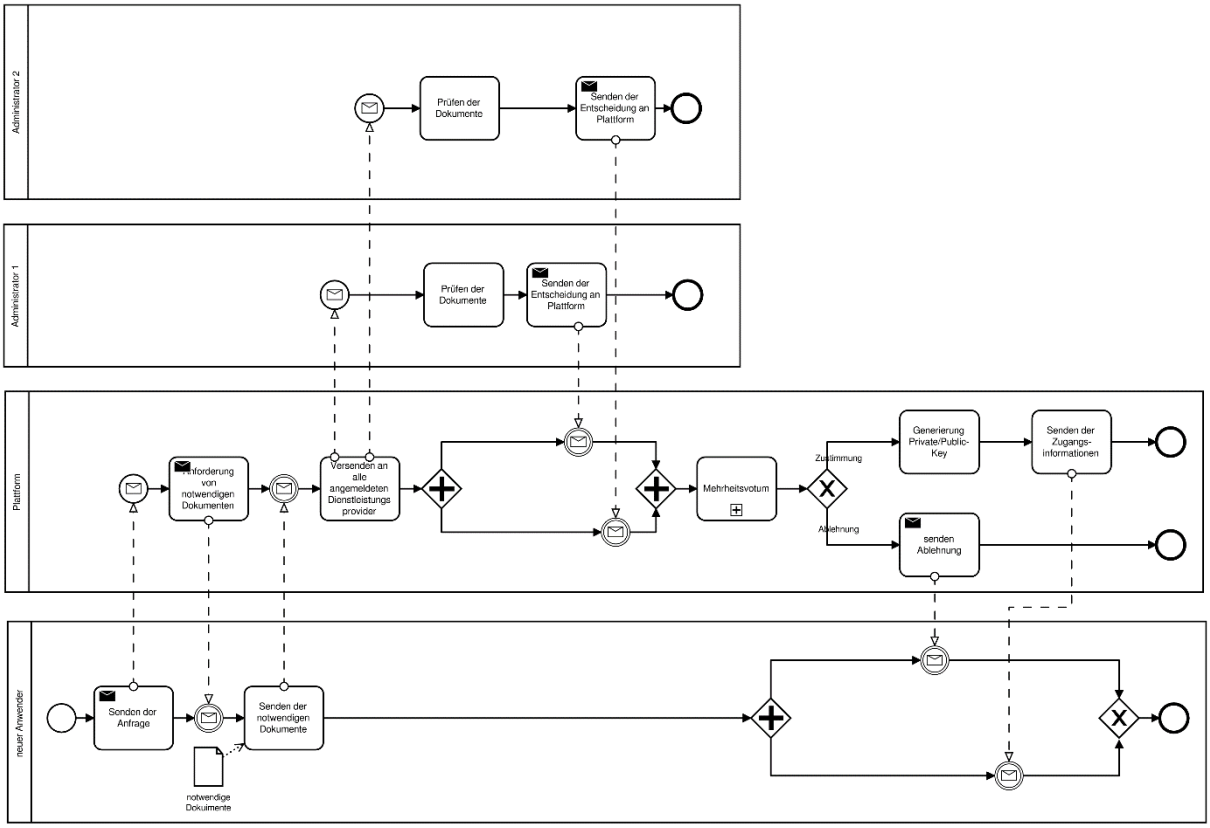


Abbildung C1-2.2: Prozessdarstellung der Zulassung auf der Kollaborationsplattform anhand BPMN 2.0.2

Daten-Schicht (off-chain)

Außerhalb der Blockchain werden Daten in drei verschiedenen Datenbanken auf der Kollaborationsplattform gespeichert. Die erste stellt die Marktplatz-Datenbank dar. Auf dieser werden alle notwendigen Informationen und Daten für den Betrieb des Marktplatzes gespeichert. Die zweite Datenbank ist die Analytics-Datenbank. Diese Datenbank beinhaltet große Datenmengen, welche z.B. zum Trainieren von verschiedenen maschinellen Lernverfahren notwendig sind. Die Cloud-Datenbank dient zum einen zum Speichern von Daten, welche nicht für die unmittelbare Rückverfolgbarkeit von Ergebnissen innerhalb der Wertschöpfungsnetzwerke relevant sind (REQ6). Zum anderen können auf dieser Datenbank Zertifikate zu Produktchargen, Produktionsprozessen oder Sensoren durch die Zertifizierungs-Provider gespeichert werden (REQ39). Die Kollaborationsplattform muss permanent verfügbar sein (REQ8) und allen Datenschutzansprüchen der Anwender genügen (REQ9). Zudem werden die Prüfsummen der auf der Cloud-Datenbank gespeicherten Daten auf der Blockchain zur Absicherung abgelegt (REQ7).
Im Rahmen des Projektes wurde die Anbindung einer SolR-Datenbank implementiert. Ebenso wurde der eigene io.storage so weiterentwickelt, dass dieser als nebenstehendes ECM die Möglichkeit zur Ablage von Daten bietet. Der io.storage bietet die Möglichkeit automatischer Verknüpfungen zwischen Objekten, sodass insbesondere Fragestellungen zur Verfolgung in Lieferketten damit abgebildet werden können. In der Plattform ist die Anbindung unterschiedlicher File Provider für den Storage vorgesehen, sodass das externe Speichern gegeben ist. Auf die Entwicklung eines Blockchain-Moduls ist oben bereits eingegangen worden.

2 Prozessdarstellung innerhalb der Kollaborationsplattform

Die Zulassung eines neuen Anwenders auf der Plattform wird im BPMN-Schaubild (Abbildung C1-2.2) dargestellt[1]. Zur besseren Darstellung wird das Vorgehen mit zwei angemeldeten Dienstleistungs-

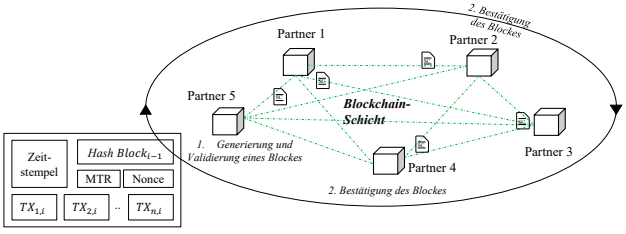


Abbildung C1-2.3: Vorgehen bei der Block -Generierung und – Validierung auf der Kollaborationsplatt-

[1] Das BPMN-Schaubild richtet sich nach der Syntax des BPMN-2.0.2-Standards. Die Spezifikation des Standards ist unter folgendem Link zu finden: www.omg.org/spec/BPMN/2.0.2/PDF (Stand: 24.08.2019).

Providern für die Zulassungsverwaltung dargestellt.
Wenn ein neuer Anwender Teil der Kollaborationsplattform werden will, muss er dies über die Administration der Plattform beantragen. Diese Administration wird von allen Dienstleistungs-Providern vorgenommen, welche für die Zugriffsrechte verantwortlich sind (REQ18). Die Plattform übernimmt die Anforderung aller relevanten Dokumente, damit alle Dienstleistungs-Provider den neuen Anwender nach dem „Know-Your-Customer"-Prinzip sowie nach Erfüllung von technischen Anforderungen für die Plattform überprüfen können (REQ20). Anhand eines Mehrheits-Votums, welches durch das Zulassungsmanagement verwaltet wird, wird über die Zulassung des Anwenders entschieden und der Anwender informiert (REQ19). Erhält der Anwender die Zulassung, wird zusätzlich durch das Modul ein Private/Public-Schlüsselpaar für diesen generiert. Eine Speicherung des Schlüsselpaares durch den Dienstleistungs-Provider darf nicht erfolgen. Staatliche Organisationen hingegen erhalten durch Dienstleistungs-Provider Lesezugriff auf die Plattform und können durch die bereitgestellte Schnittstelle alle gespeicherten Daten auf der Plattform lesen (REQ17). Die Umsetzung erfolgt durch eine separate Anwender-Schnittstelle.
Die Zugriffsverwaltung lässt sich aktuell über die Modellierung im Rahmen eines Prozesses umsetzen. Ebenso ist der Zugriff über Tokens in der Plattform implementiert. Perspektivisch ist eine Weiterentwicklung des User-Managements vorgesehen, so dass auch Externe auf einzelne Funktionalitäten der Plattform zugreifen können.
Der Ausschluss aus der Plattform erfolgt ebenfalls nach einem Mehrheitsprinzip. Sollte ein Anwender einen weiteren Anwender auf Grund von Fehlverhalten melden, müssen die Dienstleistungs-Provider diesen Sachverhalt prüfen und ähnlich wie bei der Zulassung durch ein Mehrheits-Votum dem Vorgang zustimmen oder ihn ablehnen. Sollte die Entscheidung fallen, dass ein Anwender ausgeschlossen wird, muss sein Schlüsselpaar ungültig gemacht sowie die Zugangsrechte zu der übrigen Infrastruktur der Plattform verwehrt werden.
Der Vorgang der Block-Generierung sowie -Validierung erfolgt anhand eines festgelegten Konsens-Algorithmus. An diesem Prozess müssen sich alle Anwender der Kollaborationsplattform beteiligen (REQ3). Forschungsbeiträge sowie die durchgeführte Interviewstudie zeigen verschiedene mögliche Konsens-Algorithmen. Für diese Kollaborationsplattform wird ein Konsens-Algorithmus gewählt, der eine gleichmäßige Verteilung der Generierung und Validierung von Blöcken ermöglicht. Je nach eingesetztem Verfahren können auch weitere Knoten in diesen Prozess involviert sein, um den validierten Block zu bestätigen. Ebenso erfolgt die Bestätigung der Validierung anhand eines gleichverteilten Verfahrens. Die Reihenfolge, wann welcher Knoten eine Generierung sowie Validierung vornimmt, wird durch die Blockchain-Schicht der Plattform verwaltet. Dieser Ansatz wird in Abbildung C1-2.3 dargestellt.
Im ersten Schritt fasst ein Knoten eines Unternehmens alle entstandenen Transaktionen, welche noch nicht einem zuvor generierten Block zugeordnet wurden, zusammen und generiert auf deren Basis einen neuen Block. Alle Inhalte sowie der Block werden validiert. Anschließend wird der Block an weitere Knoten zur Bestätigung weitergeleitet. Die Anzahl der notwendigen zu bestätigenden Blöcke sowie zusätzliche Rahmenbedingungen werden durch die Wahl des Konsens-Algorithmus festgelegt. In Anlehnung an Kapitel 2.3 sowie der interviewten Person *G* kann der pBFT genutzt werden, welcher eine Zweidrittel-Mehrheit bei der Anzahl aller Bestätigungen (B) aller Knoten (n) voraussetzt ($B \geq \frac{2n}{3}$).
Die Eingabe auf der Plattform erfolgt anhand verschiedener Schnittstellen, welche im vorherigen Kapitel beschrieben sind. Diese manuellen Eingaben werden getätigt, um Informationen, welche nicht durch die automatisierte API der Plattform in die Blockchain geschrieben werden können, zu speichern. Diese sind Eingabe von externen Parteien wie Zertifizierungsstellen, welche Produkte, Produktchargen, eingesetzte Sensorik, Smart Contracts, Oracles sowie deren Quellen überprüfen und auf Basis der Überprüfung Zertifikate für die geprüften Objekte ausstellen (REQ31, REQ39 und REQ40). Diese Zertifikate werden durch manuelle Eingaben der Plattform hinzugefügt. Ähnlich erfolgt dies für die Zertifizierung von Smart Contracts oder Oracles (REQ40). Ebenso können Anwender, abhängig von dem eingesetzten Anwendungsszenario, manuelle Eingaben machen. Falscheingaben durch solche Rollen können durch die unwiderrufliche Speicherung der Blockchain nicht rückgängig gemacht werden. Daher werden alle manuellen Eingaben durch eine automatische Plausibilitätsprüfung validiert (REQ44).
Anhand einer Suchfunktion sollen die Anwender gezielt nach Leistungen innerhalb des Marktplatz-Moduls suchen können (REQ33). Als Leistung können dies branchenspezifische Smart Contracts (REQ34), Analyseverfahren oder die Übernahme von Verpflichtungen wie die Validierung der Blöcke innerhalb der Blockchain-Schicht in Form einer Dienstleistung an die Dienstleistungs-Provider (REQ5) sein. Dieser Marktplatz bietet somit einen digitalen und automatisierten Einkauf und Verwaltung von Dienstleistungen an. Sollten weitere individuelle Abstimmungen zwischen den Anwendern und den Dienstleistungs-Providern notwendig

sein, kann dies über eine Kommunikationsschnittstelle zwischen den betroffenen Parteien innerhalb des Marktplatz-Moduls erfolgen (REQ35).
Durch die oben beschriebene Templatisierung von Prozessen ist die Handelbarkeit von Smart Contract Entwürfen bereits gegeben. Die Darstellung in einem Shop mit möglicher Durchsuchbarkeit befindet sich in der Konzeption.
Das Bezahl-Management wird zum einen durch Administratoren verwaltet, welche einen Austausch von Währungen wie Euro und Dollar in eine Blockchain-basierte Token-Währung umwandeln. Anhand dieser Tokens können die verschiedenen Anwender auf der Kollaborationsplattform die automatische Bezahlung durch Smart Contracts oder die Bezahlung der Dienstleistungs-Provider für Dienstleistungen vornehmen (REQ36). Umgewandelte Tokens können zu jedem Zeitpunkt wieder in die Währung Euro oder Dollar zurück umgewandelt werden (REQ37). Anhand dieses Umtauschs können Anwender und Dienstleister ihre monetären Werte außerhalb der Kollaborationsplattform nutzen. Das Bezahl-Management sowie die Administrations- sowie Anwender-Schnittstelle bieten entsprechende Eingabemasken an, um diesen Umtausch in Tokens und umgekehrt zu ermöglichen. Ebenso akzeptiert diese Logik die Verarbeitung von Banküberweisungen sowie Schecks zur Bezahlung auf dem Marktplatz-Modul (REQ38). Auch können Smart Contracts über das Bezahl-Management einen Anstoß von Banküberweisungen erzeugen.

3 Entwicklung und Nutzung von Dienstleistungen

Smart Contracts

Die Entwicklung von Smart Contracts wird durch Vorlagen unterstützt. Die Vorlagen müssen dabei den branchenspezifischen und regulatorischen Anforderungen der Wertschöpfungsnetzwerke entsprechen. So können bestehende Anforderungen und Standards auf die Kollaborationsplattform adaptiert werden (REQ26). Daher müssen pro aktive Branche auf der Blockchain entsprechende Vorlagen für Smart Contracts angeboten werden (REQ24). Ebenso muss verpflichtend für jeden Smart Contact ein zeitlicher Gültigkeitsbereich definiert werden (REQ29). Sollten für die Ausführung eines Smart Contracts Daten notwendig sein, welche nicht auf der Blockchain gespeichert sind, müssen diese Daten durch Oracles integriert werden. Nur zertifizierte Quellen dürfen für solche Oracles genutzt werden. Die Vorlagen sind durch Web-Schnittstellen für die Entwickler erreichbar (REQ27) und leiten den Entwickler durch Tipps und Anleitungen, welche interaktiv eingebettet sind, durch die Konfiguration der Smart Contracts (REQ24). Ebenso kann über grafische Modellierungswerkzeuge eine Gestaltung von Smart Contracts vorgenommen werden (REQ25). Abschließend wird der Smart Contract durch Darstellung des Quellcodes sowie eine Überführung in Pseudocode auch für nicht technische Anwender transparent dargestellt (REQ28). Die Entwicklung von Smart Contracts kann durch Dienstleistungs-Provider erfolgen oder durch Anwender selbst entwickelt werden, welche die branchenspezifischen Vorlagen, die durch das Marktplatz-Modul bereitgestellt werden, nutzen. Die Verwaltung bzw. Nutzung von Smart Contracts erfolgt anhand einer implementierten grafischen Darstellung. Diese beschreibt einen Überblick über alle Aktivitäten von Smart Contracts sowie deren Beziehungen zu weiteren Smart Contracts sowie Teilnehmern (REQ30).

Analyseverfahren

Durch die Implementierung des Marktplatz-Modules kann neben der Entwicklung von Smart Contracts auch die Entwicklung von weiteren Analyse-Verfahren vorgenommen werden. Der Einsatz solcher Analyse-Verfahren wie aus dem Bereich der Advanced Analytics und somit dem Einsatz von maschinellen Lernverfahren kann erhebliche Prozessverbesserungen innerhalb von Wertschöpfungsnetzwerken bewirken. Im Gegensatz zu Smart Contracts, welche redundant auf allen beteiligten Knoten der Blockchain-Schicht aktiv sind, sind solche Analyse-Verfahren deutlich rechenintensiver und würden bei der Ausführung alle Knoten mehr belasten als durch Smart Contracts (Wang et al. 2018a, 590ff.). Daher werden die durch Dienstleistungs-Provider entwickelten Analyse-Verfahren nicht in Form von Smart Contracts auf der Blockchain-Schicht gespeichert und ausgeführt, sondern durch ein separates Modul verwaltet. Zum einen dient hierfür das Analytics-Management-Modul aus der Logik-Schicht zur Verwaltung der Verfahren für die Anwender, welche durch ihre Schnittstellen darauf Zugriff haben. Zum anderen werden die notwendigen Daten für diese Verfahren permanent durch eine Analytics-Datenbank auf der Kollaborationsplattform abgelegt (Abbildung C1-2.1).

Block-Generierung und –Validierung

Wie zuvor beschrieben, wird die Generierung und Validierung der entstehenden Blöcke der Blockchain durch ein gerechtes Verfahren an die Anwender ausgelagert. Ebenso ist es möglich, im Zuge dieses Marktplatz-Moduls für den Anwender eine Dienstleistung einzukaufen, wodurch die Generierung und Validierung von Blöcken in dem eingesetzten Konsens-Algorithmus durch einen gewählten Dienstleistungs-Provider übernommen wird (REQ5).

4 Darstellung eines Anwendungsszenarios

Im Folgenden werden die zwei genannten möglichen Anwendungsszenarien von der befragten Person E aus Interview I4 der Interviewstudie auf Grund der inhaltlichen Nähe zu einem Szenario zusammengefasst. Das im folgenden gezeigte Anwendungsszenario wird durch die Darstellung des einhergehenden Wertschöpfungsnetzwerks präsentiert. In diesem Kontext wird die Verleihung von Transportboxen innerhalb eines internationalen Wertschöpfungsnetzwerkes dargestellt und die verschiedenen Bestandteile beschrieben. Dieses Wertschöpfungsnetzwerk ist für die Umsetzung in die Wertschöpfungsnetzwerk-Schicht aus Abbildung C1-2.1 einzubetten. Ebenso muss für alle Beteiligten ein Aufbau einer Blockchain-Schicht wie in Abbildung C1-2.1 erfolgen, da das vorgestellte Anwendungsszenario auf dem Konzept der Kooperationsplattform basiert. Sollte der Produzent mehrere Kunden haben, ist dieses Szenario auf mehrere Kunden multiplizierbar.

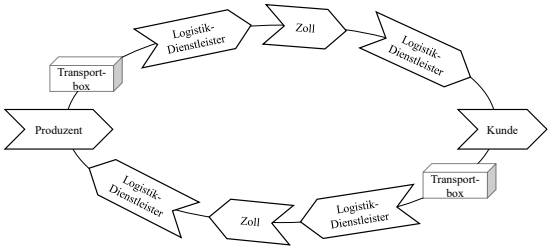


Abbildung C1-2.4: Darstellung des Wertschöpfungsnetzwerkes für das Anwendungsszenario

Im Folgenden werden die verschiedenen Anwender sowie deren Prozessvorgehensweisen sowie die Interaktion mit der Kollaborationsplattform dargestellt. Die Darstellung der Vorgänge erfolgt geordnet nach den einzelnen Anwendern.

Produzent

Der Produzent ist ein Hersteller für Isolierpanels und bietet neben der Produktion dieser Elemente auch als Dienstleistung an, gekühlte Transportboxen für Kunden zu verleihen. Durch die eingesetzten Isolierpanel in diesen Boxen können Kunden über einen Zeitraum von 100 Stunden nach der Auslieferung einen Transport von Waren in einem Kühlbereich zwischen 2 und 9 Grad Celsius durchführen. Innerhalb des Produzenten wird der Prozess der Bestückung dieser Boxen durch Sensorik überwacht, pro Box aggregiert und die Dateien auf der Cloud-Lösung der Plattform sowie deren Prüfsummen auf der Blockchain gespeichert. Durch diese Maßnahme soll der Zeitpunkt, wann und durch welche Kühlakkus die Boxen bestückt werden, für alle Teilnehmer des Wertschöpfungsnetzwerkes überprüfbar sein und ermöglichen dem Unternehmen somit eine rechtliche Absicherung bei Einhaltung der ausgestellten Zertifikate. Ebenso kann somit nachvollziehbar gemacht werden, wie diese Kühlakkus vorbereitet sowie in welcher Station die Kühlakkus gelagert wurden.

Transportbox

Die im Abschnitt des Produzenten genannte Transportbox stellt keinen Kooperationspartner innerhalb des Wertschöpfungsnetzwerk dar, ist jedoch das zu handelnde Gut in diesem Anwendungsfall und wird daher im Folgenden beschrieben. Innerhalb der Transportboxen sind nach I4 bereits verschiedene Sensoren zur Überwachung der Temperatur installiert. Durch die Integration von weiteren Modulen wie Erschütterungssensoren, GPS-Sensoren oder einem Funkmodul könnte jedes Ereignis, welches den Zustand der Ware oder der Transportbox ändern könnte sowie den zugehörigen Zeitpunkt und Standort der Box in festgelegten Intervallen aggregiert, auf der Blockchain gespeichert werden. Neben der Absicherung über einen korrekt durchgeführten Transport z.B. durch die genutzten Logistik-Dienstleister kann ebenso der Kunde mittels der Blockchain den Ort sowie die Beschaffenheit der Transportbox nachvollziehen.

Logistik-Dienstleister

Der Logistik-Dienstleister wird von dem Produzenten sowie dem Kunden beauftragt, die leere oder beladene Transportbox weiter zu versenden. Der Logistik-Dienstleister kann verschiedene Transportwege nutzen und speichert ebenso Vorkommnisse wie Frachtnummern oder Sensordaten über die korrekte Behandlung und Verladung der Transportbox auf der Blockchain ab. Dies kann als Rücksicherung des Logistik-Dienstleister gelten, dass alle notwendigen Maßnahmen und Anforderungen während der Auftragsabwicklung eingehalten wurden. Der Logistik-Dienstleister kann eine automatische Bezahlung durch den Einsatz von Tokens sowie Smart Contracts durchführen lassen. Wird eine Transportbox durch einen Dienstleister an den Zielstandort transportiert, kann dies bei Einhaltung aller gegebenen Anforderungen eine automatische Auslösung der Bezahlung in Form von Tokens des Produzenten oder des Kunden an den Dienstleistungs-Provider sein. Die Plattform ermöglicht ebenso die Entwicklung von Analyse-Anwendungen für Anwender durch Dienstleistungs-Provider. Ein Anwendungsfall kann die Implementierung von Advanced-Analytics-Verfahren wie LSTM zur Vorhersage von Lieferzeitpunkten der Transportboxen zur Routen-Kalkulation sein.

Zoll

Der Zoll stellt innerhalb dieses Wertschöpfungsnetzwerkes eine staatliche Institution dar, welche bei internationalem Handel für die Überprüfung der verschickten Waren zuständig ist sowie bei

Überschreitung von bestehenden Geldwerten Zollgebühren erhebt. Zum einen kann der Zoll somit an dem Wertschöpfungsprozess des Netzwerkes teilnehmen, indem er Überprüfungen der Transportboxen und Waren vornimmt und anschließend auf der Blockchain speichert. Die Speicherung erfolgt anhand der Prüfung von manuellen Eingaben auf der Plattform. Hier nutzen Mitarbeiter des Zolls die Anwender-Schnittstelle aus Abbildung C1-2.1. Die Entwicklung der personalisierten Schnittstelle erfolgt durch den Plattform-Provider in Zusammenhang mit dem Anwender und enthält Mechanismen, um Falscheingaben zu vermeiden. Ebenso kann durch den Einsatz von Tokens und Smart Contracts eine Automatisierung der Bezahlung von Zollgebühren gegenüber dem Produzenten sowie dem Kunden stattfinden. Hierdurch kann die Prozessabwicklung durch die Digitalisierung sowie Automatisierung verbessert und verkürzt werden.

Kunde

Der Kunde nutzt die Transportbox, um innerhalb von eigenen Wertschöpfungsnetzwerken Waren zu versenden. Dies können z.B. Lebensmittel sein, welche auf Grund von regulatorischen Auflagen durch die von dem Produzenten gemieteten Transportboxen und der damit einhergehenden Kühlung transportiert werden müssen. Durch die automatisierte Speicherung der Transportbox kann der Kunde gegenüber Kooperationspartnern aus anderen Wertschöpfungsnetzwerken belegen, dass der Transport der Ware nach den definierten Anforderungen erfolgt ist. Ähnlich wie bei dem Logistik-Dienstleister kann der Kunde das Marktplatzmodul nutzen, um z. B. Analyse-Anwendungen einzukaufen. Dies ermöglicht dem Kunden auf Basis der Temperaturwerte innerhalb der Transportbox, eine Vorhersage über die Produktqualität zu machen oder Lieferzeitpunkte vorherzusagen. Weitere Dienstleistungen können durch den Kunden sowie durch das Modul eingekauft werden.

Literaturverzeichnis

Xu, X.; Weber, I.; Staples, M. (2019b): Architecture for blockchain applications, Springer.

Wang, B.; Zhu, X.; He, Q.; Gu, G. (2018a): The forecast on the customers of the member point platform built on the blockchain technology by ARIMA and LSTM. In: 2018 the 3rd IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA 2018). IEEE. Chengdu. Institute of Electrical and Electronics Engineers. Piscataway, NJ, 589–593.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION

actiware®
DEVELOPMENT

MAUL-THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Juniorprofessur für Information Management
Prof. Dr. Christian Janiesch
Stephanstraße 1
97070 Würzburg
https://www.wiwi.uni-wuerzburg.de/lehrstuhl/bwljp1/startseite/

Autoren und Ansprechpartner

Lukas-Valentin Herm, M.Sc.

Wissenschaftlicher Mitarbeiter
lukas-valentin.herm@uni-wuerzburg.de
+49 931 31-81730

Prof. Dr. Christian Janiesch

Juniorprofessur für Information Management
christian.janiesch@uni-wuerzburg.de
+49 931 31-84930

C3: Klassifikation betriebswirtschaftlicher Daten

Im folgenden Ergebnisbericht wird die Klassifikation von betriebswirtschaftlichen Informationen und notwendigen Daten für einen Blockchain-UseCase zur Rückverfolgung von Produkten beschrieben. Grundlage hierfür bilden herkömmliche State oft the Art Informationssysteme und bestehende Industriestandards, die von zahlreichen Unternehmen in der Praxis eingesetzt werden. Unterstützt wird zur Einordnung von technischen Informationen und Daten durch das weit verbreitete Supply Chain Referenzmodells SCOR, um eine Anwendung mehrerer heterogener Enterprise Systeme gewährleisten zu können.

1 Informationssysteme als Grundlage zur Rückverfolgung von Produkten

Unternehmen verschiedener Größen haben in der Vergangenheit zahlreiche Informationssysteme in Organisationen eingeführt, um Geschäftsprozesse in digitaler Form zu verwalten und hierdurch diverse Wettbewerbsvorteile zu erreichen (Clegg et al. 2013). Im Speziellen benötigen Unternehmen der food- und pharmazeutischen Industrie ein effizientes Leitsystem zur Visualisierung von Material- und Informationsflüssen in Produktions- und Logistikumgebung, um die Herkunft und Qualität von sensiblen Produkten in Lieferketten sicherzustellen. In der Praxis kommen hierbei klassische Systeme wie Enterprise Resource Planning (ERP) in unterschiedlichen Abteilungen wie Einkauf, Produktion oder Versand zum Einsatz, um diverse Unternehmens-, Prozess- und Produktdaten in einem zentralen Datenspeicher zu verwalten. Unternehmen dieser Branchen stehen in der besonderen Verantwortung, im Ernstfall nicht konforme Produkte schnellstmöglich identifizieren zu können, um die Gesundheit von Endkunden zu schützen und fehlerhafte Chargen schnellstmöglich zu identifizieren. Klassische ERP-Softwareanbieter haben für diese Aufgaben bereits ERP-Programme entwickelt, die eine Top-down oder Bottom-up-Chargen-Analyse ermöglichen, um relevante Lieferanten, Kunden, Produkte und Prozesse innerhalb der eigenen Systemgrenzen zu erfassen und verwalten zu können (Doller, 2013). Die Blockchaintechnologie stellt zukünftig in diesem industriellen Umfeld für Unternehmen daher eine erweiterte technische Möglichkeit dar, um sich in Logistik- und Informationsflüsse außerhalb der eigenen Unternehmensgrenzen in nicht vertrauenswürdigen Netzwerken stärker kollaborativ integrieren zu können (Rejeb et al., 2021). Die aktuellen Blockchain-Software-Lösungen werden in der Praxis von großen Softwareunternehmen wie IBM, Cisco und SAP pilotiert, die weiterführend verschiedene Mehrwerte einer ERP-Blockchain in Supply Chains bewerben (Wang et al. 2019, Hader et al., 2021). Um diese Aspekte tiefer zu untersuchen, wird im vorliegenden Ergebnisbericht ein SAP ERP System des Lehrstuhls zur Klassifizierung betriebswirtschaftlicher Daten verwendet, da dies dem höchstmöglichen Grad an Praxisnähe zum Aufbau einer Blockchain-Plattform widerspiegelt. Im Gegensatz zu siloartig organisierten Wertschöpfungsnetzwerken werden zukünftige Lieferanten- und Kundenbeziehungen vermehrt durch stärkere Integration von Informationssystemen verändert werden (Wang et al. 2019). Nach wie vor befindet sich die DLT-Technologie allerdings für viele Unternehmen einer Proof-of-Concept Phase, in der die Adaption und Integration in klassische Informationssysteme technisch komplex ist (Pytel et al. 2020). Ziel dieses Beitrages ist es daher, die Komplexität der Technologie zu reduzieren, um relevante betriebswirtschaftliche Daten in Anlehnung an bestehende Industriestandards aufzuzeigen (Mager et al. 2016). Weiterführend soll auf Basis mehrerer ERP Systeme ein META-ERP-Blockchain-Standard gebildet werden, der eine Rückverfolgung von Produkten in heterogenen IT-Landschaften erlaubt.

2 Einordnung von Enterprise Resource Planning Modulen und Daten in produzierenden Unternehmen

In den nachfolgenden Abschnitten werden zunächst grundlegende Kernprozesse eines Unternehmens beschrieben, bevor relevante Unternehmenssysteme, Module und Daten für die Rückverfolgung von Produkten eingeordnet werden.

2.1 Grundlagen zur Klassifizierung von Unternehmensdaten mittels SCOR

Das Supply Chain Council, eine amerikanische Nonprofit-Organisation von Unternehmen und Forschungsinstituten, hat im Jahr 1996 das SCOR Modell entwickelt, um Verbesserung für Wertschöpfungsketten erreichen. Das SCOR Modell hat sich im Laufe der Zeit weitgehend zum weltweit akzeptierten Standard für die Beschreibung von Prozessen in produzierenden Unternehmen durchsetzen können (Zhou et al., 2011), sodass dieser Beitrag darauf aufbauend das Modell als Grundlage zur Klassifizierung betriebswirtschaftlicher Daten verwendet (siehe Abbildung C.3.1).

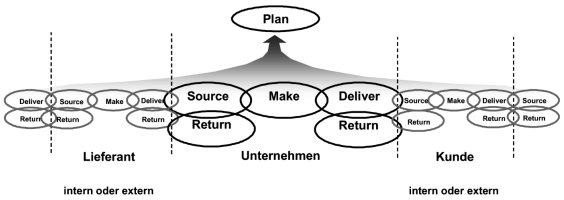


Abbildung C.3.1: Das SCOR-Modell beschreibt die Wertschöpfungskette vom Lieferanten des Lieferanten bis zum Kunden des Kunden (in Anlehnung an SCC, 2006).

2.2 SCOR Referenzmodell und Informationssysteme am Beispiel von SAP

Dieses Unterkapitel gliedert verschiedene Informationssysteme am Beispiel der Firma SAP in das SCOR Referenzmodell ein. Hierzu gehören Sys-

teme, die primäre und erweiterte Produktionsprozesse und Materialbewegungen unterstützen, wozu Systeme zur Planung von Lieferketten, ERP, Manufacturing Execution Systems und Warehouse Management Systems gehören. Um eine standardisierte Rückverfolgung von Produkten in Blockchain Applikationen zu ermöglichen, werden in diesen Systemen unterschiedliche betriebswirtschaftliche Wertschöpfungsprozesse abgebildet. Für die Auswahl eines End-to-End-Prozesses dient das SCOR-Modell aus Kapitel 2.1 nachfolgend als standardisiertes Supply Chain Framework, das eine Systemeinordnung in die Hauptschritte Plan (Planung), Source (Einkauf), Make (Produktion), Deliver (Versand) ermöglicht (Huan et al. 2004). Da in diesem Beitrag weiterführend Lagerbewegungen und Chargen zwischen diesen Schritten untersucht werden, sind in Tabelle C.3.1 weitere Ebenen zu der Klassifizierung hinzugefügt.

Tabelle C.3.1: Einordnung von ERP Modulen in das SCOR Referenzmodell

SCOR Prozess	Informationssysteme und Module
Plan	SAP APO - *Advanced Planning and Optimization*
Source	SAP ERP MM - Material Management
Make	SAP ERP PP - Production Planning SAP ME-System
Deliver	SAP ERP SD - Sales and Distribution
Lager	SAP ERP IM - Inventory Management Erweiterte Bestandsführung: SAP ERP WM – Warehouse Management
Chargen	Verteilt über mehrere Module

Die Tabelle C.3.1 zeigt auf, dass die Informationssysteme SAP APO, SAP ERP und SAP ME auf einfache Weise in das SCOR Modell eingeordnet werden können. Für die Rückverfolgung von Produkten liefern erweiterte Planungssysteme wie SAP APO allerdings keinen Mehrwert für Endkunden (Pytel et al. 2020), sodass dieses für das folgende Unterkapitel vernachlässigt wird. Darüber hinaus sind grundlegende Informationen über chargenrelevante Produktinformationen innerhalb des SAP ERP Systems verfügbar (siehe Folgekapitel), weshalb eine Analyse des SAP ME Systems zunächst nicht benötigt wird.

2.3 Klassifizierung von ERP Modulen, Datenbanktabellen und betriebswirtschaftlichen Daten

Traditionelle Informationssysteme enthalten verschiedene Module, denen sich konkrete Datenbanktabellen funktional zuordnen lassen. Die Speicherung von betriebswirtschaftlichen Daten erfolgt dabei in einzelnen Datenbankfeldern, die detailliert in frei zugänglichen Systemdokumentationen wie der LEANX-Tabellendokumentation[1] nachgeschlagen werden können. Das Informationssystem der SAP bietet damit einen hohen Grad an Transparenz, um die Struktur und den Aufbau zur Klassifizierung reproduzieren zu können.

Datenbanktabellen: Verschiedene Datenbanktabellen sind die Grundlage für Standardtransaktionen in den Bereichen Einkauf, Produktion und Versand. In diesem Ergebnisbericht werden gezielt Datenbanktabellen dargestellt, die in Anforderungen zum Aufbau zukünftiger Prototypen verwendet werden können (Pytel et al. 2020). Die folgende Klassifizierung unterteilt sich in relevante, optionale oder rein informative Datenbanktabellen, die im Fortschritt des Projektes zum Aufbau eines META-ERP-Blockchain-Standards relevant sein können. Darüber hinaus wird klassisch in Stamm- und Bewegungsdaten sowie spezifische Customizing Daten unterschieden, um die jeweiligen Tabellen in einer späteren Applikation gemäß geltender Industriestandards dokumentieren zu können (Pytel et al. 2020, Mager et al. 2016). Relevante Chargeninformationen sind in verschiedene Prozesse und SAP-Standardtabellen integriert. Für den Einkauf betrifft dies z.B. die Tabelle EBAN, EKKO und EKPO, für den Fertigungsbereich die Tabelle AUFM, für die Bestandsführung die Tabelle MSEG (Doller, 2013). Die Tabellen LIPS und LIKP enthalten zusätzlich Daten zu Lieferinformationen. Detaillierte Daten zu Herstellungs- und Verfallsdatum befinden sich in der Tabelle MSEG und MCH1. Bestandsdaten zu Chargen können der Tabelle MCHB entnommen werden. Die Tabellen KNA1 und LFA1 liefern umfangreiche Informationen über Kunden und Lieferanten. Alternativ bietet das weiterentwickelte S/4HANA-System ein anderes Modell zur Darstellung von Lieferanten und Kunden, sodass diese Informationen in Tabelle BUT000 vorgefunden werden können (Pytel et al. 2020). Als weitere Ergänzung sind auch Datenbanktabellen für die erweiterte Bestandsführung in Tabelle C.3.2 klassifiziert, da sie in zukünftigen Applikationen eine mögliche Ausbaustufe der Integration darstellen kön-

[1] http://leanx.eu/en/sap/table/search

nen. Die untenstehende Darstellung fasst die Ergebnisse dieses Kapitels nochmals in übersichtlicher Form zusammen.

Tabelle C.3.2: ERP Module, Datenbanktabellen (DBT), Datentyp (DT) und Relevanz

Modul	DBT	DT	Relevanz
MM	EKKO	Bewegungsdaten	Optional
	EKPO	Bewegungsdaten	Optional
	EBAN	Bewegungsdaten	Optional
	LFA1	Stammdaten	Optional
	ADRC	Stammdaten	Optional
	MCH1	Bewegungsdaten	Relevant
	MCHB	Bewegungsdaten	Optional
PP	MAST	Stammdaten	Optional
	STPO	Stammdaten	Optional
	MAKT	Stammdaten	Optional
	AUFK	Bewegungsdaten	Optional
	AFPO	Bewegungsdaten	Optional
	AFRU	Bewegungsdaten	Optional
	AFFW	Bewegungsdaten	Optional
	AFWI	Bewegungsdaten	Optional
	RESB	Bewegungsdaten	Optional
	AUFM	Bewegungsdaten	Optional
MM/SD	BUT000	Stammdaten	Optional
SD	LIPS	Bewegungsdaten	Optional
	LIKP	Bewegungsdaten	Optional
	KNA1	Stammdaten	Optional
IM	MSEG	Bewegungsdaten	Relevant
	MARD	Bewegungsdaten	Optional
Customizing ERP	T001L	Customizing Daten	Relevant
	T156	Customizing Daten	Relevant
Customizing WM	T300	Customizing Daten	Optional
	T301	Customizing Daten	Optional
	T302	Customizing Daten	Optional
WM	LAGP	Stammdaten	Optional
	LTAK	Bewegungsdaten	Optional
	LTAP	Bewegungsdaten	Optional
	LTBK	Bewegungsdaten	Optional
	LTBP	Bewegungsdaten	Optional

2.4 Überblick und Vergleich von Kernprozessen verschiedener ERP Systeme:

Zum Abschluss dieser Untersuchung sind weitere ERP Systeme des Lehrstuhls auf die Anwendbarkeit des SCOR Modells auf Lager-/Materialbewegungstabellen untersucht worden. Tabelle C.3.3: ERP Vergleich zeigt hierzu eine Gegenüberstellung mehrerer Prozessschritte, die exemplarisch aus freiverfügbaren Dokumentationen der ERP Systeme Microsoft Navision[2] und Weclapp ERP[3] entnommen wurden.

Tabelle C.3.3: ERP Vergleich

SCOR Prozess	ERP Systeme		
	Navision	SAP	Weclapp
Source	0 - Purchase	101 Goods Receipt (+)	IN_PURCHASE_ORDER
Make	6 Consumption (-)	261 Goods Issue Production (-)	IN_PRODUCTION_ORDER
	7 Output (+)	101 Goods Receipt (+)	OUT_PRODUCTION_ORDER
Deliver	1 Sale (-)	601Goods Issue to Customer (-)	OUT_SALES_ORDER (-)

Dieser einfache Vergleich zeigt, dass in weiteren Forschungsbemühungen eine Standardisierung von Kernprozessen eines ERP-Blockchain-Wertschöpfungsnetzwerkes notwendig ist, wenn ERP Systeme unterschiedlicher Hersteller in ein Blockchain Netzwerk integriert werden, um die Rückverfolgung von Produkten über eigene Unternehmens- und Systemgrenzen hinaus zu gestalten.

3 Fazit

Wie sich in dieser Untersuchung zeigte, ist in der Forschung und Praxis die Komplexität eines ERP Systems bis zu diesem Zeitpunkt nicht im Detail untersucht worden. Eine Klassifizierung von betriebswirtschaftlichen Daten muss für jedes ERP System und Blockchainprojekt individuell angefertigt werden, damit ein Standard zum Austausch von Produkt- und Prozessdaten über mehrere Organisationen hinweg gebildet werden kann (Pytel et al. 2020). Auch wenn bestehende Industriestandards wie die der GS1 eine Hilfestellung zum Aufbau eines Rückverfolgungssystems bieten,

[2]https://dynamicsdocs.com/nav/2016/w1/table/item-ledger-entry

[3]https://www.weclapp.com/api/#/warehouse-StockMovement

zeigt sich nach wie vor, dass es keine globale Perspektive auf Daten und Prozesse in unternehmensübergreifenden Lieferketten gibt (Sunyaev et al., 2021). Dieser Beitrag hilft damit zukünftigen Praktikern und Forschern bestehende Forschung fortzusetzen, um eine ERP-DLT-Integration für Anwendungsfälle im Supply Chain Bereich zu voranzutreiben.

Literaturverzeichnis

Clegg, B., MacBryde, J., Dey, P., and Powell, D. 2013. “ERP systems in lean production: new insights from a review of lean and ERP literature,” International Journal of Operations & Production Management ().

Rejeb, A., J. G. Keogh, S. J. Simske, T. Stafford and H. Treiblmaier (2021). “Potentials of blockchain technologies for supply chain collaboration: a conceptual framework” The International Journal of Logistics Management 32 (3), 973–994.

Doller, A. 2013. Chargenverwaltung mit SAP, SAP: Logistik. Rheinwerk Verlag GmbH.

Hader, M., A. El Mhamedi and A. Abouabdellah (2021). “Blockchain Integrated ERP for a Better Supply Chain Management”. In: 2021 The 8th International Conference on Industrial Engineering and Applications(Europe). New York, NY, USA: ACM, pp. 193–197

Huan, S. H., Sheoran, S. K., and Wang, G. 2004. “A review and analysis of supply chain operations reference (SCOR) model,” Supply Chain Management: An International Journal ().

Mager, L. et al. 2016. GS1 Global Traceability Compliance Criteria for Food - Application Standard, GS1 AISBL.

Pytel, Norman, Adrian Hofmann, and Axel Winkelmann. "Tracing Back the Value Stream with Colored Coins." (2020).

SCC (Supply-Chain Council) (Eds.) (2006): Supply-chain reference-model
SCOR Version 8. Pittsburgh: Supply-Chain Council. Weitere Angaben zum SCC: http://www.supply-chain.org

Sunyaev, Ali, et al. "Token economy." Business & Information Systems Engineering (2021): 1-22.

Wang, Y., Han, J. H., and Beynon-Davies, P. 2019. “Understanding blockchain technology for future supply chains: a systematic literature review and research agenda,” Supply Chain Management: An International Journal ().

Zhou, H., W. C. Benton, D. A. Schilling and G. W. Milligan (2011). “Supply Chain Integration and the SCOR Model” Journal of Business Logistics 32 (4), 332–344

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Lehrstuhl BWL und Wirtschaftinformatik
Prof. Dr. Axel Winkelmann
Sanderring 2
97070 Würzburg
https://www.wiwi.uni-wuerzburg.de/lehrstuhl/wiinf2/startseite/

Autoren und Ansprechpartner

Norman Pytel, M. Eng.

Wissenschaftlicher Mitarbeiter
norman.pytel@uni-wuerzburg.de
+49 931 31- 86348

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 931 31- 80501

C4: Konzeption von Smart Contracts

Smart Contracts ermöglichen es, abgesichert über die Blockchain Lieferketten regelbasiert zu automatisieren und nachvollziehbar zu gestalten. Im Rahmen des Projektes PimKoWe hat sich das Projektteam mit einer Vielzahl unterschiedlicher Konzepte im Bereich Smart Contracts beschäftigt und daraus eine Konzeption zur Umsetzung von Smart Contracts in Blockchain-Anwendungen entwickelt.

1 Smart Contracts in Blockchain-Anwendungen

Seit der Weiterentwicklung einfacher Blockchains hin zu intelligenten Systemen haben sich Smart Contracts zur dezentralen Ausführung von Code etabliert (Lu et al., 2019; Tonelli et al., 2018; Xu et al., 2016, 2017), wobei die Grundlagen bereits auf die Arbeiten von Szabo (1997) zurückgehen (Korpela et al., 2017; Szabo, 1997). Danach ist ein Smart Contract ein computerisiertes Transaktionsprotokoll, das die Bedingungen eines vorher festgelegten Vertrags ausführt. Die allgemeinen Ziele des Entwurfs von Smart Contracts sind die Erfüllung allgemeiner Vertragsbedingungen (z. B. Zahlungsbedingungen), die Minimierung von Ausnahmen (sowohl böswilligen als auch zufälligen) und den Bedarf an vertrauenswürdigen Vermittlern zu minimieren (Szabo, 1997). Obwohl ein Smart Contract als rechtlicher Vertrag wahrgenommen wird, kann er auch als willkürliches Programm verwendet werden, um Vereinbarungen und deren Auswirkungen zwischen Vertragspartnern zu übertragen (Hofmann et al., 2021).
Die genaue Rolle und Gestaltung von Smart Contracts ist jedoch noch nicht vollständig geklärt und erforscht (Hofmann et al., 2021). Einige Autoren sehen in Smart Contracts klassische Verträge oder Vereinbarungen (Korpela et al., 2017), manche vergleichen sie mit Mikroservices (Mishra und Sil, 2019; Tonelli et al., 2018) und Ramachandran und Krishnamachari stellen ihren Sinn und Zweck grundsätzlich in Frage (Ramachandran und Krishnamachari, 2019).
Zum besseren Verständnis über die Technologie und als konkreter Fahrplan zur Umsetzung von Smart Contracts wurden daher drei wissenschaftliche Publikationen erarbeitet, welche die wichtigsten Schritte zusammenfassen.

2 Building Scalable Blockchain Applications – A Decision Process

Hofmann, A., 2020. Building Scalable Blockchain Applications - A Decision Process. In Designing for Digital Transformation. Co-Creating Services with Citizens and Industry. Springer International Publishing

Eine große Herausforderung für viele Anwendungen ist die mangelnde Skalierbarkeit der zugrundeliegenden Architektur. Zwar gibt es verschiedene Technologien, die Lösungen für dieses Problem bieten, jedoch werden sie oft übersehen, wenn neue Anwendungen entwickelt werden. Um dieses Problem zu lösen, haben wir mit Hilfe eines Design-orientierten Forschungsansatzes einen Entscheidungsprozess entwickelt, der es Entwicklern ermöglicht, die richtigen Technologien zu wählen und die Skalierbarkeit ihrer Blockchain-Anwendungen zu gewährleisten. Das Ergebnis ist ein vierstufiger Prozess, der dabei hilft, die geeigneten Skalierbarkeitslösungen unter Berücksichtigung des geschäftlichen und technologischen Umfelds zu finden. Darüber hinaus bietet das entwickelte Framework einen Überblick über bestehende Lösungen und zeigt Lücken auf, in denen es noch keine Lösungen gibt, was einen Ausgangspunkt für weitere Forschung darstellt.

3 Building a Taxonomy for Gambling Smart Contracts

Kolb, J., Hofmann, A. & Becker, L., 2020. Building a Taxonomy for Gambling Smart Contracts. In 28th European Conference on Information Systems (ECIS). Marrakech, Morocco.

In den letzten Jahren ist die Blockchain-Technologie gereift und hat neue Möglichkeiten in der digitalen Welt geschaffen. Mit der Veröffentlichung der Blockchain 2.0, dem Ethereum-Netzwerk und intelligenten Verträgen ist es nun möglich, Anwendungen dezentral und unabhängig zu betreiben. Diese Anwendungen versprechen niedrigere Transaktionskosten, bessere Effizienz und höhere Sicherheit. Allerdings fehlt es bei der Vielzahl der neu entwickelten Smart Contracts noch an einem tiefgreifenden Verständnis und einer Standardisierung. Darüber hinaus gibt es noch keine geeignete Taxonomie, die die technischen Elemente eines Smart Contracts strukturiert und vergleichbar macht. Daher entwickeln wir eine Smart-Contract-Taxonomie mit Hilfe eines induktiven Forschungsansatzes. In Anlehnung an Nickerson et al. (2013) analysieren wir die Smart Contracts von 47 Glücksspiel-DApps und haben dabei 18 Dimensionen und 41 Merkmale für eine technische und codebasierte Taxonomie identifiziert.

4 A Source-Code-Based Taxonomy for Ethereum Smart Contracts

Hofmann, A., Kolb, J., Becker, L. & Winkelmann, A., 2021. A Source-Code-Based Taxonomy for Ethereum Smart Contracts. In ICIS 2021 Proceedings.

In der vorangegangenen Arbeit haben wir eine Taxonomie für Smart Contracts in einem spezifischen Umfeld geschaffen. Im nächsten Schritt werden diese Erkenntnisse nun erweitert und für allgemeine Smart Contracts verifiziert.
Da die Blockchain seit ihrem Aufkommen in der IS-Forschung viel Aufmerksamkeit erregt hat, ist sie durch die Entwicklung von Netzwerken und

Anwendungen für zahlreiche Industriezweige äußerst relevant geworden. Dennoch zeigen Beobachtungen, dass es nach wie vor an fundiertem Wissen und Standardisierung mangelt, insbesondere im Bereich der Blockchain-Anwendungen (DApps). Diese DApps bestehen oft aus mehreren intelligenten Verträgen, die zur Automatisierung verschiedener Prozesse verwendet werden und die technischen Elemente sind bisher noch nicht eingehend erforscht worden. In diesem Beitrag gehen wir dieses Problem an, indem wir eine datengestützte Taxonomie der technischen Elemente von 150 Smart Contracts in 101 DApps nach dem Ansatz von Nickerson et al. (2013) erstellen. Wir haben 28 Dimensionen und 64 Merkmale in unserer technischen und codebasierten Taxonomie identifiziert.

Literaturverzeichnis

Hofmann, A., Kolb, J., Becker, L., und Winkelmann, A. (2021). *A Source-Code-Based Taxonomy for Ethereum Smart Contracts*. *ICIS 2021 Proceedings*.

Korpela, K., Hallikas, J., und Dahlberg, T. (2017). *Digital Supply Chain Transformation toward Blockchain Integration*. Hawaii International Conference on System Sciences 2017 (HICSS-50).

Lu, Q., Xu, X., Liu, Y., Weber, I., Zhu, L., und Zhang, W. (2019). *uBaaS: A unified blockchain as a service platform*. Future Generation Computer Systems, *101*, 564–575.

Mishra, S., und Sil, S. (2019). *Blockchain Reference Architecture – A Smarter way to implement Agile and Effective Blockchain Solutions*.

Ramachandran, G. S., und Krishnamachari, B. (2019). *A Reference Architecture for Blockchain-based Peer-to-Peer IoT Applications*. Computer Science.

Szabo, N. (1997). *Formalizing and Securing Relationships on Public Networks*. First Monday, *2*(9).

Tonelli, R., Pinna, A., Baralla, G., und Ibba, S. (2018). *Ethereum smart contracts as blockchain-oriented microservices*. *19th International Conference on Agile Software Development: Companion (2018), Part F147763*, 1–2. New York, New York, USA: Association for Computing Machinery.

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., und Chen, S. (2016). *The blockchain as a software connector*. *13th Working IEEE/IFIP Conference on Software Architecture, WICSA 2016*, 182–191. Institute of Electrical and Electronics Engineers Inc.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., … Rimba, P. (2017). *A Taxonomy of Blockchain-Based Systems for Architecture Design*. *IEEE International Conference on Software Architecture, ICSA 2017*, 243–252. Institute of Electrical and Electronics Engineers Inc.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt "PIMKoWe"

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg
Lehrstuhl für BWL und Wirtschaftsinformatik
Prof. Dr. Axel Winkelmann
Sanderring 2
97070 Würzburg

Autoren und Ansprechpartner

Julian Kolb, M.Sc.
Wissenschaftlicher Mitarbeiter
julian.kolb@uni-wuerzburg.de
+49 931 31-80501

Adrian Hofmann, M.Sc.
Wissenschaftlicher Mitarbeiter
adrian.hofmann@uni-wuerzburg.de
+49 931 31-80501

Prof. Dr. Axel Winkelmann
Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 931 31-80501

C5: Konzeption der Architektur für Eventverarbeitung

Im folgenden Ergebnisbericht wird die theoretische Herleitung einer Echtzeiteventarchitektur für Blockchain-basierte Wertschöpfungsnetzwerke beschrieben. Grundlage hierfür bildet eine Referenzarchitektur für Blockchain-basierte Wertschöpfungsnetzwerke. Hierfür werden ebenso eine strukturierte Literaturanalyse sowie der Einzug bei der Anforderungsanalyse genutzt, um die Echtzeiteventarchitektur zu modifizieren und wissenschaftlich zu validieren.

1 Notwendigkeit der Überwachung von Wertschöpfungsnetzwerken

Durch die Globalisierung agieren Unternehmen auf einem internationalen Markt und können sich durch die Eingliederung in ein Wertschöpfungsnetzwerk auf Kernkompetenzen konzentrieren (Levitt 1993). Mit diesen Potentialen gehen jedoch auch Risiken einher. Durch den internationalen Wettbewerbermarkt entsteht ein enormer Konkurrenzdruck, welcher die Unternehmen zwingt, Kooperationen mit neuen und unbekannten Unternehmen einzugehen. Diese Notwendigkeit führt oftmals zu Vertrauensproblemen, da die Anwendung von illegalen Praktiken sowie Verletzung von vertraglichen Rahmenbedingungen durch komplexe und intransparente Wertschöpfungsnetzwerke befürchtet wird (Triepels et al. 2018). Die Blockchain-Technologie stellt ein transparentes, dezentrales und verteiltes Verfahren zur verketteten Speicherung von Daten dar und ermöglicht so ein Vertrauen in deren fälschungssichere Speicherung, selbst wenn kein Vertrauen in die Kooperationspartner besteht (Wu et al. 2016). Ebenso ermöglicht der Einsatz der Blockchain Prozesse innerhalb von Wertschöpfungsnetzwerken zu digitalisieren, zu automatisieren sowie in nahezu Echtzeit zu überwachen (Korpela et al. 20017).

Im Gegensatz zu einer Wertschöpfungskette wird diese bei der „digitalen supply chain“ (DSC) durch Integration und Vernetzung von Informationssystemen erweitert. Diese Erweiterung ermöglicht, die siloartige Datenhaltung verschiedener Unternehmen und Informationssysteme innerhalb einer Wertschöpfungskette zu überwinden. Das Ergebnis stellt ein transparentes und überwachbares Ökosystem dar. So ist eine DSC heutzutage nicht als Innovation, sondern als Notwendigkeit zu sehen, um im globalen Unternehmenskonkurrenzkampf zu bestehen (Korpela et al. 2017; Wu et al. 2016).

Grundannahme hierfür ist, dass durch das Internet der Dinge sowie mit Sensoren ausgestattete Produktionsanlagen alle Prozesse innerhalb eines Wertschöpfungsprozesses erfasst und verfolgt werden können und damit gravierende Veränderungen in allen Bereichen der Wertschöpfungsnetzwerken hervorrufen (Hoberg und Alicke 2016). So wäre eine einfache und kosteneffiziente Integration von neuen Dienstleistungen für alle Beteiligten der DSC auf Basis einer gemeinsamen Plattform zu integrieren möglich (Taifi und Passiante 2012). Nach Wu et al. (2016) zeichnen sich drei potenzielle Anwendungsfelder ab, welche durch den Einsatz einer DSC-Plattform entstehen. Diese sind Analyseverfahren (Advanced Analytics), Prozess Automatisierung und Integration und Innovationen in DSC. Durch den Einsatz von Advanced-Analytics-Verfahren kann die Produktivität der Unternehmen innerhalb einer Wertschöpfungskette verbessert werden. So kann ebenso durch Echtzeitanalysen und Vorhersagen-Methoden die Lagerverwaltung innerhalb von Distributions- und Produktionsprozessen angepasst und damit ressourcenschonender umgesetzt werden oder präventiv der wertschöpfungsnetzwerktypische Peitscheneffekt abgeschwächt werden (Waller und Fawcett 2013; Wu et al. 2016). Aktuelle Forschungsbeiträge demonstrieren diese Einsatzmöglichkeiten und damit Prozessverbesserungen anhand von verschiedenen Machine Learning-Ansätzen oder Echtzeitanalysen (Morariu und Borangiu; Lundberg 2006). Auch ist es möglich, durch Überwachung eine verbesserte und damit schnellere sowie effizientere Routenplanung von kritischen Transportprozessen zu ermöglichen (Hoberg und Alicke 2016).

Gleichzeitig können hieraus im Bereich der Integration und Innovationen innerhalb einer DSC durch deren Einsatz neuartige datenorientierte (Überwachungs)-Dienstleistungen für die Verwaltung innerhalb von Wertschöpfungsnetzwerken entstehen, welche als ein wichtiger Bestandteil innerhalb der kompetitiven Unternehmensführung zu sehen sind (Wu et al. 2016; Hoberg und Alicke 2016).

Bei genauerer Betrachtung zeigt sich, dass obwohl die durch die Echtzeitverarbeitung einhergehenden Potentiale einen disruptiven Charakter haben, die Umsetzung in der Praxis nur spärlich erfolgt. Dies kann unter anderem an der Neuigkeit beider Thematiken liegen, da insbesondere die Kombination beider Thematiken ein erhöhtes Schnittstellenwissen erfordert. Ziel dieses Beitrages ist es daher, eine Referenzarchitektur zu entwickeln, welche die Integration von (Echtzeit)-Datenverarbeitungen auf Blockchain-basierten Wortschöpfungsnetzwerken ermöglicht. Grundlage für diese Referenzarchitektur bildet eine im Zusammenhang mit dem Forschungsprojekt PIMKoWe entwickelte Referenzarchitektur für Blockchain-basierte Wertschöpfungsnetzwerke.

Der vorliegende Beitrag gliedert sich dabei wie folgt: Zuerst erfolgt die Herleitung und Darstellung einer Referenzarchitektur für Blockchain-basierte Wertschöpfungsnetzwerke nach Kolb (2022). Diese Referenzarchitektur wird anschließend auf den Anwendungsfall der Echtzeitverarbeitung angepasst und demonstriert. Abschließend folgt eine kompakte Zusammenfassung der Erkenntnisse.

