WHITEPAPER

DIE BLOCKCHAIN IM MITTELSTAND

Herausgeber:
eco – Verband der Internetwirtschaft e.V.

VERBAND DER INTERNETWIRTSCHAFT

Die Blockchain im Mittelstand

Inhaltsverzeichnis

Die nachfolgenden Abbildungen 1-5 sind dem Fachartikel „Blockchain-Technologie unter der Lupe" von Prof. Dr. Norbert Pohlmann entnommen. Erschienen in IT-Sicherheit, 05/2018, S. 58 ff., unter https://norbert-pohlmann.com/app/uploads/2018/10/388-Blockchain-Technologie-unter-der-Lupe--Sicherheit-und-Vertrauenswürdigkeit-kryptografisch-verkettete-Datenblöcke-Prof.-Norbert-Pohlmann.pdf

1. Einleitung

Die Blockchain hat den Sprung in die Öffentlichkeit geschafft: Tageszeitungen, Wirtschaftsmagazine, Newsportale und Blogs berichten fast täglich über die Technologie, die Grundlage der Kryptowährung *Bitcoin* ist. Und nicht nur IT-Unternehmen erforschen die Blockchain. Auch Versicherungen, Logistikunternehmen, Banken, Börsen und Unternehmen vieler anderer Branchen arbeiten an Szenarien für mögliche Anwendungen.[1] Was anfänglich nach einem Hype aussah, verfestigt sich zu einem Trend mit vielversprechender Zukunft. Die Blockchain hat als eine typische Querschnittstechnologie das Potenzial, ganze Wertschöpfungsketten zu revolutionieren – denn sie ermöglicht die Transaktion von Werten im digitalen Raum ohne Intermediäre und stellt damit eine neuartige, effiziente Methode zur Verifikation von Daten und Datentransfers in Multistakeholder-Systemen dar.

Waren die vergangenen Jahre – mit Ausnahme der *Bitcoin*-Blockchain – geprägt von theoretischen Konzepten und Proof-of-Concepts, sieht man inzwischen weniger Visionäre als vielmehr Ingenieure, welche die Blockchain-Technologie einem Reality-Check unterziehen. Die Frage nach der IT-Sicherheit ist hier ein wichtiges Element. Schließlich spielt sich eine Vielzahl möglicher Anwendungen in sehr sensiblen Bereichen wie Finanzen, Versicherungen oder der Medizin ab. Ein Vorteil der Blockchain: Die Technologie bietet „Security by Design" – die Blockchain ist schon aufgrund ihrer grundlegenden Konzeption nur schwer zu kompromittieren. Wie stets bei IT-Systemen, bleiben trotzdem einige Herausforderungen.

Eine Adaption der Technologie im Mittelstand erfordert dort vor allem Vertrauen[2] in die Sicherheit und Verlässlichkeit: Damit die Technologie tatsächlich eingesetzt wird, muss sie nicht nur sicher sein, sondern ebenso ressourceneffizient und nutzerfreundlich. Wichtig ist außerdem die Interoperabilität mit anderen Systemen.

---

[1] Siehe für Anwendungsszenarien Weltwirtschaftsforum, The future of financial infrastructure – An ambitious look at how blockchain can reshape financial services, 2016, unter http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf; Blockchain Bundesverband, Statement on Token Regulation with a Focus on Token Sales, 10.02.2018, unter https://bundesblock.de/de/token-regulation-paper/; BDEW, Blockchain in der Energiewirtschaft, 2017, unter https://www.bdew.de/media/documents/BDEW_Blockchain_Energiewirtschaft_10_2017.pdf

[2] Eingehend Werbach, The Blockchain and the New Architecture of Trust, 2018; Werbach, 33 Berkeley Tech. L.J. 2018, S. 487.

Das vorliegende Arbeitspapier der Kompetenzgruppen Blockchain und Sicherheit im *eco – Verband der Internetwirtschaft e.V.* gibt einen Überblick über die wichtigsten Fragen, die vor dem Einstieg in das eigene Blockchain-Projekt beantwortet werden sollten.

2. Was ist die Blockchain?

Die Blockchain ist ein Kommunikationsprotokoll, in dem durchgeführte Transaktionen in verteilten Datenbanken transparent gespeichert werden können. Das Protokoll selbst stellt eine Reihe von Funktionen bereit, damit die Kommunikation sicher, transparent und pseudonym durchgeführt werden kann. So sind alle gespeicherten Transaktionen und Informationen an vielen verschiedenen Orten gleichzeitig gespeichert. Ihre Integrität ist durch die Speicherung von Hashwerten des jeweils vorangegangenen Datensatzes gesichert.[3]

Die grundlegenden Eigenschaften der Blockchain-Technologie sind folglich:

- die dezentrale Datenstruktur,
- die redundante Verteilung der Daten im Netzwerk,
- die manipulationssichere Speicherung der Daten im Netz und
- die Nachvollziehbarkeit der gespeicherten Daten.

Inzwischen existieren zahlreiche Weiterentwicklungen (beispielsweise Lightning und Raiden[4]) und Erweiterungen der ursprünglichen *Bitcoin*-Blockchain, wie etwa sogenannte Smart Contracts[5], die eine automatisierte Abwicklung von Anwendungsprozessen ermöglichen. Gerade Smart

[3] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, S. 2, unter https://bitcoin.org/bitcoin.pdf.
[4] Lightning entlastet ein Blockchain-Netzwerk und verbessert die Skalierbarkeit. Mithilfe eines separaten Zahlungskanals können zwei Knoten durch Benutzung eines 2-2-Multisignatur-Wallets untereinander gebührenfrei Transaktionen durchführen. Der Kanal wird durch eine initiale Funding Transaction geöffnet. Danach können die Knoten beliebig viele Transaktionen untereinander tätigen, ohne diese in der Blockchain zu speichern. Die Forderungen werden erst saldiert und wieder in die Blockchain geschrieben, sobald einer der beiden Teilnehmer den Kanal schließt, indem er eine Settlement Transaction veröffentlicht, die den finalen Saldo beider Parteien aus der letzten Commitment-Transaction enthält. Raiden wird für die Ethereum-Blockchain entwickelt und setzt auf das gleiche Prinzip.
[5] Das Konzept der Smart Contracts geht bereits zurück auf Szabo, The Idea of Smart Contracts, 1997, unter https://nakamotoinstitute.org/the-idea-of-smart-contracts/

Contracts eröffnen eine Vielzahl von Anwendungen über den originären Bereich der Kryptowährungen hinaus.[6]

Kernstück der Blockchain ist ein auf alle Nodes (Knoten) des Netzwerks verteiltes Transaktionsregister (Distributed Ledger). Alle Transaktionsdaten werden zwischen den Teilnehmern in einem Peer-to-Peer-Netzwerk geteilt.[7] Im Regelfall haben alle Teilnehmer dieses Netzwerks die gleichen Rechte, die gleichen Informationen und somit die gleichen Voraussetzungen, um an dem System teilzunehmen und neue Informationen beziehungsweise Transaktionen hinzuzufügen. Jeder Knoten speichert hierzu den gesamten Informationsbestand. Sollte ein Node gehackt oder Werte verändert worden sein, wird diese Abweichung vom gesamten System bemerkt. Die vollständige Redundanz der Datenbank schützt daher das System gegen einseitige Machtausübung, Ausfall und Manipulation.[8]

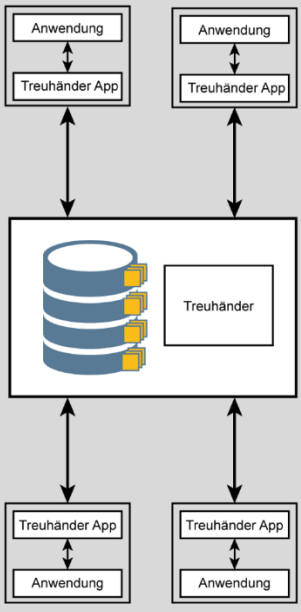

Abb. 1: Herkömmliche zentrale Architektur

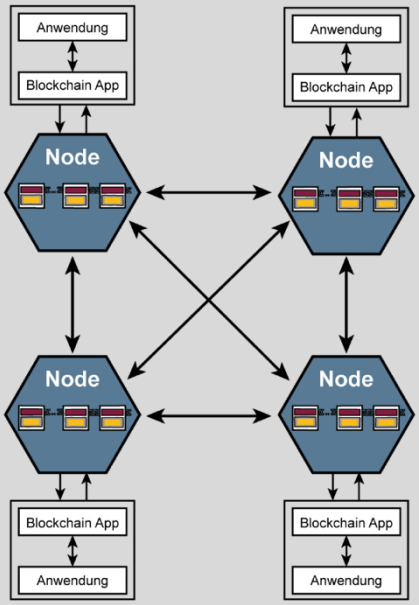

Abb. 2: Dezentrale Blockchain-Architektur

[6] Beispiele hierfür sind etwa Entscheidungsfindungsstrukturen (http://boardroom.to/#About) oder Streitschlichtungsmechanismen (https://www.bitrated.com/) auf Blockchain-Basis; eingehend zur letztgenannten Anwendung Ortolani, Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin, 36 Oxford J. Legal Studies 2016, S. 595-629; Kolain, Die Blockchain als „vollkommenes Gesetzbuch"?, Rechtshistorische Überlegungen zur Konfliktlösung in Smart Contracts, in: Hill/Martini/Kugelmann, Perspektiven der digitalen Lebenswelt, 2017, S. 147-162

[7] De Filippi, Journal of Peer Production, 2015, Issue 9, unter http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies/

[8] Siehe zur Funktionsweise auch Bechtolf/Vogt, ZD 2018, S. 66 f.; Martini/Weinzierl, NVwZ 2017, S. 1251; Heckelmann, NJW, 2018, S. 504 f.; Hofert, ZD 2017, S. 161 ff.

Ist eine bestimmte Anzahl von Transaktionen aufgelaufen, wird ein neuer Block berechnet. Hierfür wird ein Konsensverfahren genutzt. Das Konsensverfahren ist der entscheidende Baustein, um die Blockchain vor Manipulationen zu schützen. Es löst das so genannte Double-Spending-Problem[9], indem es verhindert, dass ein Teilnehmer einen Wert mehrfach transferiert – also zum Beispiel denselben *Bitcoin* einmal an Teilnehmer A sendet und danach ein weiteres Mal an Teilnehmer B. Erst wenn die Mehrheit der an das Peer-to-Peer-Netzwerk angeschlossenen Nodes sich über die Schaffung eines neuen Blocks einig ist, wird dieser validiert und an die zuvor erstellten Blöcke gehängt.

