



BLOCKCHAIN
REALLABOR
RHEINISCHES REVIER

Bericht AP2.1 | Distributed Ledger Technologies

Dr. Birgit Weimert

Juli 2020

INHALTSVERZEICHNIS

1	GRUNDLAGEN.....	3
1.1	Einleitung.....	3
1.1.1	Motivation	3
1.1.2	Distributed Ledger Technology und Blockchain.....	4
1.2	Blockchain.....	5
1.2.1	Blockchain-Generationen	5
1.2.2	Grundlagen.....	6
1.2.2.1	Transaktionen	6
1.2.2.2	Blöcke.....	7
1.2.3	Blockchain-Typen	9
1.2.4	Eigenschaften und grundlegende Vorteile/Herausforderungen	10
1.2.5	Architektur von Blockchain-Systemen	13
1.2.6	Bestandteile	13
1.2.6.1	Verteilte P2P-Netzwerke.....	13
1.2.6.2	Hashing und Kryptografie	14
1.2.6.3	Konsensbildung	15
1.2.7	Smart Contracts und dezentrale Applikationen.....	21
1.2.8	Ausgewählte Blockchain-Beispiele	22
2	ANWENDUNGEN	25
2.1	Entscheidungskriterien für den Blockchain-Einsatz	25
2.2	Anwendungsfelder.....	26
2.2.1	Finanzen und Versicherungen	28
2.2.2	Daseinsfürsorge, öffentlicher und juristischer Sektor	30
2.2.3	Produktionsökonomie und Industrie 4.0	31
2.2.4	Logistik und Supply Chain Management	31
2.2.5	Energie	33
2.2.6	Weitere Felder.....	33
2.3	Geschäftsmodelle.....	34
2.4	Akteure.....	34
3	TECHNOLOGIEKOMPLEX.....	35
4	TRENDS UND ENTWICKLUNGSTHEMEN.....	38
4.1	Konvergenzen (Digitalisierung)	39
4.2	Skalierung	39
4.2.1	Speicherplatzreduktion.....	40
4.2.2	SegWit.....	40

4.2.3	Erhöhung der Blockgröße.....	41
4.2.4	Sharding	41
4.2.5	Directed Acyclic Graphs (DAG)	42
4.2.6	Off-Chains	42
4.3	Sicherheit	43
4.4	Interaktion	47
4.4.1	Interoperabilität	47
4.4.2	Orakel	49
4.4.3	Standards und Regulierung	50
4.5	Ausgewählte Alternativen zur Blockchain	50
4.5.1	IOTA	51
4.5.2	Hashgraph	53
4.5.3	Blockgitter	55
4.5.4	Auswahl weiterer Möglichkeiten	55
4.6	Sonstige Trends	56
5	ZUSAMMENFASSUNG UND AUSBLICK	57
6	LITERATURVERZEICHNIS	59

1 GRUNDLAGEN

1.1 Einleitung

Im Rahmen des Projekts Blockchain Reallabor im Rheinischen Revier sollen die Blockchain- und Distributed Ledger-Technologien (DLT) hinsichtlich ihrer Potenziale, erwartbarer zukünftiger technologischer Entwicklungen und auch relevanter beitragender sowie konkurrierender Technologien dargestellt werden. Dazu ist es von großer Relevanz die Themen einmal umfassend zu betrachten und einzuordnen. Allgemein lässt sich feststellen, dass Blockchain- und Distributed Ledger-Technologien bezüglich ihrer Anwendungspotenziale einerseits in der Phase einer überzogenen, gar an einen Hype grenzenden Erwartungshaltung¹ befinden, andererseits sehen sich diese Technologien einer erheblichen Kritik ausgesetzt (G7 Working Group on Stablecoins 2019). Ziel dieser Studie ist es, ein fundiertes Verständnis der zugrundeliegenden Technologien sowie der Eigenschaften und Zusammenhänge der Infrastruktur zu vermitteln, ohne die eine wissenschaftlich fundierte Ermittlung ihres Potenzials bzw. Bewertung aussichtsreicher Use-Cases nicht möglich ist. Eine Herausforderung in der Erschließung dieser Technologien besteht darin, dass die Kommunikation häufig im Internet in Form von White Paper, Blogs und Foren stattfindet, so dass nur ein Teil der veröffentlichten Informationen wissenschaftlichen Standards genügen. Auch die Begrifflichkeiten unterliegen nicht nur einer zeitlichen Dynamik, sondern werden inhaltlich oft inkonsistent verwendet. Wichtig ist es daher, die z. T. durch unseriöse Medienberichterstattung, aber auch durch eine zu starke Vereinfachung der Technologie oder durch HighTech-Slang hervorgerufenen Konfusionen zu entwirren. Des Weiteren machen es wenig aussagekräftige Äußerungen wie „wir nutzen einzigartige Technologien“ sowie proprietäre Software schwierig, Informationen nachzuvollziehen. Diese Studie soll daher einen fundierten Ausgangspunkt bieten, der die oft schwierig beschriebene Thematik in einer weiteren Bandbreite von Vorgehensweisen, Möglichkeiten und Alternativen erfasst und verständlich erläutert.

1.1.1 Motivation

Die Blockchain-Technologie beruht auf einer Fülle bekannter Technologien wie z.B. diversen digitalen Währungen, verteilten Rechner- und Speichersystemen sowie kryptografischen Verfahren. Im Jahr 2008 wurde in dem White Paper „Bitcoin: A Peer-to-Peer Electronic Cash System“ von Satoshi Nakamoto ein sogenannter Konsens-Mechanismus beschrieben, der im Prinzip dezentralisierte Transaktionen ohne zentrale Instanz (Intermediär)² ermöglicht und auch zensurresistent ist (Nakamoto 2008)³. 2009 startete das Bitcoin-Netzwerk, das die Unabhängigkeit

¹ Welche grotesken Ausmaße das annehmen kann, zeigte der Fall des amerikanischen Unternehmens Long Island Iced Tea, das sich ohne technische und geschäftliche Grundlage in Long Blockchain umbenannte und damit den eigenen Aktienwert kurzzeitig um 500 % steigerte (Handelsblatt Media Group GmbH & Co. KG 2017).

² Intermediäre können z.B. Banken sein oder die Plattformökonomie. Letzteres sind internetbasierte Geschäftsmodelle, die Anbieter mit Interessenten auf einem digitalen Marktplatz zusammenbringen. Dabei wirkt vor allem der Netzwerkeffekt: je mehr Anbieter auf der Plattform sind, desto interessanter für Kunden und umgekehrt.

³ Als Vorstufen für das Bitcoin-System und seine Funktionsweise dienten diverse Aktivitäten, u.a. im Zusammenhang mit der Cypherpunk-Bewegung (Casey und Vigna 2015). Konkret sind dies z.B. eCash von David Chaum (Chaum 1984a), B-money von Wei Dai (Wei 1998) und Bit Gold von Nick Szabo (Szabo 1998).

von Zentralbanken und staatlicher Regulierung gewährleisten sollte. Aufgrund der Tatsache, dass hier fast anonym, d. h. pseudonym, Transaktionen ausgetauscht werden können, wurde es von Beginn an auch für illegale Geschäfte im Darknet genutzt. Gegen diesen negativen Beigeschmack haben Interessenten und Nutzer häufig immer noch zu kämpfen. Im Laufe der Zeit entstanden eine Vielzahl von Kryptowährungen mit unterschiedlichsten Eigenschaften sowie diverse Projekte und Firmengründungen. Das Potenzial der Technologie für diverse Branchen löste 2017 einen regelrechten branchenübergreifenden Hype aus, welcher die Entwicklungsgeschwindigkeit der Technologie durch weitere Akteure sowie größerer Investitionen zusätzlich steigerte. So wurden eine Reihe neuartiger Blockchain-inspirierter Lösungsansätze ermöglicht, dieser Hype führte aber auch zu vielen Spekulationsgeschäften. Heute befinden wir uns in einer Art Konsolidierungsphase, in der die Leistungsfähigkeit erkannt, nichtseriöse Projekte und Investoren bereits vielfach ausgesondert wurden und der Aufbau und das Testen diverser Anwendungen im Mittelpunkt stehen. Es wird prognostiziert, dass über 10% des globalen BIP bis 2025 in Form von Kryptowährungen gespeichert sein werden (World Economic Forum 2015). Andere Studien besagen, dass die Blockchain bis 2030 einen Geschäftswert von 3,1 Billionen Dollar schaffen wird. Gemäß Zahlen des Marktforschungsunternehmens IDC wurden 2018 etwa 1,5 Milliarden US-Dollar in DLT-Lösungen investiert. Für das zu erwartende Blockchain-Marktvolumen divergieren die Zahlen für den Zeitraum um 2014 zwischen 20 und 60 Milliarden US-Dollar (Fridgen et al. 2019). Diese sowie Schlussfolgerungen vieler weiterer Studien (z.B. (Schlatt et al. 2016), (Fraunhofer FIT)) lassen nicht nur auf ein hohes wirtschaftliches, sondern auch auf große gesellschaftliche und kulturelle Disruptionspotenziale schließen. Auch Frost and Sullivan sehen in ihrer neuesten Studie die Blockchain bis 2030 als grundlegenden Baustein für vielfältige Anwendungen (Frost & Sullivan 2019).

1.1.2 Distributed Ledger Technology und Blockchain

Die Distributed⁴ Ledger Technology (DLT, Distributed Ledger Technik) stellt im Prinzip eine verteilte Datenbank dar bzw. ein Journal, wie man es aus der Buchführung kennt. Diese Datenbank wird von einem dezentralen Netzwerk unterhalten. Das heißt, eine Instanz, über die jede Interaktion stattfinden muss wie in einer zentralen Struktur, gibt es hier nicht. Jeder Teilnehmer (Knoten) in einem solchen Netzwerk speichert, verbreitet und synchronisiert die Daten. Die Technologie ermöglicht die Einigung der verschiedenen Knoten, auch Node genannt, über den allgemein gültigen Zustand der Datenbank bzw. Logbuch, die Konsensfindung. Erhält ein Knoten eine Transaktion teilt er diese daraufhin mit dem Netzwerk. Die Validität und Reihenfolge der Transaktion im Netzwerk werden von den Teilnehmern mit Hilfe einer vorher implementierten Vorgehensweise überprüft. Ist die Validität bestätigt, wird die Transaktion dem Logbuch hinzugefügt. Der so ständig weiter anwachsenden Dokumentation können Transaktionen jedoch nur hinzugefügt werden (append only). Sie können nicht, wie in herkömmlichen Datenbanken, verändert oder gelöscht werden (Kannengiesser et al.).

Der DLT sind mehrere DLT-Konzepte untergeordnet. Diese unterscheiden sich hauptsächlich in der Art und Weise, wie Transaktionen gespeichert und validiert werden. Es lässt sich z.B. nach den Konzepten wie Blockchain, Directed Acyclic Graphs (DAG), hybride und Sharded Strukturen unterscheiden. Diese lassen sich dann wiederum auf verschiedenste Arten implementieren, wie dies u.a. bei Bitcoin oder Ethereum für Blockchains, IOTA oder Helder Hashgraph für DAGs,

⁴ Distributed, also verteilte, Systeme können zentral oder dezentral betrieben werden.

BigChainDB für hybride oder z.B. Radix für Sharded Ledger der Fall ist (DLT Design) (siehe dazu auch Kapitel 1.2.8 und 4.5).

Die DLT-Konzepte stellen einen Fortschritt gegenüber den heute noch üblichen Datensilos⁵ bei der Sammlung, Kommunikation und Prozessierung verteilter Daten dar (Yaffe 2017). Sie eignen sich sowohl für die Erfassung statischer Daten (Registry) als auch für die Erfassung dynamischer Daten (Transaktionen), was sie zu einer Weiterentwicklung von Aufzeichnungssystemen macht. Die Daten können auf drei verschiedene Arten gespeichert werden: Unverschlüsselt können sie von jedem Knoten eingesehen werden, verschlüsselt nur von denjenigen, die den Entschlüsselungsschlüssel besitzen, oder als sogenannte Hashes als digitale Fingerabdrücke für offchain-gespeicherte Daten, um anzuzeigen, dass die Daten nicht manipuliert wurden.

Eine Blockchain lässt sich demnach als eine spezielle Form eines Distributed Ledgers verstehen, die sich durch eine spezielle Datenstruktur (Blöcke) auszeichnet. Diese Blöcke werden durch einen kryptografisch-gestützten Konsensprozess validiert und aneinandergereiht. Die Blockchain verfügt über ein festgelegtes, programmiertes Regelsystem, das nicht ohne weitere Einverständnisse geändert werden kann. Das Vertrauen in die algorithmische Richtigkeit der Entscheidung basiert auf Annahmen der Dezentralität, des Konsens, der Netzwerkteilnehmer sowie deren Überprüfbarkeit in der offen einsehbaren Software⁶. Oftmals wird diese abstrakte algorithmische Richtigkeit (= Echtheit) fälschlicherweise mit der inhaltlichen oder physikalischen Richtigkeit (= Wahrheit) gleichgesetzt, die eine Blockchain aber nicht sicherstellt.

1.2 Blockchain

1.2.1 Blockchain-Generationen

Die Entwicklung der Blockchain wird oft in Generationen aufgeteilt, wobei hier unterschiedliche Auffassungen nebeneinander existieren. Meist werden drei Generationen der Blockchain unterschieden. Die erste Generation implementiert Kryptowährungen in Anwendungen im bargeldbezogenen Bereich (z.B. Geldtransfer, Überweisung und digitale Zahlungssysteme). Die zweite Generation nutzt Verträge. Sie repräsentieren die wirtschaftlichen, marktwirtschaftlichen und finanziellen Anwendungen von Kryptowährungen wie Aktien, Anleihen, Futures, Kredite, Hypotheken, Titel oder Smart Property und Smart Contracts. Die dritte Generation setzt Blockchains jenseits von Währung, Finanzen und Märkten ein (z.B. Regierung, Gesundheit, Wissenschaft, Bildung, Kultur und Kunst) (Swan 2015). Die Entwicklung der Blockchain-Technologie lässt sich auch in fünf Stufen unterteilen: Blockchain als Infrastruktur für Kryptowährungen. Blockchain zur Verwaltung weiterer virtueller Werte, als Anwendungen für Transaktionsaufzeichnungen, als Anwendung zur Aufzeichnung von Rechten und als Basis zukünftiger Prozesse und Verarbeitungen (Automatisierung), z.B. in Form von Smart Contracts für IoT (Nomura Research Institute 2016).

⁵ Datensilos geben ihre Daten nur sehr selten außerhalb ihrer eigenen geschlossenen Umgebung weiter. Dies führt zu einem enormen Verlust an Informationen, oft über 99%, da die Daten nicht weiter genutzt werden (Manyika und Chui 2015).

⁶ Das Kriterium einer offen einsehbaren Software, womöglich als Open-Source-Software (OSS), ist in der Praxis jedoch nicht immer realisiert.

Token und Coins

Token können im weiteren Sinne als Wertmarken definiert werden. Obwohl hierzu schon Bücher erschienen sind, wie z.B. (Voshmgir 2019), gibt es noch keine einheitliche Definition. Token sind in vielen Fällen essenziell für die Blockchain-Funktionalität. Viele Blockchains besitzen native Tokens, die typischerweise dazu dienen, die Miner bzw. Validatoren zu entlohnen sowie Spam- und DDoS-Angriffe zu verhindern oder als Ausführungsgebühr/Treibstoff für Smart Contracts zu fungieren. Permissioned Blockchains lassen sich aber auch Tokenless gestalten. Anhand der Austauschbarkeit lassen sich Tokens in fungible, z.B. Kryptowährungen, und non-fungible, die oft im Zusammenhang mit Sammlerstücken genannt werden, unterteilen. Letztere bieten jedoch weitaus mehr Möglichkeiten. So kann dieser mit individuellen Rechten und Ansprüchen versehen werden. Tokens, die einen monetären Wert repräsentieren, bezeichnet man als Coin oder Pure Currency Token (Camp et al. 1995). Weiterhin lassen sie sich u.a. auch weiter in Utility Token, Security Token und Equity Token unterteilen (Momtaz et al. 2019). Utility Token werden als eine Art Gutschein für Produkte oder Dienstleistungen eines Unternehmens oder als Zugangsberechtigung ausgegeben. Security Token knüpfen ihren Wert an die Wertentwicklung eines Basiswerts. Sie räumen Investoren die gleichen Rechte ein wie traditionelle Finanzmarktemissionen und unterliegen daher in den meisten Ländern den Wertpapiergesetzen mit einer Regulierung durch Wertpapieraufsichten wie die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) oder die Securities and Exchange Commission (SEC). Für den Fall, dass ein Security Token in der Funktion einer Aktie einen digitalen Unternehmensanteil mit Eigentums- und Stimmrechten repräsentiert, spricht man auch von einem Equity Token (Drobetz et al. 2019). Es lassen sich auch Asset-backed Token als Entsprechung eines Anspruchs auf ein Anlagegut sowie Network Value Token unterscheiden (Hahn und Wons 2018). Token können auch standardisiert werden, beispielsweise mittels den auf Ethereum basierenden ERC-20 oder ERC-721 Token, die dann als Referenzmaß dienen. Auf diesen Tokenized Blockchains lassen sich mit unterschiedlichen Mechanismen weitere Tokens aufsetzen, z.B. Bitcoin/Colored Coins⁹.

1.2.2.2 Blöcke

Ein Block in der Blockchain enthält verschiedene Parameter, die hier am Beispiel der Bitcoin-Blockchain dargestellt ¹⁰ und in den Folgekapiteln ausführlicher erklärt werden.

⁹ Das Colored Coin-Prinzip baut auf einer bereits bestehenden Blockchain auf und fügt zu den bereits vorhandenen Werten, bei Bitcoin den UTXO, zusätzliche Informationen hinzu, wodurch diese einen neuen materiellen oder immateriellen Wert repräsentieren.

¹⁰ Unter <https://blockexplorer.com> können alle Blöcke der Bitcoin-Blockchain eingesehen und die Transaktionshistorie bis zum ersten Block, dem sogenannten Genesis Block, transparent nachvollzogen werden.

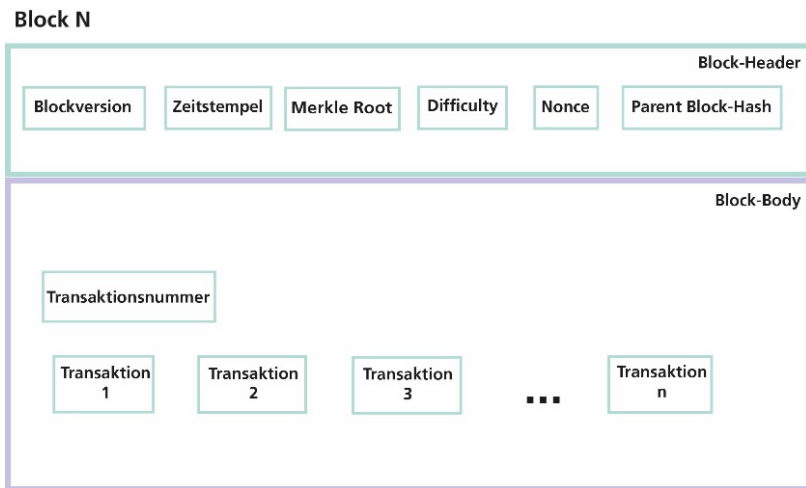


Abbildung 2: Blockformat (eigene Darstellung).

Jeder Block enthält den Hash-Wert¹¹ des Block-Headers des vorherigen Blocks, d. h. dem letzten Block in der Blockchain (Parent Block-Hash), wodurch dieser an die Kette angehängt werden kann. Ein Block besteht aus einem Block-Header und einem Block-Body. Der Kopf eines Blocks enthält die Blockversion, das ist die Versionsnummer der Software, einen Zeitstempel und den sogenannten Merkle Root¹², der auf eine Datenstruktur, die alle Transaktionen im Block enthält, verweist. Des Weiteren einen nBit-Wert, der Mindestanforderung an den neu zu generierenden Hash-Wert festlegt (Difficulty), und die sogenannte Nonce, ein 4 Byte-Feld, das mit 0 startend hochgezählt wird und als einzige Komponente veränderbar (frei wählbar) ist, um die Mindestanforderungen an den resultierenden Hash erfüllen zu können (Zheng et al. 2017). Der Block-Body enthält im Wesentlichen die Transaktionen.

Verkettung

Die Blöcke einer Blockchain sind durch die Hash-Werte des jeweils vorhergehenden Blockes miteinander verbunden. Wird ein einziger Wert in der Kette eines Netzwerkteilnehmers manipuliert, stimmen die Hashes des jeweiligen Blockes und damit auch aller nachfolgenden Blöcke nicht mehr mit den übrigen Teilnehmern des Blockchain-Netzwerkes überein. Dies ermöglicht es, schnell Manipulationen zu identifizieren, aber auch schnell einen gemeinsamen Konsens über die Transaktionshistorie herzustellen.

Prozess

Der typische Prozess wird im Folgenden am Beispiel der Bitcoin-Blockchain vorgestellt (Nakamoto 2008): Im Prinzip kann jeder Netzwerkknoten die Transaktionen, die innerhalb des Zeitfensters angefallen sind, auswählen, diese validieren, zu einem Block aggregieren und den vorgegebenen Konsensalgorithmus ausführen. Im Fall der Bitcoin-Blockchain ist für den Block eine Aufgabe zu lösen. Findet ein Knoten die richtige Lösung (Nonce), teilt er diese allen anderen Netzteilnehmern mit. Dieser Prozess wird Mining genannt. Die anderen Knoten akzeptieren den Block nur dann, wenn die enthaltenen Transaktionen valide sind und noch nicht zuvor verstetigt wurden. Die

¹¹ Ein Hash-Wert ist eine Prüfsumme. Diese wird mittels einer mathematischen Funktion oder einem Computeralgorithmus ermittelt. Dabei werden Eingabewerte (Zahlenwerte, Buchstaben- oder Zeichenfolgen) mit einer variablen Länge in eine Prüfsumme mit fixer Länge (digitaler Fingerabdruck) umgerechnet.

¹² Genauer gesagt ist der Merkle Root ein Hash-Baum, dessen Wurzel einen Hash über alle enthaltenen Transaktionen darstellt.

Knoten schreiben in diesem Fall den Block in ihre Version der Blockchain und der Knoten, der die richtige Lösung gefunden hat, wird mit einer bestimmten Menge Bitcoins belohnt (Ertrag). Anschließend wird am nächsten Block gearbeitet und der Hash des jetzt akzeptierten Blocks für den nächsten verwendet.

Theoretisch validieren alle Knoten Transaktionen, verbreiten diese bzw. die Blöcke, erkennen andere Teilnehmer und sind mit diesen verbunden. In der Praxis werden jedoch nicht alle Prozessschritte von allen Knoten (gleich) ausgeführt. Grob unterschieden werden können die Full Nodes und Light(weight) Nodes. Bei Full Nodes handelt es sich um Knoten, die autonom und verbindlich nach entsprechenden Regeln Transaktionen und Blöcke validieren/verifizieren und die gesamte Blockchain gespeichert haben. Dafür ist jedoch nicht das Vorhalten der gesamten Transaktionshistorie notwendig. Diese Aufgabe wird von den Archival Nodes übernommen¹³. Lightweight Nodes halten lediglich die Block-Header vor und sind auf die Full Nodes angewiesen (Bitcoin Community 2018). Eine Auswahl von den im Netzwerk anfallenden Transaktionen werden innerhalb eines bestimmten Zeitraums¹⁴ von den Minern (in der Regel Full Nodes) gesammelt und durch einen Konsens-Mechanismus an die vorherigen Blöcke, d. h. die Blockchain, angehängt. Finden innerhalb eines Zeitfensters mehr Transaktionen statt, als im Bitcoin-Netzwerk verarbeitet werden können, obliegt den Minern die Auswahl der Transaktionen für einen Block. Die Miner wählen in diesen Fällen dann gerne die Transaktionen mit den höchsten Transaktionsgebühren und dem Miner somit entsprechend mehr Ertrag (in Form von sogenannten nativen Tokens) bringen. Miner haben auch die Möglichkeit, sich Pool Mining Plattformen anzuschließen, auf denen die Miner ihre Ressourcen gemeinsam verwenden und die Erträge aufteilt werden.

Ein Knoten erzeugt eine Transaktion nach dem o.g. Vorgehen (s. Abbildung 1) und verteilt diese nach eigener Prüfung auf Gültigkeit im Netzwerk. Knoten, die eine gültige Transaktion erhalten, verifizieren diese, legen sie in ihren Mempool¹⁵ und leiten diese an alle Knoten weiter, mit denen sie verbunden sind. Die Transaktion wird erst Teil der Blockchain, wenn sie in einen Block eingefügt wurde, dessen Gültigkeit mittels bestimmter Mechanismen sichergestellt wurde. Jeder Knoten kann dann die Transaktion in der Blockchain unabhängig als gültig und nutzbar verifizieren, wobei die Light(weight) Nodes die sogenannte Simplified Payment Verification nutzen, indem sie prüfen, ob eine Transaktion in der Blockchain steht.

Jeder Block mit mehr als sechs Bestätigungen wird als unwiderruflich betrachtet, da es eine immense Rechenleistung erfordern würde, sechs Blöcke neu zu berechnen.

1.2.3 Blockchain-Typen

Die Ausgestaltungsmöglichkeiten einer Blockchain sind vielfältig. Sie kann für jeden frei zugänglich sein oder Restriktionen besitzen. Unterschieden wird bezüglich des Zugriffs auf die Daten und die Nutzung des Netzwerkes (Public, Private) als auch bezüglich der Möglichkeiten zur Beteiligung an der Validierung von Blöcken im Konsens-Mechanismus (Permissioned, Permissionless)¹⁶. Die meisten bekannten Kryptowährungen wie Bitcoin und Ethereum setzen

¹³ Das sind spezialisierte Full-Nodes, die die Transaktionshistorie des gesamten Blockchain-Netzwerkes vorhalten und auf Anfrage diese Informationen anderen Knoten zur Verfügung stellen.

¹⁴ Bei der Bitcoin-Blockchain beträgt der Blockbildungszyklus in der Regel 10 Minuten.

¹⁵ Einfach gesagt ist ein Mempool eine Referenz auf eine Sammlung von Transaktionen, die von den Knoten verifiziert, aber noch nicht zur Blockchain hinzugefügt wurden.

¹⁶ Daneben kann ein allgemeines Rollen- und Rechtemanagement individuell definiert werden.

derzeit auf Public Permissionless Blockchains. Herausforderungen ergeben sich hier aufgrund des großen Datenvolumens bezüglich der Skalierbarkeit sowie aufgrund der Notwendigkeit einer Mehrheitsentscheidung für Änderungen bezüglich der Governance. In einer privaten Blockchain ist der Ledger nur mit Berechtigungen (Zugriffsrechten), die von zentralen Instanzen verwaltet werden, zugänglich. In der Regel sind private Blockchain-Anwendungen Permissioned. Permissioned Blockchains beinhalten ein zentrales, vertrauenswürdigen Identitäts-Management-System (IMS) und sind daher eher für den Einsatz in Unternehmen oder Konsortien geeignet. Dieses IMS stellt kryptografische Zertifikate an qualifizierte neue Teilnehmer aus, mit denen diese autorisiert werden (Shen und Pena-Mora 2018), aber auch im Betrugsfall identifiziert und zur Rechenschaft gezogen werden (Yaga et al. 2018). Änderungen und Updates können einfacher durch wenige Entscheider beschlossen und durchgeführt werden. Durch die geringe Anzahl an Teilnehmern verringert sich aber auch die Sicherheit und Verfügbarkeit, welche in Public Blockchains aufgrund der großen Anzahl an sich am Konsens beteiligenden Akteuren und der vorhandenen Redundanz der Daten gewährleistet werden. Der Anonymitätsgrad ist aufgrund der Zugriffsbeschränkung grundsätzlich geringer als bei einer Public Blockchain. Konsortiale Blockchains sind Blockchains mit mehreren juristischen Personen, z.B. Unternehmen und lassen sich als eine Kombination aus Permissioned Public und Permissionless Private Blockchain verstehen. Sie werden auch Federated Blockchain genannt (Bonneau et al. 2015). Die Sicherheit wächst auch hier mit steigender Zahl von sich am Konsens beteiligenden Akteuren. Aufgrund des autonomen DLT-Protokolls bedeutet es auch hier erhöhten organisatorischen Aufwand, nachträgliche Änderungen an der Architektur durchzusetzen oder fälschlich durchgeführte Transaktionen, nutzerseitige Verluste von „Accountinformationen“ oder nutzerseitige Hacks rückgängig zu machen. Es besteht jedoch bei Weitem keine Eindeutigkeit in den Bezeichnungen. Das National Institute of Standards and Technology (NIST) (NIST 2017) z.B. kategorisiert die Blockchain nach den beiden Kategorien Permissioned und Permissionless. Permissionless Blockchains sind öffentlich zugänglich, jeder hat das Recht sowohl als User und als Validator teilzunehmen und sind meistens Open, während private Blockchains Open oder Closed (Polyzos und Fotiou 2017) sein können. Die Kategorisierung von Permissionless vs Permissioned kann sich auch auf den Lese- und Schreibberechtigungen beziehen (Carson et al. 2018).