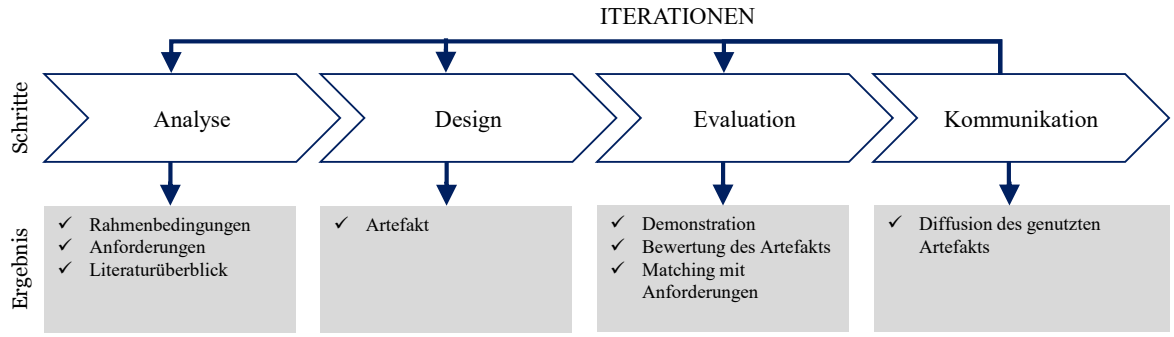


Abbildung C.5.1: Design-Science-Prozess nach Österle et al. (2011)

2 Darstellung Referenzarchitektur Echtzeitverarbeitung

2.1 Grundlagen Referenzarchitektur für Blockchain-Anwendungen in Wertschöpfungsnetzwerken

Während eine Vielzahl von Forschungs- und privatwirtschaftlichen Entwicklungsprojekten Erfahrungen im Umgang mit Blockchain-Technologie sammelt und Problemstellungen mit Hilfe prototypischer Softwarelösungen bearbeitet, bleibt die Definition klarer Standards bisher ungelöst. Nicht nur für Rieger (2019) ist der nächste wichtige Schritt für den weitverbreiteten Einsatz von Blockchain-Anwendungen die Etablierung von Standards und Referenzarchitekturen, die die Interoperabilität verschiedener Blockchain-Technologien und -Lösungen sicherstellen. Auch die International Organization for Standardisation (kurz ISO) verfolgt die Entwicklung einer Referenzarchitektur für Blockchain- und Distributed-Ledger-Technologie unter der ISO 23257 (ISO 2021). Im Rahmen dieser Arbeit wurde daher eine Referenzarchitektur für Blockchain-Anwendungen erarbeitet, welche als Grundlage für künftige Standardisierungsbemühungen in Wertschöpfungsnetzwerken dient.

Auf Grund des konstruktions- und gestaltungsorientierten Charakters einer Referenzarchitektur wird im Rahmen dieser Arbeit ein konstruktives Forschungsvorgehen verfolgt, da Referenzmodelle und -architekturen nach heutigem Verständnis gestaltungs- bzw. konstruktionsorientiert sind (siehe Abbildung C.5.1). Design Science Research (DSR) hat sich als gestaltungsorientiertes und praxisnahes Forschungsparadigma in vielen Projekten bewährt und bedient sich unterschiedlicher Methoden, um ein Problem mit Hilfe eines Artefakts zu lösen. In der Literatur haben sich dazu unterschiedliche Vorgehensmodelle entwickelt, wobei sich Österle et. al (2011) in der deutschen IS-Community etabliert haben. Sie unterteilen ein DSR-Projekt dabei in die Schritte Analyse, Design, Evaluation und Kommunikation. Um im Schritt „Design und Entwicklung“ des DSR-Projekts ein Artefakt zu konstruieren, sind weitere Methoden zur Gewinnung und Auswertung von Daten notwendig. Im Rahmen dieser Arbeit wird dabei zunächst auf bestehende Literatur zurückgegriffen, welche mit Hilfe einer strukturierten Literaturanalyse untersucht wird. Anschließend werden die Ergebnisse mit Hilfe einer qualitativen Querschnittsanalyse weiter geschärft und ihre praktische Relevanz überprüft.

2.2 Darstellung Referenzarchitektur

Nachdem die Ergebnisse der Literaturanalyse nach vom Brocke et. Al (2009) untersucht und durch weitere Experteninterviews bestätigt wurden, konnte in mehreren Iterationen eine Referenzarchitektur für Blockchain-Anwendungen aufgebaut werden (siehe Abbildung C.5.2). Dazu wurde zunächst die grobe Modellstruktur festgelegt und anschließend einzelne Komponenten in das Modell integriert. Dabei wurden die in der Literaturanalyse identifizierten Aspekte den jeweils passenden Schichten im Modell zugeordnet sowie bei Bedarf zusammengefasst, verändert oder extrahiert. Anschließend wurde die Referenzarchitektur durch Experteninterviews weiter geschärft und angepasst. Im Folgenden wird die Referenzarchitektur kurz vorgestellt:

Environment

Die Umweltfaktoren (engl. environment) einer Blockchain-Anwendung beziehen vor allem Stakeholder der jeweiligen Anwendung mit ein. Diese Stakeholder haben dabei meist Bedenken bzgl. Datenschutz und Datensicherheit. Zudem haben rechtliche Vorgaben und Regularien einen Einfluss auf die Gestaltung von Blockchain-Anwendungen.

Viele der untersuchten Publikationen beschäftigen sich mit dem Thema Vertrauen (engl. trust) im Um-

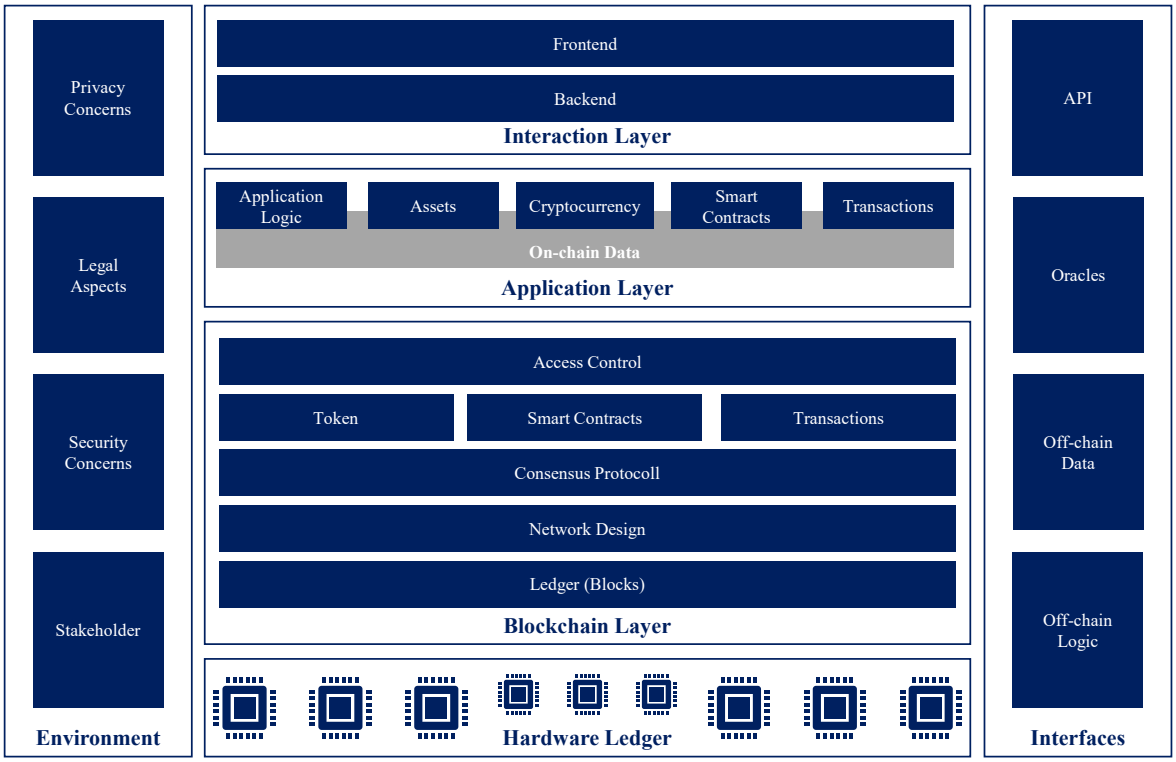


Abbildung C.5.2: Die Referenzarchitektur für Blockchain-Anwendungen in Wertschöpfungsnetzwerken nach Kolb (2022)

feld der Blockchain-Technologie. Bei näherer Analyse wird dabei jedoch meistens auf das übergeordnete Ziel der Blockchain-Technologie eingegangen, Vertrauen durch Dezentralität herzustellen. Als übergeordnetes Ziel hat Trust jedoch nur einen indirekten Einfluss auf die Gestaltung von Blockchain-Anwendungen und wird deshalb im vorliegenden Modell nicht weiter betrachtet.

Hardware Layer

Der Hardware Layer bildet die physische Grundlage einer Blockchain und umfasst alle integrierten Knoten in ihrer physischen Form (z.B. Server).

Blockchain Layer

Die in der Literaturanalyse dem Bereich Infrastruktur zugeordneten Aspekte werden im Blockchain Layer zusammengefasst. In dieser Schicht der Referenzarchitektur muss sich ein Entwickler mit Fragen rund um die technische Ausgestaltung der Blockchain in seiner Anwendung machen. Dabei spielt vor allem das Network Design eine zentrale Rolle, welches die Architektur des zugrundeliegenden Netzwerkes definiert und damit fundamentalen Einfluss auf die gesamte Anwendung hat. Zudem wird ein Konsensmechanismus festgelegt und die technische Ausgestaltung von Token, Smart Contracts und Transaktionen festgelegt. Über die Access Control wird anschließend die Verknüpfung zur Application Layer geregelt. In vielen Fällen kann die Blockchain Layer auch ausgelagert und als Blockchain-as-a-Service in die Anwendung integriert werden.

Application Layer

Im Bereich der Businesslogik wurden Smart Contracts, Transaktionen und Kryptowährungen unverändert als Komponenten übernommen und ihre organisatorische bzw. inhaltliche Ausprägung definiert. Zusammen mit den abgebildeten Gütern (engl. assets) und der grundlegenden Anwendungslogik wird hier das eigentliche Ziel einer Anwendung adressiert und dem User die notwendige Funktionalität bereitgestellt.

Interaction Layer

Im Bereich der Benutzerinteraktion werden in der Literatur vor allem Frontend und Backend unterschieden und daher in den Interaction Layer integriert.

Interfaces

Neben den Umwelteinflüssen sind insbesondere Schnittstellen für den Erfolg moderner Software-Anwendungen entscheidend. Gerade für Blockchain-Anwendungen, welche durch den Fokus auf unternehmensübergreifende Prozesse charakterisiert sind, ist eine Anbindung an bestehende IT-Systeme unerlässlich. Dabei wird vor allem zwischen APIs und Oracles unterschieden, welche sowohl die Nutzung externer Daten als auch externer

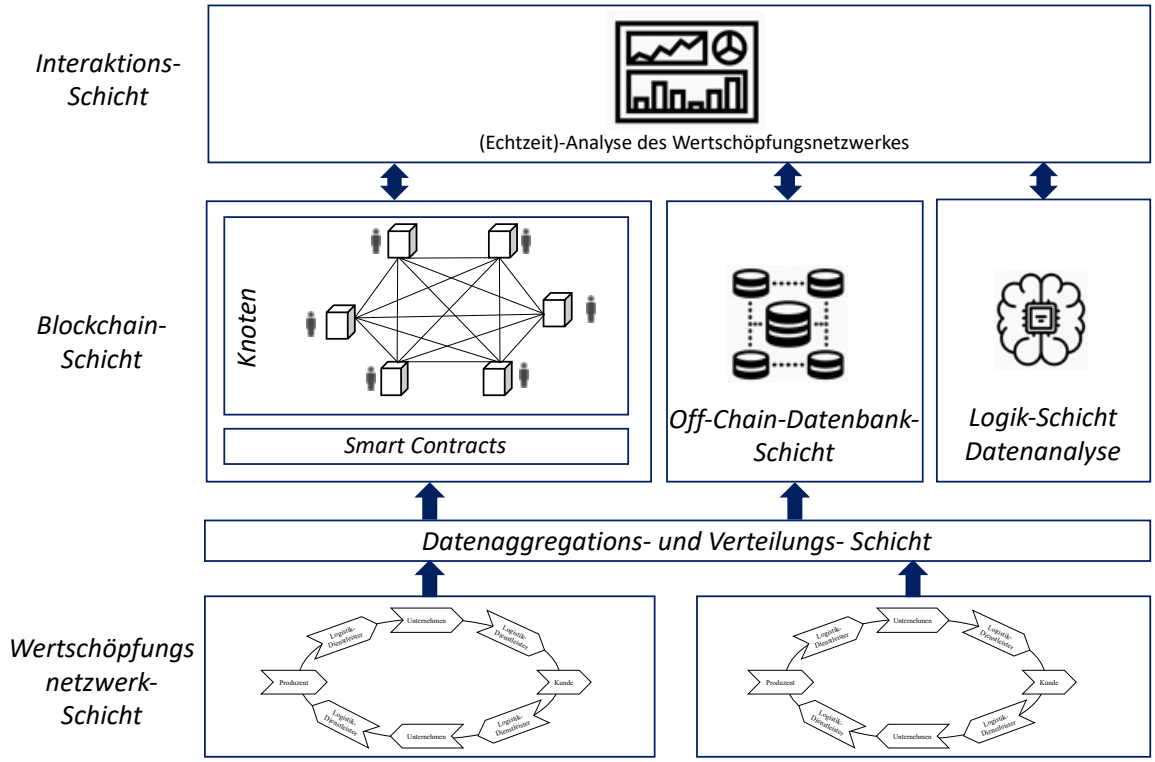


Abbildung C.5.3. Darstellung der Referenzarchitektur für (Echtzeit)-Verarbeitungen innerhalb eines Blockchain-basierten Wertschöpfungsnetzwerk

Programmlogik erlauben und so einen durchgehenden Datenfluss gewährleisten.

2.3 Darstellung Referenzarchitektur für eine Echzeitverarbeitung

In diesem Kapitel erfolgt die Darstellung der Referenzarchitektur für die Echtzeitverarbeitung (siehe Abbildung C.5.3). Grundlage bildet hierfür die in Kapitel 2.1 dargestellte Referenzarchitektur für Blockchain-basierte Wertschöpfungsnetzwerke. Die Ableitung der Komponenten der angepassten Referenzarchitektur erfolgt anhand einer strukturierten Literaturanalyse nach Vom Brocke et al. (2009). Ebenso werden diese Komponenten mit der Anforderungsanalyse für Blockchain-basierte Wertschöpfungsnetzwerke (Arbeitspaket B1-3) abgeglichen und ergänzt. Die entsprechenden Ergebnisse werden im Folgenden dargestellt:

Wertschöpfungsnetzwerks-Schicht

Innerhalb dieser Schicht wird das Wertschöpfungsnetzwerk zwischen den verschiedenen Partnern eines Netzwerkes abgebildet. Durch die Skalierbarkeit und kryptografischen Eigenschaften einer Blockchain (Swan 2016), können mehrere (überschneidende) Wertschöpfungsnetzwerke innerhalb einer Blockchainarchitektur abgebildet werden (Xu et al. 2019). Die innerhalb dieser Schicht anfallenden Daten werden kontinuierlich erfasst und an die Datenaggregations- und Verteilungsschicht gesendet. Ein Beispiel für anfallende Daten können Sensordaten sein, welche Zustände von Materialien innerhalb eines Wertschöpfungsprozesses erfassen.

Datenaggregations- und Verteilungs-Schicht

Innerhalb dieser Schicht werden die angefallenen Daten vorverarbeitet und anschließend an verschiedene Komponenten weitergeleitet. Die Datenvorverarbeitung muss je nach Anwendungsszenario mehrere Schritte umfassen. Diese Schritte ergeben sich aus den Eigenschaften aktueller Blockchainimplementierungen, da z.B. hochfrequente Sensorwerte nicht, auf Grund der eingeschränkten Skalierbarkeit von Transaktionsvalidierungen, unaggregiert gespeichert werden können (Xu et al. 2019). Eine Aggregation kann dabei eine Zusammenfassung gemeinsamer Sensorwerte sein, welche durch die Erstellung einer kryptografischen Hashfunktion fälschungssicher gemacht werden kann (REQ7). Ebenso muss in diesem Schritt eine Vorverarbeitung im Sinne der Datenschutzgrundverordnung (DSGVO) vorgenommen werden (REQ14). Aus diesem Grund muss die Verteilung an mehrere Schichten erfolgen.

Blockchain-Schicht

Die Blockchain-Schicht umfasst die eigentliche Implementierung einer konsortialen Blockchain-Lösung (REQ1). Innerhalb dieser Lösung werden die

verschiedenen Knoten, passend zu den Wertschöpfungspartnern innerhalb der Netzwerke, abgebildet. Durch die Nutzung von Smart Contracts erfolgt die Speicherung von Daten aus der Datenaggregations- und Validierungsschicht. Anhand der Durchführung der Anforderungsanalyse ergibt sich hierbei, dass auf eine Hyperledger-Fabric Implementierung zurückgegriffen werden muss, um verschiedene Wertschöpfungsnetzwerke anhand mehrerer Channels abbilden zu können (REQ2, 15).

Off-Chain-Datenbank-Schicht

Sollten innerhalb des Wertschöpfungsnetzwerkes Daten anfallen, welche nicht unaggregiert auf der Blockchain gespeichert werden können oder dürfen, muss eine Off-Chain-Datenbank genutzt werden. Dies betrifft aus einer technischen Perspektive die Speicherung von Sensordaten, aber auch aus einer rechtlichen Sicht die Speicherung von sensiblen Informationen, welche nicht unwiderruflich auf der Blockchain gespeichert werden dürfen (REQ6).

Datenanalyse-Logik-Schicht

In dieser Schicht wird die genutzte Logik für die datengetriebene Verarbeitung der Wertschöpfungsnetzwerke gespeichert. Dies kann bei der Anwendung von Echtzeitverarbeitungen die Speicherung von Filterregeln sein, welche genutzt werden, um Ereignisse effizient zu analysieren. Ebenso bietet dies die Möglichkeit für zukünftige Anwendungszwecke, weitere Logik im Bereich des (Online-) Machine-Learning zu integrieren (Morariu und Borangiu 2018). Die Speicherung erfolgt innerhalb einer Datenbank, welche durch den Administrator oder Anwender erweitert oder modifiziert werden kann.

Interaktions-Schicht

Die Interaktionsschicht dient dem Anwender, um die Ereignisse des Wertschöpfungsnetzwerkes zu analysieren. Hierbei nutzt dieser lokal eine (Web-) Anwendung, welche die Filterregeln aus der Datenanalyse-Schicht nutzt, um die anfallenden Daten aus der Blockchain-Schicht sowie der Off-Chain-Datenbank-Schicht zu verarbeiten. Die Verknüpfung der verschiedenen Schichten ermöglicht zusätzlich die Ergänzung um weitere Anwendungsmöglichkeiten der Echtzeitanalyse, wie der Überprüfung potenzieller Manipulation durch andere Wertschöpfungspartner.

3. Fazit

Wie sich zeigt, ist in der Forschung noch keine Referenzarchitektur für die Echtzeitverarbeitung von Blockchain-basierten Wertschöpfungsnetzwerken entworfen worden. In Anlehnung an der Referenzarchitektur für Blockchain-basierte Wertschöpfungsnetzwerke nach Kolb (2022), adressiert dieser Beitrag die Forschungslücke und ermöglicht damit die fundierte Erhebung einer Architektur für die Echtzeitverarbeitung. Gleichzeitig erlaubt die modulare und abstrakte Gestaltung dieser Architektur eine zukünftige Integration und Erweiterung weiterer Datenanalyseverfahren wie aus dem Bereich Machine-Learning. Diese theoretischen Vorarbeiten dienen als Grundlage für die Implementierung eines Anwendungsfalles in Arbeitspaket D4.

Literaturverzeichnis

Hoberg, K.; Alicke, K. (2016): How SC4. 0 will Enhance the Customer Experience. In: Supply Chain Management Review, 9 (10), 28–37.

Kolb, J. (2022): Erstellung einer Referenzarchitektur für Blockchain-Anwendungen in Wertschöpfungsnetzwerken. Dissertation an der Universität Würzburg.

Korpela, K.; Hallikas, J.; Dahlberg, T. (2017): Digital supply chain transformation toward blockchain integration. In: Proceedings of the 50th Hawaii International Conference on System Sciences (2017), 4182–4191.

Levitt, T. (1993): The globalization of markets. In: Harvard Business Review, 61 (3), 92–102.

Lundberg, A. (2006): Leverage complex event processing to improve operational performance. In: Business Intelligence Journal, 11 (1), 55–65.

Morariu, C.; Borangiu, T. (2018): Time series forecasting for dynamic scheduling of manufacturing processes. In: 2018 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR). IEEE. Cluj-Napoca, 1–6.

Swan, M. (2015): Blockchain: Blueprint for a new economy, O'Reilly Media, Inc.

Rieger, A., Lockl, J., Urbach, N., Guggenmos, F., und Fridgen, G. (2019). Building a blockchain application that complies with the EU general data protection regulation. MIS Quarterly Executive, 18(4), 263–279.

ISO. (2021). ISO - ISO/FDIS 23257 - Blockchain and distributed ledger technologies — Reference architecture. Abgerufen 18. Juli 2021, von https://www.iso.org/standard/75093.html

Taifi, N.; Passiante, G. (2012): Speeding up 'New Products and Service Development' through strategic community creation: case of automaker after-sales services partners. In: The Service Industries Journal, 32 (13), 2115–2127.

Triepels, R.; Daniels, H.; Feelders, A. (2018): Data-driven fraud detection in international shipping. In: Expert Systems with Applications, 99, 193–202.

Vom Brocke, J.; Simons, A.; Niehaves, B.; Riemer, K.; Plattfaut, R.; Cleven, A. (2009): Reconstructing the giant: on the importance of rigour in documenting the literature search process. In: ECIS 2009 Proceedings.

Waller, M. A.; Fawcett, S. E. (2013): Data Science, Predictive Analytics, and Big Data: A Revolution That Will Transform Supply Chain Design and Management. In: Journal of Business Logistics, 34 (2), 77–84.

Wu, L.; Yue, X.; Jin, A.; Yen, D. C. (2016): Smart supply chain management: a review and implications for future research. In: The international journal of logistics management, 27 (2), 395–417.

Xu, X.; Weber, I.; Staples, M. (2019): Architecture for blockchain applications, Springer.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Juniorprofessur für Information Management
Prof. Dr. Christian Janiesch
Sanderring 2
97070 Würzburg

https://www.wiwi.uni-wuerzburg.de/lehrstuhl/bwljp1/startseite/

Autoren und Ansprechpartner

Lukas-Valentin Herm, M.Sc.

Wissenschaftlicher Mitarbeiter
lukas-valentin.herm@uni-wuerzburg.de
+49 931 31-80501

Julian Kolb, M.Sc.

Wissenschaftlicher Mitarbeiter
julian.kolb@uni-wuerzburg.de
+49 931 31-80501

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 931 31-80501

Prof. Dr. Christian Janiesch

Juniorprofessur für Information Management
christian.janiesch@uni-wuerzburg.de
+49 931 31-84930

C6: Simulator als Proof of Concept

Essentiell für den Erfolg und Mehrwert der Blockchain-basierten Plattform sind neben einer konzeptionellen Entwicklung die Überprüfung der Machbarkeit, Kompatibilität und Anforderungskonformität der einzelnen Blockchain-basierten Plattformkomponenten. Um dies zu evaluieren, werden einzelne Komponenten im Rahmen von Simulations-Studien implementiert. Die daraus entstehenden Ergebnisse werden evaluiert und mit den Anforderungen des Lastenhefts abgeglichen. Anschließend wird die Kongruenz der Ergebnisse und Anforderungen festgestellt.

1 Blockchain als Lösungskomponente für eine dezentrale Plattformarchitektur

Die digitale Transformation ist ein fortlaufender Prozess, der Unternehmen dazu veranlasst, verschiedene innovative Technologien zur Bewältigung von Komplexität einzusetzen (Vial 2019). Die Blockchain-Technologie verspricht, eine verteilte Informationsweitergabe zu ermöglichen. Als eine aufstrebende Technologie hat sie das Potenzial, die Qualität der Lieferkette zu unterstützen. Die Eigenschaft der Unveränderlichkeit erzeugt eine unbekannte Form des digitalen Vertrauens zwischen den Teilnehmern, indem sie relevante Qualitätsinformationen in Bezug auf bestehende Industriestandards und -normen austauscht (Chen u. a. 2017).

Blockchain als aufstrebende Technologie erfordert Zeit und einen strukturierten Ansatz, um sie in komplexen Produktionsumgebungen zu etablieren. Mit dem Aufkommen von Informationssystemen implementieren Unternehmen ERP-Systeme (Enterprise Resource Planning), um Geschäftsanforderungen zu erfüllen, die Leistung globaler Wertschöpfungsketten zu verbessern und Kosten zu senken, indem sie Produktionsmanagement und -prozesse mit Hilfe von IT-Systemen unterstützen (Chorafas 2001). Inzwischen sind die IT-Landschaften immer komplexer und verteilter geworden. Sie erfordern ein spezifisches Domänen- und Prozesswissen, um sie effizient zu managen (Fleig, Augenstein, und Mädche 2018). Daher ist es wichtig, kritisch zu betrachten, wie die Blockchain-Technologie reale interorganisatorische Probleme lösen und einen Mehrwert für verteilte Produktionsunternehmen schaffen kann. Sie bietet zwar vielversprechende Umsetzungsmöglichkeiten, wird aber zu einer Neugestaltung isolierter industrieller Geschäftsprozesse und historisch gewachsener IT-Landschaften führen. Für Unternehmen bedeutet dies, ihr Innenleben zu analysieren und zu verändern und ihre Prozesse und Organisation an eine wettbewerbsfähigere Form anzupassen, so dass der Einsatz der Blockchain-Technologie den Faktor Mensch in den Geschäftsprozessen beeinflussen kann (Mendling u. a. 2018).

Ganzheitlich betrachtet steht und fällt der Bedarf und Einsatz der Blockchain-Technologie mit der Integration in bestehende IT-Landschaften, der Akzeptanz der Anwender und den lokalen rechtlichen Anforderungen. Traditionell benötigt die Einführung der Blockchain-Technologie in Geschäftsprozesse ein standardisiertes Betriebsmodell, um die Interoperabilität zwischen verschiedenen Teilnehmern und Informationssystemen sicherzustellen (Hastig und Sodhi 2020).

Diese Standards werden in der Praxis von führenden Dienstleistern wie IBM, Cisco oder SAP gebildet, so dass Unternehmen die Vorteile beobachten können, bevor sie in diese neuen Technologien investieren. Zusätzlich verlangen Kunden zunehmend Informationen über die Produktion, die logistischen Prozesse und die Quellen der Produkte. Aufgrund ihrer dezentralen Struktur kann die Blockchain-Technologie Produkte auch über komplexe Lieferketten hinweg verfolgen und nachverfolgen (Wang, Han, und Beynon-Davies 2019a). Wir sehen, dass die Begriffe "Tracking" und "Tracing" in diesem Zusammenhang zwei unterschiedliche Zielgruppen ansprechen. Während Kunden eine durchgängige Rückverfolgbarkeit und Nachhaltigkeit wünschen, verwenden Unternehmen diesen Begriff, um die Rückverfolgbarkeit zur Optimierung ihrer Lieferketten zu verfolgen (Mondal u. a. 2019; Tian 2016). In aktuellen Lösungen werden die digitalen Zwillinge von Produkten durch intelligente Verträge verwaltet, die von Dienstleistern wie IBM, Cisco und SAP pilotiert werden (Wang, Han, und Beynon-Davies 2019b). Wir haben jedoch festgestellt, dass diese intelligenten Verträge zunehmend komplexer werden, wenn die Lieferkette Produktionsschritte umfasst, bei denen Waren kombiniert werden, um ein neues, anderes Gut zu schaffen. Neben den intelligenten Verträgen haben wir ein oft übersehenes Konzept zur Darstellung von realen Vermögenswerten in der Blockchain identifiziert, die "Colored Coins“ (Anand u. a. 2017). Daher besteht unsere Motivation darin, die Komplexität der Technologie zu reduzieren, um sie für künftige Forscher und Praktiker verständlich und praktisch zu machen.

Um die Kompatibilität und Anforderungskonformität der verschiedenen Blockchain-basierten Plattformkomponenten zu bewerten, werden in diesem Teilarbeitspaket die Ergebnisse ausführlicher Simulationsstudien ausgewertet. Ziel ist es aufzuzeigen, wie genau Warenbewegungen und Produktionsprozesse von aktuellen ERP Systemen auf einer Wertschöpfungsnetzwerk Blockchain abgebildet werden können. Die Ergebnisse der Simulationsstudien zielen ebenfalls darauf ab, die Durchführbarkeit des Vorhabens zu belegen und beweisen den positiven technischen Machbarkeitsnachweis in Form von fertiggestellten Simulationsprototypen.

2 Rückverfolgung von Warenströmen in Wertschöpfungsnetzwerken

Eine Herausforderung für die Industrie besteht darin, Echtzeitdaten entlang einer Lieferkette zu erhalten (Heng 2014). Für Hersteller fasst Buer u. a. (2018) zahlreiche Studien aus der Vergangenheit zusammen, die RFID-Technologie zur Abbildung von Echtzeit-Wertströmen nutzen. Die Autoren stellen fest, dass es immer noch an Wissen über

die Umsetzung in einer schlanken Produktionsumgebung mangelt. Dennoch stellen Buer u. a. (2018) fest, dass es noch unklar ist, welche Praktiken und Technologien kombiniert werden können.

Ein effizientes Steuerungssystem zur Visualisierung des Material- und Informationsflusses wird in der Produktion und Logistik grundsätzlich benötigt, um die Herkunft und Qualität von End-to-End-Prozessen in Lieferketten zu überwachen. Dies ist vor allem für produzierte Chargen in der Lebensmittel- und Pharmaindustrie notwendig, da nicht konforme Produkte die Gesundheit der Kunden gefährden können. Zur Sicherstellung der Rückverfolgbarkeit in Lieferketten existieren anbieterspezifische ERP-Programme, die eine Top-down- oder Bottom-up-Chargenanalyse ermöglichen (Doller 2013). In diesem Fall liegt die Datenhoheit bei den Unternehmen und wird von deren Bedürfnissen bestimmt.

Um die unternehmensübergreifende Zusammenarbeit effizienter zu gestalten, kann die Blockchain-Technologie ein innovatives Instrument zur Neugestaltung isolierter Geschäftsprozesse bieten. Dies gilt insbesondere für Geschäftsumgebungen, in denen keine vertrauenswürdige und zentralisierte Partei die Rückverfolgbarkeit von Produkten über Organisations- und Informationssystemgren-zen hinweg koordinieren kann (Rejeb u. a. 2021). Die Unternehmen haben jedoch im Laufe der Jahrzehnte verschiedene Informationssysteme zur Verwaltung von Geschäftsprozessen in zentralen Datenspeichern eingeführt. Daher stellt die Kombination von traditionellen Informationssystemen und Blockchain-Technologie eine zusätzliche Möglichkeit zur Integration von Geschäft und Technologie dar. In der Praxis werben große Dienstleister dafür, Geschäftsbereiche wie Einkauf, Produktion, Lager oder Qualitätssicherung durch den Einsatz von ERP und Blockchain-Technologie zu verbinden, um weitere Prozessverbesserungspotenziale zu erzielen (Hader u. a. 2021; Sokolov und Kolosov 2021).

Der am weitesten verbreitete Ansatz zur Darstellung von realen Vermögenswerten auf Blockchains sind Token, die auf *Ethereum Request for Comments (ERC)* Standards basieren (Vogelsteller und Buterin 2015). Die am häufigsten verwendeten Token sind ERC20 für fungible Token und ERC721 für nicht-fungible Token (Fröwis, Fuc6.hs, und Böhme 2019). Während fungible Token Objekte repräsentieren, die beliebig austauschbar sind, wie z. B. Aktien, repräsentieren nicht-fungible Token eindeutig identifizierbare Objekte wie z. B. Immobilien (Vogelsteller und Buterin 2015). Nur nicht-fungible Token können verwendet werden, um Objekte entlang einer Lieferkette zu verfolgen. Sie eignen sich jedoch nicht für Produktionsprozesse, bei denen Güter kombiniert und in andere Güter umgewandelt werden. Dabei können die ursprünglichen Güter zerstört werden und es entsteht ein neues Gut. Daher müssen alte Token zerstört und neue Token eines anderen Typs erzeugt, und die alten Token müssen in den neuen referenziert werden. Dieses Problem wurde in der Literatur durch die Verwendung eines Token-Rezeptmodells oder Token-Kompositionen angegangen (Westerkamp, Victor, und Küpper 2018, 2020). Dieser Ansatz fügt den Tracking-Smart-Contracts eine weitere Komplexitätsebene hinzu, die die dezentralen Berechnungen verteuert und möglicherweise die Skalierbarkeit behindert (Scherer 2017).

Anstatt Token zu verwenden, setzen viele Lieferkettenlösungen auf verschiedene Smart-Contract-basierte Lösungen, wie die Protokollierung von Warenbewegungen im dezentralen Ledger (Bocek u. a. 2017; Lu und Xu 2017).

Software-Dienstleister, wie beispielsweise SAP, haben bereits Blockchain-Lösungen entwickelt, die eine Produktverfolgung auf einer Blockchain ermöglichen, die auf SAP-spezifischen Smart Contracts (SC) basiert. Neben anbieterspezifischen Smart Contracts hat die Blockchain-Technologie ihren Ursprung im einfachen Konzept der nativen Token, in denen Werte nach dem UTXO-Modell aufgeteilt und kombiniert werden können (Nakamoto 2008). Die Idee, Token zu verwenden, um reale Güter zu repräsentieren und zu verfolgen, gab es bereits vor der Einführung der ERC-Token-Standards. Das erste Konzept zur Darstellung von Vermögenswerten auf der Blockchain waren sogenannte Colored Coins (Anand u. a. 2017). Die Verwendung von Colored Coins ist nicht sehr weit verbreitet, da die für die Darstellung von Colored Coins erforderliche Transaktionsstruktur auf unverbrauchten Transaktionsausgaben (UTXO) basiert, die Ethereum-basierte Blockchains nicht verwenden (Vogelsteller und Buterin 2015). Die Grundidee besteht darin, nativen Transaktionen eine Eigenschaft (die Farbe) zuzuweisen, die den Wert angibt, den sie repräsentieren. Bei der Bitcoin-Blockchain zum Beispiel kann jeder Satoshi (der kleinstmögliche Wert von Bitcoin) einen anderen Vermögenswert darstellen. Dieses Konzept dient vor allem dazu, das Eigentum an den Token und damit an den Vermögenswerten zu verfolgen. Da die Transaktionen kombiniert oder in neue Transaktionen aufgeteilt werden können und die Farbe nach jeder Transaktion leicht geändert werden kann, besteht ein großes Potenzial, Colored Coins als effizientes Mittel zur Nachverfolgung in Produktionsumgebungen zu nutzen. Schließlich können die Transaktionen mit bestehenden Tools wie Blockchain-Explorern (Kuzuno und Karam 2017) leicht visualisiert und analysiert werden.

3 Simulation eines Wertschöpfungsnetzwerks

Eine der größten aktuellen Herausforderung in Wertschöpfungsnetzwerken ist es, die überbetriebliche Zusammenarbeit zwischen allen Akteuren des Netzwerkes zu verbessern. Durch solch eine Zusammenarbeit aller Netzwerkteilnehmer könnte sowohl die unternehmensinterne als auch die unternehmensüber-greifende logistische Wertschöpfung optimiert werden. Diese Erfolgspotenziale werden innerhalb des Supply Chain Managements allerdings bis heute häufig vernachlässigt und könnten durch eine effektive Integration von Prozessen und Systemen erschlossen werden. Mithilfe historischer Transaktionsdaten von Unternehmen können anschließend Optimierungspotenziale innovativer Technologien, wie beispielsweise der Blockchain-Technologie, festgestellt werden.
Aufgrund von mangelndem Vertrauen sowie fehlender Transparenz innerhalb von Wertschöpfungsnetzwerken ist es nur schwer möglich, solche historischen Transaktionsdaten für empirische Analysen von realen Netzwerken zu erhalten. Eine Lösungsmöglichkeit der Analyse ist die Verwendung simulierter betriebswirtschaftlicher Daten anhand eines repräsentativen Netzwerks. Beispielsweise werden zur Lösung von Fragestellungen in komplexen ökonomischen Systemen inzwischen häufig Simulationen verwendet, um betriebs- oder volkswirtschaftliche Probleme zu lösen.
Um die Warenbewegungen und Produktionsschritte innerhalb eines Wertschöpfungsnetzwerks zu simulieren, wurde ein Simulationstool basierend auf einem Agenten-basierten Ansatz in Python implementiert. Für eine benutzerfreundliche Nutzung des Netzwerk-Simulators wurde ein zugehöriges Web-Frontend entwickelt. Durch dieses Frontend können alle notwendigen Daten zur Simulation übersichtlich über eine Eingabemaske eingegeben werden und werden anschließend der eigentlichen Simulation im Backend übergeben.

3.1 Programmierung

Für die Programmierung wurde zuerst ein Pflichtenheft für die Muss- und Kann-Kriterien des Simulationstools aus dem Anforderungskatalog der Plattform abgeleitet. Das Pflichtenheft enthielt dabei Informationen über die Funktionsweise und Attribute der einzelnen Agenten sowie der Simulation. Die Programmierung selbst wurde nach dem Aufbau einer Grundstruktur iterativ nach den Muss- und Kann-Kriterien des Pflichtenhefts ausgeführt. Die Basis des Simulationsmodells ist in Abbildung C.6.1 mithilfe eines Entity-Relationship-Diagramms dargestellt.

Simulationsablauf

Um in der Simulation Perioden darzustellen, wurde ein rundenbasierter Ansatz gewählt. Somit stellt jede Runde der Simulation jeweils einen Zeitraum dar, in dem die beteiligten Agenten wirtschaftliche Prozesse starten können. Dabei werden die Agenten rundenweise in der immer gleichen Reihenfolge aufge-rufen. In jeder Runde wird jeder Agent dreimal aufgerufen bzw. dessen Geschäftsprozesse gestartet:
1. Aufruf einer Planungsfunktion
2. Aufruf der „manage"-Funktion
3. Aufruf einer Funktion zum Periodenabschluss
Dabei ist wichtig zu beachten, dass in der Simulation verschiedene Implementierungen für unterschiedliche Arten von wirtschaftlichen Entitäten für die genannten Prozesse erfolgt sind. So lassen sich Unterschiede beispielsweise zwischen einem Rohstoffproduzenten, einem Handelsbetrieb oder einem Endkonsumenten darstellen. Ein Handelsbetrieb benötigt zum Beispiel keine Produktionsfunktion, ähnlich wie ein Endkonsument keine Verkaufsfunktion benötigt.

Produktionsprozess

Der Produktionsprozess ist in der Simulation von essentieller Bedeutung und setzt sich aus zwei Funktionen zusammen: *„produce(self, productName, amount)"* und *„checkProducableAmount(self, product)."* Letztere Methode wird dabei innerhalb der *„produce"*-methode aufgerufen. Zum Abschluss wird das Lager mit den produzierten Mengen des Produktes aufgefüllt und die Produktionskosten des Produkts werden vom Kontostand abgezogen.

Geschäftsprozesse Kaufen und Verkaufen

Des Weiteren stehen im Mittelpunkt der Simulation die Geschäftsprozesse *„Kaufen"* und *„Verkaufen"*, um Produkte innerhalb des Netzwerkes auszutauschen und Profit zu generieren. Aus diesem Grund werden beide Vorgänge im Folgenden ausführlicher beleuchtet.

Verkaufsprozess

Der Verkaufsprozess wird durch die Methode *sell(self, order*) implementiert, wobei der Input-parameter *„order"* ein Objekt der Klasse Order darstellt. Mithilfe der Angabe dieses Parameters erhält man Zugriff auf für den Verkaufsprozess relevante Daten wie die Menge des zu verkaufenden Produktes, den Produktnamen und damit, mithilfe der Hilfsfunktion *getProductByProductName (self, productName)* auch auf das Produktobjekt.
Der Ablauf der Funktion wird im Interface *„CompanyInterface"* definiert und ist sowohl für einen Produzenten als auch für einen Händler gleich. Der Prozess läuft folgendermaßen ab: Zunächst wird über das Orderobjekt auf die Menge des Auftrags zugegriffen und überprüft, ob der Auftrag in dieser Periode bedienbar ist. Dabei gibt es drei mögliche

Ausgänge. Im Optimalfall ist die Menge im kompletten Umfang verfügbar. Ist das nicht der Fall und die georderte Menge ist höher als die Menge der Einheiten des Produktes im Lager des verkaufenden Unternehmens, wird die zu verkaufende Menge auf den Wert des aktuellen Lagerbestands des Produkts gesetzt. Somit gibt es entweder die Möglichkeit eine Teillieferung in Gang zu setzen oder - sollte die Menge der verfügbaren Einheiten Null sein - den Verkaufsprozess zu stoppen und mithilfe einer Fehlermeldung über diese Situation zu informieren.

Gesetzt den Fall, dass (Teil-) Mengen verkauft werden, werden zunächst die entsprechenden Einheiten aus dem Lager entfernt. In diesem Zuge wird direkt überprüft, ob das zu verkaufende Produkt bestandsabhängig nachgekauft wird und ausgehend davon nachgekauft, um möglichst lange einen ausreichenden Lagerbestand für zukünftige Aufträge bewahren zu können. Im Anschluss wird das eigene Orderbuch aktualisiert und dadurch entweder die ausstehende Menge der zu liefernden Produkte reduziert (bei einer Teilmengenlieferung) oder der komplette Auftrag aus dem Register gelöscht.

Zum Abschluss wird der Auftrag (bzw. die Auftragsidentifikationsnummer und die eventuell neu gesetzte Menge) dem zugehörigen Logistikdienstleister des Unternehmens übergeben und der Kunde über *informDeliveryStart(self, orderID)* über den Beginn der Lieferung informiert.

Kaufprozess

Der Kaufprozess gliedert sich in zwei Methoden: *buyProcess(self, goodName, period,bannedSupplier)* sowie *buy(self, amount, goodName, supplier):* Die Funktion „*buyProcess*“ soll dabei den Kaufprozess initiieren und mithilfe der Hilfsmethode *findBestSuppliers(self, amount, goodName, bannedSupplier)* den günstigsten (mit Berücksichtigung der Verfügbarkeit des gewünschten Gutes) Lieferant finden. Zunächst wird geprüft, ob für die benötigte Menge genug Platz im Lager ist. Dabei wird ebenfalls beachtet, dass für die eingehenden Lieferungen der aktuell noch ausstehenden Bestellungen ausreichend Lagerkapazität vorhanden ist. Sollte die ursprüngliche Bestellmenge größer sein als die freie Kapazität, wird sie auf genau die Menge reduziert, mit der das Lager komplett ausgelastet ist.

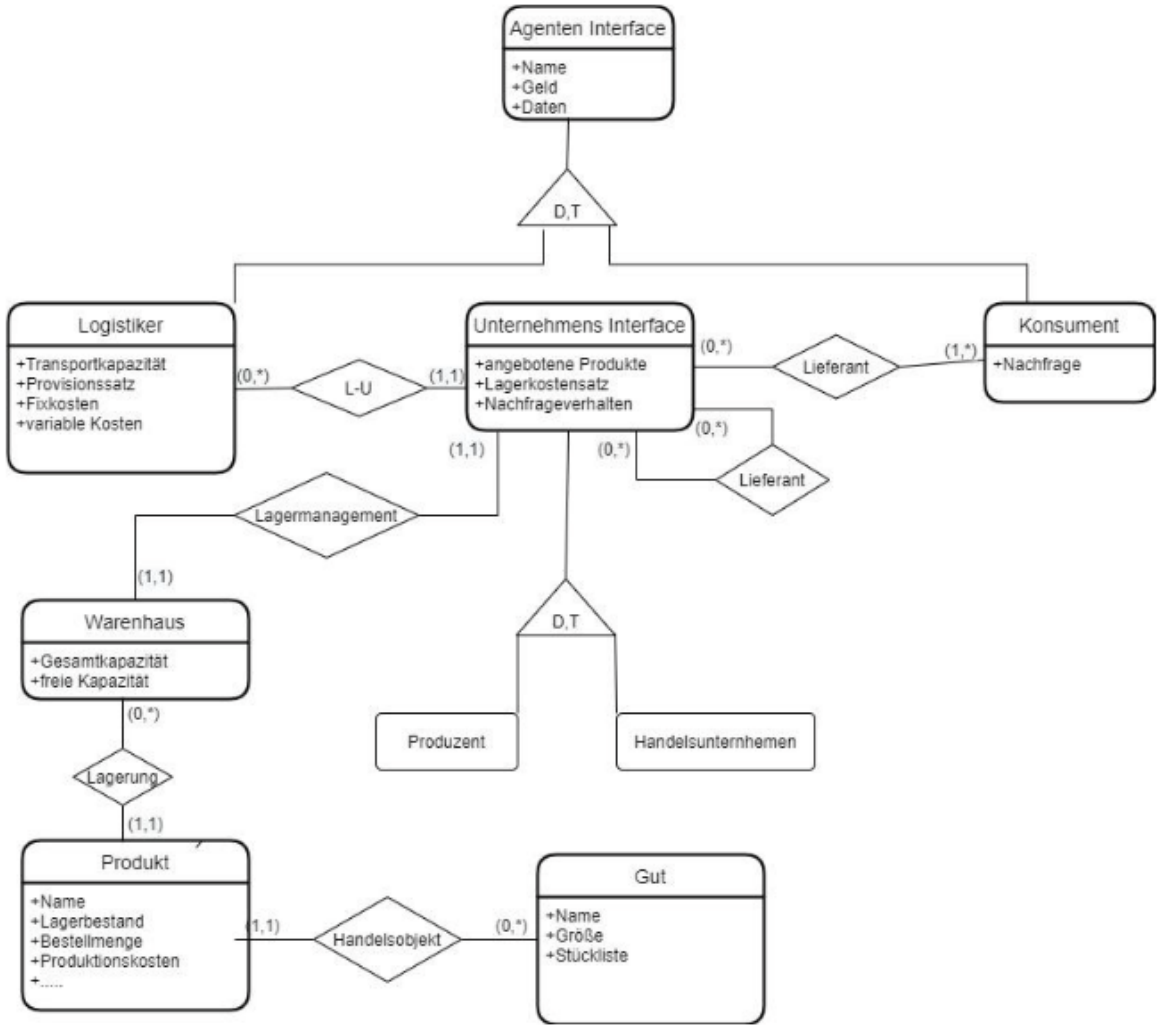


Abbildung C.6.1: Basis ERM-Diagramm des Simulationsmodells

Danach wird mithilfe der Methode „*findBestSuppliers*“ der oder die (bei mehreren gleichbewerteten Zulieferern) beste/n Lieferant/en gesucht. Dabei wird nach folgendem Ablauf vorgegangen: Zu Beginn werden alle Zulieferer, die das benötigte Gut anbieten, gefiltert und in einer Liste zusammengestellt. Jedes Listenelement enthält dabei sowohl das Zulieferer-Objekt als auch den Angebotspreis pro Einheit des Gutes sowie die verfügbare Menge. Sollte es zu der Situation kommen, dass kein einziger Zulieferer das benötigte Gut anbietet, bricht die Funktion ab und gibt eine Fehlermeldung aus. Dieses Problem kann allerdings nur dann auftreten, wenn bei der Konfiguration des Netzwerkes ein Fehler gemacht worden ist und für bestimmte benötigte Güter kein passender Lieferant (bzw. mehrere Lieferanten) definiert worden sind. Im zweiten Schritt wird versucht, aus der Liste mit möglichen Lieferanten den vorher festgelegten bzw. als Inputparameter übergebenen Lieferanten zu entfernen und diesen somit nicht bei der Lieferantenauswahl weiter zu berücksichtigen. Dabei ist anzumerken, dass ein „*banned Supplier*“ nur dann der Funktion mit übergeben wird, wenn ein Auftrag gecancelt wird (aufgrund zu langer Wartezeiten) und das Unternehmen somit auf andere Zulieferer zurückgreifen möchte. In Anschluss daran wird kontrolliert, ob aktuell ein (oder mehrere) Unternehmen aus der Liste der möglichen Lieferanten genug Einheiten anbietet (bzw. anbieten), um die komplette Bestellmenge zu bedienen. Ist das der Fall, können alle restlichen Unternehmen aus der Liste entfernt werden. Zusätzlich wird danach überprüft, ob alle Lieferanten aktuell den verfügbaren Bestand von Null aufweisen, d.h. das Gut zwar anbieten, aber aktuell (noch) nicht liefern können. In dieser Situation wurde entschieden, dass das Unternehmen trotzdem die komplette Menge bestellt, weil es im Endeffekt keine Alternativen hat. Gibt es allerdings mindestens ein Partnerunternehmen, das mindestens eine Einheit vorrätig hat, werden alle anderen Unternehmen aus der Lieferantenliste entfernt und es wird die Liste, aufsteigend sortiert nach dem Preis des anbietenden Unternehmens, zurückgegeben.

In der „*buyProcess*“-Methode wird nun weiterhin geprüft, ob es mögliche Lieferanten gibt und bei Nicht-Vorhandensein „false“ zurückgegeben und somit der Bestellprozess abgebrochen. Im Fall möglicher Lieferanten wird die Liste durchgegangen und solange die maximal verfügbare Menge des jeweiligen Unternehmens mit dem Aufruf der „*buy*“-Methode bestellt, bis die Bestellmenge gedeckt ist oder keine weiteren Lieferanten mehr vorhanden sind. Konnte der Bedarf nicht vollständig gedeckt werden, wird beim Lieferanten mit dem besten Preis bestellt, auch wenn das Gut bei diesem Unternehmen aktuell nicht verfügbar ist.

Die Funktion „*buy*“ ist im Vergleich zur „*buyProcess*“-Methode deutlich weniger umfangreich: Sie regelt nur das Eintragen in das Orderbuch der ausgehenden Bestellungen und sendet dem Lieferanten den Auftrag.

Nachfrageabhängige Preispolitik und Produktion

Die nachfrageabhängige Preispolitik und Produktion wird in dem Fall genutzt, wenn der Agent mit dem Wert „true“ beim Attribut „useDemands“ konfiguriert wurde. So kann der Agent abhängig von der Nachfrage seine Produktion hoch- bzw. herunterfahren sowie den Verkaufspreis verringern, um wettbewerbsfähiger sein zu können und eventuell eine höhere Nachfrage zu generieren.

Dieses Verhalten wird in der Simulation im „*CompanyInterface*“ durch die Methode *demandbasedStuff(self, product)* implementiert, die für jedes Produkt in *calculateConsumptionDemand(self, period)* am Ende der Periode aufgerufen wird. Zunächst wird dabei der Verkaufspreis über eine Preisfunktion an die aktuelle Nachfrage angepasst. Mithilfe des aktuellen Verkaufspreises und der aktuellen durchschnittlichen Nachfrage wird ein neuer Preis ermittelt, der sich aus der Addition des aktuellen Preises und dem Produkt aus dem „*priceMultiplier*“ und der Nachfrage ergibt. Somit beeinflusst der „*priceMultiplier*“, der bei der Initialisierung eines Produktes konfiguriert wird, die Stärke der Verringerung / Erhöhung des Preises.

Im zweiten Schritt wird die Bestellmenge des Produkts auf den Wert der aktuellen durchschnittlichen Nachfrage gesetzt, falls das Produkt nicht produzierbar, sondern nur von einem anderen Unternehmen bestellbar ist.

Die Anpassung der aktuellen Produktion (sofern das Produkt überhaupt produzierbar ist und verkauft wird) erfolgt im Anschluss: Ist die für die aktuelle Periode benötigte Menge (also die durchschnittliche Nachfrage zusammen mit bereits eingegangenen Lieferungen) geringer als die maximale Produktionskapazität für das Produkt und nicht vom aktuellen Lagerbestand gedeckt (ohne dass dabei der minimale Bestand verletzt wird), wird die aktuelle Produktionsrate auf den Wert gesetzt, der nötig ist, diese Menge zu decken. Ansonsten bleibt die Produktionsrate auf der maximalen Kapazität.

Lieferprozess

Der Lieferprozess beginnt mit dem Empfang eines Auftrags zur Lieferung eines Produktes von einem verkaufenden Agenten (*receive_order(self, auftragssteller, empfaenger, product: Product, amount, orderID*)). Zunächst werden aus den übergebenen Parametern die Provision, die benötigte Lagerkapazität sowie die Entfernung zwischen Auftragsteller und Empfänger, die aus dem „*suppliers*“-Dictionary des Empfängers extrahiert werden kann, ausgerechnet. Mithilfe dieser Informationen wird ein neues „*Delivery*“-Objekt erstellt und

dem Orderbook hinzugefügt. Je nach aktueller Auslastung wird hierbei die Lieferung direkt versandt oder aber auf die Warteliste für die nächsten Perioden geschrieben.
Sobald die Lieferung in den Versand übergeben wurde, wird durch die Methode *reduceDeliveryTime(self)* die Zeit, die der Logistikdienstleister benötigt, um die Ware von A nach B zu transportieren, simuliert. In jeder Periode wird diese Methode aufgerufen und die „*periodsToDeliver*“ der aktiven Lieferungen um eins verringert und bei Erreichen des Wertes Null aus dem Register der aktiven Lieferungen entfernt und *finishDelivery(self,delivery)* des Logistikers aufgerufen. Diese Methode leitet dann die Sendung an den Empfänger weiter und informiert diesen über die erfolgte Lieferung mithilfe der *Funktion incomingDelivery(self, sender, product, amount, provision, logistiker, orderId).*

Anomalien

Um Anomalien in die Simulation mit einfließen zu lassen, wurde für jeden Agenten in der Simulation eine *anomaly*-Methode implementiert. In dieser Methode wird zuerst eine Zufallszahl zwischen 0 und 1 generiert (die sogenannte *anomalyProbability*), welche festlegt, ob eine Anomalie bei dem betrachteten Agenten auftritt oder nicht.

3.2 Simulationskonfiguration

Die Konfiguration der Simulation und der einzelnen Simulationsdurchläufe wird durch eine graphische Darstellung mithilfe eines Web-Frontends vereinfacht. Damit kann eine JSON-Datei erstellt werden, die alle notwendigen Attribute für die jeweiligen Simulationsdurchläufe beinhaltet.
In Abbildung C.6.2 ist das Eingabefeld für die Erstellung von Attributen und Objekten für verschiedene Kategorien dargestellt. Unterhalb dieser Kategorien werden alle Attribute, die man modifizieren kann, angezeigt und auch ein Actions Feld, in dem man je nach Kategorie, Objekte hinzufügen, bearbeiten oder löschen kann. Zusätzlich wird für ein besseres Verständnis des Netzwerks und der Lieferketten eine grafische Netzwerkdarstellung anhand der eingegebenen Daten ausgegeben (siehe Abbildung C.6.3).

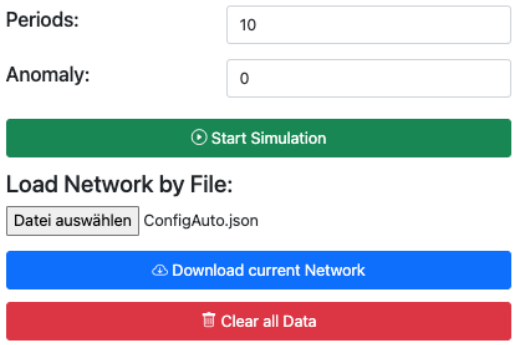


Abbildung C.6.3: Graphische Netzwerkdarstellung

In dem Eingabefeld *Periods* kann man festlegen, wie viele Perioden simuliert werden sollen; dieses Feld kann beliebig groß bestimmt werden. Unter diesem Feld folgt ein weiteres, mit welchem man die Stärke der Anomalien einstellen kann. Mit einem Wert von 0 wird die Simulation ohne jegliche Anomalien ausgeführt, desto größer der Wert der Anomalien ist (höchstens 1), desto stärker ist die Simulation von solchen befallen.
Unterhalb der Anomalien gibt es noch vier weitere Knöpfe, einmal der „Start Simulation“ Knopf, dieser kann erst benutzt werden, sobald man eine fertige Datei erstellt hat. Zusätzlich können bereits erstellte Netzwerke gespeichert und erneut wieder geladen werden (siehe Abbildung C.6.4).

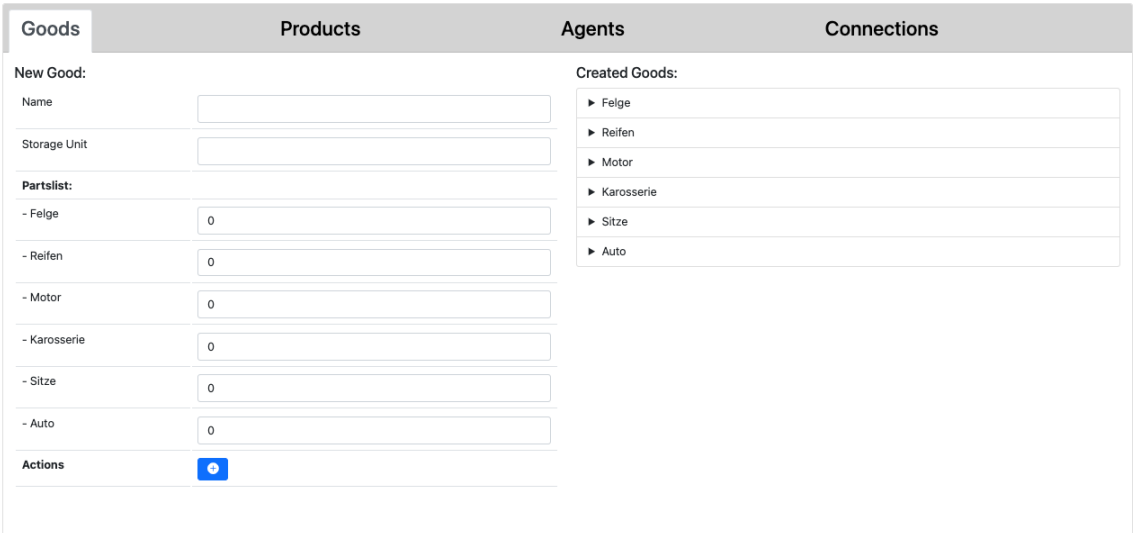


Abbildung C.6.2: Eingabefeld zur Erstellung von Attributen und Objekten

Abbildung C.6.4: Konfiguration der Simulationsdurchläufe

3.3 Auswertung der Simulationsergebnisse

Nach Durchlauf der eingestellten Simulationsperioden besteht die Möglichkeit der Einsicht einer graphischen und numerischen Auswertung der Simulationsergebnisse über das Web-Frontend. Hier werden verschiedene netzwerkspezifische Kennzahlen auf Mikro- und Makroebene ausgewertet und direkt für den Nutzer grafisch und tabellarisch aufbereitet. Darüber hinaus können die einzelnen Transaktionen innerhalb der Simulationsperioden eingesehen werden (siehe Abbildung C.6.5).

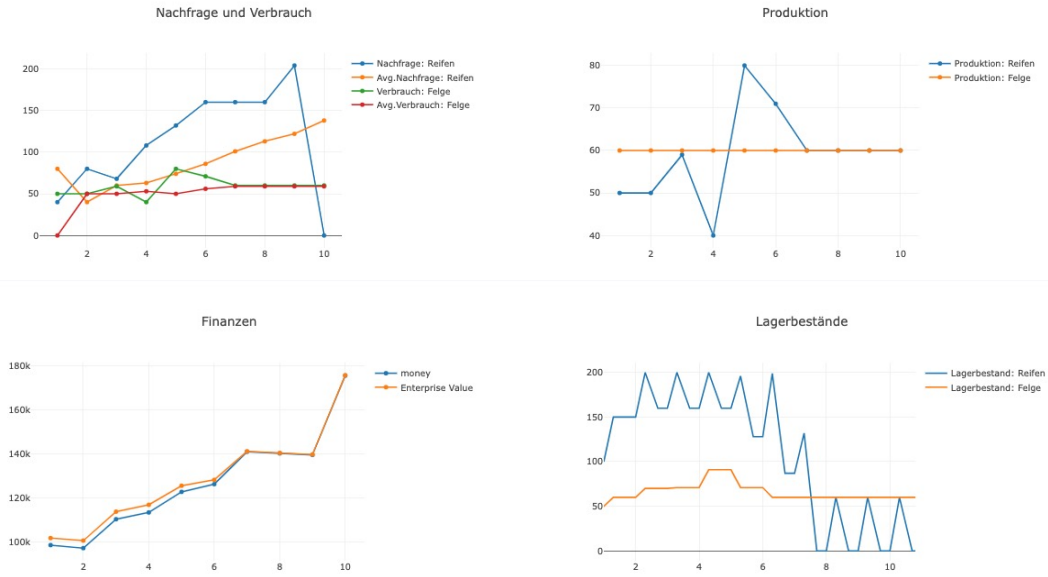


Abbildung C.6.5: Graphische Auswertung der Simulationsergebnisse

3.4 Fazit

Das Ziel des PiMKoWe Projekts ist es, eine Plattform zu schaffen, auf der Kooperationen in Wertschöpfungsnetzwerken flexibilisiert, automatisiert und abgesichert werden. Im Rahmen dieses Projekts sollen innovative Analysemethoden des gesamten Netzwerks ermöglicht werden. Allerdings ist es sehr schwer, Analysen von realen Wertschöpfungsnetzwerken durchzuführen, da viele Unternehmen ihre Daten nicht ohne Rahmenverträge oder jahrelange Zusammenarbeit Dritten anvertrauen. Deswegen wird auf Simulationen von Wertschöpfungsnetzwerken zurückgegriffen, obwohl diese nicht die gleiche Datenqualität wie eine empirische Analyse erreichen.