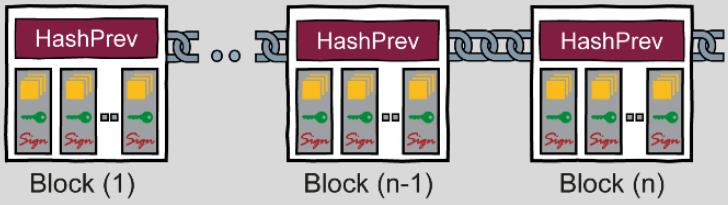

Abb. 3: Datenstruktur einer Blockchain

Um sich zu einigen, werden zuerst Vorschläge für neue Blöcke erarbeitet. Dies geschieht durch Validatoren (die bei der *Bitcoin*-Blockchain „Miner" genannt werden). Dann müssen sich die Beteiligten einigen, welcher vorgeschlagene Block tatsächlich in die Kette eingefügt wird. Die Validierung der Transaktionen und Informationen, bevor sie in die Blockchain-Datenbank geschrieben werden, erfolgt beispielsweise in einem rechenintensiven Verfahren mittels Proof-of-Work. Einem Verfahren, bei dem die Miner eine Rechenaufgabe lösen müssen und die gefundene Lösung von allen Teilnehmern im Netzwerk leicht verifiziert werden kann.[10]

Weitere Informationen zur Funktionsweise der Blockchain und der häufig verwendeten Begriffe finden Sie im Blockchain-Glossar unter: blockchain.eco.de

[9] Bereits gesehen von Chaum, 8 Sci. Am. 1992, S. 96-101.
[10] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, (Fn. 10), S. 2 im Hinblick auf den Proof-of-Work-Mechanismus; eingehend zu anderen Verifikationsmechanismen EZB, Virtual currency schemes – a further analysis, 2015, S. 10, unter https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

2.1. Typen unterschiedlicher Blockchains

Man unterscheidet in der Regel drei Typen von Blockchains: Öffentliche (public), private (private) und konsortiale (federated) Blockchains.[11] Völlig trennscharf ist diese Klassifizierung allerdings nicht: Es gibt auch Mischformen wie public-permissioned oder private-permissioned Blockchains.

A. Public Blockchain

Bei öffentlichen (public) Blockchains steht es jedem frei, sich an dem Netzwerk zu beteiligen. Die Teilnahme unterliegt keinerlei Kontrolle und jeder kann am Lesen, Schreiben und Verifizieren der Daten teilnehmen. Das macht public Blockchains offen und transparent, da jeder Teilnehmer innerhalb des Netzwerks zu einem beliebigen Zeitpunkt die Aufzeichnung überprüfen kann.[12] Die Entscheidungsfindung und die Verifizierung von Transaktionen erfolgt durch verschiedene Konsensmechansimen, wie dem Proof-of-Work oder Proof-of-Stake.[13] Öffentliche Blockchains sind beispielsweise *Bitcoin* oder *Ethereum*.

B. Private Blockchain

Eine private Blockchain – häufig auch permissioned Blockchain genannt – steht nur einem bestimmten Nutzerkreis zur Verfügung, zum Beispiel innerhalb eines Unternehmens. Im Gegensatz zur public Blockchain gibt es hier einen oder mehrere Verantwortliche, die sich um den Betrieb der Blockchain und den Zugang zu ihr kümmern.[14] In der Regel existiert auch ein System abgestufter Rechte. Es legt fest, welcher Nutzer welche Aktionen ausführen darf und Zugang zu bestimmten Daten erhält. Es sind alle denkbaren Konsensverfahren möglich; statt dem energie- und rechen-

[11] Näher Schwintowski/Klausmann/Kadgien, NJOZ 2018, S. 1401, 1403; Schrey/Thalhofer, NJW 2017, S. 1431, 1433.
[12] Schrey/Thalhofer, NJW 2017, S. 1431, 1433; Hofert, ZD 2017, S. 162 f.
[13] EZB, Virtual currency schemes – a further analysis, 2015 (Fn. 10), S. 10
[14] Evans, Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms, The University of Chicago Law School, Coase-Sandor Institute for Law and Economics Working Paper No. 685, S. 16, unter http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2424516

intensiven Proof-of-Work können auch weniger aufwändige Verfahren (Proof-of-Stake, Delegated Proof-of-Stake, Hashgraph, Proof-of-Authority etc.)[15] genutzt werden, die aber auch gleichzeitig einen Sicherheitsverlust mit sich bringen. Die private Blockchain ist streng genommen keine Blockchain im engeren Sinn, da es an dem zentralen Merkmal der dezentralen Datenspeicherung fehlt. Die Daten sind dennoch kryptographisch gesichert. Beispiele für private Blockchains sind Ripple[16] und Hyperledger[17]. Da *Ethereum* Open Source Software ist, kann der Code ohne Veränderung ebenfalls genutzt werden, eine private Blockchain aufzubauen. Private Blockchains bieten sich zur Implementierung in Unternehmen an, da es hier meist wichtig ist, dass die Daten nicht für jedermann frei zugänglich sind.

C. Konsortiale Blockchain

Die konsortiale oder auch federated Blockchain ist eine Erweiterung der privaten Blockchain. Hier ist mehr als eine Instanz für das Netzwerk verantwortlich. Meist ist es eine Gruppe von Unternehmen oder Organisationen, die zusammenarbeiten und Entscheidungen für den besten Nutzen des gesamten Netzwerks treffen. Konsens wird häufig mithilfe von Mehrheitsentscheidungen erzielt; bezüglich der Governance besteht ein großer Gestaltungsspielraum. Da die Sicherheit des Systems oft keine so große Rolle spielt wie bei public Blockchains, können viele Konsensverfahren eingesetzt werden, die eine schnelle und skalierbare Abwicklung von Transaktionen ermöglichen. Beispiele für konsortiale Blockchains sind *R3*[18], die *Energy Web Foundation*[19], *B3i*[20], *Enerchain*[21] und das Kooperations-Projekt deutscher Stromanbieter *ETH@Energy*[22].[23]

[15] Eine Übersicht der gängigen Konsensverfahren und ihrer Einsatzgebiete finden Sie unter https://www.bitfantastic.com/uebersicht-ueber-blockchain-konsensus-algorithmen/#Der-grosse-Nachteil.
[16] Siehe https://www.ripple.com/
[17] Siehe https://www.hyperledger.org
[18] Siehe https://www.r3.com
[19] Siehe https://www.energyweb.org/
[20] Siehe https://b3i.tech
[21] Siehe https://enerchain.ponton.de
[22] Siehe https://www.eth-energy.de
[23] Näher Werbach, 33 Berkeley Tech. L.J. 2018, S. 487, 490, 498 f., 536.

D. Alternative Systeme – Beispiel IOTA

IOTA (benannt nach dem kleinsten Buchstaben im griechischen Alphabet) ist ebenfalls ein System zur Durchführung digitaler Transaktionen. Obwohl *IOTA* häufig im Kontext Blockchain erwähnt wird, nutzt das System keine Blockchain auf Basis verketteter Blöcke. Bei *IOTA* werden Transaktionen in einem so genannten gerichteten azyklischen Graphen („Tangle“) erfasst. So sollen Transaktionskosten möglichst geringgehalten und eine bessere Skalierbarkeit gewährleistet werden. Der Absender bezahlt seine Transaktion im *IOTA*-Netzwerk mit entsprechender Rechenleistung (Proof-of-Work). So ist *IOTA* ein Distributed Ledger, ohne dass es eine Blockchain ist. Das System ist auf eine sichere Kommunikation und Zahlung zwischen Maschinen für IoT-Anwendungen ausgerichtet und wird von der *IOTA*-Stiftung verwaltet. Die Referenzsoftware ist Open Source. Die Sicherheit des Systems basiert teilweise auf einer zentralen Instanz, dem so genannten Coordinator.

2.2. Smart Contracts

Besonders großes Potenzial für disruptive Geschäftsmodelle bieten Smart Contracts.[24]

Smart Contracts sind Programme, die auf einer Blockchain ausgeführt werden. Ein Smart Contract ist im Prinzip ein Satz an Regeln für das Auslösen von Transaktionen – eine definierte Transaktion (Wenn-Bedingung) kann wiederum eine Transaktion (Dann-Folge) auslösen. Eine Transaktion kann hierbei sowohl eine Übermittlung von Daten (z.B. externer IoT-Sensor) oder eine Übermittlung von Kryptowährung sein.

Die Verschlüsselung und verteilte Speicherung in der Blockchain machen den Vorgang manipulationssicher und auditierbar. Smart Contracts sind nicht intelligent. Ein Smart Contract entwickelt sich nicht selbständig weiter oder passt den eigenen Code an neue Bedingungen an, wie beispielsweise eine künstliche Intelligenz.

[24] Näheres zur technischen Funktionsweise Heckelmann, NJW 2018, S. 504; Kaulartz/Heckmann, CR 2016, S. 618; Jacobs/Lange-Hausstein, ITRB 2017

Das Neue am Smart Contract ist: Er kann automatisiert Transaktionen im digitalen Raum ohne Intermediär abwickeln. Jede Transaktion ist öffentlich einsehbar. Und es ist nicht möglich, die Historie von Transaktionen zu modifizieren. Sobald ein Smart Contract ausgeführt ist, kann die Ausführung nicht mehr rückgängig gemacht werden. Das bedeutet: Ein Smart Contract ist ein Programm, das komplett autonom ausgeführt wird. Dafür sorgt die Dezentralität des Netzwerks. Eine steuernde Instanz, welche in den Programmablauf eingreifen könnte, existiert nicht – jedenfalls dann nicht, wenn der Smart Contract auf einer public Blockchain wie etwa *Ethereum* läuft.

So können Vertragspartner im Vorhinein festlegen, dass bei Regen an einem bestimmten Tag und Ort eine bestimmte Geldsumme ausgezahlt wird – dies wäre beispielsweise eine Anwendung in Form einer Schlechtwetterversicherung für Dreharbeiten. Die erforderlichen Wetterdaten kann der Smart Contract beispielsweise von einer internetfähigen Wetterstation ohne menschliches Zutun erhalten. Die Auszahlung der Versicherungssumme erfolgt über eine Blockchain-basierte Kryptowährung wie etwa *Bitcoin*. So kommt die Vertragsabwicklung gänzlich ohne zentrale Instanzen wie eine Versicherungsgesellschaft und ohne einen Sachbearbeiter aus, der den Eintritt des Schadensfalls manuell prüft. Smart Contracts können in der Regel nicht mehr von einzelnen Personen gestoppt werden, sobald sie einmal laufen – sie werden nach festgelegter Programmierung "stur" ausgeführt. Dies kann zu Konflikten mit zwingenden rechtlichen Vorgaben führen, die gegebenenfalls durch geeignete Einbettung in vertragliche Strukturen aufgefangen werden können.