1.2.4 Eigenschaften und grundlegende Vorteile/Herausforderungen

Bei den Merkmalen von DLT muss beachtet werden, dass diese je nach Implementierung unterschiedlich stark ausgeprägt sind und verschiedene Abhängigkeiten untereinander bestehen. Des Weiteren erfüllen auch andere Technologien einige dieser Merkmale oder sie sind in einigen Implementierungen bereits verbessert.

Unveränderbarkeit: Alle Teilnehmer eines Distributed-Ledger-Systems sind Kontrollinstanzen. Werden Daten in das System eingetragen, müssen die Teilnehmer zu einem Konsens kommen. Im Anschluss werden dann die Daten auf allen beteiligten Nodes unabhängig abgespeichert. Damit ist eine spätere Änderung oder Fälschung schwer möglich und erfordert die Kontrolle über die Mehrheit der Knoten im Netz. Je weiter hinten ein Block in der Blockchain angeordnet ist, desto schwerer ist es ihn zu manipulieren, denn ein Betrüger müsste den zu manipulierenden Block verändern und auch jeden darauffolgenden Block bis zum neuesten Block in der Blockchain.

Datensicherheit, Datenschutz, Datensouveränität und weitere rechtliche Aspekte: Dies beinhaltet sowohl die Sicherheit sensibler Daten als auch den Datenschutz. Die Netzwerkteilnehmer müssen zwar ihre Identität nicht preisgeben, dennoch ist es möglich, durch

bestimmte Rückrechnungen Rückschlüsse auf die Identität zu ziehen. Anonymität lässt sich demnach nicht ohne Weiteres erreichen, wohl aber Pseudonymität. Die Inhalte der Blockchain sind im Prinzip transparent und auf sehr vielen Rechenknoten dauerhaft gespeichert. Werden sensible, personenbezogene Daten verwendet, ergeben sich u.a. juristische Probleme (siehe z.B. die DSGVO¹⁷), wie beispielsweise die Rechte auf Berichtigung, Löschen¹⁸ und Vergessen werden. Es ist unklar, wie die neuen Vertragsverhältnisse einzuordnen sind: Wenn autonom handelnde Agenten über die Blockchain selbständig Verträge abschließen, wer hat dann eine gültige Willenserklärung abgegeben? Wer haftet bei Softwarefehlern? Probleme ergeben sich auch dadurch, dass der Ort der Ausführung solcher Verträge nicht bekannt ist oder dass die unmittelbare Beendigung oder Rückabwicklung nicht möglich sind oder dadurch, dass, wenn zusätzlich zur reinen Programmierung rechtliche Prüfungen vorgenommen werden oder diese vorgenommen werden müssten. Schwierigkeiten können sich auch durch die automatische rücksichtslose Durchsetzung von Verträgen ergeben, die ethische Aspekte unberücksichtigt lässt. Eine weitere Frage betrifft die grundsätzliche Regulierbarkeit der Blockchain. Erfahrungen im Bereich der Kryptowährungen zeigen, dass Rechtsverletzungen mit Peer-to-Peer-Technologien in der Praxis nur schwer zu entdecken und gerichtsfest nachzuweisen sind. Zivil- und strafrechtliche Fragestellungen sind weitestgehend noch ungeklärt. Sie betreffen u.a. Verantwortlichkeiten und Haftungsfragen und Datenschutz, aber auch Themen wie die Speicherung strafrechtlich relevanter Inhalte oder die Validität der Daten aus der realen Welt (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019). Das BSI kommt zu dem Schluss, dass die Blockchain nach jetzigem Stand im Allgemeinen nicht als datenschutzfördernde Technologie geeignet ist und nicht ohne Weiteres dazu geeignet, die Datensouveränität der Nutzer zu befördern (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019). Das Löschen von z.B. strafbaren Inhalten erfordert sozusagen eine editierbare Blockchain.

Vertrauen: Blockchain wird in der Literatur auch häufig als „trusted trustless networks“, distributed trust oder als Trust Machine beschrieben (The Economist 2015). Obwohl sich die Nutzer untereinander nicht trauen, wird durch Kryptografie und Konsensverfahren das Vertrauen in die Technologie erzeugt. Für den Datenabgleich werden im Distributed Ledger keine vertrauenswürdigen Institutionen mehr benötigt, denen alle Teilnehmer vertrauen.

Dezentralität/Governance: Innerhalb der Blockchain gelten die programmierten Protokolle als unumstößliche Gesetze, die die möglichen Interaktionen regulieren und ein Handeln ohne überwachende und leitende Instanzen ermöglicht („Governance by the network“) (Sclavounis 2017). Die Software muss allerdings von einem Entwicklerteam programmiert und auch gewartet werden. Die Governance regelt, wie Blockchains produziert, verändert und wie Konflikte zu den festgelegten Protokollen gehandhabt werden (Sclavounis 2017). Die Governance wird als ein relevanter, jedoch weniger diskutierter Aspekt gesehen.

Skalierbarkeit: Skalierbarkeit beschreibt, wie sich Wachstum auf die Leistungsfähigkeit des Systems auswirkt (Tasca und Tessone 2017). Wenn man über die Skalierbarkeit von Blockchains spricht, kann es u.a. um die Anzahl an Knoten und User im Netzwerk, den Datenaustausch im Netzwerk oder die Anzahl an Transaktionen gehen. Diese Faktoren sind jedoch voneinander abhängig.

¹⁷ Datenschutzgrundverordnung

¹⁸ Nach der DSGVO besteht ein Recht auf Löschung personenbezogener Daten. Des Weiteren besteht die Pflicht, strafbare oder rechtswidrige Inhalte zu entfernen wie kinderpornografische Inhalte oder Nachrichten, die von Wikileaks 2010 der Öffentlichkeit zugänglich gemacht wurden (Lumb et al. 2016).

Transparenz: Mithilfe der DLT ist es möglich, Daten für viele Nutzer verfügbar zu machen. Für jeden ist es dann möglich, genau nachzuvollziehen, wem oder welchem Pseudonym welche Informationen, zu welchem Zeitpunkt zur Verfügung gestellt wurden.

Offenheit: Die Blockchain kann so konzipiert werden, dass es keine Zugangsbeschränkungen gibt und somit potenziell allen offen steht.

Redundanz: Aufgrund der Dezentralität liegt eine immense Redundanz an Datenspeicherung vor, was auf der einen Seite Ineffizienz bedeutet, andererseits vor der Vernichtung von Daten schützt.

Verantwortlichkeit: Rechtliche Fragestellungen, wie die Umsetzung von Vorgaben der DSGVO, die mit Transparenz und Manipulationssicherheit kollidieren, sind noch Gegenstand von Untersuchungen.

Starrheit: Aufgrund der Tatsache, dass die Mehrheit der Knoten Änderungen oder neuen Features zustimmen muss, kann es länger dauern, bis die Änderungen akzeptiert wurden. Des Weiteren besteht die Gefahr der Abspaltung/Aufspaltung (Fork)¹⁹ einer Blockchain. Mit dem Einbau von Smart Rules lässt sich die Starrheit aufweichen. Einige Smart Rules wie die (Mining) Difficulty gibt es bereits.

Neutralität: Gültige Transaktionen werden unabhängig vom Ursprung oder Inhalt propagiert.

Das **Blockchain-Trilemma** besagt, dass man die drei Kerneigenschaften Skalierbarkeit, Sicherheit und Dezentralität immer zulasten der anderen erreicht, bzw. dass alle drei Eigenschaften nicht gleichzeitig maximiert werden können (s. Abbildung 3).²⁰ Das Blockchain/DLT-Trilemma ist höchstwahrscheinlich nicht lösbar. Es ist deshalb anzunehmen, dass es in Zukunft mehrere Blockchains/DLTs nebeneinander geben wird, die dann auf Anwendungsbereiche maßgeschneidert sind.

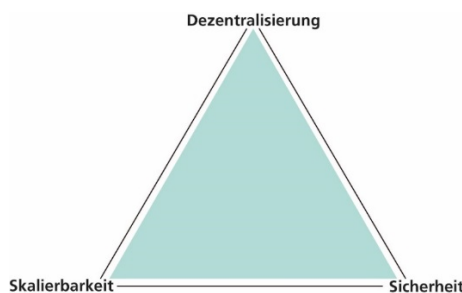


Abbildung 3: Blockchain-Trilemma (eigene Darstellung).

¹⁹ Das Aufspalten einer Blockchain (Fork) kann bei Protokoll-Updates oder Upgrades passieren oder bewusst durchgeführt werden. Der Soft Fork entsteht, wenn unterschiedliche im Blockchain-Netzwerk verwendete Software-Versionen zueinander abwärts kompatibel sind und somit weiterhin miteinander kommunizieren können. Beim Hard Fork können die unterschiedlichen Versionen der Blockchain-Architektur nicht mehr miteinander kommunizieren. Es entstehen zwei separate Stränge.

²⁰ Häufig findet man das Trilemma auch zwischen Konsistenz, Sicherheit und Skalierbarkeit bzw. Effizienz, Sicherheit und Skalierbarkeit dargestellt.

1.2.5 Architektur von Blockchain-Systemen

Es gibt verschiedene Architekturen in Blockchain-Systemen, die diese i.A. in Schichten unterteilen. So können beispielsweise eine Implementierungs- und eine Applikationsschicht unterschieden werden (Drescher 2017), (Glaser). Diese Schichten selbst können jedoch zu weiteren Schichten abstrahiert werden. So können spezifische Eigenschaften der Blockchain wie Sicherheit, Lebendigkeit, Stabilität und Korrektheit bestimmten Schichten zugeteilt werden (Bonneau et al. 2015).

Bei einem anderen Ansatz wird die Sicherheit in der Konsensschicht erreicht und erfordert den Aufbau einer Konsensfunktion, die nicht dazu verleitet, ein alternatives Ledger zu akzeptieren (Xiao 2016). Die Lebendigkeit wird auf der Miner-Schicht erreicht und erfordert einen ausreichenden Anreiz für die Teilnehmer des Netzwerks, kontinuierlich neue Blöcke zu bestätigen. Stabilität wird auf der Propagationsschicht erreicht und erfordert, dass Knoten in der Lage sind, bestätigte Blöcke schnell an andere Knoten zu verteilen, so dass sie auf den neuesten Blöcken aufbauen. Korrektheit wird in der semantischen Schicht erreicht, wo Blöcke eine Bedeutung haben. Des Weiteren gibt es auch hier eine Applikationsschicht²¹.

Ein weiterer Ansatz nutzt ein sogenanntes Computer Interface, das die Integration weiterer Funktionen erlaubt. So lassen sich basierend auf allen getätigten Transaktionen die Bilanzen der einzelnen User der Bitcoin-Blockchain oder zusätzlich komplexere Zustände erstellen, die dynamisch aktualisiert und im Hinblick auf verschiedene Kriterien ausgewertet werden können, wie beispielsweise bei Smart Contracts (Casino et al. 2019). Die Governance erweitert die Blockchain-Architektur, um menschliche Interaktionen in der realen Welt abzubilden. Um eine langfristige Funktion der Blockchain zu gewährleisten, müssen Menschen von außen auf das System zugreifen, um neue Methoden zu integrieren oder das System zu aktualisieren. Diese notwendigen Vorgänge beinhalten Prozesse außerhalb der Blockchain. Die Blockchain Governance kümmert sich darum, wie und von wem diese Prozesse durchgeführt werden (Casino et al. 2019).

1.2.6 Bestandteile

1.2.6.1 Verteilte P2P-Netzwerke

Peer-to-Peer (P2P)-Netzwerke sind ein dezentrales Konzept, d. h. es kommt ohne zentrale Server aus. In diesen Netzen sind alle Rechner im Netzwerk gleichberechtigt, was bedeutet, dass jeder Rechner anderen Knoten Funktionen, Ressourcen und Dienstleistungen anbietet und andererseits

²¹Raikwar et al. (Raikwar et al. 2019) unterscheiden Smart Contract-, Transaktions-, Konsens-, Netzwerk- und Datenbankschicht, während Anwar (Anwar 2018) die Applikations-, Dienste-, Protokoll-, Netzwerk- und Infrastrukturschicht unterscheiden. Yuan Wang (Yuan und Wang 2018) wiederum unterteilt Data, Network, Consensus, Incentive, Contract und Application Layer.

von ihnen selbiges nutzen kann. Die Daten bei DLT liegen in solchen Netzwerken auf vielen Rechnern redundant vor. Dies bietet eine hohe Ausfallsicherheit und Zensurresistenz.

1.2.6.2 Hashing und Kryptografie

Um trotz der transparenten Eigenschaften der Blockchain-Technologie ein hohes Maß an Manipulationssicherheit zu erreichen, kommen kryptografische Mechanismen zum Einsatz. Dabei spielen die Hashing-Mechanismen in der Blockchain bei Transaktionen, Blockbildung sowie bei der Verkettung der Blöcke eine zentrale Rolle.

Bekannte Hash-Funktionen sind u. a. SHA („Secure Hash Algorithm“), welcher auch in der Bitcoin-Blockchain als SHA-256 verwendet wird und KECCAK-256, wie er in Ethereum genutzt wird (Wood). Um als sicher zu gelten, müssen Hash-Funktionen einige Bedingungen erfüllen. So muss z.B. die Wahrscheinlichkeit, dass verschiedene Inputs denselben Hashwert erzeugen, gegen null gehen (Kollisionsresistenz). Aus einem kryptografischen Hash muss es praktisch unmöglich sein, die zugrundeliegende(n) Information(en) ohne erheblichen Aufwand zu errechnen („one-way-function“) und derselbe Input muss immer denselben Hash generieren. Ein Hash muss schnell berechnet werden können, um einen effizienten Einsatz zu gewährleisten ((Merkle 1990), (Bundesamt für Sicherheit in der Informationstechnik 2018)). Zum Hashing größerer Datenmengen kommen zudem sogenannte Merkle-Trees zum Einsatz. Bei den Merkle Trees werden die Hashes einzelner Transaktionen eines Blocks sukzessive zu einem einzigen Hash kombiniert (Merkle 1988).

Die Blockchain-Technologie bedient sich neben dem Hashing zur Sicherung der Integrität der Daten, Vertraulichkeit, Verbindlichkeit, Zurechenbarkeit und Authentizität auch der asymmetrischen Kryptografie. Bei der asymmetrischen Verschlüsselung werden für die Ver- und Entschlüsselung unterschiedliche Schlüssel eingesetzt, ein öffentlicher und ein privater Schlüssel (public and private key). Statt einem Benutzernamen und einem Passwort, wählt der Nutzer eine willkürliche Zahlenkombination als private key aus. Dieser wird in einem Wallet²² gespeichert (Antonopoulos 2018). Aus diesem kann in Folge ein zugehöriger public key durch eine Einwegfunktion errechnet werden (leichte Richtung). Mit dem öffentlichen Schlüssel, der allgemein verfügbar ist, kann nun von einem beliebigen Sender eine Nachricht verschlüsselt werden. Diese kann dann nur von dem Nutzer mit dem passenden privaten Schlüssel entschlüsselt werden. So kann der Sender sicher sein, dass nur der Empfänger die Nachricht einsehen kann. Dieser öffentliche Schlüssel des Empfängers kann zusätzlich - nachdem er zur Sicherheit noch mehrfach umgewandelt/„verhasht“ wurde - ähnlich wie eine Kontonummer genutzt werden.

²² Ein Wallet dient der Schlüsselaufbewahrung und als Kommunikationswerkzeug mit der Blockchain. So zeichnet sie u.a. Transaktionen auf, an denen der öffentliche Schlüssel der Wallet beteiligt ist. Sie enthält jedoch keine Token (Voshmgir 2019).

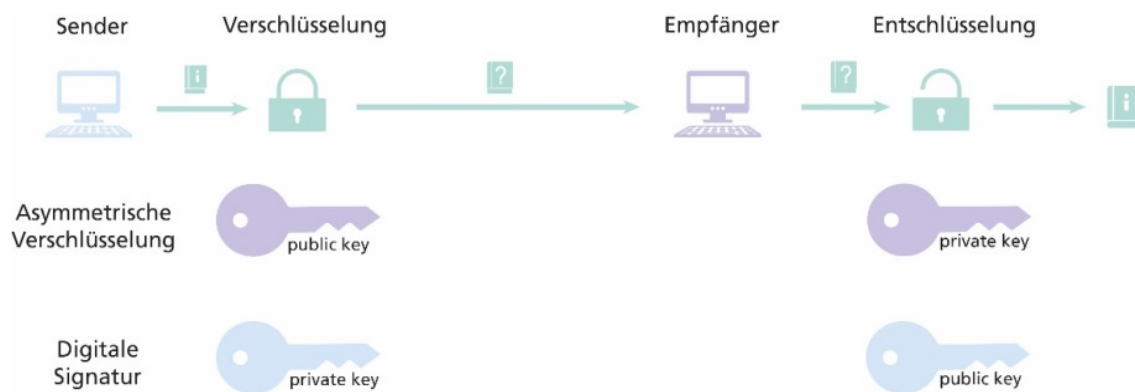


Abbildung 4: Asymmetrische Verschlüsselung und digitale Signatur (eigene Darstellung).

Die Authentifizierung von Nutzern einer Blockchain kann durch eine Digitale Signatur erfolgen. Hierbei wird ein privater Schlüssel erzeugt, mit dem eigene Dokumente, Nachrichten oder Transaktionen signiert werden. Der dazu gehörige öffentliche Schlüssel des Nutzers wird, wie bei der asymmetrischen Verschlüsselung, aus dem private key erstellt. Dieser kann dann durch den Empfänger dazu eingesetzt werden die verschlüsselten Daten zu entschlüsseln. Durch dieses Vorgehen können sich die Empfänger sicher sein, dass die Nachricht oder Transaktion des Nutzers authentisch ist.

Zur Erstellung eines Schlüsselpaares auf einer Blockchain wird in der Regel ein standardisierter Signaturalgorithmus, der sogenannte Elliptic Curve Digital Signature Algorithm (ECDSA) verwendet (Bitcoin Community 2018).

1.2.6.3 Konsensbildung

Im P2P-Netzwerk liegt jedem Teilnehmer (Full Node) im Prinzip eine eigene Kopie der gesamten Blockchain vor. Ziel des Konsensverfahrens ist es, die Daten auf einem gemeinsamen, aktuellen Stand zu halten. Damit wird die Blockchain über das Netzwerk hinweg in einem konsistenten Zustand gehalten (BSI – Bundesamt für Sicherheit in der Informationstechnik). Die Knoten im Netzwerk müssen die Transaktionen und deren Reihenfolge bestätigen, in der sie in einem neuen Block angeordnet sind. Wenn die Überprüfung von den einzelnen Knoten unterschiedlich ausfällt, haben die Knoten im Netzwerk verschiedene Zustände derselben Blockchain. Bei einer solchen Uneinigkeit arbeiten die Knoten solange an ihrer eigenen Blockchain weiter, bis sie über eine längere Blockchain informiert werden, die regelkonform dann als die richtige angesehen wird. Die kürzeren Arme werden kurzzeitig zu verwaisten Ketten (Orphan Chains) (s. Abbildung 5), deren Transaktionen wieder zurück in den Pool an unbestätigten Transaktionen (Unspent Transaction Output (UTXO)) gehen (Fraunhofer FIT). Aus diesem Grund ist es sicherer, einige Blockbildungszyklen abzuwarten bis davon ausgegangen werden kann, dass die Transaktion auch wirklich „gilt“.

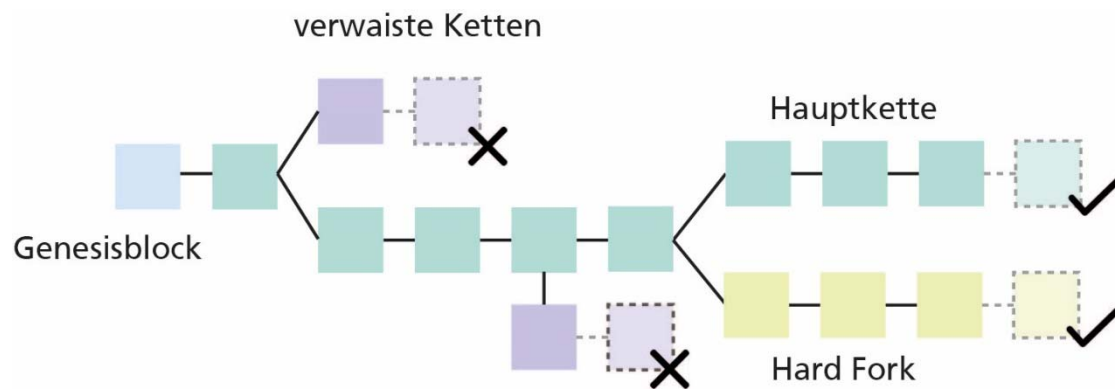


Abbildung 5: Blockchain (eigene Darstellung).

Bei diesen Verfahren können jedoch auch längerfristige Probleme auftreten, z.B. hervorgerufen durch Protokoll-Updates oder Upgrades (Lin und Liao 2017). Dabei kann es auch zu einer Aufspaltung einer Blockchain kommen, zu einem sogenannten Fork bzw. einer Gabelung der Blockchain. Ein Soft Fork entsteht beispielsweise dann, wenn unterschiedliche im Blockchain-Netzwerk verwendete Software-Versionen, die zueinander abwärts kompatibel sind und somit weiterhin miteinander kommunizieren können, verwendet werden. Dabei akzeptieren die Nodes sowohl das alte als auch das neue Protokoll. „Alte“ und „neue“ Nodes arbeiten weiterhin zusammen, bis sich alle Nutzer auf den Einsatz der neuen Software verständigt haben. Bei Hard Forks können die unterschiedlichen Softwareversionen der Nutzer der Blockchain-Architektur jedoch nicht mehr miteinander kommunizieren. Daher kommt es zu einer echten Spaltung der Blockchain. Es entstehen zwei separate Stränge, wobei die neu gebildete Blockchain nicht unbedingt stabil sein muss.

Konsens-Protokolle

Um innerhalb des dezentralen Netzwerks eine Übereinkunft über den aktuellen Stand der Blockchain zu treffen, werden Konsens-Protokolle eingesetzt. Diese Mechanismen stellen im Wesentlichen sicher, dass sich alle beteiligten Knoten auf den gleichen Block einigen ((Baliga 2017), (Castor 2017)). Sie funktionieren ohne Intermediäre und verhindern Double Spendings²³ oder Sybil-Attacken²⁴. Weiterhin können sie dafür sorgen, dass der Datenaustausch zwischen den Knoten auch dann funktioniert, wenn einige Knoten versuchen, die Blockchain zu manipulieren, d.h. wenn diese Knoten kompromittiert wurden (Byzantinischer Fehler²⁵).

²³ Beim Double Spending versucht ein User, die gleichen Bitcoins parallel an unterschiedliche Empfänger zu verteilen.

²⁴Ein Angreifer kriert dafür eine große Menge von Accounts, um Mehrheitsabstimmungen und die Netzwerk-Organisation zu beeinflussen, das Netzwerk gezielt zu verlangsamen, die Vernetzung im Netzwerk zu stören oder etwa Kommunikation zwischen anderen Peers abzuhören.

²⁵ Byzantine Fault Tolerant (BFT) Systeme lösen das sogenannte Problem der byzantinischen Generäle (Lamport et al. 1982): Byzantinische Generäle mussten eine Stadt von mehreren Stellen aus gleichzeitig angreifen, um erfolgreich zu sein. Nun bestand die berechtigte Gefahr, dass sich unter den Generälen Verräter befanden und Falschinformationen verbreiteten bzw. dass ausgesandte Boten der Generäle zur Abstimmung des Angriffs abgefangen wurden. Von dem Problem selbst gibt es verschiedene Varianten. Für 2 Generäle bzw. mehr als 1/3 bössartiger Generäle gibt es mathematisch gesehen (noch) keine Lösung für das Problem.

Neue Blöcke werden von jedem Knoten im dezentralen Netzwerk auf Validität überprüft. Wie die Entscheidungen im Netzwerk zu einem gemeinsamen Konsens überführt werden, um den neuen Block entweder an die Blockchain anzuschließen oder zu verwerfen, ist im Protokoll hinterlegt. Grundsätzlich gilt, wenn eine Mehrheit an Knoten im Netz der Validität eines Blocks zustimmt, wird dieser an die Blockchain angefügt. Die neue Version der Blockchain wird abgespeichert und alle Transaktionen im neuen Block ausgeführt. Diese sind nun Teil der Blockchain und dementsprechend unveränderbar in der Blockchain hinterlegt. Alle Knoten im Netzwerk arbeiten dann mit der nun verlängerten Blockchain (Nofer et al. 2017).

Die Konsensmechanismen sind u.a. abhängig von der Netzwerkarchitektur und dem Blockchain-Typ. Bei der Lösung des Konsensproblems müssen folgende Bedingungen erfüllt sein: Gültigkeit (validity), Integrität (integrity), Übereinstimmung (agreement) und Beendigung (termination). Aufgrund der Relevanz der Konsensverfahren hat sich ein neues Forschungsfeld herausgebildet, das sich intensiv mit optimierten Konsens-Logiken auseinandersetzt und auf spieltheoretischer Basis testet und beweist. Derzeit existiert deshalb eine derart große Vielzahl an unterschiedlichen Konsens-Modellen mit unterschiedlichem Entwicklungsstatus und individuellen Vor- und Nachteilen, dass hier nicht alle diskutiert werden können. Im Folgenden werden einige wichtige Konsens-Protokoll-Typen vorgestellt (Zhang und Lee 2019), (Firdaus et al. 2019).

Dezentrale Systeme sind u.a. mit Problemen wie hohen Netzwerklatenzen, Übertragungs- und Softwarefehlern, Sicherheitsverletzungen, Hackerangriffen und dergleichen konfrontiert. Diese Herausforderungen müssen die Systeme adressieren, um praxistauglich zu sein.

Konsensmechanismen lassen sich grob in nachrichten-, nachweis- und abstimmungsbasierte Algorithmen unterteilen (NExT e.V. in Zusammenarbeit mit der Initiative "Blockchain in der Verwaltung Deutschland" (BiVD) und der Community of Practice Blockchain des NExT-Expertennetzwerks 2019). Die bekanntesten und am weitesten verbreiteten Beispiele wie Proof-of-Work oder Proof-of-Stake gehören zu den nachweisbasierten Verfahren, die auf dem Konzept einer eingeschränkten Ressource beruhen, deren Knappheit die willkürliche Manipulation durch Angreifer erschweren soll.

Wird die Fehlertoleranz der Konsensmechanismen als Kategorisierungskriterium gewählt, lassen sich die Crash-Fault-Tolerant (CFT), Byzantine-Fault-Tolerant (BFT), asynchronous-Byzantine-Fault-Tolerant (aBFT) (Hedera Hashgraph 2018) und undefinierte Konsensmechanismen unterscheiden. CFT-Systeme garantieren dabei eine Sicherheit über das Erreichen des korrekten Konsens, solange weniger als 50% der Knoten im System ausfallen, wobei dies die einzige tolerierte Fehlerart eines Knotens darstellt²⁶ (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019), (Dwork et al. 1988). Zu den CFT-Systemen zählen u.a. Raft und Paxos. BFT-Systeme können die Konsistenz und Lebendigkeit des DLT gewährleisten, solange weniger als 1/3 (je nach Algorithmus kann die Grenze auch deutlich niedriger sein) der Knoten im System fehlerhaft oder manipuliert sind. Dies gilt allerdings nur, wenn die Knoten innerhalb einer bekannten Zeitspanne miteinander kommunizieren können (Castro und Liskov 2002), (Dwork et al. 1988). Für aBFT-Systeme, wie sie Hashgraph verwendet, gilt letztere Einschränkung nicht, so dass sie unter realen Bedingungen im Internet im Hinblick auf verschiedene Angriffsvektoren die Unaufhaltsamkeit und die Korrektheit des Konsenses garantieren (Baird 2016). Die als undefiniert bezeichneten Algorithmen erlauben aufgrund ihrer auf Wahrscheinlichkeiten und spieltheoretischen Mechanismen basierender Natur keine formale Einstufung oder gar Beweisführung über deren Sicherheitsniveau (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019). Hierunter fallen der Proof-of-Work-Ansatz,

²⁶ Je nach Konsens-Verfahren können allerdings solche Systeme sogar durch die gezielte Manipulation eines einzigen Leader-Knotens ihre Lebendigkeit verlieren (Fischer et al. 1985).

unterschiedliche economy-based Mechanismen mit Proof-of-Stake (PoS), aber auch einige auf Directed Acyclic Graphs (DAG) basierende Ansätze wie der Tangle von IOTA.

