

Studie

Automation und Digitalisierung

Potenzial und Einsatz von Blockchain- und
Distributed-Ledger-Technologien in der Automatisierungstechnik





Automation und Digitalisierung

Herausgeber:

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e. V.

Fachverband Automation

Lyoner Straße 9

60528 Frankfurt am Main

Verantwortlich: Dr. Markus Winzenick

Telefon: +49 69 6302-426

E-Mail: winzenick@zvei.org

www.zvei.org

Februar 2019



Dieses Werk ist lizenziert unter einer Creative Commons
Namensnennung – Nicht-kommerziell – Weitergabe unter
gleichen Bedingungen 4.0 International Lizenz.

Trotz größtmöglicher Sorgfalt übernimmt der ZVEI für
Vollständigkeit und Richtigkeit der Inhalte keine Gewähr.



Hochschule für Angewandte
Wissenschaften Hamburg

Forschungs- und Transferzentrum
für digitale Wirtschaftsprozesse
Arbeitsgruppe DLT³-Hamburg

Berliner Tor 5
20099 Hamburg

Autoren:

Prof. Dr.-Ing. Volker Skwarek

Julian Reher, B. Sc.



Julius-Maximilians-
Universität Würzburg

Lehrstuhl für Informatik III

Sanderring 2
97070 Würzburg

Autoren:

Stefan Geißler M. Sc.

Prof. Dr. Thomas Zinner

Inhalt

Vorwort	5
Kurzfassung	5
Executive Summary	6
1 Einführung	7
1.1 Zusammenhang Industrie 4.0 und Blockchain / Distributed Ledger	7
1.2 Überblick über Potenziale von BC/DLT	9
1.3 Aufbau und Ziel der Studie	10
2 Die Blockchain-Technologie	11
2.1 Blockchain am Beispiel Industrie 4.0	11
2.2 Die Blockchain-Technologie	13
2.2.1 Technologischer Hintergrund	13
2.2.2 Weiterentwicklungen und Anwendungen der Blockchain-Technologie	17
3 Anwendungsszenarien mit Blockchain- Mechanismen in der Automation	18
3.1 Anwendungsszenarien der Blockchain-Technologie	18
3.2 Anwendungsszenarien aus der Industrie 4.0	20
3.3 Übertragung der Blockchain-Technologie auf die Anwendungsszenarien der Plattform Industrie 4.0	21
3.3.1 Auftragsgesteuerte Produktion (AGP)	21
3.3.2 Wandlungsfähige Fabrik (WFF)	21
3.3.3 Selbstorganisierende adaptive Logistik (SAL)	21
3.3.4 Value-based Services (VBS) und Transparenz und Wandlungsfähigkeit ausgelieferter Produkte (TWP)	22
3.3.5 Smarte Produktentwicklung für die smarte Produktion (SP2) und innovative Produktentwicklung (IPE)	22
3.4 Gegenüberstellung: Industrie-4.0- Anwendungsszenarien und Blockchain-Archetypen	22
4 Industrie 4.0: Gestaltungspotenziale durch Blockchains	24
4.1 Analyse der Anwendungsszenarien	24
4.2 Abgeleitete strategische Herausforderungen	25
4.3 Maßnahmen zur Akzeptanz im Markt	28
4.4 Standardisierung	29
4.5 Aktuelle Forschungsaktivitäten	30
5 Zusammenfassung und Empfehlungen	32

Vorwort



Quelle: Phoenix Contact

Die Technologie ist da, wo bitte sind die Anwendungen?

Die digitale Durchdringung aller Lebensbereiche – „Internet of Things“ und Industrie 4.0 – eröffnet neue Möglichkeiten, die mitunter disruptive Auswirkungen auf Unternehmen und deren Geschäftsmodelle und auch auf ganze Wirtschaftssysteme haben. Blockchain wird in diesem Zusammenhang wiederholt als Technologie genannt, die ein Potenzial besitzt, die „digitale Welt“ noch einmal revolutionär zu verändern. Mit dem Hype der Kryptowährung Bitcoin (2017/2018) wurde Blockchain, die eine sichere Kontoführung technologisch ermöglicht, als attraktive Technologiebasis in den Fokus gerückt.

Bleibt Blockchain weiterhin ein wesentliches Synonym für Kryptowährung und Applikationen im Bankverkehr oder entwickelt sich diese Technologie hin zu einem weiteren Mittel, spezifische Anforderungen in industriellen Applikationen zu lösen?

Banken, Versicherungen und erste Industrieunternehmen sehen hier bereits wirtschaftliche Vorteile und evaluieren bzw. forschen an Blockchain-Mechanismen jenseits der Kryptowährung. Die Nutzung von Smart Contracts in der Logistik ist dafür ein gutes Beispiel: Die automatisierte Abarbeitung von Transportverträgen zwischen Partnern durch Maschinen erfolgt, ohne dass der Menschen als Vermittler oder Kontrolleur eingreift. Die Blockchain sorgt hierbei für ein handlungsgemäß richtiges Arbeiten.

Vieles könnte mit Blockchain gelöst werden. Dennoch gibt es derzeit keine großflächigen Applikationen in der Industrie. Die im Raum stehende Frage ist: Was bedeutet Blockchain für die Industrie und wo ist Blockchain sinnvoll und auch kommerziell nutzbar?

Wir wissen – Blockchain ist kein Allheilmittel, aber eine junge, sich dynamisch entwickelnde Technologie mit viel Potenzial. Aus heutiger Sicht stellt sie bereits eine sinnvolle Ergänzung im industriellen Technologieportfolio dar. Dieses gilt es hier zu betrachten.

Johannes Kalhoff

Vorsitzender des Technischen Ausschusses Automation im ZVEI,
Phoenix Contact GmbH & Co KG

Kurzfassung

Im Rahmen dieser Studie werden Anwendungsmöglichkeiten der Blockchain- und Distributed-Ledger-Technologien (BC/DLT) – kurz: Blockchain-Technologie – in der Automatisierungstechnik aufgezeigt. Dabei wird zunächst die Blockchain-Technologie in ihren Grundzügen beschrieben. Anschließend werden verschiedene Anwendungen der Technologie in der Automation dargestellt, ihr jeweiliger Nutzen gegenüber heutigen Lösungen herausgearbeitet und gegebenenfalls Besonderheiten gegenüber anderen Anwendungen und Branchen beleuchtet. Schlussendlich werden hieraus Empfehlungen für die Automatisierungsbranche abgeleitet.

Executive Summary

Im Rahmen der vorliegenden Studie werden zwei Trends der Digitalisierung – nämlich Industrie 4.0 (I4.0) und Blockchain-Technologien – in einen gemeinsamen Zusammenhang gebracht. Blockchain-Technologien stehen dabei abkürzend für den Begriff Blockchain- und Distributed-Ledger-Technologien (BC/DLT) und bezeichnen ein Protokoll aus Verteilen und Verketteten sowie Konsens über Transaktionen. BC/DLT stellt einen Sammelbegriff aus einer Vielzahl¹ von Technologie- und Implementierungsvarianten dar, die in dieser Studie nicht weiter differenziert oder betrachtet werden. Vielmehr wird hier angenommen, dass Daten in Transaktionen verpackt, versendet und durch Verkettung untereinander gegen Manipulation abgesichert werden. BC/DLT steht hier somit für hierarchielose, vertrauenswürdige, verteilte und asynchrone Kommunikation/Datenhaltung.

Aufgrund der Dezentralität, die mit Blockchain-Technologien einhergeht, und derselben Dezentralität, die in einem komplexen Automatisierungsszenario für Industrie-4.0-Anwendungen auftreten kann, ist es denkbar und wahrscheinlich, dass BC/DLT eine geeignete Lösung zur Erhöhung der Datensicherheit darstellt. Darüber hinaus ist es möglich, in bestimmten Ausprägungen von BC/DLT auch dezentrale Software (Smart Contracts / Chaincode o. Ä.) mithilfe von Transaktionen zu aktivieren. Derartige Smart Contracts sind dann in der Lage, an einer beliebigen Stelle des Systems Ergebnisse zu berechnen, die an einer anderen Stelle zur Automatisierung und Ausführung verwendet werden. Einerseits wird mit einer solchen Flexibilität eine hohe Redundanz und Ausfallsicherheit geschaffen, andererseits lassen sich so freie Rechenressourcen im Gesamtsystem nutzen.

Die Blockchain-Technologie wird in dieser Studie – abgesehen von einer generellen funktionalen Einleitung – technologisch nicht weiter erläutert. Vielmehr wird ein 5W-Analyseschema zur Verfügung gestellt, mit dem Schritte und Rollen in BC/DLT genauer beleuchtet werden, um eine technologische Entscheidung hinsichtlich bestimmter Technologieausprägungen zu unterstützen.

Charakteristische Eigenschaften von BC/DLT werden im Verlauf der Studie herausgearbeitet und auf Geschäftsfälle bzw. Szenarien wie Tracking und Tracing, Energiemanagement, Existenz- und Eigentumsnachweis, Finanztransaktionen, Lizenzmanagement, Informationsaustausch zwischen Systemen, verteilte Anwendungen und Anwendungen mit vertraglichen Bindungswillen übertragen. Diese sogenannten atomaren Elemente werden dann mit den Anwendungsszenarien Industrie 4.0 in Zusammenhang gebracht und tabellarisch Ausprägungsintensitäten zugeordnet. Dabei lassen sich dann besondere Anwendungsszenarien herausarbeiten, bei denen Blockchain-Technologien hohe Anwendungspotenziale bieten. Dazu zählen insbesondere die selbstorganisierende adaptive Logistik (SAL) und die auftragsgesteuerte Produktion (AGP). Aber auch andere Szenarien wie beispielsweise wandlungsfähige Produkte (TWP) oder die intelligente Produktentwicklung (IPE) können von Blockchain-Technologien zum Beispiel durch Existenznachweise, Lizenzmanagement oder nachvollziehbare, verteilte Finanztransaktionen profitieren.

Insgesamt kann BC/DLT als eine Kommunikationsebene im Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0) integriert werden, um eine sicherere, dezentrale Datenkommunikation zu ermöglichen. Hierbei entstehen aber andere Herausforderungen wie Privacy (Öffentlichkeit der Daten) und Security (Manipulationssicherheit der Daten), Echtzeitfähigkeit und Latenzzeiten sowie Datenverfügbarkeit, die in Gänze gelöst werden müssen. Zwar gibt es einzelne BC/DLT, die jeweils Teilaspekte davon abdecken. Für industrielle Anwendungen kann es aber sinnvoll und erforderlich sein, eine eigene Technologie aus den marktverfügbaren Systemen abzuleiten. Blockchain selbst setzt hierbei auf einer über Security-Mechanismen abgesicherten Rechner- und Kommunikationsstruktur auf.

Zusammenfassend lässt sich somit feststellen, dass BC/DLT zwar noch eine sehr junge Technologiegruppe im Bereich der Digitalisierung ist, diese aber ein hohes Potenzial zur Automatisierung und Datenabsicherung im Zusammenhang mit Industrie-4.0-Anwendungsfällen und RAMI 4.0 aufweist. Um diese Technologie in marktverfügbare Lösungen zu überführen und letztendlich auch einen langfristigen Investitionsschutz zu gewährleisten, bedarf es der Zusammenarbeit von Herstellern von Industrie-4.0-Systemen, damit Aspekte wie Datenmigration, Interoperabilität und Standardisierung sichergestellt werden. Diese Zusammenarbeit bietet sich in weiteren Forschungsprojekten ebenso an wie auf Verbandsebene und in internationalen Standardisierungsgremien, um Blockchain- und Distributed-Ledger-Technologien in der Industrie-4.0-Welt industrietauglich verfügbar zu machen.

1 Einführung

1.1 Zusammenhang Industrie 4.0 und Blockchain / Distributed Ledger

Industrie 4.0 stellt in der Digitalisierungsstrategie der vergangenen und der aktuellen Bundesregierung eines der Kerngebiete dar. Dazu heißt es in der digitalen Agenda: *„Wir unterstützen die Zukunftsprojekte Industrie 4.0 und Smart Services der Hightech-Strategie, die zu einer ressortübergreifenden Innovationsstrategie weiterentwickelt werden soll.“* Gemäß Siepmann² (2016, S.19) ist Industrie 4.0 geprägt durch die neuen Möglichkeiten der sich ausweitenden und verbesserten Informations- und Kommunikationstechnologie wie das Internet der Dinge und Dienste (IoT) sowie der cyber-physischen Systeme (CPS). Laut einem Dokument des Wirtschaftsministeriums zur Weiterentwicklung des Interaktionsmodells für Industrie 4.0-Komponenten wird *„[...] zur gleichberechtigten Zusammenarbeit zwischen I4.0-Komponenten, bei der eine ergebnisoffene Verhandlung erforderlich ist, [...] eine protokollorientierte Interaktion benötigt.“* (BMWi, 11/2016, Kap.2.2)³

Im Vergleich zu traditionellen hierarchischen Kommunikations- und Steuerungsansätzen im Rahmen der Automatisierungspyramide⁴ steht also die Verhandlung einer optimalen Lösung zwischen mehreren gleichberechtigten Komponenten im Vordergrund. Der situativ optimale Prozesspfad zur Fertigung und Auslieferung kann durch eine zunehmende Dezentralität beispielsweise noch während des Produktionsablaufs durch ein Produkt oder eine Maschine selbst geändert werden.

Die darauf aufbauende Automatisierung umfasst sowohl aktive Software- als auch beschreibende Datenkomponenten. Während die Software heute in der Regel noch als fester Bestandteil einer Maschine und somit als vergleichsweise schwer manipulierbar angesehen wird, bieten öffentlich ausgetauschte Daten im Vergleich dazu ein hohes Angriffspotenzial, um Automatisierungsabläufe versehentlich oder bewusst zu beeinflussen⁵. Dieses wird durch Security-Mechanismen in einen beherrschbaren Bereich gebracht und mit „Security by Design“ z. B. in Industrie 4.0 als Fähigkeit mit integriert.

Aufgrund der mittlerweile weltweit ausgeprägten Vernetzung über das Internet ist auch unabhängig von Industrie 4.0 ein deutlicher Trend des offenen Informationsaustauschs und der darauf aufbauenden Automatisierung festzustellen. Um die Datenintegrität ohne Intermediäre als Vertrauensbasis sicherzustellen bzw. eine Datenmanipulation transparent zu gestalten, werden hier zunehmend Blockchain- und Distributed-Ledger-Technologien (BC/DLT) eingesetzt.

Für BC/DLT ist dabei deutlich zwischen deren Anwendung und dem zugrundeliegenden Protokoll zu unterscheiden. Zum System selbst heißt es zusammenfassend in unterschiedlicher Literatur: *Die Blockchain- und Distributed-Ledger-Technologie (BC/DLT) stellt ein schwer manipulierbares Softwaresystem dar, das auf verteilter, gleichberechtigter und konsensbasierter verketteter Datenhaltung beruht* (vgl. UK, 2016⁶; Swan, 2015⁷; Tschorsch/Scheuer, 2016⁸). Daraus ergeben sich dann entsprechend bevorzugte Anwendungsgebiete wie Finanztransaktionen oder Behördendienste, die eines besonderen Vertrauens bedürfen.