Die bekannteste Blockchain für Smart Contracts ist die *Ethereum*-Blockchain. Diese Blockchain mit integrierter Programmiersprache stellt Entwicklern in einer offenen Plattform die Werkzeuge zur Verfügung, um selbst Smart Contracts zu entwickeln und in einer Blockchain zu verwenden. Die Erstellung von Smart Contracts war von Anfang an fester Bestandteil der Technologie. Darin unterscheidet sich *Ethereum* am stärksten von der *Bitcoin*-Blockchain. Mittlerweile gibt es aber auch Smart-Contract-Lösungen für die *Bitcoin*-Blockchain[25] und Chain-übergreifende Ansätze[26].

[25] Siehe nur Ortolani, Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin, 36 Oxford J. Legal Studies 2016, S. 595-629.
[26] Näher Kolain/Wirth, MultiChain-Governance, in: Taeger, Jürgen (Hrsg.), Recht 4.0, Innovationen aus den rechtswissenschaftlichen Laboren, 2017, S. 833-845.

2.3. Schnittstellen und Wallets

Jede Blockchain-Anwendung benötigt eine Anbindung an die reale Welt – Transaktionen müssen veranlasst, Guthaben gespeichert und Daten für die Auslösung von Aktionen in die Blockchain übermittelt werden. Die Handhabung und Verwaltung von Werteinheiten auf einer Blockchain erfolgt in der Regel über so genannte Wallets – also Softwareprogramme, die den Bestand von Kryptowährungen verwalten und die Übermittlung von Währungseinheiten an andere Teilnehmer ermöglichen. Ein Wallet ist hierbei nicht nur für die Nutzer erforderlich, die einen Betrag X von A nach B übermitteln wollen. Über ein Wallet wird auch der Betrieb einer public Blockchain bezahlt, die für ein Projekt eingesetzt wird. Denn in der Regel kostet jede Transaktion, die über eine public Blockchain abgewickelt wird, einen bestimmten Betrag – ähnlich einer Transaktionsgebühr – in der jeweiligen Kryptowährung. Hier gibt es mittlerweile eine Vielzahl von Anbietern und Handelsplattformen[27], so dass an dieser Stelle keine eigenen Entwicklungen mehr notwendig sind.

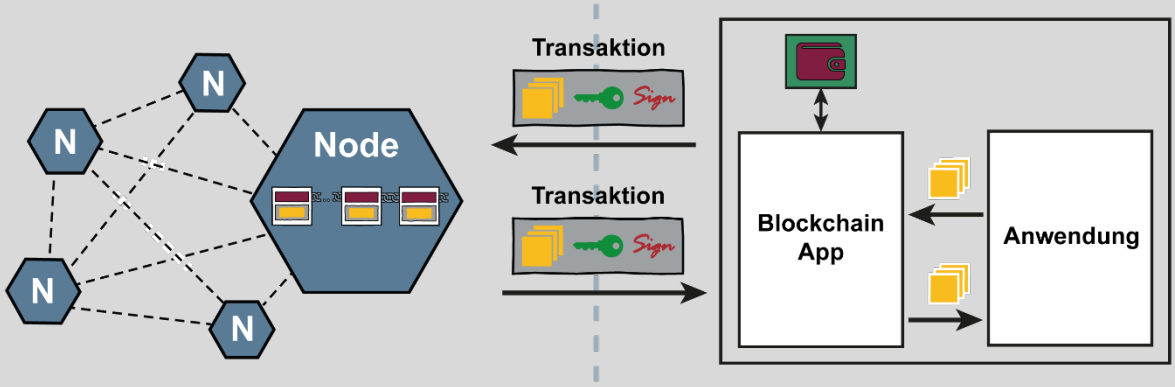

Abb. 4: Schnittstellen zwischen Blockchain-Infrastruktur und Blockchain-Anwendung

Eine weitere Schnittstelle nach außen ist notwendig, wenn externe Datengeber angeschlossen werden sollen, die Aktionen eines Smart Contract auslösen. Hierzu laufen derzeit eine Reihe von Initiativen zur Normierung von Standards, beispielsweise die DIN SPEC 3103 "Smart Contracts und

[27] Siehe https://www.btc-echo.de/tutorial/wallet-bitcoins-sicher-aufbewahren/

Sensoren in Blockchains für Industrie 4.0-Anwendungen".[28] Die Standardisierung wird international auch durch ISO vorangetrieben; hier wurde 2016 ein Technisches Komitee zu "*Blockchain und Distributed Ledger Technologies*" gegründet, welches derzeit die Entwicklung von elf Standards vorantreibt.[29]

Sinnvoll ist es, sich an vorhandenen Curricula für Blockchain-Entwickler zu orientieren, die online verfügbar sind.[30]

Unternehmen, die selbst nicht über eine ausreichende interne Expertise zum Einsatz der Blockchain-Technologie verfügen, können auf einen externen Dienstleister zurückgreifen, der idealerweise bereits mehrere Blockchain-Projekte erfolgreich umgesetzt hat.

2.4. Grenzen der Blockchain-Technologie

Die Blockchain ist kein Allheilmittel. Sie kann bestimmte Prozesse beschleunigen und effizienter gestalten und sie ermöglicht die Umsetzung von Prozessen und Use-Cases, die zuvor nicht möglich waren. Aber es gibt Grenzen: Die Transparenz öffentlicher Blockchains kann in bestimmten Szenarien ein Problem darstellen. Wenn sensible oder geschäftsrelevante Daten geteilt werden, sollte unter Umständen erwogen werden, dies in einer geschützten Umgebung zu tun, den Nutzerkreis klar zu definieren und entsprechend einzugrenzen. Für diesen Fall eignet sich eventuell eine private oder eine konsortiale Blockchain. Es gibt auch technische Hürden: Die Rechenleistung von Miniaturrechnern ist für den Betrieb einer Node oft unzureichend, weshalb der Miniaturisierung, insbesondere im IoT-Bereich, derzeit noch Grenzen gesetzt sind. Auch im Hinblick auf die Skalierbarkeit, also die Verarbeitung einer großen Zahl von Transaktionen in kurzer Zeit, gibt es derzeit, insbesondere bei public Blockchains, noch Beschränkungen.[31]

---

[28] Siehe https://www.din.de/de/wdc-beuth:din21:287248829
[29] Siehe https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0,
[30] Röder, Curriculum für Blockchain-Entwickler, 2018, Computerwoche 2018, unter https://www.computerwoche.de/a/curriculum-fuer-blockchain-entwickler, 3545842
[31] Hofert, Regulierung der Blockchains, 2018, S. 46 ff.; Fairfield, 88 S. Cal. L. Rev. 2015, S. 805, 828 ff.; Croman et al., On Scaling Decentralized Blockchains, A Position Paper, 2016, unter http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf

Hinzu kommen rechtliche Herausforderungen, wenn beispielsweise in der Blockchain personenbezogene Daten verarbeitet werden.[32]

Es sollte immer geprüft werden, ob ein Projekt wirklich eine Blockchain braucht. In vielen Fällen lassen sich die Funktionen auch mit bekannten technischen Lösungen abbilden.

3. Die Blockchain im Mittelstand – Voraussetzungen und Herausforderungen

Automatisierte Transaktionen und Wertschöpfungsketten sind vor allem für kleine und mittelständische Unternehmen interessant. Sie eröffnen Unternehmen die Möglichkeit, sich zusammenzuschließen und zu vernetzen, um dadurch verlässlich, automatisiert und flexibel zu produzieren und Transaktionen abzuwickeln. Darüber hinaus birgt die Blockchain-Technologie das Potenzial für automatisierte Austausch- und Abrechnungsprozesse sowie die Verfolgung von Lieferketten und Produktionsdaten. Ein weiteres Einsatzgebiet ist die Ausgabe eigener Kryptowährungen als Finanzierungsinstrument für definierte Projekte oder eigene Crowdfunding-Ansätze mit sogenannten Initial Coin Offerings (ICOs).[33]

Bei allem Potenzial der Technologie gibt es derzeit nur wenige Mittelständler, die die Blockchain-Technologie für eigene Produkte und Prozesse einsetzen. Ein Grund dafür ist die Komplexität der Technologie: Um eine Vorstellung von den Möglichkeiten, Einsatzszenarien und auch Hürden zu bekommen, ist eine intensive Auseinandersetzung mit dem Thema erforderlich. Bislang gibt es nur wenige Standards beziehungsweise Normen, die Orientierung geben. Viele Entwicklungen werden von einem kleinen Kreis von Enthusiasten vorangetrieben. Trotzdem gibt es eine Reihe von Unternehmen, die bereits Projekte umsetzen, wie beispielsweise das Zertifikats-managementsystem der *CERTIVATION GmbH*[34], die *Deutsche Bahn AG* mit

[32] Siehe für datenschutzrechtliche Implikationen Schrey/Thalhofer, NJW 2017, S. 1431; Hofert, ZD 2017, S. 161; Bechtolf/Vogt, ZD 2018, S. 66; Pesch/Böhme, DuD 2017, S. 93.
[33] Näher Kaulartz/Matzke, NJW 2018, S. 3278; Borkert, ITRB 2018, S. 39; Weitnauer, BKR 2018, S. 231.
[34] Siehe https://www.certivation.com

der Blockchain-basierten Einnahmeaufteilung[35] oder die *AXA Versicherung* mit der automatischen Flugkostenerstattung *FIZZY*[36].

Jedoch eignen sich nicht alle Projekte für den Einsatz von Blockchains. Und auch dort, wo die Blockchain grundsätzlich Sinn macht, sollte sich jedes Unternehmen zuvor einige wichtige Fragen stellen und beantworten, welche dieses Arbeitspapier im Folgenden kurz erläutert.

3.1. Welche Voraussetzungen müssen vor dem Einsatz der Blockchain geschaffen werden?

Vor Beginn eines Blockchain-Projekts sollte zunächst geklärt werden, ob der Einsatz der Technologie wirklich Vorteile gegenüber anderen Möglichkeiten der Umsetzung bringt. Interne Anwendungen könnten vielleicht besser mit konventioneller Datenbank-Technologie umgesetzt werden. Anwendungsfälle für die Blockchain finden sich oft in Multistakeholder-Szenarien, in denen die Nachvollziehbarkeit und Verifizierbarkeit des Datenaustauschs beziehungs-weise der Transaktionen wichtig ist.