4 Simulation eines Blockchain-basierten Tracking und Tracing Systems

Viele Forscher und Praktiker nutzen die Blockchain-Technologie als innovatives Instrument für die Rückverfolgung von Produktinformationen in komplexen Liefernetzen. Für die Rückverfolgung wird in der Forschung und Praxis vor allem ein Token-basierter Ansatz, der auf ERC Standards aufbaut, favorisiert. Obwohl die Technologie seit mehr als einem Jahrzehnt auf dem Markt ist, sind das Wissen und die Verwendung von Token oder zur Rückverfolgung von Produkten immer noch begrenzt. Mit Hilfe eines designwissenschaftlichen Forschungsansatzes zielen wir in diesem Kapitel darauf ab, ein ERP-Blockchain-Token-System (EBTS) zu entwickeln, um Standards für die Verwendung von Token in Geschäftsprozessen zu schaffen. Die Ergebnisse können in der akademischen Welt und in der Industrie genutzt werden, um weitere Standards zu entwickeln und den Einstieg in eine Token-Wirtschaft zu erleichtern.

Um die Qualität unserer Blockchain-Forschung sicherzustellen, zeigen wir zunächst die beabsichtigten Ziele und die Bedeutung für Wissenschaft und Industrie auf. In der folgenden Forschung konzentrieren wir uns auf die Verwendung von Token mit ERP-Systemen, um der akademischen Forschung und der Industrie ein System zur Rückverfolgung von Token zur Verfügung zu stellen, das künftige gesetzliche Anforderungen an die Sorgfaltspflicht unterstützt. Wir gehen davon aus, dass eine Wirtschaft mit „*ERP Blockchain Token System*“ nur dann aufgebaut werden kann, wenn es leicht anpassbare Standards und einen offenen Zugang gibt, die die Verbreitung (Agarwal und Prasad 1997) der Blockchain-Technologie unterstützen könnten.

4.1 Methode und Simulationsdesign

Wir folgen der in der Wirtschaftsinformatik etablierten Design Science Research Methode, welche die anwendungsorientierte Ausarbeitung verschiedener Methoden, Modelle und Prototypen ermöglicht (Hevner u. a. 2004). Designprinzipien (DP), die aus empirischen Erkenntnissen oder Erfahrungen abgeleitet werden, gelten als grundlegende Leitprinzipien für die Gestaltung einer Problemlösung (Fu, Yang, und Wood 2015; Möller, Guggenberger, und Otto 2020). DP können als Artefakt als Endergebnis eines DSR-Prozesses archiviert werden (Hevner u. a. 2004). In Anlehnung an (Kuechler und Vaishnavi 2008) verwenden wir das Vorgehensmodell zur Strukturierung unseres DSR-Prozesses (siehe Abbildung C.6.6). Die klare Strukturierung des Vorgehens unterstützt eine problemlösungsorientierte Konzeption und praktische Umsetzung. Unser Konzept ist die Integration mehrerer ERP-Systeme auf dem Blockchain-Netzwerk, um Produkte über Organisations- und IT-Systemgrenzen hinweg mittels Smart Contracts und Token zu verfolgen. Daher sind das Konzept zur Standardisierung und der implementierte Smart Contract unsere Design-Artefakte. Unter Verwendung der allgemeinen Leitprinzipien der DV können Lösungswege für andere Probleme abgeleitet werden. Phase eins unseres Ansatzes liefert ein Problem und Designanforderungen (siehe Abbildung C.6.1). Die DR werden von einer Datengrundlage abgeleitet, die aus einem iterativen, unterstützenden Prozess nach Möller, Guggenberger, und Otto (2020) stammt. Durch eine systematische Literaturrecherche entwickeln wir zunächst einen ersten Satz von Anpassungsbarrieren. Die Barrieren werden in einer zweiten Iteration mit Experteninterviews überprüft, erweitert und in Designanforde-

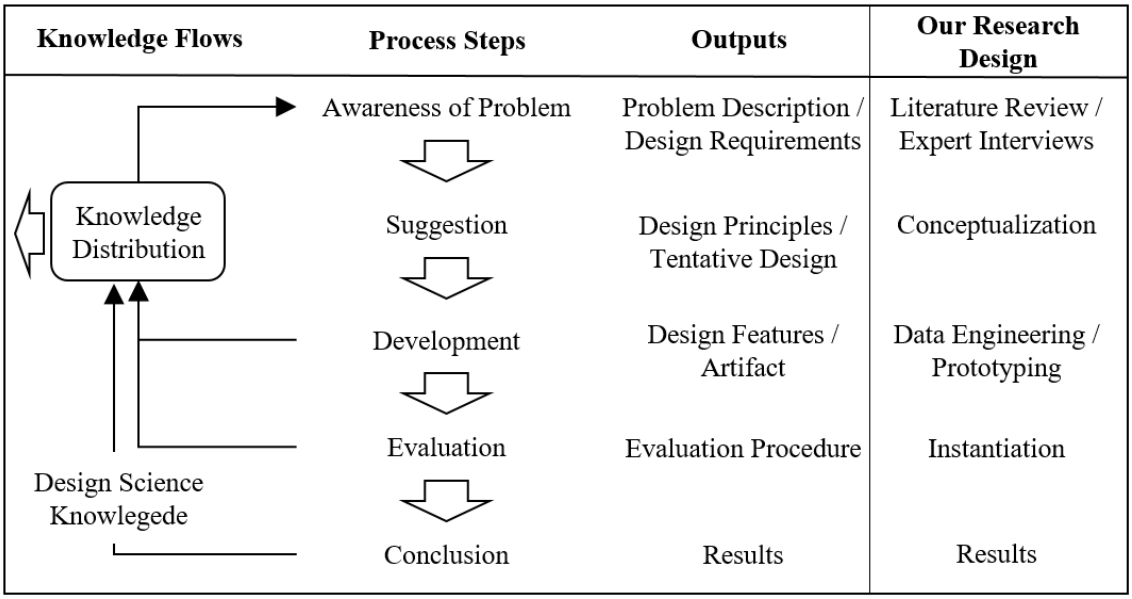


Abbildung C.6.6: Vorgehen mit Design Science Research nach Küchler und Vaishnavi (2008)

rungen (DR) überführt. In der zweiten Phase werden aus den DR Gestaltungsprinzipien (DP) abgeleitet, die als allgemeine Leitprinzipien zur Lösung des praktischen Problems dienen (Möller u. a. 2020; Vaishnavi und Küchler 2004). In der dritten Phase werden die DF durch die konkrete, praktische Anwendung der zuvor erarbeiteten DP gewonnen. Ein Mapping-Diagramm unterstützt unsere Forschung bei der endgültigen Formulierung der DV und zeigt auch die Abhängigkeiten zwischen den verschiedenen DR, DV und DF auf (Möller u. a. 2020). Die DF unserer Forschung ist die konzeptionelle Ausarbeitung eines ERP Blockchain Token Systems. Abschnitt vier beschreibt die Instanziierung, bei der das konzeptionelle Modell und der Prototyp funktional sind. Phase fünf umfasst den Abschluss der Forschungsmethodik.

4.2 Strukturierte Literaturrecherche

Um verschiedene Hindernisse für den Aufbau einer Integration eines Token-basierten Blockchainsystems in die ERP-Welt zu identifizieren, führten wir eine strukturierte Literaturrecherche durch (Vom Brocke u. a. 2009). Für die Suche haben wir die Datenbanken Web of Science, EBSCO, IEEE Xplore und AIS eLibrary abgefragt. Für die Schlagwortsuche wurde die Zeichenfolge ("Token" AND "Supply Chain" OR "Logistic" OR "Manufacturing") verwendet. Die Datenbankrecherche ergab 445 Treffer, von denen nach der Reduktionsphase neun relevante Artikel übrigblieben. Eine weitere Vorwärts- und Rückwärtssuche (Webster und Watson 2002) führte zu weiteren vier Artikeln. Die folgenden 13 Artikel wurden auf verschiedene Hindernisse bei der Verwendung von Token untersucht, die im Folgenden vorgestellt werden. Skalierbarkeit (Asprion, Hübner, und Moriggl 2019; Ghode u. a. 2020; Kim u. a. 2018), Latenz (Asprion u. a. 2019; Beck, Kildetoft, und Radonic 2020; Felipe Munoz u. a. 2021) und Größe (Beck u. a. 2020) der Blockchain sowie die Unveränderbarkeit von Daten (Ghode u. a. 2020; Kuhn u. a. 2021) werden häufig als **technische Barrieren** genannt. Diese Herausforderungen beziehen sich auf eine allgemeine technische Eigenschaft der Blockchain und müssen auch beim Einsatz von Token berücksichtigt werden.

	Dimension	Barrieren						
ID	Article	Technische Faktoren	Objekte (Daten)	Interoperabilität	Ökonomische	Soziale Faktoren	Standards	Governance
1	Basnayake and Rajapakse (2019)	X	X		X	X		
2	Kim et al. (2018)	X	X		X	X		X
3	Ghode et al. (2020)	X	X				X	X
4	Blossey et al. (2019)		X				X	
5	Asprion et al. (2019)	X	X		X		X	X
6	Westerkamp et al. (2020)	X	X	X	X	X		
7	Kuhn et al. (2021b)	X	X	X	X	X	X	
8	blinded	X	X	X		X		
9	Nielsen et al. (2020)	X	X					
10	Madhwal et al. (2021)		X					
11	Felipe Munoz et al. (2021)	X	X		X			
12	Watanabe et al. (2019)	X	X		X	X	X	
13	Beck et al. (2020)	X	X		X	X	X	X

Tabelle C.6.1: Ergebnisse der Literaturrecherche

Darüber hinaus werden notwendige **Daten** für die Nachverfolgung von **Objekten** diskutiert. Genannt werden Datenintegrität (Ghode u. a. 2020; Westerkamp u. a. 2020) und Datenvertraulichkeit (Asprion u. a. 2019; Ghode u. a. 2020; Kim u. a. 2018), die zunächst in den Kontext der Datensicherheit gehören. Zu den Daten gehören aber auch der obligatorische Datenumfang und die Datenqualität, die für die Rückverfolgung von Produkten durch Produktionsumgebungen erforderlich sind.

Weiterer Schlüsselfaktor ist die **Interoperabilität** mit bereits implementierten Informationssystemen (z.B. ERP). Daher ist die horizontale Integration entlang eines heterogenen IT-Liefernetzwerks ein **wirtschaftlicher Faktor** für Unternehmen, den jeder Handelspartner in eine geschäftliche und technologische Integration investieren muss. Nach Kim u. a. (2018) ist es ein kritischer **sozialer Faktor**, alle Akteure zur Integration zu bewegen. Der Mangel an technischem Know-how für Blockchains (Ghode et al., 2020) und der Mangel an Vertrauen bilden verschiedene Barrieren für eine potenzielle Token Economy (Beck u. a. 2020).

Speziell im Hinblick **auf Standards & Regulatorien** wird der Aspekt des privaten Datenschutzes von Asprion u. a. (2019) und der Qualitätssicherung wie ISO 9001 oder IATF 16949 (Kuhn u. a. 2021;

Westerkamp u. a. 2020) genannt. Keiner der Autoren erwähnt Normen in der Blockchain, wie z. B. ISO/TC 307, die derzeit noch in Arbeit ist, aber keinen Bezug zu technischen Normen für Token vorschlägt. Daher werfen die oben genannten Herausforderungen die Frage auf, wie ein ausgewogenes Anreizsystem (**Governance**) für verschiedene Teilnehmer entlang eines Versorgungsnetzes gestaltet werden kann, um widersprüchliche oder konkurrierende Interessen in Einklang zu bringen (Beck u. a. 2020).

4.3 Semi-strukturierte Interviews

Auf der Grundlage der Ergebnisse unserer Literaturrecherche führten wir halbstrukturierte Interviews (Glaser und Strauss 1967) durch, um unsere Ergebnisse in einer zweiten Iteration mit den Anforderungen von Industrieunternehmen zu validieren (Möller u. a. 2020).
Die Experten wurden aus Unternehmen ausgewählt, die identifizierbare und rückverfolgbare Produkte herstellen, Informations-systeme zur Unterstützung der Qualitätsdokumentation einsetzen und somit über Berufserfahrung im Management der Rückverfolgbarkeit von Produkten verfügen.
Die Fragen waren offen und wurden in Form von Videointerviews von Oktober bis November 2021 durchgeführt. Die Transkripte wurden mit Hilfe von Schlüsselwörtern kodiert, um die Informationen aus den Aussagen so genau wie möglich herauszuarbeiten (Übersicht siehe Tabelle C.6.2).
Die Anzahl der Experten wurde nicht erhöht, da mit den letzten Interviews eine Sättigung (Corbin und Strauss 1990) erreicht wurde. Der Aufbau und die Integration einer Plattform in die überbetriebliche Produktverfolgung wurden mit den Experten aus verschiedenen Bereichen, ihren Produkten und Lieferkettensituationen diskutiert. Durch offene Fragen wurden Informationen über soziale Faktoren, organisatorische Anforderungen zur Sicherung der Qualität von Produkten und Prozessen sowie technische Aspekte der eingesetzten Informationssysteme gewonnen.
Die Befragten bestätigten die festgestellten Hindernisse für die Einrichtung eines ERP Blockchain Token Systems und die Schwierigkeit, einen einfachen Standard über ihre Unternehmensgrenzen hinaus zu schaffen.

4.4 Problembeschreibung und Designanforderungen

Die Notwendigkeit einer strukturierten Rückverfolgbarkeit von Produkten und Geschäftsprozessen ist in Unternehmen, die qualitäts- oder sicherheitsrelevante Produktionsschritte durchführen, seit vielen Jahren bekannt. Das vorangegangene Kapitel zeigt, dass Unternehmen Qualitätsstandards und IT-Systeme etabliert haben, um eine grundlegende oder erweiterte Rückverfolgbarkeit innerhalb ihrer Unternehmensgrenzen zu gewährleisten. Aufgrund der stetig gestiegenen Geschäftsanforderungen wurden im Laufe der Jahre zahlreiche individuelle Anpassungen in den Informationssystemen entwickelt, die ein kostengünstiges ERP Blockchain Token System für die Rückverfolgbarkeit in Form einer Plattform erschweren.
Dieses Problem wurde insbesondere von den Autoren Sunyaev u. a. (2021) angesprochen, die darauf hinweisen, dass die organisatorische Koordination eines Netzwerks bis zu 80 % des Aufwands erfordern kann, was eine kosteneffiziente Umsetzung behindert.

Wir schließen mit der ersten Anforderung **DR1 Wirtschaftliche Faktoren:** Die Integration eines Blockchainsystems sollte einen möglichst geringen organisatorischen und technischen Implementierungsaufwand verursachen, um eine hohe Akzeptanz bei Unternehmen unterschiedlicher Größe zu erreichen.
Im Design Science Forschungsprozess wurde diese Anforderung von allen Interviewpartnern bestätigt. Aufgrund der Neuartigkeit eines Token-basierten Ansatzes ist ein einfacher Zugang wesentlich, um die Technologien und Entwicklungen rund um Smart Contracts zu verstehen.

Dieser **soziale Faktor** ist in **DR2** enthalten und wird dort erläutert: "Ein ERP Blockchain System sollte die Integration von Praktikern und Forschern ermöglichen, um die Konzepte der Blockchain-Technologie und Token zu verstehen." Die Rückverfolgbarkeit von Produkten mit Token sollte auf der Grundlage von **DR1** und **DR2** weiter diskutiert werden. Token müssen daher mit den bestehenden Rückverfolgungspraktiken aus dem operativen Betrieb der Lieferkette kompatibel sein (Zhou u. a. 2011). Die Befragten nannten auch Anforderungen an die Integration von indirekt genutzten Objekten (z.B. Messgeräte oder Software) und detaillierte Fachprozesse wie Qualitäts- oder Lagertransaktionen, die ebenfalls kundenindividuell dokumentiert werden.

DR3: Daten-Objekte: EBTS muss die Möglichkeit haben, direkte Produkte und indirekt verwendete Objekte über mehrere Wertschöpfungsstufen hinweg zu verfolgen. Dazu muss eine ausreichende Datenqualität vorhanden sein, um die Rückverfolgbarkeit zu gewährleisten. Die Integration bestehender Informationssysteme ist ein weiterer kritischer Faktor beim Aufbau einer Token Economy. IT-Systeme, die bereits implementiert sind und seit vielen Jahren Produktionsumgebungen unterstützen, werden nicht fundiert. Stattdessen werden sie

			Mechanical Engineering	Mechanical Engineering	Mechanical Engineering	IT Product Development	ERP Provider	IT Management	Automotive	Plattform Provider
ID	**Barrier**	**Requirement**	**I1**	**I2**	**I3**	**I4**	**I5**	**I6**	**I7**	**I8**
1	Wirtschaft-liche Faktoren	Wirtschaftlichen Eintritt in die Token Economy reduzieren	X	X	X	X	X	X	X	X
2	*Soziale Faktoren*	Technologie und Token erläutern	X	X	X	X	X	X	X	X
3a	Rückver-folgbare Objekte	Tracing of Direct Components or	X	X	X	X	X		X	X
3b		Verfolgung von indirekten Objekten (Messwerk-zeuge, QM-Zertifikate)		X		X	X		X	
4	Inter-operabilität	Integration verschiedener Informations-systeme				X	X	X	X	X
5	Standards und Regulatorie n	ISO 9001, IATF 16949, Schutz privater und geschäftlicher Daten	X	X	X	X	X		X	
6	Technische Faktoren	Obligatorische Token-Daten definieren	X	X		X	X		X	
7	Governance	Sollte einen flexiblen Beitritt zum Netzwerk in Betracht ziehen	X	X	X			X	X	

Tabelle C.6.2: Überblick über Interviews und Anforderungen

für die Gegebenheiten des Konsortiums durch Anpassungen oder individuelle Modifikationen verändert. Definierte globale Datenfelder müssen die Interoperabilität zwischen Informationssystemen sicherstellen, um Transaktions- und Organisationsdaten über eine Middleware abzubilden.

DR4: Interoperabilität: Es müssen bestehende Informationssysteme berücksichtigt werden, da bereits implementierte Software zur Erfüllung der Anforderungen nicht ersetzt, sondern zur Bereitstellung von Transaktionsdaten verwendet wird.

Aufgrund der bestehenden Komplexität und Vielfalt der bestehenden Informationssysteme wurde in den Interviews festgestellt, dass die Zusammenführung der Systeme eine große Herausforderung darstellt. Eine Trennung zwischen notwendigen und optionalen Informationen in einer Blockchain wäre dabei hilfreich. Diese Hilfestellung wird bereits von Organisationen wie GS1 vorgeschlagen,

deren Standard jedoch nicht allen Befragten bekannt ist oder umgesetzt wird.

DR5: Technische Faktoren: Es wird zwischen obligatorischen und optionalen Daten unterschieden, um den Rahmen für den Aufbau eines Rückverfolgbarkeitsnetzwerks für ein Konsortium zu definieren. Die Anforderungen an die Qualitätssicherung werden bei den Interviewpartnern durch Normen wie ISO 9001, IATF 16949 umgesetzt. I7 weist jedoch darauf hin, dass "diese Anforderungen innerhalb der Grenzen eines Unternehmens auf unterschiedliche Weise erfüllt werden können". Daher besteht eine Herausforderung darin, innerhalb des Konsortiums einen einheitlichen Standard für die Prozessdokumentation zu gewährleisten, um die erforderliche Datenqualität zu erreichen und das Unternehmen und die personenbezogenen Daten zu schützen.

DR6: Normen und Vorschriften: Es sollte sich an Industriestandards zur Qualitätssicherung orientiert werden. Im weiteren Sinne gehören zu den Standards auch eine standardisierte Prozessdokumentation zur Identifizierung der zu schützenden Daten innerhalb des Konsortiums. Aufgrund der oben beschriebenen Herausforderungen und möglichen Barrieren bei der Etablierung eines standardisierten Plattformkonzepts muss der Beitritt von Einzelpersonen zum Netzwerk möglich sein. Wir definieren das folgende Anreizsystem, um die organisatorische und technische Beteiligung an der Plattform sicherzustellen.

DR7 Steuerung: Es muss ein flexibler Weg für den Beitritt von Unternehmen geboten werden, da es zu Beginn eines Konsortiums keine einheitlichen technischen und organisatorischen Standards gibt. Ein Anreiz zur Integration kann nur geschaffen werden, wenn eine einfache horizontale Integration möglich ist. Das System sollte eine Möglichkeit bieten, Token-Flüsse zu Handelspartnern zu dokumentieren, die außerhalb der Blockchain liegen.
Um die ermittelten Gestaltungsanforderungen zu erfüllen, haben wir aus jeder dieser Anforderungen mehrere Gestaltungsprinzipien abgeleitet. Sowohl DR1 als auch DR2 beinhalten eine organisatorische und technische Perspektive. Im Kern sollte die Blockchain-Technologie allen Interessenten dezentral zur Verfügung stehen, um eine Zentralisierung durch führende Softwareanbieter oder große Unternehmen zu vermeiden. Eine Wirtschaft kann nur aufgebaut werden, wenn es einen offenen Zugang zur Technologie gibt.

DP1: EBTS sollte eine weitere unabhängige Entwicklung durch Industrie und Forschung ermöglichen, um die Akzeptanz und Verbreitung von Token zu ermöglichen. Mit einer dezentralen Denkweise und einem offenen Zugang zur Technologie kann ein langfristiger Konsens über Standards erreicht und eine Token-Liefer(ketten)-Netzwerkwirtschaft unterstützt werden. Die in DP1 formulierte dezen-trale Denkweise bietet sowohl Chancen als auch neue Hindernisse für die Standardisierung. Wir verwenden das SCOR-Modell als Grundlage für grundlegende SCM-Ereignisse (Source, Make, Deliver), ein bekanntes Lieferketten-Framework, das bereits in verschiedenen Unternehmen implementiert wurde (Zhou u. a. 2011).

DP2: EBTS bietet die Möglichkeit einer einfachen Anpassung an einen stabilen Kern von Standardprozessen. Diese Vereinfachung komplexer Wertschöpfungsprozesse kann jedoch zu einem Mangel an Akzeptanz bei den Handelspartnern führen. Insofern sollte es eine weitere Möglichkeit geben, die beschriebenen Kernprozesse um spezialisierte Prozesse (z.B. Qualitäts- oder Lagerbestellungen) des Konsortiums zu erweitern.

DP3: EBTS muss es ermöglichen, bestehende Kernprozesse um spezialisierte Prozesse zu erweitern. Es sollte daher möglich sein, individuelle und zusätzliche Token-Transaktionsereignisse im Konsortium zu definieren. Diese Individualisierung sollte mit den zentralen Mechanismen der Nachvollziehbarkeit konform gehen. Die Rückverfolgbarkeit von Produkten und Geschäftsschritten (Ereignissen) muss also weiterhin möglich sein.

DP4: Die Rückverfolgbarkeit von Produkten und Dienstleistungen ist nach wie vor durch technische Eigenschaften und technische Standards gegeben. Durch die mögliche Verbreitung und verstärkte Einbindung von Industriepartnern sollte es möglich sein, neue anonyme Kommunikation zu gestalten, um zwischengeschaltete oder ineffiziente Kommunikationskanäle mit dem Netz zu verbessern (z.B. für Rückgabeabklärungen).

DP5: BTMS ermöglicht die Gestaltung neuer und anonymer Kommunikationskanäle entlang einer Lieferkette. Aufgrund der zunehmenden Integration von Handelspartnern sollte das Netz jedoch eine Möglichkeit bieten, Unternehmensdaten und persönliche Daten zu schützen.

DP6: BTMS muss bei der Gestaltung und Verwendung von Token Sicherheitsoptionen oder Anonymisierung für sensible Daten des Informationssystems ermöglichen.

4.5 Entwicklung

der Entwicklung von EBTS konzentrieren wir uns auf die Möglichkeit der Integration mehrerer hete-

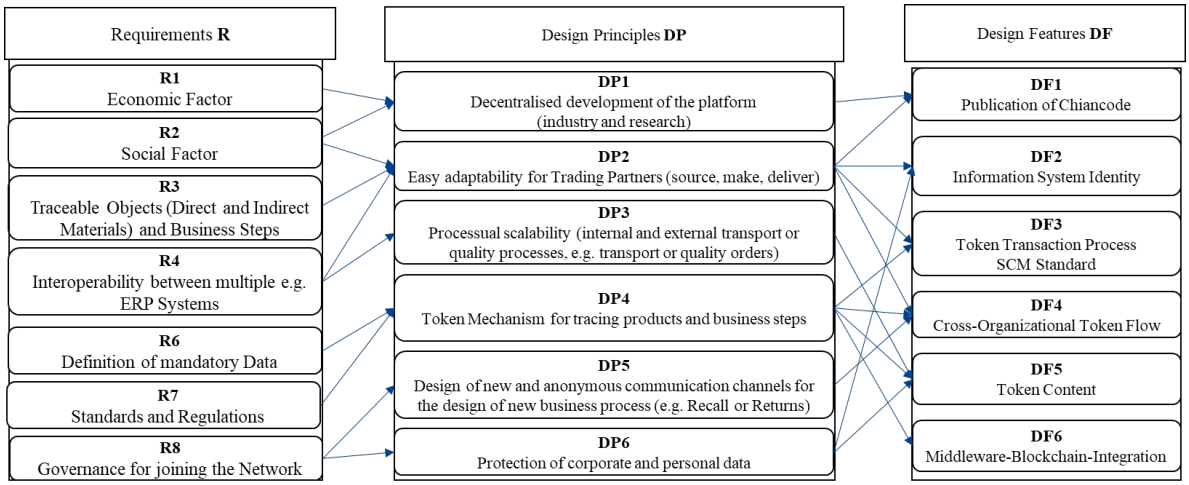


Abbildung C.6.7: Verbindung von Designanforderungen, -prinzipien und -merkmalen

Auf der Grundlage unserer Designprinzipien haben wir ihre Merkmale genutzt, um verschiedene Designmerkmale (DF) zu entwickeln. Die spezifischen DFs und Beziehungen werden im folgenden Abschnitt beschrieben und in Abbildung C.6.7 als Mapping-Diagramm dargestellt.

Nachfolgend stellen wir sechs Gestaltungsmerkmale vor, die zwei Aspekte verfolgen. Erstens beschreiben wir das auf Hyperledger Fabric basierende Blockchain-Konzept und einen Token, den wir "colored coin" nennen (DF1, DF3, DF5). Zweitens gehen wir auf die notwendige ERP-Blockchain-Integration ein (DF2, DF3, DF4, DF6), die erforderlich ist, um einen Standard für unseren Anwendungsfall zu bilden.

Veröffentlichung des Chaincodes (DF1)

Wir haben uns für ein Hyperledger Fabric-Netzwerk entschieden, da es von Unternehmen genutzt wird, die an der Rückverfolgung ihrer Produkte über ihre Unternehmensgrenzen hinaus interessiert sind. Außerdem bietet Hyperledger Fabric ein hohes Maß an Flexibilität für die Gestaltung von Token, um komplexe Lieferkettenprozesse technisch abzubilden (Miehle u. a. 2019). Wir haben unseren Token und Smart Contract (in Fabric Chaincode genannt) auf Github zur allgemeinen Nutzung veröffentlicht. Wir haben uns entschieden, Node.js für die Entwicklung von Chaincode zu verwenden. In den nächsten Schritten werden wir erklären, wie dieser Chaincode für die Standardisierungsforschung genutzt und integriert werden könnte.

Identität des Informationssystems (DF2)

In Hyperledger Fabric wird die Teilnahme an der Blockchain von MSP (Membership Service Providers) organisiert, die eine Organisation mit einer MSP-ID innerhalb des Netzwerks identifizieren. Bei

rogener ERP-Systeme. Tabelle C.6.3 zeigt die Konfigurationsmöglichkeiten der ERP-Systeme SAP, Navision und Weclapp, die wir mit frei verfügbarer Dokumentation und wissenschaftlicher Literatur verglichen haben.

EBTS	**Org1**	**Org2**	**Org3**
ERP System	**SAP ERP**	**Navision**	**Weclapp ERP**
Eindeutige Identifizierung eines Systems	Systemname / ID = Benutzer		
Organisatorische Strukturen	Mandant, Werk, Lagerort, Lagerhaus, Lagertyp, Lagerbereich MD: Lagerplatz	Ortscode, Lagerplatzcode	Lagerhaus, Lagerplatz-ID

Tabelle C.6.3: Vergleich der ERP-Strukturen

Für die Verwaltung von Produkten und Beständen innerhalb eines ERP-Systems stehen verschiedene organisatorische Strukturen (OS) zur Verfügung, die zur Abbildung von Produktionsanlagen genutzt werden können. Die Schaffung eines einheitlichen Standards auf Basis von OS könnte in der Praxis zu einem erhöhten Aufwand führen und die Akzeptanz und Bereitschaft der Handelspartner zur Teilnahme an einem Netzwerk verringern. Daher sollte jedes ERP-System über eine eindeutige Identifizierung eines Systems (*engl. Unique Identification of a System* (UIS)) verfügen, das die höchste gemeinsame Abstraktionsebene und einen möglichen

SCM	SCOR Process	Source	Make	Deliver
ERP	Navision	0 - Purchase	6 Consumption (-) 7 Output (+)	1 Sale (-)
	SAP	101 Goods Receipt (+)	261 Goods Issue Production (-) 101 Goods Receipt (+)	601Goods Issue to Customer (-)
	Weclapp	IN_PURCHASE_ORDER	IN_PRODUCTION_ORDER ,OUT_PRODUCTION_ORDER	OUT_SALES_ORDER (-)
BC	Token Function	Mint, Transfer, Redeem		
BC	Token Event	SM: Source Mint, TS: Transfer Mint	MT: Make Transfer	DT: Deliver Transfer, DR: Deliver Redeem

Tabelle C.6.4: Bildung eines Token Event Standards

Standard darstellt. Wir werden daher das UIS eines ERP-Systems als Benutzer im Netzwerk verwenden und ihm eine organisatorische Identität (MSP-ID) zuweisen. Dieser Benutzer kann dann als Tokenbesitzer verwendet werden, um verschiedene Transaktionen innerhalb eines Kanals auszuführen. In Fabric wird die Verwaltung der Identitäten in Form von Wallets organisiert, deren Metadaten mit den MSP-IDs verknüpft sind. Um mehrere ERP-Systeme einer Organisation in EBTS abzubilden, nutzen wir die Konfigurationsmöglichkeit der Wallets, da diese mehrere Identitäten verwalten können.

Token Event Standard für die unternehmensübergreifende Produktverfolgung (DF3 & DF4)

Zahlreiche Organisationen haben bereits mit der Entwicklung von Blockchain-Standards begonnen, deren Ausarbeitung noch im Gange ist. Neben dem Mangel an standardisierten Begriffen gibt es auch Probleme mit der Interoperabilität, da auf Blockchains unterschiedliche Konzepte (z. B. UTXO und kontobasiertes Modell) verwendet werden. Beide Konzepte definieren unterschiedliche technische Eigenschaften von Token, die wir in diesem Beitrag nicht im Detail erläutern werden. Sie verfügen jedoch über standardmäßige Funktionen, die das Generieren/Münzen (M), Übertragen (T) und Brennen/Einlösen (R) von Token auf Basis von SC ermöglichen. Darüber hinaus beschreiben sie Bewegungen von Werten zwischen einem Sender und einem Empfänger innerhalb eines Blockchain-Systems. Die Umwandlung dieser drei Arten von Bewegungen ermöglicht ein standardisiertes und einfaches Verständnis, das auf komplexe Lieferkettenprozesse anwendbar ist. Wie oben erwähnt, beschreibt das SCOR-Modell die Kernprozesse

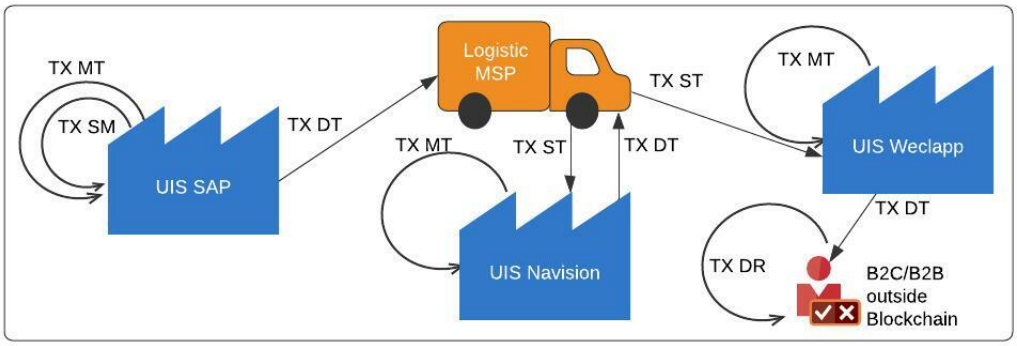


Abbildung C.6.8: Unternehmensübergreifender Token Fluss aus Sicht der Lieferkette

Source (S), Make (M), Deliver (D). Im Folgenden werden die beiden Konzepte für ERP-Systeme zusammengeführt, um die Möglichkeit von unternehmensübergreifenden Transaktionsflussereignissen standardisiert darzustellen (Tabelle C.6.4). Der Vergleich zeigt, dass ERP-Systeme die Kernprozesse des SCOR-Modells berücksichtigen und in einen Token-Event-Standard überführt werden können. Das Referenzmodell und die Eigenschaften der Token können als Basis für ein Konzept verwendet werden, das auf weitere ERP-Systeme ausgedehnt werden kann. Abbildung C.6.8 zeigt den Token-Übergang von mehreren ERP-Systemen (UIS) zu einem Logistik-MSP. Dieser zusätzliche MSP wird als Eigentümer benötigt, um den Fluss von Produkten und Informationssystemen in Token zwischen verschiedenen Produktionsstätten synchron abzubilden. Wird ein Warenausgang (WA) in einem ERP-System gebucht, muss die generierte Transaktions-ID (TXID) am Produkt-etikett oder per EDI übertragen werden. Bei einem ST wird die Anlage über Materialnummer, Chargennummer und empfangene TXID auf dem Logistik-MSP identifiziert und an das eigene System übertragen. Abgesehen davon berücksichtigen wir, dass zu Beginn eines Netzwerks nicht alle Organisationen am Netzwerk teilnehmen. Der MSP B2C/B2B außerhalb der Blockchain weist nach, dass die Ware versandt wurde (DT) und im Kanal oder Netzwerk nicht mehr benötigt wird (DR).

Wahl des Tokens und des Token-Inhalts (DF5)

Nach Sunyaev u. a. (2021) ist ein Token definiert als eine "Zeichenfolge, die als Kennung für einen bestimmten Vermögenswert oder Vermögenstyp dient". Die Darstellung eines Tokens umfasst somit ein eindeutig identifizierbares Produkt oder eine eindeutig identifizierbare Dienstleistung, die durch eine Kombination aus Materialnummer/GTIN, Chargen- oder Seriennummer gekennzeichnet sein kann. In einer weiteren Ausarbeitung werden wir einen hybriden Token-Ansatz verwenden, den wir Colored Coin nennen. Die Farbe beschreibt Metadaten oder Informationsattribute, die für die Rückverfolgung von Produkten erforderlich sind (siehe Tabelle C.6.5). Dieser Token-Ansatz basiert auf dem UTXO-Modell, das in Fabric unter dem Namen FabToken erläutert wird. Die Datenfelder stellen unseren Token dar und zeigen obligatorische und optionale Informationen, um die Rückverfolgbarkeit von Produkten zu gewährleisten (siehe Tabelle C.6.5)

NR	Attribute(M/O)	Description of attribute
1	Owner (M)	MSPID = Eigentümer: kennzeichnet den Eigentümer von Vermögenswerten (z. B. ERP-System)
2	txEvent (M)	Token-Ereignisse (z. B. MT, ST, DT, Rücküberweisung = RT, Qualitätsüberweisung = QT)
3	txID (M)	Identifiziert ein eindeutiges Transaktionsereignis, das im ERP-System eine Quell-, Produktions- oder Kundenauftragsnummer darstellt.
4	spent (M)	Gibt an, ob das Unternehmen über einen bestimmten Bestand verfügt. Diese zusätzliche Logik gilt für Chargenmaterial, das keine 1:1-Beziehung zwischen Produktion und Lagerbewegungen aufweist, wie z.B. Seriennummern. Wahr bedeutet, dass es keine Restmenge im Informationssystem gibt. Falsch bedeutet daher, daß sich ein Materialbestand im Informationssystem befindet.
5	matNr (M)	Identifizierende Materialnummer oder GTIN-Nummer.
6	batchNr (M)	Identifizierung der Chargennummer einer Komponente.
7	serialNr (M)	Identifizierende Seriennummer einer Komponente.
8	timestampErp(O)	Zeitstempel für die Ausführung eines bestimmten Vorgangs.
9	Q-Contact (O)	Kontaktmöglichkeit für die Meldung von Qualitätsmängeln.

Tabelle C.6.5: Obligatorisches und optionales Token für das UTXO-Modell.

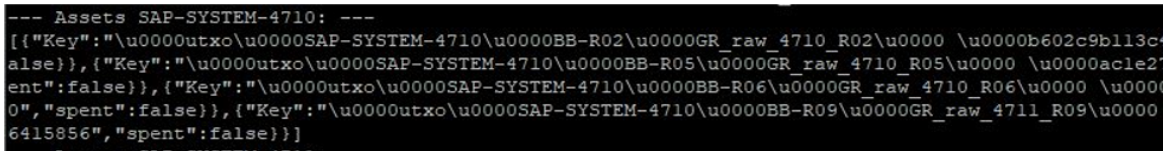


Abbildung C.6.10: Rückgabe von Query-Chaincode nach Prägung (SM-Transaktion) Vermögenswerte

Middleware-Blockchain-Integration (DF6)

Das letzte Merkmal zur Schaffung eines EBTS ist der Entwurf einer Middleware. Sie verbindet das Fabric-Netzwerk und die ERP-Systeme, um ein Konsortium im Blockchain-Netzwerk zu gewährleisten (siehe Abbildung C.6.9). Dazu werden Transaktionsdaten aus den ERP-Systemen geladen und in einen systemübergreifenden semantischen und syntaktischen Standard überführt. Die Datensätze der Systeme werden einheitlich aufbereitet und die einzelnen Warenbewegungen in txEvents übersetzt. Die Funktionen des implementierten Chaincodes werden mit dem Fabric SDK ausgelöst. Nach der Ausführung der Daten innerhalb des Blockchain-Netzwerks werden die Bewegungsdaten durch Re-Mapping in die jeweiligen Datenmodelle der ERP-Systeme zurückgeführt.

4.6 Evaluation

Unsere Forschungsergebnisse (Konzept und Chaincode) werden durch Instanziierung und Prototyping evaluiert (Peffers et al., 2012; Möller et al., 2020). Zu diesem Zweck verwenden wir einen Datensatz, der auf einer SAP-Unternehmenssimulation basiert. Für die prototypische Evaluation haben wir die beschriebene Middleware in Python als Verbindung zwischen Blockchain und ERP-Systemen implementiert. Für die Instanziierung verwenden wir einen simulierten Batch-Prozess, der eine einfache Make-to-Stock-Produktion zwischen zwei ERP-Systemen darstellt.

Tokeninhalt und Chaincode

Wir haben ein Hyperledger Fabric Netzwerk auf einem Linux Server instanziiert, um die beschriebene Token-Konfiguration zu testen. Zu diesem Zweck wurden für jedes ERP-System ein Benutzer und eine Organisation (MSP-ID: "SAP-SYSTEM-4710", "SAP-SYSTEM-4711") angelegt. Die Organisationen und Benutzer sind über die gleiche MSP-ID mit den Identitäten der jeweiligen Wallets verknüpft. Um Token-Transaktionen durchführen zu können, wurden beide Benutzer zu einem Kanal hinzugefügt. Zusätzlich haben wir den "LOGISTIC MSP" konfiguriert, der die system- und unternehmensübergreifende Kommunikation unterstützt. Wir können die Funktionalität unseres Chaincodes in Abbildung C.6.10 demonstrieren. Des Weiteren können wir die systemübergreifende Warenbewegung mit einer DT-Transaktion (siehe Abbildung C.6.11) vom "SAP-System-4710" zum "LOGISTIC MSP" und mit einer ST-Transaktion zum "SAP-System-4711" auf der Blockchain persistieren. Dabei wird das Attribut "Spent" des linken Assets durch die nachfolgende ST-Transaktion auf true gesetzt, da diese Transaktion das Asset in einer anderen Transaktion verbraucht hat. Die beschriebenen Inputs und Outputs sind über eine eindeutige TXID verknüpft, die eine eindeutige Rückverfolgbarkeit der verschiedenen Produktionsschritte und Materialien gewährleistet.

Middleware - unternehmensübergreifende Produktverfolgung

Zum Abschluss zeigen wir durch Prototyping, dass das Konzept in ERP-Systeme integriert werden

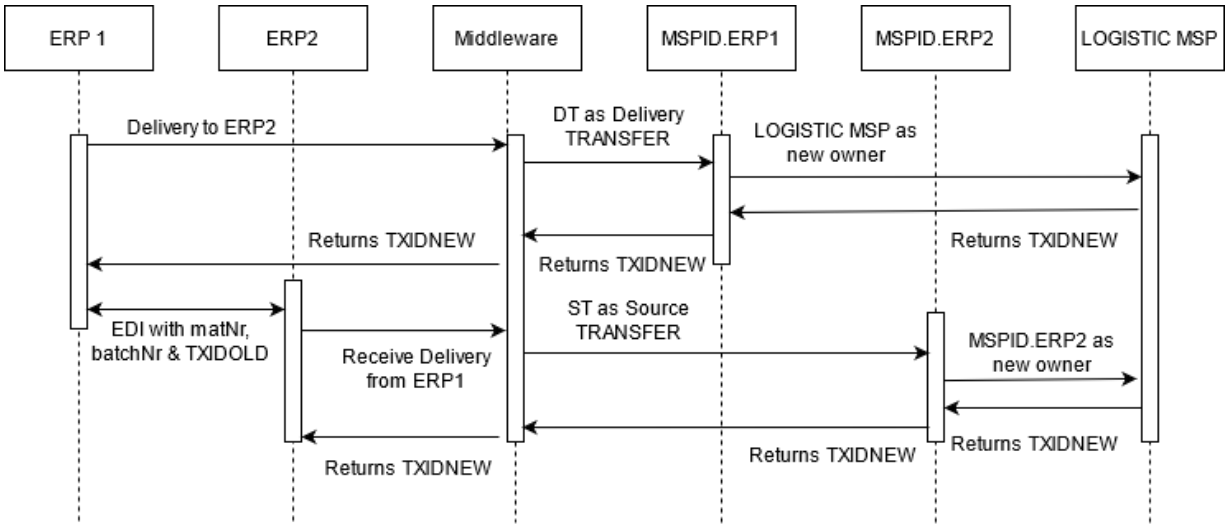


Abbildung C.6.9: Sequenzdiagramm für die unternehmensübergreifende Kommunikation auf ERP & Blockchain

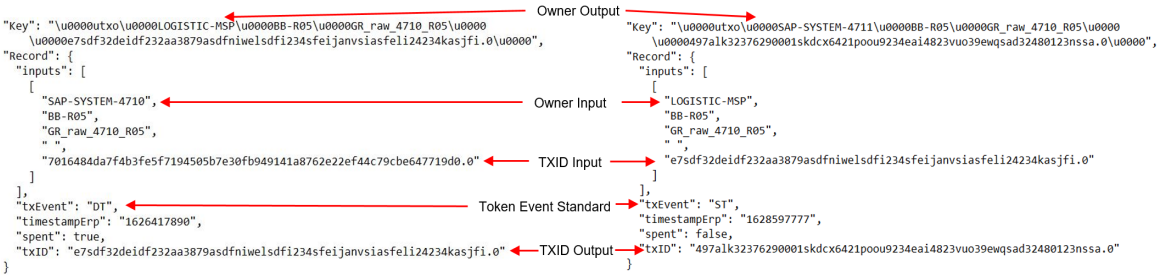


Abbildung C.6.11: JSON-Rückgabe für Token aus der Blockchain für DT- und ST-Transaktionen

			MATERIALNR		BATCHNR	TXIDNEW	TXIDOLD	TXEVENT	EXTERNOWNER				SERIALNR	TIMESTAMPERP
#	BWART	SHKZG	MATNR	VGART_MK	CHARG	TXIDNEW	TXIDOLD	TXEVENT	EXTERNOWNER	MENGE	MEINS	AUFNR	XBLNR_MKPF	SERIENNU	TIMESTAMPERP
0	101	S	BB-R02	WE	GR_raw_4710_R02	b602c9b113c41a7a		SM		36000	KG		4500000001		1625310656
1	101	S	BB-R05	WE	GR_raw_4710_R05	b602c9b113c41a7a		SM		84000	KG		4500000001		1626156656
2	101	S	BB-R06	WE	GR_raw_4710_R06	b157462d40cc83f7		SM		8400	KG		4500000002		1626156000
3	101	S	BB-R09	WE	GR_raw_4711_R09	13be84a96af004e5		SM		2500	ST		4500000003		1626415856
4	101	S	BB-F12	WR	GR_Finish_4711_F12	d715461ff000ee8c		MT		24000	ST	5001			1626417000
5	261	H	BB-R02	WR	GR_raw_4710_R02	d715461ff000ee8c	b602c9b113c41a7	MT		7200	KG	5001			1626417000
6	261	H	BB-R05	WR	GR_raw_4710_R05	d715461ff000ee8c	b602c9b113c41a7	MT		8400	KG	5001			1626417000
7	261	H	BB-R06	WR	GR_raw_4710_R06	d715461ff000ee8c	b157462d40cc83f7	MT		8400	KG	5001			1626417000
8	601	H	BB-F12	WA	GR_Finish_4711_F12	m14adskajfs4832ka	d715461ff000ee8c	DT	LOGISTIC-MSP	4464	ST		80000000		1626417800
9	601	H	BB-F12	WA	GR_Finish_4711_F12	m14adskajfs4832ka	d715461ff000ee8c	DT	LOGISTIC-MSP	4191	ST		80000000		1626417800
10	601	H	BB-F12	WA	GR_Finish_4711_F12	m14adskajfs4832ka	d715461ff000ee8c	DT	LOGISTIC-MSP	4608	ST		80000000		1626417800
11	601	H	BB-R05	WA	GR_raw_4710_R05	e7sdf32deidf232aa	d715461ff000ee8c	DT	LOGISTIC-MSP	75600	KG		80000001		1626417890
12	601	H	BB-F12	WA	GR_Finish_4711_F12	as60jes2334589kdj	m14adskajfs4832k	DT	LOGISTIC-MSP	3989	ST		80000002		1626417950
13	601	H	BB-F12	WA	GR_Finish_4711_F12	as60jes2334589kdj	m14adskajfs4832k	DT	LOGISTIC-MSP	4687	ST		80000002		1626417950
14	601	H	BB-F12	WA	GR_Finish_4711_F12	as60jes2334589kdj	m14adskajfs4832k	DT	LOGISTIC-MSP	2061	ST		80000002		1626417950
#	BWART	SHKZG	MATNR	VGART_MK	CHARG	TXIDNEW	TXIDOLDTXIDOLD	TXEVENT	EXTERNOWNER	MENGE	MEINS	AUFNR	XBLNR_MKPF	SERIENNU	TIMESTAMPERP
1	101	S	BB-F12	WE	GR_Finish_4711_F12	1b0792e51e1c6c89	as60jes2334589kd	ST	LOGISTIC-MSP	10737	ST		4500000004		1628597560
2	101	S	BB-R07	WE	GR_raw_4712_R07	ak32askdfj834512a		SM		7200	KG		4500000005		1628597650
3	101	S	BB-R09	WE	GR_raw_4712_R09	ak32askdfj834512a		SM		84000	KG		4500000005		1628597650
4	101	S	BB-R05	WE	GR_raw_4710_R05	497alk3237629000	e7sdf32deidf232a	ST	LOGISTIC-MSP	75600	KG		4500000006		1628597777
5	101	S	BB-F15	WR	GR_Finish_4712_F15	uf57281atwoe0877		MT		17252	ST	5002			1628597800
6	101	S	BB-F30	WR	GR_Finish_4712_F30	uf57281atwoe0877		MT		20000	ST	5002			1628597800
7	261	H	BB-R07	WR	GR_raw_4712_R07	uf57281atwoe0877	ak32askdfj834512	MT		7200	KG	5002			1628597800
8	261	H	BB-R09	WR	GR_raw_4712_R09	uf57281atwoe0877	ak32askdfj834512	MT		8400	KG	5002			1628597800
9	261	H	BB-F12	WR	GR_Finish_4711_F12	uf57281atwoe0877	1b0792e51e1c6c8	MT		8400	ST	5002			1628597800
10	601	H	BB-F15	WA	GR_Finish_4712_F15	7016484da7f4b3fe	uf57281atwoe087	DT	LOGISTIC-MSP	4464	ST		80000002		1628598200
11	601	H	BB-F15	WA	GR_Finish_4712_F15	7016484da7f4b3fe	uf57281atwoe087	DT	LOGISTIC-MSP	4191	ST		80000002		1628598200
12	601	H	BB-F15	WA	GR_Finish_4712_F15	7e67f3a9e3a35485	7016484da7f4b3fe	DT	LOGISTIC-MSP	4608	ST		80000003		1628598230
13	601	H	BB-F15	WA	GR_Finish_4712_F15	59611db42cef6501	7e67f3a9e3a3548	DR	B2C/B2B outside I	3989	ST		80000004		1628598300
14	101	S	BB-F16	WR	GR_Finish_4712_F16	42fas439p97fgxc54		MT		16378	ST	5003			1628598370
15	261	H	BB-R05	WR	GR_raw_4710_R05	42fas439p97fgxc54	497alk3237629000	MT		7200	KG	5003			1628598370
16	261	H	BB-R09	WR	GR_raw_4712_R09	42fas439p97fgxc54	uf57281atwoe087	MT		8400	KG	5003			1628598370
17	261	H	BB-F12	WR	GR_Finish_4711_F12	42fas439p97fgxc54	uf57281atwoe087	MT		2337	ST	5003			1628598370
18	261	H	BB-F16	WA	GR_Finish_4712_F16	8223ads32i823ajife	42fas439p97fgxc5	DT	LOGISTIC-MSP	8400	ST		80000005		1628598500
19	601	H	BB-F16	WA	GR_Finish_4712_F16	8223ads32i823ajife	42fas439p97fgxc5	DT	LOGISTIC-MSP	3989	ST		80000005		1628598500
20	601	H	BB-F16	WA	GR_Finish_4712_F16	212jeiefd2839kjase	8223ads32i823ajif	DR	B2C/B2B outside I	3989	ST		80000006		1628598723

Abbildung C.6.12: End-to-End-Betrachtungen: Middleware, ERP-Anpassungen und Systembetrieb

kann. Wir haben die Middleware als Prototyp in Python implementiert und mit unserer Hyperledger Fabric verknüpft. Mit einem simulierten Batch-Datensatz werden die Vorgänge aus einer Materialbewegungstabelle (MSEG) auf die Blockchain übertragen. Abbildung C.6.12 zeigt eine vereinfachte Darstellung von zwei ERP-Systemen mit den entsprechenden Warentransaktionen für den Prozess Source, Make, Deliver. Um die Integration in ein Blockchain-Netzwerk und die Token-Logik zu ermöglichen, mussten wir die Standardtabelle um zusätzliche Felder (TXIDNEW, TXIDOLD, EXTERNOWNER) ergänzen. In diesem Papier können wir zunächst zeigen, dass alte TXIDs für neue Transaktionen verwendet werden, die vom ERP-System an die Blockchain übertragen werden. Die Middleware pflegt dann neue TXIDs aus der Blockchain für das Datenmodell der ERP-Systeme. Abbildung C.6.11 zeigt auch die Funktionalität für systemübergreifende Übergänge. Im TXEvent DT (System 1 Zeile 14) und ST (System 2 Zeile 1) werden IDs weitergegeben, um den Warenfluss systemübergreifend nachvollziehbar zu machen.

4.7 Fazit

In diesem Kapitel werden unsere Forschungsziele für Wissenschaft und Industrie formuliert und eine prototypische Implementierung durchgeführt. Wir erläutern unsere angewandte Forschungsmethodik und präsentieren die Forschungsergebnisse. Obwohl es die Blockchain-Technologie bereits seit mehr als einem Jahrzehnt gibt, sind das Wissen über sie und ihre Auswirkungen auf Geschäftsprozesse noch immer unklar. Es werden verständliche und einfache Standards benötigt, um eine globale Perspektive auf Prozesse und Daten zu entwickeln. Die künftige Herausforderung und Verbreitung der Technologie wird daher davon abhängen, inwieweit ERP-Anbieter und Unternehmen Blockchain-Systeme entwickeln, die eine gemeinsame standardisierte Sprache in heterogenen IT-Liefernetzwerken ermöglichen. In unserer ersten Forschungsfrage haben wir untersucht, wie ein Token-basiertes Blockchain-System gestaltet werden kann, um Produkte über Unternehmens- und Systemgrenzen hinweg zu verfolgen. Aus diesen An-

forderungen ergaben sich allgemeingültige Designprinzipien, die verallgemeinerbar für ERP- und Blockchain-Systeme genutzt werden können. Unsere zweite Forschungsfrage konzentrierte sich auf die Untersuchung von semantischen und syntaktischen Blockchain-Standards, um die Rückverfolgbarkeit von Produkten mit mehreren ERP-Systemen zu ermöglichen. Zur Beantwortung dieser Forschungsfrage verwendeten wir das SCOR-Referenzmodell und die technischen Eigenschaften von Token, um einen einfachen Standard für die Kernprozesse eines Liefernetzwerks zu entwerfen. Wir haben auch Middleware verwendet, um zu zeigen, wie ERP-Systeme modifiziert werden müssen, um mit Token zu arbeiten und eine gemeinsame standardisierte Sprache in heterogenen IT-Liefernetzwerken zu ermöglichen.

5 Abgleich der Ergebnisse mit der Anforderungsdefinition

Das folgende Kapitel fasst die Ergebnisse der Machbarkeitsstudie zum Abschluss der **Projektphase C Plattformkonzeption** zusammen. Zusätzlich wird die Anforderungskonformität der Plattformkomponenten mit den zu Beginn aufgestellten Anforderungen an die Kollaborationsplattform abgeglichen. Umfang der Machbarkeitsstudie ist die Überprüfung der technischen Machbarkeit in Form eines umfassenden Simulators, welcher die Kernfunktionalitäten der Plattformkonzeption sicherstellt.

Dimension Plattform-Implementierung. Die Anforderungsdefinition hinsichtlich der Plattformimplementierung umfasst die Definition des Blockchain-Typs, der Blockchain-Implementierung sowie des verwendeten Konsens-Algorithmus. Der Blockchain-Typ sollte für die Kollaborationsplattform in Form einer Konsortial-Blockchain implementiert werden (REQ1). Aus der existierenden Auswahl an Softwareplattformen für die Umsetzung einer Blockchain im Supply Chain Management Umfeld wurde Hyperledger Fabric als Plattform ausgewählt. Zusätzlich geht aus der Anforderungserhebung hervor, dass der gewählte Konsensalgorithmus und Knotenstruktur eine gleichmäßige Verteilung der Konsensbildung auf alle Anwender der Kollaborationsplattform ermöglicht sowie die Möglichkeit besteht, dass diese in Form einer kontinuierlichen Dienstleistung ausgelagert werden kann.
Für einen ersten Machbarkeitsnachweis wurde ein Hyperledger Fabric Netzwerk auf einem Linux Server instanziiert, um die Blockchain-Komponente der Blockchain-basierten Kollaborationsplattform zu testen.
Innerhalb dieses Fabric-Netzwerks wurde mithilfe eines simulierten Batch-Prozesses einer Make-to-Stock Produktion prototypisch ein Wertschöpfungsszenario mit Blockchain-ERP-Integration simuliert. Für jedes ERP-System wurde ein Benutzer und eine Organisation angelegt, um den Konsensalgorithmus sowie die Knotenstruktur prototypisch zu prüfen. Konsensus umfasst in Hyperledger Fabric mehr als nur Konsensbildung über die Reihenfolge von Transaktionen und definiert die Überprüfung der Korrektheit einer Reihe von Transaktionen, die einen Block bilden. Deshalb verwendet Hyperledger Fabric Orderer-Knoten zur Konsensbildung. Für die Implementierung des Ordering Services zur Konsensbildung wurde zunächst Apache Kafka eingerichtet, da Kafka seit Fabric v1.0 verfügbar ist. Seit Fabric v1.4.1 ist der Einsatz eines Raft-basierten Ordering Services für die Konsensbildung möglich, weshalb dieser als aktuelle Lösung eingesetzt wurde. Beide Ordering Services sind Crash Fault Tolerance (CFT)-Konsensus-Implementierungen.
Hinsichtlich der Ausgestaltung der Transaktionen im Netzwerk bietet Hyperledger Fabric ein hohes Maß an Flexibilität für die Gestaltung von Token zur Abbildung von Lieferkettenprozesse. Für die prototypische Implementierung haben wir einen hybriden Token-Ansatz verwendet, der „Colored Coin“ genannt wird. Dieser Token Ansatz basiert auf dem UTXO-Modell und bietet die erforderlichen Eigenschaften, die für eine Rückverfolgung von Produkten notwendig sind. Hinsichtlich der Plattform-Implementierung konnten prototypisch die Kernfunktionalitäten der Kollaborationsplattform abgebildet und ein positiver technischer Machbarkeitsnachweis dargelegt werden.