Der **Proof-of-Work** (PoW)-Algorithmus war in der Blockchainwelt der erste funktionierende Konsens-Mechanismus (Nakamoto 2008) und ist bis heute der am weitesten verbreitetste in einer Public und Permissionless Umgebung (Baliga 2017). Das Grundprinzip basiert auf einem Verfahren, das den Aufwand durch den Teilnehmer an dem Konsensmechanismus nachweist, der betrieben werden muss, um eine Aufgabe zu lösen. Im Rahmen dieses als Mining bezeichneten Vorgehens muss z.B. bei Bitcoin ein kryptografisches Rätsel gelöst werden. Aufgabe des Miners ist es, die Informationen aus anstehenden Transaktionen und den vorhergehenden Block mittels eines Hashing-Algorithmus in eine Zahlenkombination bestimmter Länge zu überführen, wobei das Ergebnis bestimmte Vorgaben erfüllen muss, die die Schwierigkeit²⁷ (Difficulty) des Rätsels bestimmen. Umgesetzt wird diese durch die Anzahl der ersten Ziffern in diesem Hash, die den Wert 0 besitzen sollen. Dazu muss der Miner einen frei wählbaren Parameter, die sogenannte Nonce, so lange variieren, bis das Ergebnis den Anforderungen entspricht. Im Bitcoin-Netzwerk ist die Geschwindigkeit, mit denen die Werte durchgespielt werden, die sogenannte Hash-Power, im Bereich von Exahashes pro Sekunde (10^{18} Hashes/s). Mit diesem Prozedere lässt sich vermeiden, dass Akteure eine „Fakechain“ (Wobst 2019) konstruieren – dazu wäre ein Vielfaches der globalen Rechenleistung aller Miner notwendig. Wurde ein Ergebnis von einem Miner gefunden, kann dieses durch einmalige Ausführung der Hash-Funktion mit der gefundenen Nonce von allen beteiligten Knoten bestätigt werden. Der Miner mit der richtigen Lösung wird mit neu geschaffenen Bitcoins vergütet. Da im Falle des Bitcoin-Netzwerks die maximale Anzahl an Bitcoins²⁸ limitiert ist, wird entsprechend in regelmäßigen Abständen die Vergütung für einen gefundenen Block, der sogenannte Block Reward, reduziert²⁹. Zusätzlich zum Block Reward³⁰ erhält der Miner eine Transaktionsgebühr, die für jede Transaktion vom Sender bezahlt wird (Baliga 2017), (Castor 2017). Der neu erzeugte Block wird mit den vor ihm liegenden Blöcken verknüpft. Es kann, wie oben beschrieben, passieren, dass zeitweise mehrere Ketten parallel existieren, wobei sich nach einer gewissen Latenzzeit immer die längste valide Kette als richtig herausstellt (Mingxiao et al. 2017). Bei dem PoW-Vorgehen besteht das Problem, dass es zu einer Konzentration von großen Mining-Kapazitäten in einzelnen Pools / Mining Farmen³¹ kommt, die maßgeschneiderte Application Specific Integrated Circuit (ASIC) einsetzen. Aufgrund des enormen Energieverbrauchs sind solche Pools auf Standorte mit niedrigen Energiekosten wie z.B. China und Island begrenzt. Um Monopolisierungstendenzen entgegenzuwirken, die dem Dezentralisierungsgedanken widersprechen, gibt es zunehmend Bestrebungen, der Hardwareabhängigkeit mit mehr oder weniger Erfolg entgegenzuwirken (ASIC-Resistance) (Bitcoin Community 2018), (Turan et al. 2011), (Hadedy et al. 2010), (Duffield und Diaz 2018). Um die Kette manipulieren zu können, müssten gemäß dem mehrheitlichen Konsens mehr als 50% der weltweiten Hashing-Power von einer Instanz kontrolliert werden, was mit einem enormen finanziellen Aufwand verbunden wäre und somit das Risiko von Manipulation reduziert. In Bezug auf den hohen Energieverbrauch der Blockchains mit PoW-Konsensalgorithmus gibt es zwei Fragen, die es zu beantworten gilt: (1) Wie kann man den Energie-Verbrauch der Blockchain senken? (2) Kann man die Rechenleistung anwenden, um dabei sinnvolle Berechnungen

²⁷ Der Schwierigkeitswert wird durch den Bitcoin Mining Algorithmus dynamisch angepasst, so dass trotz fortwährend steigender Rechenleistung von Computerhardware die Erzeugung eines Blocks ca. 10 min in Anspruch nimmt.

²⁸ auf ca. 21 Mio. Coins

²⁹ Alle 210 000 Blöcke, die in etwa vier Jahren zustande kommen, findet ein Halving statt, bei der der Block Reward halbiert wird. Gestartet mit 50 BTC, liegt der Wert 2019 bei 12,5 BTC, 2020 bei 6,25 BTC.

³⁰ Crypto-Token Mining

³¹ Die größten Mining-Kapazitäten befinden aktuell u.a. in China, USA, Island, Schweiz und Russland (O'Neal 2019). Alleine die fünf größten BTC-Mining-Pools BTC.com, AntPool, SlushPool, F2Pool und BTC.TOP schürfen zusammen knapp 60 % aller Bitcoin-Blöcke (Schneider 2019).

durchzuführen? (Casino et al. 2019). Ansätze zur Senkung des Energieverbrauchs von Blockchain bestehen in der Entwicklung von neuen Konsens-Mechanismen, die weniger Rechenleistung benötigen (siehe z.B. auch (Sompolinsky und Zohar 2013) oder (Decker et al. 2014)). Es gibt zudem bereits verschiedene Projekte, die sich mit Frage auseinandersetzen, wie man die Rechenleistung sinnvoll nutzen könnte. Primecoin fordert die Miner dazu auf, lange Reihenfolgen von Primzahlen statt Computer-Hashes zu generieren. Weitere Anwendungsbereiche stellen Genome Sequenzierung oder Personalised Genomics dar, die Datenverarbeitung im großen Stil benötigen (Casino et al. 2019). Bitcoin als bekannteste Blockchain und Währung mit der höchsten Marktkapitalisierung (ca. 136 Mrd. US \$, Stand: Oktober 2019 (CoinMarketCap 2019)) verwendet ein auf PoW basierendes Konsensmodell namens HashCash (Castor 2017), Ethereum Ethash, das sich zusätzlich dadurch auszeichnet, eine höhere ASIC-Resistenz, also einer Resistenz gegenüber Mining Farmen zu besitzen (Baliga 2017). PoW besitzt relativ lange Transaktions-Bestätigungszeiten – im Bitcoin-Netzwerk sind ca. 7 Transaktionen pro Sekunde (tps) möglich, während Transaktionsraten bei MasterCard oder VISA im Mittel 4 000 (maximal 56 000) tps erreichen, so dass sich diese Art der Konsensbildung in diesem Bereich nicht eignet. PoW bieten zwar eine hohe Sicherheit, aber eine schlechte Skalierbarkeit. Weitere Nachteile sind die fehlende Finalität und keine 100%-ige Sicherheit (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019). Auch das häufig vorgebrachte Argument, dass Angriffe durch die Miner aufgrund des mit PoW verbundenen Anreizsystems ökonomisch nicht sinnvoll sind, lässt z.B. außer Acht, dass ein Angreifer über finanzielle Anreize außerhalb des Blockchain-Netzwerks verfügen kann. Solche Goldfinger-Angriffe könnten etwa die Destabilisierung einer Kryptowährung zum Ziel haben (Kroll et al. 2013).

Die Erstellung von neuen Blöcken im **Proof-of-Stake** (PoS), als Beispiel für sogenannte economy-based Konsensmechanismen, wird auch als Schmieden (Forging) beschrieben, um den Unterschied zum Mining von neuen Blöcken im PoW zu verdeutlichen. Statt Hardware und Ressourcen bieten die potenziellen Validatoren im Proof-of-Stake (PoS)-Algorithmus eine Art Pfand (Einlage, stake) an, den sie – zusammen mit dem Recht am Forging-Prozess teilzunehmen – verlieren können, falls sie sich nicht regelkonform verhalten. PoS ist daher ohne gekoppelte Kryptowährung nicht möglich. Die Auswahl des Validators für die Blockerstellung erfolgt abhängig von dieser Einlage entweder randomisiert oder auf Basis des Coin-Alters. Letzteres ermöglicht auch den nicht wohlhabendsten Knoten an den Konsensverfahren teilzunehmen. PoS-Blockchains starten entweder mit einem Vorverkauf von Coins oder launchen erst mit dem PoW-Konsensprotokoll, um dann später auf PoS umzustellen. Die Berechnungen in PoS benötigen deutlich weniger Energieressourcen, denn es muss hier nur bewiesen werden, dass ein bestimmter Betrag an eine Art treuhänderischen Tresor gesendet wurde (Baliga 2017), (Ethereum Community 2019), (Vavilov et al. 2015). Entlohnt werden sie über Transaktionsentgelte. PoS bietet aufgrund ökonomischer Überlegungen eine Art Sicherheit. Eine manipulierende Marktmacht müsste 51% der Gesamtzahl der Coins kaufen, um das Netzwerk zu kontrollieren. Damit würde sowohl der Markt mit einer schnellen Preissteigerung reagieren als auch die Kosten des Angriffs in die Höhe getrieben (Vavilov et al. 2015), womit der Anreiz eines solchen Angriffs sinkt (Bitcoin Community 2018). Mit dem PoS sind deutlich kürzere Block-Zeiten und somit höhere Transaktionsraten möglich (Manning 2016), (Zamfir 2015), (Ethereum Community 2019). Der PoS-Algorithmus wurde erstmals bei PeerCoin genutzt (Mingxiao et al. 2017). Mittlerweile gibt es einige Kryptowährungen, die PoS verwenden. Ethereum läuft aktuell noch mit PoW, plant jedoch einen Wechsel zu PoS (s. auch Kapitel 1.2.8). Beim PoS ergibt sich die Gefahr, dass Validatoren nach einem Fork mit einer einzigen Einlage auf verschiedenen Zweigen weiterarbeiten, wodurch u.a. die Gefahr des Double Spendings und des Einkassierens von doppelten Gebühren besteht. Hier gibt es jedoch bereits Ansätze, dass der Validator in einem Zweig mit dem Betrag belastet wird, den er auf dem anderen Zweig erhalten hat (Nothing at Stake-Problem). Beim PoW besteht die Gefahr nicht in dem Maße, da die Miner dann ihre Hashpower auf beide Zweige verteilen müssen, wodurch sich ihre Wahrscheinlichkeit erniedrigt, den Rechenwettbewerb zu gewinnen. Beim *delegated-Proof-of-Stake* (dPoS)-Ansatz nehmen Delegierte in Vertretung vieler kleiner Akteure

an dem Konsensmechanismus teil. Eingesetzt wird das System z. B. bei BitShares (Zheng et al. 2017), (Hammerschmidt 2017). Beim *Liquid-Democratic-Proof-of-Stake* (LDPoS) besteht die Möglichkeit, einen Vertreter zu wählen oder selber am Konsensmechanismus teilzunehmen. Eine ähnliche Lösung ist auch das sogenannte *Leased-Proof-of-Stake* (LPoS), bei dem die Teilnehmer ihre Einlage an die validierenden Knoten verleihen und hierfür eine Vergütung erhalten.

Blockchains mit **Proof-of-Authority (PoA)** zählen zu den Permissioned Blockchains, bei denen der Zugang zum Konsensmechanismus (Tasca und Tessone 2017) erst autorisiert werden muss. Die Algorithmen funktionieren rundenbasiert. In jeder Runde wird ein Knoten gewählt, der als Leader fungiert und die Aufgabe hat, neue Blöcke vorzuschlagen, für die ein verteilter Konsens erzielt wird oder nicht (Prusty 2017) (Angelis et al. 2017). Jeder Nutzer kann im Blockheader die Signatur des Leaders bzw. „trusted signers“ zuordnen. Aktuell gibt es eine Vielzahl von vorgeschlagenen PoA-Protokollen.

Practical-Byzantine-Fault-Tolerance (PBFT) ist ein BFT-Verfahren, bei dem Blöcke deterministisch erzeugt werden können, solange mehr als 2/3 der Prüfer sich auf das gleiche Ergebnis einigen. PBFT setzt voraus, dass jeder Knoten dem Netzwerk bekannt ist. In jeder Runde wird ein Knoten nach bestimmten Regeln für die Durchführung der Transaktion ausgewählt. Die Entscheidung, welcher Block schließlich als rechtmäßig gesehen wird, erfolgt durch einen Mehrundenprozess, bei dem jeder Validator seine Stimme für einen bestimmten Block abgibt. Am Ende des Prozesses sind sich alle aktiven Validatoren darüber einig, ob ein bestimmter Block Teil der Kette ist oder nicht. Ein Client muss also mindestens 1/3 derselben Ergebnisse zurückbekommen, um die Transaktion zu bestätigen/bestätigt zu bekommen (Shen und Pena-Mora 2018), (Christidis und Devetsikiotis 2016).

Das **Tendermint-Protokoll** ist ähnlich zu PBFT mit dem Unterschied, dass hier von den Knoten Coins als Einsatz hinterlegt werden müssen.

Auch das **Ripple-Netzwerk** verwendet einen Konsens-Algorithmus, der sich vom PBFT ableitet. Man unterscheidet hier zwei Typen von Knoten, die Server bzw. Gateways, die am Konsensprozess teilnehmen und die Clients, die lediglich Transaktionen durchführen können. Ein weiterer Ansatz ist *delegated-Byzantine-Fault-Tolerance-Ansatz*, bei dem professionelle Knoten durch ein delegiertes Abstimmungsverfahren von den normalen Knoten ernannt werden (Buntinx 2017).

Proof-of-Elapsed-Time (PoET) stammt von Intel, die momentane Implementierung wird SawtoothLake genannt und ist mittlerweile Teil des Open-Source-Projekts HyperLedger der Linux-Foundation (Hyperledger Sawtooth). Vorausgesetzt wird hier Vertrauen in eine Laufzeitumgebung (Trusted Execution Environment (TEE)), wie Intels Software Guard Extensions (SGX), in der ein Lotterieverfahren läuft, das über zufällig vom Knoten gewählte Wartezeiten für vertrauenswürdige Funktionen einen zufälligen Gewinner ermittelt, der als Leader dann die Blöcke kreiert (Baliga 2017).

Bei dem **Proof-of-Burn** (PoB) müssen die Validatoren einen Teil an Coins zu einer öffentlich verifizierbaren Adresse senden, an die man eigentlich keine Coins schicken kann. Wenn ein Knoten die erforderliche Summe somit vernichtet bzw. verbrannt hat, wird ihm das Recht erteilt neue Blocks zu minen (Salah et al. 2019).

Beim **Proof-of-Activity** (PoAc) werden aktive Nodes für ihre Beteiligung belohnt. Das Konsens-Protokoll ist eine Kombination aus PoW und PoS (Florian Tschorsch and Björn Scheuermann), wird jedoch kaum angewendet. Der Prozess beginnt mit dem PoW, bei dem ein Miner den Rechenwettbewerb gewinnt, wobei der Block je nach Implementierung keine Transaktionen, sondern nur eine Kopfzeile und die Adresse dieses Miners enthält. Nun wird eine zufällige Gruppe von Validatoren aus dem Netzwerk ausgewählt, wobei ihre Chancen erhöht sind, je mehr Coins sie besitzen. Sobald alle in der Gruppe den neuen Block mitsamt ihren Transaktionen signiert

haben, erhält er den Status eines vollständigen Blocks und wird der Blockchain hinzugefügt. Ist jedoch ein Validator nicht online, so verfällt der Block und der Prozess beginnt von neuem. Die Belohnung wird anschließend unter den Minern und Unterzeichnern aufgeteilt (Bentov et al.).

Beim **Proof-of-Capacity** (PoC) wird nicht mit Einlagen oder Rechnerzeit, sondern mit Speicherplatz die Seriosität nachgewiesen.

Neben den genannten Konsens-Mechanismen bestehen eine Vielzahl weiterer Vorschläge und Konzepte (siehe (Raikwar et al. 2019), (Mattila 2016), (Wang et al. 2019b; Wang et al. 2019a)). So gibt es u.a. noch Proof-of-Validation (PoV), Proof-of-Importance (PoI), Proof-of-Existence (PoE), Proof-of-Weight, Proof-of-Prestige (PoP) oder Proof-of-Reputation. Dabei werden oft auch Konsens-Algorithmen kombiniert.

1.2.7 Smart Contracts und dezentrale Applikationen

In modernen Blockchain-Technologien können auch Prozesslogiken hinterlegt werden. Bei dem 1994 von Szabo eingeführten Begriff Smart Contract (SC) handelt es sich um ein Konzept zum automatisierten Ausführen eines bereits wirksam vereinbarten Vertrags. Dabei werden die Vertragsklauseln in Code implementiert und in eine Software eingebettet, die die Inhalte eigenständig umsetzt. Der Name suggeriert einen juristischen Zusammenhang, obwohl es sich bei SC lediglich um Quellcode handelt, der automatisch ausgeführt wird (Vitalik Non-giver of Ether on Twitter). Eigentlich handelt es sich eher um eine Wenn-Dann-Anweisungen bzw. State-Response-Regeln (Yuan und Wang 2018).

Im Blockchain-Kontext bestehen SC aus Quelltext, der auf der Blockchain gespeichert ist. Jeder SC hat eine einzigartige Adresse. Ein SC wird initiiert, indem eine Transaktion an diesen adressiert wird. Danach führt sich der SC im Fall von Ethereum automatisch auf der virtuellen Maschine jedes Knotens im Netzwerk aus (Christidis und Devetsikiotis 2016). Nach der Ausführung eines SC wird das gesamte Netzwerk per Konsens-Protokoll aktualisiert. Im Wesentlichen unterscheiden sich SCs in drei Aspekten von herkömmlichen Verträgen: (1) Sie werden durch Programmcode ausgeführt ohne menschlichen Tätigwerdens. (2) Ein SC kann nicht verändert werden, hierfür muss ein neuer SC unter Zustimmung der an der Transaktion beteiligten Nutzer eingeführt werden. (3) Die Einführung von SC für Vereinbarungen mehrerer verschiedener Nutzer mit verschiedenen Konditionen ist möglich. Dies erlaubt eine hohe Kosteneffizienz bei hoher Flexibilität (Shen und Pena-Mora 2018). Die erste und auch wohl bekannteste Plattform zur Ausführung von Smart Contracts ist Ethereum. Mittlerweile laufen Smart Contracts auf diversen Blockchains/DLTs.

Dezentrale Applikationen (DApps) sind eher mit Computerprogrammen vergleichbar. Sie basieren auf Smart Contracts bzw. erweitern deren Funktionalität (Raval 2016), (Buterin 2013).

Durch die Verknüpfung von mehreren Smart Contracts lassen sich auch sogenannte dezentrale autonome Organisationen (DAO) organisieren, die ohne zentrale Geschäftsführung operieren. Eine Schwachstelle bei Smart Contracts im Allgemeinen und DAOs im Besonderen können Programmierfehler sein. Ein bekanntes Beispiel ist „The DAO“ von Slock.it. Dabei handelte es sich um einen automatisierten Venture Capital-Fonds, der in Startups investiert. Die auf Ethereum basierende DAO besteht im Prinzip nur aus Smart Contracts und einem E-Voting-System. Anteilig an seiner Investitionssumme kann der Investor seine Stimmrechte nutzen, um die Investmententscheidungen des Fonds mitzubestimmen. Eine Software-Lücke führte dazu, dass ein unbekannter Hacker dem virtuellen Investmentfonds im Juni 2016 Tokens im Wert von über 50 Millionen US-Dollar entwenden konnte, indem er eine Funktion zum Anlegerschutz missbrauchte. Diese sah vor, dass Anleger ihre Gelder abziehen konnten, wenn sie mit einer

Investitionsentscheidung der DAO unzufrieden waren. Um den finanziellen Schaden zu beheben, wurde der Source-Code umgeschrieben. Seitdem existieren zwei Versionen der Digitalwährung – Ethereum (mit Änderungen im Source-Code) und Ethereum Classic (ohne Änderungen) (Falkon 2017).

1.2.8 Ausgewählte Blockchain-Beispiele

Die 2008/2009 entstandene **Bitcoin-Blockchain** gilt als Pionier von Blockchain, die weitere Open-Source-Plattformen hervorgebracht hat. Sie wird in diesem Kapitel nicht noch einmal explizit beschrieben, da Aufbau, Eigenschaften und Mechanismen bereits an verschiedenen Stellen in diesem Dokument aufgezeigt wurden.

Ethereum ist wie Bitcoin ein Public Permissionless System. Erstmals 2013 im Whitepaper „Ethereum: A Next Generation Smart Contract & Decentralized Application Platform“ beschrieben und 2015 in Betrieb genommen, wird die Entwicklung heute von der Ethereum Foundation fortgeführt (Buterin 2013). 2017 wurde die Enterprise Ethereum Alliance (EEA) u.a. aus etablierten Unternehmen und Startups gegründet, die dezentrale Lösungen für den kommerziellen Markt entwickelt. Die Entwicklung von Ethereum erstreckt sich von Ethereum Frontier im Jahr 2015, über Homestead und Metropolis mit den Zwischenstufen Byzantium und Constantinople (aktueller Stand) bis hin zu Serenity, in der u.a. der Wechsel zum PoS-Konsensverfahren endgültig vollzogen werden soll. Die Roadmap sieht vor, einen Weg für eine Infrastruktur des Internets von morgen zu ebnen (s. auch Kapitel 5) (Schiller 2018). Mit einer Marktkapitalisierung von ca. 18 Milliarden Euro ist der Ether zweitstärkste Kryptowährung (Stand Oktober 2019) (Coinbase 2019). Mit Ethereum lässt sich nicht nur Geld transferieren, sondern auch Smart Contracts ausführen und DApps erstellen (programmierbare Blockchain). Neben den Transaktionsdaten in der Blockchain gibt es in Ethereum einen übergreifend akzeptierten Systemstatus (world state), der im Speicher der einzelnen Knoten abgelegt ist (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019). Ein Smart Contract von Ethereum wird z.B. in der Programmiersprache Solidity geschrieben und der kompilierte EVM-Bytecode als eigenständige Transaktion ohne Angabe einer Empfängeradresse an das Ethereum-Netzwerk geschickt. Beim Mining wird dem Contract eine neu erzeugte Adresse zugeordnet und der Programmcode in der Blockchain veröffentlicht. Spätere Transaktionen an Contract-Adressen bewirken, dass der entsprechende Contract ausgeführt werden muss – einmal vom Miner bei Aufnahme der Transaktion in einen Block und anschließend von jedem anderen Knoten bei dessen Verifikation. Die Programmausführung erfolgt jeweils lokal in der Ethereum Virtual Machine (EVM) des betreffenden Knotens. Wenn man eine Transaktion oder einen Smart Contract ausführen will, kostet dies etwas, das sogenannte Gas. Man gibt an, wie hoch der maximale Gasverbrauch sein darf sowie den Gaspreis in Ether. Im Normalfall sollte das Programm terminieren bevor das Gaslimit erreicht ist. Ist das nicht der Fall, ist das Gas weg und der ursprüngliche Status des Smart Contracts wird wiederhergestellt. Die Ethereum-Blockchain nimmt derzeit ca. 1TB an Speicherplatz ein. Damit gehen einige Herausforderungen einher, die später diskutiert werden (siehe dazu Kapitel 4.2.1).

Das 2012 ins Leben gerufene **Ripple**-Netzwerk soll sichere, sofortige und nahezu kostenlose globale Finanztransaktionen ermöglichen. Das Netzwerk kann auch ohne die RippleLabs betrieben werden. Zu den Trusted Validators gehören neben RippleLabs, Partnerunternehmen, Internet Service Provider und z.B. das Massachusetts Institute of Technology (MIT). Das Besondere an der Ripple-Technologie ist die Währungsunabhängigkeit, mit der z.B. das Problem gelöst werden soll, dass es bei Cross-Border-Payments aufgrund komplizierter Währungswechsel zu hohen Gebühren kommt, Banken liquide bleiben und sogenannte Nostrokonten in den Empfangsländern besitzen

müssen. Dennoch ist XRP das native, initial erzeugte Token³² des Netzwerks und alle anderen Währungen sind Schuldtitel. Ripple versucht mit dem klassischen Bankensystem zusammenzuarbeiten, wobei Produkte wie On-Demand-Liquidity (ODL)(ehemals xRapid), xCurrent und xVia von den Banken eingesetzt werden können. Als Brückenwährung im Ripple-Netzwerk dient XRP³³. Im Netzwerk agieren sogenannte Gateways als Intermediäre, die eine ankommende Zahlung entgegennehmen und entsprechend weiterleiten. Dabei kann eine Transaktion auch über mehrere Gateways laufen. Ist das der Fall müssen die Schuldscheine (IOUs – I owe you), jeweils von der nachfolgenden Partei ausgeglichen werden. Dadurch können Transaktionen schnell durch das Netzwerk geschleust werden, ohne, dass immer erst auf eine Begleichung der IOUs gewartet werden muss. Im Vergleich zu einer herkömmlichen SWIFT³⁴-Überweisung lässt sich so die Transaktionsdauer um ein Vielfaches reduzieren. In dem Ripple-Register werden also die Schuldscheine der User gespeichert, also welche Person wie viel von welcher Währung einem anderen Individuum schuldet. Neben dem Schuldensystem ermöglicht das Protokoll einen Devisenmarkt, der sich stets weiterentwickelt. Zu den größten Kunden/Partnern von RippleLabs³⁵ gehören u.a. die Bank of America, Santander, American Express, UniCredit und Western Union. Diese fokussieren sich hauptsächlich auf xCurrent. Eine andere von Ripple entwickelte Open Source-Plattform ist Interledger. Dadurch können verschiedene Zahlungsnetzwerke miteinander verbunden werden.

Quorum ist eine konsortiale Blockchain-Software, die auf der Ethereum-Blockchain basiert. Durch gebührenfreie und mit höherem Grad an Privatsphäre ausgestatteten Transaktionen sowie einem alternativen Konsensmechanismus könnte diese Blockchain insbesondere für Unternehmen interessant werden (Baliga et al. 2018).

Das 2015 gestartete Projekt **Hyperledger** ist ein Projektzusammenschluss unter Führung der Linux Foundation, in dem es um Blockchain-Implementierungen und Tools geht. Dabei liegt der Fokus vor allem auf Private und Permissioned Blockchain-Systemen. Projekte beinhalten z.B. unterschiedliche Implementierungsansätze wie Fabric, Sawtooth, Burrow, Indy und Iroha oder Tools wie Composer, Explorer sowie Cello. Hyperledger Fabric wird hier als reifester und aktivster Ansatz näher beschrieben (Hyperledger 2019b), (Androulaki et al. 2018). Ziel von Hyperledger Fabric ist es, ein modular aufgebautes Blockchain-System bereitzustellen, bei dem einzelne Komponenten individuell zusammengestellt werden können. Es handelt sich in erster Linie um eine Plattform für Smart Contracts, hier Chaincode genannt. Es stellt dabei keine Kryptowährung zur Verfügung. Bei Hyperledger Fabric ist die Konsensfindung losgelöst von der Ausführung der Smart Contracts, sowohl bezüglich des zeitlichen Ablaufs als auch bezüglich der verantwortlichen Knoten. Jeder Contract betraut eine Gruppe von Knoten mit seiner Ausführung, die unabhängig voneinander lokal die Ausführung des Contracts simulieren und das Ergebnis an den Aufrufenden zurückmeldet. Ist eine ausreichende Menge an übereinstimmenden Rückmeldungen eingegangen, wird eine Transaktion aufgesetzt und an eine andere Gruppe von Knoten, den ordering service, geschickt. Diese entscheidet mittels eines Konsensmechanismus über die Reihenfolge, in der diese Transaktionen in die Blockchain kommen. Diese Validierung wird dann schließlich von allen Knoten durchgeführt.

³² Insgesamt wurden 100 Milliarden XRP ausgegeben, von denen über die Hälfte im Besitz von RippleLabs sind und der Finanzierung des Projekts und Netzwerks dienen sollen.

³³ XRP dienen dem Währungsausgleich und zur Bezahlung der Transaktionsgebühren, die lediglich Spamversuche abwehren soll und anschließend zerstört werden.

³⁴ Die Society for Worldwide Interbank Financial Telecommunication (SWIFT) betreibt ein weltweites Bankennetz, setzt Standards und bietet Services im Bereich Finanztransaktionen.

³⁵ Da sich Ripple immer mehr auf den kommerziellen Unternehmenssektor richtete, erschufen ehemalige Mitglieder von Ripple Stellar-Lumen, eine Währung, welche sich aber auf den privaten Sektor mit Schwerpunkt auf Entwicklungsländer ausrichtet.

2014 gründete sich das Konsortium R3, initial als reines Bankenkonsortium. Mit **R3 Corda** wurde eine Open-Source-Plattform entwickelt, welche die Interoperabilität zwischen Unternehmen industrieübergreifend verbessern kann³⁶. Corda Settler ist darauf ausgelegt, die Verarbeitung von Zahlungsverpflichtungen, die auf der Corda-Plattform erhoben werden, über jedes Zahlungssystem der Welt, das in der Lage ist, einen kryptografischen Nachweis der Abrechnung zu erbringen, zu ermöglichen, sei es traditionell oder auf Blockchain-basiert. Es nutzt Ripples XRP als ersten Abwicklungsmechanismus.