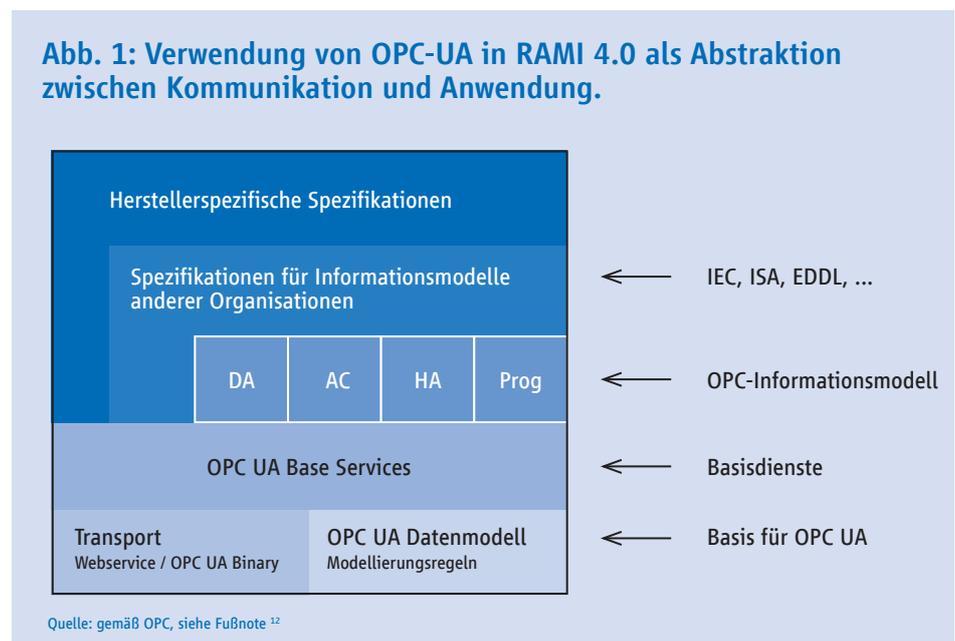
Die Ursprünge von BC/DLT liegen aber nicht in Transaktionen von digitalen Währungen, wie in Nakamoto (2008⁹) für ein Protokoll beschrieben, das als Bitcoin bezeichnet wurde. Vielmehr beziehen sich auch deren Entwickler auf schon länger in der Informatik bekannte Verfahren des Verkettens und

- 01 Presse- und Informationsdienst der Bundesregierung: Kabinettsklausur in Meseberg: Digitalisierung gemeinsam vorantreiben. <https://www.bundesregierung.de/breg-de/aktuelles/digitalisierung-gemeinsam-vorantreiben-411484> (2018), abgerufen am 6.11.2018.
- 02 Siepmann, D.: Struktur und Historie. In: Roth, A.: Einführung und Umsetzung von Industrie 4.0: Grundlagen, Vorgehensmodell und Use Cases aus der Praxis. Springer/Gabler: Berlin/Heidelberg, 2016.
- 03 Bundesministerium für Wirtschaft und Energie (Hrsg.): Weiterentwicklung des Interaktionsmodells für Industrie 4.0-Komponenten, (2016).
- 04 Linke P. (2015) Grundlagen zur Automatisierung. In: Grundlagen Automatisierung. Springer Vieweg, Wiesbaden
- 05 Stuxnet-Virus als Beispiel eines externen, dezentralen Angriffs auf industrielle Anlagen: <https://thehackernews.com/2011/07/stuxnet-source-code-released-online.html> (2018). Abgerufen am 2.11.2018. 06 Government Office for Science - UK Government ed: Distributed ledger technology: beyond block chain, <https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain> (2016).
- 07 Swan, M.: Blockchain: blueprint for a new economy. O'Reilly, Beijing : Sebastopol, CA (2015).
- 08 Tschorsch, F., Scheuermann, B.: Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Communications Surveys Tutorials. 18, 2084–2123 (2016).
- 09 Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. (2008).

Verteilens, um öffentlich zugängliche Informationen abzusichern. Wichtige Publikationen beschreiben beispielsweise das zeitliche Signieren eines digitalen Dokuments (Haber/Stornetta, 1991¹⁰) oder das Absichern von Protokolldateien auf nichtvertrauenswürdigen Systemen (Schneider/Kelsey, 1997¹¹). Abstrakt betrachtet, stellen BC/DLT-Verfahren also eine Möglichkeit dar, wie Transaktionspartner untereinander versandte Daten absichern können.

Genau hier entstehen die Parallelen zu Industrie-4.0-Anwendungen: Insbesondere die dezentralen, verteilten Systeme, die im Fertigungskontext auf der Shopfloor-Ebene eingesetzt werden, steuern sich untereinander, indem sie entsprechende Datenpakete austauschen. Für I4.0-Anwendungen bieten Blockchain-analoge Kommunikationsprotokolle, die auf der Basis des Verkettens und Verteilens ablaufen, ein besonderes Potenzial, weil sie in das RAMI 4.0 integriert werden können. Darauf aufbauend, erfolgt dann der weitere, semantische Datenaustausch über die Open Protocol Communication – Unified Architecture (OPC-UA)^{12,13}, (siehe Abb. 1).

Abb. 1: Verwendung von OPC-UA in RAMI 4.0 als Abstraktion zwischen Kommunikation und Anwendung.



OPC-UA selbst ist hinsichtlich des Kommunikationsmediums generisch gehalten und lässt beispielsweise auch die TCP/IP-Kommunikation über Web-Services zu. Ohne weitere Protokollschichten können aber genau hier potenzielle Probleme durch die Asynchronität der Kommunikation entstehen: Während bei einer unmittelbaren TCP/IP-Kommunikation davon ausgegangen wird, dass Sende- und Empfangsknoten unmittelbar synchronisiert kommunizieren, kann dies in einer sehr heterogenen und stark verteilten Systemumgebung mit teilweise im Schlafzustand befindlichen Sensorknoten nicht erwartet werden (vgl. beispielsweise Karl/Willig, 2005, Kap.1.4-1.6¹⁵; Obaidat/Misra, 2014, Kap. 2.1-2.2¹⁶).

Hier können dann Blockchain-Verfahren genutzt werden, um trotz der Asynchronität eine gesicherte Datenkommunikation zwischen Transaktionssendern und -empfängern ohne hierarchische Systemarchitektur oder zentrale Intermediäre protokollbasiert zu ermöglichen.

10 Haber, S., Stornetta, W.: How to time-stamp a digital document. Journal of Cryptology, Vol. 3, No. 2, pp. 99-111, (1991).

11 Schneider, B., Kelsey, J.: Cryptographic Support for Secure Logs on Untrusted Machines. In: Proceedings of the 7th USENIX Security Symposium. , San Antonio, Texas, USA (1997).

12 OPC Foundation (Hrsg.): OPC Unified Architecture – Interoperability for Industrie 4.0 and the Internet of Things, <https://opcfoundation.org/wp-content/uploads/2017/11/OPC-UA-Interoperability-For-Industrie4-and-IoT-EN.pdf>, (2017).

13 OPC Foundation (Hrsg.): OPC Unified Architecture: Wegbereiter der 4. industriellen (R)Evolution, https://opcfoundation.org/wp-content/uploads/2014/03/OPC-UA_I_4.0_Wegbereiter_DE_v2.pdf.

14 Gerhard Gappmeier: OPC-UA-Architektur, https://de.wikipedia.org/wiki/Datei:UA_Architecture_1024.png, CC BY-SA 3.0 (2006).

15 Karl, H., Willig, A.: Protocols and architectures for wireless sensor networks. (2005).

16 Obaidat, M.S., Misra, S.: Principles of wireless sensor networks. Cambridge University Press, Cambridge, United Kingdom ; New York (2014).

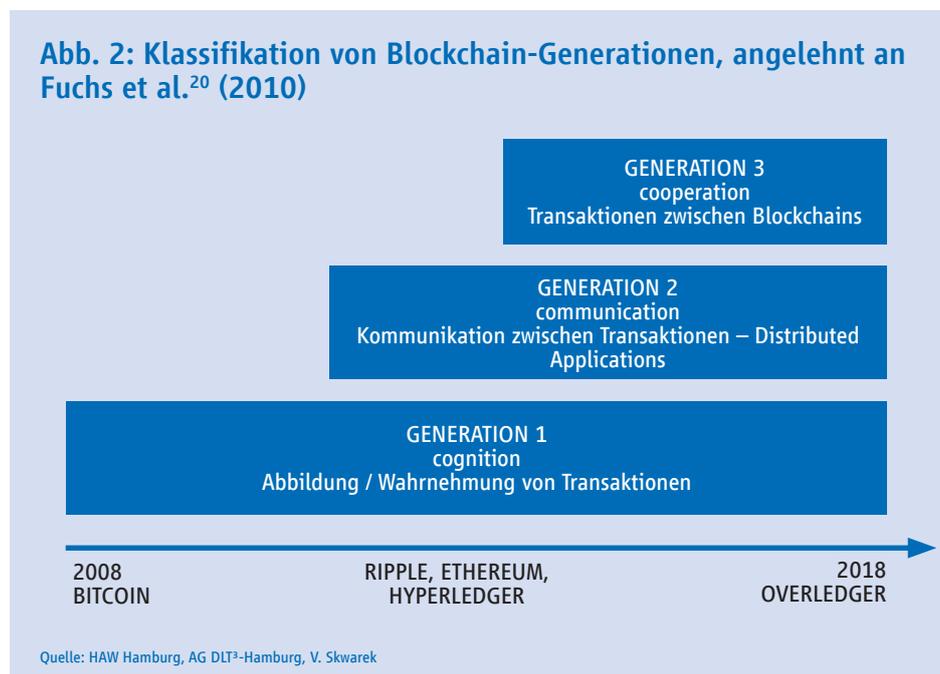
1.2 Überblick über Potenziale von BC/DLT

Unterschiedliche Generationen von Blockchains ermöglichen über die oben genannten Transaktionen hinaus weiterführende Anwendungen (s. Abb. 2):

Das Ursprungsprotokoll nach Nakamoto, das in Bitcoin zum Einsatz kommt, sah zunächst nur geringe und sehr auf digitale Währungen zweckgebundene Transaktionsumfänge vor. Neben einigen Protokolldaten sind dies im Wesentlichen die Absenderadresse, die Empfängeradresse, das Transaktionsvolumen, öffentliche kryptografische Schlüssel und Signaturen (Antonopoulos 2015), S. 44ff.).¹⁷

Folgenerationen ermöglichen es, beispielsweise mit sogenannten *colored coins* (Swan 2015, S. 16)^{18 19} Transaktionen *farblich* zu markieren. Konkret bedeutet dies, dass beispielsweise in einem Klarfeld eine Klassifikation der Transaktion hinterlegt werden kann, um diese somit einem bestimmten Zweck oder einer Kategorie zuzuordnen.

Abb. 2: Klassifikation von Blockchain-Generationen, angelehnt an Fuchs et al.²⁰ (2010)



Den aktuellen im operativen Einsatz befindlichen Stand der Technik stellen Blockchains dar, die darüber hinaus in der Lage sind, nicht nur Transaktionen zu speichern und zu verteilen, sondern auch in gleicher Art Softwarecode unter den Teilnehmern zu verteilen und auszuführen.

In Anlehnung an Szabo, der in einem anderen informationstechnischen Kontext versucht hat, in dieser Form Vertragsklauseln zu automatisieren, wird dieser innerhalb der Blockchain beliebig oft verteilte und ausgeführte Code *smart contract*²¹ genannt, ohne damit zwingend Verträge im juristischen Sinne beschreiben zu wollen. Bekannte Blockchains, die über eine Smart-Contract-Funktionalität verfügen, sind beispielsweise Ethereum, Hyperledger oder Ripple.

Hieraus entsteht insbesondere für I4.0-Anwendungen das Potenzial, dass Transaktionen zwischen zwei Systemen automatisch weitere Transaktionen²² auslösen können, indem diese weitere Smart Contracts aktivieren. Im Gegensatz zu herkömmlichen Softwaresystemen erfolgt dies aber potenzi-

17 Antonopoulos, A.M.: Mastering bitcoin. O'Reilly, Sebastopol CA (2015).

18 Swan, M.: Blockchain: blueprint for a new economy. O'Reilly, Beijing : Sebastopol, CA (2015).

19 <http://coloredcoins.org/>, abgerufen am 8.2.2018.

20 Fuchs, C. et. al.: Theoretical Foundations of the Web: Cognition, Communication, and Co-Operation. Towards an Understanding of Web 1.0, 2.0, 3.0. Future Internet. 2, 41–59 (2010).

21 N. Szabo, „The Idea of Smart Contracts“, 1997. [Online]. Verfügbar unter: <https://perma.cc/V6AZ-7V8W>, (abgerufen am: 12.4.-2017).

22 K. Christidis und M. Devetsikiotis, „Blockchains and Smart Contracts for the Internet of Things“, IEEE Access, Bd. 4, S. 2292–2303, 2016.

ell vollständig asynchron, da die Kommunikation nicht zwingend durch synchrone Systemaufrufe, sondern auch nachrichtenbasiert über die Blockchain erfolgen kann. Beispielsweise führt die Anforderung eines Materialtransports dazu, dass eine solche Anwendung über einen Smart Contract aus dem Lagermanagementsystem ausgebucht werden kann, ohne dass das Transportfahrzeug oder die anfordernde Einheit dies zu übernehmen braucht. Letztlich befinden sich gerade auch weitere Systeme – sogenannte Metachains²³ – in der Entwicklung, die Transaktionen zwischen mehreren Blockchains ausführen.

1.3 Aufbau und Ziel der Studie

Das Ziel dieser Studie besteht darin, die Möglichkeit des Einsatzes von Blockchains im Kontext von I4.0 und bestehenden Bausteinen wie beispielsweise RAMI oder OPC-UA in der Automation zu untersuchen, darzustellen und kritisch zu diskutieren. Dazu werden zunächst in Kapitel 2 die technischen Abläufe und Begriffe innerhalb des Blockchain- und Distributed-Ledger-Kontexts erläutert, bevor sie in Kapitel 3 in Archetypen unterteilt und an Industrie-4.0-Anwendungsfällen der Plattform Industrie 4.0^{24, 25} gespiegelt werden. Aus dieser Betrachtung ergeben sich dann prädestinierte Anwendungsfälle für den Einsatz von BC/DLT im I4.0-Umfeld.

In Kapitel 4 werden daraus Handlungs- und Gestaltungsoptionen herausgearbeitet sowie Vor- und Nachteile diskutiert. Die Studie wird in Kapitel 5 mit einer Zusammenfassung und einem Ausblick abgeschlossen.