Dimension Datenspeicherung, Datenaustausch und Datenschutz. Mit der prototypischen Integration zweier ERP Systeme in ein Hyperledger Fabric Netzwerk konnten die Anforderungen an die Datenspeicherung ausgetestet werden. Auf der Konsortial-Blockchain wurden nur Datensätze gespeichert, welche für die unmittelbare Rückverfolgbarkeit innerhalb von Netzwerken notwendig sind (REQ6). Zusätzlich wurde prototypisch evaluiert, wie Daten, welche nicht auf der Blockchain gespeichert werden sollen, mithilfe von kryptografischen Hash-Funktionen auf Unveränderlichkeit überprüft werden können (REQ7). Für die Speicherung von Daten außerhalb der Blockchain wurden dezentrale Datenspeicherungslösungen, wie IPFS, prototypisch für die Kollaborationsplattform getestet. IPFS (Inter Planetary File System) ist ein versioniertes und verteiltes Dateispeicher- und Freigabesystem und kann mit verschiedenen Transportschichtprotokollen wie TCP, uT, UDT etc. verwendet werden. Jede mit IPFS hochgeladene Datei ist

mit einem eindeutigen Hash verknüpft. IPFS verfügt über eine eingebaute Sicherheit, da der Hash der angeforderten Datei und der bereitgestellten/heruntergeladenen Datei immer überprüft werden kann (REQ9).
Für den Austausch von Daten war eine Anforderung an die Blockchain-Komponente der Kollaborationsplattform das Festlegen eines gemeinsamen Datenformats zwischen den ERP-Systemen. Ebenso wurde die Anforderung aufgestellt, dass die Kollaborationsplattform standardisierte Dateistrukturen unterstützen können muss. Darüber hinaus sollte für eine standardisierte und automatisierte Speicherung von Produktionsdaten auf der Blockchain eine Schnittstelle zur Verfügung stehen, welche den Datenaustauschstandard OPC-UA unterstützt.
Mit der prototypischen Implementierung des UTXO-Modells zur Integration zweier ERP-Systeme konnte eine Datenaustauschstruktur initial festgelegt werden (REQ10). Zur Unterstützung standardisierter Dateistrukturen wie JSON bietet Hyperledger Fabric LevelDB oder CouchDB. LevelDB speichert Daten als einfache Key-Value Paris und unterstützt nur Schlüssel-, Schlüsselbereichs- und zusammengesetzte Schlüsselabfragen. CouchDB dahingegen unterstützt Daten im Ledger als JSON zu modellieren und umfangreiche Abfragen auf Datenwerte, anstatt auf Schlüssel zu stellen. Deshalb wurden die Peer Knoten innerhalb des prototypischen Netzwerks mit CouchDB instanziiert (REQ12). Zusätzlich wurde für den Aufbau einer Echtzeiteventarchitektur für Produktionsdaten die technische Machbarkeit der Implementierung des Datenaustausch-standards OPC-UA auf der Kollaborationsplattform getestet (REQ13).
Die definierten Datenschutzanforderungen an die Kollaborationsplattform wurden von technischer Seite her getestet. Hyperledger Fabric bietet für jeden Peer zwei Kommunikationsschnittstellen, welche die Peer-to-Peer Kommunikation und Knoten zu Eigentümer Kommunikation unterstützen. Peers können miteinander und mit Anwendungen auf sogenannten Channels miteinander interagieren (REQ2, 15). Channels sind ein Mechanismus, mit welchem die verschiedenen Komponenten innerhalb eines Fabric-Netzwerks private Transaktionen durchführen können. Unternehmensarchitekturen können in Fabric-Blockchain-Netzwerken über Organisationen abgebildet werden, welche auf mehreren Peers aufgebaut werden. Darüber hinaus gibt es eine Zertifizierungsstelle, die die digitalen Identitäten der Netzwerkteilnehmer verwaltet. Eine zen-trale Rolle hat insbesondere der Membership Service Provider inne, welcher die Netzwerkteilnehmer, ihre Rollen und Zugriffsrechte basierend auf der Zertifizierungsstelle und durch Auflistung der Teilnehmer-IDs identifiziert. Diese technischen Eigenschaften erfüllen die Anforderung an ein mehrstufiges Rechtesystem für die Blockchain-basierte Kollaborationsplattform. Insbesondere können Lese- und Schreibrechte verschiedener Teilnehmer im Netzwerk festgelegt werden (REQ14, 15, 16, 17).

Positiver Machbarkeitsnachweis. Abschließend stellen wir fest, dass sich Hyperledger Fabric als Open-Source-Plattform für genehmigungspflichtige dezentrale Kollaborationsplattformen eignet. Hyperledger Fabric unterscheidet sich von anderen Konsortial-Blockchains vor allem hinsichtlich ihrer Mitgliedschaftsdienste und ihrer modularen Architektur, die eine Anpassung an bestimmte Anwendungsfälle und Vertrauensmodelle ermöglicht. Die prinzipielle Durchführbarkeit der Initiierung einer Blockchain-basierten Kollaborationsplattform für Wertschöpfungsnetzwerk-szenarien konnte mit der Entwicklung der prototypischen Implementierung und Simulation, welche die Kernfunktionalitäten aufweist, festgestellt werden.

Literatur

Agarwal, Ritu, und Jayesh Prasad. 1997. „The Role of Innovation Characteristics and Perceived Voluntariness in the Acceptance of Information Technologies“. *Decision Sciences* 28(3):557–82.

Anand, A., M. McKibbin, und F. Pichel. 2017. „Colored Coins: Bitcoin, Blockchain, and Land Administration – Cadasta“. in *2017 WORLD BANK CONFERENCE ON LAND AND POVERTY*. Washington DC: The World Bank.

Asprion, Petra, Philipp Hübner, und Pascal Moriggl. 2019. „Towards a Distributed Ledger System for Supply Chains“ herausgegeben von T. Bui. *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Beck, R., M. B. Kildetoft, und N. Radonic. 2020. „Using Blockchain to Sustainably Manage Containers in International Shipping“. *ICIS 2020 Proceedings*.

Bocek, Thomas, Bruno B. Rodrigues, Tim Strasser, und Burkhard Stiller. 2017. „Blockchains everywhere - A use-case of blockchains in the pharma supply-chain“. *Proceedings of the IM 2017 - 2017 IFIP/IEEE International Symposium on Integrated Network and Service Management* 772–77.

Vom Brocke, Jan, Alexander Simons, Björn Niehaves, Kai Riemer, Ralf Plattfaut, und Anne Cleven. 2009. „Reconstructing the giant: On the importance of rigour in documenting the literature search process“. S. 161 in *17th European Conference on Information Systems, ECIS 2009*.

Buer, Sven Vegard, Jan Ola Strandhagen, und Felix T. S. Chan. 2018. „The link between Industry 4.0 and lean manufacturing: mapping current research and establishing a research agenda“.

Chen, Si, Rui Shi, Zhuangyu Ren, Jiaqi Yan, Yani Shi, und Jinyu Zhang. 2017. „A Blockchain-Based Supply Chain Quality Management Framework“. S. 172–76 in *Proceedings - 14th IEEE International Conference on E-Business Engineering, ICEBE 2017 - Including 13th Workshop on Service-Oriented Applications, Integration and Collaboration, SOAIC 207*. Institute of Electrical and Electronics Engineers Inc.

Chorafas, Dimitris N. 2001. *Integrating ERP, CRM, Supply Chain Management, and Smart Materials Library of Congress Cataloging-in-Publication Data*. CRC Press LLC.

Corbin, Juliet M., und Anselm Strauss. 1990. „Grounded theory research: Procedures, canons, and evaluative criteria“. *Qualitative Sociology* 13(1):3–21.

Doller, A. 2013. „Chargenverwaltung mit SAP“. in *SAP: Logistik*. Rheinwerk Verlag GmbH.

Felipe Munoz, Mario, Kaiwen Zhang, Aamir Shahzad, und Mustapha Ouhimmou. 2021. „LogLog: A Blockchain Solution for Tracking and Certifying Wood Volumes“. *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* 1-9 TS-CrossRef.

Fleig, Christian, Dominik Augenstein, und Alexander Mädche. 2018. „Process Mining for Business Process Standardization in ERP Implementation Projects – An SAP S/4 HANA Case Study from Manufacturing“. in *16th International Conference*.

Fröwis, Michael, Andreas Fuchs, und Rainer Böhme. 2019. „Detecting Token Systems on Ethereum“. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11598 LNCS:93–112.

Fu, Katherine K., Maria C. Yang, und Kristin L. Wood. 2015. „Design Principles: The Foundation of Design“. *Volume 7: 27th International Conference on Design Theory and Methodology*.

Ghode, Dnyaneshwar J., Rakesh Jain, Gunjan Soni, Sunil K. Singh, und Vinod Yadav. 2020. „Architecture to Enhance Transparency in Supply Chain Management using Blockchain Technology“. *Procedia Manufacturing* 51:1614–20.

Glaser, B., und A. Strauss. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. London: Wiedenfeld and Nicholson M4

Hader, Manal, Abderrahman El Mhamedi, und Abdellah Abouabdellah. 2021. „Blockchain Integrated ERP for a Better Supply Chain Management“. *2021 The 8th International Conference on Industrial Engineering and Applications(Europe)* 193-197 TS-CrossRef.

Hastig, Gabriella M., und Man Mohan S. Sodhi. 2020. „Blockchain for Supply Chain Traceability: Business Requirements and Critical Success Factors“. *Production and Operations Management* 29(4):935–54.

Heng, Stefan. 2014. „Industry 4.0: Upgrading of Germany's Industrial Capabilities on the Horizon“. *SSRN*.

Hevner, Alan R., Salvatore T. March, Jinsoo Park, und Sudha Ram. 2004. „Design science in information systems research“. *MIS Quarterly: Management Information Systems* 28(1):75–105.

Kim, Mark, Brian Hilton, Zach Burks, und Jordan Reyes. 2018. „Integrating Blockchain, Smart Contract-Tokens, and IoT to Design a Food

Traceability Solution“. *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* 335-340 TS-CrossRef.

Kuechler, Bill, und Vijay Vaishnavi. 2008. „On theory development in design science research: anatomy of a research project“. *European Journal of Information Systems* 17(5):489–504.

Kuhn, Marlene, Felix Funk, Guanlai Zhang, und Jörg Franke. 2021. „Blockchain-based application for the traceability of complex assembly structures“. *Journal of Manufacturing Systems* 59:617–30.

Kuzuno, Hiroki, und Christian Karam. 2017. „Blockchain explorer: An analytical process and investigation environment for bitcoin“. *eCrime Researchers Summit, eCrime* 9–16. doi: 10.1109/ECRIME.2017.7945049.

Lu, Qinghua, und Xiwei Xu. 2017. „Adaptable Blockchain-Based Systems: A Case Study for Product Traceability“. *IEEE Software* 34(6):21–27.

Mendling, Jan, Gero Decker, Hajo A. Reijers, Richard Hull, und Ingo Weber. 2018. „How do Machine Learning, Robotic Process Automation, and Blockchains Affect the Human Factor in Business Process Management?“ *Communications of the Association for Information Systems* 43(1):19.

Miehle, Daniel, Dominic Henze, Andreas Seitz, Andre Luckow, und Bernd Bruegge. 2019. „PartChain: A Decentralized Traceability Application for Multi-Tier Supply Chain Networks in the Automotive Industry“. *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)* 140-145 TS-CrossRef.

Möller, Frederik, Tobias Moritz Guggenberger, und Boris Otto. 2020. „Towards a Method for Design Principle Development in Information Systems“. S. 208–20 in *Designing for Digital Transformation. Co-Creating Services with Citizens and Industry*. Bd. 12388, *Lecture Notes in Computer Science TS - CrossRef*, herausgegeben von S. Hofmann, O. Müller, und M. Rossi. Cham: Springer International Publishing.

Mondal, Saikat, Kanishka P. Wijewardena, Saranraj Karuppuswami, Nitya Kriti, Deepak Kumar, und Premjeet Chahal. 2019. „Blockchain inspired RFID-based information architecture for food supply chain“. *IEEE Internet of Things Journal* 6(3):5803–13.

Nakamoto, Satoshi. 2008. „Bitcoin: A peer-to-peer electronic cash system“. *Decentralized Business Review* 1260.

Rejeb, Abderahman, John G. Keogh, Steven J. Simske, Thomas Stafford, und Horst Treiblmaier. 2021. „Potentials of blockchain technologies for supply chain collaboration: a conceptual framework“. *International Journal of Logistics Management* 32(3):973–94.

Scherer, Mattias. 2017. *Performance and Scalability of Blockchain Networks and Smart Contracts*.

Sokolov, B., und A. Kolosov. 2021. „Blockchain Technology as a Platform for Integrating Corporate Systems“. *Automatic Control and Computer Sciences* 55(3):234–42.

Sunyaev, Ali, Niclas Kannengießer, Roman Beck, Horst Treiblmaier, Mary Lacity, Johann Kranz, Gilbert Fridgen, Ulli Spankowski, und André Luckow. 2021. „Token Economy“. *Business & Information Systems Engineering* 63(4):457–78.

Tian, Feng. 2016. „An agri-food supply chain traceability system for China based on RFID & blockchain technology“. *2016 13th International Conference on Service Systems and Service Management, ICSSSM 2016*.

Vaishnavi, Vijay, und Bill Küchler. 2004. „Design Science Research in Information Systems“.

Vial, Gregory. 2019. „Understanding digital transformation: A review and a research agenda“. *The Journal of Strategic Information Systems* 28(2):118–44. doi: 10.1016/j.jsis.2019.01.003 M4 - Citavi.

Vogelsteller, Fabian, und Vitalik Buterin. 2015. „ERC-20 token standard“. *Ethereum Foundation (Stiftung Ethereum)*.

Wang, Yingli, Jeong Hugh Han, und Paul Beynon-Davies. 2019a. „Understanding blockchain technology for future supply chains: a systematic literature review and research agenda“. *Supply Chain Management* 24(1):62–84.

Wang, Yingli, Jeong Hugh Han, und Paul Beynon-Davies. 2019b. „Understanding blockchain technology for future supply chains: a systematic literature review and research agenda“. *Supply Chain Management: An International Journal* 24(1):62–84.

Webster, Jane;, und Richard T. Watson. 2002. „Analyzing the Past to Prepare for the Future: Writing a Literature Review“. *MIS Quarterly* 26(2):13–23.

Westerkamp, M., F. Victor, und A. Küpper. 2018. „Blockchain-Based Supply Chain Traceability: Token Recipes Model Manufacturing Processes“. S. 1595–1602 in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing*

(CPSCom) and IEEE Smart Data (SmartData).

Westerkamp, Martin, Friedhelm Victor, und Axel Küpper. 2020. „Tracing manufacturing processes using blockchain-based token compositions“. *Digital Communications and Networks* 6(2):167–76.

Zhou, Honggeng, W. C. Benton, David A. Schilling, und Glenn W. Milligan. 2011. „Supply Chain Integration and the SCOR Model“. *Journal of Business Logistics* 32(4):332–44.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PiMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PiMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Lehrstuhl für BWL und Wirtschaftsinformatik
Prof. Dr. Axel Winkelmann
Sanderring 2
97070 Würzburg

Autoren und Ansprechpartner

Norman Pytel, M.Sc.

Wissenschaftlicher Mitarbeiter
norman.pytel@uni-wuerzburg.de
+49 0931 31-86348

Christian Zeiß, M.Sc.

Wissenschaftlicher Mitarbeiter
christian.zeiss@uni-wuerzburg.de
+49 0931 31-88518

Myriam Schaschek, M.Sc.

Wissenschaftliche Mitarbeiterin
myriam.schaschek@uni-wuerzburg.de
+49 0931 31-87662

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 931 31-89640

– Inhaltsverzeichnis Arbeitspaket D –

In AP D – Plattformimplementierung - sind unterschiedliche Anforderungen aus AP C umgesetzt worden. Es wurden dabei Anwendungsfälle der Konsortialpartner im Bereich Produktions- und Qualitätsbereich adressiert.

D Abstract Kapitel. Einführung in Plattformansätze und Zusammenarbeit des Konsortiums zu Teilkomponenten.

D1 Implementierung der Blockchain. Umsetzung von Netzwerk und Implementierung der Hyperledger Fabric.

D2 Implementierung von Smart Contracts. Gestaltung und Installation von Smart Contracts sowie Überblick zu Prozessautomaten zur automatisierten Daten-integration aus Informationssystemen in die Plattform.

D3 Entwicklung der Datenaustauschstruktur. Untersuchung von zentralen und dezentralen Ansätzen zur Gestaltung und Integration von Informationsflüssen.

D4 Implementierung der Eventarchitektur. Technische und praktische Evaluation der in AP C definierten Eventarchitektur anhand eines Industrie 4.0 – Szenarios.

D5 Entwicklung des Front-Ends. Visualisierung von Problemen und aussagekräftige Darstellung der Kommunikation in mehreren Front-Ends.

D6 Integration von Teilkomponenten. Zur Sicherstellung der Funktionalitäten der finalen Plattformen ist die Integration der Teilkomponenten von den Partnern aus bisherigen Use-Cases und APs notwendig.

D7 Umsetzung von Datenschutz und Datensicherheit. Kritische Betrachtung von Datenschutz- und Sicherheit bei Anwendungsfällen der Nutzung von Informations-systemen über Unternehmensgrenzen hinaus.

D8 Geschäftsmodellanalyse- und Management. Identifikation von nachhaltigem und innovativem Geschäftsmodell für die Plattform.

– Plattformimplementierung Arbeitspaket D –

Im folgenden Kurzbericht wird eine Orientierungshilfe für die acht Teilergebnisse des Arbeitspaketes D geliefert. Ziel ist es, den Leser zu unterstützen und einen Überblick über die Projektarbeiten und die implementierten Anwendungsfälle zu geben. Hierzu werden die Softwareanbieter, Anwendungspartner und Abhängigkeiten mit der universitären Einrichtung dargestellt, um gemeinsame Projekttätigkeiten besser nachvollziehen zu können.

1 Überblick der Arbeitspakete

Im Arbeitspaket D (Plattformimplementierung) sind unterschiedliche Anforderungen aus Arbeitspaket C umgesetzt worden. In iterativen Schritten wurden durch teilnehmende Projektpartner acht Teilpakete D1-D8 für verschiedene Anwendungsfälle aus dem Produktions- und Qualitätsbereich erstellt. Hierbei sind die Partner Actiware, Infosim, Signavio, Universität Würzburg sowie die teilnehmenden Anwendungsunternehmen (AU) Robur Automation und Maul Theet mit je unterschiedlichem Fokus aus ihrem eigenen Kompetenzgebiet in zahlreichen Workshoprunden physisch und digital zusammengekommen, um die Zielstellungen der AU zu behandeln, die unten beispielhaft formuliert sind:

- Flexibilisierung von Transaktionen / des Informationsaustausches mit anderen Unternehmen des Wertschöpfungsnetzwerks zur Absicherung der Produktion
- Erhöhung der Kundenzufriedenheit in Bezug auf die sichere Dokumentation von Produktionsstörungen und Erhöhung der Reaktionsfähigkeit über die eigenen Unternehmensgrenzen hinaus
- Qualitätssicherung und Steigerung der Datenqualität in Bezug auf die Rückverfolgung von Produkten und Messgeräten

Um individuelle Zielstellungen und verschiedene Kompetenzen zu bündeln, wurden zur Zielerreichung die folgenden acht Arbeitspakete definiert.

D1: Implementierung der Blockchain
In diesem Kapitel wird die Umsetzung des Netzwerkes und die Implementierung der Blockchain mittels Hyperledger Fabric beschrieben.

D2: Implementierung von Smart Contracts
Darauf aufbauend wurde auf der Hyperledger Fabric ein Smart Contract implementiert, dessen Logik zunächst an die Informationssysteme der teilnehmenden Anbieter integriert ist. Darüber hinaus bietet das Kapitel einen Überlick über verschiedene transparente und einfache grafische Oberflächen zur Gestaltung und Bildung von Prozessautomaten, die eine automatische Integration von Daten in die Plattform ermöglichen.

D3: Entwicklung der Datenaustauschstruktur
Im Bereich der Datenaustauschstruktur werden zentrale und dezentrale Ansätze zur Gestaltung und Integration von Datenflüssen verschiedener Informationssysteme behandelt. Hierzu wird zum einen nach einem zentralen, anpassungsfähigen Datenmodell und zum anderen einem dezentralen und standardisierten Ansatz vorgegangen. Es zeigte sich während der Umsetzung der Projekte, dass unterschiedliche Datenstrukturmodelle anwendbar sind. Die Ansätze sind in Verknüpfung eines Qualitäts-Anwendungsfalls beschrieben, um eine Vergleichbarkeit anhand eines einfachen Szenarios zu ermöglichen.

D4: Implementierung der Eventarchitektur
Auf Basis der in Arbeitspaket C definierten Eventarchitektur wird innerhalb dieses Kapitels eine Blockchain-basierte Evaluierung vorgenommen. Hierbei wird die implementierte Hyperledger Fabric Blockchain genutzt, um anhand eines Industrie 4.0 Szenarios eine technische und praktische Machbarkeit der Eventarchitektur zu überprüfen. Das Anwendungsszenario beinhaltet eine simulierte Produktionsüberwachung, welche durch ein Fischertechnik-Modell realisiert wird. Durch den erhöhten Sensorikumfang sowie der hohen Abgriffsfrequenz wird ebenso überprüft und diskutiert, inwiefern die Blockchain-Technologie per se für den Einsatz einer Echtzeitüberwachung geeignet ist.

D5: Entwicklung des Front Ends
Um effizienten Zugriff auf die Informationen der verschiedenen Teilkomponenten zu ermöglichen, wurden mehrere Front-Ends für die Plattformen entwickelt. Primäre Aufgaben der Front-Ends sind eine aussagekräftige Darstellung der Kommunikation einzelner Komponenten und die Visualisierung von entstandenen Problemen. Details zur Umsetzung und den jeweils zugehörigen Plattformkomponeten der Front-Ends finden sich in diesem Kapitel. Ebenfalls werden Hintergründe für die Entscheidung genannt, mehrere Front-Ends zu entwickeln.

D6: Integration der Teilkomponenten
Über die verschiedenen Use Cases und Arbeitspakete hinweg wurde von den Partnern an mehreren separaten Teilkomponenten für die Plattformen gearbeitet. Für die Umsetzung der geplanten Funktionalitäten der finalen Plattformen war es notwendig, die Komponenten zu kombinieren. In diesem Kapitel werden erst die hierfür verwendeten Teilkomponenten beschrieben und anschließend wird auf das Vorgehen bei deren Integration zu den Plattformen eingegangen.

D7: Datenschutz, Datensicherheit & Zertifizierung
Die Integration von traditionellen Informationssystemen über Unternehmensgrenzen hinaus erfordern ein Umdenken in der Ausgestaltung von Datenschutz und Datensicherheitsaspekten. In diesem Ergebnisteil werden die verschiedenen Anwendungsfälle aus unterschiedlichen Perspektiven betrachtet und Limitiationen zu Zertifzierungsmöglichkeiten diskutiert, die in zukünftigen Blockchainprojekten berücksichtigt und kritisch betrachtet werden sollten.

D8: Geschäftsmodellanalyse und management
Zur Identifikation eines nachhaltigen und innovativen Geschäftsmodells für die entwickelte Platt-

form wird eine Geschäftsmodellanalyse durchgeführt. Die AU betrachten hierbei die Erweiterung und Ausbaumöglichkeiten eines digitalen Angebots zum Teilen von Daten in Wertschöpfungsnetzwerken.

2 Einführung in verschiedene Plattformansätze und Teilkomponenten

Die Gestaltung verschiedener Blockchain Plattformen ist grundsätzlich abhängig von den formulierten Business Requirements eines Konsortiums und dem potentiellen Mehrwert, der sich durch den Einsatz der Blockchain ergibt (Hastig et al. 2020). Die Partner des Konsortiums bringen zur Gestaltung der gesetzten Zielstellungen verschiedene **Kompetenzen** in das Projekt mit ein, um die Verbesserung von **Produktion**s- und **Qualitäts**prozessen zu erreichen. Die unten stehende Darstellung bietet hierfür einen kurzen Überblick über zwei verschiedene Plattformansätze P1 und P2 für den Qualitäts- und Produktionsbereich.

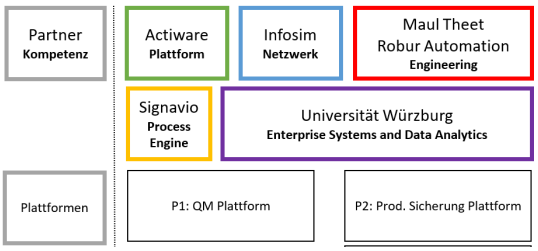


Abbildung D.0.1: Übersicht Partner, Plattformen und Teilkomponenten

Partnerkompetenzen zur Gestaltung der Plattformen:

Maul Theet:

Das kleine Unternehmen mit weniger als 10 Mitarbeitern befindet sich im regulierten Produktionsumfeld verschiedener großer Unternehmen und Forschungseinrichtungen und produziert hoch komplexe Messgeräte und Prüfstände, mit denen sicherheitsrelevante Bauteile gemessen werden. Die Sicherheit und Nachweispflicht dieser Produkte wird nach Ansicht des Unternehmens steigen, sodass das Unternehmen die Eigenschaften der Blockchain zum sicheren und transparenten Austausch von Daten nutzen kann.

ROBUR Automation:

ROBUR Automation ist ein mittelständischer Automatisierungsdienstleister mit ca. 100 Mitarbeitern in den Bereichen Engineering, Softwareentwicklung und technische Dokumentation mit Sitz in Niedernberg in Unterfranken. ROBUR Automation ist Teil der Robur Industry Services Group, einem Verbund von 28 Unternehmen im Bereich Industrial Services. Den Schwerpunkt bildet die intelligente Automatisierung von Arbeitsplätzen und Anlagen. Häufig tritt ROBUR Automation als Generalunternehmer auf, der verschiedene Zulieferer koordiniert und die Gesamtlösung für den Kunden umsetzt. Diese Aufgaben beinhalten nachweispflichtige Dokumentation und verbindliche Absprachen, weshalb der Einsatz einer Kollaborationsplattform auf Blockchain-Basis interessant ist.

Actiware:

ACTIWARE bietet als Softwarehersteller und Consultinghaus im Bereich des Enterprise Content Managements umfassende Expertise zur Anbindung unterschiedlicher Datenquellen und deren Verknüpfung in der geschäftlichen Logik. ACTIWARE Development entwickelt dabei ein eigenes ECM System und kann über einen eigenen Prozess- und Formulargenerator Prozesse auf low- bzw. no-code Basis abbilden. Dabei können nicht nur Daten aus dem geschäftlichen Kontext wie ERP und CRM-Systemen genutzt, sondern auch Daten aus dem Bereich IoT integriert werden. Damit wird die Möglichkeit geschaffen, geschäftliche Prozesse abzubilden und die Blockchain sowohl als Speicherort als auch mögliche Smart Contracts als Trigger für Geschäftsprozesse zu nutzen.

Infosim:

Als Hersteller einer automatisierten Netzwerk- und Service-Management Lösung sind die Kernkompetenzen von Infosim Überwachung, Performance-Monitorung und Konfiguration von Netzelementen und IT-Infrastrukturen. Im Rahmen des Projekts konnte Infosim diese Kompetenzen beim Implementieren von Schnittstellen zu Plattformkomponenten und bei der Überwachung der Plattformen vorteilhaft einbringen.

Signavio:

Die von SIGNAVIO angebotene Plattform stellt den derzeitigen State of the Art im Bereich kollaborativer Software für das Geschäftsprozessmanagement dar. Die SIGNAVIO Business Transformation Suite ist ein System von nahtlos integrierten Prozessmanagementprodukten. Die Business Transformation Suite bildet alle Schritte des Geschäftsprozessmanagement-Lebenszyklus ab, kann jedoch auch als Design-, Analyse- und Kollaborationstool in Kombination mit Drittsystemen wie Open Source Prozessausführungsumgebungen (BPX Engines) oder klassischen ERP-Systemen verwendet werden.

Universität Würzburg:

Der Lehrstuhl für BWL und Wirtschaftsinformatik bringt verschiedene Kompetenzen aus dem Bereich Enterprise Systems and Data Analytics zur Gestaltung beider Plattformen mit ein und unterstützt die Projektpartner aus dem Forschungsbereich mit dem Einsatz von innovativen Ansätzen zur Rückverfolgung von digitalen Assets bei der Gestaltung von Prototypen.

3 Zusammenarbeit des Konsortiums zu Komponenten

Im Folgenden wird aufbauend auf den vorigen Darstellungen eine kurze Übersicht der Zusammenarbeiten in verschiedenen **Komponenten** dargestellt. Die Teilkomponenten 1-5 umfassen dabei eine Kurzerklärung der genutzten IT-Infrastruktur, die als Grundlage zur Integration mit einer Blockchain fungierten.

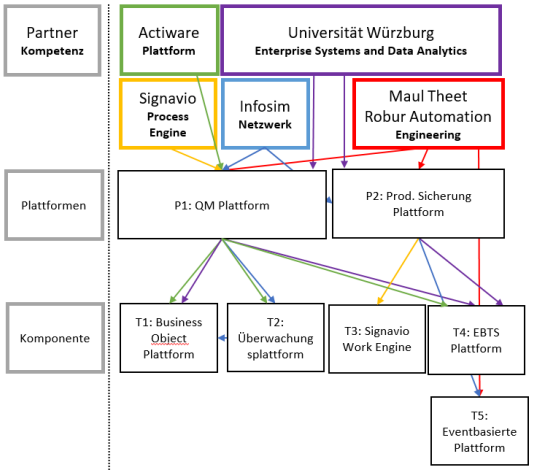


Abbildung D.0.2: Übersicht der Komponenten und gemeinsamen Arbeiten

T1 Actiware:
ACTIWARE hat im Rahmen des Projektes den eigenen Prozessdesigner um Blockchainfunktionalitäten erweitert. Hierzu wurden beginnend mit Hyperledger Fabric Möglichkeiten zu schaffen, Daten zu schreiben und zu konsumieren sowie Smart Contracts auf der Hyperledger Fabric zu konfigurieren. Zugleich wurde das bereits im Consulting verwendete Business-Objekt-Modell für die zugrunde liegenden Fälle adaptiert und für die beiden Fälle der QM-Plattform P1 und der Produktionssicherungsplattform P2 angepasst. Um mit dem Anwender in Kontakt zu treten, wurde ferner ein Formulargenerator entwickelt, der Daten konsumieren und an die Prozessengine zurückgeben kann. Letzteres wurde vor allem im QM-Use-Case gemeinsam mit der Universität Würzburg und Maul-Theet umgesetzt.

T2 Infosim:
Im Rahmen des Projekts hat Infosim in Zusammenarbeit mit Actiware und der Universität Würzburg Komponenten zur Überwachung von sowohl der QM-, als auch der Produktionsabsicherungsplattform entwickelt. Diese wurden in Form einer Erweiterung durch die Installation der StableNet Software von Infosim sowohl bei Actiware als auch bei der Universität zur Überwachung der Plattformen T1 bzw. T5 in die Plattformen P1 bzw. P2 integriert.

T3 Signavio Work Engine:
Technisch verwendet die Business Transformation Suite einen Mix aus NoSQL- und SQL-basierten Datenbanktechnologien in Verbindung mit einer Java-Webservice-Architektur im Backend und modernen Webtechnologien im Frontend. Integrationen mit beliebigen Drittsystemen können über REST-Schnittstellen, die standardisierte Datenaustauschformate (insbesondere BPMN 2.0 XML) unterstützen, realisiert werden.

T4 Universität Würzburg:
Im Rahmen des Projektes erstellte der Lehrstuhl auf Basis eines traditionellen Enterprise Systems ein **Enterprise Blockchain Token System (EBTS)**, das als innovative Möglichkeit zur Rückverfolgung von Produktstrukturen genutzt werden kann. Um dieses Konzept zu implementieren, wurden Anforderungen durch Produkte der Firma Maultheet aufgenommen und mit technischer Unterstützung der Actiware implementiert.

T5 Eventbasierte Plattform:
Im Rahmen des Projektes erstellte der Lehrstuhl anhand der zuvor entwickelten Eventarchitektur eine Plattform, welche eine Machbarkeitsanalyse der Echtzeitüberwachung von Wertschöpfungsprozessen ermöglicht. Grundlagen bieten hierfür neben theoretischen Erkenntnissen zum Thema Referenzarchitektur (Arbeitspaket C5) und die zu Projektbeginn erhobene Anforderungsanalyse (Arbeitspaket B1) auch die in Arbeitspaket D1 implementierte Blockchain-Lösung, das von ROBUR Automation zur Verfügung gestellte Fischertechnik-Modell sowie die von Infosim entwickelte Softwarelösung zur Netzwerkanalyse.

Literaturverzeichnis:

Hastig, Gabriella M., and ManMohan S. Sodhi. "Blockchain for supply chain traceability: Business requirements and critical success factors." Production and Operations Management 29.4 (2020): 935-954.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

MAUL-THEET
Vibration Test & Analysis

actiware®
DEVELOPMENT

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Juniorprofessur für Information Management
Prof. Dr. Christian Janiesch
Stephanstraße 1
97070 Würzburg
https://www.wiwi.uni-wuerzburg.de/lehrstuhl/bwljp1/startseite/

Autoren und Ansprechpartner

Norman Pytel, M.Eng.

Wissenschaftlicher Mitarbeiter
Norman.Pytel@uni-wuerzburg.de
+49 931 31-86348

Lukas-Valentin Herm, M.Sc.

Wissenschaftlicher Mitarbeiter
lukas-valentin.herm@uni-wuerzburg.de
+49 931 31-81730

Dr. Michael Kröhn

Head of Research
ROBUR Automation GmbH
michael.kroehn@robur-automation.com

Michael Baumgart, M.Sc.

Senior Consultant Research & Development
Infosim GmbH & Co. KG
baumgart@infosim.net
+49 931 205 92 200

Julian Kolb, M.Sc.

Wissenschaftlicher Mitarbeiter
Julian.Kolb@uni-wuerzburg.de
+49 0931 31-86166

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 0931 31-89640

D1: Implementierung der Blockchain

Die Kombination verschiedener traditioneller Informationssysteme mit der Blockchainplattform Hyperledger Fabric kann zu neuartigen Ansätzen und innovativen Gestaltungsmöglichkeiten moderner Wertschöpfungsprozesse genutzt werden. Fabric erfüllt dabei mehrere Zwecke, um mithilfe von Smart Contracts verschiedene Events und Automatisierungsmöglichkeiten bereitzustellen, die zu positiven Auswirkungen für mehrere Teilnehmer in Netzwerken führen können. Darüber hinaus ermöglicht die Blockchainplattform mit ihren technischen Eigenschaften zuordenbare Muster wie eine regelmäßige Verifikation von Daten zur Steigerung des Vertrauens von Datenobjekten. Die unterschiedlichen Gestaltungsmöglichkeiten führen zu verschiedenen Plattformansätzen zur Absicherung von Produktions- und Qualitätsanwendungsfällen, die in diesem Ergebnisbericht beschrieben werden.

1 Grundlegende Terminologien

Zu Beginn dieses Kapitels werden die grundlegenden **Begrifflichkeiten** der Blockchain-Plattform Hyperledger Fabric (kurz: Fabric) dargestellt, um verschiedene Plattformansätze P1+P2, Entscheidungen, Herausforderungen sowie Barrieren im Rahmen des Forschungsprojektes besser nachvollziehen zu können. Die Anforderungsanalyse des Arbeitspakets C (vorgelagerter Arbeitsblock) hat ergeben, dass eine Vielzahl von Blockchain-Technologien existieren, bei der besonders Fabric als Enterprise Plattform zur Verwaltung und Integration von verschiedenen Informationssystemen eingesetzt werden kann. Zur grundsätzlichen Auswahl der Blockchain sei auf die Kategorisierung nach Joannou 2020 et al. verwiesen.
Zusätzlich bietet Fabric weitere essenzielle Datenschutz und Datensicherungsfunktionalitäten, um Vertrauen über technische Mechanismen zu garantieren. Dabei handelt es sich u.A. um das Erstellen und Verwalten von Netzwerken zur abgesicherten Kommunikation, das Ausführen von Smart Contracts, die Möglichkeit der Anwendung unterschiedlicher Konsensmechanismen und die Nutzung diverser Services für die sichere Teilnahme am Netzwerk. Wie bereits einführend dargestellt, werden einige der bereits verwendeten Begriffe nachfolgend detaillierter erklärt, um die Einrichtung und Anbindung der Plattform für einen einfachen Anwendungsfall darzustellen.

Peer:
Ein Peer ist ein Server, der dazu dient, Ledger zu speichern und Chaincode auszuführen. Ein Peer gehört immer zu genau einer Organisation im Netzwerk. Er kann mehrere Ledger speichern und gleichzeitig in mehreren Channels sein. Über einen Peer werden Transaktionen auf ein Blockchainnetzwerk gesendet. Ebenso werden Anfragen zum Lesen von Daten aus dem Netzwerk durch einen Peer behandelt.

Ledger:
Ein Ledger besteht aus einer Blockchain und einem Datenspeicher (auch World-State genannt). In der Blockchain werden in jedem Block eine oder mehrere Transaktionen gespeichert, die Geschäftsobjekte ändern. Der World State umfasst eine Liste an Statuswerten für die Objekte. Er dient dazu, eine Berechnung des aktuellen Status der Objekte nicht durch Nachvollziehen aller Transaktionen auf der Blockchain notwendig zu machen.
Bei Fabric hat jeder Channel seine eigene Ledger, es kann also mehrere Ledger bzw. Blockchains im Netzwerk geben. Ein Ledger ist immer einem Channel zugeordnet und umgekehrt.

Channel:
Ein Channel ist ein eigenes Subnetzwerk innerhalb des Gesamtnetzwerks, über den die Kommunikation zwischen den im Channel vertretenen Organisationen stattfindet. Mit Ausnahme von leeren Channels können beliebig viele Organisationen des Netzwerks an einem Channel teilnehmen. Eine Organisation kann in mehreren Channels gleichzeitig Mitglied sein, muss aber in jedem Channel, in dem sie Mitglied ist, mit mindestens einem Peer vertreten sein.

Wallet:
Eine Wallet ist ein digitaler Ablageort für Benutzeridentitäten. Darin werden für jeden Benutzer Zertifikate, die Identifikation des Membership Service Providers (**MSP**) und der private Schlüssel der Identität gespeichert. Diese Informationen werden genutzt, um auf die Blockchain zuzugreifen. Eine Wallet hält jedoch keine Assets im Netzwerk.

Smart Contract:
In Smart Contracts werden Transaktionslogiken definiert, die den Lebenszyklus eines im World-State enthaltenen Geschäftsobjekts steuern. Um einen Smart Contract im Netzwerk bereitstellen zu können, muss er in einen Chaincode (nachfolgend erklärt) integriert werden. Zusammen mit dem Ledger bilden Smart Contracts das Herzstück des Fabric Netzwerksystems. Während ein Ledger Fakten über den aktuellen und historischen Zustand einer Reihe von Geschäftsobjekten enthält, definiert ein Smart Contract die ausführbare Logik, die dem Ledger hinzugefügt wird.

Chaincode:
Ein Chaincode ist ein Programmcode, welcher auf der Blockchain gespeichert wird und außerhalb des Netzwerkes aufgerufen werden kann. Chaincode dient dazu, zu entscheiden, wie Smart Contracts für die Bereitstellung technologisch verpackt werden. In Fabric kann Chaincode in Go, Java und Node.js geschrieben werden. Fabric-Nutzer verwenden die Begriffe Smart Contract und Chaincode oft synonym.

2 Einrichtung des Blockchainnetzwerkes

Im Rahmen des Projekts wurde zu Beginn ein einfaches Netzwerk mit einem Peer aufgesetzt. Die Konzeption sieht bei zukünftigen Erweiterungen vor, dass bei mehreren Organisationen jede Organisation einen Peer betreibt und somit das Netzwerk gegenseitig abgesichert wird. Das Netzwerk wiederum sollte eine Supplychain abbilden und in unterschiedlichen Channels direkte Transaktionen zwischen unterschiedlichen Marktteilnehmern speichern. Die in der Anforderungsanalyse vermuteten Skalierungsprobleme wurden in der Praxis und Implementierung bestätigt. Die Erweiterung des Netzwerkes um weitere Organisationen stellt

eine beträchtliche technische Hürde dar und wird auch über verfügbare wissenschaftliche Quellen anderer Marktteilnehmer bestätigt (vgl. Miehle 2019).
Grundsätzlich sieht die Konfiguration dennoch vor, dass, sobald ein weiteres Unternehmen dem Netzwerk beitritt, eine neue Organisation erstellt wird und mit einem Peer einem Channel beitritt. Bei der Überlegung zur Erstellung neuer Channel oder neue Organisation in einen bestehenden Channel hinzuzufügen, treten Fragen zu Transparenzbedenken in Wertschöpfungsnetzwerken auf. Es sollte deshalb analysiert werden, ob in dem bestehenden Channel Informationsobjekte gespeichert werden, welche die Teilnehmer nicht untereinander teilen möchten. Ist dies der Fall, muss ein neuer Channel eingerichtet werden, in dem die Peers der beiden Organisationen Mitglied sind. Spätestens wenn ein zweiter Handelspartner (Lieferant oder Kunde) dem Netzwerk hinzugefügt werden soll, können separate Channel eine sinnvolle Erweiterung darstellen. Da eventuell auch Informationen über die Blockchain ausgetauscht werden sollen, welche bidirektional zwischen einem der beiden Lieferanten und dem zu beliefernden Hersteller sind, erscheint eine Trennung der Daten hier essenziell. Dieser Fall wurde im Rahmen der Plattform **P2** im Anwendungsfall zur Produktionsabsicherung sowie zur Verhinderung von Produktionsstörungen umgesetzt.

3 Anbindung der Plattform an die Projektpartner Enterprise Systeme

Als einer der Projektpartner hat ACTIWARE seine Enterprise Content Management (ECM) Plattform eingesetzt, um traditionelle Enterprise Resource Planning (ERP) Systeme in einem Netzwerk zu integrieren. Die ECM Plattform diente hierbei als „technische und fachliche Brücke“, um mit bestehenden Ressourcen ein Wertschöpfungsnetzwerk aufzubauen. Darüber hinaus wurde die bestehende ECM-Plattform in einzelnen Bereichen so erweitert, dass die Anforderungen des Projekts erfüllt werden konnten. Dies beinhaltet insbesondere die Möglichkeit, Daten auf die Blockchains zu schreiben und von diesen zu lesen sowie eine Interaktion mit dem Endanwender (Anwendungspartner Maul-Theet) zu ermöglichen. Nicht zuletzt konnte darüber auch der Zugriff auf die Daten in der Fabric-Plattform für einen Qualitätsanwendungsfall ermöglicht werden. Die Struktur des Netzwerks und das Datenmodell sind dabei so aufgebaut, dass auch weitere Fabric-Plattformbetreiber teilnehmen könnten. Perspektivisch sollen sich so weitere Netzwerkeffekte und Vorteile sowie eine gewisse Offenheit der Implementierung ergeben. Für den Qualitätsplattformtyp (siehe hierzu Überblick Arbeitspaket D – Plattformtyp **P1**) sind auf Basis vergangener Kundenprojekte wiederverwendbare Geschäftsobjekte als Datenmodell implementiert, das per se für die Nutzung in verschiedenen Plattformtypen (Beispielsweise Plattformtyp **P2**) ebenso geeignet ist. Geschäftsobjekte werden von der ACTIWARE Gruppe zur standardisierten Einführung von ECM Systemen benutzt. Die Standardisierung besteht in der einheitlichen Erfassung und Klassifizierung von Geschäftsvorfällen und standardisierten Events. Die Adaption des Modells wurde in den Plattformtypen zur Produktions- und zur Qualitätssicherung durch das Projekt weiterentwickelt, getestet und prototypisch angewendet. Beispielhaft ist dies in Abbildung D.1.1 als Netzwerkstruktur dargestellt.
Hierbei kam ein vom Projektpartner ACTIWARE bestehender low-code und no-code Ansatz in der ECM-Plattform zum Einsatz, der die Implementierung vereinfachte. Dabei wurde ein zentraler Smart Contract erstellt, der in der ECM-Plattform modellierte Prozesse für Fabric übersetzte und somit ausführbar machte. Es zeigte sich, dass die fachliche Umsetzung mit Fabric möglich ist, die technische Umsetzung jedoch hohe Hürden hat, was für eine spätere Anwendung in der wirtschaftlichen Verwertung zu Herausforderungen führen kann.
Die ECM-Plattform der ACTIWARE wurde dabei um verschiedene Methoden wie Schreiben und Lesen von Daten sowie die Erstellung von Smart Contracts erweitert. Ergebnis dieser Umsetzung war ebenso, dass die Entwicklung einer einzigen Plattform zur Generierung von Smart Contracts wenig hilfreich erscheint. Stattdessen ist aus Sicht von ACTIWARE der Aufbau eines Netzwerkes sowie der Datenstruktur vorzuziehen, die unterschiedliche Plattformen anbinden kann und eine standardisierte Interaktion zwischen den Plattformen ermöglicht. Dies ist aus folgenden Gründen vorzuziehen:
1. Über den Einsatz unterschiedlicher Plattformen lässt sich die Einbindung unterschiedlicher Vorsysteme, insbesondere von verschiedenen ERP Systemen, sicherstellen.
2. Die Implementierung von Smart Contracts auf den aktuellen Blockchain Netzwerken setzt ein hohes technisches Verständnis voraus. Die Abbildung der Transaktionslogik rein auf Codebasis schränkt unseres Erachtens die Nutzergruppe ein, was einer späteren wirtschaftlichen Verwendung und damit erfolgreichen Dissemination entgegensteht. Daher präferieren wir den Ansatz, die Logik des Smart Contracts auf Low-Code oder gar auf No-Code Basis zu modellieren und somit umfassend rezipierbar zu machen.
Abbildung D.1.1 beschreibt eine holistische Darstellung des Netzwerkes und Anbindung mit ver-

schiedenen Teilnehmern in einer Lieferkette in einem Channel, sodass Transaktionen für Produkte nachvollzogen werden können. Ausgangspunkt der Überlegung ist, dass die ERP-Systeme der beteiligten Partner an einer Lieferkette auch weiterhin als führendes System angesehen werden. Die Blockchain selbst dient als sichere Datensenke zur Validierung von Transaktionen und kann darüber hinaus Auslöser für nachfolgende Aktionen sein.

Dadurch sind Möglichkeiten zum Monitoring und damit auch zur Flexibilisierung, zur Automatisierung und zur Absicherung in Wertschöpfungsnetzwerken geschaffen worden. Darüber hinaus wurde softwareseitig die Möglichkeit zum Schreiben und Lesen auf Blockchainnetzwerken geschaffen. Der Ansatz ist so ausgewählt, dass neben dem Fabric Netzwerk auch auf weitere Blockchain-Netzwerke geschrieben und von diesen gelesen werden kann.

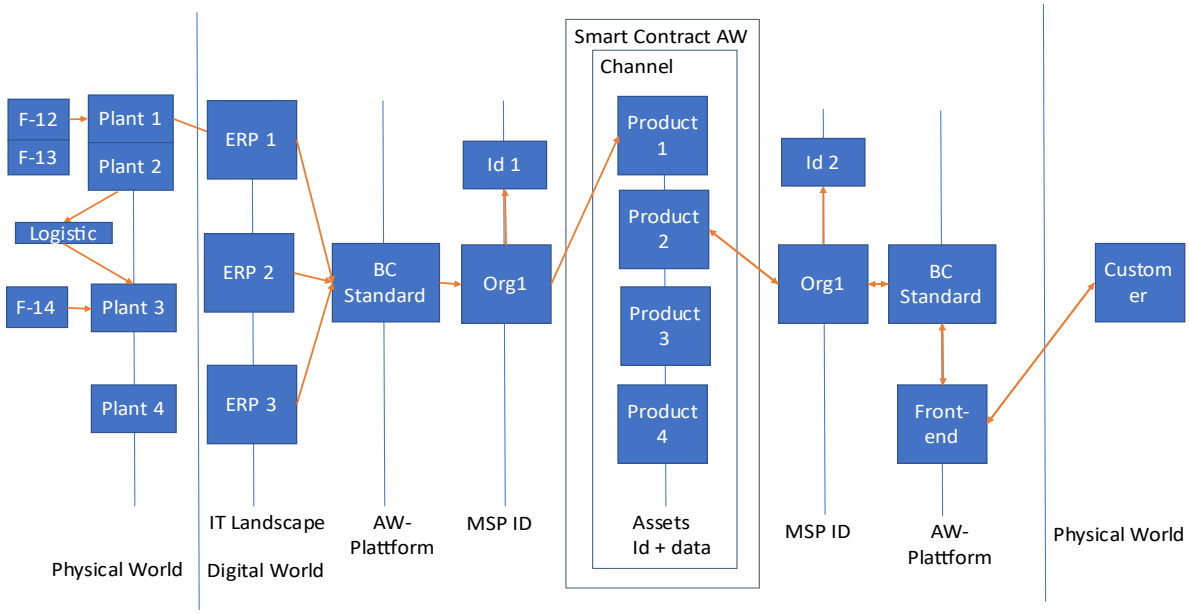


Abbildung D.1.1: Beispielhafte Netzwerkstruktur und Integration von ERP, ECM und Fabric

Für die Umsetzung der Qualitätsplattform P1 wurde ein bereits bestehendes Template der ACTIWARE Gruppe zur Einführung von ECM Projekten adaptiert und weiterentwickelt. Die dort beschriebene Supply Chain Event Konfiguration, die ERP-System-übergreifend einsetzbar ist, bildet eine Voraussetzung zur Abbildung von standardisierten Geschäftsvorfällen, die über die Blockchain abgewickelt und gesichert werden sollen. Das fachliche Modell beschränkt sich auf kaufmännische Belege wie Angebote, Bestellungen, Rechnungen oder auch Gutschriften sowie die Beschreibung von Artikeln. Um eine Eindeutigkeit im Blockchain-Netzwerk zu erzielen, werden die Artikel mit einer eindeutigen ID versehen. Über die Historie der gesamten Blockchain lassen sich Änderungen direkt am Objekt für den Endanwender erkennen.
Auf der rechten Seite von Abbildung D.1.1 wird das Abrufen von Informationen durch den Kunden mittels eines konfigurierbaren Formulars illustriert. Damit lässt sich lesend und je nach Benutzerrechten auch schreibend auf die Blockchain zugreifen. Über dieses jeweils frei konfigurierbare Front-End lassen sich unterschiedliche Szenarien abbilden, die vom reinen Konsumieren von Daten aus der Blockchain bis hin zur Bestätigung von Aktionen oder Status reichen.

Dies halten wir aus mehreren Gründen für notwendig.
1. Es lässt sich angesichts der noch unklaren Marktsituation nicht eindeutig festlegen, welche Blockchain-Technologie (Ethereum, Fabric, etc.) sich für die Nachverfolgung sowie Optimierung von Lieferketten durchsetzen wird.
2. Es ist auch kritisch zu hinterfragen, ob es herstellerseitig ausreichen wird, sich auf ein Blockchain-Netzwerk festzulegen, da je nach Anforderung und Kulturraum unterschiedliche Anbieter denkbar sind. Als Beispiel sei auf die Fragmentierung im ERP-Markt verwiesen, wo es teils stark branchenspezifische Lösungen gibt (Dasaklis et al. 2022). Dies ist auch bei Blockchain-Netzwerken denkbar. Bei der Infrastruktur sei auf die unterschiedlichen Aktivitäten in verschiedenen Weltregionen verwiesen, wo der chinesische Markt eine entscheidende Rolle in den Lieferketten spielt und dort durch staatliche Restriktionen nicht von einer Technologiefreiheit ausgegangen werden kann.
Abschließend kann festgehalten werden, dass das in Abbildung D.1.1 gezeigte Beispiel sich über die Middleware auch verschiedene Channel und Blockchain-Netzwerke anbinden und über das Modell verknüpfen ließ. Darüber hinaus bietet sich die Möglichkeit, die Daten mit Informationen anzureichern, die außerhalb der Blockchain gespeichert

sind. Der Projektpartner Signavio konnte ein ähnliches Verfahren und Szenario darstellen. Hier werden Smart Contracts allerdings per Compiler über ein BPMN Modell modelliert. Signavio hat neben Fabric ebenfalls in Ethereum Smart Contracts implementiert. Beide Partner streben langfristig eine Netzwerkunabhängigkeit an, um Lock-In-Situationen für zukünftige Kundenprojekte zu vermeiden.

4 Anbindung der Plattform zur technischen Überwachung

Wie im oberen Szenario beschrieben, ist bei einem Wachstum des Netzwerks und mehr Organisationen eine technische Analyse der Leistungsfähigkeit der Peers zwingend notwendig. Es muss fortlaufend überprüft werden, ob ein Peer je Organisation weiterhin ausreicht, oder ob weitere Peers in einer Organisation hinzugefügt werden sollten. Je nachdem, wie hoch die Datenlast in den einzelnen Channels ist, kann es notwendig sein, pro Channel einen separaten Peer je teilnehmender Organisation bereitzustellen. Diese Überwachung kann durch die Software des Praxispartners Infosim und der im Projekt angebundenen Netzwerkplattform StableNet für verschiedene Partner im Konsortium als Service übernommen werden. Falls wichtige Daten in einem Channel ausgetauscht werden, kann es zudem sinnvoll sein, weitere Peers als „Backup“ hinzuzufügen, damit kein Single Point of Failure entstehen kann. Diese Backup Peers müssen jedoch nicht unbedingt „Endorsing Peers“[1] sein. Das bedeutet, sie müssen nicht zwingend einen Chaincode installiert haben, um Transaktionen in das Netzwerk zu schreiben. Ein „normaler“ Peer, der nur die Ledger des Channels speichert, genügt, um die Sicherheit des Netzwerks zu erhöhen.

Die Projektarbeiten beschäftigten sich mit zwei verschiedenen Unternehmen und den angebunden Plattformen **P1+P2**, für die jeweils Smart Contracts auf Fabric hinterlegt wurden. Durch den Austausch der Logiken der Prozesse sowie durch die Blockchain als zentraler Händler sowohl von Daten als auch von Automatisierungsregeln ist somit grundsätzlich eine übergreifende Plattformimplementierung zwischen den Anwendungsfällen gegeben. Dies hängt allerdings nach wie vor vom fachlichen Integrationsgrad ab.

Weiterhin galt es, eine ereignisgesteuerte Architektur auf der Plattform **P2** für die Produktionsabsicherung zu implementieren, die die Reaktion auf Informationen nahe Echtzeit ermöglicht. Im Rahmen des Projekts wurden dabei verschiedene Szenarien abgebildet, so dass die Transaktionen in unterschiedlich skalierenden Wertschöpfungsnetzwerken nachgestellt wurden. Skalierung bedeutet in diesem Zusammenhang, dass die Netzwerke hinsichtlich der genutzten Transaktionsdaten verschiedene Ausprägungen haben.

Festzuhalten bleibt, dass die Umsetzung der Plattformen P1+P2 sowohl auf fachlicher als auch auf technischer Ebene zu Herausforderungen für die Teilnehmer führte. Die ECM Plattformen des Partners Actiware vereinfachte allerdings für beide Anwendungsfälle die Integration mehrerer Enterprise Systeme zum Aufbau eines Wertschöpfungsnetzwerkes. Zusätzlich konnten die Peers über die Netzwerksoftware des Partners Infosim bei zunehmender Skalierung technisch überwacht und abgesichert werden.

Literaturverzeichnis

Joannou, Demetrios & Kalawsky, Roy & Martínez-García, Miguel & Fowler, Chris & Fowler, Kevin. (2020). Realizing the Role of Permissioned Blockchains in a Systems Engineering Lifecycle. Systems. 8(4). 10.3390/systems8040041.

D. Miehle, D. Henze, A. Seitz, A. Luckow and B. Bruegge, "PartChain: A Decentralized Traceability Application for Multi-Tier Supply Chain Networks in the Automotive Industry," 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), 2019, pp. 140-145, doi: 10.1109/DAPPCON.2019.00027.

Dasaklis, T. K., Voutsinas, T. G., Tsoulfas, G. T., and Casino, F. 2022. “A Systematic Literature Review of Blockchain-Enabled Supply Chain Traceability Implementations,” Sustainability (14:4), p. 2439.

[1] Endorsing Peer ist der Peer, der eine vorgeschlagene Transaktion "befürwortet" bzw. ihr ein Gütesiegel verleiht. Nachdem die Transaktion gebilligt wurde, wird die Transaktion (zusammen mit der Billigung) an die Blockchain übermittelt.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Juniorprofessur für Information Management
Prof. Dr. Christian Janiesch
Stephanstraße 1
97070 Würzburg
https://www.wiwi.uni-wuerzburg.de/lehrstuhl/bwljp1/startseite/

Autoren und Ansprechpartner

Lukas-Valentin Herm, M.Sc.

Wissenschaftlicher Mitarbeiter
lukas-valentin.herm@uni-wuerzburg.de
+49 931 31-81730

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 0931 31-89640

Dr. Michael Kröhn

Head of Research
ROBUR Automation GmbH
michael.kroehn@robur-automation.com

Prof. Dr. Christian Janiesch

Juniorprofessur für Information Management
christian.janiesch@uni-wuerzburg.de
+49 931 31-84930

Michael Baumgart, M.Sc.

Senior Consultant Research & Development
Infosim GmbH & Co. KG
baumgart@infosim.net
+49 931 205 92 200

Dr. Patrick Bredebach

Productmanager
Actiware Development GmbH
patrick.bredebach@actiware-development.com
+49 231 5347 2540

Ole Jankowski, B.Sc.

Solution Architect
Actiware Development GmbH
ole.jankowski@actiware-development.com

D2: Implementierung von Smart Contracts

Smart Contracts ermöglichen die Absicherung und Ausführung von Transaktionen über die Blockchain, um Lieferketten regelbasiert zu automatisieren und nachvollziehbar zu gestalten. Im Rahmen des Projektes sind hierzu mehrere Smart Contracts für verschiedene Plattformtypen und Anwendungsfälle programmiert worden, die im Detail auf Objektebene beschrieben werden. Weiterhin wird die Integration in spezifische Herstellerplattformen dargestellt, um eine technische und betriebswirtschaftliche Integrationsmöglichkeit darzustellen.

1 Einführung von Smart Contracts

Smart Contracts sind Programme, die in einem Blockchain-Netzwerk gespeichert und ausgeführt werden können. Hierzu müssen bestimmte Bedingungen erfüllt sein, die es ermöglichen, eine rechtsgültige Ausfertigung eines Vertrags zu automatisieren, so dass alle Netzwerkteilnehmer Kenntnis über Transaktionen erhalten. Darüber hinaus können sie verschiedene organisatorische und technische Funktionen übernehmen, die durch die Projektpartner in folgenden Abschnitten dargestellt werden.

2 Implementierung von Smart Contracts

Um die direkte Ausführung von Prozessmodellen auf der Blockchain-Technologie zu ermöglichen, wurden von den Projektpartnern unterschiedliche Ansätze zur Einbindung von Blockchain-Netzwerken verfolgt. Der Projektpartner **Signavio** entwickelte hierzu eine Schnittstelle, die den Export, die Kompilierung, das Testen, und das Deployment von Prozessmodellen, die im Signavio Process Manager (Softwaretool des Herstellers) modelliert wurden, weitestgehend automatisiert. Nach bestimmten Regeln modellierte Prozessmodelle können in der Modellierungsumgebung mit Testfällen versehen und anschließend über einen Zwischenschritt, der die Modelle in den offenen BPMN 2.0 XML-Standard umwandelt, zu Smart Contracts in der Programmiersprache *Solidity* kompiliert werden. Anschließend werden die modellierten Testfälle ausgeführt, was die Testspezifizierung durch User mit grundlegenden technischen Kenntnissen ermöglicht. Beispielhaft ist dies durch folgenden Screenshot der Kompilierungsansicht in Abbildung D.2.1 dargestellt.

Abbildung D.2.1: Schnittstelle zur testgetriebenen Modellierung von Smart Contracts

Da die Schnittstelle von Prozessmodellen zu Solidity Smart Contracts lösungsspezifisch ist und es keine nennenswerte Kundennachfrage nach direkten Schnittstellen zu Blockchain-Umgebungen gibt, wurde die entwickelte Technologie als Open Source-Komponenten auf GitHub verfügbar gemacht:

- https://github.com/signavio/BPMN-Sol
- https://github.com/signavio/Test-Driven-Process-Modeling

An dieser Stelle ist nochmals hervorzuheben, dass die Implementierung weitestgehend auf dem BPMN 2.0 XML-Standard beruht und daher im Prinzip in jeder Modellierungsumgebung nutzbar ist, die den Standard unterstützt. Generell wurde im Zuge der Entwicklung ein starkes Augenmerk auf die Verbesserungen unserer REST und BPMN 2.0-Schnittstellen gelegt, wobei Letzteres in enger Zusammenarbeit mit der OMG BPMN 2.0 Model Interchange Working Group erfolgt ist.