Für die erfolgreiche Umsetzung eines Blockchain-Projekts ist im zweiten Schritt wesentlich, dass die für das Projekt am besten geeignete Blockchain identifiziert wird. Alle derzeit am Markt verfügbaren Lösungen haben ihre Vor- und Nachteile und die Auswahl hängt von der geplanten Anwendung, der Zahl der Beteiligten, der gewünschten Skalierbarkeit und Geschwindigkeit und der erforderlichen Anbindung an bereits vorhandene Systeme ab. Handelt es sich um ein unternehmensinternes Projekt, fällt die Wahl wahrscheinlich auf eine private Blockchain. Für die Zusammenarbeit von Unternehmen, beispielsweise entlang einer Supply-Chain, dürfte hingegen eine konsortiale Blockchain die erste Wahl sein. Falls innerhalb des Unternehmens nicht ausreichend Expertise für die Beurteilung vorhanden ist, können spezialisierte Beratungsunternehmen bei der Entscheidung und Durchführung des Projekts Unterstützung leisten.

[35] Siehe https://www.deutschebahn.com/de/Digitalisierung/technologie/Neue-Technologien/blockchain-3241170
[36] Siehe https://www.fizzy.axa

3.2. Wie teuer ist ein Blockchain-Projekt?

Auch wenn es sich bei vielen Blockchain-Infrastrukturen um Open-Source-Projekte handelt, ist die Nutzung nicht vollkommen kostenfrei: Wie bereits beschrieben, kostet bei public Blockchains wie *Bitcoin* oder *Ethereum* jede Transaktion einen bestimmten Betrag an Kryptowährung.[37] Wer eine private Blockchain nutzt, muss selbst für die Infrastruktur aufkommen und die Kosten für Hardware und Energiebedarf tragen oder auf eine der mittlerweile verfügbaren "Blockchain-as-a-Service"-Angebote zurückgreifen – dazu mehr im Abschnitt 3.5.

Gerade die schwankenden Transaktionskosten von public Blockchains stellen durchaus ein Risiko dar. Unternehmen, die auf konstante Kosten für den Eintrag ihrer Daten in die Blockchain angewiesen sind, sollten die Nutzung einer öffentlichen Blockchain sehr genau abwägen und stattdessen eine private Blockchain oder Blockchain-Alternativen, wie beispielsweise *IOTA*, in Erwägung ziehen. In einer public Blockchain kann es sein, dass aufgrund einer steigenden Anzahl von Transaktionen in der Blockchain die Transaktionskosten drastisch steigen und der Eintrag nicht mehr 0,01 Cent, sondern 5 Euro kostet. In einer öffentlichen Blockchain ist es zudem in der Regel so, dass die Transaktionen von den Minern dann priorisiert werden, wenn der für die Transaktion offerierte Betrag hoch ist – wer im Mittelfeld bietet, landet dann eben nicht ganz vorne auf der Liste und die Transaktion dauert länger. Mit Lightning und Raiden wird hier aber bereits bei den großen und etablierten Blockchain-Technologien aktiv daran gearbeitet, ein deutlich größeres Transaktionsvolumen beherrschen zu können (vgl. Abschnitt 2). Sind erst einmal mehr als eine Million Transaktionen pro Sekunde möglich, werden auch die Transaktionskosten noch weiter sinken.

[37] Siehe etwa für eine historische Übersicht über die Transaktionsgebühren im System Bitcoin https://bitcoinfees.info.

3.3. Wie effizient ist die Blockchain?

Das Potenzial der Blockchain-Technologie für effizientere Ressourcennutzung und niedrigere Betriebskosten hängt maßgeblich vom jeweils verwendeten Blockchain-Typ ab (vgl. Abschnitt 2.1). Die bekanntesten Blockchains – die Kryptowährungen *Bitcoin* und *Ether* – setzen zur Validierung der Transaktionen auf das sogenannte Proof-of-Work-Verfahren, welches extrem sicher ist, aber einen hohen Rechen- und damit Energiebedarf hat und nur eine begrenzte Anzahl Transaktionen pro Zeiteinheit zulässt. Als Alternativen zum Proof-of-Work-Verfahren wurden alternative Validierungsverfahren (beispielsweise Proof-of-Authority und Proof-of-Stake) entwickelt. Diese sind rechen- und damit energieeffizienter, setzen aber mehr Vertrauen in die Administratoren oder die beteiligten Akteure voraus. Hier besteht ein Zielkonflikt, da hohe Sicherheit bislang durch einen hohen Energieverbrauch mithilfe des Proof-of-Work-Verfahrens erkauft wird.[38] Natürlich widerspricht es der Kernidee der Blockchain-Technologie, wieder einige Netzwerkteilnehmer mit erweiterten Berechtigungen auszustatten (beispielsweise Proof-of-Authority) oder anderen Stakeholdern den Zugang zur Blockchain zu verwehren (beispielsweise private und permissioned Blockchains). Wie im Abschnitt 4 zum Thema Datenschutz in Blockchain-Systemen näher beschrieben, können solche Anpassungen die Rechtssicherheit erhöhen, da Verantwortlichkeiten mit entsprechender Haftung definiert werden.

Besonders hohe Effizienzgewinne lassen sich vor allem dort realisieren, wo die Blockchain manuelle Prozesse durch automatisierte Prozesse ersetzt beziehungsweise die Funktion eines selbständigen Dritten, wie etwa eines Treuhänders oder einer Zertifizierungsstelle, übernimmt. In diesen Fällen fallen oft selbst hohe Transaktionskosten nicht weiter ins Gewicht, da eine komplette Wertschöpfungsstufe – und damit auch Kostenstelle – entfällt.[39]

[38] Siehe für eine Übersicht über die Verifikationsmechanismen EZB, Virtual currency schemes – a further analysis, 2015 (Fn. 10), S. 10.
[39] Weltwirtschaftsforum, The future of financial infrastructure – An ambitious look at how blockchain can reshape financial services, 2016 (Fn.1).

3.4. Middleware und Plattformen – Status Quo

Viele Open-Source-Projekte sowie zahlreiche große Hersteller und Serviceprovider bieten professionellen Support für Distributed-Ledger-Technologie-Plattformen an. So hat beispielsweise *Amazon* unlängst eigene Vorlagen für die unkomplizierte Bereitstellung von verschiedenen Blockchain-Netzwerken und die notwendigen Entwicklertools in die hauseigene *Amazon Web Services (AWS)* Plattform integriert.[40] *Microsoft* geht mit dem Blockchain-as-a-Service unter *Azure*[41] einen ähnlichen Weg (vgl. Abschnitt 3.5).

Für alle populären Programmiersprachen stehen inzwischen passende Frameworks zur Verfügung. Webentwickler finden sich mit *web3js* schnell im *Ethereum*-Netzwerk zurecht. Das von *IBM* und anderen großen Firmen getriebene Hyperledger-Konsortium setzt mit seinem Chaincode auf eine Basis aus Go, node.js und das im Enterprise-Umfeld etablierte Java.

Doch nicht nur öffentliche Distributed-Ledger-Systeme sind gefragt. Das Berliner Start-Up *BigchainDB* stellt mit seinem gleichnamigen Produkt eine Komponente zur Verfügung, die sich wie ein Drop-In Replacement für eine Datenbank verhält.[42] Das bedeutet, *BigchainDB* verhält sich wie eine Datenbank, aber mit den Eigenschaften einer Blockchain. Legacy-Systeme profitieren davon, da die notwendigen Anpassungen in der Regel deutlich geringer ausfallen.

Daraus ergibt sich insbesondere für den Mittelstand eine Reihe von Vorteilen für den Einstieg in die Technologie:

- Mittelständler sollten in Wertschöpfungsnetzwerken darauf achten, nicht zu spezifisch in eine spezielle proprietäre Blockchain-Architektur eines einzelnen großen Anbieters zu investieren, um einer Hold-Up-Situation vorzubeugen.
- Ein Lösungsansatz kann sein, aus bestehenden Wertschöpfungs-netzwerken heraus frühzeitig Konsortien zu gründen, die sich mit der Implementierung von Blockchain-Lösungen, wie beispielsweise im Supply-Chain-Management, beschäftigen. So können mittelständische Unternehmen im Konsortium an der Entwicklung der

[40] Siehe https://aws.amazon.com/de/partners/blockchain
[41] Siehe https://azure.microsoft.com/de-de/solutions/blockchain/
[42] Siehe https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

Blockchain-Lösung mitwirken, sich den Aufwand im Konsortium teilen und Abhängigkeitsverhältnisse vermeiden.
- Bilden Sie eigene technische Mitarbeiter in entsprechenden Ausbildungsformaten[43] weiter, oder treten Sie entsprechenden Interessensverbänden[44] und Arbeitsgruppen[45] bei, um Kompetenzen aufzubauen. Schöner Nebeneffekt: Sie erhöhen Ihre Attraktivität als innovativer Arbeitgeber bei IT-Fachkräften.

3.5. Usability und Blockchain-as-a-Service (BaaS)

Blockchain-as-a-Service (kurz BaaS) ermöglicht einen relativ günstigen und schnellen Einstieg in Distributed-Ledger-Technologien. Die Infrastruktur kann mit dem Bedarf wachsen und meist stehen bei diesen Services dedizierte Ansprechpartner zur Verfügung. Insbesondere Pilotprojekte profitieren davon, da sie sich auf den Mehrwert von Distributed-Ledger-Technologie für das Geschäftsmodell konzentrieren können – die Technologie wird bereits lauffähig und getestet zur Verfügung gestellt.

Daraus ergeben sich insbesondere für den Mittelstand eine Reihe von Vorteilen, die den Einstieg in die Technologie vereinfachen:

- Es ist weniger IT-Kompetenz im eigenen Unternehmen erforderlich. Daher sind BaaS-Angebote vor allem für kleine und mittelständische Unternehmen wichtig und nützlich, wenn eigene Fachkräfte fehlen.
- Die Blockchain-Lösung kann einfacher implementiert werden.
- Es ist zu erwarten, dass die Usability der BaaS-Angebote schnell steigt, da es einen Wettbewerb unter den Anbietern gibt.

BaaS Angebote können aber auch Nachteile für den Mittelstand haben:

- Geringere Flexibilität bei der Ausgestaltung der Blockchain-Lösung.
- Abhängigkeit von den großen Plattformanbietern (genau diese Abhängigkeit sollte die Blockchain ja eigentlich überwinden).

[43] Ausbildung zum qualifizierten Blockchain-Entwickler TüV Rheinland Akademie https://www.maibornwolff.de/blockchain-development-school
[44] Siehe https://www.eco.de/themen/blockchain/
[45] EAM Gremium und Arbeitsgruppe mit Bezug zu DLT https://www.cba-lab.de

Wann eine BaaS-Lösung in Frage kommt:

- BaaS-Angebote ermöglichen einen schnellen und einfachen Einstieg in die Blockchain-Technologie.
- BaaS-Angebote können gut als Testumgebungen für Blockchain-Lösungen im Unternehmen genutzt werden, da BaaS-Lösungen mit weniger Investitionsrisiko verbunden sind.
- Wenn sich der Blockchain-Einsatz in der BaaS-Phase als sinnvoll im Unternehmen erweist, können Sie mittel- bis langfristig den Aufbau eigener Kompetenzen für originäre Blockchain-Lösungen anstreben, da diese flexibler und langfristig günstiger sind und die Abhängigkeit von einem Anbieter verringert wird.