Der von Facebook initiierte und von der Libra Association betriebene **Libra** (Libra Association 2019) soll Anfang 2020 als Wertanlagen-gestützten Stablecoin eingeführt werden. Technisch gesehen handelt es sich um eine Blockchain, die den Mitgliedern der Libra Association und evtl. Aufsichtsbehörden zugänglich ist. Im Oktober 2019 kündigten jedoch einige der derzeit noch 28 Teilnehmer ihre Mitgliedschaft wieder auf. Dies könnte u.a. im Zusammenhang mit der seit Monaten andauernden Kritik, die das Projekt als potenzielle Gefahr für die gesamte Finanzwirtschaft und für die Autonomie demokratischer Staaten stehen. Diesen gravierenden Punkten, die noch durch die Datenschutzbedenken sowie die Möglichkeit, den Markt zu beherrschen, ergänzt werden können, stehen auch einige positive Punkte entgegen. Insbesondere können hier die Möglichkeit der Inklusion bislang Ausgeschlossener, vor allem in Schwellen- und Entwicklungsländern, genannt werden (Vyjayanti et al. 2018) oder die Beförderung der Standardisierung internationaler Regulierung³⁷. Die designierte Einführung des Libra bietet eine Palette ungeklärter rechtlicher, politischer, gesellschaftlicher und ökonomischer Fragestellungen. Andere sehen die Diskussion um Libra als Anstoß zu einer längst überfälligen Debatte über die Schaffung einer offenen globalen Zahlungsinfrastruktur (Weizsäcker et al. 2019). Als Reaktion auf Libra kündigte die chinesische Zentralbank eine digitale Version des Yuan an, um die chinesische Souveränität zu verteidigen (Bloomberg News 2019). Die deutsche Bundesregierung stellt in ihrer Blockchain-Strategie (Presse- und Informationsamt der Bundesregierung 2019) dar, dass auch sie keine Stablecoins als Konkurrenz zu nationalen Währungen duldet und plädiert für einen e-Euro (Bankenverband 2019), wie auch (Prinz 2019).

Die ursprünglich 2016 entwickelte und derzeit in der Version 2.0 erhältliche **BigchainDB** verbindet die Vorteile einer Blockchain mit denen von sogenannte NoSQL-Datenbanken³⁸ (BigchainDB GmbH 2018). Sie ist mittlerweile für ausgewählte Anwendungsfälle nutzbar. Aufgrund ihres Designs eignet sie sich hauptsächlich für private Blockchain-Netzwerke, die eine hohe Aktivität und Datenmenge aufweisen. Eine public BigChainDB ist jedoch vorgesehen. **Holochain** ist ein Framework für DApps. Jeder Knoten speichert seine eigene Historie der signierten Transaktionen und synchronisiert Hashes mit anderen Knoten in der sogenannten Distributed Hash Table (DHT). Verteilte Anwendungen werden von Hosts ausgeführt, die die Verarbeitung und Speicherung übernehmen und gleichzeitig Credits verdienen (Harris-Braun et al. 2018). Ein weiteres interessantes Projekt mit vielen interessanten Anwendungsfällen ist **Multichain**, die durch einen Fork der Bitcoin-Blockchain im Jahr 2015 als Private Permissioned Blockchain entstand (Greenspan 2019), (Prinz 2018). **Byteball** ist ein Kryptowährungskonzept. Hier können die sogenannten Daten bzw. Transaktionen enthaltenden Units durch jeden Teilnehmer im Netzwerk veröffentlicht werden. Anfallende Transaktionsgebühren werden an nachfolgende Units entrichtet, die auf sie verweisen. Technologisch ähnelt das Konzept dem Tangle von **IOTA** (s. auch Kapitel 4.5.1), besitzt jedoch einige Besonderheiten, die Byteball zu einem vielversprechenden neuen Projekt machen (Churyumov o. J.). **RChain** ist eine neue Blockchain-Plattform, die Latenz und Durchsatz gegenüber konkurrierenden Projekten,

³⁶ Corda Enterprise nennt sich die kommerzielle Version.

³⁷ Dies sind u.a. die Einlagensicherung, Kundenidentifikation (know your customer, KYC) oder die Bekämpfung von Geldwäsche (anti money laundering, AML).

³⁸ NoSQL steht für „Not only SQL“ und bezeichnet Datenbanksysteme, die einen nicht-relationalen Ansatz verfolgen. Mit ihnen lassen sich u.a. große, exponentiell wachsende Datenmengen performant verarbeiten.

wie Bitcoin, verbessern will. Dies soll mit Hilfe der Rho Virtual Machine Execution Environment gelingen, die mehrere Umgebungen betreiben kann, die jeweils einen Smart Contract ausführen. Diese intelligenten Verträge werden gleichzeitig ausgeführt, was mehrere Blockchains pro Node ermöglicht.

2 ANWENDUNGEN

2.1 Entscheidungskriterien für den Blockchain-Einsatz

Für die Einsatzbewertung von Blockchains für bestimmte Anwendungsbereiche wurden Flow Charts und Frameworks entwickelt, um zu entscheiden, ob eine Blockchain die geeignete technische Lösung für ein gegebenes Problem oder Anwendungsfeld sein kann (Wüst und Gervais 2018 - 2018). Ein Beispiel ist in Abbildung 6 dargestellt.

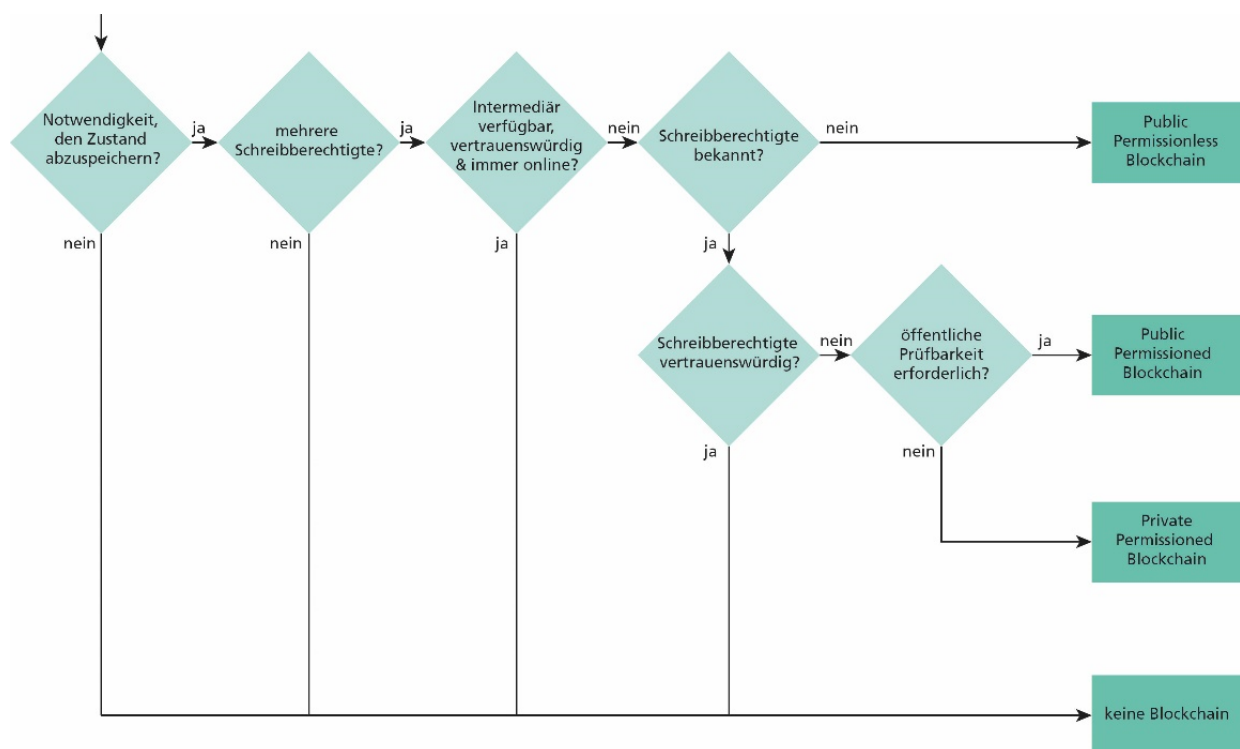


Abbildung 6: Einfaches Flussdiagramm, um festzustellen, ob eine Blockchain die geeignete technische Lösung für das Problem ist (in Anlehnung an (Wüst und Gervais 2018 - 2018)).

Sehr viel ausführlicher können potenzielle Nutzer mit dem Use Case Identification Framework sowie einem Use Case Canvas bei der Frage unterstützt werden, welcher Use Case passend für Blockchain-Technologie ist und welchen Impact diese dann auf den Use Case hat (Klein et al. 2018). Dazu gibt es weitere Veröffentlichungen (Androulaki 2017), (Graham 2018), (Meunier 2018), (Pisa 2018), (Peck 2017), (Suichies 2015). Geeignete Bewertungskriterien müssen alle relevanten technischen Aspekte, funktionale (anwendungsbezogene) Anforderungen sowie die

rechtlichen Rahmenbedingungen und Statuten berücksichtigen. Für das Bundesamt für Migration und Flüchtlinge z.B. wurde ein solches Vorgehen auf Basis des Blockchain Use Case (BUC) Evaluation Framework detaillierter entwickelt (Fridgen et al. 2018a), (Fridgen et al. 2018b). Eine weitere Möglichkeit stellt das Emerging Technology Analysis Canvas zur Analyse der Blockchain-Technologie dar (Perera et al. 2019). Von den Autoren wird betont, dass der Wert und die Notwendigkeit von Dezentralisierung im Vergleich zu zentralisierten und semi-zentralisierten Alternativen oft noch unklar ist und schätzen die Zeit bis zu größeren (finanziellen) Durchbrüchen auf 5-10 Jahre. Noch zu lösende Probleme sehen sie vor allem im Leistungsvermögen, der Unwiderruflichkeit von gespeicherten Daten und dem noch hohen Regulierungsbedarf.

Es hat sich außerdem gezeigt, dass in vielen Anwendungsfällen nicht auf zentrale externe Dienste verzichtet werden kann. Grundsätzlich muss bei der Umsetzung von Lösungen vorab geklärt und Einigkeit darüber erzielt werden, welche Knoten auf der Blockchain welche Rollen und Rechte bekommen sollen. Bei dieser Entscheidung können auch gesetzliche Vorgaben relevant sein. Auch die Frage nach den Kosten spielt in der Praxis bei der Entscheidung für oder gegen den Einsatz der Blockchain-Technologie und der konkreten Ausgestaltung eine große Rolle und ist stark Einzelfall-abhängig (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019).

Während sich die Entwicklungen in der Technologie noch grob prognostizieren lassen, lassen sich die Use Cases kaum prognostizieren (Gassmann und Sutter 2019).

Ein weiterer Rahmen für die Annahme von Blockchain-Anwendungen berücksichtigt institutionelle, marktwirtschaftliche und technische Faktoren (Janssen et al. 2020), andere wiederum legen besonderes Augenmerk auf die Sicherheitsrisiken (Hebert und Di Cerbo 2019). Unterstützungshilfe liefern zudem Modelle von Rogers bzw. davon abgeleitete Vorgehensweisen (Rogers 2003), von Tavares (Tavares et al. 2019) oder von Du (Du et al. 2019).

Kürzlich hat die Bitkom eine Entscheidungsstütze für die Evaluierung und Implementierung von Blockchain Use Cases herausgebracht (Bitkom e.V. 2019). Der Evaluierungsrahmen für Blockchain Use Cases ist dreistufig. Der Auswahl und Strukturierung möglicher Use Cases folgt der Technologie-Check und die Risiko- und Nutzenbewertung. Die Implementierungs-Roadmap ist ebenfalls in drei Phasen aufgeteilt (Ramp Up, Proof of Concept, Scale Up) und stark angelehnt an (Deloitte 2017).

2.2 Anwendungsfelder

Selbst wenn die Blockchain keine mit dem Internet vergleichbare Transformationskraft entwickelt, so zeigen sich die Anwendungspotenziale, auch wegen der recht unterschiedlichen Ziele, enorm vielsichtig. Es gibt derzeit Hunderte von Blockchains mit vielversprechenden und zukunftsrelevanten Anwendungsfeldern und Geschäftsmodellen von unterschiedlichsten Akteuren und das, obwohl die Nutzung von DLT aus rein technischen Gründen aufgrund ihrer geringeren Effizienz gegenüber zentralen Systemen eigentlich nicht sinnvoll ist. Ihr Einsatz ist vielmehr in den meisten Fällen wirtschaftlich bzw. organisatorisch motiviert.

Blockchain und DLT wurden bereits in verschiedenen Anwendungsbereichen eingesetzt, aber es sind durchaus eine große Menge weiterer Anwendungsfelder angedacht oder sogar bereits in prototypischen Umsetzungen. Das Interesse an diesen Technologien hängt insbesondere mit den spezifischen Eigenschaften der Blockchain bzw. DLT zusammen. Dabei müssen nicht immer alle Kriterien für die Implementierung entscheidend sein. In Bezug auf die Datenspeicherung sind jedoch häufig die Merkmale Redundanz und Transparenz von besonderer Wichtigkeit. In DLT-Systemen gespeicherte Daten eignen sich in Bezug auf die genannten Eigenschaften z.B.

besonders gut für Trackingnachweise. Vorstellbar bzw. teilweise demonstriert wurde die Anwendung beispielsweise in den Bereichen Prozesskontrolle, Supply Chain Management, Verkehr, Spenden, Energie, Steuern, Bildung, in der Pharmaindustrie, bei Wahlen oder für Audits jeglicher Art. Des Weiteren können Blockchain und DLT in der Automatisierung von Vorgängen von Vorteil sein, insbesondere in Zusammenhang mit Smart Contracts und deren Einsatz mit ökonomisch autonomen Maschinen (Fridgen et al. 2019). Dadurch, dass Werte als Tokens auf einem DLT dargestellt werden, entsteht zudem eine Kompatibilität unter den virtuellen und realen Werten (Tokenisierung), was insbesondere für Handels- und Finanzströme von Interesse ist. Darüber hinaus können Blockchain und DLT auch in verschiedensten Bereichen zur Integritätssicherung genutzt werden (z.B. von Dokumenten). Hierbei wird urheberrechtlich zu schützendes Material, wie Zeugnisse oder Zertifikate, beispielsweise in Form von Hashwerten in einer Blockchain gespeichert. Die Echtheit der Dokumente kann später mit entsprechenden Signaturen bestätigt werden. Auf eine ähnliche Weise lassen sich Blockchain und DLT zur Identifizierung und zum Zugriffsschutz (Authentisierung und Autorisierung) verwenden oder Identitätsdaten verwalten (Identitätsmanagement). Die Unveränderbarkeit einer Blockchain eignet sich zudem, um (Herkunfts-)nachweise jeglicher Form unzensurierbar und unwiderruflich darzustellen, dabei können sie von Rohstoffen (wie Diamanten), Lebensmitteln und Pharmazeutika, bis hin zum Immobilienmarkt eine Rolle spielen.

Betrachtet man verschiedene Studien zu realen und potenziellen Anwendungsfeldern ((Boucher et al. 2017), (Grover et al. 2018), (Voshmgir), (Lu 2018), (Gatteschi et al. 2018), (Perera et al. 2019), (Blockchain Bundesverband 2018) und (Singh 2018)) wird das Potenzial der DLTs in folgenden Anwendungsfelder am größten eingeschätzt:



Abbildung 7: Anwendungsfelder (eigene Darstellung).

Die Diffusion der Blockchain Technologie in verschiedene Industriebereiche wurde zudem neben einer Analyse der akademischen Literatur auch mit Hilfe von Twitternachrichten untersucht (Grover et al. 2018). Die (antizipierte) Nutzung von Blockchains konnte dabei vornehmlich für die Bereiche Finanzen, Dienstleistungen, Transport und den öffentlichen Sektor bestätigt werden. Die Bereiche Handel und Produktion wurden in diesen Quellen weniger häufig genannt, obwohl

Blockchains und DLT einen wichtigen Baustein rund um das Internet of Things (IoT)³⁹ (Dai et al. 2019) darstellen.

Neben den spezifischen Ansätzen für einzelne Branchen und Industrien konnten auch bereits verallgemeinerte Anwendungsmuster erarbeitet werden. Diese beziehen sich auf den Einsatz von neutralen Plattformen, zur fälschungssicheren Dokumentation, im Zahlungsverkehr, zum Management organisationsübergreifender Prozesse, als digitale Identitäten und Urkunden, für verschiedene Dienstleistungen ohne Dienstleister sowie für ökonomisch autonome Maschinen (Fridgen et al. 2019).

Im weiteren Projektverlauf sollen insbesondere die ersten fünf der oben gelisteten Anwendungsbereiche näher betrachtet und später Geschäftsmodelle entwickelt werden. Daher werden im Folgenden hier diese fünf Anwendungsfelder kurz vorgestellt und im Anschluss das Potenzial einiger weiterer Bereiche angerissen.

2.2.1 Finanzen und Versicherungen

Aus dem Anwendungsfeld Finanzen und Versicherungen werden hier Kryptowährungen und Kapitalbeschaffung stellvertretend dargestellt.

Kryptowährungen

Kryptowährungen sind Blockchain-Systeme mit einer i. d. R. fest vorgegebenen Anzahl an Transaktionsobjekten, den Coins, die ihren Wert durch die Nutzung selbst erhalten. Neben dem Bitcoin als erste und immer noch mit Abstand mit der größten Marktkapitalisierung, gibt es noch Vielzahl weiterer Kryptowährungen⁴⁰ wie Ethereum (ETH), Ripple (XRP), Bitcoin Cash (BCH) oder Tether (USDT)⁴¹. Insgesamt gibt es derzeit ca. 3000 Währungen mit einer Marktkapitalisierung von über 200 Mrd. Euro (CoinMarketCap 2019). Abbildung 8 zeigt ein Kategorisierungsschema für Kryptowährungen, das Yuan (Yuan und Wang 2018) entnommen wurde.

³⁹ Juniper Research hat ermittelt, dass die Gesamtzahl der angeschlossenen IoT-Sensoren und -Geräte bis 2022 50 Milliarden überschreiten wird, gegenüber geschätzten 21 Milliarden im Jahr 2018. Schwerpunkte im Bereich von Unternehmen sind Industrie 4.0, Qualitätskontrolle und Logistik (Juniper Research Ltd 2018).

⁴⁰ Altcoins sind als jede andere Kryptowährung als Bitcoin definiert.

⁴¹ Aufgelistet nach ihrer Marktkapitalisierung (Stand 20. Oktober 2019) (CoinMarketCap 2019).

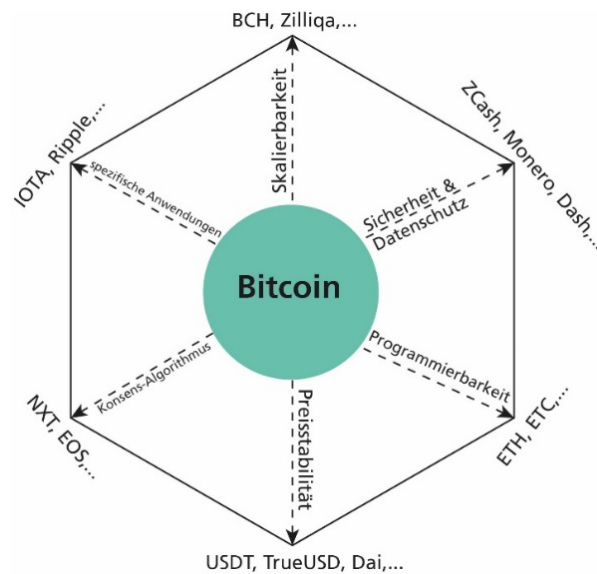


Abbildung 8: Kategorisierung der Kryptowährungen nach Innovationen (eigene Darstellung, in starker Anlehnung an (Yuan und Wang 2018)) .

Kryptowährungen lassen sich mittels Over The Counter (OTC) Services oder an Börsen wie Binance, Gemini, Bitfinex, Coinbase, eToro oder Kraken kaufen oder verkaufen. Aktuelle Kurse und Börsen, auf welchen Kryptowährungen gehandelt werden können, können u. a. (CoinMarketCap 2019) entnommen werden.

Für viele Anwendungsbereiche sind die hoch volatilen Kryptowährungen ungeeignet. Sogenannte Stable Coins sollen durch spezielle Mechanismen die Wertparität zu einem Basiswert, wie z.B. dem US-Dollar halten. Beispiele hierfür sind Tether, TrueUS oder DAI (BTC-ECHO GmbH 2019a).

Im Zuge der Blockchain-Entwicklung wurde neben der traditionellen Finanzierung und Financial Technology Services (Fintech) das Decentralized Finance (Defi) als fester Begriff etabliert, die einen Finanzmarkt frei von Manipulation und Zensur mit einfachstem Zugang für alle verspricht.

Kapitalbeschaffung

Initial Coin Offerings (ICO) sind Smart Contracts auf einer Blockchain, die darauf abzielen, Fremdfinanzierungen durch die Ausgabe von Utility Token oder Coins zu beschaffen (Momtaz 2018). ICOs sind die Verbindung von Crowdfunding bzw. Crowdfunding mit der Blockchain, wobei das Wort an Initial Public Offering (IPO)⁴² angelehnt ist, was fälschlicherweise suggeriert, ein ICO sei vergleichbar mit einer Aktienemission. Es werden jedoch keine Unternehmensanteile zum Kauf angeboten, sondern Utility Tokens oder Coins. In den meisten Fällen dienen die Tokens/Coins der Finanzierung eines dahinter liegenden Projekts. Nach dem ICO werden die Tokens als neue Kryptowährung auf den gängigsten Plattformen und Börsen öffentlich gehandelt. Zum Vergleich dazu handelt es sich beim Venture Capital (VC) um eine zeitlich begrenzte Kapitalbeteiligung an nicht börsennotierten Unternehmen (Breuer 2009). Dabei werden die ICOs die VC Startup-Finanzierung voraussichtlich nicht ersetzen, denn für Investoren bringen sie den Nachteil mit sich, dass sie in den meisten Fällen mit keinerlei Informations- oder Gewinnbezugsrechten verbunden sind und es sich bei den meisten ICOs formal gesehen eher um

⁴² IPO ist das erstmalige öffentliche Angebot einer bislang nicht börsennotierten Aktiengesellschaft (AG) oder Kommanditgesellschaft auf Aktien (KGaA), Aktien des emittierenden Unternehmens zu zeichnen mit der Zielsetzung, diese an einer Wertpapierbörse zum Handel zuzulassen und zu notieren.

Spenden handelt. Eine aktuelle Liste von anstehenden ICOs finden sich z.B. unter (o. A. o. J.), (Smith + Crown 2019). Wegen des großen Missbrauchspotenzials, das in der Vergangenheit des Öfteren ausgenutzt wurde und aufgrund des in einigen Ländern herrschenden Verbots für Kryptowährungen zu werben sowie negativen Regularien und Gesetzgebungen sinkt das Interesse an ICOs. In China sind ICOs sogar seit 2017 verboten. Deshalb haben sich neue Formen der Kapitalbeschaffung entwickelt. Eine davon ist das Initial Exchange Offering (IEO), bei der der Verkauf der Token nicht durch den Coin-Anbieter selbst, sondern über eine Kryptobörse erfolgt. Bei den Initial Futures Offerings (IFO) geht es um Token, die zum Zeitpunkt des Kaufs noch nicht existieren. Bei einem Airdrop werden kostenlos Tokens oder Coins an bestimmte Personen ausgegeben, z.B. zum Zwecke der Kundenbindung. Bei dem Security Token Offering (STO) dienen die Token nicht als Bezugsrecht für später auszugebende Coins, sondern als tatsächliche Vermögenswerte wie Wertpapiere, Immobilien oder Kunstobjekte (<https://www.facebook.com/bitcoinecho>). In dieser Tokenisierung von Vermögenswerten wird ein enormes Potenzial gesehen. Weltweit sind Aufsichtsbehörden damit beschäftigt, hier Rechtssicherheit zu schaffen. In vielen Staaten ist derzeit jedoch noch nicht abschließend geklärt, wie die Tokens steuerlich und juristisch behandelt werden sollen. Weiterhin gibt es keine verbindliche Rechtsprechung, die die Verbindung von Token und Vermögenswert anerkennt und Handelsplätze sind erst im Entstehen (Stockschläger 2019).

2.2.2 Daseinsfürsorge, öffentlicher und juristischer Sektor

Im Anwendungsfeld Daseinsfürsorge, öffentlicher und juristischer Sektor sind die Möglichkeiten für Blockchain und DLT-Lösungen breit gefächert. In diesem Bereich kommt zu den bereits sehr großen Hauptherausforderungen, Sicherheit, Dezentralität und Skalierbarkeit, noch die Gesetzeskonformität. Beispielsweise könnte eine Blockchain-artige Lösung⁴³, in der die Daten einerseits unter der Kontrolle der Bürger bleiben und andererseits Behörden (z.B. Standesämter) prozessübergreifend miteinander kooperieren können, etabliert werden. Selbstsouveräne Identitäten, Koordination Behörden-übergreifender Verwaltungsvorgänge, digitale Verwaltung von Dokumenten und die Modernisierung der Registerlandschaft sind neben Micropayment, Zweckbindung von Zuschüssen, automatischem Einzug von Steuern und Wahlen einige weitere Anwendungsfälle in diesem Bereich. Besondere Anforderungen des öffentlichen Sektors wie die Flexibilität der Programmcodes z.B. zur Berücksichtigung geänderter Gesetzeslage, bei von der DSGVO geforderten Notwendigkeit zur Berichtigung und Löschung der Daten durch berechtigte Instanzen oder zur Realisierung des Recht auf Vergessenwerden eines Individuums stehen mit der der Integritätssicherung bzw. Beweiswerterhaltung dienlichen Unveränderlichkeit einer Blockchain eigentlich im Widerspruch, sind aber durchaus realisierbar (NExT e.V. in Zusammenarbeit mit der Initiative "Blockchain in der Verwaltung Deutschland" (BiVD) und der Community of Practice Blockchain des NExT-Expertennetzwerks 2019).

⁴³ Im öffentlichen Sektor (wie auch im Finanzsektor) kann der Einsatz Permissioned Public Ledger in vielen Fällen vorteilhaft sein, z.B. aufgrund technisch-juristischer Anforderungen wie KYC-, AML- DSGVO- und eIDAS-Konformität oder no-fork Garantien (KYC-Know Your Customer, AML- Anti Money Laundering (Antigeldwäsche), DSGVO-Datenschutzgrundverordnung, eIDAS - electronic IDentification, Authentication and trust Services).

2.2.3 Produktionsökonomie und Industrie 4.0

In der produzierenden Industrie kann durch die Nutzung intelligenter Steuerungsmechanismen/-algorithmen die Produktivität und Effizienz der Produktionssysteme entlang von Wertschöpfungsketten erhöht werden. Hierfür werden vernetzte Informations- und Kommunikationsinfrastrukturen in der Fertigung genutzt, die aktuelle Maschinenzustände, technologische Fähigkeiten von Maschinen, Kundenanforderungen an Produkte und weitere systemrelevante Informationen erheben und aggregieren. Im Kontext von Industrie 4.0 werden verschiedene Plattformen und Methoden zur Erhebung, Verarbeitung und Speicherung entwickelt und bereits angewandt (s. u.a. auch Plattform Industrie 4.0 (Bundesministerium für Wirtschaft und Energie/Plattform Industrie 4.0 2016), (Bundesministerium für Wirtschaft 2016) oder International Data Spaces (Otto et al. 2016)). So werden diese Methoden im Rahmen des Internet of Production dazu verwendet, um mit kontextbezogenen und semantisch adäquaten Daten aus der Entwicklung, Produktion und Nutzung sogenannte digitale Schatten zu erzeugen und Produktionssysteme in Echtzeit anzupassen bzw. zu optimieren (Gehrke et al. 2015), (Trauth 2018a), (Trauth 2018b).

Eine zentrale Herausforderung bei den oben aufgeführten Entwicklungen zur Optimierung gesamter Wertschöpfungsketten bzw. -netzwerke ist der Umgang mit einer Vielzahl beteiligter Akteure. Neben den produzierenden Unternehmen haben weitere Unternehmen wie bspw. Material- und Halbzeuglieferanten (über mehrere Wertschöpfungsstufen), Maschinenhersteller, Werkzeugproduzenten oder Lieferanten von Betriebsstoffen einen signifikanten Einfluss auf das Wertschöpfungsnetzwerk. Dabei wird dem gegenseitigen Vertrauen in z.B. Qualität oder Termintreue bei gleichzeitiger Sicherung des unternehmensinternen Know-Hows große Bedeutung zugewiesen. In diesem Zusammenhang werden DLT als hochrelevante Entwicklungen und technologische Grundlage für eine Vielzahl an Anwendungsfällen betrachtet. Beispielsweise kann die DLT dazu genutzt werden, um relevante Produktinformationen bzw. die Produktqualität entlang der gesamten Herstellung zu verfolgen, Daten und Modelle von Prozessen zu handeln oder die Ökobilanzierung von Fertigungsprozessen transparent zu gestalten.

Zukünftig soll DLT auch dazu genutzt werden, um eine sog. Produktionsökonomie zu etablieren, indem ein vertrauenswürdiger Datenaustausch und intelligente Verträge zwischen Maschinen implementiert werden. In dieser Ökonomie sind selbstüberwachende und autonome Maschinen bzw. Systeme in der Lage, Dienstleistungen zu bestellen (z.B. Wartungen), ihre eigene Produktion zu organisieren und selbstständige Entscheidungen zu treffen (Rajasingham 2017). In diesem Zusammenhang sind ein Maschinendatenmarktplatz, Werkzeug- und Maschinenabonnementmodelle sowie Echtzeit-Leasing zukünftige Entwicklungen.