3 Implementierung von Anwendungs-fällen in Produktion und Qualitäts-bereichen – genutzte Teilkomponenten

Der Projektpartner **Actiware** hat für verschiedene Anwendungsfälle in Produktion und Qualität (Plattformtyp P1+P2) ein Smart Contract für die Hyperledger Fabric Umgebung in Go implementiert. Dessen Logik lässt sich durch den Prozessdesigner (Softwarekomponente der Actiware ECM Plattform) heraus direkt designen und gibt somit die Möglichkeit, normalen Anwendern ohne technische Kenntnisse die Logik über eine grafische Oberfläche darzulegen. Actiware bietet hierzu den sog. *Prozessautomaten (Teilkomponente)* an, der auf No-Code-basis die regelbasierte Verarbeitung von Daten ermöglicht und Teil der ECM-Plattform ist. Diese Teilkomponente ermöglicht es standardisiert verschiedene ERP- oder CRM-Systeme, aber auch Daten aus dem IoT Kontext, zu verarbeiten und beispielsweise in ECM-Systemen abzulegen. Im Folgenden sind exemplarisch zwei Prozessoren abgebildet. In den Prozessoren selbst kann über eine grafische Oberfläche Logik abgebildet werden, so beispielsweise mittels des Decision/ Entscheidungsknoten Parameters ausgewertet und der Prozess gesteuert werden.

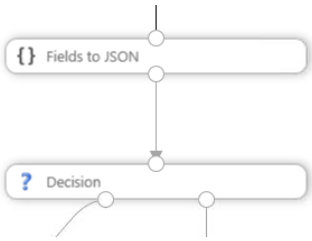


Abbildung D.2.2: Simplifizierte Darstellung von Prozessoren

Ferner ist ein Objektmodell implementiert, das standardisierte Informationen auf Business-Objekte ablegen kann. Die Business-Objekte wurden im Rahmen des Projektes genutzt, um beispielsweise die Qualitätssicherung zu unterstützen.
Die Plattform ist per Skript und erweiterbare Module konfigurierbar und kann an kundenspezifische Anforderungen angepasst werden. Zusätzlich lassen sich die Parameter der Ausführung über den Reportviewer der Actiware-Plattform für jeden Aufruf nachvollziehen. Der auf der Blockchain abgelegte Smart Contract nimmt Daten entgegen und speichert diese manipulationssicher ab. Das System ist darüber hinaus selbstdokumentierend, indem es Prozesse automatisch dokumentiert und Reports hierzu speichert. Zusammen mit der eingebundenen StableNet-Plattform des Partners Infosim ist es somit möglich, den Nachweis über die Umsetzung und Modellierung der Smart Contracts zu führen. Damit kann nachgewiesen werden, dass der Smart Contract selbst manipulationssicher erstellt worden ist und dem modellierten Prozess entspricht. Im Folgenden ist der gesamte Prozess eines Smart Contracts zum Schreiben auf die Blockchain visualisiert.

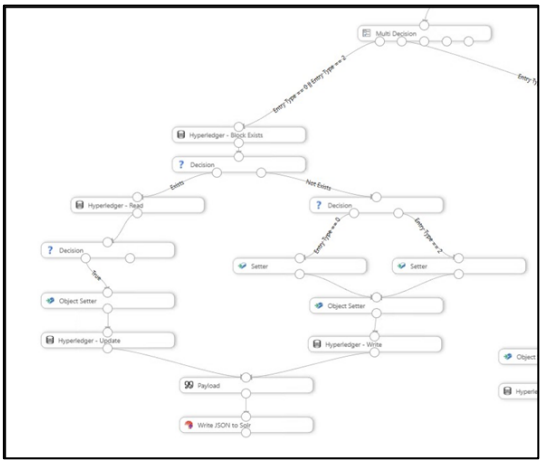


Abbildung D.2.3: Beispielhafter Prozess und Abhängigkeiten zum Ablegen von Daten innerhalb der ECM-Plattform

Das Design der jeweiligen Smart Contracts über das Prozessmodell erfolgt sowohl in der Signavio als auch in der Actiware Plattform (siehe als Beispiel obenstehende Abbildung D.2.3) und ermöglicht es, die Logik des Smart Contracts als Prozess abzubilden und damit diesen selbst als digitalen Gegenstand handeln zu können. Darüber hinaus ergibt sich der Vorteil, diese technisch einfacher zugänglich zu machen, um damit die Transparenz des Datenflusses herzustellen. Im Projekt wurde ebenso deutlich, dass die Ausgestaltung von Smart Contracts mindestens Branchen-, wenn nicht gar Fall-sensitiv ist. Auf die unterschiedlichen Fälle wird in Folgekapiteln eingegangen. Umso wichtiger erscheint es daher, einen *Prozessautomaten* nutzen zu können, der logische Prozesse in Code übersetzt und somit Geschäftslogiken wie -prozesse sichtbar macht und in die Blockchain überträgt.
Die gegenseitige Ansteuerung der Signavio- und der Actiware-Plattform ist dabei über eine REST-Schnittstelle möglich, kann aber auch über die Hyperledger Fabric Plattform durchgeführt werden. Innerhalb des Projektes wurde deutlich, dass es der Konsolidierung von Daten sowie den Voraussetzungen für die Anbindung unterschiedlicher Datenquellen und Informationssysteme bedarf. Die in den unterschiedlichen Anwendungsfällen herausgearbeiteten Anforderungen an die zur Verfügung stehenden Daten zeigten eine entsprechende Varianz auf. So sind die zu erhebenden Rahmenbedingungen der Supply Chain am jeweiligen Use Case auszurichten – je nachdem, ob Daten zur Qualitätssicherung, zur manuellen Bestätigung von Mitarbeitern oder möglicherweise zur Erfüllung von Anforderungen im Rahmen von Due Diligence Initiativen erhoben werden sollen (Zamfir et al. 2020). Daher ist aus Sicht der Firma Actiware die Einbindung einer Middleware notwendig, die die unterschiedlichen Systeme eines kleinen und mittleren Unternehmens anbinden und die Dateien gemäß der Anforderung anreichern kann. Dies wurde im Rahmen des Projekts an mehreren Beispielen durchgeführt. Damit konnten die in den Interviews erhobenen Kundenanforderungen bestätigt und umgesetzt werden, wonach die Datenmenge auf der Blockchain aus logischer Sicht zu begrenzen ist und außerhalb dieser zur Nachverfolgung zur Verfügung gestellt werden müssen.

4 Implementierung mehrstufige Produktion

In einem ersten Anwendungsfall wurde für den Fall der Massenverarbeitung am Beispiel eines fiktiven Produktionsbeispiels einer Müsliproduktion nachvollzogen, welche Daten aus den ERP Systemen (hier Dynamics 365, ebenso SAP ERP) gematcht werden müssen, um Kunden in der Lieferketten Informationen über den aktuellen Produktionsprozess geben zu können. Die Herausforderung besteht darin, einen standardisierten Prozess und ein entsprechendes Objektmodell zu entwerfen, das verschiedene ERP Systeme einbezieht. Der Aspekt der Standardisierung in Unternehmensprozessen

und Blockchain Applikationen spielt dabei für Forschung und Praxis eine zunehmende Rolle und führte auch in diesem Projekt zu kontroversen Diskussionen (Heines et al. 2021; Sedlmeir et al. 2022; Sunyaev et al. 2021).
Das Ziel dieser Tätigkeit war es dennoch, einen höheren Automatisierungsgrad zu erreichen. Umgesetzt wurde dies mittels eines Prozesses zur automatisierten Verarbeitung eines ERP Systems des Herstellers Microsoft (Navision 365). Ebenso sind Objekte auf der Blockchain definiert worden, die ein Matching von Ausgangsprodukten und Fertigprodukten über eine Middleware erlaubten. Damit ist eine grundlegende Nachvollziehbarkeit der Produktion auf der Blockchain hergestellt und zugleich kann bei tiefergehenden Informationen das Matching auch mit gespeicherten Daten außerhalb der Blockchain hergestellt werden, da diese wiederum über Hashes gesichert werden können. Die Smart Contracts dienen dabei zum automatisierten Notifizieren von Geschäftspartnern in der Supply Chain. Das Datenmodell ist in der folgenden Abbildung D.2.4 dargestellt und basiert auf grundlegenden Empfehlungen der GS1 zur Rückverfolgung von Lebensmittelproduktionen (Mager et al. 2016).

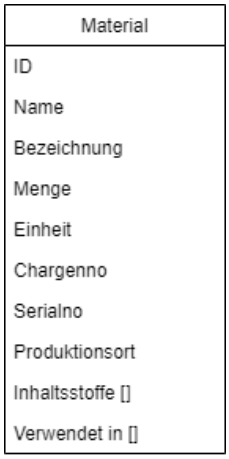


Abbildung D.2.4: Datenmodell Beispielproduktion

Innerhalb einer Supply Chain wird das Matching des Produktes über eindeutige Identifikatoren wie Chargen- und Seriennummern vorgenommen. Damit ist eine Rückverfolgung über die verschiedenen Produktionsstufen der Lieferkette möglich. Zugleich ist es über diesen Primärschlüssel möglich, Daten sowohl auf als auch außerhalb der Blockchain zu speichern und somit unterschiedlichen Anforderungen an Skalierungsaspekte gerecht zu werden.

5 Implementierung Qualitätssicherung

Ein zweiter implementierter Anwendungsfall hatte zum Ziel, über verschiedene Produktionsschritte hinweg Produkte mit der Losgröße 1 nachzuverfolgen sowie eine angemessene Mensch-Maschine Interaktion zu ermöglichen. In dem Qualitätsanwendungsfall des Plattformtyps P2 handelt es um die Erfassung von Auftrags- sowie Testspezifikationen. Dabei zeigte sich, dass es in kleinen Unternehmen eine unterschiedlich stark entwickelte IT-Landschaft gibt, die darüber hinaus sehr heterogen ist. Das bedeutet, dass der Plattformgedanke mit einer vorgelagerten Middleware neben einer Blockchain hinreichend flexibel ist, um die Anforderungen erfüllen zu können. Im konkreten Fall wurde die komplette Dokumentation vom Auftrag, über Einzelkomponenten zur Erstellung eines Produkts, bis hin zur Anlage von Testmaterialien zur Durchführung der spezifischen Tests betrachtet. Dabei wurden visuelle Formulare angeboten, die die manuelle Bestätigung von Auftragsdaten ermöglichten. Zusätzlich wurde im Use Case die Bestätigung von Versandlieferungen im Dual Use Bereich wie hier beispielsweise dem Zoll ermöglicht. Im Unterschied zum ersten Use Case[1] besteht die Herausforderung hier in der Anbindung unterschiedlicher Informationssysteme sowie der sinnvollen Einbindung von manuellen Auftragsbestätigungen. Die Blockchain wurde dabei sowohl als manipulationssichere Datensenke als auch zur automatisierten Transaktion via Smart Contract verwendet.

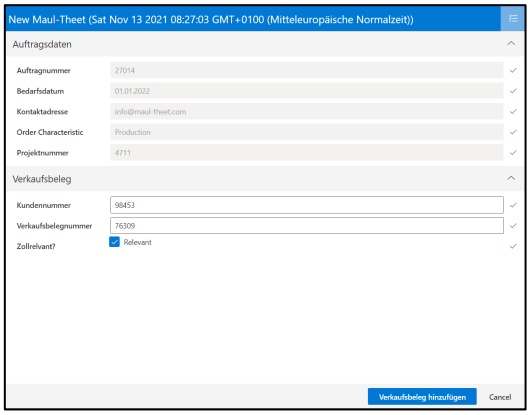


Abbildung D.2.5: Beispielhaftes Eingabeformular

Das oben dargestellte Formular ist über einen im Rahmen des Projektes entwickelten Formulargenerator entstanden. Damit lassen sich die im einführenden Unterkapitel genannten Teilkomponenten (siehe Kapitel 3) flexibel und einfach anbinden

[1] Dual-Use beschreibt die prinzipielle Verwendbarkeit von Technologien oder Gütern zu zivilen als auch zu militärischen Zwecken.

und auf Ereignisse aus den unterschiedlichen Plattformen jeweils reagieren und mit diesen interagieren. Hier ist beispielsweise in einem Anwendungsszenario möglich, Änderungen aus der Umgebung an angebundene Komponenten, wie z.B. die StableNet Plattform, zur Weiterverarbeitung zur Verfügung zu stellen oder auch auf StableNet zu reagieren. Das Formular kann so technisch eingebunden und bei der Validierung von Informationen berücksichtigt werden. Die unterschiedlichen Plattformtypen lassen sich hierdurch miteinander kombinieren.

6 Überblick der implementierten und getesteten Funktionen

Die von Actiware für die drei Anwendungsfälle berücksichtigten Funktionen des Smart Contracts sind:

- Anlegen eines Objektes auf der Blockchain
- Lesen eines Objektes
- Update eines Objektes, indem Informationen als Text abgelegt werden
- Löschen eines Objektes (Statusindikator auf der Blockchain)
- Überprüfen, ob ein Objekt auf der Blockchain existiert
- Alle Objekte von der Blockchain lesen
- Die Änderungshistorie eines Objektes auslesen

7 Zusammenfassung

Zusammenfassend lässt sich für die Kapitel D1 und D2 konstatieren, dass die Umsetzung des Netzwerks und die Implementierung der Blockchain mittels Hyperledger Fabric möglich ist. Der Demonstrator ist dabei in einer kontrollierten Umgebung aufgebaut worden. Er kann in der Komplexität gesteigert werden, sodass das Wertschöpfungsnetzwerk nach Bedarf erweiterbar ist. Darauf aufbauend wurde auf der Hyperledger Fabric Plattform ein Smart Contract implementiert, dessen Logik in der Plattform anpassbar ist und dessen Transparenz durch die grafische Oberfläche des in der ECM Actiware Plattform integrierten Prozessautomaten-Add-ons gegeben ist. Im Bereich der Datenaustauschstruktur sind unterschiedliche anpassungsfähige Datenmodelle entworfen worden, die die notwendigen Daten sowohl für die Automatisierung von Transaktionen in der Supply Chain als auch für die Qualitätssicherung bereitstellen können und weiterführend auch zur Überwachung des Netzwerkes selbst dienen. Während der Umsetzung der Projekte zeigte sich, dass unterschiedliche Datenstrukturmodelle anwendbar sind, die Akzeptanz dieser aber mit weiteren Praxispartnern evaluiert werden muss.

Literaturverzeichnis

Heines, R., Kannengiesser, N., Sturm, B., Jung, R., and Sunyaev, A. 2021. “Need for Change: Business Functions Affected by the Use of Decentralized Information Systems,” in: Proceedings of the Forty-Second International Conference on Information Systems, Association for Information Systems.

Mager, L. et al. 2016. GS1 Global Traceability Compliance Criteria for Food - Application Standard, GS1 AISBL.

Sedlmeir, J., Lautenschlager, J., Fridgen, G., and Urbach, N. 2022. “The Transparency Challenge of Blockchain in Organizations,” Electronic Markets (forthcoming) 2022.

Sunyaev, A., Kannengießer, N., Beck, R., Treiblmaier, H., Lacity, M., Kranz, J., Fridgen, G., Spankowski, U.,and Luckow, A. 2021. “Token economy,” Business & Information Systems Engineering (63), pp. 1–22.

Zamfir, I. 2020. Towards a mandatory EU system of due diligence for supply chains. Tech. rep. BRIEFING EPRS | European Parliamentary, pp. 1–10.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Juniorprofessur für Information Management
Prof. Dr. Christian Janiesch
Stephanstraße 1
97070 Würzburg
https://www.wiwi.uni-wuerzburg.de/lehrstuhl/bwljp1/startseite/

Autoren und Ansprechpartner

Lukas-Valentin Herm, M.Sc.

Wissenschaftlicher Mitarbeiter
lukas-valentin.herm@uni-wuerzburg.de
+49 931 31-81730

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 0931 31-89640

Dr. Timotheus Kampik

Principal Scientist in Residence
SAP Signavio
timotheus.kampik@signavio.com

Prof. Dr. Christian Janiesch

Juniorprofessur für Information Management
christian.janiesch@uni-wuerzburg.de
+49 931 31-84930

Dr. Michael Kröhn

Head of Research
ROBUR Automation GmbH
michael.kroehn@robur-automation.com

Michael Baumgart, M.Sc.

Senior Consultant Research & Development
Infosim GmbH & Co. KG
baumgart@infosim.net
+49 931 205 92 200

Dr. Patrick Bredebach

Productmanager
Actiware Development GmbH
patrick.bredebach@actiware-development.com
+49 231 5347 2540

Ole Jankowski, B.Sc.

Solution Architect
Actiware Development GmbH
ole.jankowski@actiware-development.com

D3: Entwicklung der Datenaustauschstruktur

Die Datenaustauschstruktur ermöglicht es, definierte Objekte zwischen traditionellen Informationssystemen und einem Blockchain Netzwerk auszutauschen. Hierbei ist die Wahl zwischen zentralen und dezentralen Austauschstrukturen zu treffen, in denen die Anforderungen des Konsortiums, semantische sowie syntaktische Standards berücksichtigt werden müssen. In diesem Kapitel werden zwei verschiedene Konzepte in Anlehnung an Anwendungsfälle aus dem Qualitäts- und Produktionsumfeld beschrieben, die im Rahmen der Projektarbeiten umgesetzt wurden.

1 Entwicklung der Datenaustauschstruktur

In diesem Abschnitt werden verschiedene Entwicklungsmöglichkeiten zum Aufbau einer Datenaustauschstruktur in Wertschöpfungsnetzwerken beleuchtet. Unter einer Datenaustauschstruktur wird in diesem Forschungsprojekt der Informationsaustausch zwischen traditionellen Informationssystemen und Anwendungsfällen des Projektkonsortiums verstanden, die einen Transfer von zentralisierten Informationssystemen in verteilte Netzwerke ermöglichen. Aufgrund der Neuartigkeit von Blockchain Applikationen bestehen zu diesem Thema nach wie vor nur wenige wissenschaftliche Erkenntnisse, wie eine fachliche und technische Integration aus klassischen Informations- bzw. Produktionssystemen wie Enterprise Resource Planning oder Manufacturing Execution Systeme (ERP) gestaltet werden kann (Dasaklis et al. 2022; Kuhn et al. 2021). Um eine Integration von Daten und Prozessen in Blockchain Systeme zu ermöglichen, wird eine Middleware Software benutzt, die einzelne Geräte oder Informationssysteme mit einer Blockchain Plattform verbindet (Leske et al. 2019; Pytel et al. 2020). In diesem Ergebnisbericht wird zwischen zwei Ansätzen unterschieden: Einer **zentralen** oder **dezentralen Datenaustauschstruktur**. Hierzu wird zunächst der Austausch zwischen physischen Objekten und traditionellen ERP Systemen aufgezeigt, bevor der Übergang von ERP Systemen in ein Blockchain-Netzwerk dargestellt wird. Darauf aufbauend beschreiben die Kapitel verschiedene Möglichkeiten zum Design und der Definition von Objekten in Blockchain-Systemen.

2 Dezentraler Ansatz: Organisation des Netzwerks und digitaler Assets

Wie bereits in der oberen Sektion eingeführt, gilt es zwischen Events und Objekten der physischen Welt (Abbildung D.3.1 - rot) und der digitalen Welt (Abbildung D.3.1 - orange) zu unterscheiden. Zu diesem Zweck wird in diesem Ergebnisbericht ein Anwendungsfall zur Rückverfolgung von Produkten über mehrere Produktionswerke beschrieben, der eine Nachbildung komplexer Gegebenheiten und Gestaltungsmöglichkeiten für die Praxis zulässt. Abbildung D.3.1 zeigt hierzu eine simplifizierte Darstellung von vier Produktionsstandorten, die mit drei unterschiedlichen ERP Systemen verwaltet werden. Weiterhin sind verschiedene Materialien (Materialbezeichnung: „F12-F14“) dargestellt, die als digitale Zwillinge in herkömmlichen ERP Systemen verwaltet werden können. In dieser Ausgangssituation beginnt der erste Schritt zu einem standardisierten Datenaustauschkonzept in Wertschöpfungsnetzwerken bereits mit der Abbildung von physischen Lokationen und Produkten in Informationssystemen. Die dort gecustomizten statischen und erzeugten dynamischen Objekte können je nach Anforderungen und UseCase in einem Datenaustauschmodell berücksichtigt werden (Hastig et al. 2020, Pytel et al. 2020). Diese Flexibilität an Gestaltungsmöglichkeiten erschwert es allerdings, einen akzeptierten und zentralen Standard zu entwickeln. In der Zukunft wird das Design solcher Systeme unterstützt, da globale Standardisierungsgesellschaften im Rahmen der ISO 307[1] verschiedene Richtlinien entwickeln, die eine einfachere Integration innovativer Blockchain Systeme ermöglichen wird. Ein möglicher Ansatz zur Erhöhung der Akzeptanz innovativer Blockchain Systeme könnte durch jeweilige Blockchain Communities entstehen, die an verschiedenen Blockchain Standards zur Abbildung digitaler Assets in Form von Tokens arbeiten[2]. Hierbei werden die Funktionen auf einer Blockchain nicht durch eine zentrale Autorität vorgegeben, sondern vielmehr dezentral durch ein Netzwerk von Teilnehmern. Die untenstehende Darstellung stellt in diesem Kontext die Möglichkeit dar, wie jedes Unternehmen sich an einen Blockchain Standard anpassen könnte.

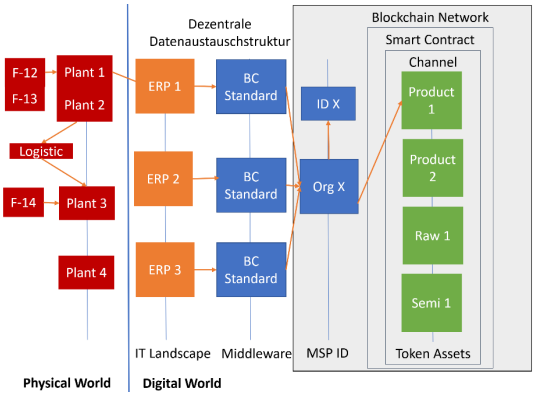


Abbildung D.3.1: Darstellung der dezentralen Datenaustauschstruktur im Blockchain-Netzwerk.

3 Dezentrales Netzwerk: Infrastruktur zwischen Informationssystemen und Blockchain-Plattform

Als Grundlage zur Bildung eines Datenaustausches besteht die Herausforderung, verschiedene digitale Objekte der Produkte und Informationssystemstrukturen für den Anwendungsfall aufzubereiten und geordnet in die Blockchain-Plattform zu

[1] https://www.iso.org/standard/81978.html?browse=tc Stand 24.02.2022

[2] ERC | Ethereum Improvement Proposals

überführen. Die Austauschstruktur sollte dabei von allen Organisationen bekannt und akzeptiert sein, da diverse Informationssysteme und die dazugehörige Middleware im ersten Ansatz **dezentral** organisiert werden. Für das Aufrufen bestimmter Informationen müssen die entsprechenden Datenbanktabellen ausgelesen und für vordefinierte Events bestimmt werden, um Informationen über mehrere Enterprise Systeme zu ermöglichen. Jedes IT-System, obgleich derselben oder eines unterschiedlichen Softwareproviders (ggf. auch unterschiedliche Releasestände), hat eine eigene Logik, Informationen in Datenbanken zu persistieren. Bevor die Transaktionsdaten von Produkten bzw. digitalen Zwillingen in das Blockchain-Netzwerk überführt werden, muss eine Middleware (Abbildung D.3.1, blau) einen Blockchain-Standard für diese vordefinierten Objekte und Events im Netzwerk gewährleisten. Anschließend wird das Blockchain-Netzwerk (für diesen Ergebnisbericht basierend auf Hyperledger Fabric) über eine entsprechende Identität und Organisation konsultiert. Die Besonderheit des dezentralen Datenaustausches liegt darin, dass jedem IT-System und jeder Organisation eine eigene Middleware und ein eigener Zugang zum Blockchain-Netzwerk zur Verfügung gestellt werden muss. Somit ist keine zentrale Instanz – im Sinne einer Plattform – in der Verantwortung, die Netzwerkintegration zu definieren.

3.1 Datenaustausch: Digitales Token-Asset-Modell

Die Gestaltung eines Datenaustausches zur Abbildung digitaler Zwillinge birgt zahlreiche Gestaltungsmöglichkeiten, von denen die Rückverfolgung von Produkten und Events nur einen Anwendungsfall darstellt. Erste Forschungsarbeiten bieten hierbei die Möglichkeit, verschiedene Token-basierte Ansätze bzw. ERC-Standards (ERC721, ERC1155, UTXO) zur Rückverfolgung von Produkten zu verwenden (Westerkamp et al. 2020, Kuhn et al. 2021, Pytel et al. 2020). Die Daten aus ERP-Systemen müssen hierfür in den jeweiligen Token Standard mithilfe der Middlewares transformiert werden.
Auch an diesem Punkt zeigt sich, dass auf Grund der stark unterschiedlichen Datenmodelle in Enterprise Systemen die Transformation der digitalen Produkt- und Buchungs-/Transaktionsdaten in den Blockchain-Standard unerlässlich ist. Im Blockchain Netzwerk werden die verschiedenen digitalen Assets mit Business Logiken schließlich durch einen Smart Contract (Chaincode) verknüpft (Abbildung D.3.1, grün). Bei der Konzeption von Smart Contracts kann auf verschiedene Standards oder Frameworks zurückgegriffen werden.
Der konzipierte Smart Contract impliziert ein Token Design, welches den digitalen Assets auf der Blockchain eine klare Struktur bei Transaktionen gibt. Für die Eindeutigkeit im Netzwerk kann beispielsweise ein kombinierter Primärschlüssel aus verschiedenen Attributen verwendet werden: Owner, Materialnummer, Serien-/Chargennummer und Transaktions-ID. Als weitere Attribute werden ein Zeitstempel, eine boolesche Mengenvariable sowie die Art der Transaktion gespeichert. Die benötigten Daten werden dezentral in der jeweiligen Middleware standardisiert bereitgestellt.
Speziell zur Abbildung komplexer Produktstrukturen zeigt sich beispielsweise der ERC-1155 Token Standard als potentielles Medium für zukünftige Anwendungen und wird sowohl auf Hyperledger[3] als auch Ethereum[4] genutzt (Kuhn et. Al 2021; Madhwal et. al 2022). Die Dezentralität bei der Verwendung eines Token Standards liegt darin, dass dieser Standard durch eine Blockchain-Community und nicht durch einen zentralen Anbieter bereitgestellt wird. Weiterhin besteht das Token Konzept darauf, jedes Enterprise-System auf einer Blockchain-Plattform als eigene Organisation auftreten zu lassen, das nicht durch einen zentralen Anbieter gesteuert wird. Die Systeme können über zugewiesene Identitäten digitale Assets in Form von Token kreieren und transferieren. Zudem können die Daten aus den Blöcken für Auswertungen abgerufen werden, um den Verlauf der jeweiligen Produktstrukturen zu erkennen.

3.2 Zentraler Ansatz: Organisation des Netzwerks und digitaler Assets

Neben der Möglichkeit, dezentral in ein Schema auf der Blockchain zu schreiben, kann die Möglichkeit einer Standardisierung auf der Ebene einer einzigen Middleware gewählt werden. Dieser zentralisierte Ansatz der Datenaustauschstruktur zeigt sich, indem der Datenfluss zur Blockchain über einen zentral verwalteten Middleware-Dienstleister gewährleistet und organisiert wird. Dies kann beispielsweise über eine Plattform integriert werden, die zusätzlich separate Account- und Zugangsrechte zur Verwaltung bereitstellen kann.
Es wird im Folgenden der Datenaustausch zwischen den Informationssystemen und dem Block-

[3] https://github.com/hyperledger/fabric-samples/blob/main/token-erc-1155/README.md

[4] https://eips.ethereum.org/EIPS/eip-1155

chain-Netzwerk sowie zwischen verschiedenen digitalen Assets in einem zentralisierten Ansatz veranschaulicht.

3.3 Infrastruktur zwischen Informationssystemen und Blockchain-Plattform

Äquivalent zu dem dezentralen Ansatz des Datenaustausches wird auch bei dem zentralisierten Vorgehen eine Middleware verwendet. Diese verknüpft die Datenmodelle der verschiedenen IT-Systeme aus der IT-Landschaft (Abbildung D.3.2, orange) mit dem Blockchain-Netzwerk.
Es können sowohl eine Instanz zentral oder auch mehrere Instanzen pro Entität eingerichtet werden – beispielsweise pro ERP-System, Standort oder Abteilung. Es ist dabei möglich, sowohl eine einzige Middleware oder auch mehrere Middleware Bausteine einzusetzen. Entscheidend ist hierbei, dass ein zentralisiertes Objektmodell auf Ebene der Middleware vor dem Schreiben in die Blockchain durch alle Teilnehmer angenommen wird.

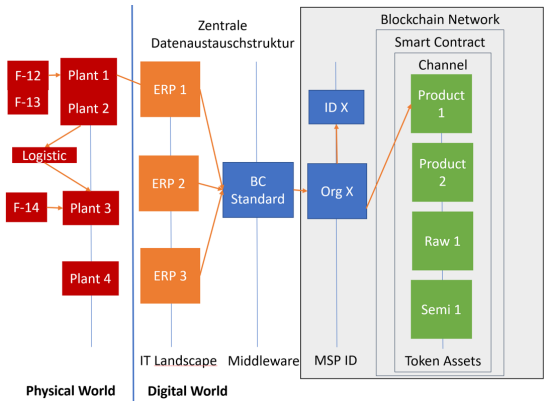


Abbildung D.3.2: Darstellung der zentralen Datenaustauschstruktur im Blockchain-Netzwerk.

Eine zentral bereitgestellte Middleware (Abbildung D.3.2, blau) fügt dabei die unterschiedlichen Informationen aus den vorgelagerten Systemen zusammen und mappt diese aufeinander. Die Middleware kann über eine Plattform oder Web-Applikation dem Anwender zur Verfügung gestellt werden. Über diese zentrale Instanz wird auch der Zugang zum Blockchain-Netzwerk organisiert, wenn diese ein eigenes Zugangs- und Regelmanagement besitzt. Auch beim Einsatz einer zentralisierten Middleware ist es möglich, pro ERP System eine eigene Identität auf der Blockchain zu nutzen. So kann auch bei diesem Ansatz die Darstellung von Materialflüssen allein auf der Blockchain nachvollzogen werden. Hierfür muss nur der Transaktionsverlauf der Eigentümerwechsel nachvollzogen werden.

Der zentralisierte Ansatz der Datenaustauschstruktur wurde im Rahmen des Forschungsprojekts ebenfalls implementiert, um die physische Welt mit Hilfe von ERP-Systemen auf entsprechende digitale Objekte abzubilden, welche kaufmännische Operationen darstellen. Dabei werden kaufmännische Objekte genutzt, die Gemeinsamkeiten zwischen ERP-Systemen und Nutzen aufzeigen. Hierbei werden grundlegende kaufmännische Objekte wie Verkauf, Auftrag, Rechnung etc. als Grundlage für kaufmännische Transaktionen angenommen. Diese können ebenfalls als Token dargestellt werden, solange sich die enthaltenen Attribute überschneiden.

3.4 Datenaustausch: Digitales Objektmodell

Im Unterschied zum dezentralisierten Vorgehen ist beim zentralisierten Ansatz im Rahmen des Projektes - in objektorientierter Ausprägung – in Ergebnisbericht D2 dargestellt worden, dass neben den Informationen, die transparent auf den Blöcken der Blockchain gespeichert werden, auch Offchain-Daten zur Verfügung gestellt werden. Der Ansatz geht davon aus, dass nicht alle Daten aus Datenschutzgründen gespeichert werden können. Darüber hinaus wird eine Offenheit je nach sich möglicherweise ändernder Fragestellung ermöglicht. Wenn dies berücksichtigt werden soll, ist aber das Halten der Datenstruktur und die Möglichkeit des Mappings von Daten außerhalb der Blockchain-Netzwerkstruktur notwendig und wurde in einem Anwendungsfall auch so abgebildet. Damit wird durch den/die Anbieter der Middleware ein Objekt-Modell vorgegeben und findet eine anbieterzentrierte Datenverarbeitung statt.
Das jeweilige ERP System wird dabei als führend angesehen und das Mapping über die zentral bereitgestellte Middleware ausgeführt. Transaktionen werden durch eindeutige Primärschlüssel identifizierbar sein, wobei durch eine rekursive Rückverfolgung der Warenströme die Daten jeweils konsumiert werden können. Dieser Primärschlüssel kann beispielsweise aus beliebig vielen zusammengesetzten Attributen eines Objektes bestehen und bietet somit die Möglichkeit, entsprechende Informationen bereits selbst zu tragen.
Dabei lassen sich Kernbestandteile solcher Modelle mit gewöhnlichen Geschäftsvorfällen wie Kauf und Verkauf beschreiben. Daneben ist ein variabler Teil zu nennen, der jeweils projektspezifisch angepasst werden kann. Als Beispiel lassen sich Daten zur Qualitätssicherung eines Produktes nennen, die je nach Branche und Projekt gestaltet werden. So kann je nach Lieferkette der Fokus beispielsweise auf Produktionsprozesse oder Produktstrukturen gelegt werden.

Zentralisiert bezieht sich dabei auf den Ansatz, zentral auf eine Middleware zu bauen, die dann die unterschiedlichen Informationen mappen kann. Hierbei ist zu erwähnen, dass auch mehrere unterschiedliche Middlewares im Netzwerk verwendet werden können, solange eine einheitliche Datenaustauschstruktur eingehalten wird. Vorteilhaft erscheinen dabei die Möglichkeiten, datenschutzrechtliche Bestimmungen erfüllen und zugleich mehrere Datensenken flexibel abbilden zu können. Als Nachteil lässt sich hervorheben, dass man bei der Interpretation der Daten und der Sicherstellung einer Vollständigkeit auf die Middleware angewiesen ist. Buchungen werden weiterhin durch die ERP Systeme abgebildet. Diese sind in dem Konstrukt führend.

Literaturverzeichnis

Dasaklis, T. K., Voutsinas, T. G., Tsoulfas, G. T., and Casino, F. 2022. “A Systematic Literature Review of Blockchain-Enabled Supply Chain Traceability Implementations,” Sustainability (14:4), p. 2439.

Hastig, Gabriella M., and ManMohan S. Sodhi. "Blockchain for supply chain traceability: Business requirements and critical success factors." Production and Operations Management 29.4 (2020): 935-954.

Kuhn, Marlene, et al. "Blockchain-based application for the traceability of complex assembly structures." Journal of Manufacturing Systems 59 (2021): 617-630.

Leske, C., Göbel, A., and Joswig, S. 2019. Blockchain mit SAP, SAP PRESS. Rheinwerk Verlag GmbH.

Madhwal, Y., Chistiakov, I., and Yanovich, Y. 2021. “Logging multi-component supply chain production in blockchain,” in: 2021 The 4th International Conference on Computers in Management and Business, pp. 83–88.

Westerkamp, Martin, Friedhelm Victor, and Axel Küpper. "Tracing manufacturing processes using blockchain-based token compositions." Digital Communications and Networks 6.2 (2020): 167-176.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL-THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Lehrstuhl für BWL und Wirtschaftsinformatik
Prof. Dr. Axel Winkelmann
Sanderring 2
97070 Würzburg
https://www.wiwi.uni-wuerzburg.de/lehrstuhl/wiinf2/startseite/

Autoren und Ansprechpartner

Norman Pytel, M.Eng.

Wissenschaftlicher Mitarbeiter
norman.pytel@uni-wuerzburg.de
+49 931 31-86348

Christian Zeiß, M.Sc.

Wissenschaftlicher Mitarbeiter
christian.zeiss@uni-wuerzburg.de
+49 931 31-88518

Dr. Patrick Bredebach

Productmanager
Actiware Development GmbH
patrick.bredebach@actiware-development.com
+49 231 5347 2540

Ole Jankowski, B.Sc.

Solution Architect
Actiware Development GmbH
ole.jankowski@actiware-development.com

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 0931 31-89640

D4: Implementierung der Eventarchitektur

Im folgenden Ergebnisbericht wird die praktische Umsetzung der erhobenen Referenzarchitektur für Blockchain-basierte Echtzeitverarbeitung vorgenommen. Hierfür wird ein mit Sensorik ausgestattetes Fischertechnik-Modell überwacht. Neben der Echtzeitverarbeitung wird zusätzlich eine Komponente zur Hash-basierten Überprüfung von Sensordaten, welche nicht in der Blockchain gespeichert werden können, entwickelt.

1 Blockchain-basierte Produktionsabsicherung durch Echtzeitüberwachung

Mit dem Zukunftsprojekt der Industrie 4.0, welches einen zentralen Aspekt der Innovationsstrategie der Bundesregierung widerspiegelt, soll die Digitalisierung der klassischen Industrie vorangetrieben werden. Dieser Fortschritt ist so beachtlich, dass Industrieexperten dies als die vierte industrielle Revolution (s.g. *Industrie 4.0*) einordnen (Soder 2014). Der Fokus dieser aktuellen Industrie 4.0 Anwendungen liegt in der Ausschöpfung der Optimierungspotentiale, die sich aus einer permanenten Informationsverarbeitung für die industrielle Fertigung ergeben. Der zentrale Aspekt der Industrie 4.0 ist die Aufhebung der Trennung zwischen physischer und virtueller Welt. Reale Gegenstände sind mit Sensorik und Prozessoren ausgestattet, sodass sie bei Bedarf Daten über sich und ihre Umgebung an verbundene IT-Systeme übermitteln können (sog. Internet der Dinge) (Schlick et al. 2014).

Diese Sichtweise des Internets der Dinge lässt sich auch auf die Produktion übertragen. Das gesamte Produktionsumfeld kann durch sog. Cyber-Physische Systeme (CPS) zu einer intelligenten Umgebung vernetzt werden (Kagermann et al. 2013). Die CPS umfassen unter anderem Produktionsanlagen, die ihre Umwelt mit Hilfe von entsprechender Sensorik erfassen, untereinander Informationen austauschen und selbstständig Entscheidungen treffen können (Bauernhansl 2014). Ziel ist eine dezentrale und echtzeitnahe Selbstorganisation der Systeme.

Ein Merkmal der intelligenten Fabrik ist es, Daten in Echtzeit zur Verfügung zu haben. Diese Tatsache ermöglicht es, ein virtuelles Abbild der Realität zu kreieren und dieses permanent mit Hilfe von Echtzeitdaten zu aktualisieren. Somit ermöglicht diese Vorgehensweise eine entscheidende Kosten- und Zeitreduzierung und damit erhebliche Wettbewerbsvorteile. Expertenschätzungen gehen davon aus, dass hier Einsparungspotential von bis zu 30 % gegenüber den heutigen Produktionsmethoden besteht (Soder 2014).

Bei der sogenannten Echtzeitverarbeitung (eng. stream processing) handelt es sich um einen Ansatz, bei dem anfallende Datenströme schnellstmöglich verarbeitet werden. Bei dieser Vorgehensweise ist es dabei essenziell, eine möglichst flexible und modulare Verwaltung der Echtzeitverarbeitung zu ermöglichen, um dynamisch auf Änderungen im Produktionsumfeld reagieren zu können (Bruns und Dunkel 2015). Daher wird innerhalb dieser Ansätze meist auf sogenannte Assoziationsregeln zurückgegriffen, welche als eine Art Filterregel funktionieren. Durch die ressourceneffiziente Analyse ermöglicht dieser Ansatz auch im Kontext großer Datenmengen eine gute Skalierbarkeit (Wanner et al. 2019).

Während innerhalb der eigenen Industrie 4.0 Produktion die verwendeten Technologien und Sensoren zur Überwachung der Produktionsanlagen genutzt werden und damit einen enormen Mehrwert bieten können, werden diese Daten meist siloartig nur innerhalb der eigenen Unternehmensstruktur gehalten. Oftmals haben Unternehmen die Befürchtung, dass die von ihnen erhobenen Daten Rückschlüsse auf den Produktionsprozess liefern könnten und damit Firmengeheimnisse preisgeben. Dieses Verhalten wird in der heutigen Zeit dadurch erschwert, dass die Globalisierung Unternehmen dazu zwingt, internationale Kooperationen, oftmals auch mit unbekannten Partnern, einzugehen, um wettbewerbsfähig zu bleiben. Gleichzeitig kann eine effiziente Handhabung einer Wertschöpfungskette nur stattfinden, wenn Engpässe und Problemstellen frühzeitig erkannt und behoben werden, da es ansonsten erhebliche Auswirkungen auf das komplette Wertschöpfungsnetzwerk haben kann (Herm und Janiesch 2021).

Ein potenzieller Lösungsansatz kann hier die Blockchain-Technologie sein. Bei der Blockchain-Technologie handelt es sich um ein transparentes und dezentrales Verfahren zur verketteten Speicherung von Transaktionen innerhalb eines Prozesses (Nakamoto 2008). Durch die Unveränderlichkeit und Transparenz von Transaktionen innerhalb einer Blockchain werden Manipulationen und damit Betrugsversuche bei Handelsbeziehungen in einem Wertschöpfungsnetzwerk erschwert (Xu et al. 2019). Die Blockchain-Technologie gewährleistet somit, trotz nicht vorhandenem Vertrauen in die Kooperationspartner, ein Vertrauen in die Fälschungssicherheit aller gespeicherten Transaktionen (Wang et al. 2017). Der Einsatz der Blockchain-Technologie ermöglicht es ebenso, Prozesse in Handelsbeziehungen zu automatisieren, digitalisieren und in Echtzeit zu überwachen (Iansiti und Lakhani 2017).

Ziel dieses Arbeitspaketes ist es, auf Basis der bereits entwickelten Referenzarchitektur für Blockchain-basierte Echtzeitverarbeitung (Arbeitspaket C5) die Implementierung und Bewertung eines Industrie 4.0 Anwendungsfalles vorzunehmen. Um die Praxisnähe sicherzustellen, wird der Anwendungsfall basierend auf einem mit Sensorik ausgestatteten Modell zur Fabriksimulation umgesetzt.

Der Bericht gliedert sich dabei wie folgt: In Kapitel 2 wird die genutzte Fabriksimulation sowie die umgesetzte Referenzarchitektur beschrieben. In Kapitel 3 erfolgt die Darstellung der entwickelten Dashboards. Kapitel 4 stellt eine Bewertung der gewonnenen Erkenntnisse da, während Kapitel 5 ein prägnantes Fazit zieht.

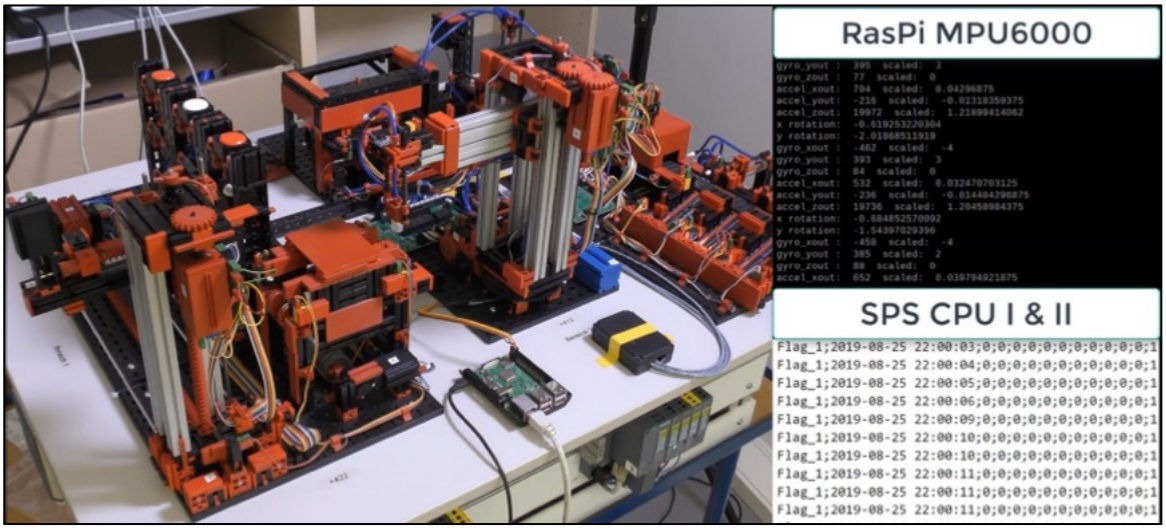


Abbildung D.4.1: Foto des Fischertechnik-Modells-Versuchsaufbaus (links) sowie Darstellung der anfallenden Daten durch interne und externe Sensorik (rechts)

2 Strukturelle Vorarbeiten

2.1 Beschreibung des Fischertechnik-Modells

Die Fabrik-Simulation von Fischertechnik (im folgenden Fischertechnik-Modell genannt) ist ein Trainingsmodell, welches eine Fabrik simuliert. Das Modell ist in Abbildung D.4.1 (links) dargestellt und wurde durch das Unternehmen ROBUR Automation GmbH zur Verfügung gestellt. Auf Grund seines modularen Aufbaues und der einfachen Integration von Sensoren wird es häufig dazu genutzt, neue Produktionsstraßen zu simulieren oder wissenschaftliche Experimente durchzuführen (Seiger et al. 2020).

Abbildung D.4.2 veranschaulicht den Aufbau des Modells. Es besteht aus mehreren Einzelkomponenten wie dem *(1)* automatisierten Hochregal, einer *(2)* Multi-Bearbeitungsstation mit Brennofen, einem *(3)* Vakuumsauggreifer und einer *(4)* Sortierstrecke mit Farberkennung. Durch diese Verkettung mehrerer Stationen lassen sich somit die Abläufe einer Bearbeitungslinie simulieren.

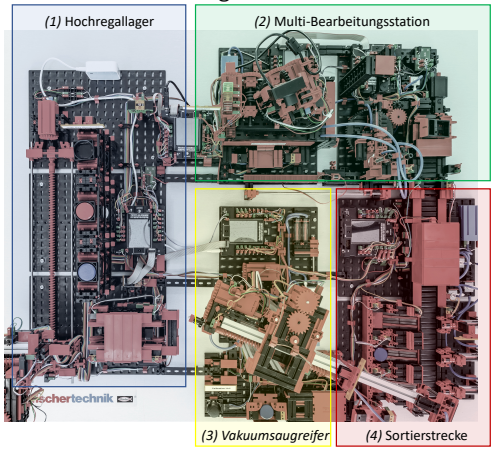


Abbildung D.4.2. Aufbau Fischertechnik-Modell in Anlehnung an Fischertechnik (2019a)

Der simulierte Produktionsablauf innerhalb des Modells gestaltet sich dabei wie folgt:

Der integrierte Vakuumsauggreifer belädt das Regalbedienungsgerät des automatisierten Hochregallagers mit unverarbeiteten Werkstücken. Diese werden nach der Farbe der Werkstücke entsprechend einsortiert. Darauffolgend werden die Werkstücke zur Weiterverarbeitung wieder ausgelagert sowie anschließend zur Multi-Bearbeitungsstation transportiert. Der Weitertransport funktioniert ebenfalls über den Vakuumsaufgreifer, welcher das Werkstück an einen simulierten Brennofen befördert. Der Brennofen führt eine „Vorverarbeitung“ auf dem Werkstück durch. Anschließend wird es an einer Sägestation „veredelt“. Infolgedessen werden verarbeitete Werkstücke anhand einer Sortieranlage entsprechend ihrer Farbe eingeordnet und zum Zwischenlager befördert, bis diese vom Vakuumsauggreifer wieder aufgenommen und zum Hochregallager zurück transportiert werden. Dieser Produktionsablauf wird in Endlosschleife durchgeführt (Fischertechnik 2019b).

Das Fischertechnik-Modell umfasst vier 24V Platinen und wird über verschiedene speicherprogrammierbare Steuerungen (SPS) gesteuert werden. Für den beschriebenen Anwendungsfall werden zwei Siemens SIMATIC S7 verwendet, um ein möglichst realitätsnahes Anwendungsszenario abzubilden. Insgesamt sind in dem Modell über 200 binäre Sensoren (wie z.B. Lichtschranken) verbaut, deren Werte kontinuierlich dem OPC-UA-Server der SPS übergeben werden. Zusätzlich wird weitere Sensorik wie Beschleunigungs-, Luftdruck-, oder Geräuschsensoren durch zwei Raspberry Pis abgefragt und ebenfalls für das Anwendungsszenario genutzt. Ein Ausschnitt der genutzten Sensordaten ist in Abbildung D.4.1 (rechts) dargestellt.

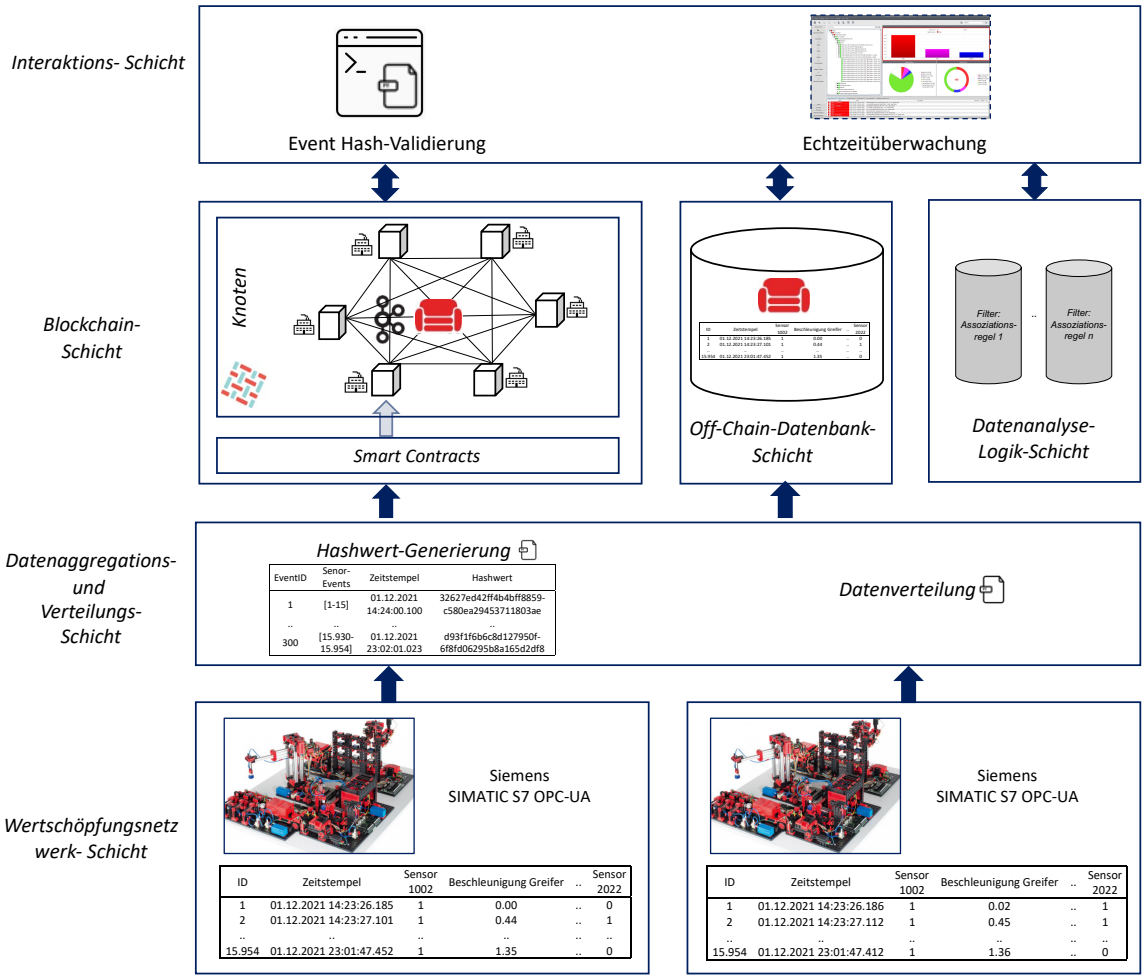


Abbildung D.4.3: Umsetzung der Echtzeit-Referenzarchitektur zur Blockchain-basierten Produktionsabsicherung (in Anlehnung an Ergebnisse aus Arbeitspaket C5)

2.2 Komponenten der Implementierung

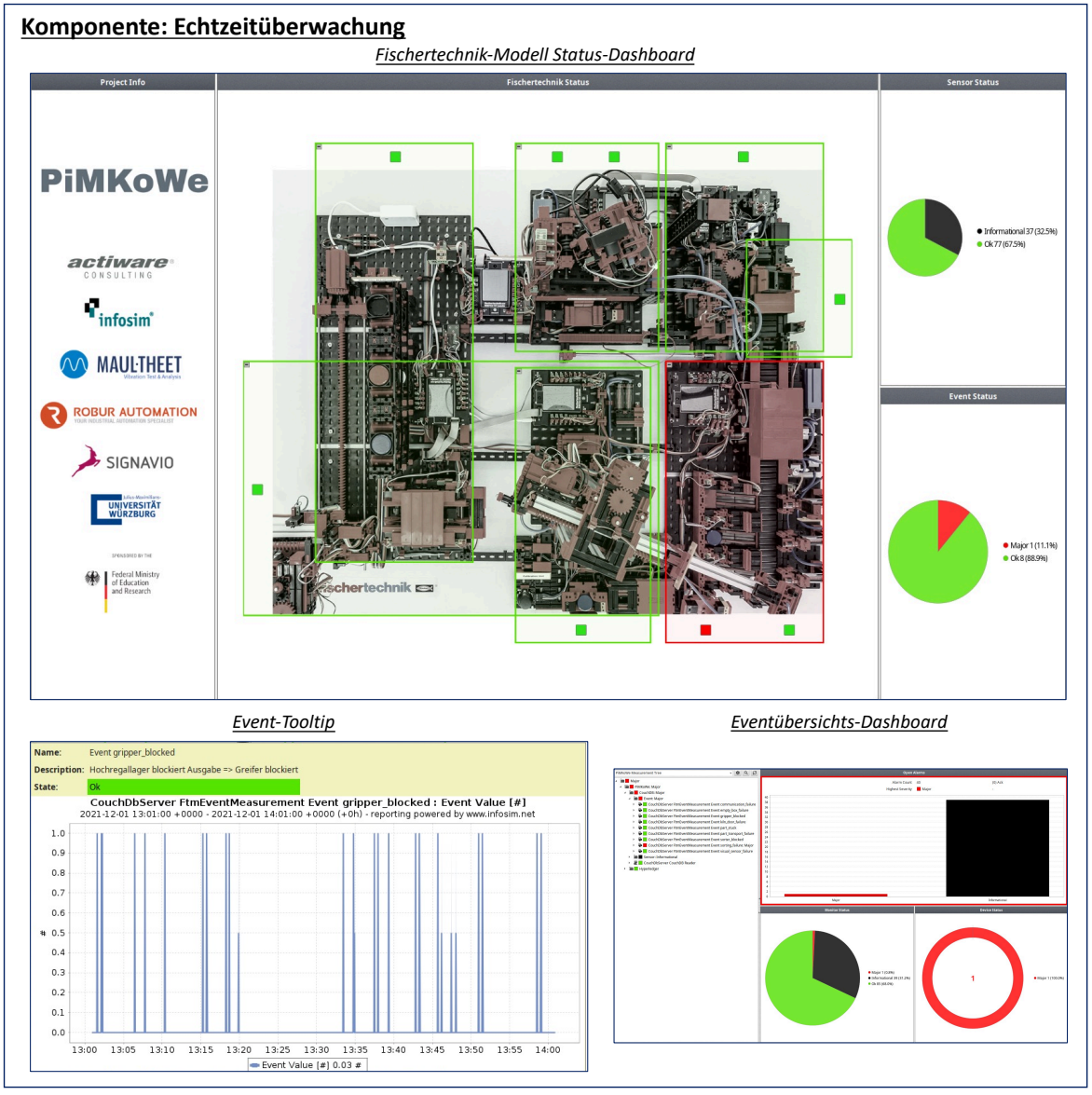
Die Umsetzung der Implementierung erfolgt anhand der Referenzarchitektur für Blockchain-basierte Echtzeitverarbeitung aus Arbeitspaket C5. Hierfür wird ein Servercluster, bestehend aus insgesamt 8 vCPUs, 18GB RAM und 315GB Speicherplatz genutzt. Die genutzten Schichten werden in Abbildung D.4.3 vorgestellt und im Folgenden beschrieben.

Wertschöpfungsnetzwerk-Schicht. Diese Schicht wird durch das Anwendungsszenario der Produktionsabsicherung umgesetzt. Hierfür wird das beschriebene Fischertechnik-Modell genutzt, welches mit verschiedenen Sensoren und industrienahen Siemens SPSen ausgestattet ist. Die Sensordaten werden mittels eines OPC-UA-Klienten ausgelesen und an die Datenaggregations- und Verteilungs-Schicht weitergeleitet. In diesem Anwendungsszenario fallen pro Modell alle 3 Sekunden ca. 230 Sensordaten an. Um die Inkludierung mehrerer Wertschöpfungsnetzwerke in einer Blockchain zu simulieren, können mehrere dieser Produktionsanlagen angebunden werden.

Datenaggregations- und Verteilungs-Schicht. Innerhalb dieser Schicht finden zwei Prozesse statt. Zum einen werden die Daten aus den Wertschöpfungsnetzwerken in einer unaggregierten Struktur an eine Off-Chain-Datenbank-Schicht weitergeleitet. Zum anderen werden die Sensorwerte anhand einer Logik aggregiert. Für die aggregierten Werte wird ein Hashwert generiert, um die Fälschungssicherheit der Rohdaten zu gewähren. Um ein Höchstmaß an Sicherheit sicherzustellen, wird hier eine SHA3-Hashfunktion angewendet. Die aggregierten Daten sowie der zugehörige Hashwert werden anschließend an die Blockchain-Schicht weitergeleitet. Beide Schritte werden durch eine Python-basierte Middleware umgesetzt, welche zum einen mittels http-requests Sensordaten an die Off-Chain-Datenbank sendet und zum anderen mittels eines Methodenaufrufes, des zugehörigen smart contracts, die aggregierten Daten in die Blockchain speichert.

Blockchain-Schicht. Die Blockchain-Implementierung erfolgt mit einer Hyperledger Fabric (Androulaki et al. 2018), welche zur Sicherung der Transaktionszustände je Knoten eine Apache CouchDB als dokumentenorientierte Datenbank nutzt (Apache

Software Foundation 2021). Ebenso wird innerhalb der Blockchain die Datenverteilung über die verschiedenen Knoten hinweg durch das Publish/ Subscribe-System Apache Kafka bewerkstelligt (Apache Software Foundation 2017). Die Hyperledger Fabric wird in der Version 2.1 betrieben, wobei zur realitätsnahen Evaluierung drei Knoten (eng. peers) genutzt werden. Ein JavaScript-basierter smart contract (Hyperledger Fabric Kontext: chaincode) wird genutzt, um Transaktionen in die Blockchain zu schreiben oder Daten herauszulesen. Um mehrere Wertschöpfungsnetzwerke und damit verschiedene Lese- und Schreibberechtigungen abzubilden, werden mehrere Kommunikationskanäle (engl. channel) auf der Blockchain genutzt.



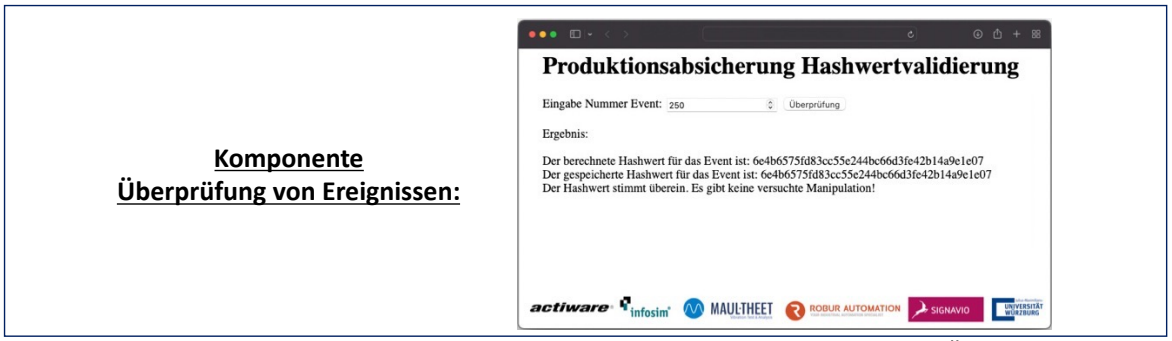


Abbildung D.4.4: Darstellung der Echtzeitüberwachungskomponente (oben) sowie der Überprüfung von Ereignis-Komponente (unten) innerhalb der Interaktions-Schicht.