3.6. Interoperabilität

Wie häufig bei der Einführung neuer Software und IT-Systeme, erfordert der Einsatz einer Blockchain in vielen Fällen Anpassungen an bestehenden Anwendungen und Systemen. Dabei werden viele unterschiedliche Technologien und Kommunikationsprotokolle verwendet. Regelmäßig kommen neue Werkzeuge hinzu. Standards etablieren sich derzeit jedoch noch langsam. Eine Herausforderung ist, mit der schnellen Entwicklung Schritt zu halten.

Die Blockchain hat das Potenzial, einige Branchen maßgeblich zu revolutionieren. Die Automobilindustrie, Banken, Retail (beispielsweise Nahrungsmittel und Textil) oder auch der Energiesektor untersuchen aus diesem Grund intensiv die Auswirkungen von Blockchain-Technologien auf bestehende Geschäftsmodelle und die existierende technische Infrastruktur. Der Anhang I gibt einen Überblick zu einer Reihe weiterer Blockchain-Anwendungen.

Handlungsempfehlungen für den Mittelstand:

Ein insbesondere im Mittelstand häufig genannter Hinderungsgrund für die Adaption lässt sich unter dem Stichwort „Interoperabilität" zusammenfassen. Interoperabilität bezeichnet die Fähigkeit zur Zusammenarbeit von verschiedenen Systemen, Techniken oder Organisationen.[46]

Je mehr Distributed-Ledger-Technologien in Softwarearchitekturen Einzug halten, desto wichtiger wird also die Standardisierung gemeinsamer Schnittstellen und Protokolle, um eine hohe Interoperabilität zwischen Bestandssystemen und einem Blockchain-Netzwerk zu gewährleisten. Die Herausforderung der Interoperabilität ist jedoch nicht Blockchain-spezifisch, sondern ist für die Einführung neuer Software- und Datenbanksysteme so gut wie allgemeingültig.

3.7. Standardisierung

Es ist eine Hürde für kleine und mittelständische Unternehmen, dass sich die Technologie noch in der Entwicklungsphase befindet. Es ist nicht klar, wie die Blockchain-Systeme der Zukunft aussehen werden. Bisher hat sich kein nationaler oder internationaler Standard für die Implementierung herauskristallisiert.

Bestrebungen, offizielle Standards einzuführen, existieren aber durchaus. Beispielsweise arbeitet die *ISO* seit 2016 unter deutscher Beteiligung (der *DIN-Normenausschuss Informationstechnik und Anwendungen, NIA*) an der Ausarbeitung und Etablierung von ISO/TC 307 als Standard für Blockchain.[47] Auch das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* hat inzwischen zwei Papiere veröffentlicht, in denen es Konzepte und Anforderungen an die Technologie bewertet.[48]

[46] Zur Interoperabilität von Blockchains Kolain/Wirth, MultiChain-Governance, in: Taeger, Jürgen (Hrsg.), Recht 4.0, Innovationen aus den rechtswissenschaftlichen Laboren, 2017, S. 833-845.
[47] International Organization for Standardization, ISO/TC 307 – Blockchain and distributed ledger technologies, unter https://www.iso.org/committee/6266604.html.
[48] Bundesamt für Sicherheit in der Informationstechnik, Blockchain sicher gestalten – Eckpunkte des BSI, Version 2.0, unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Eckpunktepapier.pdf?__blob=publicationFile&v=3 und Bundesamt für Sicherheit in der Informationstechnik, Blockchain sicher gestalten – Konzepte, Anforderungen, Bewertungen, unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=5

Noch ist allerdings nicht garantiert, dass verschiedene Blockchain-Architekturen ausreichend zueinander kompatibel sein werden.

Fazit für den Mittelstand:

Gerade für mittelständische Unternehmen resultiert daraus ein gewisses Risiko kostspieliger Fehlinvestitionen und die Gefahr einer Hold-Up Situation. Gleichzeitig sollte bei der Frage nach Standards der Innovationseffekt nicht vernachlässigt werden: Findet eine zu frühe Festlegung auf Standards statt, besteht die Gefahr, dass Innovationen gehemmt werden. Es besteht folglich immer ein gewisser Trade-Off zwischen Innovation und Standardisierung.

4. Sicherheit und Datenschutz

Eine Schlüsselfrage bei der Einführung neuer Software und Systeme in Unternehmen – spätestens, wenn es um den Produktivbetrieb geht – ist die Sicherheit. Daher soll im Folgenden auf einige Sicherheitsaspekte eingegangen werden, die es zu beachten gilt, wenn Sie den Einsatz von Distributed-Ledger-Technologien im eigenen Unternehmen planen oder in Erwägung ziehen.

4.1. IT-Sicherheit

Die Blockchain-Technologie kann bereits vorhandene IT-Sicherheits-probleme in mittelständischen Unternehmen nicht lösen. Die Architektur der Blockchain gewährleistet zwar eine systeminhärente Sicherheit beim Datenaustausch, allerdings bestehen weiterhin die Sicherheitsrisiken an den Endpunkten, das heißt bei den mit der Blockchain verknüpften Systemen und Endgeräten. Bewahren diese die übermittelten Daten in entschlüsselter Form außerhalb der Blockchain auf, ist die Gefahr von Datendiebstahl ungemindert. Somit erübrigen sich in den vorhandenen Systemen die

Basissicherheitsmaßnahmen, wie beispielsweise Virus- und Malware-Schutz, professionelles Rechtemanagement oder Authentifizierung, durch die Blockchain-Technologie keineswegs.[49]

Die klassischen Fragen der IT-Sicherheit für herkömmliche Systeme bleiben auch für die Blockchain-Technologie relevant: Hardware- und Software-Sicherheit, Bugs, sichere Authentifizierung, Passwortsicherheit, Schlüssel und ihre Verwaltung, Protokolle etc. Sicherheitskritisch sind insbesondere die Schnittstellen zur realen Welt.

Die Kryptographie ist eines der Kernelemente der Blockchain-Technologie. Ebenso wie die Technologie der Kryptographie, entwickelt sich auch die Technologie zum Brechen der Kryptographie weiter. Kryptoalgorithmen, die heute noch sicher sind, können in Zukunft sehr wahrscheinlich geknackt werden. Wie für andere Technologien auch, besteht daher für Blockchain-Anwendungen die Notwendigkeit, Kryptoalgorithmen austauschen zu können. Dies lässt sich bei private Blockchains einfacher umsetzen als bei public Blockchains, wo stets eine Abstimmung in der jeweiligen Community notwendig ist.

In großen Netzwerken mit vielen Nodes muss außerdem grundsätzlich davon ausgegangen werden, dass alte Daten, mit dann nicht mehr sicherer Kryptographie geschützt, als Kopie bei einem oder mehreren Nodes weiterhin bestehen bleiben und vorhanden sind. Vor diesem Hintergrund unterscheidet sich die Blockchain-Technologie in Fragen der IT-Sicherheit kaum von anderen Systemen.

4.2. „Garbage In – Garbage Out" Problematik

Wer kontrolliert die Daten, die in der Blockchain abgespeichert werden? Um das Risiko von Betrug oder menschlichem Versagen bei der Übertragung der Daten auf die Blockchain zu vermindern, kommt unter anderem der Qualität

[49] Hierzu und zum Folgenden Bundesamt für Sicherheit in der Informationstechnik, Blockchain sicher gestalten – Eckpunkte des BSI, Version 2.0 (Fn. 31) und Bundesamt für Sicherheit in der Informationstechnik, Blockchain sicher gestalten – Konzepte, Anforderungen, Bewertungen; Pohlmann, 2019, Cyber-Sicherheit - Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, Springer Vieweg Verlag, Wiesbaden.

der Datenerfassung und der Sensorik eine wichtige Rolle zu. Grundsätzlich ist es sehr wichtig, wie Daten aus der realen Welt in die Blockchain kommen. Hier müssen Korrektheit, Konsistenz, Authentizität und Vollständigkeit stets gewährleistet werden. In Produktionsprozessen sollten idealerweise Sensoren die Daten erfassen und automatisch an die Blockchain senden.

Die Blockchain-Technologie sollte daher in Bezug auf die Digitalisierung des Mittelstands nicht isoliert gedacht und betrachtet werden. Erst in Verknüpfung mit der Automatisierung beziehungsweise Sensorik können Blockchains ihr volles Potenzial entfalten und die Datenintegrität sicherstellen. Der Einsatz von Distributed-Ledger-Technologie eignet sich für Unternehmen, die bereits einen gewissen Digitalisierungsgrad erreicht haben.

Eine Herausforderung für mittelständische Unternehmen beim Einsatz von Blockchains im Supply-Chain-Management liegt darin, dass die Übertragung der Daten auf die Blockchain auf der ersten Wertschöpfungsstufe, also „upstream", erfolgen muss. Gerade diese Wertschöpfungsstufen sind aber häufig am geringsten digitalisiert. Ein gutes Beispiel ist die Nahrungsmittelindustrie. Soll beispielsweise bei einem Fertiggericht ad hoc nachvollziehbar sein, von welchen Erzeugerbetrieben die verwendeten Zutaten stammen, müssen die Daten von jedem einzelnen Landwirt in die Blockchain geschrieben werden. Um die Wahrscheinlichkeit des Betrugs und menschliches Versagen auszuschließen, sollte im Ernteprozess der Datentransfer auf die Blockchain automatisch durch Sensoren erfolgen. Dafür ist ein gewisser Digitalisierungsgrad auf den Upstream-Ebenen erforderlich. Nur wenn über die gesamte Wertschöpfungskette hinweg die nötige digitale Infrastruktur in Form von automatischer und qualitätsgesicherter Datenerfassung beziehungsweise Sensorik gegeben ist, kann die „Garbage In – Garbage Out"-Problematik gelöst werden. In längeren, komplexen Wertschöpfungsketten können nur die großen Marktakteure ausreichend Druck aufbauen, um alle Beteiligten zu einer Implementierung der nötigen digitalen Infrastruktur zu bewegen.