2.2.4 Logistik und Supply Chain Management

Die Blockchain-Technologie bietet vor allem in der Logistik und im Supply Chain Management großes Potenzial zur Optimierung einer Vielzahl an Prozessen. Anwendungsfelder entstehen überall dort, wo Nachweise über den Gütertransfer oder geleistete Transaktionen erbracht werden müssen. Neben der manipulationssicheren Speicherung können mittels Smart Contracts Prozesse automatisiert und im Zusammenspiel mit cyberphysischen Systemen im Internet der Dinge zunehmend auch autonomisiert werden. Daraus ergeben sich Vorteile wie Kosteneinsparungen, die Optimierung der weltweiten Ressourcennutzung (Effizienz- und Effektivitätssteigerung) oder die Verbesserung von Transportwegen. Durch die Erhöhung von Transparenz, Vertrauen und Planungsgenauigkeit können Unternehmensrisiken gesenkt werden (Pournader et al. 2019).

Die Kombination von Blockchain und Auto-ID-Technik ermöglicht eine Produktnachverfolgung über den gesamten Produktlebenszyklus. Außerdem können Logistik- und Zahlungsprozesse verbessert und Verluste verhindert bzw. Unterbrechungen in Supply Chains verringert werden. So kann beispielsweise im Transportwesen mithilfe der Blockchain eine effiziente Handhabung von Dokumenten ermöglicht werden. Dabei werden unübersichtliche, papierbasierte Vorgänge, die bislang manuell durchgeführt werden mussten, digital abgebildet. Ein weiterer Anwendungsfall für die Blockchain bieten Pay-per-Use-Geschäftsmodelle. Anstelle eines einmaligen Erwerbs einer Maschine bietet Pay-per-Use die Möglichkeit einer nutzungsabhängigen Bezahlung, wie beispielsweise die Abrechnung der tatsächlich angefallenen Betriebsstunden. Die Nutzungsdaten werden dabei in der Blockchain gespeichert und über Smart Contracts kann eine automatisierte Abrechnung erfolgen. Im Bereich Smart Maintenance können Produktionsmittel mit der Blockchain vernetzt werden, um Wartungseinsätze und Instandhaltungsmaßnahmen, bei entsprechendem Condition Monitoring, planbar und koordiniert durchzuführen. Die Blockchain kann bei einem ganzheitlichen Instandhaltungsansatz dazu eingesetzt werden, um diese Maßnahmen automatisch zu initiieren und durchgeführte Tätigkeiten manipulationssicher zu dokumentieren. Über entsprechend ausgelegte Smart Contracts können diese nachweislich erbrachten Instandhaltungsmaßnahmen ferner automatisch verbucht und abgerechnet werden.

Im Sinne einer Plattformökonomie sind Blockchain und Smart Contracts nicht auf die Vermittlung und Interaktion von zwei Partnern beschränkt, sondern können dazu dienen viele verschiedene Partner branchenübergreifend zu vernetzen. Die Abbildung 9 dargestellte Smart Contract Plattform zeigt dabei einen beispielhaften Kreislauf von Waren-, Informations- und Finanzflüssen. In diesem haben alle Partner, vom Lieferanten, über den Spediteur, Banken und Versicherungen bis zum Empfänger Zugriff auf die für sie jeweils relevanten Informationen. Über Smart Contracts können außerdem bei Vertragserfüllung oder auch im Schadensfall automatische Benachrichtigungen und Handlungen angestoßen werden (Henke et al. 2015), (Sabine Jakob et al. 2018).

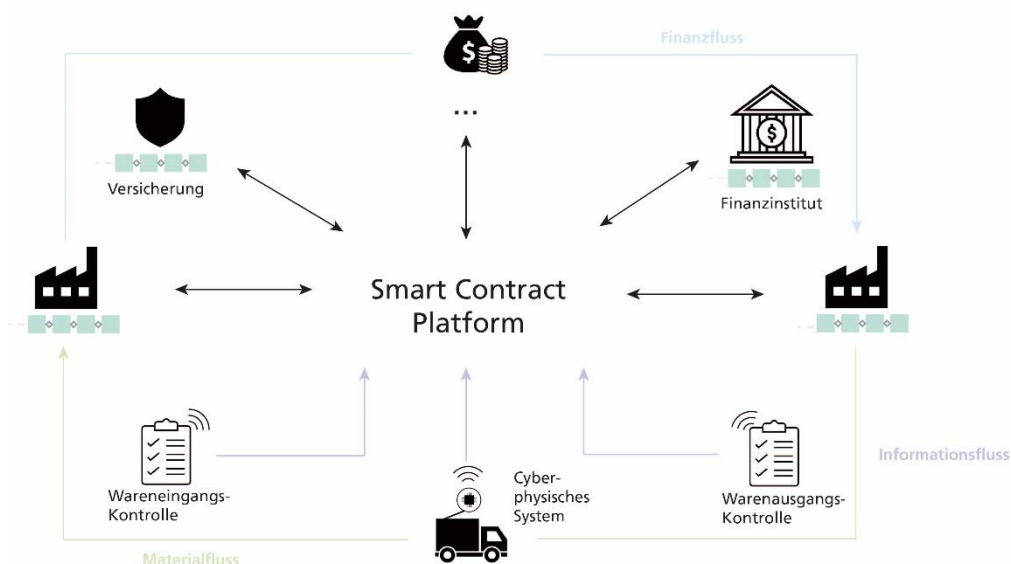


Abbildung 9: Blockchain-basiertes Supply Chain Netzwerk (eigene Darstellung in enger Anlehnung an (Sabine Jakob et al. 2018)).

2.2.5 Energie

Auch die digitale Energiewende könnte durch DLT unterstützt werden, wobei z.B. der Stromhandel, der Lieferantenwechsel, das Assetmanagement und entsprechende Abrechnungsmodelle (Token) besser gemanagt werden könnten. Durch den Ausbau der regenerativen, dezentralen und regionalen Energieerzeugung und die Berücksichtigung der Anforderungen und Flexibilität des Verbrauches sind digitale Technologien in diesem Bereich zunehmend unverzichtbar. In diesem Anwendungsfeld werden auch zunehmend konkrete Anwendungen der DLT gefordert und es wurden bereits erste Pilotprojekte initiiert. So können DLT z.B. innerhalb eines Smart Grids eingesetzt werden, um die Sammlung, Transaktion, Speicherung und Analyse von wesentlichen Daten zu unterstützen. Ein weiteres Ziel ist es, die Kosten für die Herstellung von bestehenden zentralisierten Lösungen, bei denen die Wartung und Verwaltung sehr hoch sind, mit Hilfe von DLT zu senken.

2.2.6 Weitere Felder

Neben den fünf bereits genannten Anwendungsfeldern, auf die im Projektverlauf ein besonderes Augenmerk gelegt wird, sind jedoch auch noch eine Vielzahl weiterer potenzieller Anwendungsfelder für DLT und Blockchain-Lösungen denk- und umsetzbar, wie oben gezeigt.

Im Bereich der Informations- und Kommunikationstechnologien sind Blockchain und DLT-Lösungen beispielsweise zur Netzwerküberwachung und -verwaltung denkbar. Der Handel kann von Konzepten des bargeldlosen Zahlungsverkehrs mit DLT profitieren, insbesondere dann, wenn die Vertrauenswürdigkeit der Handelspartner in Frage gestellt wird. Im Gesundheitswesen müssen die Informationen von Patienten und die Daten der medizinischen Forschung mit unterschiedlichen Parteien geteilt werden. Dabei muss sichergestellt sein, dass sensible personenbezogene Daten nicht unerlaubt weitergegeben oder manipuliert werden können. Die Speicherung von medizinischen und gesund- und ernährungsrelevanten Daten in einer Blockchain birgt in diesem Zusammenhang vielerlei Vor- aber auch Nachteile. Deren Abwägung stellt insbesondere aus datenschutzrechtlicher Sicht große Herausforderungen. Dienstleistungen über die Blockchain-Infrastruktur unterstützen auf verschiedenste Weise die Shared Economy. Im Bereich von Wissenschaft und Bildung ergeben sich mehrere mögliche Anwendungsgebiete für Blockchain und DLT. Neben der bereits genannten Speicherung von Zertifikaten und Zeugnissen, kann im Prinzip auch der gesamte Verlauf von Forschungsprojekten fälschungssicher festgehalten werden. Unter Federführung der Max Planck Digital Library arbeiten bedeutende Forschungseinrichtungen an einer internationalen Blockchain für den Wissenschaftsbetrieb namens bloxberg (Kleinfurter et al. 2020). Im Bereich Kultur und Medien sind DLT u.a. in Hinblick auf Urheberrechtsfragen von Interesse. Auch für weitergehende Sicherheitsanwendungen könnte Blockchain vorteilhaft implementiert werden. Dies betrifft sowohl Safety als auch Security Aspekte, wie z.B. die Überwachung von Lebensmittelketten oder die Inventarisierung von Waffen. Blockchain und DLT eignen sich auch für viele verschiedene individuen-zentrierte Anwendungen wie die Social Networking Anwendungen, Treuepunkte-Angebote sowie verschiedene Arten von Datenverwertungen (Data Marketplaces und Data Monetisation).

Diese potenzielle Vielzahl an Anwendungsfeldern bedeutet jedoch nicht, dass die Anwendung von Blockchain und DLT in diesen Bereichen per se die beste Wahl darstellt. Eine Abwägung aller Einflussfaktoren ist in diesem Kontext von größter Bedeutung. Neben technologischen Faktoren sind auch immer soziale, politische, ökonomische und juristische Faktoren zu berücksichtigen.

2.3 Geschäftsmodelle

Der reale Nutzen von Blockchain und DLT entfaltet sich erst durch die praktische Anwendung und eine ausreichend breite Akzeptanz. Neben der technologischen Machbarkeit und Zuverlässigkeit sowie die generelle Eignung für eine gegebene Aufgabenstellung ist es auch nötig, einen geeigneten wirtschaftlichen Verwertungsrahmen für die Technologien zu finden. Dazu ist die Entwicklung geeigneter innovativer Geschäftsmodelle⁴⁴ nötig. Von einigen Forschern wird dazu die Ansicht vertreten, dass der Wertgewinn einer DLT-Implementierung erst bei komplexen multilateralen Prozessen gegenüber dem Aufwand und den Skalierungsnachteilen groß genug ist (Gassmann und Schmück 2019). Dabei können die durch DLTs angebotenen Wertversprechen beispielsweise fünf Bereichen zugeordnet werden: DLT-basiertes Datenmanagement, Asset-Management, Organisations- und Prozessmanagement sowie der DLT-zugehörigen Hardwareentwicklung und Beratung und Investment (Gassmann und Sutter 2019). Aus diesen können derzeit drei archetypische Geschäftsmodelle identifiziert werden: Zum einen handelt es sich um dezentrale Plattformen (business pull), bei denen die Kunden im Vordergrund stehen, zum anderen um Technologieanbieter (technology push), deren Fokus auf der Weiterentwicklung der Technologie liegen. Als drittes mögliches Geschäftsmodell kann die Technologieberatung bzw. der Einsatz als finanzieller Investor genannt werden.

2.4 Akteure

Eigene Recherchen ergaben, dass die Anzahl an Forschungspublikationen⁴⁵ rasant ansteigt. Über 80% der wissenschaftlichen Artikel wurden allein in den letzten beiden Jahren veröffentlicht. Die meisten Publikationen stammen aus den Bereichen Computer- und Ingenieurwissenschaften sowie Telekommunikation. Gegenwärtig ist China führend, gefolgt von den USA. Mit etwas Abstand folgen u.a. Großbritannien, Südkorea, Indien, Deutschland, Australien, Kanada, Italien, Frankreich, Japan bzw. Russland. Deutschland scheint im Ranking 2019 wieder ein wenig abzufallen. Bestätigt werden konnte dies durch eine ähnliche Studie, die ergab, dass asiatische Staaten, allen voran China, mehr an der Kombination Blockchain und IoT bzw. Anwendungen interessiert sind, während es den USA wichtiger scheint, Daten mit Blockchain zu sichern (Firdaus et al. 2019). Forschungsgelder werden vor allem von der National Natural Science Foundation of China (NSFC) in dieses Thema gesteckt. Relevante Akteure sind u.a. die Beijing University of Posts Telecommunications, Chinese Academy of Science (CAS), Commonwealth Scientific and Industrial Research Organisation (CSIRO), einige weitere chinesische Universitäten wie z.B. die University of Electronic Science and Technology of China oder die Tsinghua University, die University of New South Wales Sydney sowie die Technical University Nanyang. Insgesamt liegt das Feld jedoch nicht so weit auseinander. In den USA sind u.a. die University of Texas System, die University of California System, die National University of Defense Technology sowie das Massachusetts Institute of Technology (MIT) und IBM, in Europa u.a. die University of Cagliari, das Imperial

⁴⁴ Eine neue, relative kurze Definition haben Osterwalder und Pigneur beigetragen - „A business model describes the rationale of how an organization creates, delivers, and captures value.“ (Osterwalder und Pigneur 2010).

⁴⁵ Es wurden Analysen u.a. im Web of Science und Scopus sowie weiteren Publikations- und Patentdatenbanken durchgeführt. Die dargestellten Ergebnisse ergeben sich aus einer Synopse der Analysen. Für eine gesicherte Argumentation sind jedoch ausführlichere Untersuchungen notwendig.

College London, die University of Oxford, Université du Luxembourg, The University of Edinburgh, Delft University of Technology, National Centre for Scientific Research (CNRS) sowie die Swiss Federal Institutes of Technology zu nennen. Deutschland ist u.a. mit der TU Darmstadt, TU München, TU Berlin und dem Karlsruher Institut für Technologie (KIT) vertreten.

Die Anzahl der Patente steigt seit 2015 noch stärker an als die Publikationen⁴⁶. Die USA gefolgt von China nehmen auch hier die Spitzenplätze ein, Deutschland liegt im Mittelfeld. Wichtige Akteure im Bereich der Patentanmeldungen sind u.a. Alibaba Group Holding Ltd., IBM, NChain Holdings Ltd., Bizmodeline Co Ltd., China Unicom, Coinplug Inc., Bank of America, Mastercard International Inc., BOE Technology, Visa oder Fuzamei Technology.

Diese (Datenbank-)Recherchen sollen einen ersten groben Überblick vermitteln. Die Anzahl der globalen Akteure auf diesem Feld, sowohl im wissenschaftlichen als auch im unternehmerischen Umfeld, ist jedoch nahezu unüberschaubar. Dies gilt ebenso für Allianzen und andere Zusammenschlüsse im Kontext von Blockchain bzw. DL. In Europa ist die von der European Union Blockchain Observatory and Forum veröffentlichte European Blockchain Map (EU Blockchain Observatory and Forum o. J.) hilfreich. Für Deutschland und speziell NRW wurde im Laufe des Projekts eine Akteursliste aufgebaut, die einen möglichst umfassenden regionalen Überblick geben soll.

Detaillierte bibliometrische Untersuchungen finden sich zudem in späteren Arbeitspaketen des Projekts.

3 TECHNOLOGIEKOMPLEX

Für die Vorausschau technologischer Entwicklungslinien muss bedacht werden, dass sich eine Technologie in einem technologischen Gesamtsystem befindet, das die Herstellung, Funktionstüchtigkeit und Zweckerfüllung ermöglicht. Auf der anderen Seite setzt sie auch die Abgrenzung der zu untersuchenden Technologie voraus. Nach Geschka (Geschka et al. 2017) wird der Wirkungsverbund unterschieden nach

- vorgelagerten Technologien, die in das Produkt eingehen
- komplementäre/ergänzende Technologien, die gemeinsam mit dem Produkt zur Anwendung kommen
- nachgelagerte Technologien, in denen das Produkt verarbeitet wird bzw. zum Einsatz kommt
- substitutive/konkurrierende Technologien, die den Bedarf durch andere Problemlösungsansätze erfüllen.

Das in Abbildung 10 dargestellte Gefüge wird als Technologiekomplex bezeichnet.

⁴⁶ Einige Beobachter sehen in der rasant steigenden Anzahl der Patentanmeldungen die Gefahr des Patent Trollings, bei der außer der Anmeldung von Patenten bereits existierender Ideen keine Eigenleistung zur Entwicklung von Unternehmen und Wissen beigetragen wird.

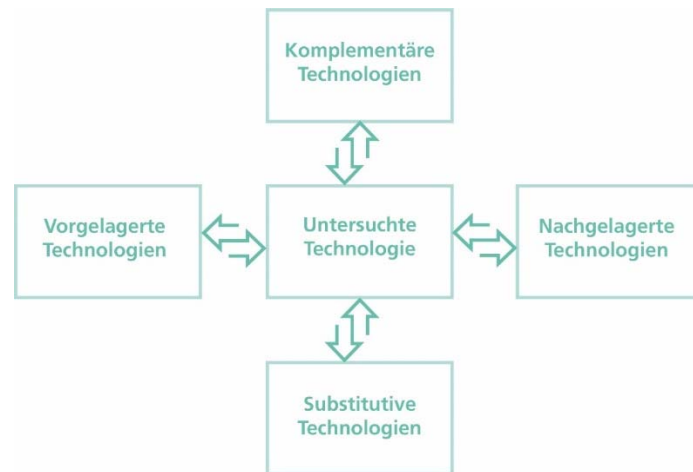


Abbildung 10: Technologiekomplex nach Geschka (Geschka et al. 2017) (vereinfachte eigene Darstellung).

Eine Einteilung wie sie der Technologiekomplex vorsieht ist bei neuen konvergierenden, komplex verwobenen Technologien wie Blockchain aufgrund der Möglichkeit von Mehrfachzuordnungen nicht mehr so einfach möglich. So lassen sich u.a. kryptografische Verfahren sowohl als eine vorgelagerte als auch als eine komplementäre Technologie auffassen.

Eine funktionierende Blockchain setzt ein weitgehend intaktes globales Kommunikationsnetzwerk voraus, sie ist also mindestens auf das Internet und die Stromversorgung angewiesen. Um die Anforderungen an die Kommunikation mit einer größeren globalen Abdeckung, höheren Datenraten und eine allgegenwärtige Verfügbarkeit in einer vernetzten und sicheren Informationsgesellschaft zu erfüllen, sind neue Mobilfunk- und Netztechnologien erforderlich wie das 5G (Fokusgruppe 5G 2015) und Beyond (B5G oder 6G)⁴⁷ (IEEE COMMUNICATIONS SOCIETY 2019). Andererseits kann die Blockchain-Technologie eine zugrundeliegende sichere und transparente Netzwerkgrundlage für B5G anbieten. So ist z.B. die Federal Communications Commission (FCC) der Ansicht, dass Blockchain eine Schlüsseltechnologie für die dynamische Frequenzteilung in 6G sein wird. Die Sicherheit der Blockchains hängt wesentlich von den eingesetzten kryptografischen Verfahren ab. In diesem Zusammenhang werden neben Weiterentwicklungen das Konzept der Kryptoagilität und die Post-Quantum-Kryptografie eine Rolle spielen.

Die Directed Acyclic Graphs (DAG) und weitere Systeme lassen sich als konkurrierende Technologien zu den klassischen Blockchains auffassen. Ihre Funktionsweise und Kennzeichen sowie die Vor- und Nachteile gegenüber dem Einsatz einer Blockchain werden ausführlich in Kapitel 4.5 beschrieben. Auf einer höheren Ebene lassen sich Datenbanksysteme (Greenspan 2015b) als konkurrierende Technologien ansehen. Ein Vergleich klassischer (Client-Server)-Datenbanken mit Blockchain-Technologien sind in Tabelle 1 dargestellt (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019). Dabei ist zu beachten, dass einzelne Aspekte je nach konkreter Ausgestaltung variieren können. Blockchains bzw. DLTs bieten gegenüber klassischen Datenbanken Vorteile in der Manipulationssicherheit und ggf. der Verfügbarkeit, während Effizienz und Vertraulichkeit Stärken klassischer Datenbanken sind. So stellen zentrale Server einen Single-Point-of-Failure dar. Wegen der zentralen Infrastruktur ist aber der Rechen- und

⁴⁷ 5G ermöglicht eine Vielzahl verschiedener Dienste – von verbesserter mobiler Breitbandkommunikation bis hin zu Virtual Reality, automatisiertem Fahren, IoT usw.. 6G soll Dinge realisierbar machen wie holografische Kommunikation, Hochpräzisionsfertigung, eine weit verbreitete Einführung von Künstlicher Intelligenz und die Integration neuer Technologien, wie Sub-THz oder Visible Light Communications (VLC), in ein echtes 3D-Abdeckungssystem, das terrestrische und lufttechnische Funkzugangspunkte integriert, um Cloud-Funktionalitäten bei Bedarf zu ermöglichen (Strinati et al. 2019).

Kommunikationsaufwand geringer als bei DLT-Lösungen, wodurch bereits Durchsätze von 56.000 tps nachgewiesen wurden (Visa Inc. 2015). Datenbanken stellen weiterhin die Integrität der gespeicherten Daten u.a. durch die regelmäßige Erstellung von Sicherheitskopien und Log-Dateien sowie eine starke Zugriffskontrolle auf die Daten sicher.

	Blockchain (öffentlich genehmigungsfrei)	Blockchain (privat genehmigungsbasiert)	Client-Server-Datenbank
Integrität	++	++	++
Authentizität	umsetzungsabhängig		
Verfügbarkeit	++	++	+
Vertraulichkeit	--	o*	+
Pseudonymität	o	--	--
Dezentralität	++	o	--
Robust gegen Missbrauch	++	+	o
Transparenz	++	o	--
Ressourcenbedarf	(sehr) hoch ⁺	gering	sehr gering
Durchsatz	--	+	++

Tabelle 1: Vergleich von Blockchain und Datenbank (eigene Darstellung in starker Anlehnung an (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019)). *: Es gibt Fortschritte, in vielen Lösungen ist die Vertraulichkeit jedoch schwächer zu beurteilen; hochgestelltes +: die meisten Public Permissioned Blockchains benötigen energieintensive Konsensmechanismen.

Da eine herkömmliche Datenbank im Hinblick auf Transaktionsgeschwindigkeit den klassischen Blockchains überlegen ist, kann sie, ein Vertrauensverhältnis zu einer Instanz vorausgesetzt, zum Einsatz kommen. Es gibt verschiedene Kriterien, die erfüllt werden müssen, damit die Nutzung der Blockchain gegenüber einer Datenbank sinnvoll ist (Greenspan 2015a). Diese sind beispielsweise, dass überhaupt eine Art Datenbank benötigt wird; es viele Parteien gibt, die Schreibrechte haben; kein Vertrauen untereinander und gegenüber einer zentralen Instanz (Disintermediation) herrscht; die Transaktionen untereinander abhängig sind; jeder Knoten die Transaktionen nach festgelegten Regeln prüft; ein verbindliches Transaktionsprotokoll erforderlich ist, über dessen Inhalt alle Knoten nachweislich übereinstimmen⁴⁸; und dem, was in der Blockchain steht, physische Werte gegenüberstehen. In Bezug auf zentrale Datenbanksysteme gibt es verschiedenste Ausprägungen, die zu Blockchain-Systemen in Konkurrenz stehen, wie z.B. die sogenannte Master-Slave Datenbankreplikation. Auch verteilte Datenbanksysteme können unter bestimmten Bedingungen eine Alternative zu DLT Lösungen darstellen. Der Übergang zwischen Blockchain-Lösungen und verteilten Datenbanken ist in der Praxis häufig fließend, wie (All In Bits, Inc. 2019) zeigt. In diesem Zusammenhang spielen insbesondere auch Entwicklungen im Bereich

⁴⁸ Dieses Vorgehen erfordert Validatoren. Ein Transaktionsprotokoll ist erforderlich, damit neu hinzugefügte Knoten oder Knoten, die aufgrund von Systemausfällen, Kommunikationsproblemen oder Angriffen Transaktionen verpasst haben, ohne Vertrauen auf den neusten Stand gebracht werden können.

kryptografischer Verfahren, Cloud Computing⁴⁹, Trusted Computing⁵⁰ sowie Edge Computing⁵¹ eine Rolle.

Ergänzende Technologien zu DLT sind verschiedenste kryptografische Verfahren. Es bestehen weiterhin Möglichkeiten DLT mit anderen Technologien zu verknüpfen. So stellt die Verbindung von Blockchain und Künstlicher Intelligenz (Artificial Intelligence) eine interessante Kombination dar. KI-Ansätze sind u.a. in der Lage, die optimalen Parameter für eine Blockchain zu bestimmen, was die z.B. Rechen-, Kommunikations- und Speicherleistung von 5G-Netzwerken erheblich verbessern könnte. Blockchain-Systeme andererseits könnten KI-Methoden unterstützen. So konnte gezeigt werden, dass mit einem Blockchain-System als Grundlage ein Anreiz für die regelkonforme Teilnahme am kooperativen Maschinenlernen geschaffen wurde (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019), (Salah et al. 2019), (Dinh und Thai 2018). KI-Systeme komplett auf Blockchain-Basis, sind aus technologischer Sicht jedoch bestenfalls langfristig umsetzbar und würden als solche ein hohes Bedrohungspotenzial darstellen. Hinter dem Begriff Quanten-Blockchain verbergen sich unterschiedliche Ansätze (s. (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019)). Bereits implementiert und getestet ist eine Blockchain, die auf einem Quantum-Key-Distribution (QKD)-Netzwerk aufbaut (Kiktenko et al. 2018). Spekulativer sind Ansätze, in denen das Blockchain-Netzwerk selbst aus Quantencomputern aufgebaut ist (Rajan und Visser 2019) oder Blockchain-Transaktionen die durch Quanten-Teleportation in einem klassischen Netzwerk übermittelt werden (Ikeda 2017). Als besonders vielversprechend gelten auch (Fridgen et al. 2019) die Kombinationen von DLT mit dem Internet der Dinge (IoT), den Methoden des Privacy-Preserving Computings (Kerschbaum o. J.) sowie z.B. des industriellen 3D-Drucks (Additive Manufacturing) (Diemer 2019).

Als nachgelagerte Technologien lassen sich u.a. die Smart Contracts, DApps sowie Orakel (siehe Kapitel 4.4.2) anführen.

4 TRENDS UND ENTWICKLUNGSTHEMEN

Es gibt einige Literaturlauswertungen, die Kategorisierungen der Paper in derzeit wichtige Themen vornehmen, wie z.B. Durchsatz, Latenz, Größe und Bandbreite, Sicherheit, Ressourcenverschwendung, Benutzerfreundlichkeit, Versionierung, Datenschutz und weitere (Yli-Huumo et al. 2016). Hier werden die Trends in die Hauptkategorien Konvergenzen, Skalierung, Sicherheit, Interaktion, Alternativen und Sonstige gegliedert.

⁴⁹ Beim Cloud Computing handelt es sich um die dynamische Bereitstellung von Anwendungen auf Abruf und den entsprechenden IT-Ressourcen über ein Netzwerk.

⁵⁰ Oft wird Trusted Computing als Zusicherung einer korrekten Arbeitsweise beschrieben oder als Ausdruck gewählt, wenn ein Trusted Platform Modul (TPM) zum Einsatz kommt. TPM ist ein kryptografischer Prozessor, der fest mit dem Mainboard eines Computersystems verbunden ist.

⁵¹ Beim Edge Computing werden Daten dezentral in der Netzwerkperipherie verarbeitet – an dem Ort, wo sie generiert wurden. Deswegen und nicht zuletzt aufgrund der „Echtzeitrelevanz“ bzw. der besseren Servicequalität, Skalierbarkeit und Sicherheit sind sie daher ein unverzichtbarer Bestandteil für das Internet der Dinge (IoT). Nachteile hingegen ergeben sich allerdings, wenn sehr hohe Datenmengen zu verarbeiten oder zu speichern bzw. der Rechen- oder Speicherbedarf sehr unregelmäßig ist.

4.1 Konvergenzen (Digitalisierung)

Für das Entwicklungspotenzial einer Technologie ist nicht nur das technologische Umfeld des Technologiekomplexes von großem Interesse, sondern auch das Zusammenspiel verschiedener technologischer (Mega-)Trends. Abbildung 11 soll dies auszugsweise demonstrieren.

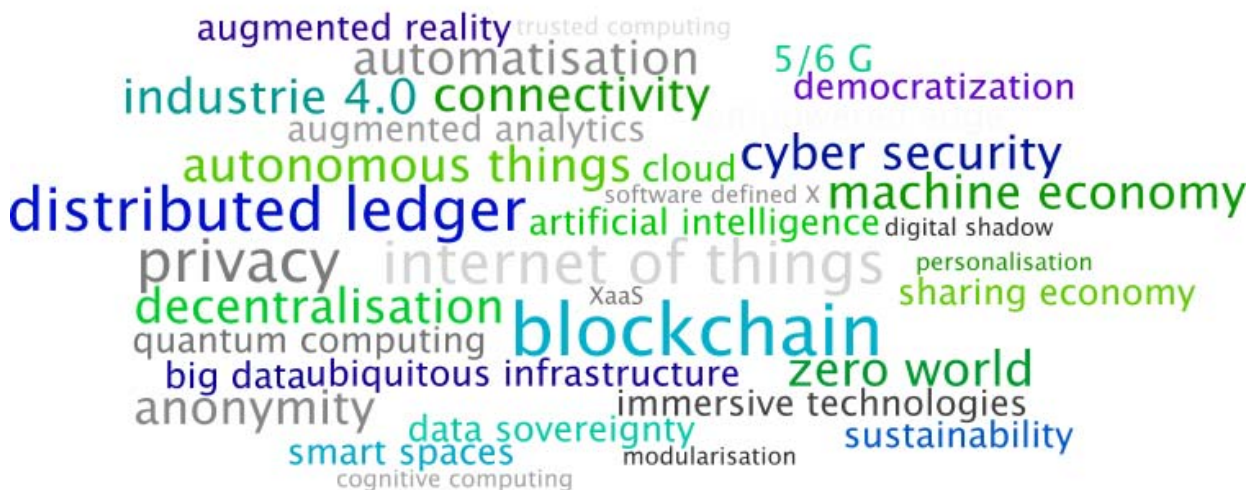


Abbildung 11: Zusammenspiel der Megatrends (eigene Darstellung).