Off-Chain-Datenbank-Schicht. Die Speicherung der Sensordaten aus der Datenaggregations- und Verteilungs-Schicht erfolgt ebenfalls durch eine Apache CouchDB. Anschließend speichert die CouchDB die Sensordaten der verschiedenen Wertschöpfungsnetzwerke dezentral über ein mehrstufiges Rechtesystem ab.

Datenanalyse-Logik-Schicht. In dieser Schicht sind die verschiedenen Regelwerke für die Filterung der Sensordaten nach Anomalien gespeichert. Diese Assoziationsregeln dienen dazu, Produktionsmängel oder Fehler in nahezu Echtzeit zu erkennen. Durch die Anpassung dieser Regeln kann die Definition und Erkennung neuer Anomalien innerhalb der Interaktions-Schicht vorgenommen werden.
Innerhalb des Anwendungsszenarios werden exemplarisch neun Regelwerke definiert, um potenzielle Produktionsvorkommnisse oder Produktionsfehler automatisiert und in nahezu Echtzeit zu erfassen.
Ein vereinfachtes Beispiel verdeutlicht den Sachverhalt: *Regelwerk: (sensor20037 =1) -> (timer:interval(1 sec) and (sensor20030 =1)) -> (timer:interval(2 sec) then (sensor20033 =0))*
Dieses Regelwerk beschreibt den Zustand innerhalb einer Produktion, wenn der Saugnapf am Drehkranz aktiv ist *(Sensor 20037 = 1)*, der Drehkranz sich anschließend im Uhrzeigersinn zur Sägeanlage bewegt *(Sensor 20030 = 1)*, die Sägeanlage jedoch danach das Werkstück nicht weiterbearbeitet *(Sensor 20033 = 0)*. In diesem Fall kann bspw. von einem (technischen) Kommunikationsfehler ausgegangen werden.

Interaktions-Schicht. Durch diese Schicht kann der Anwender die Geschehnisse innerhalb der Wertschöpfungsnetzwerke sowie der Blockchain verfolgen. Zum einen kann der Anwender, falls es z.B. Vertrauensprobleme gibt, eine Validierung der Hashwerte der verschiedenen Events anfordern und damit einen Vergleich zwischen den unaggregierten Off-Chain-Daten und den Daten, welche auf der Blockchain gespeichert sind, vornehmen. Zum anderen kann durch die Verknüpfung des Dashboards für die Echtzeitüberwachung zu der Blockchain-Schicht sowie der Off-Chain-Datenbank-Schicht eine Überwachung der Ereignisse durch die Datenstromanalyse vorgenommen werden. Beide Komponenten werden im Folgenden detailliert beschrieben

3 Darstellung des Produktions-überwachungs-Dashboards

Im Folgenden werden die Dashboards, auch Komponenten genannt, die in Abbildung D.4.4 dargestellt sind, beschrieben. Die Darstellung erfolgt anhand der Leserechte eines Administrators, welcher auf die verschiedenen channels und damit die Wertschöpfungsnetzwerke der Hyperledger-Fabric Zugriff hat. Die Multimandantenfähigkeit des Systems erlaubt zudem eine selektive Darstellung der Wertschöpfungsnetzwerke, je nach zugeteilter Leserechte auf der Blockchain.

3.1 Echtzeitüberwachung

Grundlage für das Dashboard bietet eine im Rahmen des Projekts entwickelte Erweiterung zum automatisierten Netzwerk- und Service-Management-System StableNet® der Firma Infosim®. Die Erweiterung greift auf die verschiedenen Datenbanken zu, um Ereignisse, die in der Produktionsanlage stattfinden, abzufragen, zu filtern und zu visualisieren. Dieses System lässt sich in weitere Dashboards untergliedern:

Fischertechnik-Modell Status-Dashboard. Die Ansicht des Dashboards zeigt einen Überblick über die verschiedenen Teilbereiche der simulierten Produktionsanlage respektive des Wertschöpfungsnetzwerkes. Die Teilbereiche sind durch Rahmen getrennt, die den Zustand der zugehörigen Komponenten durch ihre Farbe vorgeben. Ist der Teilbereich grün eingefärbt, wurde bei der letzten Sensormessung in der Produktion kein Problem festgestellt. Ist der Bereich jedoch rot gefärbt, liegt eine Störung oder ein besonderes Ereignis vor. Entstandene Ereignisse werden automatisch den verschiedenen Teilbereichen zugeordnet. Die zwei Kreisdiagramme auf der rechten Seite beschreiben zusätzlich den aktuellen Status der Sensorinformationen sowie die aus den Sensordaten berechneten Ereignisse.

Event-Tooltip. Innerhalb dieser Detailansicht wird zu den einzelnen Events Name, Beschreibung, Status und ein Verlauf der Sensorwerte innerhalb einer definierten Zeitspanne angezeigt und damit eine Detailprüfung sowie Analyse des Prozessablaufes innerhalb eines Wertschöpfungsnetzwerkes ermöglicht. Der in der Abbildung beschriebene Ausschlag an Sensorwerten demonstriert einen Produktionsfehler, bei dem ein Greifer ein Produktionsteil nicht aus dem Hochregallager entnehmen kann und es somit zu Komplikationen im Produktionsablauf kommt. Durch diese Vorgehensweise können insbesondere Engpässe innerhalb von Wertschöpfungsnetzwerken erkannt und somit langfristig Optimierungen vorgenommen werden.

Eventübersichts-Dashboard. Dieses Dashboard ist aufgrund der Multimandantenfähigkeit des Sys-

tems allen Anwendern zugänglich. Innerhalb dieser Ansicht wird eine kompakte Darstellung des Zustandes der Produktionsanlage dargestellt.

3.2 Überprüfung von Ereignissen

Im Folgenden wird die Komponente zur Überprüfung von Ereignissen dargestellt. Diese Funktionalität wird durch eine Webanwendung den Anwendern und den Partnern innerhalb des Wertschöpfungsnetzwerkes zur Verfügung gestellt. Die Webanwendung basiert auf dem Python-Framework Flask (Pallets 2021). Die Komponente validiert dabei die Authentizität und damit Unversehrtheit von entstandenen Sensorwerten.
Hierfür werden die durch die Datenaggregations- und Verteilungsschicht generierten Hashwerte, welche in der Blockchain gespeichert sind, den Sensorwerten in der Off-Chain-Datenbank gegenübergestellt. Die Webanwendung generiert auf Basis der Sensorwerte aus der Off-Chain-Datenbank eigene Hashwerte und vergleicht diese mit den Hashwerten, welche in der Blockchain gespeichert sind. Sollte es Differenzen zwischen beiden Ergebnissen geben, ist davon auszugehen, dass ein Wertschöpfungspartner versucht hat, Daten, welche nicht in der Blockchain gespeichert sind bzw. nicht gespeichert werden dürfen, zu manipulieren. Durch dieses Vorgehen können nicht nur Wertschöpfungsnetzwerke überwacht werden, sondern auch die Integrität aller Daten (On-Chain und Off-Chain) sichergestellt werden. Damit ein Anwender einen Vergleich zwischen den Hashwerten anstoßen kann, muss dieser über ein Eingabefeld die IDs der Sensorwerte eingeben, welche er überprüfen möchte.

4 Bewertung der Implementierung

Im Folgenden wird eine Bewertung der Implementierung vorgenommen. Diese Bewertung erfolgt anhand des Aufwandes, der Manipulationssicherheit, der Ausfallsicherheit sowie der Performance.
Aufwand der Implementierung. Die Konfiguration von Hyperledger Fabric ist komplex und erfordert Fachwissen und Erfahrung. Für den Fall von Softwareänderungen (im chaincode) muss das gesamte Konsortium aktiv werden, die Änderungen prüfen, auf allen peers installieren und ggf. die WebAPI anpassen. Der Personalaufwand erfordert zudem Spezialisten in den Bereichen Blockchain-Netzwerk, chaincode-Programmierung oder Container-Administration. Gleichzeitig zeigt sich durch die hohen Automatisierungspotentiale bei der Chaincodeausführung ein erheblicher Mehrwert, der die Anwendung einer Blockchain legitimieren kann.

Manipulationssicherheit. Hier zeigen sich die Stärken der Blockchain. Jede Organisation speichert auf den bereitgestellten peers eine Kopie der bisherigen Transaktionen und kann somit jederzeit auf ihre eigene Datenbasis zugreifen. Zudem ist die Blockchain-Historie über kryptografische Verfahren gegen Manipulationen abgesichert. Würde eine Organisation ihre Kopie der Datenbank (Knoten) manipulieren, würde es den anderen Organisationen unmittelbar auffallen. Insbesondere im Anwendungsfall von internationalen Wertschöpfungsnetzwerken mit neuen und unbekannten Partnern kann dies ein entscheidender Aspekt sein, eine Kooperation einzugehen.

Ausfallsicherheit. Hyperledger Fabric bietet die Möglichkeit, alle Komponenten redundant auszulegen, so dass ein Ausfall von einem oder mehreren Teilen kein Problem darstellt. Auch ein Ausfall des Internets wäre nur teilweise ein Problem. Lesezugriffe auf die organisationsinterne Datenbank, die auf den peers gespeichert wird, funktionieren weiterhin. Gerade innerhalb einer Produktion können diese Limitationen häufig auftreten.

Performance. Blockchain-Netzwerke sind aufgrund ihrer komplexen, dezentralen Struktur und rechenintensiver Kryptografie um einige Größenordnungen langsamer. Im praktischen Einsatz, im vorliegenden Beispielfall, liegt die Latenz einer vollumfänglichen Schreiboperation im Bereich von 2000ms, eine Leseoperation im Bereich 10ms. Eine zusätzlich hierfür durchgeführte Studie zur Performance von Hyperledger Fabric zeigt, dass die Latenz bei vielen parallelen Schreibzugriffen erheblich ansteigt. Bei 100 gleichzeitigen Transaktionen ist mit 10 Sekunden zu rechnen, ab 140 liegt die Latenz bereits im Minutenbereich.
Bei Lasttests mit einer recht klein dimensionierten Hardwarearchitektur (2 VCPUs) waren bereits ab 40 gleichzeitigen Transaktionen sporadische Timeouts zu beobachten, die den durchschnittlichen Durchsatz von 3.6 Transaktionen pro Sekunde auf 3.0 Transaktionen pro Sekunde verringerten. Ab 80 gleichzeitigen Transaktionen ist der Durchsatz mit 1.4 TPS eingebrochen. Die Auswahl der Hardwarearchitektur basiert auf typischen Hardwarelimitationen im Produktionsumfeld.

5 Fazit

Beschränkt durch die Limitationen in der Performance eignet sich eine Blockchain Architektur zwar nur bedingt für das unaggregierte Erfassen und Verarbeiten hochfrequenter Prozessdaten, aufgrund der Manipulationssicherheit aber sehr wohl für das oben beschriebene Szenario der Bereitstellung von Daten zu Anomalien im Prozess.

Die Vorteile kommen insbesondere dann zum Tragen, wenn die Prozessdaten verschiedenen unabhängigen Parteien, die an dem Prozess beteiligt sind, zugänglich gemacht werden müssen. Dennoch müssen auf Grund der komplexen Datenhaltung Einschränkungen bei der Abfrage von Daten aus der Blockchain berücksichtigt werden, welche eine Auswertung in Echtzeit nur bedingt zulässt. Praktische Erfahrungen innerhalb des Projektes zeigen jedoch, dass oftmals der Faktor „Echtzeit" unterschiedlich interpretiert wird und somit eine Blockchain-basierte Lösung für einige Anwendungsbereiche relevant sein kann. Gleichzeitig konnte diese Limitation innerhalb dieses Anwendungsszenarios durch die hybride Datenhaltung mit einer Off-Chain-Datenbank größtenteils überwunden werden. Schlussendlich lässt sich daher feststellen, dass der Einsatz der Blockchain innerhalb einer Produktionsabsicherung erhebliche Vorteile bieten kann, wobei mit Restriktionen in der technischen Umsetzung zu rechnen ist. Eine Machbarkeitsstudie ist dabei je Anwendungsszenario unerlässlich.

Literaturverzeichnis

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the thirteenth EuroSys conference (pp. 1-15).

Apache Software Foundation (2017). Apache Kafka. In: https://kafka.apache.org, zugegriffen am 02.3.2021.

Apache Software Foundation (2021). Apache CouchDB. In: https://couchdb.apache.org, zugegriffen am 01.05.2021.

Bauernhansl, T. (2014). Die Vierte industrielle Revolution – Der Weg in ein wertschaffendes Produktionsparadigma. Bauernhansl et al. (Hrsg.). Industrie 4.0 in Produktion, Automatisierung und Logistik: 5–35.

Bruns, Ralf, und Jürgen Dunkel (2015). Complex event processing: komplexe Analyse von massiven Datenströmen mit CEP. Springer.

Fischertechnik (2019a). Fischertechnik Lernfabrik. In: https://www.fischer.group/-/media/corporate/international/presse/images-presseinformationen/fischertechnik/2019/2019-05-all-about-automation/fischertechnik-lernfabrik.ashx, zugegriffen am 02.12.2021.

Fischertechnik (2019b). Fabrik Simulation 24V. In: https://content.ugfischer.com/cbfiles/fischer/Zulassungen/ft/536634-Factory-simulation-24V-extended-description.pdf, zugegriffen am 02.12.2021.

Herm, L. V., Janiesch, C. (2021). Towards an Implementation of Blockchain-based Collaboration Platforms in Supply Chain Networks: A Requirements Analysis. In Hawaii International Conference on System Sciences, IEEE, Hawaii.

Iansiti, M.; Lakhani, K. R. (2017): The truth about blockchain. In: Harvard Business Review, 95 (1), 118–127.

Kagermann, Henning, Wolfgang Wahlster und Johannes Helbig (2018). Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0: Abschlussbericht des Arbeitskreises Industrie 4.0. https://www.bmbf.de/files/Umsetzungsempfehlungen_ Industrie4_0.pdf.

Nakamoto, S. (2008). Bitcon: A peer-to-peer electronic cash System [white paper]. In: https://bitcoin.org/bitcoin.pdf, zugegriffen am 01.10.2021.

Pallets (2021). Flask. In: https://github.com/pallets/flask, zugegriffen am 11.08.2021.

Schlick, Jochen, u. a. 2014. „Industrie 4.0 in der praktischen Anwendung". Bauernhansl et al. (Hrsg.). Industrie 4.0 in Produktion, Automatisierung und Logistik: 57–84.

Seiger, R., Zerbato, F., Burattin, A., García-Bañuelos, L., & Weber, B. (2020). Towards iot-driven process event log generation for conformance checking in smart factories. In 2020 IEEE 24th International Enterprise Distributed Object Computing Workshop (EDOCW) (pp. 20-26). IEEE.

Soder, J. (2014). Use Case Production: Von CIM über Lean Production zu Indistrie 4.0. Bauernhansl et al. (Hrsg.). Industrie 4.0 in Produktion, Automatisierung und Logistik: 85– 102.

Wang, J.; Wu, P.; Wang, X.; Shou, W. (2017). The outlook of blockchain technology for construction engineering management. In: Frontiers of Engineering Management, 4 (1), 67–75.

Wanner, J., Herm, L. V., & Janiesch, C. (2019). Countering the fear of black-boxed ai in maintenance: Towards a smart colleague. In Proceedings of the 2019 Pre-ICIS SIGDSA Symposium.

Xu, X.; Weber, I.; Staples, M. (2019). Architecture for blockchain applications, Springer.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Juniorprofessur für Information Management
Prof. Dr. Christian Janiesch
Sanderring 2
97070 Würzburg
https://www.wiwi.uni-wuerzburg.de/lehrstuhl/bwljp1/startseite/

Autoren und Ansprechpartner

Lukas-Valentin Herm, M.Sc.

Wissenschaftlicher Mitarbeiter
lukas-valentin.herm@uni-wuerzburg.de
+49 931 31-81730

Dr. Michael Kröhn

Head of Research
ROBUR Automation GmbH
michael.kroehn@robur-automation.com

Michael Baumgart, M.Sc.

Senior Consultant Research & Development
Infosim GmbH & Co. KG
baumgart@infosim.net
+49 931 205 92 200

Julian Kolb, M.Sc.

Wissenschaftlicher Mitarbeiter
Julian.Kolb@uni-wuerzburg.de
+49 0931 31-86166

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 0931 31-89640

Prof. Dr. Christian Janiesch

Juniorprofessur für Information Management
christian.janiesch@uni-wuerzburg.de
+49 931 31-84930

D5: Entwicklung des Front-Ends

Im folgenden Ergebnisbericht werden Hintergründe, Komponenten und Details zur Entwicklung der einzelnen Front-Ends der im Projekt entwickelten Plattformen vorgestellt. Die dargestellten Arbeiten in diesem Ergebnisbericht sind aufbauend auf vorhergehenden Plattformansätzen in Produktion und Qualität erstellt worden, sodass die Entwicklung teils fallspezifisch entwickelt wurde.

1 Hintergründe der Front-End-Entwicklung

Im Rahmen der Aufgabenstellung der Plattformimplementierung für PIMKoWe war geplant, die initiale Vorsimulation in einem vollständig funktionsfähigen Plattformdemonstrator umzusetzen. Dies umfasst im Kontext des vorliegenden Teilarbeitspaketes die Realisierung der Anwenderschicht. Während hierfür ursprünglich die Entwicklung eines einzelnen Front-Ends für das gesamte Projekt und alle Plattform-Komponenten vorgesehen waren, haben es verschiedene Gründe im Projektverlauf erforderlich gemacht, diese Planung zu überdenken und stattdessen eine verteilte, aus drei Komponenten bestehende Anwenderschicht zu implementieren.

Ausgangspunkt war zunächst eine organisatorische Veränderung der Projektpartner. Die ursprünglich am Konsortium beteiligte faizod GmbH & Co. KG konnte aufgrund einer Übernahme durch die iSAX GmbH & Co. KG nicht weiter am Projekt teilnehmen. Sie konnte in angemessener Frist durch die Actiware GmbH ersetzt werden. Bei der Plattform, auf der die von Actiware in das Projekt eingebrachten Kompetenzen und Komponenten beruhen, handelt es sich ebenfalls um eine Businesskontextplattform, die jedoch nicht auf Blockchain-Technologien, sondern auf klassischen Enterprise Systemen basiert. Gleiches gilt für den beteiligten Partner Signavio, weshalb es in Summe nicht möglich war, das Kompetenzgebiet der faizod GmbH & Co. KG vollständig zu ersetzen. Die ursprüngliche Konzeption des ausgeschiedenen Partners umfasste ein erweitertes Hintergrundwissen über Blockchain-Technologien. Im Rahmen des vorgesehenen Arbeitsplans war dementsprechend abzusehen, dass sowohl die Konzeption und Umsetzung der Front-End Applikationen für die Anwendungsszenarien als auch eine schnelle und unkomplizierte Anbindung an die Blockchain nicht im gleichen Umfang möglich sein würde, da die weggefallenen Kompetenzen erst aufgebaut werden mussten. Eine weitere Änderung infolge dieses Partnerwechsels war, dass zusätzlich zur Signavio-Plattform die Actiware-Plattform an die Blockchain angebunden werden sollte. Zusammen mit der Blockchain wäre also die Anbindung des neu zu entwickelnden Front-Ends an insgesamt drei verschiedene Anwendungen notwendig gewesen. Die oben dargestellte Koordination und Abstimmung stellt im Rahmen von Blockchain zunächst verschiedene Herausforderungen dar, die ebenso in der Forschung wiederzufinden sind. Organisatorische Hindernisse behandeln dabei meist mit hohem Koordinationsaufwand innerhalb von BC-Konsortien (Sunyaev et al. 2021), Datenschutz- und Sicherheitsfragen, regulatorische Unsicherheit, da mehrere Parteien ihre Kräfte bündeln müssen. Weiterhin können solche Situationen nur durch gemeinsame Kollaborationen behandelt werden, da in der Praxis oft Widerstand gegen Veränderungen und das Fehlen eines klaren Nutzens der BC-Technologie wahrgenommen wird (Hackius und

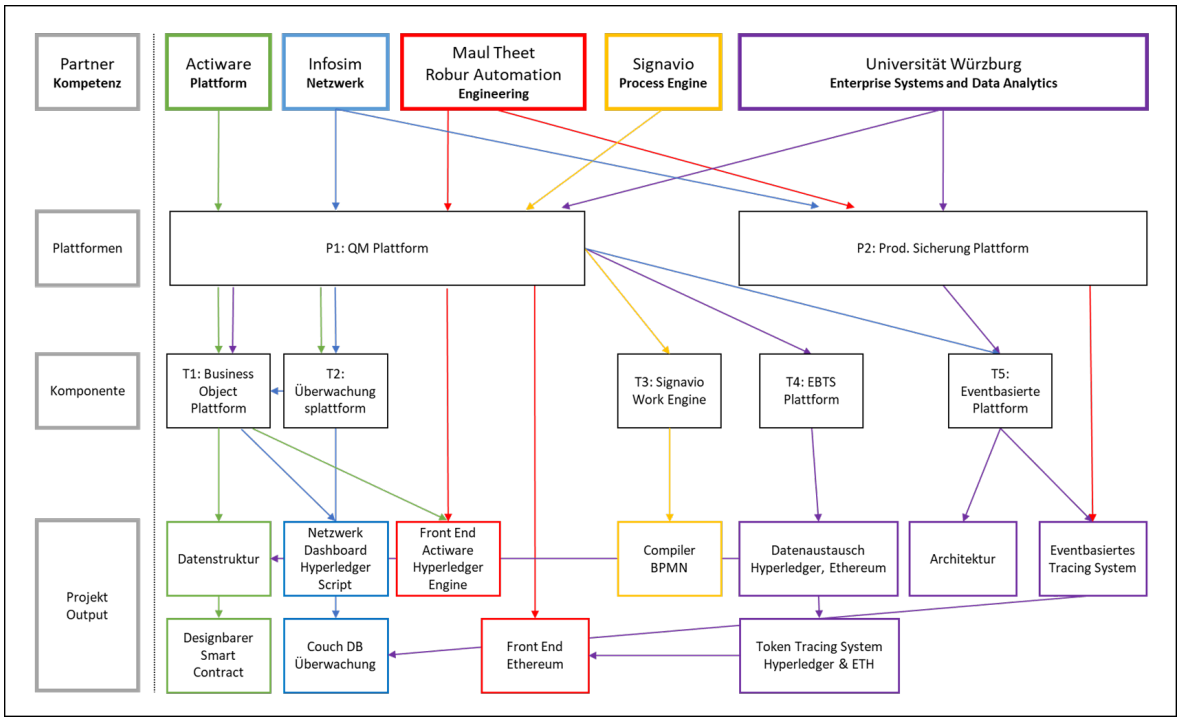


Abbildung D.5.1: Übersicht über die Projektpartner, Plattformen und Outputs

Petersen 2017). Daher hat sich das PIMKoWe-Konsortium mit der Frage befasst, inwieweit es sinnvoll ist, auf bestehende Tools zurückzugreifen, um die Mehraufwände zu verringern und gleichzeitig Mehrwerte im Sinne einer Integration und den gesteigerten Nutzen der Blockchain in bestehende Geschäftsmodelle zu schaffen. Daraufhin wurde die Entscheidung getroffen, anstelle eines neu zu entwickelnden Front-Ends vorhandene Softwarelösungen zu verwenden, darauf aufzusetzen und mithilfe passender technischer Schnittstellen die Darstellung und Interaktion mit den anzubindenden und vorhandenen Komponenten leicht zu modifizieren und zu realisieren.

Da Infosim als Hersteller eines automatisierten Netzwerk- und Servicemanagementsystems bereits ein Produkt zur Visualisierung besitzt, das die Anbindung und Überwachung verschiedener Datenquellen sowie die Datenverarbeitung und -darstellung als Fokus hat, bot dieses Softwareprodukt bereits die Basis für die Implementierung von Front-End Komponenten. Die von Actiware entwickelte Blockchain-Überwachungsplattform sowie die von der Universität Würzburg entwickelte eventbasierte Plattform konnten so auf effektive Weise umgesetzt werden (siehe Abbildung D.5.1).

Durch diese Entscheidung konnten zusätzlich zur Zeitersparnis weitere positive Effekte erzielt werden. Dadurch, dass der Fokus primär auf der Anbindung an eine bestehende Software lag, konnte besonderes Augenmerk auf die Entwicklung und Anpassung der Schnittstellen zu den Datenquellen gelegt werden. Im Zuge dessen sind zusätzlich von Infosim Ansatzpunkte identifiziert worden, die bestehende Softwarelösung hinsichtlich Anbindung weiterer Schnittstellen und erweiterter Darstellungsmöglichkeiten weiterzuentwickeln. Zudem konnten die Anbindungen der Datenquellen robuster gestaltet werden.

2 Einzelne Front-Ends

Die drei im Rahmen des Teilarbeitspakets entwickelten Front-End Anwendungen dienen dazu, die in der zugehörigen Komponente erzeugten Daten einheitlich zu visualisieren. Dazu wurde als Teilkomponente der Front-Ends jeweils ein zugehöriges Dashboard entwickelt, auf dem die entsprechenden gesammelten Daten übersichtlich dargestellt werden. Im Folgenden werden die einzelnen Front-Ends der Plattformen und alternative Ansätze zu Hyperledger Fabric vorgestellt.

3 Hyperledger Überwachungs-plattform

Zur Überwachung der Hyperledger Plattform im Rahmen der Qualitätssicherungs-Plattform wurde von Infosim ein Überwachungsskript für Blockchains entwickelt, das Daten aus einer Blockchain an Remote Procedure Call (RPC)[1] oder Representational State Transfer (REST)[2] Endpunkten extrahieren kann. Dieses Skript liest unter anderem Informationen über die Länge der Blockchain, die Größe des letzten Blocks in Byte und die Anzahl der zugehörigen Transaktionen aus, die als KPIs von der Blockchain-Software zur Verfügung gestellt werden.

Zur Visualisierung wurden die Analyzer- und Dashboard-Komponenten der StableNet® Software von

Abbildung D.5.2: Blockchain Monitoring Dashboard

[1] Ein Remote Procedure Call (engl. „Aufruf einer fernen Prozedur“) ermöglicht es, einen Prozess auf einem anderen Computer zu starten. Der Start erfolgt durch eine Anfrage an einen bestimmten Endpunkt, an dem, je nach aufgerufenem Prozess, auch die ermittelten Daten ausgelesen werden können.

[2] Representational State Transfer ist ein Paradigma für die Softwarearchitektur von verteilten Systemen und definiert Anforderungen, aus welchen ein vereinfachter Datenaustausch erfolgen soll. Insbesondere beinhaltet REST Vorgaben zur Definition von Schnittstellen.

Blockchain-Software zur Verfügung gestellt werden.
Zur Visualisierung wurden die Analyzer- und Dashboard-Komponenten der StableNet® Software von Infosim verwendet. Das zugehörige Dashboard, zu sehen in Abbildung D.5.2, zeigt die vom Skript gemessenen KPIs an. Zu erkennen sind mehrere Diagramme, die den zeitlichen Verlauf der einzelnen KPIs angeben und minütlich automatisch neu generiert werden.
Durch die zugrunde liegende Software können weitere Ansichten manuell generiert und bei Bedarf auch in das Dashboard integriert werden. Beispielsweise ist der verwendete Zeitausschnitt beliebig anpassbar und durch die Kombination von Messwerten können Durchschnittswerte errechnet werden, um einen vorhandenen Trend besser herauszustellen.
Diese Komponente wurde von Actiware verwendet, um ein Monitoring der Blockchainverbindung zur ACTIWARE.IO-ECM Plattform durchzuführen. Wie in den vorherigen Ergebnisberichten D1 und D2 dargelegt, ist in dem Use Case das Tool zum externen Monitoring des gesamten Netzwerks aufgesetzt worden. Hintergrund ist dabei, den Nachweis führen zu können, dass in dem Channel nur diejenigen Einträge vorgenommen werden, die auch von den beteiligten Unternehmen jeweils getätigt worden sind. Damit wird eine Unabhängigkeit von denjenigen Plattformen wie beispielsweise der ACTIWARE ECM Plattform erreicht, die sich für das Schreiben, Lesen und die inhaltliche Ausgestaltung der Smart Contracts verantwortlich zeigt.
Neben der Überwachung des Netzwerks war die Implementierung eines Front-Ends für die Anwender vonnöten. Zur inhaltlichen Überprüfung der vorgenommenen Transaktionen wurde von ACTIWARE ein Smart Form Generator für D-Apps entwickelt, der die Daten aus unterschiedlichen Quellen konsumieren kann. Das in Abbildung D.5.3 gezeigte Systemdesign illustriert dabei die angewendete Struktur des Netzwerks.
Über den Generator lassen sich individualisierte Formulare erstellen, die somit auf die unterschiedlichen Projektgegebenheiten angepasst werden können. Die Anzeige von Informationen wird dabei als Website/D-App möglich. Im Rahmen des Projekts war dies für den Qualitätssicherungs-Use

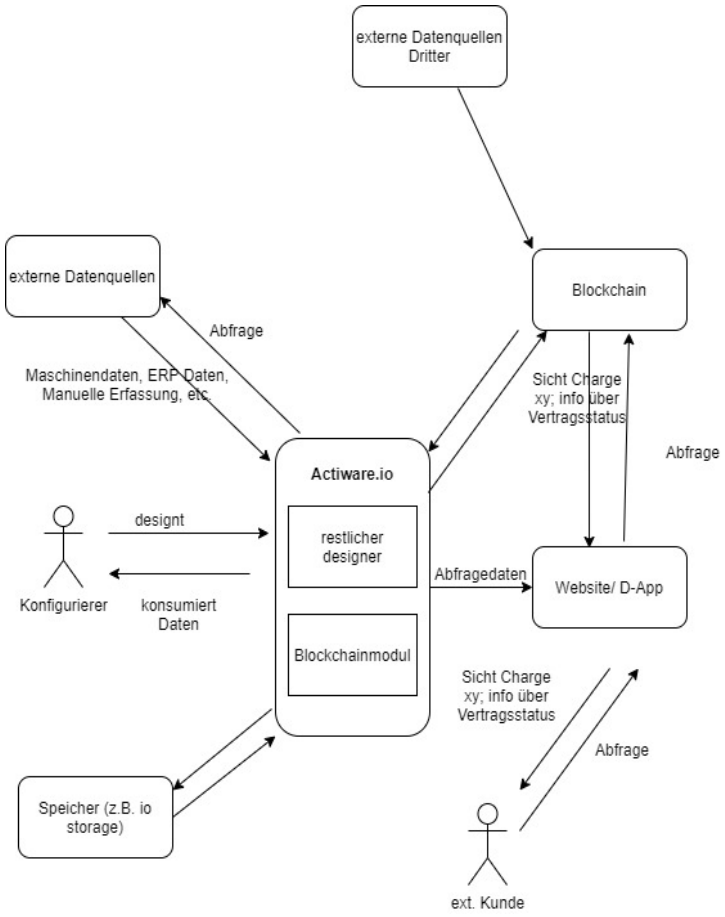


Abbildung D.5.3: Systemdesign der unterschiedlichen Komponenten zur Einbindung der ACTIWARE Plattform

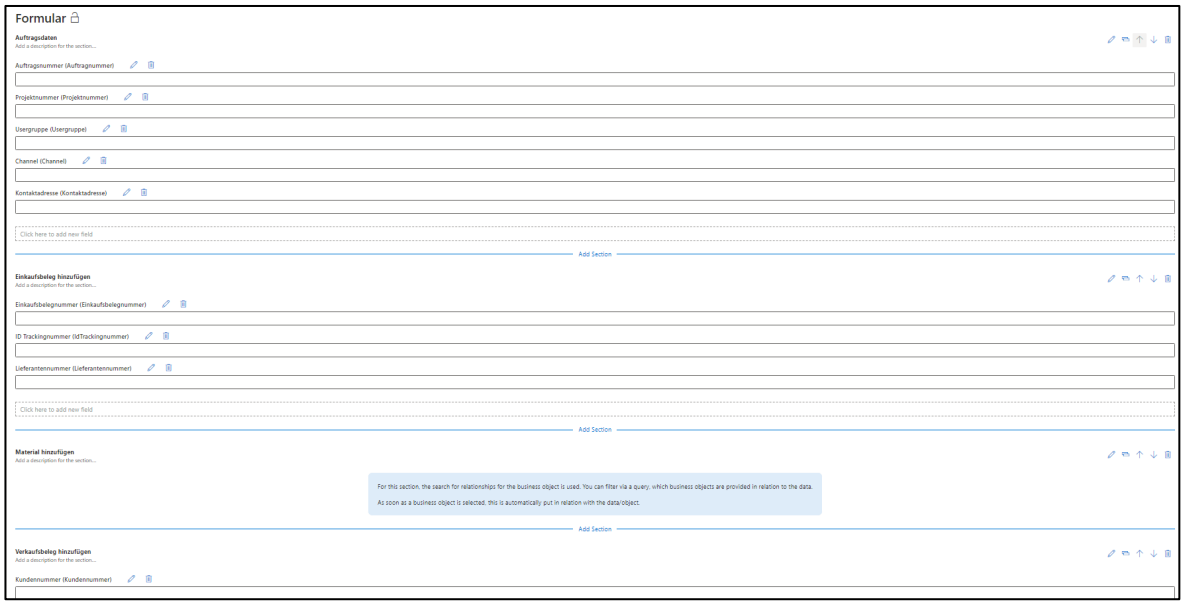


Abbildung D.5.5: Formular in der Designer-Ansicht

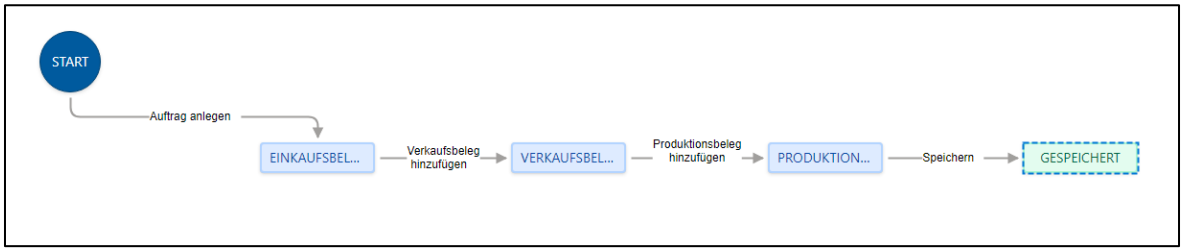


Abbildung D.5.4: Modellierter Flow auf dem Formular

Case beim Anwendungspartner Maul-Theet GmbH notwendig. Hier wurde ein Front-End konfiguriert, das die Bestätigung von Produktions- sowie Qualitätssicherungsprozessen ermöglicht. Dabei lassen sich verschiedene Workflows konfigurieren, die Daten auf der Blockchain inklusive Smart Contracts einbeziehen können. Damit können Transition Flows definiert werden, der per Formular dann abgebildet werden. In den Abbildungen **Fehler! Verweisquelle konnte nicht gefunden werden.**D.5.4 und Abbildung D.5.6 kann man den Designer für das Formular, den dahinterliegenden modellierten Prozess sowie das fertige Formular erkennen. Durch die flexible Gestaltung über die ACTIWARE Plattform ist es somit möglich, auf unterschiedliche Events zu reagieren und gleichzeitig auf unterschiedliche Datenquellen zugreifen zu können. Smart Contracts und Daten unterschiedlicher Datensenken werden somit für den Endanwender konsumierbar.

4 Eventbasierte Plattform

Das zweite entwickelte Front-End basiert ebenfalls auf der Software StableNet, jedoch wird hier zusätzlich zu den oben verwendeten Komponenten auch die Weather Map-Komponente benutzt. Die angezeigten Daten werden mit einem Programm verarbeitet, das speziell für diesen Zweck entwickelt wurde. Von diesem Programm werden Daten aus der Off-Chain-Datenbankschicht der in Teilarbeitspaket D4 entwickelten Eventarchitektur ausgelesen, aggregiert und zur Darstellung weitergegeben. Die Darstellung der Daten erfolgt ebenfalls durch ein Dashboard, das mehrere Komponenten beinhaltet und in Abbildung D.5.7 zu sehen ist. Die zentrale Komponente zeigt eine vogelperspektivische Ansicht des zugrundeliegenden Fabrikmodells Industrie 4.0 der Marke Fischertechnik. Die

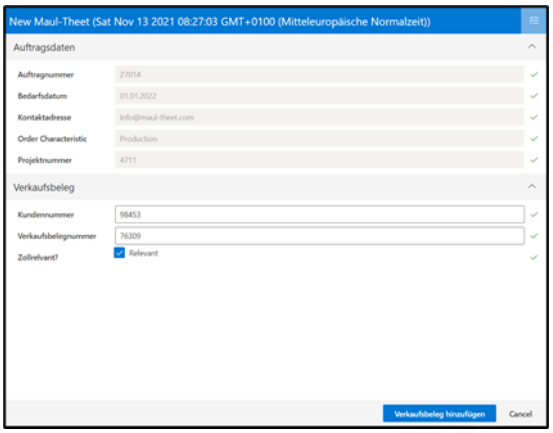


Abbildung D.5.6: Formular in der Endanwender-Ansicht

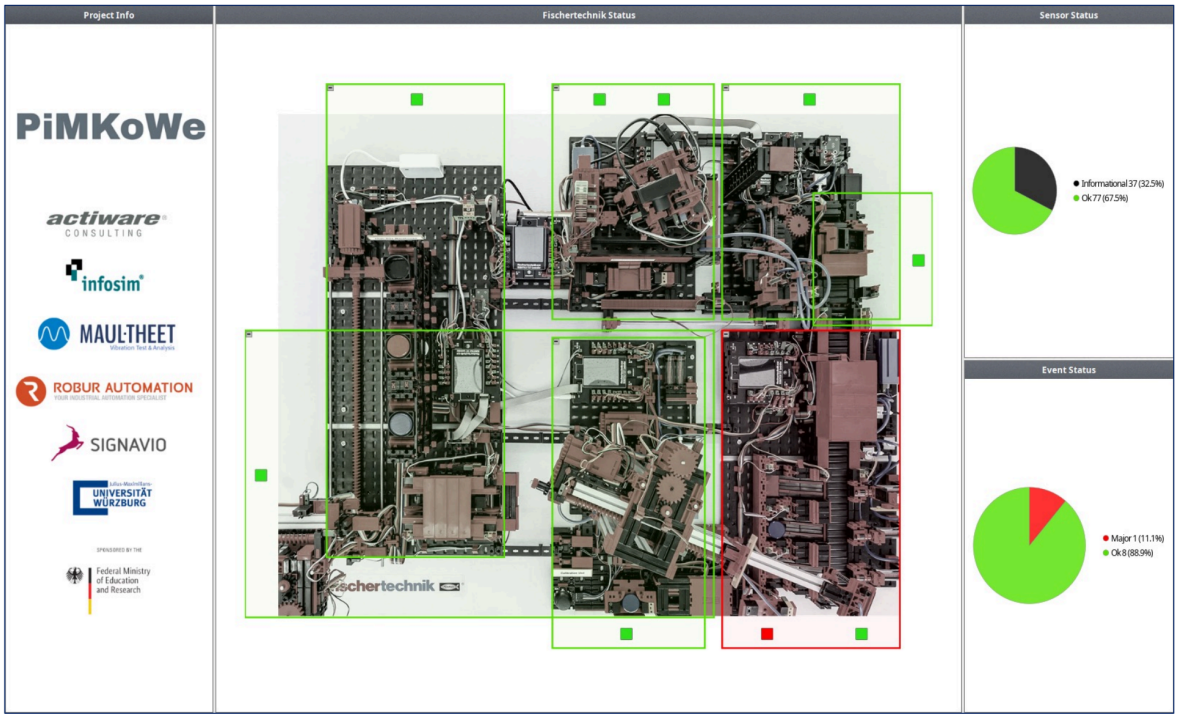


Abbildung D.5.7: Dashboard im Front-End der eventbasierten Plattform

Ansicht ist in mehrere Teilbereiche unterteilt, die durch Rahmen getrennt sind und den Zustand der zugehörigen Modellkomponenten durch ihre Farbe vorgeben. Ist der Teilbereich grün eingefärbt, wurde bei der letzten Sensormessung in der Produktion kein Problem festgestellt. Ist der Bereich rot gefärbt, liegt eine Störung oder ein besonderes Ereignis vor. Entstandene Ereignisse werden automatisch den verschiedenen Teilbereichen zugeordnet. Die zwei Kreisdiagramme auf der rechten Seite beschreiben zusätzlich den aktuellen Status der Sensorinformationen sowie die aus den Sensordaten berechneten Ereignisse. Bei der Entwicklung des Dashboards wurde besonderes Augenmerk daraufgelegt, dass für einen Benutzer auf einen Blick alle relevanten Informationen über den aktuellen Status des Modells, bzw. in Zukunft über eine Industrie 4.0-Fabrik, zu erfassen sind. Das Dashboard kann außerdem einfach angepasst werden, um die angezeigten Daten auf bestimmte Benutzergruppen zu beschränken.

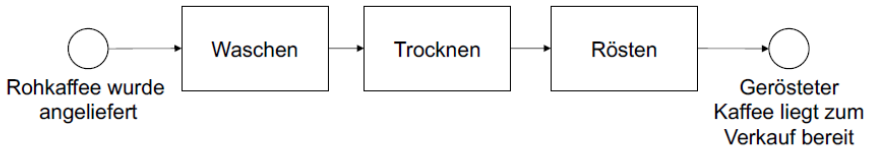
Zusätzlich zum Dashboard kann eine interaktive Version der zentralen Komponente in der Weather Map-Ansicht geöffnet werden. Hier besteht die Möglichkeit, die Komponente zu bearbeiten und mit Tooltips weitere Details zu den einzelnen Ereignissen anzuzeigen.
Weitere Details zur Implementierung des Programms finden sich im Abschlussbericht der in Teilarbeitspaket D4 implementierten Eventarchitektur.

5 Front-End auf Basis eines Ethereum Blockchain Netzwerkes

Dieses Unterkapitel behandelt die Darstellung und Entwicklung einer einfachen Applikation, in der Kaffeebohnen hergestellt und an den Kunden ausgeliefert werden. Die universitäre Einrichtung hat sich dazu entschlossen, die Ethereum Plattform als alternativen Ansatz zur Hyperledger Fabric Plattform zu betrachten, da verschiedene Forscher Token-basierte Ansätze (ERC 721 und ERC1155) zur Rückverfolgung von Produkten oder Produktstrukturen verwenden (Kuhn et al. 2021; Madhwal et al. 2021; Westerkamp et al. 2020).
Ausgehend von dieser Möglichkeit wurde eine einfache Lieferkette in einem ERP System abgebildet. Der Produktionsprozess besteht dabei aus drei Aktivitäten und zwei Zuständen. Abbildung D.5.8 stellt diesen in einer einfachen BPMN-Notation

Abbildung D.5.8: Produktionsprozess Rohkaffee

dar. Im Initialzustand wurde das Ausgangsprodukt Rohkaffee angeliefert. Dieses wird zunächst im ersten Prozessschritt gewaschen. Dabei werden die Kaffeekirschen in Schale und Bohne aufgeteilt. Dadurch entsteht das Produkt „gewaschener Kaffee“. Durch den zweiten Prozessschritt (Trocknen) resultiert daraus das Produkt „getrockneter Kaffee“. Im dritten und letzten Prozessschritt findet die Veredelung statt: Die Röstung des getrockneten Kaffees. Das Endprodukt „gerösteter Kaffee“



liegt anschließend im Endzustand des Prozesses zum Verkauf bereit.
Zentrale Visualisierung des Kaffeebeispiels und einer Applikation ist die Speicherung von Daten zur Transparenzherstellung für den Endanwender in einem Frontend (siehe Abbildung D.5.9). Die Blockchain Technologie dient dabei als ein dezentraler Datenspeicher, der diese Transparenz von verschiedenen Lokationen bereitstellen kann und zudem eine hohe Unveränderbarkeit für notwendige Daten aufweist. Diese Attribute qualifizieren die Blockchain Technologie für die dargestellte Anwendung zur Rückverfolgbarkeit entlang der Kaffeewertschöpfungskette. Das Front-End bedient sich dabei nur den Informationen aus dem Blockchain Netzwerk.
Vorab und während der konzeptionellen Phase sowie während der Entwicklung einer Middleware traten unterschiedliche Herausforderungen auf, von denen im Folgenden einige näher erläutert werden. Das aktuelle ERP System eines Softwareproviders, die Ethereum Blockchain und IPFS bieten im Standard keine integrierte Möglichkeit, um direkt miteinander interagieren zu können. Somit mussten zuerst die bereits existierenden Schnittstellen aller Systeme eruiert und im Detail betrachtet werden. Für das ERP-System bestand durch eine Webhook- Funktionalität eine Möglichkeit, Benachrichtigungen zu versenden, sobald innerhalb des Systems ein bestimmter Prozess getriggert wird. Diese gesendeten Daten sollten ursprünglich zur Nachverfolgbarkeit verwendet werden, allerdings waren diese sehr grob gehalten und nicht ausreichend für den Anwendungsfall und die anvisierte Visualisierung. Bei der Erstellung einer Lagerbestandsbewegung im ERP-System werden beispielsweise zu wenig Daten bereitgestellt, sodass sowohl auf ERP Seite und Middleware Seite Erweiterungen erstellt werden mussten, um die Daten in einem standardisierten Format in die Blockchain zu übergeben. Für das Abrufen der Daten aus der Blockchain wurde schließlich eine Web-anwendung entworfen (siehe Abbildung D.5.10). Diese wurde mithilfe des JavaScript-Frameworks React entwickelt. Im Folgenden wird mithilfe von JavaScript und React exemplarisch der Verlauf eines Produktes über verschiedene Lagerhäuser mit Zeitstempeln dargestellt. Der Endanwender erhält so einfache Informationen zum Verbleib des Kaffees.
Aufgrund verschiedener ERP Datenmodelle bestehen bei der Entwicklung eines Front-Ends grundsätzlich die Herausforderungen, verschiedene Objekte korrekt darzustellen. Im oben genannten Beispiel sind beispielsweise Warehouse Name und Number dargestellt, die verschiedene Lokationsobjekte und den physischen Verlauf des Produktes wiedergeben. Speziell bei ERP Systemen kann es in einem Konsortium allerdings zu einem erhöhten Abstimmungsbedarf und konkurrierende Interessen kommen. Exemplarisch kann dies an verschiedenen Industrielösungen aufgezeigt werden. Führende Softwareprovider bieten beispielsweise Lösungen an, bei der Lokationsobjekte als optionale Information betrachtet werden. Industrieunternehmen aus dem Automobilbereich entwickelten dagegen erste Prototypen, die eine Lokation eines Bauteils berücksichtigen (vgl. SAP 2021, und Miehle et al. 2019). Es gilt grundsätzlich vor der Entwicklung eines Front-Ends, den genauen Informationsbedarf im Konsortium abzustimmen, um mögliche Fehlentwicklungen zu vermeiden.

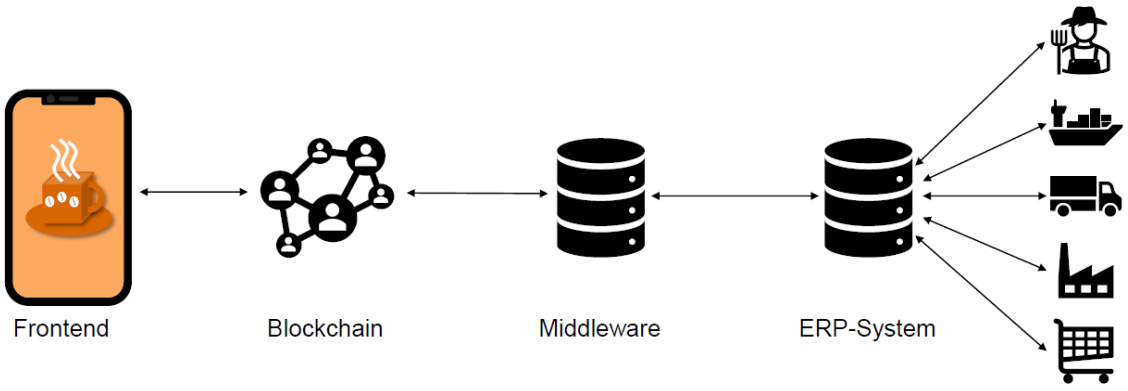


Abbildung D.5.9: Simplifizierter Informationsfluss von Daten zur Darstellung der Kaffeeproduktion

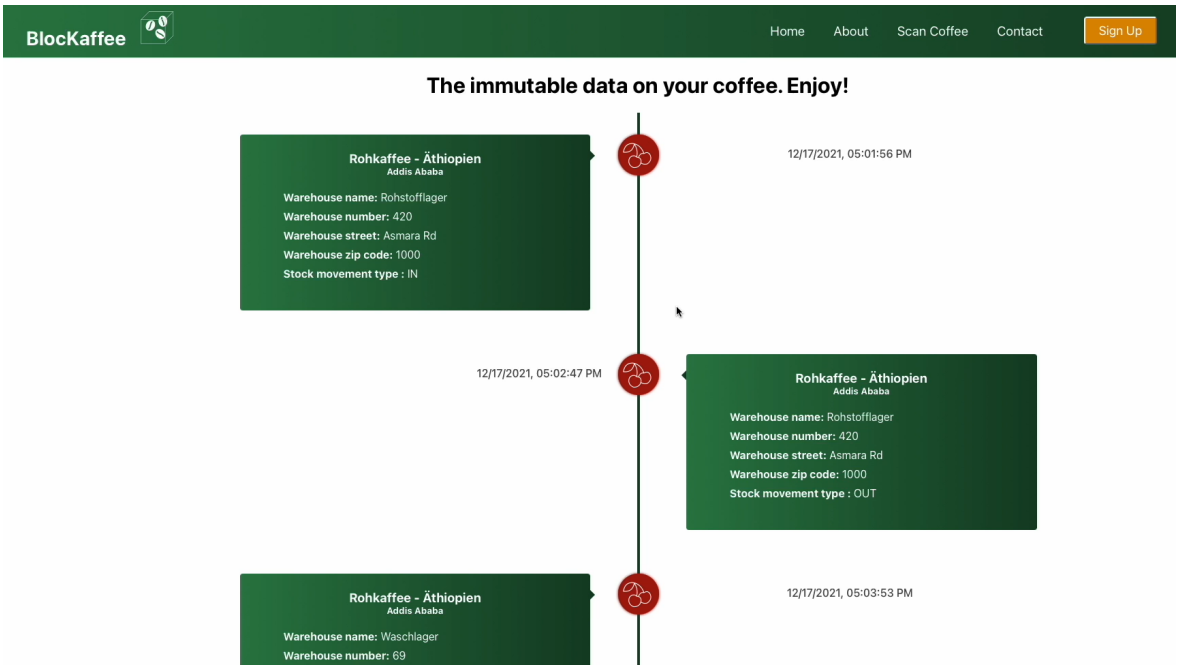


Abbildung D.5.10: Front-End BlocKaffee React APP

6 Fazit

Im Rahmen der Umsetzung des Front-Ends zeigte sich, dass die Verwendung von mehreren Front-Ends statt wie ursprünglich geplant, einem Einzelnen von Vorteil ist.
Einerseits konnte dadurch besser auf die unterschiedlichen Anforderungen der Use Cases eingegangen werden. Dadurch, dass die Front-Ends auf bestehenden Lösungen aufbauen, konnte zusätzlich der Anwendungsrahmen der Lösungen um weitere Use Cases wie z.B. dem Einsatz in neuen industriellen Anwendungsgebieten, erweitert werden. Auch konnten von den Partnern Use Case-spezifische Kenntnisse gewonnenen werden, die in Zukunft unmittelbar in die Produktentwicklung einfließen können.

Literaturverzeichnis

Kuhn, M., Funk, F., Zhang, G., and Franke, J. 2021. "Blockchain-based application for the traceability of complex assembly structures," Journal of Manufacturing Systems (59), pp. 617–630.

Madhwal, Y., Chistiakov, I., and Yanovich, Y. 2021. "Logging multi-component supply chain production in blockchain," in: 2021 The 4th International Conference on Computers in Management and Business, pp. 83–88.

Miehle, D., Henze, D., Seitz, A., Luckow, A., and Bruegge, B. 2019. "PartChain: a decentralized traceability application for multi-tier supply chain networks in the automotive industry," in: 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), IEEE, pp. 140–145.

SAP, S. 2021. Administration Guide for LBN Material Traceability Document Version: BN MT 3.1 – 2021-12-13. Accessed: 27-04-2022.

Sunyaev, A., Kannengießer, N., Beck, R., Treiblmaier, H., Lacity, M., Kranz, J., Fridgen, G., Spankowski, U., and Luckow, A. 2021. "Token economy," Business & Information Systems Engineering (63), pp. 1–22.

Westerkamp, M., Victor, F., and Küpper, A. 2020. "Tracing manufacturing processes using blockchainbased token compositions," Digital Communications and Networks (6:2), pp. 167–176.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Juniorprofessur für Information Management
Prof. Dr. Christian Janiesch
Stephanstraße 1
97070 Würzburg
https://www.wiwi.uni-wuerzburg.de/lehrstuhl/bwljp1/startseite/

Autoren und Ansprechpartner

Lukas-Valentin Herm, M.Sc.

Wissenschaftlicher Mitarbeiter
lukas-valentin.herm@uni-wuerzburg.de
+49 931 31-81730

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 0931 31-89640

Dr. Michael Kröhn

Head of Research
ROBUR Automation GmbH
michael.kroehn@robur-automation.com

Prof. Dr. Christian Janiesch

Juniorprofessur für Information Management
christian.janiesch@uni-wuerzburg.de
+49 931 31-84930

Michael Baumgart, M.Sc.

Senior Consultant Research & Development
Infosim GmbH & Co. KG
baumgart@infosim.net
+49 931 205 92 200

Dr. Patrick Bredebach

Productmanager
Actiware Development GmbH
patrick.bredebach@actiware-development.com
+49 231 5347 2540

Ole Jankowski, B.Sc.

Solution Architect
Actiware Development GmbH
ole.jankowski@actiware-development.com

D6: Integration von Teilkomponenten

Über die verschiedenen Use Cases und Arbeitspakete hinweg wurde von den Partnern an mehreren separaten Teilkomponenten für die Plattformen gearbeitet. Für die Umsetzung der geplanten Funktionalitäten der finalen Plattformen war es notwendig, die Komponenten zu kombinieren. In diesem Kapitel werden erst die hierfür verwendeten Teilkomponenten beschrieben und anschließend wird auf das Vorgehen bei deren Integration zu den Plattformen eingegangen.

1 Integration der Teilkomponenten für die Qualitätssicherungs-Plattform ACTIWARE.IO

Im Folgenden wird ein kompakter Einblick in die ACTIWARE.IO ECM-Plattform und Komponenten gegeben, die für das Projekt verwendet wurden. Zusätzlich finden weitere Möglichkeiten der Plattform Erwähnung. Zur Einordnung in das Projekt sei auf die Abbildung D.6.1 verwiesen. Im Projekt wurde die ACTIWARE.IO für den Qualitätsanwendungsfall mittels eines Business Object Modells umgesetzt.

Die ACTIWARE.IO Plattform bietet die Möglichkeit, in Form mehrerer grafischer Oberflächen in der Teilkomponente **Prozessautomat** sogenannte Prozesse zu konfigurieren. Diese Prozesse bestehen aus einzelnen Prozessschritten, welche Prozessoren genannt werden. Prozessoren bilden einzelne Aufgaben ab und werden in Modulen nach Funktionalität gruppiert.

Module existieren für die unterschiedlichsten Aufgaben, beispielsweise zum Abfragen von SharePoint, Office 365, SAP Objekten. Über diese Module und Kernfunktionalitäten wurden beispielsweise schon über 80 ERP Systeme an die ECM Plattform in diversen Kundenprojekten angeschlossen. Die Module ermöglichen die Interaktion mit den jeweiligen Drittanwendungen, indem Daten abgefragt, gematcht und an Drittanwendungen gesendet werden.

Um an die Kundenbedürfnisse anpassbar zu sein, bietet die ECM-Plattform die Möglichkeit, kaufmännische Objekte zu definieren. Diese bilden ein kundenindividuelles Datenmodell ab und repräsentieren Objekte wie Rechnungen oder Kunden.

Die **ProcessEngine (TK1)** ist der Kern der Plattform. Hier werden die Prozesse ausgeführt und die logischen Operationen durchgeführt. Die ProcessEngine läuft als Service nativ unter Windows oder als Container in einer Docker Umgebung. In der Process-Engine werden die im Prozessautomaten designten Prozesse ausgeführt. Die Prozesse selbst können per Trigger händisch über verschiedene Clients oder beispielsweise per REST-Aufruf gestartet werden.

Die im Projekt eingesetzten Prozesse sorgen dafür, dass Daten aus ERP Systemen geladen und zusammengeführt werden. Es ist möglich, diese Daten nach der Verarbeitung in unterschiedlichen Datensenken zu speichern. Zu diesen Datensenken gehört unter anderem auch die Blockchain.

Neben den Prozessen bieten **Smart Forms** die Möglichkeit, Formulare zur Visualisierung zu definieren und für diese Workflows einzurichten. Eine Konfigurationsmöglichkeit ist, dass erfasste Daten automatisch auf eine Blockchain geschrieben und von dort wieder geladen werden, sobald sie angezeigt werden sollen. Die Formulare werden dabei auch über eine grafische Oberfläche designt. Sie können auf Daten aus unterschiedlichen Datensenken zugreifen. Dabei ermöglichen sie es nicht nur, Daten bei der Interaktion mit Nutzern anzuzeigen und validieren zu lassen, sondern stellen auch Workflows bereit, die je nach designtem Schritt einen Status auf den Prozess oder ein Objekt setzen können.

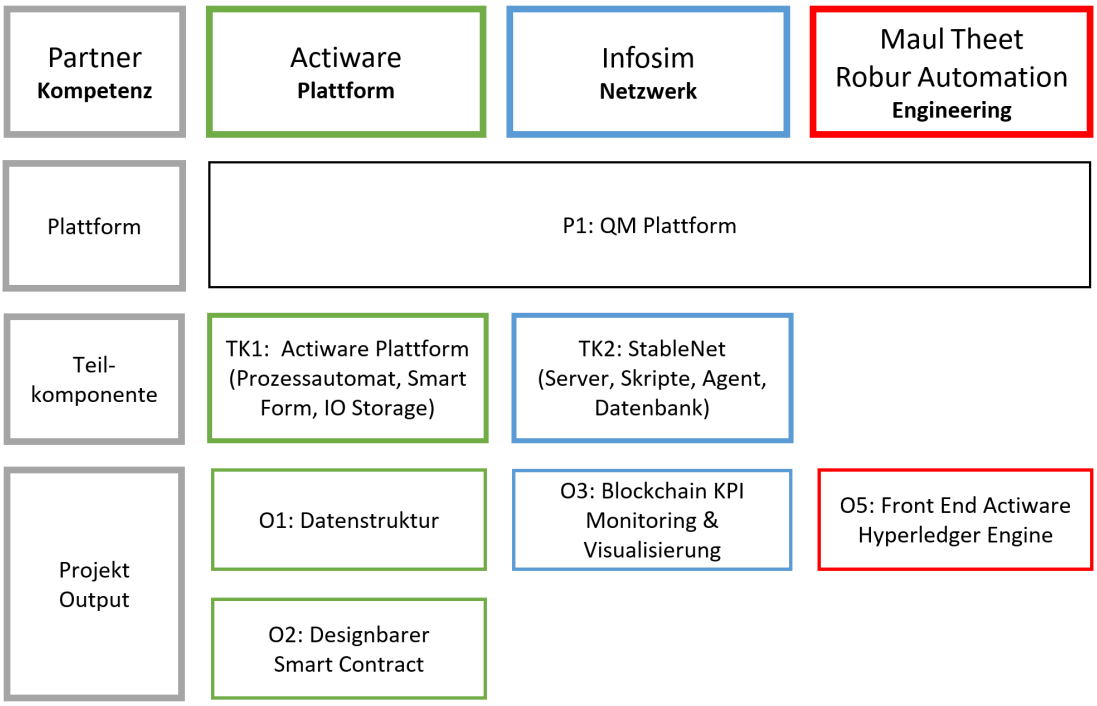


Abbildung D.6.1: Übersicht über die Komponenten der QM Plattform

Im Projekt werden Smart Forms dafür benutzt, einen Produktions- und Qualitätsmanagementprozess für P1 + P2 (siehe zur Orientierung Abstract Kapitel des Arbeitspaketes D) abzubilden und eine einfache Nachverfolgbarkeit der produzierten Güter zu ermöglichen. Zugleich dienen die Formulare zur Interaktion mit den Anwendern. Weiterhin dienen sie zur Anzeige der in den Use Cases abgebildeten Businessobjekte sowie zur möglichen Korrektur und Anreicherung der Daten durch den Anwender. Die Daten zu den Objekten können dabei in unterschiedlichen Datensenken gespeichert sein, darunter auch in verschiedenen Blockchainnetzwerken.