23 Quant Network Ltd.: Overledger. <https://www.quant.network/>, abgerufen am 8.2.2018.

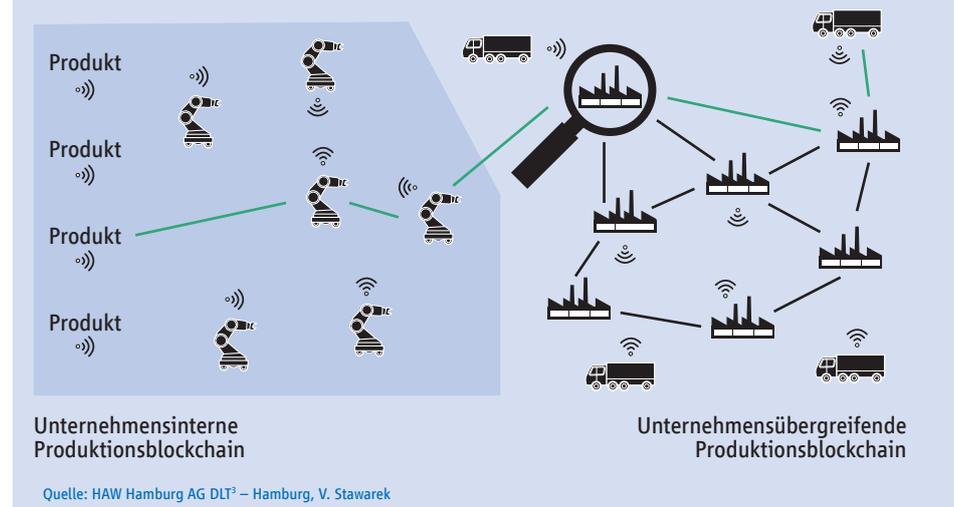
24 Plattform Industrie 4.0: Anwendungsszenario trifft Praxis: Auftragsgesteuerte Produktion eines individuellen Fahrradlenkers, https://www.bmwi.de/Redaktion/DE/Publikationen/Industrie/anwendungsszenario-trifft-praxis.pdf?__blob=publicationFile&v=6, (2017).

25 Plattform Industrie 4.0: Fortschreibung der Anwendungsszenarien der Plattform Industrie 4.0, http://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/fortschreibung-anwendungsszenarien.pdf?__blob=publicationFile&v=7, (2016)

2. Die Blockchain-Technologie

Im folgenden Kapitel wird zunächst grundlegende Terminologie im Blockchain-Kontext mit Bezug zu Industrie 4.0 anhand des konkreten Beispiels der auftragsgesteuerten Produktion (siehe Abb. 3) eingeführt, bevor ein Überblick über den technologischen Hintergrund der Blockchain-Technologie gegeben wird. Schließlich wird das Blockchain-Protokoll in Basisbausteine aufgeschlüsselt, aus denen dann im Folgekapitel mögliche I4.0-Realisierungen für verschiedene Anwendungsszenarien hergeleitet werden.

Abb. 3: Beispiel einer auftragsgesteuerten Produktion unter Verwendung mehrerer unabhängiger Blockchains.



2.1 Blockchain am Beispiel Industrie 4.0

Als Basis für die folgende Erläuterung des Ablaufs und eines möglichen Anwendungsszenarios von BC/DLT wird das Beispiel des kundenindividuellen Fahrradlenkers²⁶ von der Plattform Industrie 4.0 herangezogen. Dabei handelt es sich um einen Anwendungsfall, bei dem ein Fertigungssystem vollautomatisiert Aufträge an Zulieferer erteilt, um Aufträge effizient abzuwickeln. Das im Ergebnis-papier beschriebene Szenario wird dabei auf die Nutzung der Blockchain-Technologie angepasst.

Das Beispiel gliedert den Fertigungsprozess des individuellen Fahrradlenkers in fünf Schritte, an denen drei Parteien – Fahrradhersteller, Zulieferer, Vermittlungsdienst – beteiligt sind:

- Produktkonfiguration,
- Ausschreibung,
- Lieferantenauswahl,
- Auftragsvergabe,
- Abschließende Fertigung.

Ein wesentlicher Vorteil durch Einsatz der Blockchain-Technologie bestünde in diesem FGall darin, dass auf einen zentralen Vermittler verzichtet werden kann. Im Folgenden werden die fünf Schritte des Anwendungsszenarios und nötige Anpassungen bei Nutzung der Blockchain-Technologie behandelt.

²⁶ https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/anwendungsszenario0-trifft-praxis.pdf?__blob=publicationFile&v=12

Schritt 1: Auftragskonfiguration

Bei der Konfiguration wird dem Endkunden die Möglichkeit gegeben, das entsprechende Produkt, hier den Fahrradlenker, nach eigenen Wünschen zu individualisieren. Hierzu werden, je nach Aufbau des Konfigurators und abhängig vom Produkt, zahlreiche Typ- und Konfigurationsinformationen wie Struktur, Konstruktion und mechanische Festigkeit erfasst. Dieser vom Konfigurator erzeugte Datensatz bildet nun die Grundlage für den gesamten weiteren Prozess bis hin zum Abschluss des Auftrags. Der Datensatz wird einem Kunden dabei als unveränderlich zugeordnet. In der Terminologie von BC/ DLT handelt es sich hierbei um die Transaktion, die unveränderlich auf der Blockchain abgelegt wird. Gleichmaßen könnten sich auch Fertigungsinformationen im Sinne von Konfigurationsdaten der Produktionsanlagen als Teil der Verwaltungsschale auf einer Blockchain befinden. Hierbei wird nicht näher unterschieden, ob sich die eigentlichen Nutzdaten auf der Blockchain befinden (On-chain-Datenhaltung) oder auf einem separaten externen System abgelegt sind (Off-chain-Datenhaltung) und auf der Blockchain nur registriert und beispielsweise über Hashwerte eindeutig abgesichert werden. Diese Entscheidung hängt beispielsweise von der Größe der Datensätze sowie deren Vertraulichkeit ab.

Wie auch im Ausgangsszenario muss bei der Erzeugung des Grunddatensatzes im Wesentlichen darauf geachtet werden, dass dieser ohne weitere manuelle Bearbeitung von allen weiteren beteiligten Systemen im Lebenszyklus interpretiert werden kann, um eine korrekte Abarbeitung des Auftrags ohne manuelles Eingreifen zu ermöglichen. Bei einer solchen automatisierten Ausführung kommen auf Blockchains oft verteilte Anwendungen zum Einsatz, die auch je nach System unterschiedlich – zum Beispiel als Chaincode in Hyperledger oder als Smart Contract in Ethereum – bezeichnet werden.

Schritt 2: Ausschreibung

Der nächste Schritt im Lebenszyklus des Produkts ist der Ausschreibungsprozess, um einen geeigneten Zulieferer auszuwählen. Hierbei wird vom Auftragsverwaltungssystem zunächst der Datensatz um weitere Informationen für die Lieferantenauswahl ergänzt, was beispielsweise wiederum automatisiert durch Smart Contracts erfolgen kann. Dieser Datensatz wird dabei von allen Netzwerkknoten, die gemäß ihrer Rollendefinition in einer Blockchain neue Blöcke bilden oder verifizieren dürfen (sogenannte Miner), zugleich und in identischer Form ausgeführt. Die Ergebnisse werden dann, sofern sie widerspruchsfrei sind, wieder wie eine Transaktion auf der Blockchain abgelegt.

In diesem Fall besteht der Vorteil der Verwendung einer Blockchain darin, dass ohne einen weiteren Vermittler (Intermediär) die Daten allen beteiligten Lieferanten zugänglich gemacht werden können. Je nach Blockchain-Typ besteht sogar die Möglichkeit, individuelle Sichtbarkeit oder Zugriffsrollen zu definieren.

In einem weiteren theoretischen Szenario, das wieder durch Smart Contracts realisiert würde, können Zulieferer nun vollautomatisiert auf eine eingehende Ausschreibung reagieren und im Falle erfüllter Voraussetzungen ein Angebot generieren. Es könnte somit eine verteilte Handelsplattform ohne zentralen Intermediär bei vollem Manipulationsschutz und Vertrauen generiert werden.

Schritte 3 und 4: Auswahl des Lieferanten und Auftragsvergabe

Auch die Auswahl des Lieferanten kann nun vollautomatisiert geschehen: Alle eingegangenen Angebote werden durch einen auf den Minern ausgeführten Smart Contract verglichen und das beste Angebot wird ausgewählt. Der entscheidende Unterschied zum Szenario ohne Blockchain ist wieder das Entfallen des Vermittlungsdiensts zur Überprüfung von eingehenden Angeboten. Dabei werden dem Lieferanten alle zur Erfüllung des Auftrags benötigten Daten durch eine weitere automatisch erzeugte Transaktion zugänglich gemacht.

Schritt 5: Fertigung

Schließlich wird der im ersten Schritt konfigurierte Fahrradlenker vom Lieferanten gefertigt. Hierbei stellt die Blockchain und ihre öffentliche Einsehbarkeit die Möglichkeit zur Überwachung des Fertigungsprozesses bereit. Dabei kann natürlich die Öffentlichkeit der Datenhaltung in unterschiedlicher Weise eingeschränkt werden, beispielsweise durch die Wahl des Systems, durch die Zugangsbeschränkungen des Netzwerks oder durch eine klare Differenzierung zwischen On- und Off-chain-Datenhaltung.

In einer beispielsweise sicherheitskritischen Fertigung könnten dann auch einzelne Produktionsschritte auf einer Fertigungsblokchain unveränderlich und transparent abgelegt werden. Schließlich kann als letzter Schritt der Fertigung automatisch der Transport zum Kunden via Smart Contract initialisiert werden und der Zyklus der auftragsgesteuerten Produktion ist damit abgeschlossen. Dieses Beispiel skizziert ein Anwendungsszenario aus dem Umfeld von Industrie 4.0, in dem die Anwendung der Blockchain-Technologie zu einer Vereinfachung des Prozesses durch Reduktion von Intermediären bei gleichzeitiger Beibehaltung von Transparenz und Sicherheit führt.

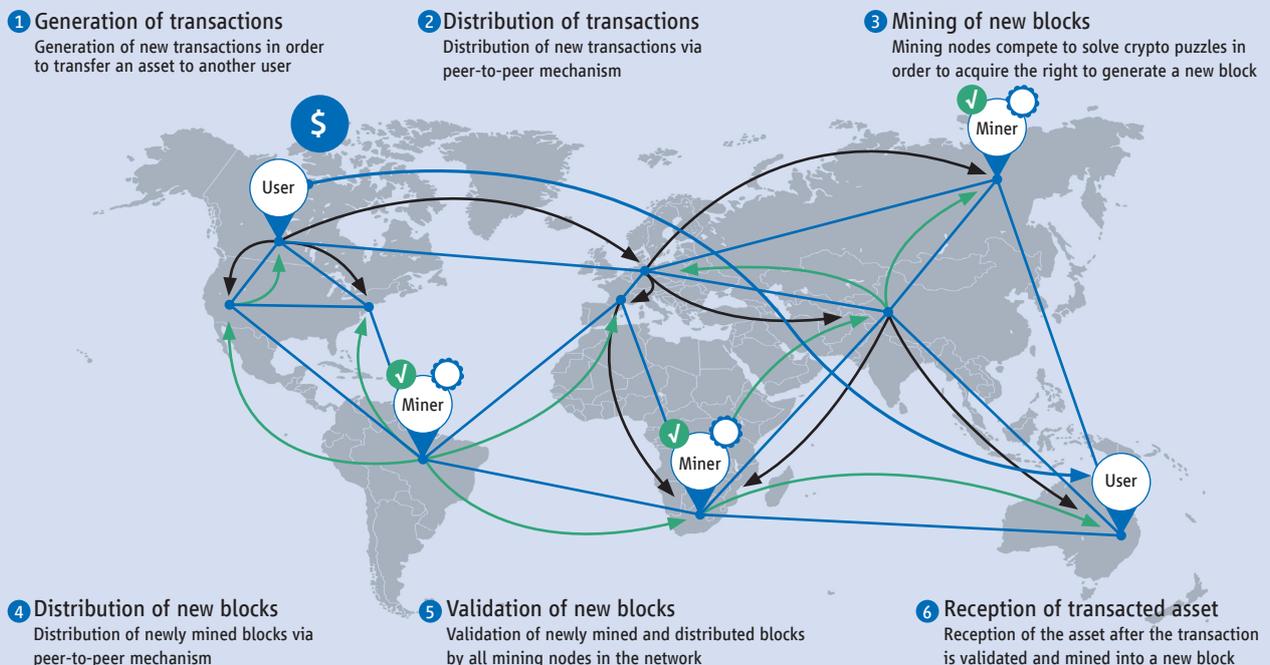
2.2 Die Blockchain-Technologie

Die im vorhergehenden Beispiel abstrakt vorgestellte Blockchain- und Distributed-Ledger-Technologie wird im folgenden Abschnitt inhaltlich näher erläutert. Den ersten Einsatz fanden BC/DLT, wie bereits in Kapitel 1 erwähnt, ursprünglich durch Bitcoin im Bereich der Kryptowährungen. Hier liegen Anforderungen wie Sicherheit, Vertrauen und Reduktion von Intermediären nahe. Diese lassen sich aber auch auf ein industrielles Umfeld übertragen. Dazu wird im Folgenden die Technologie mit Bezug auf das Einführungsbeispiel in ihre Bestandteile aufgeschlüsselt, aus denen sich schließlich Realisierungen für verschiedene Anwendungsbeispiele ableiten lassen.

2.2.1 Technologischer Hintergrund

Aus technologischer Sicht handelt es sich bei einer Blockchain schlicht um eine verteilte Datenstruktur in Form einer verketteten Liste. Zusätzlich wird über kryptografische Methoden sichergestellt, dass Einträge nachträglich nur mit erheblichem Aufwand manipuliert werden können. Der Ablauf einer Transaktion von der Erzeugung über die Verifikation bis zu ihrer Ablage auf der Blockchain sowie ihrer Verteilung und Weiterverwendung wird im folgenden Text und anhand der Illustration in Abbildung 4 näher erläutert.

Abb. 4: Exemplarischer Ablauf von Blockchain-Transaktionen.



Quelle: Lehrstuhl für Informatik III der Universität Würzburg

Den Ursprung dieses Prozesses bildet eine Transaktion, die in der Blockchain-Terminologie einen Token verschiebt. Ein Token kann hier analog zu einem Asset im I4.0-Kontext verstanden werden. Dabei wird von der sendenden Partei ein Datensatz erzeugt, der neben den Nutzdaten auch Verwaltungsdaten wie Absender oder Zieladresse enthält. Dieser wird anschließend über das Blockchain-Netzwerk an alle im Netz angemeldeten Stationen (Knoten) verteilt. Im Anschluss wird die nun im Netz bekannte Transaktion durch Mining-Knoten prozessiert, deren Aufgabe darin besteht, Transaktionen zu bündeln, zu verifizieren und neue Blöcke zu bilden. Erst nachdem ein solcher neuer Block im Netz verteilt und durch diese Miner ebenfalls validiert wurde, zählt die Transaktion als abgeschlossen. Da in einem weit verteilten Netzwerk theoretisch mehrere solcher Blöcke unabhängig voneinander entstehen können, muss im Folgenden noch beobachtet werden, welche dieser Blockchains sich am schnellsten weiterentwickelt. Erst nach einer solchen Wartezeit kann davon ausgegangen werden, dass die längste Blockchain von der Majorität der Miner akzeptiert wurde und die darin befindlichen Transaktionen wirklich gültig sind.

Im Folgenden werden die einzelnen Bestandteile des Transaktionsprozesses anhand der „fünf Ws der Blockchain“ genauer beschrieben und in Tabelle 1 zusammengefasst.