Auch bei der Erfassung von Gegenständen, um beispielsweise ihre Herkunft zu dokumentieren, stellt sich die gleiche Herausforderung für das initiale „Root-Zertifikat": Wann wird ein materielles Gut zum ersten Mal digital gekennzeichnet und erfasst? Und wer wird sich als Zertifizierungsstelle für Blockchain-Einträge etablieren und damit eine vertrauenswürdige Basis für die Verwendung der Technologie schaffen? Für digitale Güter ist das recht

einfach; Güter in der realen Welt müssen dagegen eindeutig identifizierbar und beschreibbar sein.

Fazit für den Mittelstand:

Nicht alle Anwendungsszenarien sind geeignet, auf Basis einer Blockchain umgesetzt zu werden. Daher ist es ratsam, probeweise Prototypen zu bauen, zu testen, zu verbessern oder aber auch einen nicht weiterführenden Ansatz zu verwerfen und neu zu bauen.

4.3. Datenschutzrecht

Wie bei anderen Systemen auch, ist der Umgang mit sensiblen oder personenbezogenen Daten in Blockchains sicherheitsrelevant. Schließlich sind Blockchains häufig öffentlich (public).

4.3.1. Anwendungsbereich

In einer Blockchain gespeicherte Daten können personenbezogene Daten darstellen und damit den Anwendungsbereich der Datenschutzgrundverordnung (DSGVO) eröffnen.[50] Personenbezogene Daten sind im Rahmen der DSGVO alle Informationen, die sich auf eine bestimmte natürliche Person beziehen oder beziehbar sind. Sogenannte pseudonyme Daten – also Daten, die selbst keine Identifizierung zulassen, für die aber eine Zuordnungsregel existiert – gelten ebenfalls als personenbezogene Daten. Vollständig anonyme Daten fallen nicht unter die DSGVO.

Damit gilt, dass sowohl Zugangsschlüssel (Public Keys), sonstige als Payload in einer Blockchain gespeicherte Daten sowie Hashwerte (ggf. pseudonyme)

[50] Näher Hofert, ZD 2017, S. 161, 163 f.; Bechtolf/Vogt, ZD 2018, S. 66, 68 f.; Martini/Weinzierl, NVwZ 2017, S. 1252 ff.; Schrey/Thalhofer, NJW 2017, S. 1431, 1433.

personenbezogene Daten darstellen können. Eine Verschlüsselung der Daten führt nicht automatisch aus dem Anwendungsbereich der DSGVO heraus.[51]

Wichtig ist die Frage des Personenbezugs, weil bei einer Verarbeitung personenbezogener Daten zahlreiche rechtliche Pflichten zu beachten sind. In vielerlei Hinsicht scheint die Blockchain-Technologie nicht kompatibel mit dem derzeitigen datenschutzrechtlichen Regelungsmodell zu sein. Die Möglichkeit, Blockchain-Projekte auf anonymer Basis zu gestalten, ist damit von erheblicher Bedeutung.

4.3.2. Datenschutzrechtliche Einordnung von Teilnehmern

Die DSGVO kennt drei Kategorien von Akteuren:

- Verantwortliche, welche Umfang, Art und Weise der Datenverarbeitung bestimmen;
- Auftragsverarbeiter, die weisungsgebunden bestimmte Datenverarbeitungen für den Verantwortlichen übernehmen, und
- Betroffene, das sind solche Individuen, deren personenbezogene Daten verarbeitet werden.

Ein verteiltes System wie eine public Blockchain ist in diese starre Kategorisierung nur mit Schwierigkeiten einzubinden. Bei einer öffentlichen Blockchain stellen sich dementsprechend zahlreiche Fragen im Hinblick auf den Umgang mit regulatorischen Vorgaben – angefangen bei der Frage, wer eigentlich "Verantwortlicher" im Sinne des Datenschutzrechts ist.[52]

Der *Blockchain Bundesverband e.V.*[53] schlägt daher beispielsweise vor, Nodes als Infrastruktur – ähnlich einem Internet Service Provider (ISP) oder einem Hosting-Anbieter – und somit nicht als datenschutzrechtlich relevanten Akteur einzustufen, sondern diesen datenschutzrechtliche Neutralität zu gewähren. "Verantwortlich" im datenschutzrechtlichen Sinne wäre dann

[51] Bechtolf/Vogt, ZD 2018, S. 66, 68 f.; Hofert, ZD 2017, S. 161, 163; Spindler/Bille, WM 2014, S. 1357, 1366 f.
[52] Erbguth/Fasching, ZD 2017, S. 560; Martini/Weinzierl, NVwZ 2017, S. 1251, 1253 ff.; Saive, CR 2018, S. 186.
[53] Siehe https://bundesblock.de

lediglich der Anbieter einer Anwendung, die mit der Blockchain interagiert.[54] Eine solche Handhabung ist wünschenswert, erfordert aber Anpassungen im Datenschutzrecht beziehungsweise eine – allerdings nur in Grenzen mögliche – entsprechende richterliche Rechtsfortbildung.

Allerdings bietet die DSGVO auch in ihrer derzeitigen Fassung Optionen, um vermeintliche Konflikte aufzulösen: Beispielsweise kann die Figur der "Gemeinsamen Verantwortlichkeit" (Art. 26 DSGVO) für die Governance einer private Blockchain durchaus nutzbar gemacht werden. Auch bieten Auftragsverarbeitungsverhältnisse einige Gestaltungsmöglichkeiten, etwa im Verhältnis zwischen dem Anbieter einer Blockchain-basierten Anwendung und den einzelnen Nodes.

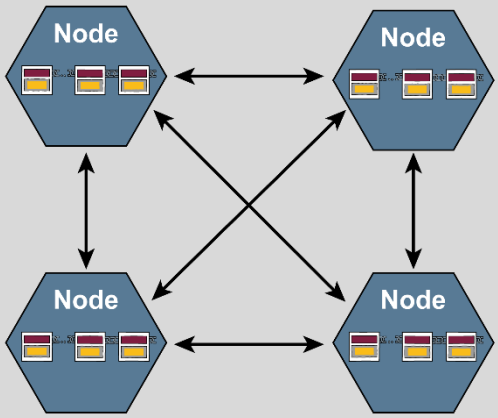

Abb. 5: Blockchain Peer-to-Peer-Netzwerk

Rechtlich kann sich die Bewältigung der Compliance-Anforderungen in komplexen Governance-Modellen sowie entwicklungstechnischen Herausforderungen niederschlagen: So erfordert die "Gemeinsame Verantwortlichkeit" mehrerer Beteiligter nicht nur einen Vertrag, in dem die Entscheidungsprozesse und Verantwortungsbereiche genau beschrieben werden, sondern auch in tatsächlicher Hinsicht die Möglichkeit, Entscheidungen innerhalb der Blockchain umzusetzen und Betroffenenrechten

[54] Blockchain Bundesverband e.V., Blockchain – Chancen und Herausforderungen einer neuen digitalen Infrastruktur für Deutschland, Version 1.1, 16.10.2017, S. 26, unter https://bundesblock.de/wp-content/uploads/2019/01/bundesblock_positionspapier_v1.1.pdf.

nachzukommen. Dies kann nur dann gelingen, wenn die rechtlichen Anforderungen auch auf technischer Ebene unterstützt werden.[55]

Eine weitere Herausforderung besteht beim Umgang mit Betroffenenrechten – so muss eine Lösung gefunden werden, personenbezogene Daten zu löschen beziehungsweise den Personenbezug zu entfernen, um den datenschutzrechtlichen Vorgaben zu genügen.

Soweit nicht ausgeschlossen werden kann, dass personenbezogene Daten betroffen sind, müssen die datenschutzrechtlichen Themen bei der Entwicklung eigener Projekte von Anfang an mitgedacht werden. Im Zweifel kann gemeinsam mit der zuständigen Datenschutzbehörde geklärt werden, wie eine rechtskonforme Umsetzung erfolgen kann.

5. Fazit

Die Blockchain-Technologie ist ohne Zweifel nicht nur eine sehr interessante Technologie, sie dürfte sich – soweit heute absehbar – in etlichen neuen Anwendungsbereichen durchsetzen. Eine Reihe von Beispielen finden Sie im folgenden Abschnitt dieses Papiers.

Trotz aller Begeisterung („technology hype"), mit der neue Technologien mitunter in der populären öffentlichen Diskussion begleitet werden, sollte man realistisch prüfen, ob der Einsatz einer Blockchain für den jeweiligen Anwendungsfall einen nachvollziehbaren Vorteil bringt. Falls eine dezentrale Datenstruktur, die zusätzlichen Ressourcen für die redundante Verteilung der Daten in einem Netzwerk und die manipulationssichere Speicherung der Daten über bisherige Sicherheitsmechanismen hinaus nicht von Vorteil sind, sind am Markt etablierte Datenbanksysteme meist die wirtschaftlich vernünftigere Wahl. Die Blockchain-Technologie löst auch keine grundlegenden Fragen der IT-Sicherheit. Eine Blockchain ist trotz „Security by Design" immer nur so sicher wie das Umfeld, in dem sie betrieben wird: Schlüssel, Passwörter und Zugangsdaten müssen ebenso weiterhin

[55] Näher Pesch/Böhme, DuD 2017, S. 473; Bechtolf/Vogt, ZD 2018, S. 66, 70 f.; Martini/Weinzierl, NVwZ 2017, S. 1251, 1256 ff.

abgesichert werden wie die Netzwerkkomponenten und Computer, auf denen die Blockchain betrieben wird.

Auch wenn Fragen der Effizienz, Usability, Standardisierung oder Interoperabilität Stand heute noch nicht für jedes Anwendungsszenario optimal sind, ist trotzdem eines sicher: Die Entwicklung der Blockchain-Technologie schreitet schnell voran und die ersten Lösungen sind bereits dabei, sich am Markt zu etablieren.

Denn insbesondere in zunehmend vernetzten Wertschöpfungsketten, die in Multistakeholder-Systemen eingebettet sind, bietet die Blockchain als Querschnittstechnologie revolutionäres Potenzial. Werte aller Art können digital und ohne Intermediär sicher und für alle Beteiligten nachvollziehbar transferiert werden.

Die Kompetenzgruppe Blockchain im *eco – Verband der Internetwirtschaft e.V.* begleitet diese Entwicklung und bietet, zusammen mit ihrem Netzwerk von Mitgliedern, allen Interessierten eine Plattform zum Austausch von Knowhow und Best-Practices: blockchain.eco.de

I. Anwendungsbeispiele

Die *Bitcoin*-Blockchain ist einerseits die bekannteste, andererseits aber nur eine von zahllosen Möglichkeiten. Für die Blockchain-Technologie gibt es keine Blaupausen, sondern man muss „selbst ran", Lösungen entwickeln und testen. Wie man die Blockchain-Technologie sinnvoll einsetzen kann, zeigen die folgenden Beispiele.