Der **IO-Storage** ermöglicht die Speicherung von Dokumenten und Daten. Zudem werden automatisch Beziehungen zwischen einzelnen Datensätzen erstellt und gepflegt. Die gespeicherten Daten und Dokumente können zusätzlich mit nützlichen Metadaten angereichert werden, welche bei einer weiteren Verarbeitung Verwendung finden können. Im IO-Storage ist es möglich, kaufmännische Objekte anzulegen und anzusehen – perspektivisch auch mit einer Abwandlung der oben genannten Formulare. Diese sind im Unterschied zu den Smart Forms nur in der Lage, ein einzelnes kaufmännisches Objekt anzuzeigen/zu bearbeiten. Zudem kann es keinen Workflow abbilden.

Im Projekt wird der **IO-Storage** zur Speicherung von Daten, der Herstellung der Beziehung unter diesen Daten sowie für die Erfassung von Materialien im Produktions- und Qualitäts-Prozess genutzt. Er ist somit der zentrale lokale Speicher von Informationen zu den Business Objekten.

Auf der Hyperledger Fabric wird ein Standard Smart Contract der ACTIWARE.IO Plattform deployt. Die Plattform stellt dann die Daten als Hashwerte, verschlüsselt oder im Klartext, im Blockchain Netzwerk bereit.

Im Projekt wird die Blockchain unter anderem als manipulationssicherer Speicher genutzt. Hierüber wird ein Lieferketten übergreifendes Fehlermanagement ermöglicht. Ferner können auf der Blockchain Smart Contracts generiert werden, deren Inhalt und Logik über Prozesse in der Plattform bereitgestellt und auf die Blockchain geschrieben werden können.

2 StableNet® Teilkomponenten

Um die korrekte Funktionstätigkeit aller Komponenten sicherzustellen, wird die Software **StableNet® (TK2),** ein automatisiertes Netzwerk- und Service Management System der Firma Infosim, verwendet.

Der primäre Nutzen, den die Software in diesem Kontext bietet, ist ein zentralisiertes Überwachen der einzelnen Komponenten. Durch das regelmäßige Abfragen von Endpunkten der Plattform-Teilkomponenten können Fehler aufgedeckt und Nutzer benachrichtigt werden, dass ein Problem vorliegt.

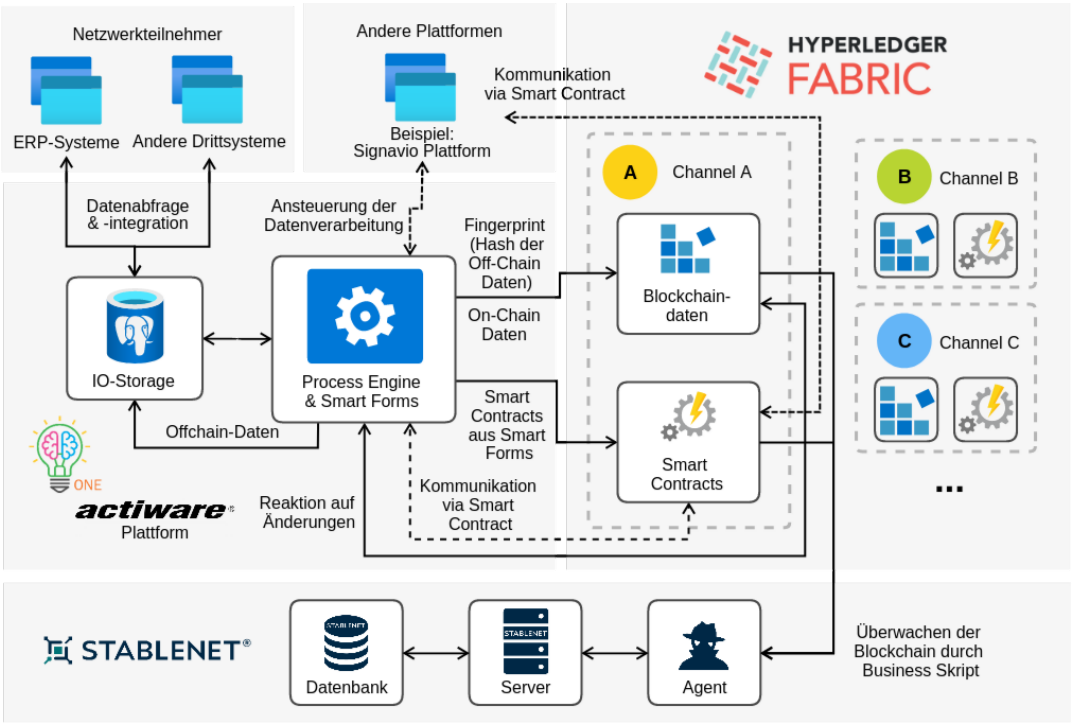


Abbildung D.6.2: Interaktion zwischen den Teilkomponenten der Qualitätssicherungsplattform (P1)

StableNet besteht aus mehreren Komponenten, die unterschiedliche Zwecke erfüllen und miteinander kommunizieren. Sie sind in Abbildung D.6.2 abgebildet.

Der Server als Kernkomponente der Software übernimmt die Orchestrierung der einzelnen StableNet Teilkomponenten und die Verarbeitung der Messdaten.

Die Datenbank dient zur langfristigen Speicherung der Messdaten. Für weit zurückliegende Ereignisse werden einzelne Datenpunkte aggregiert, um die Menge der gespeicherten Daten zu reduzieren. Auch Definitionen von Messungen, angelegte Nutzer, Einstellungen u.Ä. werden hier gespeichert.

Die Überwachung der Plattform-Komponenten wird mit dem Agenten durchgeführt. Dabei handelt es sich um ein Programm, das die periodisch auszuführenden Datenabfragen verwaltet und durchführt.

Um Abfragen auszuführen, die nicht zum vordefinierten Umfang gehören, besteht die Möglichkeit, sog. Business Skripte einzusetzen. Dabei handelt es sich um Skripte, die vom Agenten statt einer regulären Messung ausgeführt werden und das Abfragen und u.U. Vorverarbeiten anstelle des Agenten übernehmen. Zur Abfrage der Hyperledger Fabric Blockchaindaten der Qualitätssicherungs Plattform wird beispielsweise ein solches Skript verwendet.

Agenten können unabhängig vom Server in beliebigen, unterschiedlichen privaten Netzwerken platziert werden. Dadurch besteht die Möglichkeit, zusätzlich zum Monitoring von Kernkomponenten wie z.B. der Blockchain, weitere Systeme anzubinden. Hier kommen beispielsweise Drittsysteme u.U. auch in Kundenumgebungen in Frage.

Im Rahmen des Projekts wurde die Software durch das Entwickeln von drei solcher Business Skripte um Funktionalität zur Überwachung zweier zuvor nicht messbarer Endpunkte erweitert: CouchDB und verschiedene Blockchains (Dash, Hyperledger Fabric, …). Nähere Details zu Vorgehen, Funktionsweise und Implementationsdetails der Skripte finden sich in den Abschlussberichten D4 (CouchDB Skript) und D5 (Blockchain Skripte).

Eine weitere Funktionalität, die die Software anbietet, ist eine Komponente zur Automatisierung von bestimmten Tätigkeiten. Beispielsweise können Backups bestimmter Datenquellen nach einer einmaligen Konfiguration automatisiert ausgeführt und damit eine Ausfallsicherheit garantiert werden.

3 Integration der Teilkomponenten in P1 + P2

Im Rahmen der implementierten Plattformen zum Qualitätsmanagement und zur Produktionssicherung wurden die Komponenten je unterschiedlich miteinander kombiniert. So wurden mittels der StableNet Software die durch ACTIWARE.IO vorgenommenen Transaktionen validiert. Dadurch können Aktivitäten im Blockchain Netzwerk von Dritten überprüft werden, was eine weitere Sicherheitsstufe zur Plattform hinzufügt. Dies ist insbesondere dann von Interesse, wenn durch unterschiedliche Middlewares auf einen Kanal in der Lieferkette zugegriffen wird und Transparenz hergestellt werden soll. Das Datenmodell lässt es zu, dass verschiedene Teilnehmer einer Lieferkette einen gemeinsamen Channel im Hyperledger-Netzwerk und gleichzeitig unterschiedliche Vorsysteme nutzen können. Es ist vorgesehen, dass auch andere Plattformen entweder direkt mit der ACTIWARE.IO Plattform interagieren und dies auf der Blockchain per Fingerprint dokumentieren oder, dass die Plattformen über Smart Contracts miteinander interagieren (siehe Abbildung D.6.2). StableNet kann dabei in beiden Anwendungsfällen (P1+P2) sicherstellen, dass das Netzwerk funktioniert und Aktivitäten im Netzwerk offenlegen. Gemeinsam mit der oben beschriebenen Möglichkeit zu automatisierten Backups stellt dies eine wichtige Absicherung dar.

4 Teilkomponenten der Architektur und Integration einer beispielhaften ERP Ethereum Middleware

Dieses Unterkapitel beschreibt die Planung und den grundsätzlichen Aufbau einer beispielhaften Middleware, die zur Integration zwischen einem Cloud ERP System und einem Ethereum Blockchain Netzwerk verwendet wurde. Hierfür wird zuerst eine kurze Darstellung von genutzten Komponenten aufgezeigt, um nachfolgend die Gesamtarchitektur und das Zusammenwirken der einzelnen Systeme zu beleuchten. Die Middleware ist mithilfe der Teilkomponenten Docker, Nginx, Gunicorn, Django und PostgreSQL aufgebaut, welche zusammen die Gesamtfunktionalität der Middleware bereitstellen. Abbildung D.6.3 visualisiert die technische Architektur der Middleware inklusive aller zuvor beschriebenen Komponenten und aller zusätzlich relevanten Systeme. Zu erkennen ist, dass die Middleware auf demselben Ubuntu-Server ausgeführt wird, auf welchem auch die physische Instanz eines ERP-Systems läuft.

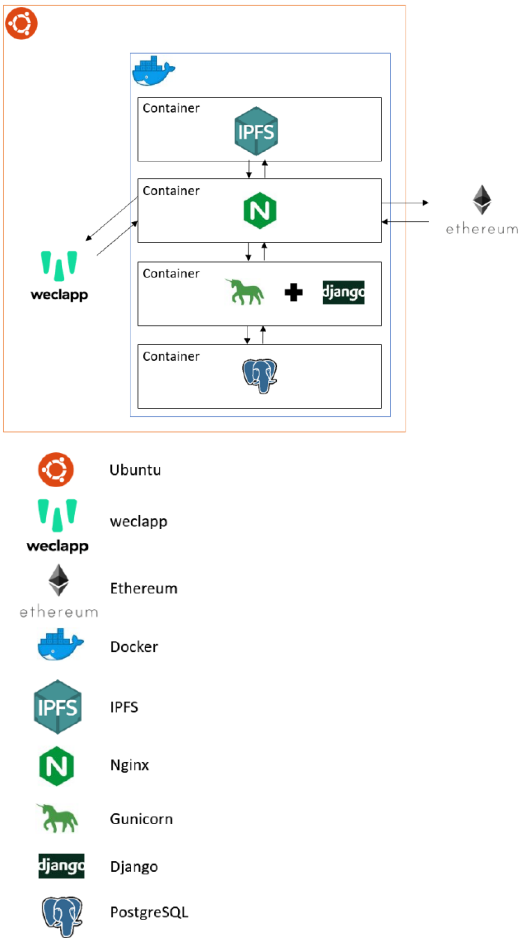


Abbildung D.6.3: Technische Architektur der Middleware

In der Integration der Middleware wird der erste Container mithilfe des **Docker Image go-ipfs**[1] gespawnt. Daraus folgend wird innerhalb der Middleware eine eigene Node des IPFS gehostet, um mit diesem interagieren zu können. Darunter fällt einerseits das Gateway, mit welchem Daten vom Netzwerk gelesen werden können und andererseits die API, die es ermöglicht, Dateien hochzuladen. Des Weiteren wird im zweiten Container der HTTP-Server Nginx ausgeführt. Hierfür wurde das Docker Image nginx[2] in der Version 1.21.1 genutzt. Da die Webserver-Software das WSGI nicht selbst implementiert, wird **Nginx** als Reverse-Proxy-Server für den WSGI-Server **Gunicorn** konfiguriert. Dies bedeutet, dass **Nginx** die Kommunikation der Middleware zu den anderen relevanten Systemen, wie beispielsweise dem ERP-System oder der Blockchain Netzwerk, übernimmt. Der Webserver nimmt somit HTTP-Anfragen von außen an und leitet diese entweder an **Gunicorn** weiter oder stellt statische Dateien direkt selbst bereit, ohne dass hierfür eine Weiterleitung an **Gunicorn** beziehungsweise Django notwendig ist. Der dritte Container beinhaltet den WSGI-Server **Gunicorn** und das **Django**-Projekt inklusive der Anwendungslogik, auf welche der Server-Prozess des WSGI-Servers zugreift. **Gunicorn** erhält die von **Nginx** weitergeleiteten HTTP-Anfragen und übersetzt diese in die entsprechenden Python-Aufrufe, sodass **Django** diese verarbeiten kann. Für diesen Container wird das Docker Image python:3[3] verwendet, da sowohl der WSGI-Server **Gunicorn** als auch das Webframework **Django** in der Programmiersprache Python implementiert sind. Im letzten Container wird das Datenbankmanagementsystem **PostgreSQL** ausgeführt. Für diesen wird das **Docker** Image **postgres**[4] in der Version 13.4 genutzt. **PostgreSQL** wird als Datenbank zur persistenten Speicherung notwendiger Daten für die Middleware verwendet, auf welche das **Django**-Projekt zugreift. Die Integration der Teilkomponenten ergab zahlreiche Herausforderungen in der Integration und Standardisierung eines einfachen Anwendungsfalls, sodass gewonnene Erkenntnisse in Bezug auf Integrationsprobleme in zukünftigen Forschungsarbeiten adressiert werden.

[1] https://hub.docker.com/r/ipfs/go-ipfs/

[2] https://hub.docker.com/_/nginx

[3] https://hub.docker.com/_/python

[4] https://hub.docker.com/_/postgres

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Juniorprofessur für Information Management
Prof. Dr. Christian Janiesch
Stephanstraße 1
97070 Würzburg
https://www.wiwi.uni-wuerzburg.de/lehrstuhl/bwljp1/startseite/

Autoren und Ansprechpartner

Lukas-Valentin Herm, M.Sc.

Wissenschaftlicher Mitarbeiter
lukas-valentin.herm@uni-wuerzburg.de
+49 931 31-81730

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 0931 31-89640

Dr. Michael Kröhn

Head of Research
ROBUR Automation GmbH
michael.kroehn@robur-automation.com

Prof. Dr. Christian Janiesch

Juniorprofessur für Information Management
christian.janiesch@uni-wuerzburg.de
+49 931 31-84930

Michael Baumgart, M.Sc.

Senior Consultant Research & Development
Infosim GmbH & Co. KG
baumgart@infosim.net
+49 931 205 92 200

Dr. Patrick Bredebach

Productmanager
Actiware Development GmbH
patrick.bredebach@actiware-development.com
+49 231 5347 2540

Ole Jankowski, B.Sc.

Solution Architect
Actiware Development GmbH
ole.jankowski@actiware-development.com

D7: Umsetzung von Datenschutz und Datensicherheit

Die in PIMKoWe entwickelte Plattform stellt einen innovativen und disruptiven Lösungsansatz dar. Es wird im Folgenden der Datenschutz und die Datensicherheit von digitalen dezentralen Plattformen betrachtet. Daher werden die erhobenen Anforderungen an die Plattform hinsichtlich Datensicherheit und Datenschutz, aber auch der Integration von Zertifikaten an Anwendungsfällen implementiert. Die Umsetzungen des Projektkonsortiums zeigen, dass bei einer Diskussion der Ergebnisse die Ausgangssituation und Ziele der einzelnen Partner berücksichtigt werden müssen.

1 Bisherige Anforderungen

In den vorangegangenen Dokumenten und im Rahmen der Anforderungsanalyse in Arbeitspaket B wurden unterschiedliche Anforderungen an Datenschutz, Datensicherheit und Zertifikate festgehalten, die als initiale Projektanforderungen notiert wurden:

Datenschutz

- Keine Speicherung von personenbezogenen Daten in einer Blockchain
- Falls personenbezogene Daten verarbeitet werden müssen, soll eine private permissioned Blockchain mit Pseudonymisierung verwendet werden
- Mehrstufiges Rechtesystem

Datensicherheit

- Datensparsamkeit auch für nicht personenbezogene Daten.
- Unveränderbarkeit von externen Daten sicherstellen
- Externe Daten auf dezentralen Cloud-Lösungen ablegen
- Externe Anbieter müssen die DSGVO umsetzen
- Anwendungssicherheit der Applikation
- Fehlerbehandlungen bei möglichen Störungen der Plattform
- Server-Sicherheit zur Sicherung der technischen Infrastruktur

Zertifikate

- Einbindung externer Zertifizierungsstellen
- Zertifizierung von Produkten und Dienstleistungen der Plattform

Um eine bestmögliche Erfüllung dieser Anforderungen zu erreichen, wird die Umsetzung der oben dargestellten Punkte im folgenden Kapitel thematisiert.

Umsetzung der Anforderungen:

Die Umsetzung diverser Sicherheitsanforderungen wurde mithilfe der Plattformen **P1** Qualitätsmanagement (QM) Plattform und **P2** (Produktionsabsicherungsplattform) in vier verschiedenen Use Cases bearbeitet. Diese sind in Tabelle 1 zusammengefasst. Zum jeweiligen Plattformtyp sind verschiedene Use-Cases (Projekt-Outputs) aufgebaut und Sicherheitskonzepte implementiert worden. Das Konsortium verfolgte hierbei unterschiedliche Ziele und Perspektiven, da die Praxispartner und Forschungseinrichtung unterschiedliche Ausgangssituationen in der Integration von Prozessen und Daten aufwiesen. Die Praxispartner konnten bereits bei der Umsetzung auf eine Vielzahl von implementierten Sicherheitsmechanismen zurückgreifen, die als Grundlage zum Auf- und Ausbau der Use-Cases dienten. Weiterhin sind verschiedene Aspekte des Datenschutzes und der Datensicherheit mit dem Aufbau der Use-Cases betrachtet worden, um initial formulierte Anforderungen bestmöglich zu erfüllen. Aufgrund der Neuartigkeit von Blockchain-Systemen und der Herausforderung in der Integration von klassischen Enterprise-Systemen ergaben sich während der Ausarbeitungen erwartungsgemäß verschiedene Änderungen in Anforderungen und Umsetzungen, sodass die Limitationen am Schluss dieses Ergebnisberichts diskutiert werden.

	Use Case 1	Use Case 2	Use Case 3	Use Case 4
Plattformen	P2	P1	P2	P1
Projektoutputs	O10 + O11		O3 + O4	O9
Datenschutz				
Keine Speicherung von personenbezogenen Daten in einer Blockchain	✓	✓	✓	✓
Falls personenbezogene Daten verarbeitet werden müssen, soll eine private permissioned Blockchain mit Pseudonymisierung verwendet werden	✓	Nicht zutreffend für den Use Case	Nicht zutreffend für den Use Case	✗
Mehrstufiges Rechtesystem	✓	✓	✓	✗
Datensicherheit				
Datensparsamkeit auch für nicht personenbezogene Daten.	✓	✓	✓	✓
Unveränderbarkeit von externen Daten sicherstellen	✓	✓	✓	✓
Externe Daten auf dezentralen Cloud-Lösungen ablegen	✗	✗	✗	✓
Externe Anbieter müssen die DS-GVO umsetzen	N/A	✓	✓	N/A
Anwendungssicherheit	✓	✓	✓	N/A
Fehlerbehandlung	✓	✓	✓	N/A
Server-Sicherheit	✓	✓	✓	N/A
Zertifikate				
Einbindung externer Zertifizierungsstellen	N/A	N/A	N/A	N/A
Zertifizierung von Produkten und Dienstleistungen der Plattform	N/A	N/A	N/A	N/A

Tabelle D.7.1: Use-Case Übersicht 1

2 Use Case 1

Anwendungsfall:
Im Anwendungsfall werden Prozessdaten einer Anlage erfasst und verarbeitet. Durch die Verarbeitung entstehen aggregierte Werte, bspw. eine Statistik über den Verlauf eines Parameters oder eine Kennzahl wie die Overall Equipment Efficiency (OEE). Die Aggregation kann dabei entweder auf einem anlagennahen Edge-Device stattfinden oder auf dem Datenserver im Intranet oder in der Cloud. Daraus entstehen Reports, die manipulationssicher gespeichert werden. Entweder werden hierzu die Kennzahlen fortlaufend in einer Blockchain abgelegt, oder der Hash-Code des Report-Dokuments, womit sich die Authentizität des Dokuments überprüfen lässt.

Datenschutz:
Allgemein steht Datenschutz für einen Sammelbegriff über die in verschiedenen Gesetzen angeordneten Rechtsnormen, die erreichen sollen, dass die Privatsphäre des Individuums in einer zunehmend automatisierten und computerisierten Welt („Der gläserne Mensch“) vor unberechtigten Zugriffen von außen (Staat, andere Private) geschützt wird. Die Angriffsflächen, denen sich der moderne Mensch zunehmend ausgesetzt sieht (oft aber auch durch eigene Sorglosigkeit im Umgang mit seinen Daten), sind vielfältig: Neben dem Umgang mit dem Computer und Internet (Stichworte hier z.B.: Viren, Trojaner, Hacking, Phishing) sind auch ganz alltägliche Situationen betroffen, wie bspw. die Diskussion um die Nutzung von Aufzeichnungen der Autobahnmautkontrollbrücken für die Rasterfahndung zeigt. (Gabler Wirtschaftslexikon)

Zentraler Grundsatz und somit auch Grundlage des Datenschutzrechts ist das sog. Verbot mit Erlaubnisvorbehalt. Dies besagt, dass jegliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten verboten ist, es sei denn, dies wird durch das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift erlaubt oder der Betroffene hat seine Einwilligung erklärt (vgl. § 4 Absatz 1 BDSG).
Grundsätzlich kommt das Bundesdatenschutzgesetz jedoch nur dann zur Anwendung, wenn personenbezogene Daten erhoben werden. Ausreichend hierfür ist, dass Videoaufnahmen geeignet sind, einer bestimmten oder bestimmbaren natürlichen Person zugeordnet zu werden. So kann beispielsweise bei Aufnahmen, die Personen lediglich von den Füßen bis zu den Knien oder Hände und Unterarme zeigen, der Personenbezug unter Umständen ausscheiden, mit der Folge, dass das Bundesdatenschutzgesetz einem Einsatz nicht entgegenstünde. Dies ist jedoch im Einzelfall zu beurteilen. Je kleiner der erfasste Personenkreis, desto größer ist die Wahrscheinlichkeit, dass man auch solche Aufnahmen einer Person zuordnen kann.
Im Anwendungsfall werden keine personenbezogenen Daten erfasst. Prozessdaten stehen lediglich in Verbindung mit der „meldenden“ Maschine (bzw. der Station oder Anlage). Es lassen sich lediglich Rückschlüsse auf Zeiträume ziehen, bspw. Frühschicht, Tagschicht, Nachtschicht. Die damit verbundenen personenbezogenen Daten sind allerdings in anderen Systemen hinterlegt und nicht Gegenstand dieses Systems.

Datensicherheit:
Globalisierung, zunehmende Vernetzung und Digitalisierung beherrschen bereits seit Jahren branchenübergreifend die Fertigungsindus-trie. Mit neuen Technologien und Entwicklungen kommen aber auch neue Herausforderungen, Ansprüche, einzuhaltende Gesetze, Normen und Verordnungen. Hier spielt u.a. die Datensicherheit eine große Rolle, bspw. bei der Verarbeitung von Prozessdaten und Bereitstellung von Analysen über Cloud Services. Am konkreten Anwendungsfall werden verschiedene Problematiken erläutert und deren Relevanz bezüglich der Datensicherheit bewertet.
Webservices werden i.d.R. in einer geeigneten Sprache entwickelt, die über eine Bibliothek oder ein Framework Webserver-Funktionalitäten bereitstellen kann. Hier kommen häufig Python oder Javascript zum Einsatz. Nachfolgend sind die Überlegungen dargestellt, die bei der Umsetzung für den Anwendungsfall zum Tragen kommen.
Bei der Entwicklung von Webservices in Python (Flask) oder Javascript (node.js) spielen folgende Punkte eine wichtige Rolle:

- Sicherheit der entwickelten Anwendung
- Fehlerbehandlung
- Server-Sicherheit
- Plattform-Sicherheit

Sicherheit der entwickelten Anwendung:
Begrenzung der Größe einer Anfrage. Validierung des Inhalts einer Anfrage (vgl. mit der Problematik Dependency Injection bei SQL Queries). Detailliertes Logging der Aktivitäten der Anwendung. Für die verschiedenen Sprachen gibt es Bibliotheken, um mit Brute-Force-Angriffen umzugehen, bspw. wenn es um Login geht. Diese können in die Anwendung integriert werden.
Beschränken der Applikation auf die wesentlichen Funktionen. Beschränken der Anfrage auf die notwendigen Parameter. Nur die erforderlichen Informationen zurückgeben.

Fehlerbehandlung:
Für eine adäquate Fehlerbehandlung ist es notwendig, einen korrekten Umgang mit Fehlern zu implementieren, da bei Ausnahmen, die nicht abgefangen werden, u.U. der komplette Fehlerbericht an den Client zurückgegeben wird. Angreifer können daraus wichtige Hinweise für ihre nächsten Attacken ableiten.

Server-Sicherheit:
Hier steht die Firewall im Mittelpunkt. Nicht verwendete Ports müssen deaktiviert werden. Eine Access Control List (ACL) stellt sicher, dass nur definierte Systeme eine Kommunikation aufbauen können. Server-Funktionalitäten wie das Verwenden von Session-Cookies sind sicher zu konfigurieren, ebenso wie die Verwendung von passenden HTTP Security-Headers.

Plattform-Sicherheit:
Die Kommunikation von Client zu Server erfolgt über das HTTPS-Protokoll. Die SSL-Zertifizierung des Servers stellt einen wichtigen Baustein zum Aufbau einer sicheren Kommunikation dar. Darüber hinaus sind durch Patch-Management die aktuellsten Security-Updates einzuspielen.

3 Use Case 2

Anwendungsfall
Im Anwendungsfall werden durch ein Formular Daten zur individuellen Herstellung eines Werkzeugs zur Prüfung eines Stoffes erfasst, im konkreten Beispiel zur Herstellung eines Prüfhammers. Ziel ist es somit, die Bedingungen der Produktion in der Losgröße 1 abzubilden und die Rahmenbedingungen sowie die konkreten Kalibrierungen des Prüfwerkzeugs entsprechend zu erfassen. Die Blockchain dient dabei zur Sicherung wesentlicher Informationen und zur Kommunikation zwischen unterschiedlichen Partnern in der Lieferkette. Damit wird es ermöglicht, von der Anforderungserstellung über die Umsetzung der Anforderungen an das Prüfwerkzeug bis hin zur Auslieferung und Anwendung des Werkzeugs einen lückenlosen Nachweis zu führen. Daraus entstehende Reports können manipulationssicher gespeichert werden, indem per Hashing Prüfsummen auf die Blockchain geschrieben werden.

Datenschutz
Wie bereits erläutert, steht Datenschutz für einen Sammelbegriff unterschiedlicher Normen zum Schutz des Individuums. Neben der gesetzlichen Grundlage zur Erhebung von Daten tritt dabei der Erlaubnisvorbehalt in Kraft. Grundsätzlich sind vom Datenschutz alle personenbezogenen Daten betroffen. Darüber hinaus gilt im Datenschutz der Grundsatz der Datensparsamkeit. Im Rahmen des Projekts wurde dabei mit dem bereits beschriebenen Objektmodell auf Middleware-Ebene versucht, die Daten ex post zu konstruieren. Dabei ist ein differenziertes Rollen und Berechtigungssystem erst beim benötigten Zugriff auf die Daten ein Matching derselben herzustellen. Auf diesem Weg wird es einerseits möglich, der Datensparsamkeit zu genügen, indem bereits vorhandene Daten nicht redundant gespeichert werden und andererseits fallbezogen und somit beim Vorliegen eines berechtigten Interesses überhaupt erst die Daten zusammen zu führen. Damit kann rechtlichen Anforderungen an die Beschränkung von physischen Zugriffen auf Daten Rechnung getragen werden. Hierbei wurden nativ aus der Plattform heraus verschiedene Sicherheitsmechanismen implementiert, über die auch der Zugriff auf gematchte Daten reguliert wurde. Als Beispiel sei der passwortgeschützte Zugriff auf Formulare genannt, der es ermöglicht, die Produktion des Prüfhammers nachzuvollziehen. Die Produktionsdaten können dabei Rückschlüsse auf Personen zulassen. Hier ist die Modellierung unterschiedlicher Sicherheitsstufen möglich. Als Beispiel wurden Prozesse modelliert, in denen beispielsweise die Beteiligung unterschiedlicher Mitarbeiter an dem Produktionsprozess durch Klardaten, durch Pseudonymisierung und durch einfachen Verweis auf den Status eines Produkts (z.B. qualitätsgeprüft) dargestellt werden können.
Zusätzlich kann durch ein differenziertes Rollensystem für jeden Nutzer einzeln bestimmt werden, welche Daten zur Verarbeitung zur Verfügung stehen. Hierbei verbleiben die Daten – sofern möglich - in den ursprünglichen Datenspeichern (bspw. im ERP System) und es werden nur Verweise auf die Originaldaten gespeichert.
Hierdurch ist der Use Case sehr datensparend implementiert, da somit Redundanzen vermieden werden.

Datensicherheit
Neben den bereits unter Use Case 1 benannten Sicherheitsmechanismen wurden im Use Case 2 folgende Sicherheitsmaßnahmen umgesetzt:
1. durch die Plattform per se (s. oben)
2. durch das Projekt. Neben den informationstechnischen Sicherheitsmechanismen ist in den konkreten Projekten auf organisatorische Maßnahmen zu achten.

Plattform-Sicherheit
Durch den in die Plattform integrierten Authentifizierungsservice ist das Verbinden von Benutzerverzeichnissen wie Active Directory o.ä. möglich. Für

die Bestätigung der Nutzer unterstützt die Plattform an dieser Stelle Authentifizierungstoken.
Für jegliche Zugriffe auf Daten wird vom Nutzer verlangt, dass sich dieser mit Bezug zur Plattform ausweist.

4 Use Case 3

Anwendungsfall

Im Anwendungsfall werden die Daten verschiedener Quellen erfasst, verarbeitet und dargestellt. Diese Daten sind einerseits IoT- Messdaten einer Fabrikanlage, simuliert durch ein Industrie 4.0-Fabrikmodell, und andererseits Schlüsselkennzahlen (KPIs) einer Blockchain. Die Überwachung beider Datenquellen wird durch eine dafür entwickelte Erweiterung zu einer bestehenden Monitoring-Plattform durchgeführt. In beiden Fällen findet die Überwachung und Vorverarbeitung der Daten in der neu entwickelten Komponente statt, während die Visualisierung durch die Plattform durchgeführt wird.
Im Mapping-Diagramm aus Abschlussbericht D entsprechen diese beiden Komponenten den Outputs **O4** bzw. **O3**.

Datenschutz

Wie im ersten Anwendungsfall werden hier keine personenbezogenen Daten verarbeitet. Bei der Verarbeitung der IoT-Messdaten gibt es keine Rückschlüsse auf natürliche Personen, außer solche, die nicht Gegenstand des Systems sind.
Die Schlüsselkennzahlen der Blockchain beinhalten zwar Informationen wie z.B. Transaktionsdaten zwischen einzelnen Teilnehmern des Blockchain Netzwerks, jedoch können diese im Regelfall auch nicht auf natürliche Personen zurückgeführt werden.

Datensicherheit

Die Plattform verwendet mehrere Konzepte, um gemessene Daten gegen den unberechtigten Zugriff Dritter zu schützen. Folgende Konzepte stehen zur Verfügung: Nutzerauthentifizierung, Integration von Identitätsmanagementsystemen, Mandantenfähigkeit mit Rechtesystem und verteilte Architektur.
Grundlage der Plattformsicherheit bildet die Nutzerauthentifizierung. Um die Plattform nutzen zu können, benötigen Nutzer einen Account, der entweder manuell von einem Administrator erstellt werden muss oder per Anbindung an ein Identitätsmanagementsystem automatisch generiert werden kann.
Durch Anbindung eines Identitätsmanagementsystems mit speziellen Konfigurationen kann die Sicherheit der Authentifizierung weiter gesteigert werden. Diese beinhalten beispielsweise zwingend erforderlichen Passwortänderungen nach bestimmter Zeit oder zusätzliche Vorgaben für Passwortinhalt und Länge, die über die Vorgaben der Plattform hinausgehen.
Zusätzlich zur notwendigen Authentifizierung kann der Datenzugriff von Nutzern durch die Mandantenfähigkeit der Software bzw. das zugehörige Rechtesystem konfiguriert werden. Durch dieses System können Nutzern oder Nutzergruppen Rechte zugewiesen werden, bestimmte Programmkomponenten einsehen oder bearbeiten zu können. Um etwa ein bestimmtes Dashboard zu sehen, muss es speziell für einen bestimmten Nutzer bzw. eine Nutzergruppe freigegeben werden. Beispielsweise könnte man so den Zugriff auf ein Dashboard mit maschinenspezifischen Informationen auf die der Maschine zugeordneten Techniker einschränken. Soll das Dashboard zudem editiert werden, ist eine zusätzliche Berechtigung erforderlich, die z.B. IT-Administratoren und Fertigungsleitern zugewiesen werden kann.
Als letzte sicherheitsrelevante Eigenschaft der Plattform ist deren verteilte Architektur zu nennen. Sie besteht aus einem zentralen Server, der mit verschiedenen verteilten Agenten kommuniziert, die zum Sammeln von Daten dienen. Der Server kann innerhalb eines sicheren Netzwerks platziert werden und kann durch die Kommunikation mit den Agenten über bestimmte Ports dennoch Daten von beliebigen anderen ggf. unsicheren Netzwerken sammeln.

5 Use Case 4

Anwendungsfall

Im Anwendungsfall werden komplexe Produktstrukturen und beiliegende Qualitätsdokumente durch den Einsatz von hybriden Tokens (UTXO oder ERC1155) betrachtet. Hierbei werden auf Basis von klassischen Enterprise Systemen und Experteninterviews die Möglichkeiten zur Adaption der Blockchain Technologie für die Rückverfolgung von sicherheitsrelevanten Bauteilen über Unternehmensgrenzen diskutiert und prototypisch implementiert. Gemäß der unterschiedlichen Ausgestaltung von Blockchain Systemen können darüber hinaus weitere Ziele wie die Steigerung der Datenqualität oder die Markierung von Produkten mithilfe technischer Identifikatoren (TokenID oder Transaktions-ID) erreicht werden. Im Fokus des Anwendungsfalls steht die Steigerung der Qualität, sowohl auf technischer, organisatorischer Ebene und objektbezogener Produktebene.

Datenschutz:
In erster Linie beschäftigt sich der Datenschutz im Anwendungsfall um die Vermeidung personenbezogener Daten. Nichtsdestotrotz konnte durch Experteninterviews die Möglichkeit zur Integration von nicht personenbezogenen Kontaktmöglichkeiten im Rahmen von Qualitätssicherungsmaßnahmen analysiert werden. Hierzu gehört ein auf Organisationsebene veröffentlichter, nicht personalisierter Qualitätskontakt (Beispiel: Generische Emailadresse), der bereits bei mehreren Industrieunternehmen im Liefernetzwerk für Qualitätssicherungsmaßnahmen (8D-Report) bereitgestellt wird. Personenbezogene Daten führen grundsätzlich zu Diskussionen von GDPR-Aspekten. Daher beschränkt sich der Anwendungsfall auf die Kontaktangaben und Empfehlungen zur Datenminimierung (Europäischer Parlamentarischer Forschungsdienst 2019), die bereits transparent von Produktionsumgebungen im Liefernetzwerk und auf einer nicht personalisierten Organisationsebene verwaltet sind. Eine Pseudonymisierung der Daten entfällt damit für den gewählten Anwendungsfall.

Datensicherheit:
Je nach Komplexität von genutzten Objekten und Daten ergeben sich verschiedene Möglichkeiten, die Datensicherheit auf Objekteebene zu gestalten. Hierzu sind exemplarisch drei verschiedene Möglichkeiten A1-A3 beleuchtet worden.
A1 - Vertragsgegenstand. Wenn strukturierte Daten direkt auf der Blockchain gespeichert werden können, werden die einzelnen Qualitätsobjekte in einem Smart Contract kodiert. Sie werden auf Variablen im Smart Contract abgebildet, wobei Beziehungen ähnlich wie in einer herkömmlichen Datenbank über die IDs der Objekte hergestellt werden können. (Beispiel: Objekte als Tokens auf Blockchains darstellen).
A2 - On-Chain-Hash und Off-Chain-Daten. Wenn die Datenmenge größer als die maximale Transaktionsgröße ist oder es zu kostspielig ist, die Daten auf der Kette zu speichern, wird nur ein Hash der Daten auf der Blockchain gespeichert. Die eigentlichen Daten oder Dokumente werden Off-Chain (d.h. auf einem Cloud-Server) gespeichert und sind nur für autorisierte Teilnehmer über eine Zugangskontrolle zugänglich. (Beispiel: Qualitätsdokument zum Fertigprodukt)
A3 - Zero-Knowledge-Beweis. Für Fälle, in denen einem Prüfer bestimmte Fakten nachgewiesen werden müssen, ist ein Ansatz, der auf Zero-Knowledge Proofs (ZKPs) basiert, besser geeignet. Der Verifizierer sendet nur den erforderlichen Sachverhalt und einen zugehörigen kryptographischen Beweis. Der Beweis ermöglicht es dem Verifizierer, die Authentizität der Behauptung zu bestätigen. Ähnlich wie bei A2 gewährleistet dieser Ansatz die Vertraulichkeit, indem er die tatsächlichen Daten verbirgt und nur die erforderlichen Fakten bereitstellt. Als ein einfaches Beispiel: ZKPs sind ideal, um zu beweisen, dass eine Zahl innerhalb eines bestimmten Bereichs liegt. (Beispiel: Die genutzte Materialmenge innerhalb eines Produktionsauftrages, um die Anzahl bzw. Range einer Chargenmenge für ein bestimmtes Los zu bestimmen, ohne es konkret offenlegen zu müssen).

Limitationen bei der Umsetzung von Zertifikaten

Zu Beginn des Projektes sind Anforderungen in Bezug auf die Nutzung von Blockchain Plattformen und externen Zertifizierungsstellen aufgestellt worden. Hierzu gehört die Einbindung externer Zertifizierungsstellen sowie die Zertifizierung von Produkten und Dienstleistungen der Plattformen. Diese Anforderungen ergaben sich im Rahmen der Umsetzung als besondere Herausforderung, da es weiterhin an technischen und organisatorischen Standards zur Umsetzung von Anwendungsfällen über Unternehmensgrenzen hinaus mangelt (Treiblmaier 2020; Sunyaev et al. 2021). Aktuelle ISO Initiativen[1] für Blockchain Systeme (ISO/TC 307) befinden sich zum Zeitpunkt des Projektes noch in Ausarbeitung (Stage 30.20). Im Rahmen des Projektes konnte darüber hinaus keine Forschung bzw. Kollaborationsframeworks ermittelt werden, die sich detailliert mit den Punkten externer Zertifizierer beschäftigen. Vielmehr geht die aktuelle Blockchain Forschung von einer Desintermediation von zentralen Parteien aus, sodass die Zertifizierung über zentrale Autoritäten kritisch für zukünftige Forschungsprojekte hinterfragt werden sollte (Ostern 2020; Beck et al. 2018).

[1]https://www.iso.org/standard/81978.html?browse=tc

Literaturverzeichnis

Beck, Roman, Christoph Müller-Bloch, and John Leslie King. "Governance in the blockchain economy: A framework and research agenda." Journal of the association for information systems 19.10 (2018): 1.

European Parliamentary Research Service 2019. Blockchain and the General Data Protection Regulation. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Accessed: 27-04-2022.

Ostern, Nadine Kathrin. "Blockchain in the IS research discipline: a discussion of terminology and concepts." Electronic markets 30.2 (2020): 195-210.

Sunyaev, Ali, et al. "Token economy." Business & Information Systems Engineering 63.4 (2021): 457-478.

Treiblmaier, Horst. "Toward more rigorous blockchain research: Recommendations for writing blockchain case studies." Blockchain and distributed ledger technology use cases. Springer, Cham, 2020. 1-31.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL-THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die pro-blemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Lehrstuhl für BWL und Wirtschaftsinformatik
Prof. Dr. Axel Winkelmann
Josef-Stangl-Platz 2
97070 Würzburg

Autoren und Ansprechpartner

Norman Pytel, M.Eng.

Wissenschaftlicher Mitarbeiter
Norman.Pytel@uni-wuerzburg.de
+49 931 31- 86348

Lukas-Valentin Herm, M.Sc.

Wissenschaftlicher Mitarbeiter
lukas-valentin.herm@uni-wuerzburg.de
+49 931 31- 80501

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 931 31-89640

Dr. Patrick Bredebach

Productmanager
Actiware Development GmbH
patrick.bredebach@actiware-development.com
+49 231 5347 2540

Michael Baumgart, M.Sc.

Senior Consultant Research & Development
Infosim GmbH & Co. KG
baumgart@infosim.net
+49 931 205 92 200

D8: Geschäftsmodellanalyse und Management

Digitale dezentrale Plattformen ermöglichen neuartige Lösungsansätze, um Akteure zweiseitiger Märkte ohne Intermediär zu verbinden. Die in PIMKoWe entwickelte Plattform stellt einen innovativen und disruptiven Lösungsansatz dar. Aus diesem Grund wird in diesem Arbeitspaket ein geeignetes Geschäftsmodelldesign für das integrierte Management von Kollaborationen in Wertschöpfungsnetzwerken entwickelt. Für die Identifikation und Analyse innovativer Geschäftsmodellideen wird das etablierte Rahmenwerk zur Geschäftsmodellentwicklung von digitalen Plattformen angewandt.

1 Einleitung

Die weltweite Wirtschaft hat hohe Erwartungen an die Potentiale der Blockchain-Technologie, welche zukünftig unser digitales Wirtschaftssystem revolutionieren könnte. Der Schwerpunkt der Blockchain-Technologie liegt darin, Informationssicherheit und Transparenz zu verbessern, indem verschlüsselte Daten in Peer-to-Peer-Netzwerken (P2P) ausgetauscht werden. Dabei sollen Vertrauen und Sicherheit gesteigert werden. Diese Aussicht lässt die Nachfrage nach Blockchain-Anwendungen in diversen Geschäftsbereichen steigen. Insbesondere durch die Fokussierung auf eine gemeinschaftliche, transparente und sichere Nutzung von Informationen (Kouhizadeh, Saberi, und Sarkis 2021) hat die Blockchain-Technologie Auswirkungen auf digitale Geschäftsmodelle. Zusätzlich bietet die dezentralisierte Natur der Blockchain-Technologie eine Grundlage für die Schaffung innovativer Geschäftsmodelle (Iansiti & Lakhani, 2017).

Aus der betriebswirtschaftlichen sowie produktbezogenen Perspektive birgt die Blockchain-Technologie vor allem großes Potential hinsichtlich des Qualitätsmanagements. Eine erhöhte Integration von Informationssystemen in das Qualitätsmanagement induziert eine bessere Verfügbarkeit von Qualitätsdaten in Bezug auf die Eindeutige Identifikation von Produkten. Die Rückverfolgbarkeit und eindeutige Identifikation von Produkten innerhalb von Wertschöpfungsnetzwerken wird als zentraler Treiber der Blockchain-Technologie aus dieser Perspektive wahrgenommen.

Die in PIMKoWe entwickelte Plattform zur Kollaboration in Wertschöpfungsnetzwerken, basierend auf der Blockchain-Technologie, stellt einen neuartigen Lösungsansatz dar. Diverse digitale und disruptive Geschäftsmodelle können auf den zugrundeliegenden Funktionalitäten aufbauen. Ein strategischer und nachhaltiger Aufbau eines Managements der möglichen Geschäftsmodelle und die Entwicklung effektiver Methoden für die Diffusion von Blockchain-basierten Plattformen haben für die Digitalisierung des Industriestandorts Deutschland eine hohe Bedeutung. Daher werden im folgenden Teilarbeitspaket **D8 Geschäftsmodellanalyse und Management** neben der Identifikation und Analyse von digitalen Geschäftsmodellmustern die Erkenntnisse anhand des etablierten Rahmenwerks zur Geschäftsmodellentwicklung nach Al-Debei und Avison (2010) beleuchtet.

2 Problemstellung und Zielsetzung

Mit der Digitalisierung entstanden für Unternehmen und deren Geschäftsaktivitäten neue Herausforderungen. Durch eine kundenspezifischere Produktion entstand eine enorme Variantenvielfalt. Gleichzeitig weiteten sich die Lieferstrukturen auf globale Maßstäbe aus. Diese Entwicklung erfordert eine stärkere Vernetzung unter den Stakeholdern, da sich die Transparenz über die gesamte Wertschöpfungskette verringert.

Zusätzlich haben digitale Plattformen in den letzten Jahren den Innovationsdruck auf Unternehmen mit klassischen Geschäftsmodellen verstärkt. Dabei waren die Architekturen solcher Plattformen stark zentralisiert. Der Betreiber einer Plattform fungiert dabei als Intermediär zwischen den Marktseiten und hat implizit die Hoheit über ausgetauschte Daten (Perscheid, Ostern, und Moormann 2020; Tumasjan und Beutel 2019). Das disruptive Konzept dezentraler Plattformen, welches durch das Aufstreben Blockchain-basierter Plattformen und Applikationen ermöglicht wird, kann diesem Abhängigkeitsverhältnis entgegenwirken. Grundlage bildet die dahinterstehende Distributed Ledger Technologie, welche eine verteilte und konsistente Datenspeicherung ermöglicht (Kouhizadeh u. a. 2021). Die verteilte Datenbasis zeichnet sich dadurch aus, dass für jeden Netzwerkteilnehmer stets eine aktualisierte Kopie sämtlicher Transaktionen verfügbar ist. Die einzelnen Knotenpunkte innerhalb eines Blockchain-Netzwerkes benötigen keine vermittelnde Vertrauensstelle, anders als bei zentralen Netzwerken, um miteinander zu interagieren (Epiphaniou u. a. 2020). Grundsätzliches Ziel einer dezentralen Netzwerkarchitektur ist das Wegfallen von Intermediären (siehe Abbildung D.8.1).

Somit kann die Blockchain-Technologie als Katalysator für dezentrale Plattformlösungen angesehen werden. Oftmals wird die Blockchain-Technologie aufgrund ihrer Bekanntheit und der Nutzung mit dem Finanzsektor in Verbindung gebracht. Jedoch bietet das Grundkonzept weitaus weitreichendere Anwen-dungs- und Einsatzmöglichkeiten, wie beispielsweise im Wertschöpfungskettenmanagement, der Pharmazie oder in der Landwirtschaft. Beispielsweise kann die Blockchain-Technologie zur inter-organisatorischen Integration von Prozessen verwendet werden (Weking u. a. 2020). Dabei zielen Unternehmen darauf ab, ausgewählte bestehende Geschäftsprozesse der unterschiedlichen Unternehmen in der Blockchain abzubilden. Über den Einsatz einer solchen Lösung soll beispielsweise die Interoperabilität der Systeme von Organisationen und damit eine Effizienzsteigerung

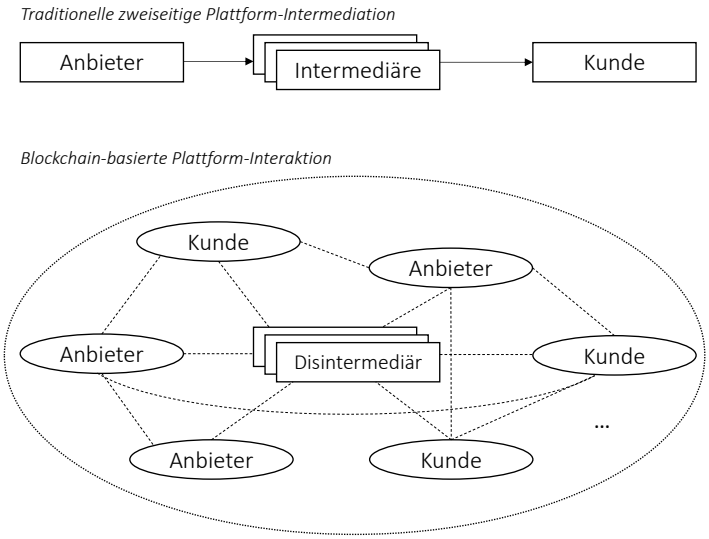


Abbildung D.8.1: Traditionelle vs. Blockchain-basierte Plattforminteraktion (nach Teutenberg und Tönnissen (2019))

sowie Datentransparenz in der Supply Chain der Endnutzer geschaffen werden (Weking et al. 2020).

Im Allgemeinen sind dezentrale digitale Geschäftsmodelle in der Praxis eine innovative Form der Wertschöpfung und werden von Wissenschaftlern zunehmend aus der Perspektive von Geschäftsmodellen analysiert. Zum heutigen Stand der Forschung wurde die Konfiguration digitaler dezentraler Geschäftsmodelle anhand spezifischer Geschäftsmodelle, wie *Blockchain as a Service*, mithilfe anerkannter Geschäftsmodell-Rahmenwerke (z.B. Gassmann, Frankenberger, und Csik 2014; Osterwalder und Pigneur 2013) analysiert. Daher teilt sich die relevante Literatur für die Gestaltung digitaler und dezentraler Geschäftsmodelle in zwei Forschungsströme auf. Auf der einen Seite stehen die taxonomischen Analysen Blockchain-basierter Geschäftsmodellmuster über die verschiedenen Anwendungsbereiche hinweg und spezifische Blockchain-Geschäftsmodelle auf der anderen Seite. Es mangelt an einer Konsolidierung der Informationen, die für die ganzheitliche Betrachtung der Gestaltungsmöglichkeiten dezentraler Blockchain-basierter Plattformgeschäftsmodelle notwendig sind, insbesondere welche, die auf die Besonderheiten des integrierten Managements von Kollaborationen in Wertschöpfungsnetzwerken eingehen.

Deshalb zielt das vorliegende Teilarbeitspaket auf die Entwicklung eines holistischen und tiefergreifenden Referenzgeschäftsmodells für digitale und Blockchain-basierte Plattformgeschäftsmodelle mit besonderem Schwerpunkt auf Kollaboration in Wertschöpfungsnetzwerken ab.

3 Geschäftsmodell für Blockchain-basierte Kollaborationsplattformen in Wertschöpfungsnetzwerken

Die Entwicklung eines Geschäftsmodells ist für die Vision und Strategie einer Organisation unentbehrlich, da es diese für die gesamte Organisation kommuniziert und strategisch ausgerichtete Entscheidungen unterstützt (Al-Debei und Avison 2010). Ein Rahmenwerk für die Entwicklung eines Blockchain-basierten Geschäftsmodells liefern Wang, Chen, und Zghari-Sales (2021) und Chong u. a. (2019), welche sich auf die Herangehensweise von Al-Debei und Avison (2010) stützen. Al-Debei und Avison (2010) identifizieren als Hauptelemente eines Geschäftsmodells das Wertangebot, die Wertarchitektur, das Wertnetzwerk und die Wertfinanzierung, während andere, wie Schön (2012) und Teece (2018), einen ähnlichen Ansatz unter anderen Begriffen vorschlagen, der aus Wertangebot, Ertragsmo-dell und Kostenmodell besteht. Wie zuvor beschrieben, existiert bisher kein Geschäftsmodell als Gestaltungsrahmen mit einem besonderen Fokus auf Blockchain-basierte Kollaborationsplattformen in Wertschöpfungsnetzwerken. Folglich berücksichtigen bestehende Rahmenwerke wie das von Al-Debei und Avison (2010) keine Blockchain-spezifischen Aspekte, die für die Nutzung und Entwicklung von Blockchain-basierten Kollaborationsplattformen essenziell sein könnten.

Für den Aufbau des Geschäftsmodells einer Blockchain-basierten Kollaborationsplattform für Wertschöpfungsnetzwerksszenarien ist es notwendig, die bestehenden Rahmenwerke um die Blockchain-Komponente und deren Einfluss zu erweitern. Das Konzept des Geschäftsmodells geht aufgrund der dezentralen Komponente der Block-

chain über den üblichen Rahmen einer Organisation hinaus und fokussiert sich auf die dezentralen Akteure, die eine Blockchain-basierte Kollaborationsplattform zur gemeinsamen Wertschöpfung nutzen. In Anlehnung an Wang, Chen und Zghari-Sales (2021) entwickeln wir einen Gestaltungsrahmen für Geschäftsmodell-Schlüsselelemente für digitale und Blockchain-basierte Kollaborationsplattformen in Wertschöpfungsnetzwerken. Im Folgenden wird der Gestaltungsrahmen entlang der vier Geschäftsmodelldimensionen *Wertentwicklung, Wertschöpfung*, *Werte-Netzwerk* und *Wert-einbringung* dargestellt.

3.1 Dimension Wertentwicklung

Die Dimension Wertentwicklung umfasst die Ausgestaltung der Strukturen die notwendig sind, um den kreierten Wert an das Zielsegment zu liefern. Dabei betrifft die Wertentwicklung die technische und organisatorische Plattformgestaltung sowie Blockchain-basierte Plattformdienstleistungen und deren Teilnehmer bzw. Anwender.

Der *wahrgenommene Wert* der Blockchain-Technologie setzt sich hauptsächlich durch die Interaktion mit anderen Netzwerkteilnehmern und den sicheren Informationsfluss innerhalb des Netzwerks zusammen. Die Hauptaktivitäten des Plattform-Providers sind die Implementierung der Konsortial-Blockchain als Notwendigkeit für eine Blockchain-basierte Kollaborationsplattform und die Gewährleistung einer effizient funktionierenden Plattform, die jeweils Wert für die Teilnehmenden schafft. Ein funktionierendes Blockchain-basiertes Plattformsystem setzt voraus, dass zu Beginn das Konsortium dem Plattform-Provider die im Netzwerk gültigen gemeinsamen Regeln und Praktiken zur Gewährleistung einer funktionierenden Plattform mitteilt. Diese Elemente sind Hauptbestandteile der Blockchain-basierten Plattformgestaltung. Allein durch die Ausgestaltung der Konsortial-Blockchain entsteht ein Wert durch die Integration der notwendigen Informationssysteme über die Blockchain-Technologie.

Für wen dieser wahrgenommene Wert entsteht, das bedeutet, was konkret die anvisierten *Kundensegmente* sind, wird hauptsächlich über den Marktumfang und den Grad der Offenheit der Kollaborationsplattform bestimmt. Der Marktumfang des angesprochenen Kundensegments der Kollaborationsplattform fokussiert sich hauptsächlich auf vertikale Märkte. Vertikale Marktplätze werden um eine bestimmte Branche herum gebildet und dienen daher einem auf ein bestimmtes Segment ausgerichteten Angebotsnetz. Ihr Hauptzweck besteht darin, die Beschaffung von Waren oder Dienstleistungen zu unterstützen, die weitgehend spezifisch für diese Branche sind. Insbesondere werden mit der Kollaborationsplattform Teilnehmer aus B2B Märkten angesprochen. Vor allem in B2B-Marktplätzen herrscht häufig ein mangelndes Vertrauen in unbekannte Anbieter, welches als Haupthindernis für die Schaffung von digitalen Plattformen gilt (Loukis, Spinellis und Katsigiannis 2011).

Die *Sicherheitsmerkmale* der Blockchain-Technologie schaffen einerseits mit Authentifizierungsprüfungen und Zugangskontrollen ein mehrstufiges Rechtesystem für die Kollaborationsplattform. Andererseits schaffen sie Vertrauen durch verschlüsselte Transaktionen und eine gewisse Transparenz durch das Konzept der Dezentralität. Das Rechtesystem bietet die Möglichkeit, dass definierte Transaktionen sowie Daten nur für bestimmte Plattformteilnehmer sichtbar sind. So werden simultan zwei wertschöpfende Aktivitäten der Kollaborationsplattform geschaffen. Auf der einen Seite wird Sicherheit geboten, um Vertrauen zwischen den Teilnehmern zu schaffen und auf der anderen Seite wird sichergestellt, dass durch die erhöhte Sicherheit die Prozesse nicht verlangsamt und Ressourcen nicht blockiert werden.

3.2 Dimension Wertschöpfung

Die Wertschöpfungsdimension bezieht sich auf jene Geschäftsmodellmuster, welche für ausgewählte Kundensegmente einen zusätzlichen Wert schaffen. Dabei bietet es die Möglichkeit, mithilfe der Geschäftslogik der Wertschöpfung die Bedürfnisse aller beteiligten Parteien durch das Angebot von Produkten und Dienstleistungen zu befriedigen. Ein kritischer Erfolgsfaktor in Wertschöpfungsnetzwerken ist die Kommunikation der Akteure entlang der Lieferketten. Durch fehlendes Vertrauen innerhalb des Netzwerks entstehen Informationsasymmetrien, welche Effizienzgewinne und Netzwerkeffekte abschwächen. Informationsasymmetrien sind in Wertschöpfungsnetzwerken vor allem in vertikalen Lieferketten zu beobachten, wenn Großunternehmen am Ende der Lieferkette an der Spitze stehen und deren Ausgestaltung dominiert.

Um Wert für alle beteiligten Akteure innerhalb des Netzwerks zu schaffen ist es wichtig zu verstehen, dass der Wert auf Plattformen im Allgemeinen gemeinsam geschaffen wird. Der Nutzen einer Kollaborationsplattform wird erst voll ausgeschöpft, wenn die Teilnehmer das Plattformangebot annehmen, es nutzen und auch darüber zusammenarbeiten.

Die Blockchain-Komponente einer Kollaborationsplattform in Wertschöpfungsszenarien kann an dieser Stelle ansetzen und eine Möglichkeit schaffen, die Bedürfnisse der Zielsegmente zu befriedigen. Dabei wirkt die Blockchain-Technologie nicht

zerstörend auf bestehende digitale Plattformmodelle, sondern sie ist als eine Erweiterung der bestehenden digitalen Plattformarchitektur zu verstehen. Jedoch ist zu beachten, dass die dezentrale Architektur grundlegend verschieden ist und eine bestehende zentrale Plattform aufgrund von Netzwerkexternalitäten schwer zu dezentralisieren ist. In zentralen Architekturen profitieren Intermediäre von ihrer Funktion als Vermittler zwischen beiden Seiten eines zweiseitigen Marktes und gewinnen daraus Wertschöpfung.

Die Blockchain-Technologie hat drei prägnante Merkmale, die für Teilnehmer an Geschäftskollaborationen von Interesse sind. Die Blockchain-Technologie ist aufgrund ihrer dezentralen Architektur vertrauenschaffend und bietet Transparenz für alle Akteure innerhalb des Netzwerks. Ein weiterer zentraler Aspekt ist das Aufbrechen von zentralisierten Strukturen im Sinne einer Dezentralisierung der Entscheidungsfindung.