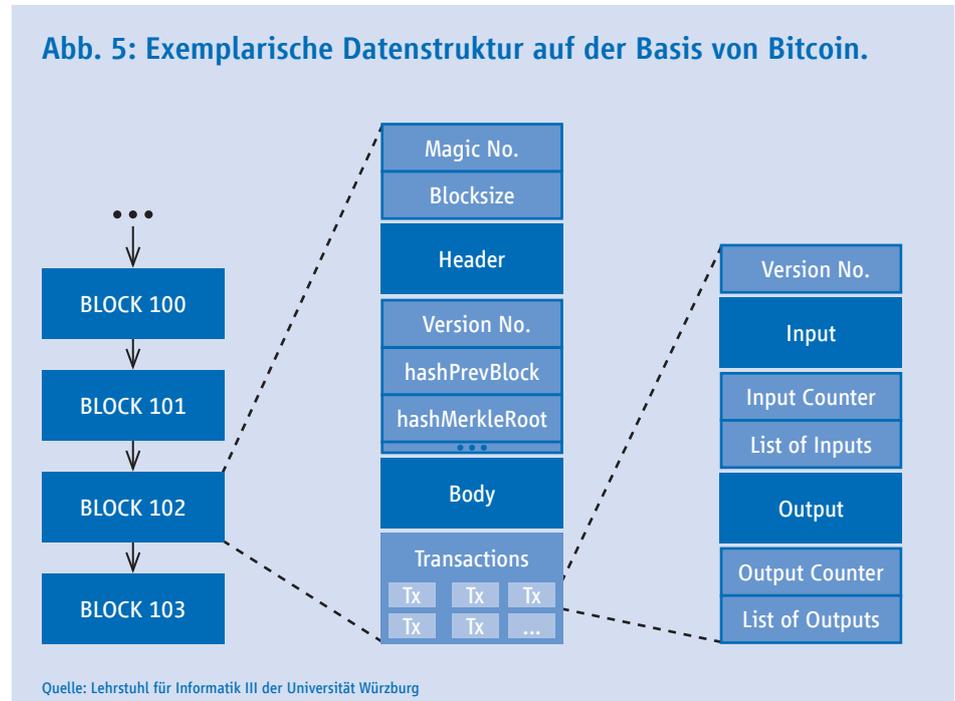
Tab. 1: 5-W-Analyse zur Bestimmung der Bestandteile einer Blockchain.

Frage	Funktion	Beschreibung	Umsetzung in Blockchains
Was	Datenstruktur	Bestimmt Blockstruktur und damit, welche Daten in der Blockchain gespeichert werden können	Transaktionen
Wer	Zugriffskontrolle	Reguliert den schreibenden Zugriff auf die verteilte Datenstruktur	Rollenverteilung wie Nodes und Miner
Wann	Validierung	Legt fest, ab wann Daten als valide angesehen werden	Eintragung in einen Block durch einen Mining-Knoten über einen Proof-of-X-Mechanismus
Wie	Konfliktlösung	Beschreibt den Mechanismus zur Konfliktauflösung im Fall asynchroner Zustände im System	Probabilistischer Konsens durch Übernehmen der längsten Kette
Wo	Verarbeitungsmechanismus	Ort der Ablage von Nutzdaten	On-chain- und Off-chain-Verarbeitung

Quelle: ZVEI, eigene Darstellung

Datenstruktur der Blockchain

Die Frage nach der Datenstruktur auf einer Blockchain lässt sich nicht pauschal beantworten, da es technologisch gesehen auch nicht „die Blockchain“ gibt. Aber aufbauend auf Bitcoin, hat sich eine prinzipielle Grundstruktur entwickelt (s. Abb. 5):



Die Datenstruktur lässt sich dabei in drei Bestandteile gliedern. Zunächst die Blockchain als Ganzes, die auf der linken Seite der Abbildung dargestellt ist und sich aus der Verkettung von einzelnen Blöcken ergibt. Die Pfeile zwischen den Blöcken repräsentieren dabei eine Verkettung, indem über jeweils einen Block (zum Beispiel Block 100) eine Prüfsumme berechnet wird (Hashwert) und diese dann im Folgeblock (zum Beispiel Block 101) abgelegt wird.

Der detaillierte interne Aufbau der einzelnen Blöcke ist dabei der zweite Bestandteil der Datenstruktur. Diese bestehen aus einem Header mit Metainformationen, wie zum Beispiel Zeitstempel, Versionsnummer und der Referenz zum Vorgänger-Block, und einem Body, der die eigentlichen Transaktionen beinhaltet.

Diese Transaktionen bilden den dritten und letzten Bestandteil der Blockchain-Datenstruktur und legen fest, welcher Typ von Daten in der Blockchain gespeichert werden kann. Im Allgemeinen werden in einer Blockchain Transaktionen dokumentiert, die einen Wert zwischen beteiligten Parteien transferieren. Der genaue Inhalt der Transaktionen ist hierbei stark vom jeweiligen Anwendungsfall abhängig, besteht in der Regel allerdings aus einem Absender, einem Empfänger und einem beliebigen Asset. Auch hierin unterscheiden sich Blockchain-Implementierungen, indem beispielsweise größere Datenmengen oder Transaktionen gar nicht auf der Blockchain abgebildet werden, sondern wiederum nur deren Hashwert, und die eigentliche Transaktion parallel auf Datenbanken gehalten wird.

Zugriffsberechtigung und Rollenverteilung

Die Zugriffskontrolle sowie die Rollenverteilung sind die entscheidenden Differenzierungsmerkmale zwischen unterschiedlichen Blockchain-Typen und sollen hier nicht extensiv diskutiert werden. Grundsätzlich wird auf Basis des Orts der Datenhaltung sowie der Verteilung bzw. der Zentralisierung der Bildung neuer Blöcke zwischen öffentlichen und privaten Blockchains unterschieden. Öffentliche sind in der Regel voll transparent und nicht zugangslimitiert, verfügen aber über den höchsten Vertrauensmechanismus. Private hingegen sind oft teilnehmerlimitiert, tragen sensiblere Daten bei einem höheren Vertrauen der Teilnehmer untereinander, wodurch weniger komplexe Vertrauensmechanismen erforderlich sind. Eine Zwischenstufe stellen die sogenannten konsortialen oder permissioned Blockchains dar, bei denen die Daten nicht vollständig transparent gehalten werden bzw. eine gewisse Zugriffsbeschränkung besteht. Allgemeine Rollen sind üblicherweise der Knoten selbst, der eine Transaktion auslösen und verwalten kann, und der Miner, der Transaktionen verifiziert, neue Blöcke erstellt und die Blockchain erweitert.

Transaktionsvalidierung

Bei der Validierung von Transaktionen müssen in zwei Schritten folgende Fragen beantwortet werden: Ist die Transaktion selbst gültig – wurde sie also von der korrekten Adresse mit dem korrekten Kontext ausgeführt und nicht zweimal verwendet (double spending)? Und: Wurde sie korrekt in die Blockchain eingefügt?

Der erste Schritt, also die Transaktionsvalidierung selbst, wird je nach Blockchain vom Knoten selbst bzw. einem Miner übernommen. So wird eine ungültige Transaktion entweder gar nicht in die Blockchain aufgenommen oder nicht prozessiert. Der zweite Schritt hingegen, also das Erzeugen eines gültigen Blocks selbst, wird durch Miner übernommen. In einem voll transparenten System mit hohem Vertrauensschutz darf dabei nicht von vornherein feststehen, welcher Miner den nächsten Block erstellen darf, denn hier könnte über Absprachen unter den Minern manipuliert werden.

Dafür werden Proof-of-X-Algorithmen eingesetzt, die den nächsten Miner über ein Konsensverfahren festlegen. Das bekannteste Verfahren zum Beispiel ist das im Bitcoin eingesetzte Proof-of-Work, bei dem eine Zufallszahl geraten werden muss, die den Hashwert des Blocks mit einer zuvor definierten Zahl von führenden Nullen versieht. Der Miner, der als erstes eine solche Zufallszahl geraten hat, ist zur Erstellung des Blocks per Bitcoin-Algorithmus legitimiert. Da insbesondere dieses Proof-of-Work-Verfahren äußerst energieaufwendig ist, existiert auch eine sehr hohe Anzahl anderer Verfahren²⁷, wie beispielsweise Proof-of-Stake, Proof-of-Authority, Proof-of-elapsed-Time und viele mehr, die auch allgemein unter Proof-of-X zusammengefasst werden.

Konfliktlösung bei widersprüchlichen Blockchains

Da Blöcke parallel berechnet werden und diese Berechnungen in einer erheblichen räumlichen Verteilung erfolgen können, besteht auch das Potenzial, dass beispielsweise durch die Latenzzeit unterschiedliche Blockchains parallel gebildet werden. Da eine Transaktion aber nur einmal verwendet werden darf, würde dies zu Widersprüchen führen. Abgesehen von diesen topologischen Einflüssen wäre es natürlich auch möglich, dass ein Miner zu seinem eigenen Vorteil bewusst fehlerhafte Blöcke erstellt.

In üblichen öffentlichen Blockchains mit verteilten Konsensmechanismen werden solche Konflikte derart gelöst, dass ein Miner nur dann incentiviert wird, wenn er als erstes einen Block berechnet und dies über die Verwendung des Blocks durch alle anderen Netzwerkteilnehmer akzeptiert wird. Diese Akzeptanz drückt sich aber in der Länge der Blockchain aus: Je mehr Miner einen Block verwenden, umso mehr Miner berechnen den nächsten Block und umso höher ist die Wahrscheinlichkeit, dass der nächste Block schnell gefunden wird. Bei höherer Geschwindigkeit entwickelt sich so aber die längere Chain. Damit kann ein Miner aber nur dauerhaft für seine erfolgreiche Rechenleistung belohnt werden, wenn dessen Block an die längste Chain angefügt wird. Erfolgt dies nicht, besteht das Risiko, dass eine sogenannte Sidechain wieder verworfen wird und das Incentive des Miners wieder verfällt. Somit werden Konflikte über einfache Anreizmechanismen gelöst, indem fehlerhafte oder widersprüchliche Blöcke oder Zweige sich nicht weiterentwickeln und gegebenenfalls verworfen werden.

²⁷ <https://adriancolyer.files.wordpress.com/2018/02/blockchain-consensus-overview.jpeg> (abgerufen am 2.11.2018)

Ort der Datenhaltung

Schließlich stellt sich im Blockchain-Kontext die Frage, wo die Nutz- und die Overheaddaten gehalten und verarbeitet werden. Als verteilte Datenstruktur bietet die Blockchain per Definition die Möglichkeit, Daten verteilt und direkt innerhalb der Blockchain selbst zu speichern. Dies ist hauptsächlich für leichtgewichtige Anwendungsfälle relevant, aus denen geringe Datenmengen resultieren. Hierbei werden, wie im Beispiel der Asset-Transaktion, die Daten direkt innerhalb der Blöcke gespeichert und auch direkt innerhalb der Blockchain bzw. auf den Mining-Knoten verarbeitet. Man spricht auch von On-chain-Datenverarbeitung.

Für komplexere Use Cases bietet sich die sogenannte Off-chain-Datenverarbeitung an, bei der Daten abseits der Blockchain gehalten und auch verarbeitet werden. Dabei werden Transaktionen oder auch komplexere Berechnungen und Verarbeitungsaufgaben abseits der Blockchain durchgeführt, und es wird meist lediglich ein Repräsentant des Werts, wie beispielsweise dessen Hash, auf der Chain als Referenz abgelegt. Hierbei ist zu beachten, dass abseits der Blockchain durchgeführte Datenverarbeitungsaufgaben auch separat abgesichert werden müssen. Die vollen Sicherungsmechanismen der Blockchain greifen hier also nicht.

2.2.2 Weiterentwicklungen und Anwendungen der Blockchain-Technologie

Neben der oben beschriebenen Blockchain-Basistechnologie haben sich seit ihrer ursprünglichen Veröffentlichung im Jahr 2008 zahlreiche Weiterentwicklungen und Anwendungsfälle abseits des Gebiets der Finanztransaktion ergeben, über die im Folgenden ein kurzer Überblick gegeben werden wird. Zunächst existieren neben der ursprünglichen Kryptowährung Bitcoin etwa 1.500 weitere Kryptowährungen. Eine große Mehrheit basiert dabei auf der klassischen Blockchain-Technologie, wie oben beschrieben. Einige Vertreter verfolgen jedoch auch andere Mechanismen oder bedienen sich Weiterentwicklungen der Blockchain-Technologie. So, zum Beispiel das Verfahren nach IOTA²⁸, das von Größe, Kosten und Geschwindigkeit her für Minimaltransaktionen zwischen Geräten des Internet-of-Things konzipiert ist. Hierbei wird ein gerichteter azyklischer Graph, genannt Tangle, anstelle der für Blockchain üblichen verketteten Liste als verteilte Datenstruktur verwendet. Diese Änderung bezüglich der Datenstruktur hat mitunter gravierende Unterschiede bezüglich Zugriffskontrolle und Transaktionsvalidierung zur Folge. So existiert hier kein Miningprozess, wie ihn die klassische Blockchain aufweist. Transaktionen werden hierbei, anstatt in Blöcken aggregiert zu werden, direkt in den Graphen integriert. Als Zugriffskontrollmechanismus kommt hierbei die Validierung von zwei bereits im Graphen vorhandenen Transaktionen zum Einsatz. Auf die genauen Implikationen, die das für Sicherheit, Unveränderbarkeit und Effizienz der Datenstruktur hat, wird an dieser Stelle nicht weiter eingegangen.

Ein weiterer wichtiger Vertreter der modernen Blockchain-Technologie ist das Ethereum-Netzwerk.²⁹ Hierbei handelt es sich um ein abstraktes Blockchain-Metasystem, das wiederum in der Lage ist, andere Blockchains zu betreiben. Dazu verfügt Ethereum über eine eigene Programmiersprache und Verteilungsmethodik, die eine verteilte Programmausführung in Form von Smart Contracts möglich macht. So ist es möglich, mithilfe von Smart Contracts neue Verteilungsmechanismen zu programmieren und weitere Anwendungen auf und mit Blockchains zu ermöglichen. Diese Form von verteilter Software wird in den folgenden Kapiteln zur Erstellung von Industrie-4.0-Anwendungen genutzt, um darüber vollautomatisierte industrielle Transaktionen umzusetzen.

²⁸ <https://iota.org/>

²⁹ <https://ethereum.org/>

3. Anwendungsszenarien mit Blockchain-Mechanismen in der Automation

Dieses Kapitel dient dazu, anhand verschiedener Anwendungsbeispiele ein grundlegendes und allgemeines Verständnis für die Vereinbarkeit von Blockchain-Technologie und Industrie 4.0 zu schaffen. Hierzu werden zunächst die Archetypen der Blockchain-Technologie tabellarisch eingeordnet. Anschließend werden die von der Plattform Industrie 4.0 erarbeiteten Anwendungsszenarien³⁰ analysiert und szenarienspezifische, relevante Charakteristika der Blockchain-Technologie aufgezeigt. Abschließend werden die Anwendungsszenarien und -beispiele einander tabellarisch gegenübergestellt, um die Schnittmengen der beiden Szenariotypen zu verdeutlichen.