Im erst kürzlich veröffentlichten Gartner Hype Cycle for Emerging Technologies 2019 stehen das Zusammenspiel von Mensch, Maschine und Künstliche Intelligenz (KI) im Vordergrund (Panetta 2019). Dabei wurden fünf Megatrends identifiziert: Sensoren und Mobilität, digitale Ökosysteme, fortgeschrittene KI und Analytik, postklassisches Computing sowie Augmented Human.

In diesem Umfeld bewegen sich auch die DLTs. Aufgrund der Verflechtungen sind sie Treiber und profitieren gleichzeitig von anderen Entwicklungen. In Kapitel 3 werden einige wesentliche Zusammenhänge der Technologien beschrieben.

4.2 Skalierung

Skalierbarkeit beschreibt die Fähigkeit einer IT-Architektur, sich an eine steigende Last anzupassen. Dabei sind Durchsatz und Latenz (Antwortzeit) von Bedeutung. Durch die sequenzielle Verkettung von Blöcken begrenzter Größe sowie eine steigende Zahl an Netzwerkteilnehmern kommt es bei den Blockchains zu Skalierbarkeitsproblemen. So beträgt z.B. die Größe der Bitcoin-Blockchain bereits heute (Stand: Oktober 2019) annähernd 250 GB (BLOCKCHAIN LUXEMBOURG S.A. 2017).

Die Ethereum-Blockchain „verstopfte“ z.B. aufgrund von CryptoKitties⁵² als das Spiel über 10% der Transaktionen im Netzwerk ausmachte (BBC 2017).

Neben der Entwicklung neuerer Konsensverfahren gibt es einige Ansätze dem Skalierbarkeitsproblem zu begegnen, von denen im Folgenden einige beschrieben werden.

4.2.1 Speicherplatzreduktion

Eine Möglichkeit, die Skalierbarkeit zu verbessern liegt in der Anwendung einer vereinfachten Zahlungsüberprüfung (Simplified Payment Verification (SPV)) der Lightweight Nodes. Diese können die Validität von Transaktionen prüfen, ohne die gesamte Blockchain herunterzuladen. Eine weitere Möglichkeit besteht in dem Erasure Coding, dabei handelt es sich ursprünglich um eine Methode, um Daten abzusichern. Hierbei werden die validierten Blöcke nach einem vorher festgelegten Algorithmus mit Überlappungen als Fragmente kodiert. Diese werden dann auf die Knoten verteilt und bei Bedarf wieder zusammengestellt (Perard et al. 2018). Eine weitere Möglichkeit, die Größe einer Blockchain adäquat zu halten, ist, die Daten auszulagern. Dabei wird u.a. neben weiteren Metainformationen der Hashwert der Daten als Referenz in der Blockchain gespeichert. Die Daten könnten in einer herkömmlichen Datenbank liegen bzw. über ein IPFS-Netzwerk verteilt sein⁵³. Um zu belegen, dass die Daten nicht verändert wurden, muss der aus diesen Daten berechnete Hashwert mit dem in der Blockchain hinterlegten Hashwert übereinstimmen.

4.2.2 SegWit

Segregated Witness (SegWit) wurde ursprünglich als Update für die Bitcoin vorgeschlagen, um einer Sicherheitslücke, der Transaktionsverformbarkeit (transaction malleability), entgegenzuwirken - gleichzeitig hilft es jedoch auch gegen Skalierbarkeitsprobleme. Bei dieser Sicherheitslücke können die Signaturen der Teilnehmer manipuliert werden, bevor sie vom Netzwerk bestätigt wurden. Diese Änderung des Transaktionshashs macht es möglich, dass ein Zahlungsempfänger vorgeben konnte, dass eine Transaktion nicht stattgefunden hat. Die 2015 vorgestellte und 2017 erstmals per Soft Fork eingeführte Implementierung trennt nun die Signaturdaten von der eigentlichen Transaktion und hängt diese als Erweiterung wieder an. Damit passen mehr Transaktionen in einen Standardblock der von Nakamoto⁵⁴ ursprünglich festgelegten Größe von 1MB. SegWit löst damit die unzureichende Transaktionskapazität von Bitcoin vermutlich nicht vollständig, sie ermöglicht jedoch auch die Implementierung von Sidechains (s. auch Kapitel 4.2.6) auf eine zweite Schicht, die aufgrund der Transaktionsverformbarkeitsprobleme zuvor nicht realisierbar war.

⁵² In CryptoKitties können die Spieler digitale Kätzchen kaufen, sammeln, tauschen und züchten. Jede Katze besitzt Charakteristika, die sie an ihre Nachkommen weitergeben. Ziel des Spiels ist es, Kätzchen mit möglichst seltenen Attributen zu bekommen.

⁵³ Das InterPlanetary File System (IPFS) ist ein verteiltes Dateisystem, das alle Geräte mit demselben Satz an Dateien verbindet. Jeder Knoten speichert für ihn relevante Inhalte (Dateien) und hält verteilte Hashtabellen (DHT) Indexinformationen bereit, über die sich herausfinden lässt, welcher Knoten welche Dateien speichert.

⁵⁴ Ein Grund für die Begrenzung lag daran, dass Denial of Service-Attacken (DoS) verhindert werden sollten.

4.2.3 Erhöhung der Blockgröße

Ein Bitcoin Block ist maximal 1 MByte groß und kann bis zu 2500 Transaktionen enthalten. Damit das Netzwerk synchron bleibt, wird nur ca. alle 10 min ein Block erzeugt, was die Zahl der Transaktionen auf maximal 7 pro Sekunde beschränkt. Die Idee, die Blöcke zu vergrößern, führte 2017 zur Abspaltung einer neuen Währung: Bitcoin Cash (BCH), die sich bislang in der Praxis gegenüber dem ursprünglichen Bitcoin (BTC) (noch) nicht durchsetzen konnte (Wobst 2019). Nach einem weiteren Hardfork gibt es sogar 32 Mbyte-Blockgrößen (Bitcoin SV) (BTC-ECHO GmbH 2019b). Jüngst hat auch Ethereum das Gaslimit für Blöcke, und damit die Blockgröße um ca. 25% erhöht (Nikolaev 2019).

4.2.4 Sharding

Sharding⁵⁵ könnte eine vielversprechende Lösung für die Skalierbarkeits- und Performanceprobleme werden. Dabei handelt es sich um eine Möglichkeit der Partitionierung, um die Rechen- und Speicherarbeitslast auf ein P2P-Netzwerk zu verteilen, so dass nicht jeder Knoten für die Verarbeitung der Transaktionslast des gesamten Netzwerks verantwortlich ist. Stattdessen verwaltet jeder Knoten nur Informationen, die sich auf seine Partition (Shard) beziehen. Mit dem Sharding ergeben sich neue Herausforderungen, wie z.B. Sicherheits- und Dezentralisierungsprobleme, die bisher noch nicht befriedigend gelöst werden konnten. Aktuelle Blockchain-Frameworks, die Sharding verwenden oder zu verwenden beabsichtigen, führen die Funktion auf unterschiedliche Arten aus (Luu et al. 2016b), (Wood 2017), (Aste et al. 2017). Die Devio-Blockchain verspricht mit ihrem Ansatz 8 Millionen tps. Ein interessanter Ansatz ist auch Polyshard von Unit-e, bei dem die Daten von verschiedenen Benutzern und Transaktionen so vermischt werden, dass eine genaue Datenwiederherstellung möglich ist, ähnlich wie bei der Virtualisierung auf Server- und Speichersystemen (Mearian 2019) (Li et al. 2018). Weitere Beispiele für solche prototypischen DLT-Infrastrukturen, die Sharding nutzen, sind auch OmniLedger (Kokoris-Kogias et al. 2018), RapidChain (Zamani et al. 2018) oder auch Zilliqa, Kadena, Near, Cosmos, Polkadot (Zilliqa 2019; Will Martino 2019; NEAR 2019; Jae Kwon; Gavin Wood 2018). Bei der Skalierung spielen Rechenleistung (Processing), Speicherplatz (Storage) und Bandbreite eine Rolle. Die gebräuchlichste Art des Sharding ist das State Sharding (Wolmarans 2019). Die Knoten bauen ihre eigenen Blockchains (Shards) auf, die Transaktionen enthalten, die nur ihren Teil des gesamten Netzwerks betreffen. Knoten müssen nur die Transaktionshistorie ihrer Shards speichern, ausschließlich Transaktionen verarbeiten, die ihren Shard betreffen, und diese Transaktionen in ihrem Shard weiterleiten. Die Pflege/Koordination des Netzwerks von Shards übernimmt oft eine weitere Kette, die z.B. bei Ethereum als Beaconchain bezeichnet wird. Sie ist u.a. für eine zufällige Zuordnung von Knoten und Validatoren zu Shards, die Aufnahme von Momentaufnahmen einzelner Shards und verschiedenen anderen Funktionen zuständig. Für Probleme, die sich bei Cross Shard Transaktionen ergeben und u.a. die Datenverfügbarkeit und Datenvalidität betreffen, gibt es zahlreiche Lösungsansätze, die jedoch in Gänze noch nicht zufriedenstellend sind (Skidanov 2018).

⁵⁵ Zilliqa Zilliqa 2019 gilt als erste öffentliche Blockchain-Plattform, die Sharding implementiert hat - im Testnetz konnten 2.828 tps erreicht werden. Ethereum will Anfang 2020 Sharding als Teil des Ethereum 2.0 Updates einführen.

4.2.5 Directed Acyclic Graphs (DAG)

Directed Acyclic Graphs (DAGs) bieten vielversprechende Lösungen des Skalierbarkeitsproblems. Jeder Knoten erhält Daten sowie den Hashwert seines Vorgängers. Obschon vielversprechend, haben sie den endgültigen Beweis für ihre Praxistauglichkeit und Sicherheit erst noch zu liefern (Hays 2019). Diese werden in Kapitel 4.5 weiterführend erläutert.

4.2.6 Off-Chains

Bei den Off-Chains werden State Channels und Sidechains unterschieden, die beide nach dem folgenden dreistufigen Prinzip funktionieren:

1. Einfrieren der Anfangszustände/-werte auf der Blockchain
2. Transaktionen finden außerhalb der Blockchain statt
3. Freischalten der Endzustände/-werte von State Channel/Sidechain auf der Blockchain.

State Channels sind Kanäle, in denen zustandsändernde Operationen wie auf der Blockchain angewendet werden. Dazu sind Smart Contract Funktionalitäten der Blockchain erforderlich. Ein Beispiel dafür stellt das 2015 ins Leben gerufene Lightning Netzwerk (Antonopoulos 2018), (Poon und Dryja 2016) dar. Es erweitert die Bitcoin-Infrastruktur (On-Chain) um neue Transaktionskanäle (Off-Chain), in denen u.a. Micropayments schnell und ohne die hohen Gebühren wie sie bei Bitcoin Transaktionen anfallen möglich sind. Die sogenannte Funding Transaktion für einen Kanal erstellt eine Bitcoin-Adresse, die von den beiden Zahlungspartnern signiert ist und den Gesamtbetrag ihrer eingesetzten Bitcoins enthält. Beide Partner können nur einvernehmlich über das Vermögen verfügen. Zusätzlich erstellen beide noch jeweils für den anderen eine (Absicherungs)-Transaktion, die ihm seinen eingesetzten Geldbetrag zurücküberweist. Der rechtmäßige Eigentümer erhält den Betrag entweder nach einer gewissen Wartezeit zurück oder der Zahlungspartner erhält sie mit dem privaten Schlüssel des ursprünglichen Eigentümers, den er zu diesem Zeitpunkt aber noch nicht kennt. Bei den folgenden Zahlungsvorgängen geht es darum, sicherzustellen, dass jede Partei im eigenen Interesse keine früheren Transaktionen veröffentlicht. Mit jeder neuen Transaktion erzeugen beide Partner ein neues Schlüsselpaar, bauen damit wie oben je eine Transaktion mit der aktuellen Zahlungsbilanz auf, tauschen sie aus und senden zusätzlich den privaten Schlüssel der vorherigen Transaktion an ihr Gegenüber. Dies aktiviert die sogenannte Vergiftung. Denn veröffentlicht eine Seite nun eine ältere Transaktion in der Blockchain, kennt die Gegenseite den passenden privaten Schlüssel und hat eine Wartezeit lang Zeit, sich den gesamten im Kanal gespeicherten Betrag einzuverleiben. Deshalb hat jeder das Interesse nur den letzten Zahlungsstand einzulösen. Jeder hat die Möglichkeit, jederzeit den Kanal aufzulösen und den aktuellen Geldbetrag in die reguläre Bitcoin-Blockchain zu überführen. Geschieht dies einvernehmlich, erstellen die Parteien eine Transaktion, die sich unmittelbar anwenden lässt. In allen anderen Fällen muss die Warte- oder Karenzzeit von z.B. 1000 Blöcken abgewartet werden. Nicht nur über direkte Kanäle zwischen Käufer und Verkäufer, sondern auch indirekt über Mittelsmänner (Hub and Spoke-Systems) können Zahlungen erfolgen. Jeder Hub leitet die Zahlung im Austausch gegen einen vom Empfänger erzeugten geheimen Schlüssel weiter, mit dem der Hub ein Feld der eingehenden Transaktion entsperren kann, um so seine Zahlungsbilanz auszugleichen. Passiert dies nicht, hat er durch die eingebaute Vergiftung der Transaktion die Möglichkeit im Zweifel die erhaltene Transaktion in der Bitcoin-Blockchain zu veröffentlichen, um an das ihm zustehende Geld zu gelangen. Die Hubs können für ihre Dienste

Gebühren erheben, die jedoch erheblich geringer sind als die der Miner. Von vielen Bitcoin-Core⁵⁶ Entwicklern wird das Lightning-Netzwerk zurzeit als beste Lösung des Skalierungsproblems angesehen.

Eine genaue Beschreibung des schrittweisen Routing über eine Folge von Hash Time Lock Contracts findet sich z.B. in (Antonopoulos 2018). Hierbei generiert der Empfänger ein Geheimnis, das er verhasht und dem Zahlungspflichtigen zusendet, der es dann in das Locking-Skript des Outputs einbindet. Das Skript enthält ebenfalls einen Teil, der bewirkt, dass dieser nach einer festgelegten Zeit eine Rückerstattung bekommt, sollte der Empfänger das Geheimnis nicht wissen. Das Besondere dabei ist, dass die Routing-Teilnehmer nur ihren Teil an Informationen entschlüsseln können, um den (vorherigen und) nächsten Hop zu finden (Onion-Routing). Im Lightning Netzwerk werden Zahlungen von Kanal zu Kanal übertragen, ohne dass den dazwischenliegenden Teilnehmern vertraut werden muss. Es gibt derzeit einige Prototypenimplementierungen, wie z.B. Raiden, aber auch Teechain, Tumblebit oder das Celer Netzwerk (Brainbot Labs Establishment o. J.), (Saini 2019), (Dong et al. 2018).

Eine weitere Möglichkeit stellen Sidechains dar. Hierbei handelt es sich um eine separate Blockchain, die an die übergeordnete Blockchain angehängt wird (Back et al. 2014). Sie benötigt im Prinzip⁵⁷ als Intermediär zwischen der Blockchain, hier Mainchain genannt, und der Sidechain eine Gruppe (Federation), die von den Sidechain-Erstellern bestimmt werden kann und das Einfrieren und Freischalten der Anfangszustände/-werte regeln. Dies bietet jedoch Hackern einen zusätzlichen Angriffspunkt. Durch den Einsatz von Sidechains ist es u.a. möglich, verschiedene Blockchains über die Seitenketten miteinander kommunizieren zu lassen (Interoperabilität). Sie lassen sich auch als Testnetzwerk einsetzen, um z.B. Änderungen im Code zu testen, bevor sie auf die Mainchain übertragen werden. Derzeitige Sidechain-Plattformen sind u.a. Loom (Loom Network 2019), Proof-of-Authority (POA) Netzwerk (Arasev 2018), (Gross und Barinov o. J.), Liquid (Dilley et al.), (Blockstream o.J.), Mumblewimble (MumbleWimbleCoin Whitepaper) und RootStock (Lerner 2015), (RSK 2019).

Welche Variante der Off-Chains sich durchsetzen wird oder ob sich aus beiden eine neue Variante entwickeln wird, kann derzeit nicht abgeschätzt werden.

4.3 Sicherheit

Derzeit werden verschiedenste Sicherheitsaspekte der DLT untersucht. In der Regel wird jedoch das Thema Schutz gegenüber unterschiedlichen Angriffsszenarien wenig differenziert betrachtet (NExT e.V. in Zusammenarbeit mit der Initiative "Blockchain in der Verwaltung Deutschland" (BiVD) und der Community of Practice Blockchain des NExT-Expertennetzwerks 2019).⁵⁸ Im Folgenden werden aufgrund der Fülle an unterschiedlichen Lösungen nur ausgewählte technologische Beispiele vorgestellt.

⁵⁶ Referenzsoftware

⁵⁷ Hier gibt es mittlerweile auch andere Möglichkeiten (Singh et al. 2020).

⁵⁸ Der Global Risk Report 2019 sieht in den Cyberangriffen, dem Zusammenbruch der kritischen Infrastrukturen und Datenbetrug und -klau große und auch wahrscheinliche Gefahren weltweit (World Economic Forum 2019). Dezentrale Systeme sind schlechter angreifbar.

Manipulationssicherheit

Die Manipulationssicherheit beginnt mit der Gewährleistung einer fairen Konsensreihenfolge der in den Ledger einfließenden Transaktionen. In einigen klassischen Blockchain-Technologien können, je nach Konsensverfahren, die Validatoren Inklusion und Reihenfolge der Transaktionen bestimmen. Bei bewusster Manipulation eines Netzwerks durch bösartige Akteure lassen sich 51%- und 34%-Angriffsszenarien unterscheiden, je nachdem, welchen Anteil der für die Konsensfindung erforderlichen Ressourcen ein Angreifer kontrollieren muss, um den Konsens in seinem Sinne zu manipulieren oder das Netzwerk sogar zum Erliegen zu bringen. Darüber hinaus können Ledger auch durch die Manipulation von außerhalb der Ledger-Infrastruktur befindlichen Komponenten angegriffen werden. Bei einer Distributed Denial-of-Service (DDoS)-Attacke kann die Kommunikation z.B. wichtiger Einzelknoten verhindert werden und damit ggf. das gesamte Netzwerk lahmgelegt werden. Bei Partition-Angriffen⁵⁹ können bestimmte Teile des Netzwerks selektiv abgetrennt werden, so dass z.B. durch den manipulativ erzeugten Fork eine Double Spending-Attacke durchgeführt werden kann. Diese Manipulationen fallen in die Kategorie der 34%-Angriffsszenarien.

Datensicherheit

Die Entwicklungen im Bereich Kryptografie und Blockchain insgesamt befruchten sich gegenseitig. Es gibt eine Vielzahl an kryptografischen Verfahren, von denen einige bereits etabliert und im Blockchain-Kontext eingesetzt werden und andere erst testweise oder noch keinen Einsatz in diesem Bereich finden. Wieder andere sind neuartig und müssen sich erst einmal bewähren, scheinen jedoch interessant für eine Anwendung rund um die Blockchain zu sein.

Um die Vertraulichkeit von sensiblen Daten zu gewährleisten gibt es eine Vielzahl von Verschlüsselungsschemata. Geeignet sind auch Verfahren, die die Daten selbst extern und nur den Verweis in der Blockchain speichern oder separat geschützte Kanäle aufbauen (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019). Neben komplexen kryptografischen Konzepten haben sich vor allem Ansätze mit Trusted Execution Environments (TEE) herausgebildet, um vertrauliche Berechnungen in Transaktionen oder vertraulich Smart Contracts auszuführen. TEEs bieten für freigeschaltete Anwendungen eine isolierte Laufzeitumgebung. Angriffsmöglichkeiten können sich hier aufgrund der Nicht-Finalität bei PoW-Blockchains ergeben oder auch durch Angriffe auf die Hardware, z.B. in Form von Seitenkanalangriffen⁶⁰. Obwohl das Suchen und Berechnen auf verschlüsselten Daten eine Herausforderung darstellt, gibt es aufgrund der Relevanz in sicherheitskritischen Bereichen bereits Lösungen bzw. Lösungsansätze, die z. T. auch in Blockchains genutzt werden (können). Hier spielen u.a. die homomorphe Verschlüsselung, wodurch sich Berechnungen auf dem Geheimtext durchführen lassen, sowie die funktionale Verschlüsselung eine Rolle. Erstere steht für den praktischen Einsatz noch kaum bereit. Anders als bei herkömmlichen Verschlüsselungsverfahren, bei denen man eine Nachricht bzw. Daten für einen gewissen Empfänger verschlüsselt, bekommt jeder Nutzer bei den funktionalen Verschlüsselungen einen privaten Schlüssel zu einer bestimmten Funktion, die seine Berechtigungen bestimmt (Universität Paderborn o. J.). Mit der Secure Multi-Party Computation (SMPC) (Genkin et al. 2018), (Luongo und Pon 2019) können mehrere Parteien eine gemeinsame Verarbeitung ihrer Daten realisieren, ohne diese Daten den jeweils anderen Parteien bekannt zu machen⁶¹. Als Anwendung von SMPC kann das Wanchain-Netzwerk angesehen werden

⁵⁹ Für diese Angriffsvektoren gibt es Lösungsansätze (Apostolaki et al. 2017) wie für andere wie Delay Angriffe auch.

⁶⁰ Ein Seitenkanalangriff richtet sich gegen die Implementierung von kryptografischen Algorithmen, die in ihrer Umsetzung physikalische Ressourcen benötigen und deren Kenntnis wiederum den Algorithmus kompromittieren können.

⁶¹ Dies ist z.B. für die medizinische Forschung interessant, um den Schutz von Patientendaten zu gewährleisten.

(WANCHAIN FOUNDATION LTD 2019) . Allgemein sind jedoch SMPC-Verfahren relativ ineffizient und damit für viele Anwendungen nicht geeignet.

Die ressourcenbeschränkte Kryptografie (lightweight cryptography) zielt u.a. auf IoT-Knoten, Sensornetzwerke, eingebettete Systeme und dergleichen ab (Dorri et al. 2019). Sie ist einfacher und schneller als die herkömmliche Kryptografie, aber im Allgemeinen weniger sicher. Ressourcenbeschränkte Blockchains sollen für mehr Sicherheit als derzeit realisiert sorgen, z.B. in Fahrzeugen oder beim Edge Computing.

Für den langfristigen Schutzbedarf müssen Sicherheitsmechanismen der Blockchain bei Bedarf ausgetauscht werden können. Dieses als Kryptoagilität bezeichnete Forschungsgebiet wird von verschiedenen Institutionen intensiv untersucht verschiedene Konzepte, wie z.B. die Neuverhashung der Blöcke erforscht (Steffen Schwalm et al. 2018), (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019), (Fraunhofer-Institut für Sichere Informationstechnologie o. J.).

Verschlüsselung und digitale Signaturen erfolgen bei vielen DLTs derzeit mit Methoden, die größtenteils nicht Quantencomputer-resistent sind. Unabhängig davon, wann genau Quantencomputer zukünftig einsetzbar werden, müssen die heute eingesetzten Lösungen kritisch betrachtet werden. Für die rückwirkende Absicherung bereits existierender Daten gegenüber der Entschlüsselung mit Quantencomputern müssten auch heute schon Verfahren der Post-Quanten-Kryptografie (PQK) eingesetzt werden, die diesen Gefahren begegnen können⁶². Neuartige kryptografische Verfahren können jedoch nicht nur vor den möglichen Auswirkungen von Quantencomputern schützen, sondern auch vor Durchbrüchen im Bereich klassischer Ansätze zum Brechen von etablierten kryptografischen Verfahren (Kreutzer et al. 2018). Ein Einsatz von entsprechenden PQK-Verfahren steht jedoch noch vor einigen Herausforderungen. Sie können z.B. durch ihre Komplexität die Leistungsfähigkeit der jeweiligen Blockchain beeinträchtigen.

Datenschutz

Eine Annäherung an die Anonymität (s. auch Kapitel 1.2.4) lässt sich dadurch erreichen, dass die Knoten nicht das gleiche Schlüsselpaar für all ihre Transaktionen verwenden. Ansonsten lässt sich die Transaktionshistorie nachverfolgen oder/und Transaktionen miteinander korrelieren und daraus Rückschlüsse auf die Person ziehen (Barcelo 2007), (Biryukov et al. 2014). Des Weiteren kann die Identität durch die Erstellung mehrerer User-Accounts (Zheng et al. 2018) geschützt werden. Sogenannte Mixer funktionieren, indem Personen, die nicht Teil der Transaktion sind, eine große Menge an Coins zur Verfügung stellen. Ist der Pool groß genug, lässt sich nicht so einfach nachvollziehen, wer welche Coins genommen hat. Die Dienstleistung dieser Zwischenhändler ist mit Kosten verbunden und birgt auch die Gefahr, dass diese die Vermögenswerte behalten. Die Blockchain Mixcoin löst dieses Problem, indem diese Intermediäre die Transaktionen ebenfalls signieren müssen. Demnach kann ein Fehlverhalten der Intermediäre aufgedeckt werden. Der Diebstahl lässt sich damit zwar aufdecken, aber nicht aktiv verhindern. Weitere Ansätze wie bei Conjoin oder Coinshuffle nutzen eine Art von zufälliger Auswahl von Intermediären, die die Transaktionen weiterleiten (Zheng et al. 2017). Anonymous ist ein neuer Ansatz, der von Zerocoin implementiert wurde. Dabei werden keine Transaktionen validiert, sondern es gibt validierte Coins, mit denen gehandelt werden kann (Miers et al. 2013). Ein wirkungsvoller Ansatz zur Verbesserung des Datenschutzes stellen Zero-Knowledge-Beweise dar (Genkin et al. 2018). Dabei handelt es sich um eine kryptografische Methode, mit deren Hilfe eine Partei einer anderen Partei beweisen kann, dass eine Aussage wahr ist, ohne weitere

⁶² Abhängig von ihrem Konstruktionsprinzip werden Gitter-, Korrekturcode- und Hash-basierte Verfahren sowie die multivariate, nichtkommutative Gruppen- und Isogenie-basierte Verfahren unterschieden. Die beiden gitterbasierten Verfahren NTRU und New Hope, das Korrekturcode-Verfahren McEliece sowie das Hash-basierte XMSS gehören derzeit wohl zu den bekanntesten post-quantenkryptografischen Verfahren.

Informationen darüber preiszugeben. Auf dieser Grundlage können z.B. finanzielle Transaktionen abgewickelt werden, ohne dass irgendwelche Informationen über den Betrag oder die Teilnehmer enthüllt werden.

Bei den Signaturschemata lassen sich zusätzliche Eigenschaften z.B. bezüglich der Anonymität explizit adressieren. Beispiele hierfür sind die blinden Signaturen (Blind Signatures) (Chaum 1984b), bei denen es nicht möglich ist, das signierte Dokument nach oder während der Signatur einem Absender zuzuordnen, oder Ringsignaturen (Ring Signatures) (Zhang und Kim 2002), bei denen die digitale Signatur von einer Person aus einer Gruppe erstellt werden kann, wobei es für einen Außenstehenden nicht möglich ist zu entscheiden, von wem aus dieser Gruppe die Signatur stammt. Von Bedeutung ist u.a. auch die Broadcast Encryption, bei der jeder Nutzer eine verschlüsselte Nachricht erhält, aber nur einer diese entschlüsseln kann – so bleibt der Empfänger unbekannt.

Sicherer Austausch

Aus mehreren privaten Schlüsseln können Multi-Signature-Adressen (MultiSig) erstellt werden (Peyrin et al. 2018). Dies ermöglicht es, dass eine beliebige Anzahl der ausgewählten Signaturen für eine Transaktion erforderlich ist bzw. Transaktionen zwischen zwei Parteien treuhänderisch durch einen neutralen Dritten überwachen und diesen ggf. über die Abwicklung einer Zahlung entscheiden zu lassen (Buterin). Mit Hilfe komplexerer Multisignatur-Schemata lassen sich Entscheidungswege organisationsübergreifend abbilden, z.B. um die notwendigen Freigaben für das Auslösen eines Prozessschrittes zu ermöglichen. Damit kann gleichzeitig auch die notwendige Flexibilität bei einer Nichtverfügbarkeit einzelner Akteure gewährleistet werden. Die Multisignatur-Funktion bietet außerdem die Möglichkeit, Geheimnisse (wie private Schlüssel) im Ledger zu hinterlegen und im Verlustfall durch die notwendige Anzahl und Kombination von Signaturen wiederherzustellen. Auf diese Weise kann die Handlungsfähigkeit auch einzelner Akteure langfristig sichergestellt werden. Dieses spezielle Vorgehen wird auch Secret Sharing genannt und ist in Abbildung 12 dargestellt.