Zuallererst profitieren Teilnehmende eines Wertschöpfungsnetzwerks an einer dezentralen Kollaborationsform durch die Kosteneinsparungen, die mit dem Wegfall von Intermediären entstehen. Es wird ein organisatorisches Rahmenwerk für dynamische Geschäftskollaborationen ermöglicht. Durch das Konzept der Dezentralität können Transaktionseffizienzen verbessert und insgesamt die Transparenz über das Netzwerk und ihre Transaktionen hergestellt werden. Diese Netzwerktransparenz fördert die Anwendungsmöglichkeiten fortgeschrittener Analysewerkzeuge, die zusätzliche Effizienzgewinne hervorrufen kann. Die gewonnene Transparenz über Transaktionen und deren Rückverfolgung kann Schwankungen in den Märkten abfedern und diesen sogar entgegenwirken. Somit kann die Versorgungssicherheit vor allem in Lieferketten, die auf Just-In-Time Politiken setzen, erhöht werden.

Sicherheitsbedenken, die häufig durch das Transparenzversprechen hervorgerufen werden, können mithilfe des Konzepts der genehmigungspflichtigen Konsortial-Blockchain beschwichtigt werden. Durch ein *mehrstufiges Rechtesystem* innerhalb der Kollaborationsplattform können Informationen vor Unbefugten geschützt und eine vertrauenswürdige Umgebung für geschäftliche Transaktionen geschaffen werden. Dies umfasst insbesondere die Teilnahme am Netzwerk sowie Lese- und Schreibrechte auf der Blockchain-basierten Kollaborationsplattform.

Beteiligte Unternehmen in der Kollaborationsplattform profitieren von einem weiteren prägnanten Merkmal der Blockchain-Technologie. Es können nicht nur Transaktionen sicher und transparent auf der Blockchain gespeichert werden, sondern auch Daten im Zusammenhang mit der *Rückverfolgbarkeit* von Ergebnissen innerhalb von Wertschöpfungsnetzwerken verfügbar gemacht werden. Daten, welche nicht direkt auf der Blockchain gespeichert werden sollen, können Off-Chain auf dezentralen Cloud-Lösungen gespeichert werden und mit kryptografischen Hash-Funktionen auf ihre Unveränderlichkeit überprüft werden. So werden Datenschutzansprüche der Teilnehmenden an die Kollaborationsplattform eingehalten und gleichzeitig ein effizienter Datenaustausch ermöglicht.

Weitere Wertschöpfungspotentiale birgt eine Blockchain-basierte Kollaborationsform durch die *Konsensbildung* der Teilnehmenden hinsichtlich *Industriestandards*, welche so gesetzt und verbreitet werden können. Insbesondere für vertikal integrierte Unternehmen, die einer Zuliefererpyramide unterliegen, ist dies eine Möglichkeit, gemeinsam Macht auf die Großunternehmen an der Lieferkettenspitze auszuüben.

Blockchain-basierte Kollaborationsplattformen haben zudem den Vorteil, dass *Geschäftslogik* durch *Programmcode* abgebildet werden kann. So werden *Automatisierungspotentiale* freigesetzt, welche zuvor menschliche Interaktion benötigten. Die Automatisierung von Geschäftsprozessen birgt ein enormes Potential für *Effizienzsteigerungen*. Zudem können so Lieferkettenstrukturen effizienter gestaltet werden, da teilweise einzelne Stufen in der Wertschöpfungskette wegfallen.

3.3 Dimension Werteinbringung: Gebührenmodell der Kollaborationsplattform

Die Dimension der Werteinbringung beschreibt, wie Gewinn aus dem wahrgenommenen geschaffenen und gelieferten Wert für die Kundensegmente erzielt wird. Das Gebührenmodell legt fest, wie die Kollaborationsplattform aus verschiedenen Einnahmemodellen Geld verdient (Osterwalder und Pigneur 2013). Das Gebührenmodell der Kollaborationsplattform leitet sich von dem Charakter eines Blockchain-Netzwerks für die gemeinsame Schaffung und Nutzung ab. Die Eigenschaften der Kollaborationsplattform implizieren somit eine gemeinsame Kostenteilung. Kosten fallen an verschiedenen Stellen an, die mithilfe der Rollen innerhalb des Netzwerks in unterschiedliche Kostengruppen eingeteilt werden können.

Die Rollen der Kollaborationsplattform umfassen den Anwender, Plattform-Provider, Dienstleistungs-Provider und Zertifizierungs-Provider. *Anwender* sind jegliche Nutzer der Plattform, die Lese- oder Schreibrechte auf der Blockchain-basierten Kollaborationsplattform besitzen. Der *Plattform-Provider* ist initial für die Entwicklung der notwendigen Infrastruktur und damit der Blockchain zuständig. Darüber hinaus übernimmt er die Entwicklung der notwendigen Verwaltungs-

instanzen sowie der User-Interfaces der verschiedenen Anspruchsgruppen. Der *Dienstleistungs-Provider* ist generell für die Verwaltung der vollständig implementierten Plattform zuständig. Zuletzt ist der *Zertifizierungs-Provider* für die Überprüfung der Persistenz von in der Blockchain gespeicherten Informationen zuständig.
Aufbauend auf diesen verschiedenen Rollen können Einnahmequellen identifiziert werden. Die allgemein möglichen Einnahmequellen zur gemeinschaftlichen Kostendeckung setzen sich zusammen aus Transaktionsgebühren, Gebühren nach Anzahl der Nodes (Rechner, die als Knotenpunkte im Netzwerk fungieren und jeweils eine Kopie der Blockchain speichern), Gebühren nach Speichernutzung, Gebühren nach der IP-Anzahl, Gebühren nach CPU-Auslastung (Kernahan, Bernskov, und Beck 2021; Onik und Miraz 2019). Zur gemeinschaftlichen Kostendeckung eignet sich ein Gebührenmodell, welches sich aus einmaligen und kontinuierlichen Kosten für die verschiedenen Anwender der Plattform zusammensetzt.
Bereits vor Markteintritt der Kollaborationsplattform müssen sich ein Konsortium zum Aufbau des Netzwerks sowie ein Plattform-Provider finden. Anreiz eine Konsortial-Blockchain aufzubauen, bieten vor allem Aufbau und Festigung strategischer Partnerschaften durch Schaffung von Transparenz und Vertrauen. Somit wird die Plattform indirekt auf beiden Marktseiten integriert und senkt bereits Eintrittsbarrieren auf die Plattform durch Erreichen eines signifikanten Konsortiums.
Damit keine weiteren Eintrittsbarrieren zur Kollaborationsplattform geschaffen werden und die Offenheit gefördert wird, muss die Preissetzung der fixen und kontinuierlichen Kosten der Leistung entsprechend angemessen sein. Die technischen Voraussetzungen zum Eintritt auf eine Blockchain-basierte Plattform sind zumeist ein wahrgenommenes Hindernis. Aus diesem Grund ist das Angebot der benötigten Infrastruktur und die fixe Preiskomponente dessen ein essenzieller Bestandteil des Gebührenmodells. Hiermit sind der Aufbau und die Nutzung eines Knotens im Netzwerk gemeint.
Zusätzlich muss bei der Preissetzung auch die Interaktion der Anwender innerhalb des Netzwerks berücksichtigt werden. Daher umfasst die kontinuierliche Komponente der Preissetzung die angefallene Speichernutzung. Diese Gebühren beinhalten die anfallenden Kosten für Transaktionen und die Verwaltung sowie die Überprüfung des Netzwerks.

3.4 Dimension Werte-Netzwerk

Die Dimension des Werte-Netzwerks bildet die Art und Weise, wie Unternehmen über die Kollaborationsplattform miteinander verbunden sind, ab. Die gemeinsame Koordination und Zusammenarbeit über die Blockchain-basierte Plattform schafft ein Werte-Netzwerk, in welchem gemeinsam ein Wert erworben wird. Wichtig ist, dass die Benutzerinteraktion auf der Kollaborationsplattform die Schlüsselaktivität darstellt und somit das zentral wertschöpfende Element ist. Diese besondere Dynamik führt zu direkten Netzwerkeffekten.

4 Fazit

Dieses Teilarbeitspaket identifiziert und analysiert die Potentiale von digitalen Geschäftsmodellen für Blockchain-basierte Kollaborationsplattformen und beleuchtet die Erkenntnisse anhand des etablierten Rahmenwerks zur Geschäftsmodellentwicklung nach Al-Debei und Avison (2010).
Im Allgemeinen konnten wir feststellen, dass vor allem in vertikalen (B2B-) Lieferketten häufig ein mangelndes Vertrauen in unbekannte Anbieter herrscht, das als Haupthindernis für die Schaffung von digitalen Plattformen gilt. Digitale Plattform-Geschäftsmodelle sind in der Wissenschaft und Praxis etablierte Geschäftsmodelle. Die Blockchain-Technologie galt lange als disruptive Technologie, welche das Potential beinhaltet, bestehende digitale Plattform-Modelle grundlegend zu verändern. Untersuchungen zeigen jedoch, dass die Blockchain Komponente lediglich als Erweiterung des bestehenden digitalen Geschäftsmodells wirkt. Daraus kann abgeleitet werden, dass für die Blockchain-basierte Kollaborationsplattform für die Koordination von Wertschöpfungsnetzwerken auch typische Plattformeffekte gelten.
Die Integration der Blockchain-Technologie für digitale Kollaborationsplattformen in Wertschöpfungsnetzwerken bietet die Möglichkeit, die Hindernisse traditioneller digitaler Plattformen zu überwinden. Durch die Integration von Informationssystemen in die Blockchain werden eine einfachere Kommunikation und ein einfacherer Informationsaustausch für die digitalen B2B-Kollaborationen geschaffen. Insgesamt wird deutlich, dass dezentrale digitale Kollaborationsplattformen im B2B-Bereich ein besonderes Spannungsfeld adressieren. Es scheint, als eröffnet sich dadurch die große Chance, vorhandene Branchenkompetenzen und Geschäftsnetzwerke für die Entwicklung eines neuen Geschäfts-modells zu nutzen. Gleichzeitig zeigt sich, dass der Aufbau eines Blockchain-basierten Ökosystems nur funktioniert, wenn Barrieren zum Einstieg auf die dezentrale digitale Kollaborationsplattform gesenkt werden. Diese treten vor allem im Bereich der Erfüllung technischer Voraussetzungen der Anwender auf. Eine besondere Herausforderung liegt darin, die Dezentralität der Kollaborationsplattform aufrechtzuerhalten und gleichzeitig die notwendige Infrastruktur anzubieten.

Literatur

Al-Debei, Mutaz M., und David Avison. 2010. „Developing a unified framework of the business model concept“. *European Journal of Information Systems* 19(3):359–76. doi: 10.1057/EJIS.2010.21/FIGURES/6.

Chong, Alain Yee Loong, Eric T. K. Lim, Xiuping Hua, Shuning Zheng, und Chee Wee Tan. 2019. „Business on Chain: A Comparative Case Study of Five Blockchain-Inspired Business Models“. *Journal of the Association for Information Systems* 20(9):9. doi: 10.17705/1jais.00568.

Epiphaniou, Gregory, Prashant Pillai, Mirko Bottarelli, Haider Al-Khateeb, Mohammad Hammoudesh, und Carsten Maple. 2020. „Electronic Regulation of Data Sharing and Processing Using Smart Ledger Technologies for Supply-Chain Security“. *IEEE Transactions on Engineering Management* 67(4):1059–73. doi: 10.1109/TEM.2020.2965991.

Gassmann, Oliver, Karolin Frankenberger, und Michaela Csik. 2014. „Revolutionizing the Business Model“. *Management of the Fuzzy Front End of Innovation* 89–97. doi: 10.1007/978-3-319-01056-4_7.

Kernahan, Alan, Ulrik Bernskov, und Roman Beck. 2021. „Blockchain out of the box - Where is the blockchain in blockchain-as-a-service?“ *Proceedings of the Annual Hawaii International Conference on System Sciences* 2020-January:4281–90. doi: 10.24251/HICSS.2021.520.

Kouhizadeh, Mahtab, Sara Saberi, und Joseph Sarkis. 2021. „Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers“. *International Journal of Production Economics* 231:107831. doi: 10.1016/J.IJPE.2020.107831.

Loukis, Euripidis, Diomidis Spinellis, und Anastasios Katsigiannis. 2011. „Barriers to the Adoption of B2B e-Marketplaces by Large Enterprises: Lessons Learned From the Hellenic Aerospace Industry“. *http://dx.doi.org/10.1080/10580530.2011.562129* 28(2):130–46. doi: 10.1080/10580530.2011.562129.

Onik, Md Mehedi Hassan, und Mahdi H. Miraz. 2019. „Performance Analytical Comparison of Blockchain-as-a-Service (BaaS) Platforms“. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST* 285:3–18. doi: 10.1007/978-3-030-23943-5_1.

Osterwalder, A., und Y. Pigneur. 2013. *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers*. Hoboken: John Wiley & Sons Inc.

Perscheid, Guido, Nadine Ostern, und Jürgen Moormann. 2020. „TOWARDS A TAXONOMY OF DECENTRALIZED PLATFORM-BASED BUSINESS MODELS“. *European Conference on Information Systems*.

Schön, Oliver. 2012. „Business Model Modularity – A Way to Gain Strategic Flexibility?“ *Controlling & Management 2012 56:2* 56(2):73–78. doi: 10.1365/S12176-012-0388-4.

Teece, David J. 2018. „Business models and dynamic capabilities“. *Long Range Planning* 51(1):40–49. doi: 10.1016/J.LRP.2017.06.007.

Tumasjan, Andranik, und Theodor Beutel. 2019. *Blockchain-Based Decentralized Business Models in the Sharing Economy: A Technology Adoption Perspective*. Bd. Business Transforma…. herausgegeben von H. . B. R. Treiblmaier. Springer International Publishing.

Wang, Yingli, Catherine Huirong Chen, und Ahmed Zghari-Sales. 2021. „Designing a blockchain enabled supply chain.“ *International Journal of Production Research* 59(5):1450–75.

Weking, Jörg, Michael Mandalenakis, Andreas Hein, Sebastian Hermes, Markus Böhm, und Helmut Krcmar. 2020. „The impact of blockchain technology on business models – a taxonomy and archetypal patterns“. *Electronic Markets* 30(2):285–305. doi: 10.1007/S12525-019-00386-3/TABLES/11.

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL-THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet werden. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Lehrstuhl für BWL und Wirtschaftsinformatik
Prof. Dr. Axel Winkelmann
Sanderring 2
97070 Würzburg

Autoren und Ansprechpartner

Myriam Schaschek, M.Sc.

Wissenschaftliche Mitarbeiterin
myriam.schaschek@uni-wuerzburg.de
+49 931 31-87662

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 931 31-89640

– Inhaltsverzeichnis Arbeitspaket E –

Das Arbeitspaket (AP) E behandelt auf Basis des Plattformdemonstrators die Evaluation. Hierzu gehören die Funktionalität und Anforderungskonformität. Die KMU-Praxispartner des Projektkonsortiums werden dabei mit Hilfe zweier, für den deutschen Mittelstand typischer, Anwendungsszenarien integriert. Die Evaluation wird auch aus Perspektive der Umsetzungspartner durchgeführt, sodass eine Selbstreflexion der erarbeiteten Ergebnisse stattfindet.

E1 & E2 Praxisbericht und Evaluation. Diese Teilarbeitspakete setzt sich mit der Evaluation und gesammelten Erfahrung der Plattformansätze auseinander. Produktions- und qualitätsbezogene Szenarien komplexer Anwendungsfälle dienen dabei als Grundlage, um die Perspektiven aller Konsortialpartner zu berücksichtigen und eine Übertragbarkeit der Ergebnisse zu beschreiben.

E1 & E2: Praxisbericht und Evaluation

Der folgende Ergebnisbericht behandelt die Evaluation verschiedener Plattformansätze aus Sicht von kleinen und mittleren Anwendungsunternehmen und Softwaredienstleistern. Hierbei sind für die Teilnehmer des Konsortiums sowohl betriebswirtschaftliche als auch technische Aspekte für verschiedene Anwendungsfälle gewählt worden, um eine möglichst holistische und allgemeingültige Betrachtungsweise aller Akteure zu erreichen. Der Ergebnisbericht beinhaltet sowohl ökonomische, technische als auch organisatorische Aspekte der Projektteilnehmer, die im Rahmen mehrerer Evaluationsworkshops für den Aufbau innovativer Blockchain Prototypen iterativ bewertet wurden.

1 Einleitung

Das Aufkommen der Blockchain-Technologie hat in vielen Bereichen wie Supply Chain Management, Produktion und Logistik erhebliche Aufmerksamkeit in Forschung und Praxis erzeugt (Rejeb et al. 2021). Das Versprechen der Dezentralisierung und der Verbesserung der Qualität der Lieferkette durch horizontale Blockchain (BC)-Integration ist nach wie vor ein Bestandteil der wissenschaftlichen Auseinandersetzung. Die technische und betriebswirtschaftliche Adaption und Integration stellen allerdings immer noch technische und organisatorische Herausforderungen für Unternehmen dar. Einerseits sind die traditionellen Informationssysteme wie Enterprise Resource Planning oder Manufacturing Execution Systems eine wertbeitragende Grundlage für horizontale Anwendungsfälle in Wertschöpfungsnetzwerken. Allerdings sind sie mehrheitlich für die vertikale Integration innerhalb der eigenen Unternehmensgrenzen konzipiert (Sunyaev et al. 2021). Darüber hinaus ist die wissenschaftliche Literatur zur unternehmensweiten BC-Integration spärlich, weshalb eine ausgewogene Auseinandersetzung mit dem Thema für Forscher und Praktiker nur bedingt transparent möglich ist (Haddara et al. 2021). In diesem Beitrag stellen die nachfolgenden Ergebnisse eine Zusammenfassung verschiedener Perspektiven der Anwendungspartner und Software-Projektpartner im Projekt PiMKoWe dar. Als Grundlage dieses Ergebnisberichts stehen verschiedene Plattformansätze (P1+P2) für die Qualitäts- und Produktionssicherung zur Verfügung, die als Referenz zur Bewertung verschiedener Kriterien in nachfolgenden Kapiteln dienen.

2 Auswahl der Kriterien zur Kollaboration in Wertschöpfungsnetzwerken

Netzwerkteilnehmer haben mit zahlreichen Anforderungen und dem Teilen von Unternehmensdaten auf mehreren Ebenen verschiedene Herausforderungen auf rechtlicher, organisatorischer und technischer Ebene zu überwinden. Aufgrund der bestehenden Komplexität in Qualitätsprozessen und der hohen Bedeutung des Datenschutzes mangelt es den Lieferketten allerdings weiterhin an Transparenz und Reaktionsfähigkeit (Kuhn et al. 2018; Miehle et al. 2019). Staatliche Institutionen und Behörden auf nationaler und internationaler Ebene verlangen allerdings zunehmend eine Observierung von Lieferketten, um die Rückverfolgbarkeit von Bauteilen und Arbeitsbedingungen einzuhalten (Zamfir 2020, Miehle et al. 2019). In diesem Spannungsumfeld haben die Partner des Konsortiums zwei Plattformansätze für einen Qualitäts- und Produktionsanwendungsfall gestaltet, der in iterativen Workshops entlang des Projektzeitraums evaluiert wurde. Um ein geeignetes Maß der Abs-traktion und Bewertung der Ergebnisse zu erreichen, sind gemeinschaftlich 19 verschiedene ökonomische, technische und organisatorische Faktoren formuliert worden, um die verschiedenen Perspektiven und Kompetenzen der Teilnehmer ganzheitlich zu erfassen.

2.1 Beschreibung zur Durchführung der Evaluation

Die Ergebnisse dieser Arbeit beruhen auf der Entwicklung und Umsetzung eines iterativen Fragebogens. Die Auswertungen wurden mittels einer Befragung der Projektteilnehmer gewonnen. Anhand von verschiedenen Dimensionen haben die Teilnehmer die Plattformen bewertet. Die Fragen konnten mit „stimme voll zu“ bis „stimme gar nicht zu“ beziehungsweise von „sehr gut“ bis „ungenügend“ beantwortet werden. Zur Vereinfachung und Abstraktion des Gesamtergebnisses wurden die Durchschnittswerte aller Faktoren der Befragten ermittelt. Die Graphen und Auswertungen zu den unterschiedlichen Dimensionen werden in dem jeweiligen Kapitel abgebildet.

2.2 Erläuterung ökonomischer Faktoren

Im folgenden Abschnitt werden sechs ökonomische Faktoren zur Bewertung der Plattformen dargestellt und in kurzer Form erklärt. Die Evaluationsergebnisse des Kapitels können der Tabelle 1 im Anhang entnommen werden. Ökonomische Faktoren behandeln dabei schwerpunktmäßig nicht technische Aspekte zwischen Anwendungs- und Softwarepartnern sowie deren Lieferanten und Kunden.

Tabelle E1-E2.1: Zusammenfassung ökonomischer Anforderungen

Nr.	Name und Definition
1	**Kundenservice**
	Beschreibt die erhöhte Transparenz für Events und Objekte im Wertschöpfungsnetzwerk für verschiedene Anwendungsfälle (z.B. Rückverfolgung von Rohkomponenten und Fertigmaterialen für Produktions- und Qualitätsevents)
2	**Entscheidungsfindung**
	Beschreibt die Fähigkeit der Organisation zu Kosteneinsparungen durch eine schnellere und einfachere Ermittlung fehlerhafter Objekte (Bauteile).
3	**Wertversprechen**
	Beim Einsatz und der Integration in unterschiedliche Informationssysteme erfahren die Organisationen die Möglichkeit, Prozesse und

	Daten auf dem Blockchain-Netzwerk abzulegen, um einen gegenseitigen Mehrwert durch das Teilen von Informationen zu erfahren.
4	**Produkte**
	Durch den Einsatz der Technologie werden die Anwendungsunternehmen dazu befähigt, höhere Qualitätsstandards in ihrem Unternehmen und dem Partnernetzwerk zu gestalten, um mittels digitaler Kennzeichnungen von Bauteilen Qualitätsmängel schneller im Netzwerk zu identifizieren.
5	**Rentabilität**
	Steigerung des Returns on Investment (ROI) für physische und digitale Produkte.
6	**Ein- und Austritt**
	Beschreibt die aufzuwendenden Onboarding- und Trennungskosten, die im Rahmen einer Wertschöpfungsnetzwerk-Konfiguration entstehen.

2.3 Auswertung ökonomischer Faktoren

Insgesamt kann anhand der Ergebnisse eine überwiegende Zustimmung bei den ökonomischen Faktoren seitens der Projektteilnehmer entnommen werden. Es gibt lediglich eine Stimme, welche nicht die Möglichkeit der Abbildung von Qualitätsprozessen und -maßnahmen, Erhöhung der Transparenz des Lieferantennetzwerks sowie einer Steigerung des Return-on-Investments mithilfe der Plattform ansieht. Bei der erhöhten Transparenz für verwendete Bauteile ist insgesamt noch Verbesserungsbedarf zu sehen, da keiner der Partner bei diesem Punkt voll zustimmt. Bei den restlichen ökonomischen Faktoren stimmen allerdings die meisten Projektpartner voll oder eher zu.

Blockchain-basierte Kollaborationsplattformen haben zudem den Vorteil, dass *Geschäftslogik* durch *Programmcode* abgebildet werden kann. So werden *Automatisierungspotentiale* freigesetzt, welche zuvor menschliche Interaktion benötigten. Die Automatisierung von Geschäftsprozessen birgt ein enormes Potential für *Effizienzsteigerungen*. Zudem können so Lieferkettenstrukturen effizienter gestaltet werden, da teilweise einzelne Stufen in der Wertschöpfungskette wegfallen.

2.4 Erläuterung technischer Faktoren

Die BC-Technologie wirkt sich auf technische Faktoren der Unternehmensarchitektur und Strategie aus, indem sie die Transparenz und Überprüfbarkeit von Transaktionen erhöht und verschiedene Bedingungen überwacht. Wie jede neue Technologie hat auch BC mit Hindernissen zu kämpfen. Technische Hindernisse betreffen beispielsweise den Durchsatz, die Latenzzeit, die Größe und den Energieverbrauch (Lu und Xu 2017; Peck et al. 2017). Die folgende tabellarische Aufstellung umfasst schwerpunktmäßig technische Faktoren und Herausforderungen zum Aufbau des Blockchain Netzwerkes. Die Integration in bestehende Informationssystem-Landschaften der Anwendungspartner sind mit technischer Unterstützung durch die teilnehmenden Softwareprojektpartner bewertet worden.

Dimension	Der Einsatz der Plattform ermöglicht…
Kundenservice	…erhöhte Transparenz für verwendete Bauteile (z.B. Rohkomponente, Fertigmaterialen)
	…Rückverfolgung der Materialflüsse
	…Gewährleistung von Qualitätsanforderungen
	…einfachere und schnellere Bearbeitung/Erfüllung von Kundenaufträgen
Entscheidungsfindung	…Kosteneinsparungen durch schnellere und einfachere Ermittlung passender Lieferanten
Werteversprechen	…Abbildung von Qualitätsprozessen und -maßnahmen
	…Erhöhung der Transparenz des Lieferantennetzwerks
	…Kosteneinsparungen durch Nachverfolgbarkeit bei gesetzlichen Rückrufen
	…Erhöhung der wahrgenommenen Datensicherheit
Produkte	…höhere Qualitätsstandards (z.B. fälschungssicherer Nachweis von Qualitätszertifikaten)
	…präziserer Rückruf verschiedener Produkte durch technische Identifikation von Qualitätsmängeln
Rentabilität	…Steigerung des Return-on-Investment (ROI)
Ein- und Austritt	…Reduktion der Anbahnungs- und Trennungskosten zu Lieferanten und Kunden
	…Steigerung des Zusammengehörigkeitsgefühl des Lieferantennetzwerks

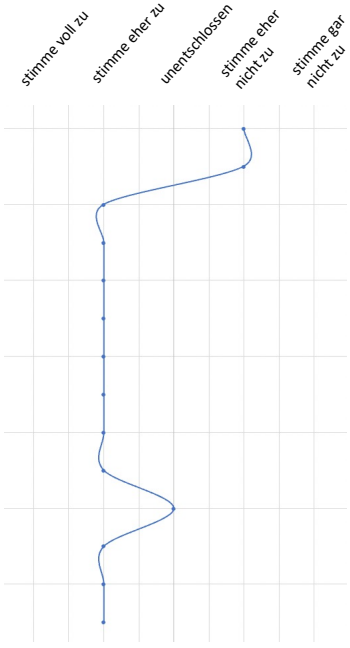


Abbildung E1-E2.1: Ökonomische Faktoren Auswertung (Median)

Tabelle E1&E2.2: Zusammenfassung technischer Anforderungen

Nr.	Name und Definition
6	**Usability**
	Beschreibt die Erlernbarkeit des neuen Systems und die Verständlichkeit zur Durchführung der Prozesse und Aufgaben. Darüber hinaus umfasst dies die Anpassbarkeit von Prozessen an individuelle Bedürfnisse.
8	**Nachvollziehbarkeit**
	Die einzelnen Transaktionen sind weiterhin für den Anwender transparent und einfach nachvollziehbar. Weiterhin gilt dies ebenso für verwendete Datenstrukturen und –flüsse, die von Entwicklern gestaltet werden.
9	**Dokumentation**
	Beschreibt den Einsatz und Workflow für verschiedene Administrations- und Entwicklungsprozesse zur Gestaltung von Anwendungsfällen mithilfe der Blockchain Technologie.
10	**Setup und Implementierung**
	Hiermit ist die Einfachheit zum Aufbau eines Konsortiums für Anwendungsfälle im Produktions- und Qualitätsumfeld gemeint. Weiterhin umfasst dies die technische Perspektive zur Integration notwendiger Informationssysteme.
11	**Änderungsmöglichkeiten**
	Möglichkeit von Änderungsvorschlägen bzw. eigenständigen Änderungsmöglichkeiten (bspw. Smart Contract, Konsortial-Blockchain-Architektur, Front-End der Plattform).
12	**Lizensierung**
	Transparenz der Lizenzierung der Software (bspw. Besitzverhältnisse, Betreibermodell)

2.5 Auswertung technischer Faktoren

Zur Beurteilung der technischen Faktoren sind sowohl die Anwendungspartner als auch Software-Integrationspartner für die beschriebenen Anwendungsfälle unabhängig voneinander befragt worden. Die Projektpartner konnten im Rahmen ihrer gesammelten Expertise und Projektaufgaben verschiedene Dimensionen in fünf Stufen (sehr gut bis ungenügend) beurteilen. Eine durchschnittliche Betrachtung aller Teilnehmer kann der Abbildung 2 entnommen werden. Nach wie vor ist die Blockchain Technologie vor allem in Bezug auf ihre technische Sicherheit von größter Bedeutung, da sie sich als algorithmisch sicher erwiesen hat. Vertrauen, Transparenz und Interoperabilität in Unternehmenslösungen sind allerdings nach wie vor immer noch eine sich entwickelnde Literatur und von vorrangiger Bedeutung. Es gibt einen Bedarf von Standards für Blockchain-Lösungen, damit sich Anbieter und Kunden einfach integrieren können. In diesem Punkt zeigt die Auswertung eine eher befriedigende Note im Zusammenhang verschiedener Dimensionen. Dies liegt nicht zuletzt daran, dass die Integration in bestehende Enterprise Systeme noch zu wenig erforscht ist (Haddara et al. 2021). Je nach Anwendungsfall empfanden die Integrationspartner die Nachvollziehbarkeit, Dokumentation sowie das Setup und die Implementierung unterschiedlich herausfordernd. Nicht zuletzt liegen die Chancen und Barrieren auch daran, wie die Komplexität verschiedener Prozesse fachlich und technisch auf einer Plattform abgebildet werden sollen. Vereinzelt waren sich die Projektteilnehmer in Bezug auf die Kompatibilität in bestehende Softwareprodukte uneinig. Im Rahmen der Integration fiel es den Partnern leicht, neue Partner bzw. mögliche neue Lieferanten in das Konsortium aufzunehmen. Dieser Punkt zeigt einen klaren

Dimension	Kriterium
Usability	Erlernbarkeit und Intuition der Bedienung
	Verständlichkeit durchzuführender Prozesse und Aufgaben
Nachvollziehbarkeit	Nachvollziehbarkeit der Funktionsweise der Plattform (bspw. Nachvollziehbarkeit der Datenstrukturen und -flüsse)
Dokumentation	Dokumentation des Workflows auf der Plattform
Setup und Implementierung	Einfachheit des Aufbaus der Konsortial-Blockchain
	Einfachheit der Integration in bestehender Systeme
Kompatibilität	Kompatibilität mit bestehender Software (Schnittstellen)
	Einfachheit der Implementierung der Plattform
Änderungsmöglichkeiten	Möglichkeit von Änderungsvorschlägen bzw. eigenständigen Änderungsmöglichkeiten (bspw. Smart Contract, Konsortial-Blockchain, Front-End Plattform)
	On- und Off-Boarding von Lieferanten
Lizensierung	Transparenz der Lizenzierung der Software (bspw. Besitzverhältnisse, Betreibermodell)

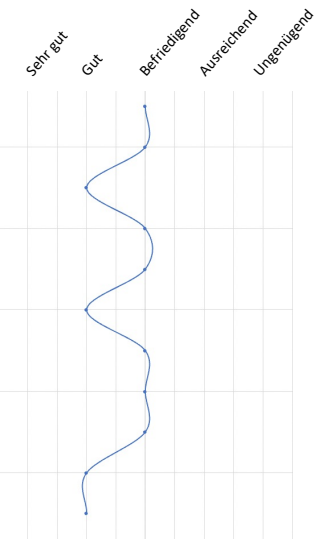


Abbildung E1-E2.2: Technische Faktoren Auswertung (Median)

Gegensatz zu in der Forschung formulierten komplexen Onboarding-Prozessen auf (Sunvay et al. 2021). Große Unternehmen haben oft aufgrund ihrer Ziele, historisch gewachsener Denkweisen und komplexer Endprodukte enorme Anforderungen an die Geschäfts- und Technologieintegration, was die Adaption solcher innovativeren Technologie verlangsamt. In diesem Punkt können die Flexibilität und Größe kleiner und mittlerer Unternehmen als ein Vorteil hervorgehoben werden, sich einfacher auf eine Plattform mit anderen Partnern integrieren zu können. Gemischt sahen die Projektpartner die Entwicklung eines technischen Betreibermodells, da es immer noch an Lizenzierungsmöglichkeiten einer konsortialen Blockchain in der Praxis fehlt.

2.6 Erläuterung organisatorische Faktoren

Weitere organisatorische Herausforderungen zur Adaption der Blockchain-Technologie betreffen den erhöhten Koordinierungsaufwand innerhalb von BC-Konsortien (Sunyaev et al. 2021), Datenschutz- und Sicherheitsfragen, regulatorische Unsicherheit, mehrere Parteien, die ihre Kräfte bündeln müssen und Widerstand gegen Veränderungen (Hackius und Petersen 2017). Infolgedessen nehmen Diskussionen über die Komplexität und Transparenz zur Adaption innerhalb der Lieferernetzwerke zu (Dasaklis et al. 2022). Die Technologie benötigt daher eine geordnete Einbettung in eine langfristige Strategie, um effizient für verschiedene Unternehmensebenen einen positiven und nachhaltigen Wertbeitrag zu generieren. Im Folgenden sind drei Faktoren in kurzer Form beschrieben.

Tabelle E1&E2.3: Zusammenfassung organisatorischer Anforderungen

Nr.	Name und Definition
16	**Strategie**
	Zum Begriff Strategie zählt das Projektkonsortium jegliche organisatorischen und technischen Faktoren zur Kollaboration mit Lieferanten und der Gestaltung neuer und innovativer Produktstrategien auf langfristiger Ebene.
17	**Struktur**
	Mitarbeiter auf operativer, taktischer und strategischer Ebene bestimmen sowohl Aufgaben als auch die Zusammensetzung von Gruppen und die Zuordnung von Aufgaben zu Lieferanten und Kunden. Der Begriff umfasst deshalb die Relationen zu Befugnissen und Kompetenzen einzelner Akteure in seiner Netzwerkstruktur für alle wertschöpfenden Tätigkeiten.
18	**Koordination**
	Beschreibt die Abhängigkeiten und Schnittstellen im Wertschöpfungsnetzwerk, mit den Prozesse, Daten und Informationen transparent gestaltet werden, um nachhaltig positive Verbesserungen durch Kollaborationen zu erreichen.

2.7 Auswertung organisatorischer Faktoren

Die BC-Technologie erfordert bei der Adaption eine Umstellung zahlreicher Faktoren auf organisatorischer Ebene. Hierzu beschreibt die Forschung beispielsweise den hohen Koordinierungsaufwand innerhalb von BC-Konsortien (Sunyaev et al. 2021),

Dimension	Durch den Einsatz der Plattform verändert/verändern sich…
Strategie	…Unternehmensstrategie (bspw. Kollaborationen auf organisatorischer Ebene)
	…Lieferantennetzwerk ("Breite" und "Tiefe")
	…Produktvarianten (Produkt-Daten-Strategien)
Struktur	…operative Aufgaben der Mitarbeiter (Durchführung)
	…Managementaufgaben der Mitarbeiter (Planung, Führung, Kontrolle)
	…Aufgabenteilung und Zuordnung/Gruppierung (z. B. Aufgaben werden überflüssig, Organisationseinheiten werden zusammengefasst)
	…potenzielle Anzahl der Mitarbeiter
	…Befugnisse und Verantwortlichkeiten (z.B. Berichtswesen, Entscheidungsfindung)
	…Fähigkeits-/Kompetenzprofile der Mitarbeiter
	…Art der Kunden
	…Art der Lieferanten (Größe, Standort etc.)

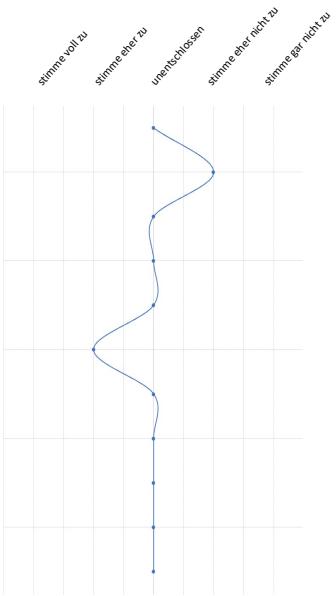


Abbildung E1-E2.3: Organisatorische Faktoren Auswertung (Median)

Dimension	Durch den Einsatz der Plattform verändert sich/verändern sich…
Koordination	…Abhängigkeiten zwischen Netzwerkpartnern
	…Schnittstellenprobleme im Lieferantennetzwerk
	…Schnittstellenprobleme zwischen einzelnen Aufgaben- und Verantwortungsbereichen im eigenen Unternehmen
	…Koordinations- und Abstimmungsintensität (dezentral vs. zentral)

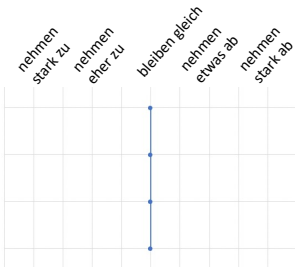


Abbildung E1-E2.4: Organisatorische Faktoren (Median)

Fragen rund um Datenschutz- und Sicherheitsfragen, regulatorische Unsicherheit, mehrere Parteien, die ihre Kräfte bündeln müssen, was nicht zuletzt zu Widerstand gegen Veränderungen innerhalb der Organisation führen kann. Dies betrifft sowohl die Unternehmensstrategie, das Lieferantennetzwerk der Anwendungspartner als auch zukünftige Produktvarianten, die von Umstellungen betroffen sein können. Weiterhin sind Organisationsstrukturen und –abläufe involviert, die neue Kompetenzprofile von Mitarbeitern erfordern. Aufgrund der Neuartigkeit von Anwendungsfällen und nicht vollständigen Implementierung in der Praxis über mehrere Lieferanten, ergibt sich zum Zeitpunkt der Befragung ein eher unentschlossenes Bild des Konsortiums (siehe Abbildung Abbildung E1&E2.3)

Die oben genannten Dimensionen zeigen vorwiegend die interne Perspektive, die zu verschiedenen Änderungen führt. Die unten dargestellte Dimension beschreibt im Kontrast dazu eine externe Perspektive von Partnern und Systemen. Auch wenn die Partner ein Potential für die jeweiligen Unternehmensumgebungen identifiziert haben, gehen sie zum Zeitpunkt der Befragung allerdings weiterhin davon aus, dass es zu Schnittstellenproblemen führen wird und keine markanten Erleichterungen in der Koordination zu erwarten sind.

Abschließend zeigt sich in der Befragung der Dimension „Koordination“, dass der Einsatz einer Blockchainplattform für die Projektteilnehmer eine Verbesserung des Datenzugriffs auf Objekte außerhalb der eigenen Unternehmensgrenzen ermöglicht, und hierdurch die Transparenz der Prozesse im Wertschöpfungsnetzwerk gesteigert werden. Weiterhin sind die Anwendungs- und Softwarepartner der Auffassung, dass die Produktsicherheit in Bezug auf implementierte Daten und physische Produkte verbessert werden kann, sofern es ein ganzheitliches Konzept für die Implementierung über die eigenen Unternehmensgrenzen hinausgibt.

2.8 Fazit der Ergebnisse

Zu Beginn dieses Ergebnisberichts wurde aufgezeigt, dass die Adaption der Blockchain-Technologie verschiedene Herausforderungen für Qualitäts- und Produktionsabsicherungs-Use Cases darstellt. Gleichzeitig wird durch die Befragung der Teilnehmer gezeigt, dass die Notwendigkeit einer effektiveren Zusammenarbeit zwischen Organisationen über Unternehmensgrenzen hinweg und einer höheren Produktqualität ein Treiber für die Adaption der Technologie darstellen. Dieser Umstand kann als eine organisatorische und technische Vertrauensherausforderung interpretiert werden. Zum einen befindet sich die Technologie nach wie vor in einem frühen Pionier-Stadium. Andererseits ist die Koordination zwischen den Handelspartnern auf organisatorischer Ebene notwendig, um ein gesteigertes Vertrauen und eine höhere Effizienz zu erreichen. Die Projektpartner waren sich einig, dass dies für jedes Informationssystem, jedes Objekt und jede Art der gemeinsamen Nutzung standardisiert und koordiniert werden muss. Entscheidend ist dabei das Kosten/Nutzen-Verhältnis, welches nach wie vor noch nicht im Einklang mit aktuellen Gegebenheiten steht. Nichtsdestotrotz zeigt diese Evaluation den theoretischen Bedarf an Zusammenarbeit und Mehrwert für mehrere Produktionsumgebungen auf.

Dimension	Der Einsatz der Plattform ermöglicht…
Koordination	…Verbesserung der Zugriffs auf Daten außerhalb des eigenen Unternehmen (Koordination und Abstimmung)
	…Speicherung der Transparenz der Prozesse im Wertschöpfungsnetzwerk
	…nachhaltige Steigerung der Datensicherheit
	…Verbesserung der Produktsicherheit außerhalb der eigenen Unternehmensgrenzen

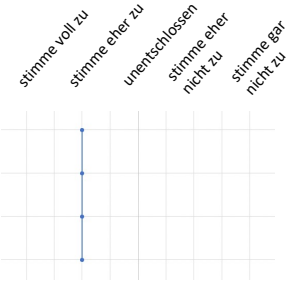


Abbildung E1-E2.5: Organisatorische Faktoren (Median)

3 Übertragbarkeit der Ergebnisse

Aufbauend auf den oben erstellten Ergebnissen werden sogenannte „Lessons learned“ und die Übertragbarkeit von ökonomischen, technischen sowie organisatorischen Faktoren dargestellt. Hierfür wird eine Beschreibung einzelner Punkte und eine Zuordnung von **Unterpunkten** in der jeweiligen Kategorie dargestellt. Zusammenfassend sind in der letzten Spalte die Projektpartner in Kurzform gekennzeichnet (Actiware = A, Maul Theet = MT, Infosim = IN, Robur Automation = RA), um überschneidende Punkte möglichst kompakt darzustellen. Die Darstellungen der einzelnen Parteien beziehen sich mehrheitlich auf innerbetriebliche und technische Umgebungen, sodass im Einzelfall Produkte und Informationssysteme (ScanningLaser, StableNet, Produkt ATIS und OMS) genannt werden, die einen spezifischen Geschäftskontext des Unternehmens haben.

Tabelle E1&E2.4: Zusammenfassung Übertragbarer Ansätze und Komponenten

Übertragbarkeit von	Zuordnung und Beschreibung der Faktoren	Partner
Ökonomischen Faktoren	**Wertversprechen:** Es können neue und innovative Userinteraktionen im Rahmen von QM-Prozessen für weitere Kunden angeboten werden.	A
	Entscheidungsfindung/Rentabilität: Neue Aufnahme und Perspektive von technischen und organisatorischen Grenzen (Do's and Don'ts) bezüglich Blockchain Implementierungsprojekten. Weiterhin ist eine verbesserte Abwägung von Kosten und Nutzen insbesondere bei KMU angesichts der relativ hohen Opportunitätskosten bei Blockchain Netzwerken für zukünftige Projekte möglich.	A
	Produkte: Die prototypische Anwendung auf Messmittel ermöglicht ein erweitertes Datenangebot (bspw. Datum der Messung, die Firma, Beschreibung der Dienstleistung) für qualitätsbewusste Kunden. Weiterhin können über die Blockchain auch Kalibrierzertifikate zur Verfügung gestellt werden, um eine gesteigerte Transparenz der Nachverfolgung zu erleichtern. Erste Berührungspunkte mit der Technologie erlauben auch den Einsatz für weiteres Produktspektrum des Unternehmens.	MT
	Kundenservice: Gesteigerte Kundenwünsche wie das Feststellen fehlerhafter "Bauteile" ist in einer Plattform möglich. Hieraus ergeben sich kürzere Kommunikationswege bzw. schnellere Bearbeitung der Reklamation, die mit alten Systemen und Prozessen nicht möglich waren. Technische Skripte können darüber hinaus in anderen Abteilungen eingesetzt werden, um derartige gesteigerte Kundenwünsche zu erfüllen.	MT, IN
Technischen Faktoren	**Nachvollziehbarkeit:** Die in den Anwendungsfällen entwickelten Modelle (Objektmodell, Transaktionsmodell) lassen sich auf weitere Blockchain- und Supply-Chain Ketten anwenden. Hier ist der Transfer möglich, der beispielsweise zur unternehmensübergreifenden Interaktion zwischen einzelnen ERP oder MES Systemen genutzt wird.	A
	Kompatibilität/Änderungsmöglichkeiten: Die Versatilität/Integrierbarkeit von StableNet bzgl. komplexer Anforderungen konnte demonstriert/verifiziert werden.	IN
	Kompatibilität/Änderungsmöglichkeiten: Als neue Funktionalität ist die Integration in das interne Produkt ATIS (Datensammler) für eine technische Neuausrichtung ermittelt und wird zukünftig umgesetzt. Damit kann das Sammeln von Prozess- und Maschinendaten integrierter und resistenter gestaltet werden, bspw. wenn es um das Quittieren von Fehlern durch Bedienpersonal geht, oder Änderungen von Rezepturen	RA
	Lizensierung/Betreibermodell: Neue und innovative Integration als optionale Funktionalität in das interne Produkt OMS (Order Management System). Hierbei handelt es sich um ein Bestellsystem, das potenziell	RA

	auch als Produkt angeboten werden kann. Eine Blockchain Funktionalität steigert hier die Wettbewerbsfähigkeit und ermöglicht neue Abrechnungsmöglichkeiten mit Partnern.	
	Kompatibilität: Generell ist es so, dass die Nutzung einer solchen Plattform für uns nur dann in Frage kommt, wenn diese als ein fertiges Modul bereitgestellt wird und am besten auch noch in unser System integriert werden kann.	MT
	Setup und Implementierung: Im Rahmen der Projektarbeiten konnten zahlreiche Kenntnisse für Blockchains allgemein, Hyperledger und CouchDB bei Entwicklern aufgebaut werden, die in zukünftigen Projekten und ähnlichen Anwendungsfällen genutzt werden können.	IN, A
Organisatorischen Faktoren	**Produkt-/Datenstrategie:** Erweiterung von unseren Standardprojekten zu Enterprise Content Management-Einführungen, um Validierungen per Blockchain zu ermöglichen.	A
	Produkt-/Datenstrategie: Übertragbarkeit auf andere Produktangebote aus unserem Sortiment (ScanningLaser und große Prüfstände) sind mit gewonnenen Erkenntnissen möglich.	MT
	Produkt-/Datenstrategie: Wir können die von uns entwickelten Überwachungsskripte (Blockchain, Hyperledger, CouchDB) auch in anderen Projekten / für Kunden verwenden/weiterentwickeln.	IN
	Strategie Lieferantennetzwerk: Die Anforderungen an die Verwendung transparenter, manipulationssicherer Lösungen zur Datenhaltung innerhalb einer Wertschöpfungskette werden weiter an Bedeutung gewinnen. Als Systemintegrator muss RA mit den Systemen der Kunden und Lieferanten interagieren. Durch das Projekt PiMKoWe konnten breite Kompetenzen im Umgang mit diesen Systemen erarbeitet werden.	RA
	Befugnisse und Verantwortlichkeiten: Bzgl. Implementierung sieht sich RA nun in der Lage, einfache Blockchain Lösungen nach Kundenanforderungen selbst zu implementieren. Bei komplexeren Projekten sollte dies gemeinsam mit den Partnern erfolgen.	RA
	Struktur Aufgabenteilung und Zuordnung: Durch die Zusammenarbeit mit Partnern konnten Einblicke in deren Arbeitsweise, Produkte, verwendete Technologien usw. gewonnen werden, die eine veränderte Arbeitsweise für zukünftige Projekte erlauben.	IN

Literaturverzeichnis

Dasaklis, T. K., Voutsinas, T. G., Tsoulfas, G. T., and Casino, F. 2022. “A Systematic Literature Review of Blockchain-Enabled Supply Chain Traceability Implementations,” Sustainability (14:4), p. 2439.

Haddara, M., Norveel, J., and Langseth, M. 2021. “Enterprise Systems and Blockchain Technology: The Dormant Potentials,” Procedia Computer Science (181). CENTERIS 2020 - International Conference on ENTERprise Information Systems / ProjMAN 2020 - International Conference on Project MANagement / HCist 2020 - International Conference on Health and Social Care Information Systems and Technologies 2020, CENTERIS/ProjMAN/HCist 2020, pp. 562–571

Hackius, N. and Petersen, M. 2017. “Blockchain in logistics and supply chain: trick or treat?,” in: Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry

Kuhn, M., Schaefer, F., and Otten, H. 2018. “Process Complexity as a Future Challenge – a Quality Management Perspective,” The TQM Journal (30:6) 2018, pp. 701–716.

Lu, Q. and Xu, X. 2017. “Adaptable blockchain-based systems: A case study for product traceability,” IEEE Software (34:6), pp. 21–27.

Peck, Morgen E. "Blockchain world-Do you need a blockchain? This chart will tell you if the technology can solve your problem." IEEE Spectrum 54.10 (2017): 38-60.

Rejeb, Abderahman, et al. "Blockchain technologies in logistics and supply chain management: a bibliometric review." Logistics 5.4 (2021): 72.

Miehle, D., Henze, D., Seitz, A., Luckow, A., and Bruegge, B. 2019. “PartChain: a decentralized traceability application for multi-tier supply chain networks in the automotive industry,” in: 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), IEEE, pp. 140–145.

Sunyaev, Ali, et al. "Token economy." Business & Information Systems Engineering 63.4 (2021): 457-478.

Zamfir, I. 2020. Towards a mandatory EU system of due diligence for supply chains. Tech. rep. BRIEFING EPRS | European Parliamentary, pp. 1–10.

Anhang

Dimension	Der Einsatz der Plattform ermöglicht…
Kundenservice	…erhöhte Transparenz für verwendete Bauteile (z.B. Rohkomponente, Fertigmaterialen)
	…Rückverfolgung der Materialflüsse
	…Gewährleistung von Qualitätsanforderungen
	…einfachere und schnellere Bearbeitung/Erfüllung von Kundenaufträgen
Entscheidungsfindung	…Kosteneinsparungen durch schnellere und einfachere Ermittlung passender Lieferanten
Werteversprechen	…Abbildung von Qualitätsprozessen und -maßnahmen
	…Erhöhung der Transparenz des Lieferantennetzwerks
	…Kosteneinsparungen durch Nachverfolgbarkeit bei gesetzlichen Rückrufen
	…Erhöhung der wahrgenommenen Datensicherheit
Produkte	…höhere Qualitätsstandards (z.B. fälschungssicherer Nachweis von Qualitätszertifikaten)
	…präziserer Rückruf verschiedener Produkte durch technische Identifikation von Qualitätsmängeln
Rentabilität	…Steigerung des Return-on-Investment (ROI)
Ein- und Austritt	…Reduktion der Anbahnungs- und Trennungskosten zu Lieferanten und Kunden
	…Steigerung des Zusammengehörigkeitsgefühl des Lieferantennetzwerks

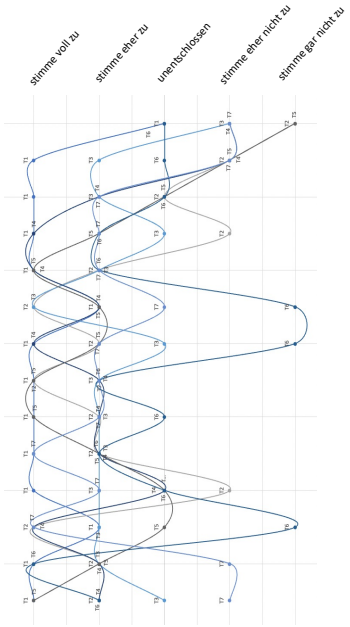


Abbildung E1-E2.6: Ökologische Faktoren (einzelne Positionen)

Dimension	Kriterium
Usability	Erlernbarkeit und Intuition der Bedienung
	Verständlichkeit durchzuführender Prozesse und Aufgaben
Nachvollziehbarkeit	Nachvollziehbarkeit der Funktionsweise der Plattform (bspw. Nachvollziehbarkeit der Datenstrukturen und -flüsse)
Dokumentation	Dokumentation des Workflows auf der Plattform
Setup und Implementierung	Einfachheit des Aufbaus der Konsortial-Blockchain
	Einfachheit der Integration in bestehender Systeme
Kompatibilität	Kompatibilität mit bestehender Software (Schnittstellen)
	Einfachheit der Implementierung der Plattform
Änderungsmöglichkeiten	Möglichkeit von Änderungsvorschlägen bzw. eigenständigen Änderungsmöglichkeiten (bspw. Smart Contract, Konsortial-Blockchain, Front-End Plattform)
	On- und Off-Boarding von Lieferanten
Lizensierung	Transparenz der Lizenzierung der Software (bspw. Besitzverhältnisse, Betreibermodell)

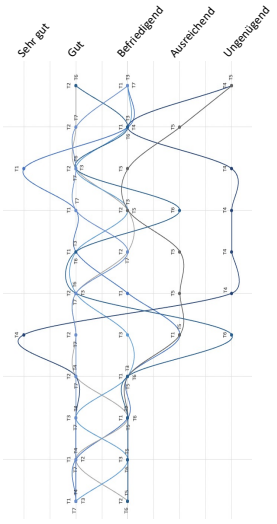


Abbildung E1-E2.7: Technische Faktoren (einzelne Positionen)

Dimension	Der Einsatz der Plattform ermöglicht…
Koordination	…Verbesserung der Zugriffs auf Daten außerhalb des eigenen Unternehmen (Koordination und Abstimmung)
	…Speicherung der Transparenz der Prozesse im Wertschöpfungsnetzwerk
	…nachhaltige Steigerung der Datensicherheit
	…Verbesserung der Produktsicherheit außerhalb der eigenen Unternehmensgrenzen

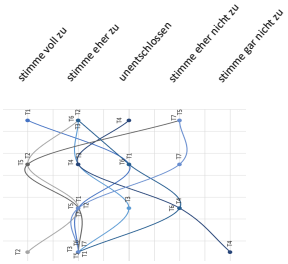


Abbildung E1-E2.8: Organisatorische Faktoren (einzelne Positionen)

	Durch den Einsatz der Plattform verändert/verändern sich…
Strategie	…Unternehmensstrategie (bspw. Kollaborationen auf organisatorischer Ebene)
	…Lieferantennetzwerk ("Breite" und "Tiefe")
	…Produktvarianten (Produkt-Daten-Strategien)
Struktur	…operative Aufgaben der Mitarbeiter (Durchführung)
	…Managementaufgaben der Mitarbeiter (Planung, Führung, Kontrolle)
	…Aufgabenteilung und Zuordnung/Gruppierung (z. B. Aufgaben werden überflüssig, Organisationseinheiten werden zusammengefasst)
	…potenzielle Anzahl der Mitarbeiter
	…Befugnisse und Verantwortlichkeiten (z.B. Berichtswesen, Entscheidungsfindung)
	…Fähigkeits-/Kompetenzprofile der Mitarbeiter
	…Art der Kunden
	…Art der Lieferanten (Größe, Standort etc.)

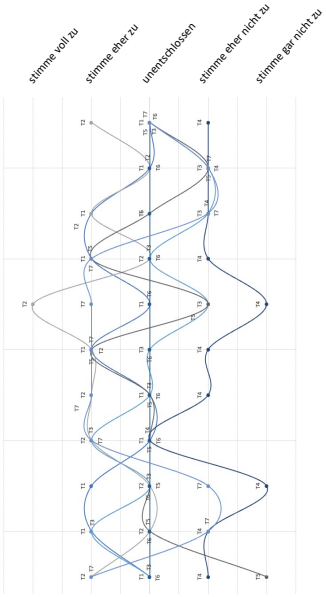


Abbildung E1-E2.9: Organisatorische Faktoren (einzelne Positionen)

Dimension	Durch den Einsatz der Plattform verändert sich/verändern sich…
Koordination	…Abhängigkeiten zwischen Netzwerkpartnern
	…Schnittstellenprobleme im Lieferantennetzwerk
	…Schnittstellenprobleme zwischen einzelnen Aufgaben- und Verantwortungsbereichen im eigenen Unternehmen
	…Koordinations- und Abstimmungsintensität (dezentral vs. zentral)

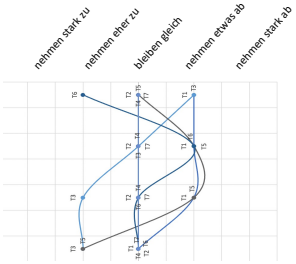


Abbildung E1-E2.10: Organisatorische Faktoren (einzelne Positionen)

Konsortialpartner

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

infosim®

SAP Signavio

ROBUR AUTOMATION
YOUR INDUSTRIAL AUTOMATION SPECIALIST

actiware®
DEVELOPMENT

MAUL·THEET
Vibration Test & Analysis

Aktuelle Informationen zum Projekt PIMKoWe

https://projekt-pimkowe.de

Das Projekt “PIMKoWe”

Eines der größten Probleme von Wertschöpfungsnetzwerken ist der verlässliche, fälschungssichere und automatisierte Austausch digitaler Daten und Informationen im Rahmen der überbetrieblichen Zusammenarbeit. Während moderne Informationssysteme bereits zahlreiche Anforderungen von integrierten Produktionsprozessen adressieren, fehlt es insbesondere an überbetrieblichen Lösungsansätzen, die das vorhandene Datenfundament über die gesamte Lieferkette hinweg nutzbar machen. Als Fundament zahlreicher Industrie 4.0-Szenarien kann die mangelnde Datenintegration die digitale Transformation kleiner und mittelgroßer Unternehmen (KMU) und damit die Wettbewerbsfähigkeit des Industriestandorts Deutschland gefährden.

Gleichwohl gehen mit der überbetrieblichen Integration zahlreiche Potenziale einher, die insbesondere für den industriellen Sektor nutzbar sind. So fördern Optimierung und Automatisierung nachhaltige Produktivitätssteigerungen, die Flexibilisierung gegenüber Nachfrageschwankungen und die Früherkennung von Engpässen oder Produktionsausfällen.

Das Verbundprojekt PIMKoWe adressiert diese Problemstellung durch die Bereitstellung einer Koordinationsplattform zur Flexibilisierung, Automatisierung und Absicherung von Kooperationen in Wertschöpfungsnetzwerken des industriellen Sektors. Auf Basis kryptographischer Verkettung werden relevante betriebswirtschaftliche Daten dezentral und unveränderbar auf einer Blockchain gespeichert, sodass die Integrität von Wertschöpfungspartnern garantiert und das Vertrauen sowie die Transparenz innerhalb entsprechender Netzwerke gewährleistet wird. Die dabei entstehende Plattform ermöglicht die Verarbeitung dezentral gespeicherter Informationen und fördert Datenschutz und Datensicherheit. Standardisierte und adaptive Schnittstellen zu handelsüblichen Informationssystemen erlauben die automatische Extraktion relevanter Daten sowie die problemlose Integration der Plattform in die vorhandene IT-Infrastruktur von KMU.

Die vorliegende Auswertung wurde durchgeführt von:

Julius-Maximilians-Universität Würzburg

Lehrstuhl für BWL und Wirtschaftsinformatik
Prof. Dr. Axel Winkelmann
Sanderring 2
97070 Würzburg

Autoren und Ansprechpartner

Norman Pytel, M.Eng.

Wissenschaftlicher Mitarbeiter
Norman.Pytel@uni-wuerzburg.de
+49 931 31- 86348

Prof. Dr. Axel Winkelmann

Lehrstuhl für BWL und Wirtschaftsinformatik
axel.winkelmann@uni-wuerzburg.de
+49 931 31-89640

Dr. Patrick Bredebach

Productmanager
Actiware Development GmbH
patrick.bredebach@actiware-development.com
+49 231 5347 2540

Ole Jankowski, B.Sc.

Solution Architect
Actiware Development GmbH
ole.jankowski@actiware-development.com

Michael Baumgart, M.Sc.

Infosim GmbH & Co. KG
baumgart@infosim.net
+49 931 205 92 200