Quelle: kinwun / Fotolia.com

3.1 Anwendungsszenarien der Blockchain-Technologie

Als Anwendungsszenarien werden übergeordnete, klassifizierte und gruppierte Anwendungsfälle bezeichnet, die sich in der praktischen Ausführung zwar in Details unterscheiden, aber klare gemeinsame Grundstrukturen aufweisen. Die folgende Tabelle 2 stellt eine Auswahl häufig auftretender Anwendungsszenarien der Blockchain-Technologie dar, denen deutliche Potenziale für den Einsatz im Bereich von Industrie 4.0 zugeschrieben werden können

³⁰ Plattform Industrie 4.0: Fortschreibung der Anwendungsszenarien der Plattform Industrie 4.0, 10/2016.
https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/fortschreibung-anwendungsszenarien.pdf?__blob=publicationFile&v=7 (abgerufen am 10.6.2018)

Tab.2: Verallgemeinerte Anwendungsszenarien von Blockchain-Technologien teilweise abgeleitet aus Fußnote 31

Szenario	Beschreibung	Charakteristika	Beispielapplikationen
Nachverfolgung (Tracking und Tracing)	Automatisierte Güterabwicklung, Herkunftssicherung und Rückverfolgung innerhalb von Versorgungsketten	<ul style="list-style-type: none"> Manipulations-sichere Produkt(-liefer-)historie zum Aufdecken gefälschter Produkte (z. B. Medikamente) Elektronischer Frachtbrief mit allen erforderlichen Informationen für alle berechtigten Parteien zugreifbar 	WalMart/IBM Merck/CryptoTec Hansebloc
Energiemanagement	Dezentrale Vernetzung von Handel und Verteilung, z. B. elektrischer Energie	<ul style="list-style-type: none"> Dezentral organisierte Microgrids mit automatisiertem Handel Nachfragegesteuertes Energieangebot 	Brooklyn Microgrid PowerLedger
Proof-of-Existence/ Proof-of-Ownership	Verifizierung der Existenz bspw. von Daten/Dokumenten mittels Blockchain mit dem Ziel, später Ansprüche geltend machen zu können	<ul style="list-style-type: none"> Existenznachweis z. B. durch Zeitstempel und Verkettung Eigentumsnachweis durch Signatur Originalitätsnachweis einer Datei über eine kryptografische Hash-Funktion 	Poex.io Storj.io
(Finanz-) Transaktionen	Tauschmittel zur Beschleunigung und Vergünstigung globaler Finanztransaktionen	<ul style="list-style-type: none"> Autorisierungsmanagement Assetmanagement – beliebige Coins / beliebige Arten Transaktionen 	Bitcoin Ethereum Ripple
Lizenzmanagement	Erzeugung einer Lizenz und Gebrauchsautorisierung mit Authentifizierung und Autorisierung der korrekten Anwendung der Lizenz	<ul style="list-style-type: none"> Quantitative oder zeitliche Freigabe einer Lizenz mit automatisiertem Lizenzzugang nach Ablauf Energiemanagement Nachweis über Besitz einer Lizenz dezentral gesichert und rückverfolgbar 	Sample (BMBF) Musikindustrie
Metachains	Datentransfermanagement zwischen verschiedenen Blockchains beispielsweise zwecks Kommunikation, Asset-Transfer oder Migration	<ul style="list-style-type: none"> Transaktionen zwischen unterschiedlichen Chains Funktionale Trennung (Separation of Concerns) Konfigurationstypische Trennung (z. B. Leistungsgrößen) Security/Privacy 	Overledger Blockstream Polkadot Sidechain
Verteilte Anwendungen (dApps) zur Prozessautomatisierung	Sicherung und Beschleunigung der Automatisierung von Produktionsabläufen und -prozessen mittels intelligenter Verträge	<ul style="list-style-type: none"> Sicherheitszugewinne durch gegenseitige Überwachung von Systemen Anomaliedetektion innerhalb von Anlagen 	Ethereum (On-chain) Hyperledger (Off-chain)
Verteilte Anwendungen (dApps) als Legal Smart Contracts	Automatisierte und rechtssichere Vertragsabwicklung mit reduzierter menschlicher Interaktion	<ul style="list-style-type: none"> Juristische Fragestellungen Juristisch verbindlicher, automatisierter Vertragsabschluss 	Ethereum Hyperledger

Quelle: ZVEI, eigene Darstellung

³¹ Fridgen, G. et al.: A Solution in Search of a Problem: A Method for the Development of Blockchain Use Cases. Presented at the AMCIS 2018 July 26 (2018).

Witt, J., Richter, S.: Ein problemzentrierter Blick auf Blockchain- Anwendungsfälle. Presented at the Multikonferenz Wirtschaftsinformatik , Lüneburg March 6 (2018).

Wüst, K., Gervais, A.: Do you need a Blockchain? (2017).

3.2 Anwendungsszenarien aus der Industrie 4.0

Vergleichbar zu den Blockchain-Anwendungsszenarien werden in folgender Tabelle 3 die Anwendungsszenarien der Plattform Industrie 4.0 tabellarisch charakterisiert, um sie dann im Weiteren einander gegenüberzustellen. Die Anwendungsszenarien selbst sind dem Ergebnispapier „Fortschreibung der Anwendungsszenarien der Plattform Industrie 4.0“ entnommen. Die Szenarien bilden somit gewissermaßen einen „Status quo“ dessen, was gemeinhin mit dem Begriff Industrie 4.0 assoziiert wird.

Tab. 3: Anwendungsszenarien für Blockchain-Technologien

Szenario	Beschreibung	Blockchain-relevante Charakteristika
Auftragsgesteuerte Produktion – AGP	Vernetzung von Produktionsfähigkeiten über Unternehmensgrenzen hinweg mit dem Ziel, langwierige Investitionsentscheidungen zu umgehen und trotzdem kontinuierlich das eigene Portfolio bei sinkenden Losgrößen auszubauen.	<ul style="list-style-type: none"> • Unveränderbarkeit von Auftrags- und Transaktionsinformationen sowie Daten beteiligter Hersteller und Kunden • Bilden von virtuellen Handelsplätzen ohne zentralen Intermediär
Wandlungsfähige Fabrik – WFF	Adaptierbare Fertigungskonfigurationen zur kurzfristigen Veränderung von Produktionsfähigkeiten und -kapazitäten.	<ul style="list-style-type: none"> • Gesicherter Datenaustausch zwischen Sensorsystemen • Anlegen von Produktlebensläufen in der Produktion • Dezentrale Maschinensteuerung/-konfiguration
Selbstorganisierende adaptive Logistik – SAL	Flexibilisierung von industriellen und logistischen Systemen in volatilen Produktionsumgebungen.	Inhaltliche und zeitliche Unveränderlichkeit von Datensätzen dient der sicheren Nachverfolgung von Produktions- und Lieferprozessen in vollautomatisierten Lieferketten
Value Based Services – VBS	Prozess- und Zustandsdaten dienen als Rohstoff für die Optimierung von bereits ausgelieferten Produkten mit dem Ziel, diese und zukünftige Produkte kontinuierlich zu verbessern.	Nachverfolgbarkeit von Produktionskonfigurationen bei überwachungspflichtigen Produkten
Transparenz und Wandlungsfähigkeit ausgelieferter Produkte – TWP	Automatische Erhebung und Verarbeitung nutzungsbezogener Daten über ausgelieferte Produkte zur nachträglichen Produkt- und Prozessoptimierung.	Aufbau und Weitergabe von Produkthistorien und -wissen beispielsweise beim Wartungsaustausch analog zum Lizenzmanagement (= dig. Produktgedächtnis)
Mensch-Technik-Interaktion in der Produktion – MTI	Interaktion von Menschen mit technischen Systemen in der Produktion in Form physischer Assistenz oder geistiger Unterstützung zum Beispiel bei der Entscheidungsfindung.	---
Smarte Produktentwicklung für die smarte Produktion – SP2	Unternehmensübergreifende Datentransparenz und -verknüpfung und deren Nutzung im Umfeld der digitalen Produktentwicklung mit dem Ziel produktionsübergreifender Wertschöpfungszuwächse.	Bereitstellung abgesicherter Informationen ohne die Erfordernis von Intermediären
Innovative Produktentwicklung – IPE	Kollaborative hersteller- und anwenderübergreifende Engineering-Prozesse fördern die richtige Entwicklung des richtigen Produkts.	Sichere, unveränderliche und verteilte Datenhaltung unterstützt Kollaboration unterschiedlicher Hersteller
Durchgängiges und dynamisches Engineering von Anlagen – DDA	Vorausschauendes und dynamisches Engineering von Anlagen unter Berücksichtigung zukünftiger Änderungen mittels eines flexiblen Strukturmodells	---

Quelle: ZVEI, eigene Darstellung

3.3 Übertragung der Blockchain-Technologie auf die Anwendungsszenarien der Plattform Industrie 4.0

3.3.1 Auftragsgesteuerte Produktion (AGP)

Dieses Anwendungsszenario repräsentiert einen der Kernbereiche von Industrie 4.0, und viele der Steuerungsprozesse lassen sich sehr gut mit der Blockchain-Technologie vereinbaren. Die in diesem Szenario aufgebaute Bestell- und auch Lieferkette eines nach Kundenwünschen individualisierten Produkts lässt sich beispielsweise mittels einer oder mehrerer automatisierter, verteilter Anwendungen (Smart Contracts) abbilden, in denen die Produktinformationen wie zum Beispiel die Herkunft verschiedener Komponenten des individualisierten Produkts transparent einsehbar und kryptografisch abgesichert vorliegen. Die Rückverfolgbarkeit der Herkunft und anderer Produktinformationen einzelner Bauteile, beispielsweise zum Schutz vor Fälschungen, kann dadurch ebenso gewährleistet werden wie die Tatsache, dass der Hersteller nach Auslieferung des Produkts die ausgehandelte Entlohnung erhält. Produktionsaufträge können mittels Smart Contract also nachweisbar und verbindlich festgehalten werden. Die Validierung der Informationen erfolgt hierbei idealerweise zunächst durch die jeweils konkret betroffenen Vertragspartner, zum Beispiel Hersteller/Kunde oder Zulieferer/Kunde. Bei der Datenhaltung kann entweder auf ein dezentrales Netzwerk zwischen den einzelnen Vertragspartnern oder auf eine zentrale, ausgelagerte Vermittlungsstelle bei einem Dienstleister gesetzt werden. Blockchain-Anwendungen wie Distributed Applications tragen zusammenfassend zur Absicherung und beschleunigten Automatisierung von herstellerübergreifenden Produktionsprozessen bei und steigern auf diese Weise die Wertschöpfung entlang der gesamten Bestell- und Lieferkette.

3.3.2 Wandlungsfähige Fabrik (WFF)

Dieses Szenario geht von modular aufgebauten Fertigungskomponenten innerhalb einer Fabrik oder Fertigungsstraße aus, die sich produktabhängig schnell und unkompliziert umkonfigurieren lassen. Um derart unterschiedliche Aufgaben auszuführen, sind Identitätsmanagementfunktionen für Fertigungssysteme ein wichtiges Systemelement. Das Identitätsmanagement kann mittels Blockchain-Technologie ohne zentrale Intermediäre bereitgestellt und nachverfolgt werden. Auf diese Weise wird einerseits einer Korruption der Komponenten durch Angreifer von außen und fehlerhafter Zusammenstellung durch Mitarbeiter von innen vorgebeugt. Durch Speicherung von zum Beispiel (Ent-)Kopplungsprozedurdaten zwischen Komponenten bei Umbauten kann die Produktionshistorie einer jeden Komponente mittels Nachbarkomponenten mit bereits vorhandener Historie validiert werden und Fehlerzustände vermieden oder zumindest schneller erkannt werden. Bei auditierungspflichtigen Systemen bieten Blockchain-Technologien hier die Möglichkeit zur manipulationsresistenten Speicherung.

Ebenso können Komponenten von nicht autorisierten Fremdherstellern erkannt und im Zweifel vom Kopplungsprozess mit dem restlichen System ausgeschlossen werden. Die Speicherung von Selbstbeschreibung und anderen kritischen Identitätsdaten erfolgt dezentral auf allen Entitäten innerhalb des Netzwerks. Grundvoraussetzung ist jedoch, dass diese hardwareseitig dafür ausgelegt sind und je nach Hardware-Leistungsfähigkeit auf unterschiedliche Weise zum Netzwerk beitragen.

Bei komplexeren, beispielsweise Standort- und herstellerübergreifenden Lieferketten ergibt sich daraus, dass verschiedene Ebenen der Lieferkette unterschiedlicher Speichermethodiken und -tiefen und somit gegebenenfalls verschiedener Blockchains bedürfen. Der Einsatz von Metachains zur Übersetzung von der einen in die andere Chain ist daher notwendig.

3.3.3 Selbstorganisierende adaptive Logistik (SAL)

Dieses Szenario stellt eine Erweiterung der auftragsgesteuerte Produktion dar, in der die Logistik von Teilerzeugnissen zwischen Produktionsstrecken und auch die Lieferung von Endprodukten an Kunden durch autonom agierende Transportfahrzeuge erfolgt. Alle Entitäten der Supply-Chain wie Hersteller, Logistik- und Vermittlungsdienstleister und ihre Betriebsmittel und Werkzeuge sind am Prozess der Herstellung und Validierung von Produktverfolgungsdaten beteiligt. Um zum Beispiel bei einer Vielzahl autonomer Transportmittel nachvollziehen zu können, zu welchem Zeitpunkt ein Fahrzeug ein Produkt aufgenommen und transportiert hat, können verteilte Anwendungen (dApps) helfen. Sie machen den Herstellungs- und Transportweg eines (Teil-)Produkts transparent und schrittweise nachvollziehbar. Dies erscheint insbesondere bei herstellerübergreifenden Produktionsprozessen als notwendig, da das Transportgut potenziell manipuliert werden kann. Während des Produktionsprozesses können einerseits Diebstahl, Zweckentfremdung oder Produktmanipulationen vorgebeugt und nach der Auslieferung andererseits Vergütungsansprüche auf Herstellerseite und rechtliche Ansprüche zum Beispiel auf Produktfunktionen oder Garantien auf Kundenseite durchgesetzt werden.

3.3.4 Value-based Services (VBS) und Transparenz und Wandlungsfähigkeit ausgelieferter Produkte (TWP)

Bei diesen Szenarien werden insbesondere „klassische“ Produkte dadurch aufgewertet, dass erweiterte kundenindividuelle Features nach dem Kauf und bei Bedarf für das Produkt freigeschaltet werden oder zusätzlich käuflich erworben werden können. Hierfür werden beispielsweise während der Nutzung (anonymisierte) Betriebsdaten von ausgelieferten Produkten gesammelt und laufend ausgewertet.

Der Vertrieb von Produkten oder Maschinen kann auf diese Weise günstiger gestaltet werden und Kunden erhalten nur die Applikationen vom Hersteller, die sie auch wirklich für ihre Anlage benötigen. Durch den Einsatz einer Produkthistorie auf Basis von Blockchain kann hierbei die Sicherheit der eigenen Produkte zum Beispiel gegenüber Softwareplagiaten gesteigert werden. Die Produktnutzer als Besitzer und Erzeuger der übermittelten Betriebsdaten können von gesicherten und vertraulichen Blockchain-Applikationen gerade auch hinsichtlich des Daten- und Know-how-Schutzes profitieren. Nutzungslizenzen für die erzeugten Daten inklusive beispielsweise notwendiger Finanztransaktionen wären mittels Smart Contracts voll automatisierbar. Die Validierung von Daten wäre durch ihre jeweiligen Erzeuger und damit Besitzer durchzuführen, wohingegen die Speicherung durch entweder externe zentrale Dienste oder dezentrale Kunden-/Herstellernetze zu gewährleisten wäre. Weil bei diesem Szenario eine Vielzahl verschiedener Daten zur automatisierten Verarbeitung anfallen, ist eine ausführliche rechtliche Betrachtung und Umsetzung von Blockchain-Applikationen, beispielsweise in Form von Legal Smart Contracts, dringend anzuraten.