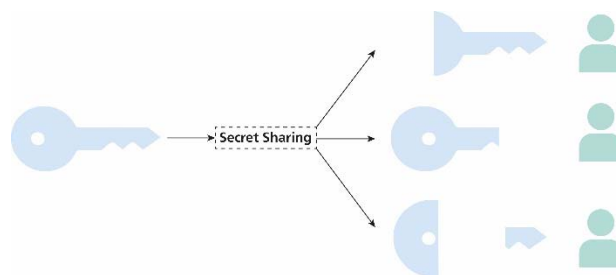


Abbildung 12: Secret Sharing (eigene Darstellung in enger Anlehnung an (Raikwar et al. 2019)).

Eine Verallgemeinerung der MultiSig, in der alle Nutzer dieselbe Transaktion signieren, sind zusammengefasste Signaturen (Aggregate Signatures), bei denen eine kompakte Signatur aus verschiedenen Signaturen von verschiedenen Transaktionen erstellt wird.

In die andere Richtung geht die sogenannte Identity-Based Encryption, die bereits in einigen Blockchain-Anwendungen eingesetzt wird (Wei et al. 2018), (Bose et al. 2018). Hier kann der öffentliche Schlüssel des Nutzers beispielsweise die E-Mail- oder IP-Adresse sein. Von Bedeutung ist außerdem die Authenticated Encryption, bei der neben der Vertraulichkeit auch die Authentizität sichergestellt wird.

Bei den Schwellensignaturen (Threshold Signatures) erstellt jede Partei unabhängig voneinander einen geheimen Schlüssel. Das zu öffnende Schloss setzt sich modular aus den Schlössern zu diesen Schlüsseln zusammen. Das modulare Schloss lässt sich dabei so gestalten, dass es, auch wenn nur eine Teilmenge der Schlüssel verfügbar ist, entsperrt werden kann.

4.4 Interaktion

4.4.1 Interoperabilität

Als aktuell neueste Entwicklungsstufe im Bereich Blockchain ist die Interoperabilität zwischen den Blockchains/DLs untereinander, aber auch die Anbindung von Legacy- und Bestandssystemen an die Blockchain zu sehen. Denn in den verschiedenen Anwendungsbereichen wird es immer wieder die Anforderung geben, auf Informationen in verschiedenen Blockchains zuzugreifen, oder Transaktionen/Smart Contracts in anderen Blockchains auszulösen. Beispiele für interoperable Blockchain-Netzwerke könnten sich z.B. in Machine-to-Machine-Anwendungen ergeben, z.B. um Authentifizierung und Autorisierung zusammenzuführen. Während sich ein großer Teil der Forschung der Interoperabilität von Datenbanksystemen (Sheth 1999) widmet, gibt es nur wenig wissenschaftliche Literatur speziell für DLT. Und das, obwohl es derzeit Hunderte von Ledger-Initiativen gibt, die sich jedoch oft noch in einem frühen Proof-of-Concept Bereich befinden (Beck und Müller-Bloch 2017). Für die Interoperabilität ist die Standardisierung gemeinsamer Schnittstellen und Protokolle unerlässlich (s. auch Kapitel 4.4.3). Im begrenzten Umfeld haben sich allerdings bereits etablierte Projekte mit einer großen Community wie Corda von R3 (Brown 2018), Ripple von Ripple Labs oder Hyperledger der Linux Foundation (Hyperledger 2019a) entwickelt. Die größte Herausforderung für die Interoperabilität liegt darin, dass die DLs keine universelle Kommunikation untereinander ermöglichen. Eine Lösung für die Interoperabilitätsprobleme bei der Cross Chain Communication oder Interchain Communication liefert z.B. die Verwendung offener Protokolle sowie Multi Chain Frameworks. Ein Beispiel für ein offenes Protokoll ist der Atomic Swap, der weiter unten ausführlicher beschrieben wird. Multi-Chain-Frameworks hingegen fungieren als offene Umgebungen, in die sich Blockchains einfügen (Goyal 2018). Die Multi-Chain-Frameworks Polkadot und Cosmos entwickelten von Grund auf neue Cross-Chain-Ökosysteme, innerhalb derer jeder Teilnehmer Blockchains erstellen kann. Subchains (Parachains oder Pegs) können innerhalb der Mainchain dann nahtlos miteinander interagieren. Die Integration externer Blockchains erfordert diverse technische Voraussetzungen. Sidechains für existierende Blockchains sind ebenfalls eine Möglichkeit, Interoperabilität zu erzeugen. Ein Beispiel dafür ist „Plasma“ der Ethereum Plattform (Schiller 2019). Sogenannte Proxy Token werden z.B. bei Wanchain eingesetzt. Diese Netzwerke blockieren Assets in ihren nativen Blockchains und geben Proxy-Token in entsprechender Höhe frei. Wenn das Asset durch einen Smart Contract entsperrt wird, „verbrennen“ diese Systeme Proxy-Token. Eine universelle Cross-Chain-Technologie verspricht EVEN (EVEN Foundation 2019a), (EVEN Foundation 2019b). Es gibt noch viele weitere Projekte, wie Overledger (Quant Network o.J.), Interledger von Ripple, Omniledger oder die Blockchain Interoperability Alliance, ein Zusammenschluss von ICON, Aion und Wanchain, die u.a. die Entwicklung gemeinsamer Industriestandards sowie die gemeinsamen Nutzung von Architekturen vorantreiben.

Technologisch erfordert die Interoperabilität weitere Aufmerksamkeit z.B. bezüglich der Sicherstellung der Finalität, des Auffindens der Knoten sowie den Folgen von Updates. Um ungünstige Zustände zwischen unveränderlichen Ledgern zu vermeiden, wird derzeit eine ausreichende Zeit gewartet (Koens und Poll 2019), was jedoch den Durchsatz erheblich verringert.

Beispielsweise wurden 12 Eigenschaften⁶³ vorgeschlagen, mit denen die Interoperabilität beurteilt werden kann (Koens und Poll 2019). Im Zusammenhang damit werden drei Arten von Interoperabilitätslösungen unterschieden: Notariatssysteme, Relaissysteme und Hash-Locking-Schemata. Bei den Notariatssystemen wird eine Trusted Third Party sowie eine separate Blockchain benötigt. Hierunter fallen z.B. Polkadot und Cosmos. Bei den Relaissystemen wird eine lokale Kopie der anderen Blockchain auf der eigenen abgelegt⁶⁴. Hash-Locking-Schemata erfordern lediglich den Austausch eines einzigen Hash zwischen den beiden Ledgern. Funktionalitäten, die eine Interoperabilitätslösung bereitstellen sollte, sind u.a. Token Portability (ein Token kann von Ledger A an Ledger B gesendet werden oder umgekehrt), Atomic Swap (ein Transfer zwischen zwei Parteien ist für beide Parteien garantiert), Cross-Chain Oracles (ein Smart Contract auf Ledger B liest aus Ledger A und führt eine Aktion durch, wenn ein bestimmtes Ereignis oder Zustand gelesen wird) und Cross-Chain Asset Ecumbrance (Token sind in Ledger A gesperrt und Sperrbedingungen sind abhängig von Ereignissen in Ledger B) (Koens und Poll 2019), (Buterin). Des Weiteren kann auch (Jin et al. 2018) zwischen einem aktiven und passiven Modus der Interoperabilität unterschieden werden. Während im passiven Modus die Quellen-Blockchain ständig überwacht wird bis das Ereignis auftritt, das eine Aktion erfordert, wird im aktiven Modus Hash-Locking eingeleitet und gewartet bis das Event eintritt.

Atomic Swaps (auch Atomic Cross-Chain Trading) ist eine 2013 veröffentlichte Methode, um z.B. Kryptowährungen aus unterschiedlichen Blockchains auf dem direkten Weg auszutauschen. Eine vertrauenswürdige Drittinanz, wie beispielsweise eine Börse (Exchange), ist dazu nicht nötig⁶⁵. Bei Atomic Swaps wird die vertrauenslose Umgebung durch Hash Timelock Contracts (HTLC) gewährleistet. Das bedeutet u.a., dass beide Ketten über den gleichen Hash-Algorithmus verfügen müssen. Es handelt sich dabei um einen Smart Contract zwischen den Blockchains, wobei der Austausch in einem festgelegten Zeitrahmen vollständig ablaufen muss oder automatisch abgebrochen wird (s. auch Kapitel 1.2.7). Bei On-Chain Swaps läuft dieser auf einer der beiden Blockchains ab, bei Off-Chain Swaps auf der zweiten Schicht, z.B. über das Lightning-Netzwerk⁶⁶. Die Transaktionen folgen dabei einem festgelegten Schema. Zuerst hinterlegt Person A einen Betrag x in eine Vertragsadresse, die sich wie eine Art Safe verhält. Den Hashwert des Schlüssels sendet sie an Person B. Als nächstes verwendet Person B den von A bereitgestellten Hash, um eine weitere sichere Vertragsadresse zu erstellen, in der er den Betrag x in seiner Währung hinterlegt. Um dies in Anspruch zu nehmen, verwendet Person A den Schlüssel und gibt ihn dank Hashlock an Person B weiter, der daraufhin ihren Betrag x beanspruchen kann. Nachteile dieses Ansatzes sind die derzeit noch relativ geringe Geschwindigkeit und der recht anspruchsvolle technologische Umgang. Trotzdem ist zu erwarten, dass diese Technologie zukünftig weiter ausgebaut wird und sich auch langfristig durchsetzen könnte (Binance.com 2019).

Wichtig ist auch die Interoperabilität mit internen Systemen wie z.B. SAP oder Cloud (Bitkom e.V. 2019).

⁶³ Zu den 12 Eigenschaften gehören die Funktionalitäten, Abhängigkeit von einer dritten Partei, Skalierbarkeit, Art der Update-Funktion, Kosten des Zustandswechsels, native Token, semantische und syntaktische Interoperabilität, technologische Entwicklungen und Regulierung und wie viele DL formal und tatsächlich miteinander interagieren.

⁶⁴ BTCRelay ist ein Smart Contract auf dem Ethereum Ledger, der aus der Bitcoin-Blockchain liest.

⁶⁵ Diese birgt Einschränkungen, aber auch Risiken wie ein begrenztes Repertoire an Kryptowährungen bzw. Paarungen, eine Anfälligkeit gegenüber Hacking-Angriffen durch Zentralität, Ausfallzeiten und Volumenverlusten durch Marktschwankungen, Fondsmismanagement, Betriebskosten oder Abhängigkeit von staatlicher Regulierungsänderungen.

⁶⁶ 2017 erstmals zwischen Bitcoin und Litecoin erfolgreich durchgeführt.

4.4.2 Orakel

Im Zusammenhang mit der realen Welt kommt es zu der Problematik, dass die Transparenz und Unveränderbarkeit der Blockchain durch fehlerhafte Eintragungen oder Überführungen der realen Werte untergraben werden kann. Diese Schnittstelle muss also anderweitig abgesichert werden. Die derzeit am meisten genutzte Lösung sind Orakeldienste, die als Schnittstelle(n) zwischen einer bzw. mehreren Datenquelle(n) und dem aufrufenden Smart Contract fungieren⁶⁷. Die Übermittlung von Daten aus der Datenquelle an den aufrufenden Smart Contract kann on-chain oder off-chain geschehen. Im ersten Fall speichert der Dienst die angefragten Werte in einem speziellen Service-Contract in der Blockchain (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019), wo sie abgerufen werden können. Im zweiten Fall werden die Daten z.B. auf einer Website zur Verfügung gestellt und die Zugangsdaten per Transaktion an den aufrufenden Smart Contract verschickt. Die Authentizität der übermittelten Daten wird entweder über kryptografische Authentizitätsnachweise bereitgestellt, die der aufrufende Smart Contract überprüfen kann (Provable Things Limited o. J.) oder durch einen Abstimmungsprozess (Peterson et al. 2018). Es gibt auch die Möglichkeit, Einspruch zu erheben, wenn die Antworten des Orakels strittig sind (Social Minds Inc (KK) o. J.). Dabei ist zu beachten, dass die Integrität der Datenquelle nicht bewiesen ist.

Um die Vertrauenswürdigkeit der Ergebnisse aus der realen Welt sicherzustellen werden wie bei zentralen Systemen auch mehrere Schutzsysteme zusammengeschaltet. Zum einen kann der Orakeldienst auf mehrere Datenquellen zurückgreifen oder/und der aufrufende Smart Contract mehrere Orakeldienste einbinden. Eine weitere Möglichkeit besteht darin, den Diensten Anreize zu geben, richtige Daten zu liefern – u.a. dadurch, dass sie einen Betrag/Stake hinterlegen müssen, der sich durch Belohnung erhöht und bei Betrug (z.T.) einbehalten werden kann. Auch eine zuverlässige Ausführungsumgebung (Trusted Execution Environment (TEE)), wie die Software Guard eXtensions (SGX) von Intel oder die TrustZone von ARM, dienen der Vertrauenswürdigkeit. Das Problem hier liegt darin, dass sie nicht vor Schwachstellen gefeit sind und einen Single Point of Failure bieten.

Orakel-Projekte lassen sich grob unterteilen in Netzwerke, die Orakeldienste bereitstellen (Oracle-as-a-Service), und Netzwerke, die Orakeldienste internalisieren. Beispiele für den ersten Fall sind ChainLink (Ellis et al. 2017) oder Oraclize⁶⁸. Internalisierte Orakel sind z.B. Prediction Markets wie Augur oder Gnosis⁶⁹ oder im Bereich Finanzen und Versicherung von Bedeutung.

⁶⁷ Orakel-gesteuerte Smart Contracts bzw. DApps finden vielfältigen Einsatz, u.a. wenn es um die automatische Freigabe von Zahlungen geht, die z.B. vom Standort oder von anderen Bedingungen abhängen. Da GPS-Daten nicht immer die zuverlässigste Wahl sind, gibt es u.a. mit FOAM (Foamspace Corp 2019) ein dezentrales Netzwerk als Standortorakel.

⁶⁸ Oraclize bietet eine zentralisierte Lösung für Orakel an und ist der am längsten aktiv laufende und am weitesten verbreitetste Blockchain-Orakelservice. Oraclize.it weist per TLSNotary nach, dass es die Daten zwischen Datenquelle und Vertrag nicht verändert hat. Aus technischen Gründen allerdings belegt das Orakel das gegenüber einer z.B. bei AWS gehosteten virtuellen Maschine, der er nun vertrauen muss (Niemann 2017).

⁶⁹ Augur (Peterson et al. 2018) und Gnosis (Gnosis Ltd. 2017) sind Beispiele für Wettplattformen, die Blockchain einsetzen und sowohl Prognosen als auch Handel ermöglichen (Prognosemärkte). Sie nutzen die Weisheit der Massen (Surowiecki 2004) und ermöglichen das Wetten auf alles Mögliche und können deshalb für Unternehmen u.a. auch zur Markterschließung genutzt werden.

4.4.3 Standards und Regulierung

Gegenwärtig gibt es noch kein gemeinsames Verständnis bei der Umsetzung der Technologien und Interoperabilität zwischen Blockchains. Diese sind ohne Standardisierung auch nur schwer zu erreichen. Standardisierungsinstitutionen sind jedoch seit einigen Jahren weltweit aktiv, dennoch etablieren sich Standards im Moment noch schleichend. Die International Organization for Standardization (ISO) gründete bereits Anfang 2016 diesbezüglich eine Kommission (International Organization for Standardization 2016). Das Deutsche Institut für Normung (DIN) hat ebenfalls ein entsprechendes Gremium eingerichtet. Beim European Telecommunications Standards Institute (ETSI) gibt es ein Gremium (European Telecommunications Standards Institute (ETSI) 2018), das an der Standardisierung von Permissioned Distributed Ledgers arbeitet. Das Institute of Electrical and Electronics Engineers (IEEE) führt Standardisierungsprojekte im Blockchain-Umfeld durch (Institute of Electrical and Electronics Engineers 2019), in denen u.a. Blockchain-Rahmenwerke für den Bereich IoT und Automotive entwickelt werden. Das National Institute of Standards and Technology (NIST) sowie das American National Standards Institute (ANSI) arbeiten ebenfalls an dem Thema. Auf der Netzwerkebene beschäftigen sich die Internet Engineering Task Force (IETF) und das World Wide Web Consortium (W3C) mit Internet-Standards für eine einheitliche Identifikation der im Netzwerk zugreifbaren Ressourcen und der Adressierung von Blockchains. Sie sollen für eine Interoperabilität der Netzwerkkommunikation zwischen verschiedenen Blockchain-Systemen sorgen (W3C 2019), (Internet Research Task Force 2018). Weiterhin zu nennen sind hier z.B. auch die International Telecommunication Union (ITU), British Standard oder die Dutch Blockchain Coalition (Skwarek 2019).

An der Regulierung von Blockchains wird national, aber vor allem auf internationaler Ebene intensiv gearbeitet. Aufgrund ihrer Dezentralität kann es auch zu Problemen und Unsicherheiten im Schadens- oder Streitfall oder bei der Reaktion auf Sicherheitsprobleme kommen, die internationale Abstimmungen erfordern. So gibt es z.B. seit 2018 die European Blockchain Partnership, die zum Ziel hat, eine European Blockchain Services Infrastructure (EBSI) zu schaffen, die die Einrichtung einer grenzüberschreitenden digitalen öffentlichen Verwaltung unterstützen soll. Ebenfalls 2018 hat die Europäische Kommission das European Blockchain Observatory and Forum eingerichtet. Die Anfang 2019 offiziell gegründete International Association for Trusted Blockchain Applications (INATBA) ist eine Multi-Stakeholder-Organisation mit Sitz in Brüssel, die Lieferanten und Anwender von DLT mit Vertretern von Regierungsorganisationen und Normenorganisationen aus der ganzen Welt zusammenbringt. Die Bundesregierung hat zudem kürzlich ihre nationale Blockchain-Strategie veröffentlicht (BMF, BMWi 2019), wobei sie sich auf europäischer und internationaler Ebene für die Schaffung eines angemessenen Regulierungsrahmens für Krypto-Assets einsetzt. Fortlaufende Arbeiten gibt es auch auf Ebene der G20 und G7 zu Krypto-Assets. Daneben kann zukünftig eine Sicherheitszertifizierung von Blockchain-Produkten oder ausgewählten Komponenten für bestimmte Anwendungen sinnvoll sein. Voraussetzung dafür sollte dann die Verwendung von kryptografischen Algorithmen sein, die vom BSI für Blockchain-Anwendungen anerkannt wurden (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019).

4.5 Ausgewählte Alternativen zur Blockchain

Es gibt bereits eine Vielzahl von DL Ansätzen mit zur Blockchain alternativen Datenstrukturen und Ergänzungen von Blockchains durch andere Netzwerkstrukturen. Da diese Technologien noch neu und in der Entwicklung sind, gibt es oft hinsichtlich der Sicherheitsaspekte, der Zentralisierung

und der Resistenz gegenüber verschiedenen Angriffsformen noch viele offene Fragen, aber auch ein enormes Potenzial.

DAG-basierte Systeme sind sogenannte allgemein gerichtete, zyklenfreie Graphen, d. h. Strukturen, die eine Menge von Objekten zusammen mit den zwischen diesen Objekten bestehenden Verbindungen repräsentiert. Die Transaktionen werden meist asynchron, also unabhängig von anderen Transaktionen und direkt ausgeführt. Theoretisch ermöglichen sie sogar unendlich viele Transaktionen pro Sekunde. Im Folgenden werden einige Beispiele vorgestellt.

4.5.1 IOTA

Ein Beispiel für ein DAG-basiertes System mit baumartiger Struktur ist der Tangle⁷⁰ von IOTA (Popov 2018), (IOTA Foundation 2019). Die IOTA-Foundation wurde gegründet (Alexander 2018), um ein Rückgrat des Internet der Dinge (IoT) und der Maschinenökonomie anzubieten, indem es in der sogenannten Machine-to-Machine (M2M) Kommunikation Möglichkeiten für Kommunikation, Datenaustausch, Mikro- und Nanozahlungen und andere Anwendungen bereitstellt. Dazu braucht es neben der Dezentralisierung eine nahezu unbegrenzte Skalierbarkeit (wobei die Netzwerkgeschwindigkeit mit der Aktivität durch die parallele Validierung steigt) sowie gebührenlose Transaktionsabwicklungen. Das IOTA-Netz zeichnet sich weiterhin durch eine quantenresistente Verschlüsselung [231], die Möglichkeit Offline-Transaktionen durchzuführen und ein modulares Konzept aus, das es anderen Technologien ermöglicht, an IOTA anzudocken. Der Tangle ist wie die Blockchain ein Distributed Ledger, in der alle Transaktionen als Kästchen eines DAG gespeichert werden⁷¹ (s. Abbildung 13). Die Transaktionen können dabei beliebige Daten enthalten wie z.B. Überweisungen oder Sensordaten. Auch hier werden die mit dem privaten Schlüssel des Senders signierten, noch unbestätigten Transaktionen (sogenannte Tips) gesammelt und zufällig zwei Tips aus dem Tangle ausgewählt, die in der neuen Transaktion dann referenziert werden. Um die Transaktion zu bestätigen, muss der Sender einen gewissen PoW erbringen, der ähnlich dem Hashcash-Algorithmus von Bitcoin ist und Spam vorbeugen soll. Sobald dies erfolgt ist, wird die Transaktion in den Tangle eingetragen. Die Transaktion referenziert dann die zwei vorherigen Transaktionen sowie indirekt auch deren vorherige. Bestätigt wird die neue Transaktion, indem dann jemand anderes die Transaktion referenziert. Die Gültigkeit von Transaktionen nimmt zu, je mehr Transaktionen hinzugefügt werden. Der Knoten, der eine Transaktion einstellt, kann bestimmen, wieviel Prozent bestätigender Tips zur Gesamtzahl der Tips für ihn ausreichend sind, um einen Konsens für eine Transaktion zu erreichen. Dabei liegt es in seinem Interesse, eine möglichst große Zahl einzugeben, um nicht Gefahr zu laufen, in eine sogenannte parasitäre Kette zu laufen (Cullen et al. 2019). Dieses Level wird durch die n-malige Ausführung einer sogenannten Monte-Carlo-Markov-Kette (MCMK) bestimmt. Bei IOTA werden zwei Transaktionsarten unterschieden – Value-Transaktionen, bei denen IOTA-Tokens übertragen werden, und Zero-Value-Transaktionen zur Übertragung von Daten. Im ersten Fall ist es im Allgemeinen notwendig, Ein- und Ausgangstransaktionen in einem Bundle zusammenzufassen. Dabei nutzt IOTA ein UTXO-ähnliches Schema (s. auch Kapitel 1.2.2.1 oder 1.2.6.3). Bis das IOTA-Netzwerk eine hinreichende Größe hat funktioniert es mit einem sogenannten Koordinator, der die Validität der Transaktionen überprüft. Dieser wird durch die IOTA-Foundation betrieben. Sein Quellcode ist nicht einsehbar. Der Koordinator erstellt im Minutentakt sogenannte Meilensteine - alle Transaktionen, die direkt oder indirekt von diesem validiert wurden, gelten als bestätigt. Da

⁷⁰ Deutsch: Wirrwar

⁷¹ Die im Tangle gespeicherten Transaktionen können beispielsweise unter <https://thetangle.org/> eingesehen werden.

die Speicherkapazitäten der Nodes begrenzt sind, führte IOTA die Möglichkeit ein, lokale Schnappschüsse vom Netzwerkzustand zu erstellen. In der Standardkonfiguration erfolgt dies alle 30 Tage, bevor die alten Daten aus dem Node gelöscht werden. Für die Fälle, in denen Daten länger verfügbar bleiben müssen oder sollten, wie im Finanzsektor oder bei der Speicherung von Identitätsdaten, sollen sogenannte Permanodes eingeführt werden, die die gesamte Transaktionsgeschichte des Tangles auf unbegrenzte Zeit speichern können sollen. Die Chronicle genannte Erweiterung ermöglicht es weiterhin, dass die Permanodes Ordnung in das Gewirr des Tangle bringen, indem sie es in adäquater Zeit durchsuchbar machen (BTC-ECHO GmbH 2019c). Zukünftig sollen auch Lightweight Knoten und auch Zahlungskkanäle, hier Flash-Netzwerk genannt, eingeführt werden sowie Privacy-Aspekte durch Vermischen von Transaktionen (Token Shuffling) berücksichtigt werden. Das Masked Authenticated Messaging (MAM) soll Sensoren und anderen Geräten ermöglichen, Datenströme zu verschlüsseln und im Tangle quantensicher zu verankern. Berechtigte Personen können den Datenstrom wiederherstellen.

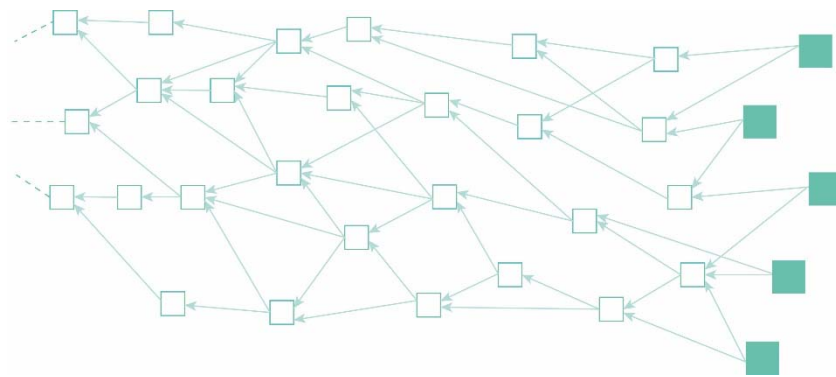


Abbildung 13: IOTA Tangle (eigene Darstellung nach (Schiener o. J.)). Die grünen Quadrate symbolisieren neue Transaktionen.

Mit internationalen Konzernen über etliche Branchen hinweg wurden bereits Kooperationen geschlossen sowie Testprojekte umgesetzt. Unter anderem entwickelt die IOTA-Foundation gemeinsam mit diesen Firmen einen Datenmarkt auf Basis der in IOTA eingesetzten Technik. Interessante Branchen für IoT und IOTA sind z.B. das Transportwesen, Infrastruktur und Fahrzeuge, das Gesundheitswesen, Lieferung und Bezahlung von Energie, Lieferketten und weltweiter Handel, Gebrauchsgeräte im Alltag und Haushalt (von Haushalts- bis Unterhaltungselektronik) sowie der Austausch von Geld und Daten. Auch für Forschungsinstituten und Universitäten ist IOTA von Interesse. So wurde z.B. ein auf IOTA basierender Platooning-Prototyp entwickelt (Fridgen et al. 2019). Durch den Datenaustausch sind die Fahrzeuge ähnlich einer elektronischen Deichsel digital aneinandergekoppelt und können eine Kolonne bilden. Für nachfolgende Fahrzeuge wird so eine teilautonome Fahrt möglich. Die dadurch verbundenen Einsparungen (etwa durch Windschatten oder Ruhezeiten) werden in einem Vergütungssystem abgebildet. Erste alltagstaugliche Anwendungen und DApps könnten ab 2020 verfügbar sein (L. 2019). Langfristig kann sich hier eine Konkurrenz zu Blockchain-Lösungen etablieren, wobei insbesondere Weiterentwicklungen wie Qubic interessant sind, mit dem das IOTA-Protokoll Smart Contracts sowie Orakel ermöglichen will (Renz 2019).

4.5.2 Hashgraph

Hashgraph bildet die technologische Basis für einen speziellen Konsensalgorithmus und die dafür notwendige Datenstruktur (Baird et al. 2019). Das Unternehmen Swirlds Inc. besitzt das Patent auf die 2016 entwickelte Idee. Die daraus entwickelte Hedera Hashgraph Plattform war ursprünglich für den privaten Unternehmensbereich gedacht, soll nun jedoch auch für den Aufbau eines öffentlichen Hashgraph-Netzwerkes genutzt werden (Keller 2018).

Jeder Teilnehmer kann zu jeder Zeit eine signierte Transaktion erstellen, die er in eine Nachricht (Event) verpackt und diese an zufällig ausgewählte Knoten verschickt, die diese weiterverbreiten (Gossip Protokoll). So gelangt das Wissen über einzelne Nachrichten zu unterschiedlichen Zeitpunkten an die Knoten. Wenn ein Knoten sein Event an einen anderen Knoten verschickt, dann erzeugt der Empfänger-Knoten ein neues Event, das über eine definierte Struktur einen Verweis auf das Sender-Event besitzt und einen Verweis auf das letzte eigene Event. Alle Events im Hashgraph sind somit über kryptografische Hashes des empfangenen Events (Other-Parent) und des eigenen vorherigen Events (Self-Parent) verbunden. Das neu erzeugte Event enthält neue, weitere Transaktionen, den Zeitstempel mit dem Zeitpunkt der Event-Erstellung und die vom Empfänger-Knoten erzeugte Signatur des Events (s. Abbildung 14 und 15).

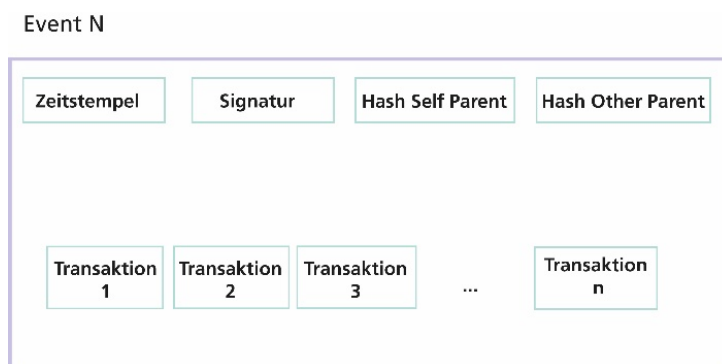


Abbildung 14: Aufbau eines Events (eigene Darstellung nach (Heinze 2019)).