A. Finance, Payment und Banking

Die bislang prominenteste Anwendung der Blockchain-Technologie ist die Kryptowährung *Bitcoin*[56], ein digitales Währungssurrogat. Die nach wie vor anonymen Gründer wollten in der Finanzkrise 2007/2008 eine „Währung" – ein Geldmittel mit Zahlungs- und Depotfunktion – schaffen, welche nicht von Menschen kontrolliert oder manipuliert werden kann. Der Kurs der *Bitcoin* gegenüber realen Währungen ist stark volatil – eine Vermögenanlage in *Bitcoins* ist daher hoch spekulativ.

Bitcoin rückt die Blockchain immer wieder stark in die Nähe von Fintech-Anwendungen.[57] Neben *Bitcoin* hat sich im Laufe der Jahre eine Reihe weiterer Kryptowährungen etabliert. Einige bekannte Beispiele sind *Bitcoin Cash*[58], *Litecoin*[59], *Ether*[60] und *XRP*[61].

Auch etablierte Bankhäuser, die *Deutsche Börse*[62] und die *BaFin*[63] beschäftigen sich inzwischen seit mehreren Jahren mit dem Einsatz von Blockchain und anderen Distributed-Ledger-Technologien. Blockchains werden getestet, um den Handel mit Wertpapieren nachvollziehbar und manipulationssicher zu dokumentieren oder die Prozesse zur Abwicklung von Transaktionen zu optimieren und zu beschleunigen. Viele Banken haben ihre eigenen Blockchain-Projekte, schließen sich aber auch zu Konsortien

[56] Siehe https://bitcoin.org/de/
[57] Dazu Hofert, Regulierung der Blockchains, 2018, S. 1 ff.; Fairfield, 88 S. Cal. L. Rev. (2015), 805, 829 ff.
[58] Siehe https://www.bitcoincash.org
[59] Siehe https://litecoin.org/
[60] Siehe https://www.ethereum.org
[61] Siehe https://www.ripple.com
[62] Siehe https://deutsche-boerse.com/dbg-de/unternehmen/gruppe-deutsche-boerse/geschaeftsfelder/blockchain-business-areas
[63] Siehe https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html

zusammen, um gemeinsam die Blockchain-Technologie zu erforschen, wie beispielsweise bei *we.trade*[64].

Zuletzt werden zunehmend so genannte Initial Coin Offerings (ICOs) angeboten und diskutiert. Für Geschäftsmodelle, die auf Kryptowährungen basieren, stellen ICOs eine noch weitgehend unregulierte Form von Crowdfunding dar. Für die Kapitalaufnahme werden Tokens oder eine neue Kryptowährung emittiert und an die Anleger verkauft. Initial Coin Offerings sind mit herkömmlichen Finanzierungsformen noch nicht gleichgestellt. Die *BaFin* hat aber bereits Leitlinien für ICOs veröffentlicht.[65]

Private Unternehmen, wie beispielsweise *Quantoz N.V.*[66] aus den Niederlanden, bieten Abrechnungssysteme auf Blockchain-Basis an, mit denen unter anderem organisationsinterne Verrechnungsprozesse abgewickelt werden können.

B. E-Government, Identitäts- und Dokumentenmanagement

Blockchain-Technologie kann nicht nur dabei helfen, die Prozesse zwischen unterschiedlichen Verwaltungsorganen zu optimieren, sondern auch bei der verwaltungsinternen Zusammenarbeit helfen – zum Beispiel zur Prüfung, ob bestimme Daten oder Dokumente in einer Verwaltung vorliegen. Auch ist es möglich, mithilfe der Blockchain-Technologie die Integrität von Daten und Dokumenten abzusichern oder die Identitäten von Personen und Gegenständen zu verifizieren.

[64] Siehe https://we-trade.com/

[65] Siehe https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/WA/dl_hinweisschreiben_einordnung_ICOs.pdf?__blob=publicationFile&v=2

[66] Siehe https://quantoz.com/

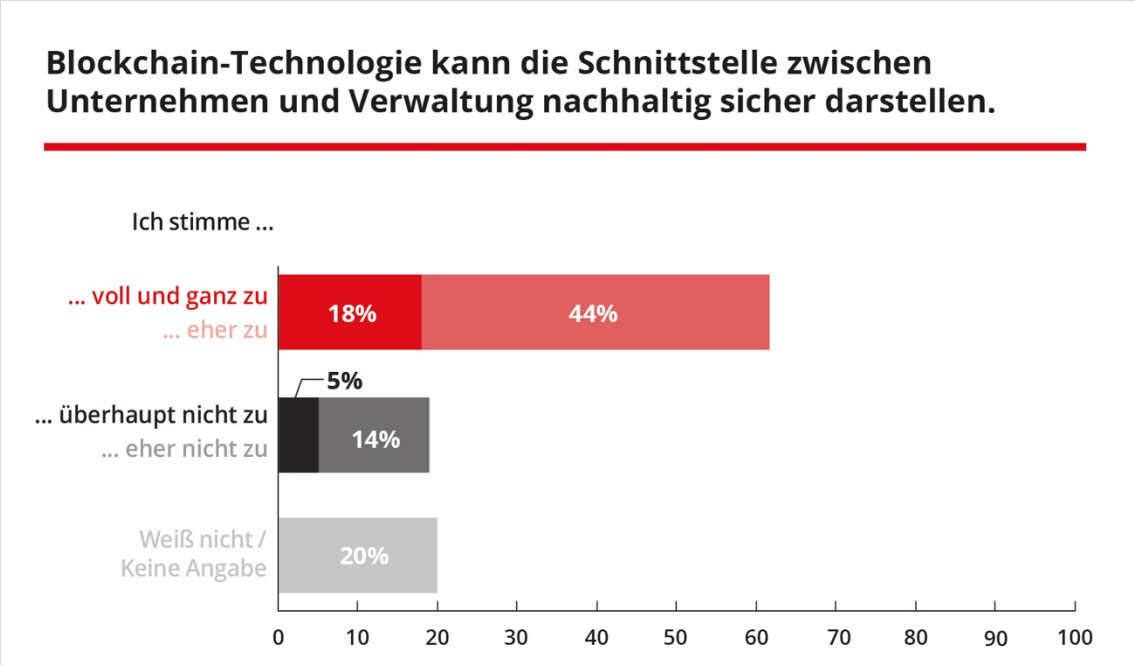

Abb. 6: Umfrage vom eco Verband aus April 2018

Die Blockchain-inhärente Sicherheit und Kryptographie erlauben die Entwicklung neuartiger Identitätsstandards, in denen beispielsweise der Nutzer selbst die vollständige Kontrolle über seine persönlichen Daten hat. Nutzer könnten mithilfe einer Blockchain-Anwendung für das Identitätsmanagement über die Weitergabe von Daten selbst entscheiden und erhalten so einen nachvollziehbaren Überblick über die Datensammlung und -verarbeitung.

Identifikationspapiere sind zwar schwer zu fälschen, da sie mittlerweile komplexe Sicherheitsmerkmale aufweisen – unmöglich ist dies aber nicht. Außerdem sind die Handhabung und Überprüfung der Sicherheitsmerkmale nicht immer leicht und schnell möglich. Daher werden inzwischen Dienste entwickelt, die eine Identität über einen Smart Contract auf der Blockchain abbilden. Diesem Smart Contract können Attribute zugewiesen und durch Dritte zertifiziert werden. Identitäten und deren (zum Teil zertifizierte) zugehörige Attribute können anschließend über einen sicheren Kommunikationskanal weitergegeben werden.

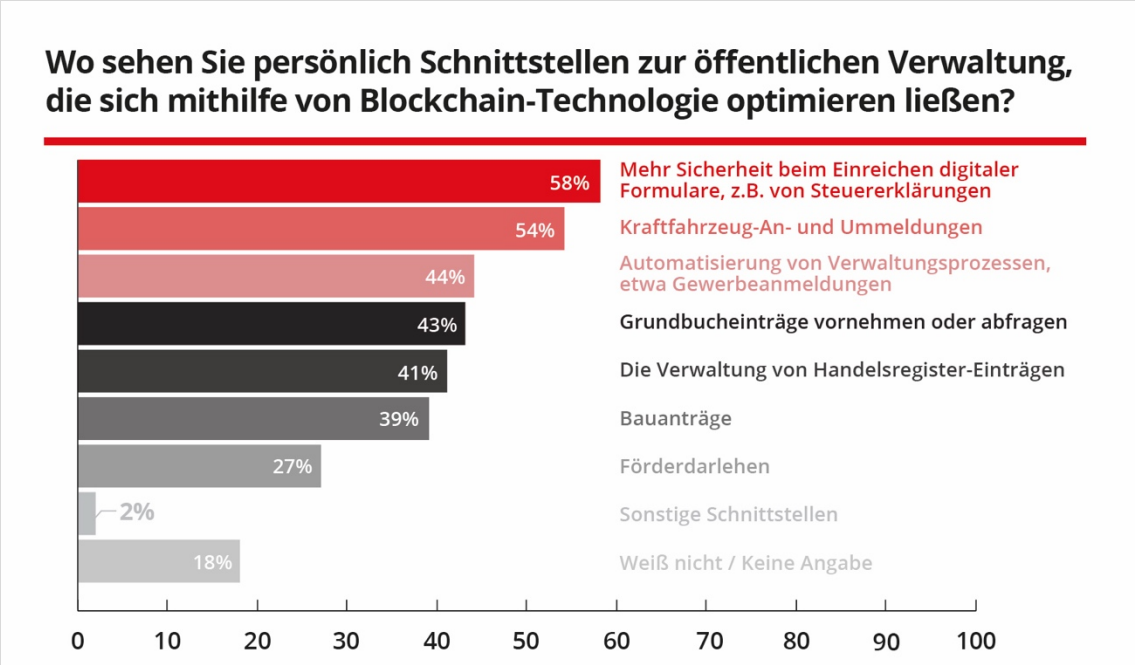

Abb. 7: Umfrage vom eco Verband aus April 2018

Eine Reihe einzelner Initiativen haben sich zum *Sovrin Network*[67] zusammengeschlossen, um an einem gemeinsamen System zusammenzuarbeiten. In Deutschland sind unter anderem die *bbw Hochschule* mit dem *Projekt ISÆN*[68], die *esatus AG*[69] oder die *regio iT gesellschaft für informationstechnologie mbh*[70] aktiv.