3.3.5 Smarte Produktentwicklung für die smarte Produktion (SP2) und innovative Produktentwicklung (IPE)

Bei der unternehmensübergreifenden digitalisierten Produktentwicklung werden verschiedene Anforderungen und Funktionen des Produkts in Abhängigkeit von Zulieferern verteilt, festgehalten und starre Engineering-Ketten so aufgebrochen. Die dezentrale Speicherung der dabei erzeugten Produktbeschreibungsdaten, wie zum Beispiel Teilanforderungen oder -funktionen, sowie die ihnen zugeordneten Hersteller und Dienstleister können insbesondere von herstellerübergreifenden Blockchain-Applikationen profitieren. Zuständigkeiten für Produkte und Prozesse stünden somit herstellerübergreifend gesichert und anerkannt zur Verfügung. Die Validierung dieser Daten würde durch die jeweiligen Entwickler und Hersteller erfolgen. Weiterhin profitieren Produktdaten für Engineeringprozesse von Folgeprodukten aus Rückflüssen von Betriebsdaten beim Endkunden resultieren, deren Nutzung und Distribution ebenfalls dynamisch per Smart Contract geregelt wird. Gleichzeitig kann der prozessübergreifende Datenschutz bei derartigen Transaktionen auf diese Weise sichergestellt werden, sodass Hersteller ausschließlich Zugriff auf jene Informationen erhalten, die sie auch benötigen. Um auch hier bewusst getrennte interne und externe Architekturen wieder gezielt an bestimmten Stellen miteinander zu verbinden, ist der Einsatz von Metachains sinnvoll.

3.4 Gegenüberstellung: Industrie-4.0-Anwendungsszenarien und Blockchain-Archetypen

Die nachfolgende Tabelle 4 fasst die im vorigen Kapitel gewonnenen Erkenntnisse zusammen und gleicht die gegenwärtigen Anwendungsszenarien für Blockchain-Technologie mit denen der Industrie 4.0 zusammenfassend ab. Es zeigt, dass sich viele Schnittstellen zwischen Industrie-4.0-Anwendungen und Blockchain-Technologien ergeben.

Dabei soll nicht der Eindruck entstehen, dass Blockchain-Technologien zwingend erforderlich seien. Vielmehr soll eine Blockchain als zeitliche und inhaltliche Absicherung von Transaktionen verstanden werden. Ein Betrieb ohne vertrauenswürdige zentrale Instanz ist möglich.

Tab. 4: Zusammenführung der Industrie-4.0- und Blockchain-Anwendungsszenarien

Einsatzgebiete	I4.0-Anwendungsszenarien						
	AGP	WFF	SAL	VBS	TWP	SP2	IPE
Nachverfolgung (Tracking and Tracing)	Grün/Grau	Grün	Grün	Grau	Grau	Grau	Grau
Existenznachweis (Proof-of-Existence) / Eigentumsnachweis (Proof-of-Ownership)	Grau	Grau	Grau	Grün	Grün	Grün	Grün
(Finanz)-Transaktionen	Grün	Grau	Grün/Grau	Grün/Grau	Grau	Grau	Grün
Lizenzmanagement	Grau	Grün	Grau	Grün	Grün	Grün	Grün
Verbindende Blockchains (Metachains)	Grün/Grau	Grau	Grün	Grau	Grün	Grün	Grün
Redundante, verteilte Software (dApps) zur Prozessautomatisierung	Grün/Grau	Grün	Grün	Grau	Grau	Grau	Grau
Redundante, verteilte Software (dApps) für legal verbindliche, vertragliche Transaktionen	Grün	Grün/Grau	Grün/Grau	Grün	Grün	Grün	Grün

Quelle: ZVEI, eigene Darstellung

Grün = I4.0-Anwendungsszenario (Spalte) greift sehr ausgeprägt auf ein Blockchain-Anwendungsszenario (Zeile) zurück

Grün/Grau = I4.0-Anwendungsszenario (Spalte) greift immer wieder erkennbar auf ein Blockchain-Anwendungsszenario (Zeile) zurück

Grau = I4.0-Anwendungsszenario (Spalte) greift gelegentlich, selten oder hier auf ein Blockchain-Anwendungsszenario (Zeile) zurück

AGP = Auftragsgesteuerte Produktion

WFF = Wandlungsfähige Fabrik

SAL = Selbstorganisierende adaptive Logistik

VBS = Value-based Services

TWP = Transparenz Wandlungsfähigkeit ausgelieferter Produkte

SP2 = Smarte Produktentwicklung für die smarte Produktion

IPE = innovative Produktentwicklung

4. Industrie 4.0: Gestaltungspotenziale durch Blockchains

Nachdem im vorhergehenden Kapitel Eigenschaften der Industrie-4.0-Anwendungsszenarien mit denen von übergeordneten Anwendungsszenarien von Blockchains in Verbindung gebracht wurden, werden diese hier hinsichtlich ihrer Anwendbarkeit diskutiert. Dabei ist klar, dass die Blockchain-Technologie und Industrie 4.0 grundsätzlich unabhängig zueinander stehen und daher einander auch nicht „bedürfen“. Vielmehr wird an dieser Stelle davon ausgegangen, dass Blockchains technologisch als ein Daten- und Transaktionssicherungsprotokoll anzusehen sind und Industrie-4.0-Anwendungen ergänzen.

Im Rahmen der folgenden Diskussion wird daher analysiert, inwieweit Industrie-4.0-Anwendungen von einer solchen Absicherung profitieren. Es sei hier noch einmal herausgestellt, dass dabei Aspekte wie Dezentralität, Intermediärfreiheit, Datensicherheit oder Vertrauen im Vordergrund der Bewertung stehen. Danach wird dargestellt, welche technologischen Herausforderungen sich daraus ergeben.

4.1 Analyse der Anwendungsszenarien

Zunächst einmal ist in Tabelle 4 offensichtlich, dass für alle betrachteten Industrie-4.0-Anwendungsszenarien die Blockchain-Technologie für bestimmte Teilanwendungen zum Einsatz kommen könnte. Dadurch, dass diese Technologie aber auch Kosten durch Infrastruktur, Programmierung und Wartung verursacht, muss aus ihrem Einsatz im Gegenzug hierfür auch ein entscheidender Mehrwert entstehen. Insbesondere dieser Mehrwert wird im Folgenden analysiert. Dabei wird vorrangig die Anzahl der herausragenden (grün) und vorteilhaften (grün/grau) Einträge in Tabelle 4 bewertet.

Bei der Prozessanalyse wird zunächst zwischen vorgelagert [produktionsplanenden](#), [produktionsumsetzenden](#) und nachgelagert [produktorientierten Prozessschritten](#) unterschieden. Bei den produktionsumsetzenden Prozessschritten weist die [selbstorganisierende adaptive Logistik \(SAL\)](#) die höchste Übereinstimmung mit Blockchain-Anwendungen auf: Neben dem Tracking und Tracing der gesamten Güterkette im Supply-Chain-Management müssen hier möglicherweise auch verschiedene Datenquellen zusammengeführt (Metachains) sowie eine Prozessautomatisierung an verschiedenen Standorten durch verteilte Anwendungen umgesetzt werden. Ergänzend kommen noch vorteilhafte Möglichkeiten zu (virtuellen) Finanztransaktionen oder auch die automatisierte Ausführung von rechtsverbindlichen Vertragsklauseln mithilfe von Blockchain-Technologien hinzu.

Nahezu dieselbe Übereinstimmung lässt sich bei der [auftragsgesteuerten Produktion \(AGP\)](#) feststellen, die gleichermaßen als vornehmlich externer Prozess vom Vertrauen innerhalb einer Blockchain und der Freiheit von Intermediären profitiert. Der wesentliche Unterschied in der Bewertung hier liegt lediglich darin, dass SAL vornehmlich auf der Metaebene einer allgemeinen Prozessautomatisierung betrachtet wird, während AGP konkret für die kaufmännische Abwicklung von Aufträgen steht.

Die [wandlungsfähige Fabrik \(WFF\)](#) stellt das Pendant zur [auftragsgesteuerten Produktion \(AGP\)](#) aus der Perspektive des Fertigungsprozesses dar. Hier ergeben sich die meisten Vorteile aus den erhöhten Sicherheitseigenschaften von Blockchains bei stark verteilten Systemen, wie sie bei einzelproduktgesteuerten Produktionen auftreten. Insbesondere vorteilhaft ist die Eigenschaft, dass eine asynchrone Kommunikation und Steuerung erfolgen kann und keine zentrale Steuerungsinstanz als potenzieller Engpass zur Ausführung von Automatisierungssoftware erforderlich ist. Im Zweifel könnte ein zu produzierendes Produkt diese Automatisierungssoftware sogar „in sich tragen“ und bei Bedarf einer ausführenden Instanz als Smart Contract zur Verfügung stellen.

Aber auch im späteren Lebenszyklus können [wandlungsfähige Produkte \(TWP\)](#) wie auch [Value-based Services \(VBS\)](#) noch von Blockchains profitieren. Hier stehen insbesondere die Möglichkeit der asynchronen Verwendung von auf einer Blockchain gespeicherten Daten oder die Autorisierung von Produkten und Anwendern durch Identitätsnachweise im Vordergrund. Daher sind Funktionen wie Eigentumsnachweise (Proof-of-Ownership) beispielsweise für Patente und Lizenzen oder auch die Vertragsabwicklung über automatisierte, rechtsverbindliche Blockchain-Anwendungen (engl.: legally binding smart contracts) prägend.

In der **Produktentwicklung selbst (SP2, IPE)** – als vorgelagerter Prozessschritt – kommen insbesondere bei firmenübergreifenden und dezentralen Entwicklungen alle abstrakten Anwendungsszenarien einer Blockchain zum Einsatz. Vom Existenz- und Eigentumsnachweis beispielsweise zur Absicherung von Lizenzen und Patenten über ein Lizenzmanagement selbst bis hin zum allgemeinen Datenaustausch über Metachains oder auch der Leistungsabrechnung über Smart Legal Contracts sind hier viele Anwendungen mit dem Einsatz von Blockchain-Technologien denkbar und möglich.

4.2 Abgeleitete strategische Herausforderungen

Auf Basis der in Kapitel 3 erarbeiteten Erkenntnisse, die in Tabelle 4 zusammengefasst sind, lässt sich im Weiteren ableiten, welche Szenarien sich aus dem Umfeld Industrie 4.0 vorrangig zur Umsetzung eignen. Ferner kann bestimmt werden, welche Anwendungsfälle zum aktuellen Zeitpunkt nicht empfehlenswert sind.

So eignen sich insbesondere unmittelbar fertigungsbezogene Prozesse wie SAL und AGP für die Integration von Blockchain-Prozessen. Aufgrund des firmenübergreifenden Charakters dieser Prozesse entsteht durch Manipulationssicherheit und Asynchronität von Transaktionen ein ausgeprägter Mehrwert durch Anwendung der Blockchain-Technologie.

Das Szenario WFF, bei dem ein Produkt im Entstehungsprozess selbst die Produktion steuert, Anlagen konfiguriert und gegebenenfalls sogar seinen eigenen Bauplan elektronisch mit sich führt, ist grundsätzlich gut mit Blockchain-Technologien realisierbar, aber technologisch selbst mit komplexeren Anforderungen verbunden. Hier stehen einer unmittelbaren Umsetzung insbesondere die Auslegung von Schnittstellen zwischen Produktionsanlagen, einem Produktionsmanagementsystem sowie dem Produkt selbst entgegen. Das erzwungene Vertrauen als eine der Kerneigenschaften von Blockchains basiert darauf, dass sich alle Transaktionen widerspruchsfrei auf einen gemeinsamen Basisknoten zurückführen lassen. Um dies im Umfeld der wandlungsfähigen Fabrik zu ermöglichen, ist eine anlagenübergreifende Schnittstelle erforderlich, die es allen am System beteiligten Entitäten ermöglicht, bestehende Transaktionen zu validieren und selbst Transaktionen zu generieren. Für ein Produktionsmanagementsystem stellt dies eine handhabbare Herausforderung hinsichtlich Systemressourcen, Speicherplatz, Bandbreite und Verarbeitungsgeschwindigkeit dar. Insbesondere ältere Produktionsanlagen könnten hinsichtlich ihrer Hauptaufgabe – nämlich der eigentlichen Produktion – bereits an ihrer Leistungsgrenze betrieben werden. Es ist daher fraglich, ob sie noch die Zusatzaufgabe eines vollwertigen Blockchain-Knotens unter Kenntnis aller Transaktionen erfüllen können. Für die in der Produktion befindlichen Produkte selbst, insbesondere wenn sie mit einfachen, günstigen Prozessorsystemen gesteuert und nachverfolgt werden, ist eine Teilnahme als vollwertiger Blockchain-Knoten kaum realisierbar. Geringer Speicher, restriktives Energiemanagement und beschränkte Bandbreiten stellen limitierende Größen dar.

Diese Aspekte werden in den Szenarien TWP und VBS noch anspruchsvoller in ihrer Umsetzung, da sich die Produkte außerhalb des kontrollierbaren Produktionsumfelds befinden und unter beliebigen Randbedingungen funktionieren müssen. Genau hier sind Absicherungen der Aktualisierungstransaktionen nach Blockchain-Prinzipien sinnvoll: Es lassen sich Blockchains zur Authentifizierung, Datenbereitstellung und -nachverfolgung einsetzen. Das Szenario unterscheidet sich durch das nachträglich hergestellte gesicherte Umfeld zur Funktionsübertragung aber nicht wesentlich von WFF, in dem ein Produkt seine Umgebung so steuert, dass es nach einem definierten Prozessschritt über weitere Funktionen verfügt.

Im Weiteren lassen sich die für alle aufgeführten Anwendungsszenarien relevanten technischen Herausforderungen in drei Bereiche aufteilen. Generelle Herausforderungen, die beim Aufbau von Blockchain-Systemen zu beachten sind, spezielle Herausforderungen in Industrie-4.0-Anwendungen und besondere Herausforderungen, die sich aus den jeweiligen Anwendungsszenarien ableiten.

Als generelle Herausforderungen lassen sich zunächst die Entscheidung über den Blockchain-Typ sowie generelle Eigenschaften von Blockchains hervorheben. Basierend auf den fünf Ws aus Kapitel 2 sind die folgenden Fragen im Vorfeld zu klären.

Die Zugriffsmöglichkeit auf Daten von Blockchains sowie Sicherheits- und Verkettungskonzepte (Mining) und die Verarbeitungsgeschwindigkeit müssen festgelegt werden. Daraus ergeben sich in der Regel bestimmte Blockchain-Typen, von denen im weiteren Lebenszyklus kaum noch bzw. nur mit erheblichem Aufwand die Daten auf einen anderen Typ migriert werden können. Hier werden üblicherweise dauerhafte, strategische Unternehmensentscheidungen getroffen, die oft auch eines erheblichen Fachwissens bedürfen. An dieser Stelle wird auch auf die Zusammenarbeit mit spezialisierten Beratungsfirmen verwiesen, da eine solche Entscheidung intensiv recherchiert und vorbereitet werden muss.

Spezielle Herausforderungen im Bereich von Industrie-4.0-Anwendungen leiten sich insbesondere aus der RAMI-4.0-Dokumentationen^{32, 33} ab:

- Privacy (Öffentlichkeit der Daten) und Security (Manipulationssicherheit der Daten)
- Echtzeitfähigkeit und Latenzzeiten
- Datenverfügbarkeit.

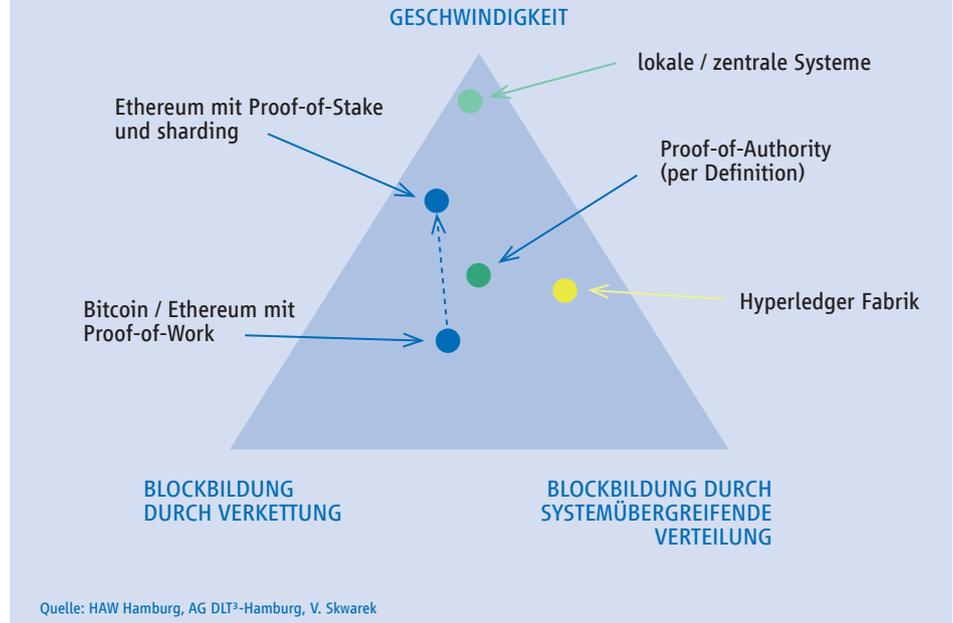
Bei Blockchain-Technologien stellen **Privacy** und **Security** zwei Faktoren dar, die nicht zwingend im Widerspruch zueinander stehen, allerdings in ihren Ausprägungen in unterschiedliche Richtungen wirken können. Als Extreme werden an dieser Stelle private und öffentliche Blockchains angeführt. In öffentlichen Blockchains werden die anfallenden Daten an alle Teilnehmer verteilt, sodass zwar deren Manipulation schwierig wird, aber der Inhalt grundsätzlich öffentlich wird. Bei privaten Blockchains wird der eigentliche Inhalt auf privaten, geschlossenen Systemen gehalten und nur Änderungstransaktionen werden an alle Teilnehmer kommuniziert. Folglich kann der Inhalt hier potenziell geheim bleiben, allerdings besteht dann auch die Gefahr einer zunächst unentdeckbaren, lokalen Manipulation. Zu beiden Extremtypen von Blockchain-Technologien bestehen auch Zwischenstufen, die die jeweiligen Effekte abzumildern versuchen, was dann aber wiederum zu weiteren Einschränkungen in anderen Bereichen wie Geschwindigkeit, Energiebedarf oder Speicherbedarf führt.

Die **Echtzeitfähigkeit** und **Latenz** von Blockchain-Systemen muss für die Auswahl geeigneter Anwendungsfälle in Betracht gezogen werden. Im Allgemeinen stellen Blockchains einen Kompromiss zwischen Datensicherheit und Ausführungsgeschwindigkeit dar, der sich mitunter signifikant auf verschiedene Leistungsparameter von entsprechenden Prozessen auswirken kann. Konkret entsteht ein Dreieck aus Geschwindigkeit, Sicherheit durch Verkettung und Verteilung (s. Abb. 6), in dem sich der Betriebspunkt befindet. Beispiel: Eine öffentliche Blockchain erfordert sehr zeit- und rechenaufwendige Prozesse zur Datenabsicherung wie beispielsweise Proof-of-Work. Durch diese Rechenzeiten entstehen wiederum hohe Latenzen. Sollen diese reduziert werden, also die Blockchain soll schneller werden, müssen einfachere Absicherungsmechanismen berechnet werden, wodurch die Unsicherheit wieder steigt. Diese Unsicherheit wiederum kann durch eine Zugangsbeschränkung auf vertrauenswürdige Teilnehmer verbessert werden.

³² DIN SPEC 91345:2016-04: Referenzarchitekturmodell Industrie 4.0 (RAMI4.0)

³³ Roland Heidel, Dr. Michael Hoffmeister, Martin Hankel, Udo Döbrich:
Basiswissen RAMI 4.0 - Referenzarchitekturmodell und Industrie 4.0-Komponente – Industrie 4.0, Beuth-Verlag, 2017.

Abb. 6: Entscheidungs-dreieck zur Einsatzoptimierung von Blockchain- und Distributed-Ledger-Systemen.



Quelle: HAW Hamburg, AG DLT³-Hamburg, V. Skwarek

So eignen sich heutige Blockchain-Systeme beispielsweise nur bedingt für Prozesse mit harten Echtzeitanforderungen, da im Allgemeinen keine Garantie bezüglich Ausführungsgeschwindigkeit von Transaktionen gegeben werden kann: Es ist nicht sichergestellt, dass alle anstehenden Transaktionen innerhalb einer vorgegebenen Zeitspanne prozessiert werden. Es existieren Blockchain-interne Beschränkungen wie maximale Blockgrößen oder Transaktionszahlen, die innerhalb eines Mining-Intervalls verarbeitet werden. Zudem steigt die Wahrscheinlichkeit der Echtheit einer Transaktion, je mehr Blöcke an diese angehängt und somit je länger Blockchain betrieben wurde.

Hinsichtlich der **Datenverfügbarkeit** muss berücksichtigt werden, dass die eigentliche Datenhaltung nicht auf einer Blockchain erfolgen sollte. Dies würde durch die kontinuierliche Verteilung neuer Daten zwischen allen Teilnehmern zu einem erheblichen Kommunikations- sowie Speicherbedarf führen. Stattdessen ist es üblich, in der Blockchain selbst Prüfsummen von Daten in Form von Hashes zu speichern und an die Teilnehmer zu verteilen sowie die Daten auf Anfrage gegebenenfalls automatisiert verfügbar zu machen. Daten in großen Mengen selbst werden eher außerhalb der Blockchain auf lokalen Speichern (off-chain) abgelegt. So können Teilnehmer bei Bedarf auf vorhandene Daten zugreifen und durch die öffentliche und manipulationsresistente Speicherung der Prüfsumme überprüfen, ob eine Manipulation der Daten vorliegt.

4.3 Maßnahmen zur Akzeptanz im Markt

Die Blockchain- und Distributed-Ledger-Technologie ist zunächst einmal ein Protokoll, das Daten im Vergleich zu einer Verschlüsselung nicht verbirgt, sondern semantisch – also in ihrer Reihenfolge und ganzheitlichen Bedeutung – absichert. Zusätzlich zu dieser Absicherung ist auch noch eine Automatisierung mithilfe von verteilter und gleichermaßen gegen Manipulation geschützter Software möglich. In diesem Sinne ist die Funktion von BC/DLT vergleichbar mit einer Datensicherungsschicht in einem Kommunikationssystem analog zum https-Protokoll beim Einsatz von Internetbrowsern, wenngleich sich beide in ihrer konkreten Umsetzung deutlich voneinander unterscheiden. Grundsätzlich sollte hier also marktseitig kein Akzeptanzhindernis dieser Technologie zu erwarten sein.

Allerdings könnte ein Akzeptanzhindernis tatsächlich durch eine Verunsicherung der Abnehmer entstehen aufgrund

- einer mangelnden technischen Strukturierung von Blockchains durch die Entwicklergemeinde,
- einer starken Differenzierungsbestrebung zwischen Blockchain-Technologien und somit einer mangelnden Harmonisierung/Standardisierung,
- einer hohen Entwicklungsdynamik neuer oder bestehender BC/DLT-Systeme und -Plattformen sowie der daraus folgenden Effekte
- mangelnde Migrationsfähigkeit,
- mangelnde Interoperabilität und
- vergleichsweise hohe Inbetriebnahme- und Wartungsaufwände.

Da ist Sinnhaftigkeit semantisch abgesicherter Datenstrukturen – und somit BC/DLT – für den Einsatz in industriellen Netzwerken wahrscheinlich nicht grundlegend infrage gestellt wird, sollten akzeptanzsteigernde Maßnahmen in zweierlei Richtung zielen: einerseits eine bessere Informationsgrundlage zur Entscheidung im Markt schaffen, andererseits die Komplexität des industrierelevanten Blockchain-Markts reduzieren.

Für eine bessere Informationslage ist es sinnvoll, sowohl über die betriebliche Weiterbildung als auch mithilfe des technischen Marketings und Vertriebs über das Thema BC/DLT hinsichtlich der technologischen Struktur und Möglichkeiten neutral zu informieren. Nur so ist es potenziellen Nutzern möglich, die Komplexität und Varianz von BC/DLT zu verstehen und zu durchdringen. Oftmals sind Befürchtungen oder Vorbehalte unbegründet, sondern basieren auf veralteten oder vermischten Informationen, die sich in dieser Form bei detaillierter Analyse und Recherche nicht bestätigen oder ausräumen lassen. Besonders wichtig für die Verbesserung des technischen Verständnisses und auch der Offenheit für diese neuartigen Datensicherungsansätze in höheren protokollarischen Schichten sind konkret ausformulierte und technisch modellierte Anwendungsszenarien und -fälle. Hierzu wäre es empfehlenswert, wenn beispielsweise eine Arbeitsgruppe auf Verbandsebene eingerichtet würde, um diese Themen weiter inhaltlich auszuführen. Dabei ist es wichtig, die Integration von BC/DLT in Industrie 4.0 und RAMI 4.0 anhand klarer Beispiele mit Abläufen und Datenabhängigkeiten zu erarbeiten und auf Standardisierung zu prüfen.

Hiermit wird dann auch eine Grundlage für die zweite akzeptanzsteigernde Maßnahme gebildet – die Vereinheitlichung/Normung/Standardisierung. Bei dezentraler Datenhaltung, der Reduktion von Intermediären und der Automatisierung durch verteilte Software muss die Effizienzsteigerung und somit eine Kostensenkung erreicht werden. Eine intermediärlose Dezentralität ermöglicht aber gleichermaßen eine unkontrollierbare Varianz an Datenstrukturen, die sich systembedingt kaum unterbinden lässt. Um ein Angebot für diejenigen zu schaffen, die eine solche Effizienzsteigerung durch gleichartige Infrastruktur und Schnittstellen nutzen möchten, bietet der zuvor vorgeschlagene Schritt der ausformulierten und modellierten Blockchain-Industrie-4.0-Anwendungsfälle eine Basis zu Standardisierung oder auch zur Normung, beispielsweise durch ISO TC 307 „Blockchain and Distributed Ledger Technologies“. Diese könnten dann auf schon vorhandene oder im Aufbau befindliche Dateninfrastrukturen wie beispielsweise der International Data Spaces Association³⁴ oder dem Interplanetary File System³⁵ betrieben werden.

³⁴ <https://www.internationaldataspaces.org/>

³⁵ <https://ipfs.io/>

4.4 Standardisierung

Die derzeit bekanntesten Blockchains wie beispielsweise Bitcoin, Ethereum oder auch Distributed-Ledger-Systeme wie Hyperledger oder IOTA sind aus einem Community-Ansatz heraus entstanden. Das heißt, Entwickler(gemeinden) haben sich in der Regel international in virtuellen Gemeinschaften zusammengeschlossen und aus der Analyse vermeintlicher Defizite des aktuellen Stands der Technik neue Blockchain- und Distributed-Ledger-Systeme entwickelt. Dieses Vorgehen führt dazu, dass sich neue Systeme durch Differenzierung auszeichnen und weniger durch Übereinstimmungen bzw. gar nicht über die Definition gemeinsamer Schnittstellen. Hierzu gibt es vereinzelt Ansätze, bei denen versucht wird, Blockchains miteinander zu verbinden – es handelt sich dabei um sogenannte Metachains, die in der Lage sind, vertrauenswürdige Transaktionen zwischen Blockchains zu erzeugen. Somit liegen auch hier weniger „gemeinsame Schnittstellen“ vor, sondern eine weitere Software, die zwischen mehreren Blockchains übersetzt. Hierin liegt derzeit ein Problem in der Akzeptanz von Blockchain-Technologien, da keine Migrationskonzepte zwischen verschiedenen Systemen existieren und somit ein Wechsel nach einer initialen Entscheidung nicht mehr unkompliziert möglich ist.

Ein weiterer Aspekt erforderlicher Vereinheitlichung besteht in der Standardisierung von Datenstrukturen, die innerhalb von Blockchains verwendet werden, und gegebenenfalls von Zugriffsschnittstellen: Grundsätzlich steht es jedem Teilnehmer an einer Blockchain frei, beliebige Daten in Form von Transaktionen auf einer Blockchain abzulegen. Diese sind dann zwar – abhängig vom Typ der Blockchain – weitgehend ungehindert von autorisierten Systemteilnehmern lesbar, aber aufgrund fehlender Metadaten nicht unmittelbar interpretierbar. Derartige Interpretationsprobleme lassen sich mindestens durch die Standardisierung von Datentypen, die auf einer Blockchain abgelegt werden, reduzieren. Darüber hinaus ist es auch möglich, im Rahmen eines objektorientierten Ansatzes nicht nur die Daten zu standardisieren, sondern mithilfe von Smart Contracts sogar Blockchain-eigene Verfahren zum einheitlichen Datenmanagement zu nutzen. In diesem Fall wären dann einheitliche Smart Contracts beispielsweise für den Versand von Gütern oder für das Generieren von Aufträgen zu definieren.

In diesem Bereich sind viele Standardisierungsgremien derzeit aktiv, um unterschiedlichste Bereiche und Eigenschaften von Blockchains aus verschiedenen Perspektiven zu vereinheitlichen. Diese Vereinheitlichung ist wichtig, um eine industrieübergreifende Nutzung von Blockchain-Technologien beispielsweise im Kontext von Industrie 4.0 zu ermöglichen. Im Folgenden wird eine Auflistung von aktuellen Standardisierungsaktivitäten gegeben, die sich im Wesentlichen auf den deutschen Raum bzw. auf ihre übergeordneten internationalen Organisationen beziehen.