Für Grundbucheinträge von Immobilien ist zukünftig folgendes Szenario denkbar: Statt Geldübergabe und Eigentumsübertragung Zug um Zug und mit einem Notar abzuwickeln, könnte die Blockchain dies übernehmen. Georgien[71] hat bereits sein Grundbuchwesen auf eine Blockchain-Lösung umgestellt; in Schweden wurde ein Pilotprojekt dazu erfolgreich abgeschlossen[72]. Während die Motivation in Georgien vor allem in der Korruptionsbekämpfung lag, wird in Schweden vor allem die Notwendigkeit

[67] Siehe https://www.quantoz.com
[68] Siehe https://www.bbw-hochschule.de/forschung/forschungsprojekte/isaen.html
[69] Siehe https://www.esatus.com/Solutions/Blockchain
[70] Siehe https://www.regioit.de/aktuelles/regio-it-nachrichten/2017/fuehrerschein-pruefen-per-blockchain/
[71] Siehe http://agenda.ge/en/news/2018/396
[72] Siehe https://www.lantmateriet.se/contentassets/8d2b5d7647634c02a329b01e46e61071/the-land-registry-in-the-block-chain---testbed-2017.pdf?qry=blockchain

betont, das Vertrauen der Bürger in die staatlichen Leistungen auch im Zeitalter von Cyberkriminalität zu erhalten.

C. Energiebranche

Der Energiesektor ist sehr aktiv bei der Erprobung des Einsatzes von Blockchains und Smart Contracts, um den Handel von Energieträgern voranzutreiben. Treiber der Entwicklung sind das Automatisierungspotenzial und die Nachvollziehbarkeit der Transaktionen. Smart Contracts bieten darüber hinaus die Möglichkeit, insbesondere das Rechnungshandling für Transaktionen kleiner Einheiten wirtschaftlich zu gestalten. Stromkäufe an Ladesäulen oder die Einspeisung von privat erzeugtem Strom sind mögliche Szenarien. Derzeit ist der Verwaltungsaufwand nicht selten teurer als die eigentlichen Stromkosten.

Über die Blockchain könnte die Kommunikation zwischen Erzeuger und Stromversorger beziehungsweise zwischen Fahrzeug und Ladesäule bei jedem Ladevorgang und für jeden Anbieter abgewickelt werden. Mittler, die Sammelverträge mit der Elektrotankstelle abschließen und jeden Ladevorgang mit dem E-Tanker abrechnen und dafür eine Kommission abrechnen, würden dadurch überflüssig.

Eine prominente und aktive Plattform für den Energiehandel auf Blockchain-Basis ist die *Enerchain*[73], aber auch der Fernleitungsnetzbetreiber für Erdgas *Open Grid Europe*[74] beschäftigt sich mit dem Einsatz von Blockchain-Technologie. Ebenso gibt es Projekte, die sich mit Mechanismen zur automatisierten Stabilisierung von Stromnetzen auf mithilfe der Blockchain-Technologie beschäftigen.[75]

Mehrere Projekte beschäftigen sich mit der Überführung der sogenannten Marktkommunikation auf Basis von Distributed-Ledger-Technologien. Die *energy web foundation*[76] fokussiert sich hierbei auf die Definition eines neuen einheitlichen Kommunikationsstandards im Datenaustausch. Beim *edna Bundesverband Energiemarkt & Kommunikation e.V.*[77] handelt es sich

[73] Siehe https://enerchain.ponton.de/
[74] Siehe https://www.open-grid-europe.com
[75] Siehe https://innovation.elia.be
[76] Siehe https://www.energyweb.org
[77] Siehe https://edna-bundesverband.de/

um ein Konsortium unterschiedlicher Dienstleister aus der Energiebranche, welche ebenfalls die Marktkommunikation mittels Blockchain umsetzen wollen. Im Projektkonsortium *ETH@Energy*[78] haben sich verschiedene deutsche Energieversorgungsunternehmen und Netzbetreiber zusammengeschlossen und pilotieren seit 2016 aktiv die Überführung relevanter Prozessschritte auf eine konsortiale Blockchain.

D. Versicherungen

Die Blockchain-Initiative der Versicherungsbranche *B3i*[79] hat es sich zum Ziel gesetzt zu prüfen, ob mit der Blockchain-Technologie branchenweite Standards und Verfahren entwickelt werden können – beispielsweise als Grundlage für neue Geschäftsmodelle.

Der Versicherungsanbieter *AXA*[80] hat bereits als Pilotprojekt eine Flugverspätungsversicherung umgesetzt. Hier werden Flugverspätungen automatisch registriert und die Auszahlung der Versicherungssumme ausgelöst.

E. E-Commerce, Logistik und Traceability

Neben klassischen Anwendungen im Zahlungsverkehr bietet sich die Blockchain auch als Handelsinfrastruktur für e-Commerce-Anbieter an, die herkömmliche Marktplätze ergänzt oder gar ersetzt. Ein besonders ambitioniertes Vorhaben in diesem Sektor ist das Projekt „*Global Alliance of Merchants on the Blockchain*"[81]. Es wird von einer Reihe namhafter Unternehmen getragen und hat sich zum Ziel gesetzt, jedes Produkt in einen Smart Contract abzulegen und es so Händlern zu erlauben, die Vermarktung ihrer Produkte unabhängig von den Bedingungen der etablierten Plattformen vorzunehmen.

[78] Siehe https://www.eth-energy.de
[79] Siehe https://www.b3i.tech
[80] Siehe https://www.fizzy.axa
[81] Siehe https://www.gamb.io

Im Bereich Supply Chain gibt es eine Vielzahl von Blockchain-Projekten und Ideen, die von Herstellungsnachweisen bis zur Digitalisierung der Frachtlogistik reichen. Der Payment-Anbieter *Wirecard*[82] bietet beispielsweise einen Prototyp einer universell einsetzbaren Supply-Chain-Plattform an. Der Prototyp konzentriert sich auf die Vernetzung von Händlern und Produzenten und erfasst alle Geschäftsprozesse in Smart Contracts.

Traceability, die lückenlose Rückverfolgbarkeit von Gütern, stellt die IT heute immer noch vor große Herausforderungen. Ein wesentlicher Grund liegt darin, dass ein kontinuierlicher Datenfluss über unterschiedliche IT-Systeme hinweg gewährleistet werden muss: von der Produktion bis zum Endkunden. Die Komplexität der heutigen Supply Chains ermöglicht es zudem, dass Manipulationen an den zu verfolgenden Gütern durchgeführt werden können, wie beispielsweise das Einschleusen von Produktfälschungen. Aber auch unsachgemäßes Behandeln der Produkte, allem voran die Unterbrechung einer zu garantierenden kontinuierlichen Kühlkette, sind bekannte Problemfelder. Die dänische *A. P. Moller-Maersk Group* ist gemeinsam mit *IBM*[83] eine der Vorreiter bei der Digitalisierung von Logistik-Prozessen mithilfe der Blockchain-Technologie. Inzwischen werden Track & Trace Lösungen auf Blockchain-Basis auch als fertige Systeme angeboten.

Das Unternehmen *Everledger*[84] registriert Diamanten mit ihren individuellen Merkmalen direkt nach dem Schürfvorgang auf der Blockchain als Identitäts- und Herkunftsnachweis. Derzeit muss man sich beim Diamantenhandel auf Echtheitszertifikate verlassen. Sie können verloren gehen oder werden gefälscht. Durch die Blockchain-Technologie macht *Everledger* den Weg der Diamanten komplett nachvollziehbar, von der Mine bis zum Kunden. Die Echtheitszertifikate werden in der Blockchain hinterlegt und können somit immer den richtigen Diamanten zugewiesen werden. Niemand kann die Einträge fälschen oder aus der Blockchain löschen. Dadurch soll der Handel transparenter und sicherer werden. Gleiches kann auch bei anderen Luxus-

[82] Siehe https://www.wirecard.com
[83] Siehe https://www.tradelens.com/
[84] Siehe https://diamonds.everledger.io

Gütern angewendet werden, wie beispielsweise bei Textilien, Kunst und Schmuck.

Auch für die Lebensmittel- und die Pharmaindustrie ist es von besonderer Wichtigkeit, die Herkunft oder die Echtheit von Produkten sowie deren Lieferketten lückenlos nachweisen zu können. So arbeiten beispielsweise *Merck* und *SAP*[85] bereits an einem Konzept und haben dazu die *SAP Pharma Blockchain POC App* entwickelt.

Die *Lufthansa*[86] und die *Deutsche Bahn*[87] testen ebenfalls eine Vielzahl von Anwendungsfeldern für Blockchain-Lösungen, sowohl im Bereich Logistik als auch für die Prozessoptimierung und Verrechnung interner Leistungen über Smart Contracts. Die *Deutsche Bahn* erprobt auch konsortiale Szenarien in Zusammenarbeit mit anderen Verkehrsverbünden. So soll die sehr komplexe Einnahmeaufteilung aus Ticketerlösen im Nahverkehr mithilfe der Blockchain transparent organisiert werden, da zunehmend nahtlose Reiseketten, die immer mehr Anbieter integrieren, die eindeutige Zuordnung erschweren.

Um eine weitere Form von Herkunftsnachweis und Berechtigungsmanagement geht es beim Projekt *SAMPL – Secure Additive Manufacturing Platform*[88]. Hier wird mithilfe einer Blockchain sowohl die zulässige Anzahl der Druckvorgänge als auch die Berechtigung und Freigabe des benutzten Druckers für die Anfertigung von so genannten 3D-Drucken in der additiven Fertigung gesteuert.

[85] Siehe https://blogs.sap.com

[86] Siehe http://blockchainforaviation.com/

[87] Siehe https://www.deutschebahn.com/de/Digitalisierung/technologie/Neue-Technologien/blockchain-3241170

[88] Siehe http://www.sampl-3d.de/

II. Autoren

Die eco Kompetenzgruppen Blockchain und Sicherheit danken allen, die an diesem Papier mitgearbeitet haben:

Sebastian Beyer
Product Manager Blockchain Ensured Certificates Service
CERTIVATION GmbH, Lingen (Ems)
sbeyer@certivation.com

Prof. Dr. Georg Rainer Hofmann
Direktor, Information Management Institut IMI
Technische Hochschule Aschaffenburg
hofmann@th-ab.de

Martin Lundborg
Leiter der Abteilung Kommunikation und Innovation
WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Bad Honnef
m.lundborg@wik.org

Christian Märkel
Senior Economist
WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Bad Honnef
c.maerkel@wik.org

André Mundo
Bereichsleiter Distributed Ledger Technologies
MaibornWolff GmbH, München
andre.mundo@maibornwolff.de

Prof. Norbert Pohlmann
Fachbereich Informatik und Kommunikation
if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule, Gelsenkirchen
pohlmann@internet-sicherheit.de

Lars Steffen
Director eco International
eco – Verband der Internetwirtschaft e.V.
lars.steffen@eco.de

Stephan Zimprich
Leiter, eco Kompetenzgruppe Blockchain
Partner, Fieldfisher (Germany) LLP, Hamburg
stephan.zimprich@fieldfisher.com