- DIN NA 043-02-04 AA: Blockchain und Technologien für verteilte elektronische Journale, Spiegelkomitee zu ISO TC 307
- DIN Spec 3103: DIN SPEC 3103. Smart Contracts und Sensoren in Blockchains für Industrie-4.0-Anwendungen
- DKE-Expertenkreis zu Blockchains im Energiesektor
- Cenelec: Focus Group on Blockchain and Distributed Ledger Technologies (DLT): Erstellen eines Positionspapiers als Eingabe der Europäischen Kommission an ISO TC 307
- ISO TC 307
 - Governance of blockchain and distributed ledger technology systems
 - Interoperability of blockchain and distributed ledger technology systems Working group
 - Foundations
 - Security, privacy and identity
 - Smart contracts and their applications
- ITU-T: Focus Group on Application of Distributed Ledger Technology
- ETSI:
 - State of the Art: Ecosystem, Terms, Definitions, Concepts
 - Applications & Services
 - Technology Reference Framework
 - Policy Reference Framework
 - Standardization Roadmap
- UN/CEFACT – Blockchain Project – P1049: Blockchain White Paper
- White Paper on the technical applications of Blockchain to United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) deliverables

- JTC 1 SC 41 AHG 18: Study Group on Integration of IoT and Blockchain
- Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques

In dieser Aufzählung sind derzeit nur Institutionen und Aktivitäten berücksichtigt, die mit nationalen und internationalen Normungsmandaten ausgestattet sind. Darüber hinaus existieren noch zahlreiche weitere Einrichtungen, die beispielsweise in anderen Konsortien Industriestandards erarbeiten. Weiterhin ist darauf hinzuweisen, dass es sich bei der Aufzählung oben zwar um einen umfassenden aktuellen Stand der Normungsaktivitäten handelt, die möglicherweise aber nicht vollständig ist.

Es fällt allerdings auf, dass das Thema der Blockchains im industriellen Umfeld und Einsatz noch nicht durch ein Standardisierungsmandat abgedeckt oder wahrgenommen wird. Für einen tatsächlich intermediärfreien Einsatz dieser Technologie wird dies aber als dringend erforderlich empfohlen. Ein erster Schritt in diese Richtung wird derzeit durch ein Projekt DIN SPEC 3103 unternommen, in dem die Interaktion von Blockchains, Smart Contracts und RAMI 4.0 beschrieben wird.

4.5 Aktuelle Forschungsaktivitäten

Hinsichtlich angehender Forschungsarbeiten im Bereich der Blockchain-Technologie können Arbeiten allgemein in drei Bereiche eingeteilt werden, die im Folgenden kurz zusammengefasst werden, ohne dabei auf die Vielzahl an Arbeiten einzugehen, die sich mit ökonomischen oder juristischen Aspekten von Blockchain-Technologien beschäftigen. Aus technischer Sicht gibt es weiterhin zahlreiche Arbeiten die sich unter anderem mit der Leistungsfähigkeit und Sicherheit von Blockchain-Systemen befassen und versuchen, diese zu verbessern. Ziel dieses Forschungsbereichs ist es, die Leistungsfähigkeit von Blockchain-Systemen durch Parameteroptimierungen sowie Protokollerweiterungen zu verbessern. Schließlich beschäftigt sich ein Teil der Forschungsgemeinschaft, wie auch diese Studie, mit der Identifikation von Anwendungsgebieten der Blockchain-Technologie. Im Folgenden sollen einige der Arbeiten aus diesem Bereich zusammengefasst werden.

- [Klein et al.³⁶](#) entwickeln in ihrer Arbeit ein Framework zur Identifikation von Anwendungsgebieten, die von einer Blockchain-Integration profitieren können. Neben einer Richtlinie für die Auswahl geeigneter Use-Cases stellen die Autoren detaillierte Informationen bezüglich der für die gewählte Anwendung zu erwartenden Vorteile bereit. Bezüglich der Anwendbarkeit und des erwarteten Nutzens analysieren Klein et al. potenzielle Use Cases hinsichtlich der fünf Kategorien [Mehrwert](#), [Daten](#) und [Prozessintegrität](#), [Dezentralisierung](#), [Werte](#) und [Rechte](#) sowie [Automatisierung](#). Aufgrund einer Bewertung der Wichtigkeit dieser Kriterien für den Anwendungsfall kann so mithilfe des vorgeschlagenen Frameworks eine fundierte Entscheidung getroffen werden.
- [Wüst et al.³⁷](#) befassen sich ebenfalls mit der Frage, für welche Probleme und Anwendungen die Blockchain-Technologie eine geeignete Lösung darstellt. Zu diesem Zweck werden zunächst die Unterschiede zwischen der Blockchain-Technologie und einer zentralisierten Datenbank analysiert. Weiterhin behandeln die Autoren die drei dedizierten Anwendungsfälle Supply-Chain-Management, Interbank und Internationale Bezahlung sowie Dezentrale Autonome Organisationen. Im Rahmen dessen entwickeln die Autoren einen Entscheidungsbaum, der bei der praxisorientierten Untersuchung, ob Blockchain eine geeignete Lösung ist, helfen kann. Dieser wird weiter ergänzt durch eine Zusammenfassung kritischer Unterschiede der Blockchain-Technologie in ihren verschiedenen Ausprägungen [Permissionless Blockchain](#) und [Permissioned Blockchain](#) zu einer klassischen, zentralen Datenbank.
- [Hofmann et al.³⁸](#) diskutieren allgemeine Entwicklungen und Chancen im Bereich Industrie 4.0 und beleuchten die Inhalte aktueller akademischer Forschungsarbeiten aus dem Bereich. Im Rah-

³⁶ Klein, Sandra, and Wolfgang Prinz. „A Use Case Identification Framework and Use Case Canvas for identifying and exploring relevant Blockchain opportunities.“ Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET), 2018.

³⁷ Wüst, Karl, and Arthur Gervais. „Do you need a Blockchain?“ IACR Cryptology ePrint Archive 2017 (2017): 375.

men dessen untersuchen die Autoren bekannte Prozesse aus dem Umfeld Industrie 4.0 auf die Anwendbarkeit moderne Technologien, unter anderem der Blockchain-Technologie. Die angestellte Untersuchung kommt zum Schluss, dass bisher keine einheitliche Definition des Begriffs Industrie 4.0 vorliegt, sich die Ziele allerdings in einer Bewegung hin zu zunehmend dezentralisierten, selbstregulierenden Wertschöpfungsketten widerspiegeln. Ermöglicht wird diese Bewegung durch Technologien wie beispielsweise Blockchain, IoT und Cloud Computing.

Zusammenfassend lässt sich sagen, dass sowohl Bestrebungen zur Weiterentwicklung der Technologie selbst als auch Untersuchungen bezüglich der Anwendbarkeit auf verschiedene Branchen und Prozesse derzeit noch Bestandteil der Forschung sind. Dabei ergeben sich beispielsweise Forschungsbedarfe zu Echtzeitfähigkeit, blockchainübergreifendem Datentransfer, Einsatz in Systemen mit geringen Verarbeitungsressourcen oder auch Pilotanwendungen. Besonders in jungen und sich rasch entwickelnden Umfeldern wie der Industrie 4.0 und Blockchain ist eine kontinuierliche Evaluation der technologischen Entwicklung von Blockchains empfehlenswert.



Quelle: zapp2photo / Fotolia.com

³⁸ Hofmann, Erik, and Marco Rüsç. „Industry 4.0 and the current status as well as future prospects on logistics.“ Computers in Industry 89 (2017): 23-34.

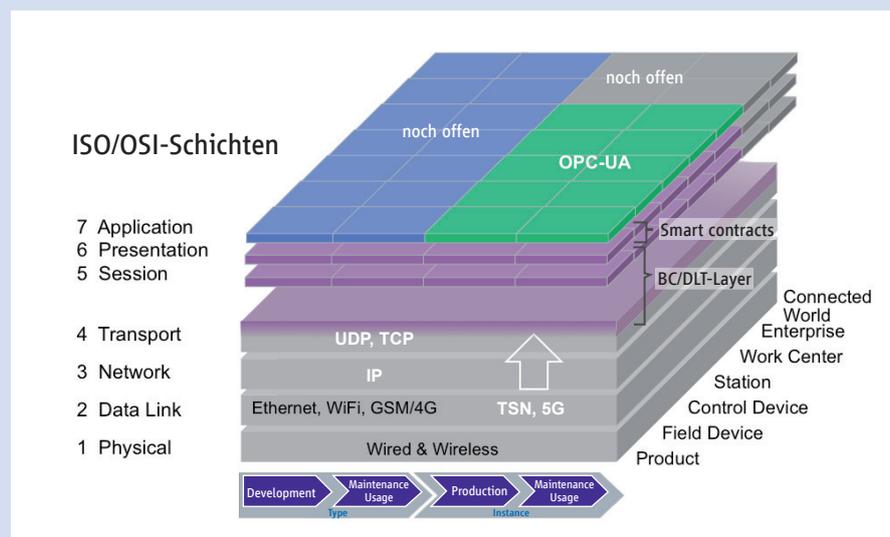
5 Zusammenfassung und Empfehlungen

Im Rahmen dieser Studie konnte gezeigt werden, dass die zunächst voneinander unabhängigen Technologien Blockchain und Industrie 4.0 über Schnittmengen verfügen. Industrie 4.0 mit seinen Anwendungsszenarien profitiert in vielen Fällen von Blockchain-Eigenschaften wie Dezentralität und Freiheit von Intermediären, Asynchronität und der Datensicherheit durch Verkettung sowie der Möglichkeit der Verarbeitungsautomatisierung mithilfe verteilter Software (Smart Contracts). Abstrakt betrachtet, lassen sich Blockchain- und Distributed-Ledger-Technologien (BC/DLT) sogar als ein Protokoll zur Absicherung einer offenen und verteilten Datenkommunikation verstehen. Da Industrie-4.0-Anwendungen durch ihre dynamische Konfigurierbarkeit einen hohen Kommunikationsbedarf aufweisen, erscheint schon diese Überlegung als ein ausreichender Grund, BC/DLT aus der Perspektive eines Datensicherungsprotokolls für Industrie 4.0 in Betracht zu ziehen.

Aus der Analyse der Industrie-4.0-Szenarien hat sich ergeben, dass ein Einsatz von BC/DLT grundsätzlich an allen Stellen denkbar wäre. Allerdings muss der erhöhte Aufwand für Kommunikation, Speicherung und Verarbeitung von BC/DLT-Daten auch durch einen signifikanten Mehrwert gerechtfertigt werden können, der nicht durch zentrale oder lediglich kryptographisch verschlüsselte Verfahren erreicht werden könnte.

Als besonders geeignet hat sich hier das Szenario der **selbstorganisierenden adaptiven Logistik (SAL)** erwiesen, da dieses vieler Prozessschritte, Schnittstellen, in- und externer Parteien sowie eines erhöhten Vertrauens bedarf, sodass sich hier eine verteilte, konsensuale Datenhaltung einschließlich einer Verarbeitungsautomatisierung als vorteilhaft erweist. Die **auftragsgesteuerte Produktion (AGP)** als ein möglicher Initiator zu SAL könnte im Sinne eines offenen Marktplatzes auch aus vergleichbaren Gründen zu SAL von BC/DLT profitieren. Bei der **wandlungsfähigen Fabrik (WFF)** handelt es sich eher um eine interne Kommunikation, bei der zwar eine erhöhte Datensicherheit erreicht werden kann, aber der effektive Nutzen im Vergleich zum Mehraufwand deutlich abgewogen werden muss. Weitere Szenarien profitieren in verschiedenen Ausprägungen auch von BC/DLT, sind jedoch deutlich komplexer in ihrer Umsetzung und sollten daher nicht im ersten Schritt angegangen werden. Hier empfehlen sich eher Forschungsprojekte, in denen zur weiteren Ausarbeitung von RAMI 4.0 Blockchain- und Distributed-Ledger-Technologien zur Datenabsicherung in den Prozess integriert werden.

Abb. 7: BC/DLT-System in RAMI 4.0 als Datenschichtungsschicht.
Quelle: angelehnt an Abbildung aus Basiswissen RAMI 4.0³⁹



Quelle: modifiziert nach Basiswissen RAMI 4.0, 2017, Beuth-Verlag

³⁹ Roland Heidel, Dr. Michael Hoffmeister, Martin Hankel, Udo Döbrich: Basiswissen RAMI 4.0 – Referenzarchitekturmodell und Industrie 4.0-Komponente – Industrie 4.0, Beuth-Verlag, 2017.

Im Rahmen der weiteren Entwicklung – und teilweise auch noch als Fragen der Forschung – von BC/ DLT in Hinsicht auf den Einsatz in Industrie 4.0 sind insbesondere Mechanismen zur Echtzeitfähigkeit und zur Reduktion von Latenzzeiten in Verbindung mit der Öffentlichkeit sowie der Manipulations-sicherheit der Daten zu untersuchen. Dabei stehen diese Parameter nicht unabhängig voneinander, sondern müssen möglicherweise anwendungsfall-spezifisch angepasst werden. Um hier auch kos-tensensible Anwendungen mit geringer Ressourcenverfügbarkeit zu berücksichtigen, ist eine mög-liche industriespezifische Adaption oder sogar Neuentwicklung von BC/ DLT-Systemen in Betracht zu ziehen. Eine Neuentwicklung könnte so weit gehen, dass Kernfunktionen von Blockchains auf eine Schicht in einem Kommunikationssystem (s. Abb. 7) reduziert werden und wie ein Treiber in einem Betriebssystem wirken.

Bei derzeitigen sehr dynamischen technischen Entwicklungsvorgängen und -zyklen im BC/ DLT-Umfeld könnte es sinnvoll sein, sich von dieser Dynamik zu entkoppeln und industrieübergreifend entspre-chende Technologien mindestens nach eigenen Ansprüchen zu adaptieren. Somit wäre eine Anpas-sung an industrieübliche Entwicklungszyklen und -prozesse möglich.

Dies führt dann auch zu einer Vereinheitlichung der Technologie, wie sie für den industriellen Einsatz notwendig ist. Da insbesondere bei BC/ DLT der intermediärfreie Einsatz über Herstellergrenzen hin-weg geplant ist, ist mindestens eine Standardisierung der Schnittstellen sinnvoll. Um hier von inter-nationalen Prozessen zu profitieren, ist es empfehlenswert, an bestehenden Aktivitäten in ISO und JTC zu partizipieren. Beispielsweise entsteht derzeit eine DIN SPEC 3103, die verbindende Schnittstellen zwischen RAMI 4.0, BC/ DLT und den Anwendungsszenarien Industrie 4.0 abstrahiert und beschreibt. Diese kann als Basis für Implementierungen und weitere Standardisierungen verwendet werden.

Insgesamt lässt sich feststellen, dass es sich bei BC/ DLT noch um eine sehr junge und im Entwick-lungsprozess befindliche Technologie handelt. Diese ist aus der Perspektive eines Datensicherungs-protokolls in verteilten, intermediärlosen Systemen aber in der Lage, Kommunikation nach Anfor-derungen und Szenarien von Industrie 4.0 abzusichern und zu automatisieren. Daher sollte BC/ DLT als Kommunikationselement in die Weiterentwicklung von RAMI 4.0 mitaufgenommen werden. Wert-schöpfungsketten von BC/ DLT-Absicherungsverfahren für Transaktionen und Datenkommunikation in Industrie-4.0-Anwendungen müssen durch Referenz- und Pilotprojekte weiterführend analysiert und implementiert werden.



ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e.V.
Lyoner Straße 9
60528 Frankfurt am Main
Telefon: +49 69 6302-0
Fax: +49 69 6302-317
E-Mail: zvei@zvei.org
www.zvei.org