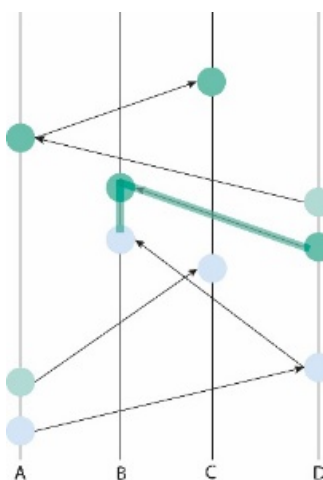


Abbildung 15: Hashgraph der Nachrichtenverteilung. In diesem Beispiel gibt es vier Knoten A-D. A schickt ein Event (hellblau) nach D und nach C. D sendet Information von A weiter an B. D sendet ein weiteres, zweites Event (dunkelgrün) an B und an A, A dieses wiederum an C. Die dunkelgrün markierte Linie deutet an, wie ein neues Event aus den Parent-Events entsteht (eigene Darstellung nach (Heinze 2019)).

Durch diese Art der Verknüpfung entsteht ein gerichteter Graph über die Events und ihre Vorfahren, mit dem sich belegen lässt, wann welche Events erstellt wurden und wer diese wann erhalten hat (Gossip about Gossip). Da jeder Knoten die Historie dieses Informationsaustausches im lokalen Hashgraph⁷² aufzeichnet, kann er nun berechnen, welche Stimme ein anderer Knoten ihm geschickt hätte, wenn sie eine traditionelle byzantinische Übereinkunft mittels Versendens von Stimmen durchgeführt hätten. Man nennt dieses „Abstimmen ohne Abstimmung“ Virtual Voting. Dieses Vorgehen zeichnet sich nicht nur durch Ressourceneffizienz aus, sondern ermöglicht sogar eine Toleranz gegenüber asynchronen byzantinischen Fehlern (aBFT⁷³ (Meinel et al. 2018)). In der Praxis werden allerdings nicht alle, sondern nur ausgewählte⁷⁴ Witness-Events geprüft. Auf geschickte Art und Weise lässt sich daraus die Konsensreihenfolge über den Konsenszeitstempel herstellen, der im Prinzip aus dem Median der Empfangszeit der Events in den einzelnen Knoten ermittelt wird.

Neben der sicheren aBFT-Kommunikation (Hedera Hashgraph 2018) verspricht Hashgraph schnelle und kostenlose Transaktionen (von 250.000 und mehr tps (Baird 2016)), Korrektheit, Konsistenz und Integrität der Daten, faire Kommunikation (niemand kann die Reihenfolge der Transaktionen manipulieren) und Effizienz (es gibt keine geminten Blöcke, die verworfen werden müssen). Im Gegensatz zur Blockchain muss diese Art von Ledger allein zur Integritätssicherung keine Transaktionshistorie mehr aufbewahren. Nachdem eine Transaktion entsprechend ihrer Konsens-Reihenfolge ausgeführt worden ist, kann diese auf Wunsch weggeworfen werden. Der Zustand des Systems, welcher durch die Ausführung der Transaktionen in Konsens-Reihenfolge fortgeschrieben wird, kann wiederum in einer dezentralen Datenbank on-ledger festgehalten werden, welches die Bearbeitung und Löschung der Daten sowie eine kryptografische Beweisführung über deren Unversehrtheit ermöglicht (Baird 2019). Auf funktionaler Ebene kann dadurch auch die Option zur kontrollierten Veränderung (Controlled Mutability) des Ledgers ermöglicht werden. Smart Contracts können dabei optional und transparent mit der Fähigkeit angelegt werden, durch die notwendige Anzahl und Kombination von Signaturen in einem vordefinierten Multisignatur-Schema aufgeschlossen zu werden, um beliebige Änderungen wie Korrekturen des Systemzustandes ebenfalls transparent und nachvollziehbar durch berechtigte Akteure vornehmen zu können (Madsen 2018). Die Vision ist, mit Hilfe der Hashgraph-Technologie eine Art Internet of Shared Worlds zu erschaffen, die einige Probleme des heutigen Internets überwinden könnte. Es würde jeder Person ermöglichen, eine eigene Welt bzw. eine eigene Gemeinschaft zu schaffen, die dann über die DL-Technologien reibungslos miteinander kommunizieren und zu einem Konsens finden könnten (Hays 2019).

⁷² Der obere Bereich des Graphen ist zwar nicht exakt gleich, aber die Knoten haben immer einen konsistenten Stand. Dies bedeutet, dass zwei Knoten, die ein Event im lokalen Hashgraph haben, auf beiden Knoten auch immer die beiden identischen Vorfahren existieren.

⁷³ Das bedeutet, dass solange weniger als $1/3$ der Netzwerkteilnehmer mutwillige Betrugsabsichten haben, kann immer ein Konsens über den Zustand des Netzwerkes und der Transaktionshistorie gefunden werden.

⁷⁴ Die ersten Witness-Events sind die ersten eines jeden lokalen Hashgraphs. Ist die Mehrzahl der Witness-Events von einem neuen Event über einen Pfad erreichbar, der über mehr als $2n/3$ der Knoten führt, so wird eine neue Runde aufgemacht, die wieder Witness-Events mit startet, u.s.w.. Die Aufteilung in Runden sowie die Ermittlung von Famous-Witness-Events spielen bei dem Verfahren eine wesentliche Rolle.

4.5.3 Blockgitter

Ein Blockgitter (Blocklattice) ist eine weitere Variante der DAG-Datenstruktur. Eingeführt wurde das Blockgitter von Nano (Nano 2019). Jeder Knoten besitzt hier seine eigene Blockkette, die eigentlich eine Account-Chain ist und die eigene Transaktionshistorie widerspiegelt. Die Knoten müssen mit einer ersten eigenen Transaktion den Prozess initiieren, um untereinander Transaktionen durchzuführen, die aus dem "Send"-Block beim Sender und den "Receive"-Block beim Empfänger besteht. Der Konsensmechanismus ist ein delegated Proof-of-Stake (dPoS). Um Spam zu reduzieren, wird zusätzlich ein kleines PoW-Element hinzugefügt - jeder Benutzer verbringt ca. 5 Sekunden damit, seine Transaktion zu signieren. Es dauert etwa 1 Mikrosekunde, bis die Knoten sie validiert haben. Diese Art des Blockgitterimplementierung besitzt einige Herausforderungen. Validatoren müssen nicht nur eine Vielzahl an Account-Chains hosten, sondern sind u.a. auch sogenannten Penny-Spend-Attacken⁷⁵ ausgesetzt und validieren unentgeltlich. Dadurch, dass es keine globale Ordnung aller Transaktionen gibt, können auch Smart Contracts nicht ausgeführt werden. Dexon geht einen etwas anderen Weg, um ein Blockgitter zu realisieren (DEXON Foundation 2019).

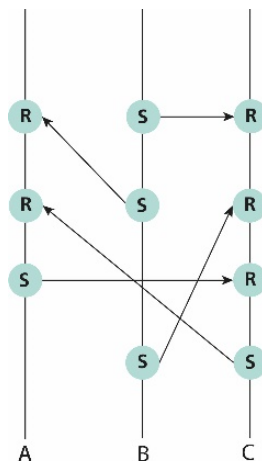


Abbildung 16: Datenstruktur für Netzwerkteilnehmer A, B und C im Blockgitter Nano. S(end) und R(eceived) stellen gesendete und erhaltene Transaktionen dar (eigene Darstellung nach (Nano 2019)).

4.5.4 Auswahl weiterer Möglichkeiten

Für manche Anwendungen kann nicht nur die Blockchain-typische Vorwärts-, sondern auch eine Rückwärtsverkettung der Datenblöcke erforderlich sein, wie beispielsweise beim Zusammenführen von Identitäts- und Rechtemanagement. Hier gibt es Lösungsansätze, deren Absicherungsmechanismus in Anlehnung an das Prinzip chemischer Bindungen funktioniert (Wilke 2017), (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019), (Keuper 2018).

⁷⁵ Bei einer Penny-Spend-Attacke lädt ein Angreifer die Guthaben einer großen Anzahl von Accounts mit Kleinstbeträgen auf, wodurch Speicherressourcen verbraucht werden.

4.6 Sonstige Trends

Aufgrund der Relevanz der **Konsensverfahren** hat sich ein neues Forschungsfeld herausgebildet, das sich intensiv mit optimierten Konsens-Logiken auseinandersetzt und auf spieltheoretischer Basis testet und beweist (siehe Kapitel 1.2.6.3).

Wie beschrieben sind **Smart Contracts**, DApps und DAOs interessante Möglichkeiten der Blockchain Technologie. Hierdurch wird ein Grundstein für eine Vertragsdurchführung ohne menschliche Kontrollen gelegt. Gegenwärtig werden u.a. Technologien entwickelt, die mögliche Fehler im Programmcode von Smart Contracts automatisiert erkennen können und Fälle wie The DAO (s. auch Kapitel 1.2.7) zukünftig vermeiden zu können (Narayanan und Clark 2017). Des Weiteren werden Möglichkeiten einer formalen Verifikation von Smart Contracts untersucht (Luu et al. 2016a). Auch die Überprüfung des Bytecodes wird in Betracht gezogen (Bhargavan et al. 2016). Es bedarf noch weiterer Arbeit in diesem Bereich, vor allem auch für Blockchains jenseits von Ethereum. In aktuellen Forschungsarbeiten wird darüber hinaus untersucht, auf welche Weise man rechtsverbindliche Verträge auf der Basis von Smart Contracts verwirklichen kann (Peters und Panayi 2015). Hier existieren unter anderem Überlegungen, in Zukunft aus einer geeigneten gemeinsamen Vorlage automatisiert sowohl das entsprechende Computerprogramm des Smart Contract als auch den dazugehörigen Vertragstext zu erzeugen⁷⁶.

In den letzten Jahren gab es eine Vielzahl von Aktivitäten rund um **konsortiale Blockchains**. Neben den in Kapitel 1.2.8 genannten sind u.a. die Blockchain-Ökosysteme EWF (Energy Web Foundation o. J.) und B3i (B3i Services AG 2019) aus dem Energie- bzw. Versicherungssektor hier erwähnenswert. Verantwortlichkeiten können in privaten und konsortialen Blockchains zugewiesen, die jeweiligen Rechte und Aufgaben der teilnehmenden Akteure individuell festgelegt werden. Dies hat Vorteile bei der Auswahl der Konsensmechanismen sowie aus rechtlicher Sicht.

Einen effektiven Einstieg in DLTs mit einer Infrastruktur, die mit dem Bedarf wachsen kann und für die ein Ansprechpartner zur Verfügung steht, ermöglichen zunehmend **Blockchain-as-a-Service-Angebote (BaaS)** in der Cloud.

Klimaschutz- und Nachhaltigkeitsaspekte finden in Anbetracht der Tatsache, dass z.B. die Bitcoin-Blockchain jährlich ca. 73 TWh, vergleichbar mit dem Energieverbrauch von Österreich und entsprechend 0,3 % des weltweiten Stromverbrauchs benötigt, eine wichtige Rolle. Diese Zahl entspricht im Mittel einem Energieverbrauch von fast 1MWh pro Transaktion (Digiconomist 2019). Neuste Ergebnisse einer Studie ergaben weiterhin, dass das Minen von Bitcoin im Wert von 1 \$ in den USA fast 0,5 \$ an Gesundheits- und Klimaschäden mit sich brachte (Goodkind et al. 2020). Artikel, die dem Bitcoin eine große Verantwortung an der globalen Erderwärmung zuschreiben (Mora et al. 2019), müssen allerdings kritisch betrachtet werden (Masanet et al. 2019). Lösungsansätze dieses durch den PoW-Algorithmus verursachten Energieproblems gibt es einige, wobei darauf geachtet werden muss, dass die Sicherheit in einem nicht vertrauenswürdigen Umfeld gewährleistet bleiben muss. Auf der anderen Seite könnten DLs helfen, Herausforderungen der Umweltpolitik anzugehen, indem sie eine sichere und nachprüfbare Aufzeichnung darüber bietet, wer welche natürlichen Ressourcen mit wem austauscht (Le Sève et al. 2018), (Herweijer et al. 2018). Einige Autoren sehen in der Blockchain bzw. DLT das Potenzial, einen Beitrag zu den UN-Nachhaltigkeitszielen leisten zu können (Hughes et al. 2019).

⁷⁶ Ein Ricardian Contract ist ein System zum automatisierten Übertragen von Rechten.

Eine Recherche zum Impact wissenschaftlicher Arbeiten in Onlinemedien (Altmetrics Attention Score) in der Datenbank Dimension, weist neben den Herausforderungen wie Datenschutz und Datensicherheit, u.a. auch auf Nachhaltigkeits- und Sicherheitsaspekte hin (hier z.B. das Thema Waffenkontrolle (Bloom 2019)).

5 ZUSAMMENFASSUNG UND AUSBLICK

DLT lässt sich als höherwertige digitale Infrastrukturtechnologie verstehen. Nach dem Internet der Informationen entwickelte sich zunehmend durch die Vernetzung intelligenter Geräte das Internet der Dinge. Die Einführung der DLT ermöglicht nun zusätzlich Werttransaktionen im sogenannten Internet der Werte (Internet of Value)⁷⁷, das in eine sogenannte Token Economy münden kann (Voshmgir 2019). Unter diesem Begriff lässt sich die digitale Abbildung und Eintragung von Werten, wie reale Gegenstände oder Rechte, sozusagen als digitaler Zwilling/Schatten in DL zusammenfassen. Alles, was einen Wert besitzt, kann dann über das Internet transferiert werden (Z_punkt GmbH 2019). Darin wird das Potenzial zu einer gesellschaftlichen Transformation gesehen.

Über eine Vielzahl von Anwendungsfeldern hinweg lässt bzw. ließe sich die Blockchain-Technologie gewinnbringend einsetzen. Ob ihr Einsatz jedoch empfehlenswert ist, muss anhand unterschiedlicher Entscheidungskriterien geprüft werden (s. auch Kapitel 2.1). Der Einsatz der Blockchain-Technologie empfiehlt sich jedoch insbesondere bei solchen Prozessen, die Werte, Rechte oder Nachweise verschiedener Art übertragen, vor allem dann, wenn die Vertrauensbasis fehlt. Je nach Anwendungsfall treten verschiedene Aspekte der Blockchain-Technologie in den Vordergrund, die eine Vielzahl an unterschiedlichen Implementierungen mit sich bringen, die dann wiederum kompatibel sein müssen. Solche Aspekte sind u.a. Datensouveränität, Automatisierbarkeit, Irreversibilität, Redundanz bzw. Ausfallsicherheit, Nachverfolgbarkeit, aber auch Effizienz- und Effektivitätssteigerung sowie Nachhaltigkeit. Sicherheit, Skalierbarkeit, Interaktion untereinander und mit der realen Welt sowie Standardisierung sind dabei von großer Relevanz. Die Entwicklungen der DLTs bewegen sich dabei in dem größeren Kontext der Digitalisierung. Im Zusammenspiel mit weiteren Technologien und als Grundlage für darauf aufbauende Geschäftsmodelle könnten sie ihr volles Potenzial entfalten. Es wird davon ausgegangen, dass langfristig viele der technologischen und rechtlichen Hürden überwunden werden (Fridgen et al. 2019). Wir beginnen jedoch gerade erst, die Möglichkeiten und Wirkungen, die mit Blockchain und DL verbunden sind, zu verstehen und können diese oft nur schemenhaft ausmalen (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2019). Es geht hier um ein stetiges Dazulernen, zu dem dieses Projekt beitragen soll. Weiterhin sollen deutsche Unternehmen unterstützt werden, denn, obwohl sich schon heute vielfältige Anwendungsmöglichkeiten abzeichnen, halten sich vor allem die kleinen und mittelständischen Unternehmen bei diesen Technologien noch zurück. Es fehlt ihnen an sinnvollen spezifischen Use Cases, an qualifiziertem Personal sowie an einem Beratungsangebot u.a. bei der Implementierung von Blockchain oder DLT (Bitkom e.V. 2019) (Gentemann 2019). Neben den organisatorischen und technologischen Herausforderungen, die u.a. mit Interoperabilitäts-, Standardisierungs- und Sicherheitsaspekten zu tun haben, ist auch die noch nicht auf alle Use Cases abgebildete Rechtssicherheit problematisch. Damit die Technologie dem Rechts- und Wertesystem entsprechend

⁷⁷ Das Internet als Transfer- und Aufbewahrungsraum für jegliche denkbare Werte (z.B. Geld, geistiges Eigentum oder Wertpapiere, Immobilien, Kunstgegenstände)).

weiterentwickelt wird und Wirtschaft und Gesellschaft einen Mehrwert bringt, muss ein Staat proaktiv bzw. gestaltend mitwirken. Die Bundesregierung geht hier mit ihrer Blockchain-Strategie in diese Richtung. Dabei werden wichtige Themen wie z.B. die Schaffung internationaler Rechts- und Handelsräume, finanzielle initiale Investitionen/Förderungen, Smart Contract Register sowie akkreditierte Zertifizierungsverfahren für Smart Contracts, Round Tables zum Thema Datenschutz, Blockchain-basierte digitale Identitäten, Blockchain-Hubs bzw. -Kompetenzzentren sowie Testräume, wie Sandboxes bzw. Reallabore, adressiert. Diese Themen werden ausführlich im Projektbericht zur Kontextanalyse betrachtet.

6 LITERATURVERZEICHNIS

- Alexander, Roman (2018): IOTA: Die Einführung in die Tangle-Technologie. Alles über die revolutionäre Blockchain-Alternative. Independently published.
- All In Bits, Inc. (2019): Tendermint - Blockchain Consensus. Online verfügbar unter <https://tendermint.com/>, zuletzt aktualisiert am 07.10.2019, zuletzt geprüft am 29.10.2019.
- Androulaki, E. (2017): Blockchain for the Enterprise: Hyperledger-fabric. Online verfügbar unter [https://www-01.ibm.com/events/wwc/grp/grp309.nsf/vLookupPDFs/2%20ElliAndroulaki%20BlockChain%20for%20the%20Enterprise/\\$file/2%20ElliAndroulaki%20BlockChain%20for%20the%20Enterprise.pdf](https://www-01.ibm.com/events/wwc/grp/grp309.nsf/vLookupPDFs/2%20ElliAndroulaki%20BlockChain%20for%20the%20Enterprise/$file/2%20ElliAndroulaki%20BlockChain%20for%20the%20Enterprise.pdf), zuletzt geprüft am 13.12.2019.
- Androulaki, Elli; Manevich, Yacov; Muralidharan, Srinivasan; Murthy, Chet; Nguyen, Binh; Sethi, Manish et al. (2018): Hyperledger fabric. In: Pascal Felber, Y. Charlie Hu und Rui Oliveira (Hg.): Proceedings of the Thirteenth EuroSys Conference. the Thirteenth EuroSys Conference. Porto, Portugal, 4/23/2018 - 4/26/2018. New York, NY, USA: ACM, S. 1–15.
- Angelis, S. de; Aniello, L.; Baldoni, R.; Lombardi, F.; Margheri, A.; Sassone, V. (2017): PBFT Vs Proof-Of-Authority: Applying The Cap Theorem To Permissioned Blockchain. In: CINI Cyber Security National Laboratory (Hg.): Italian Conference on Cybersecurity.
- Antonopoulos, Andreas M. (2018): Bitcoin und Blockchain - Grundlagen und Programmierung. Die Blockchain verstehen, Anwendungen entwickeln. 2. Auflage. Heidelberg: O'Reilly. Online verfügbar unter <http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=1804640>.
- Anwar, Hasib (2018): Web 3.0 Will Be Powered by Blockchain Technology Stack. Online verfügbar unter <https://101blockchains.com/web-3-0-blockchain-technology-stack/#19>, zuletzt geprüft am 25.10.2019.
- Apostolaki, Maria; Zohar, Aviv; Vanbever, Laurent (2017): Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. In: 2017 IEEE Symposium on Security and Privacy - SP 2017. 22-24 May 2017, San Jose, California, USA: proceedings. 2017 IEEE Symposium on Security and Privacy (SP). San Jose, CA, USA, 5/22/2017 - 5/26/2017. IEEE Symposium on Security and Privacy; Institute of Electrical and Electronics Engineers; IEEE Computer Society; SP; Symposium on Security & Privacy; S&P; IEEE S&P. Piscataway, NJ: IEEE, S. 375–392.
- Arasev, Vadim (2018): POA Network Whitepaper. Online verfügbar unter <https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper>, zuletzt geprüft am 26.11.2019.
- Aste, Tomaso; Tasca, Paolo; Di Matteo, Tiziana (2017): Blockchain Technologies: The Foreseeable Impact on Society and Industry. In: *Computer* 50 (9), S. 18–28. DOI: 10.1109/MC.2017.3571064.
- B3i Services AG (2019): B3i Home. Online verfügbar unter <https://b3i.tech/home.html>, zuletzt geprüft am 29.11.2019.
- Back, Adam; Corallo, Matt; Dashjr, Luke; Friedenbach, Mark; Maxwell, Gregory; Miller, Andrew et al. (2014): Enabling Blockchain Innovations with Pegged Sidechains.

- Baird, Leemon (2016): THE SWIRLDS HASHGRAPH CONSENSUS ALGORITHM: FAIR, FAST, BYZANTINE FAULT TOLERANCE. SWIRLDS TECH REPORT SWIRLDS-TR-2016-01. Online verfügbar unter <https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf>, zuletzt aktualisiert am 18.03.2018, zuletzt geprüft am 11.10.2019.
- Baird, Leemon (2019): Hedera Hashgraph Webinar: A stable ledger in an unstable forking world. Hedera Hashgraph.
- Baird, Leemon; Harmon, Mance; Madsen, Paul (2019): Hedera: A Public Hashgraph Network & Governing Council. The trust layer of the internet. Hedera Hashgraph, LLC. Online verfügbar unter <https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf>, zuletzt aktualisiert am 2019, zuletzt geprüft am 19.11.2019.
- Baliga, Arati (2017): Understanding-Blockchain-Consensus-Models. Santa Clara. Online verfügbar unter <https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf>, zuletzt geprüft am 11.10.2019.
- Baliga, Arati; Subhod, I.; Kamat, Pandurang; Chatterjee, Siddhartha (2018): Performance Evaluation of the Quorum Blockchain Platform, 19.07.2018. Online verfügbar unter <https://arxiv.org/pdf/1809.03421>.
- Bankenverband (2019): Jenseits von Libra: Warum die Wirtschaft einen digitalen Euro braucht. Bundesverband deutscher Banken. Online verfügbar unter <https://bankenverband.de/fachthemen/digital-banking/programmierbarer-digitaler-euro/>, zuletzt geprüft am 19.11.2019.
- Barcelo, Jaume (2007): User Privacy in the Public Bitcoin Blockchain. Online verfügbar unter <https://pdfs.semanticscholar.org/549e/7f042fe0aa979d95348f0e04939b2b451f18.pdf>, zuletzt geprüft am 15.08.2019.
- BBC (2017): CryptoKitties craze slows down transactions on Ethereum. Online verfügbar unter <https://www.bbc.com/news/technology-42237162>, zuletzt geprüft am 25.10.2019.
- Beck, Roman; Müller-Bloch, Christoph (2017): Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as Incumbent Organization. In: Proceedings of the 50th Hawaii International Conference on System Sciences (2017). Hawaii International Conference on System Sciences: Hawaii International Conference on System Sciences (Proceedings of the Annual Hawaii International Conference on System Sciences).
- Bentov, Iddo; Lee, Charles; Mizrahi, Alex; Rosenfeld, Meni: Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. Online verfügbar unter <https://eprint.iacr.org/2014/452.pdf>, zuletzt geprüft am 11.06.2019.
- Bhargavan, Karthikeyan; Delignat-Lavaud, Antoine; Fournet, Cédric; Gollamudi, Anitha; Gonthier, Georges; Kobeissi, Nadim et al. (2016): Formal Verification of Smart Contracts: Short Paper. Online verfügbar unter <https://hal.inria.fr/hal-01400469/document>, zuletzt geprüft am 29.11.2019.
- BigchainDB GmbH (2018): bigchaindb-whitepaper. Berlin. Online verfügbar unter <https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf>, zuletzt geprüft am 05.11.2019.
- Binance.com (2019): Wie funktionieren Atomic Swaps? | Binance Academy. Online verfügbar unter <https://www.binance.vision/de/blockchain/atomic-swaps-explained>, zuletzt geprüft am 08.11.2019.

- Biryukov, Alex; Khovratovich, Dmitry; Pustogarov, Ivan (2014): Deanonymisation of clients in Bitcoin P2P network. Online verfügbar unter <http://arxiv.org/pdf/1405.7418v3>.
- Bitcoin Community (2018): Bitcoin Wiki. MediaWiki. Online verfügbar unter https://en.bitcoin.it/wiki/Main_Page, zuletzt geprüft am 29.11.2019.
- Bitkom e.V. (2019): Evaluierung und Implementierung von Blockchain Use Cases. Online verfügbar unter <https://www.bitkom.org/Bitkom/Publikationen/Evaluierung-Implementierung-Blockchain-Use-Cases>, zuletzt geprüft am 13.12.2019.
- Blockchain Bundesverband (2018): Blockchain Bundesverband. Online verfügbar unter <https://bundesblock.de/de/groups/>, zuletzt geprüft am 15.10.2019.
- BLOCKCHAIN LUXEMBOURG S.A. (2017): Blockchain Size. Online verfügbar unter <https://www.blockchain.com/de/charts/blocks-size?timespan=2years>, zuletzt geprüft am 15.10.2019.
- Blockstream (o.J.): Elements. Online verfügbar unter <https://elementsproject.org/>, zuletzt aktualisiert am 12.11.2019, zuletzt geprüft am 26.11.2019.
- Bloom, Andrew (2019): Blockchain Technology and its use in the fight against Weapons being traded on the Illegal Arms Market - GBA Global. Government Blockchain Association. Online verfügbar unter <https://www.gbglobal.org/blockchain-technology-and-its-use-in-the-fight-against-weapons-being-traded-on-the-illegal-arms-market/>, zuletzt geprüft am 19.11.2019.
- Bloomberg News (2019): Why China's Rushing to Mint Its Own Digital Currency. Online verfügbar unter <https://www.bloomberg.com/news/articles/2019-09-10/why-china-s-rushing-to-mint-its-own-digital-currency-quicktake>, zuletzt geprüft am 25.10.2019.
- BMF, BMWi (2019): Blockchain-Strategie der Bundesregierung. Wir stellen die Weichen für die Token-Ökonomie.
- Bonneau, Joseph; Miller, Andrew; Clark, Jeremy; Narayanan, Arvind; Kroll, Joshua A.; Felten, Edward W. (2015): SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In: 2015 IEEE Symposium on Security and Privacy (SP). 17 - 21 [i.e. 18 - 20] May 2015, San Jose, California, USA. 2015 IEEE Symposium on Security and Privacy (SP). San Jose, CA, 5/17/2015 - 5/21/2015. Institute of Electrical and Electronics Engineers; IEEE Computer Society; IEEE Symposium on Security and Privacy; SP; IEEE Symposium on Security & Privacy; S&P. Piscataway, NJ: IEEE, S. 104–121.
- Bose, Sumanta; Raikwar, Mayank; Mukhopadhyay, Debdeep; Chattopadhyay, Anupam; Lam, Kwok-Yan (2018): BLIC: A Blockchain Protocol for Manufacturing and Supply Chain Management of ICS. In: IEEE 2018 International Congress on Cybermatics ;. 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology : iThings/GreenCom/CPSCoM/SmartData/Blockchain/CIT 2018 : proceedings : Halifax, Canada, 30 July - 3 August 2018. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCoM) and IEEE Smart Data (SmartData). Halifax, NS, Canada, 7/30/2018 - 8/3/2018. IOT (Conference); IEEE/ACM International Conference on Green Computing and Communications; IEEE/ACM International Conference on Cyber, Physical, and Social Computing; IEEE International Conference on Smart Data; IEEE International Conference on Blockchain; IEEE International Conference on Computer and Information Technology. Los Alamitos, California, Washington, Tokyo: Conference Publishing Services, IEEE Computer Society, S. 1326–1335.

- Boucher, Philip; Nascimento, Susana; Kritikos, Mihalis (2017): Wie die Blockchain-Technologie unser Leben verändern könnte. Eingehende Analyse. Brüssel: EPRS. Online verfügbar unter [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA\(2017\)581948_DE.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_DE.pdf), zuletzt geprüft am 19.11.2019.
- Brainbot Labs Establishment (o. J.): Raiden Network. Online verfügbar unter <https://raiden.network/101.html>, zuletzt aktualisiert am 30.07.2019, zuletzt geprüft am 25.10.2019.
- Breuer, Wolfgang (2009): Definition: Venture-Capital. Gabler Wirtschaftslexikon. Online verfügbar unter <https://wirtschaftslexikon.gabler.de/definition/venture-capital-49706/version-272933>, zuletzt aktualisiert am 19.02.2019, zuletzt geprüft am 15.10.2019.
- Brown, Gendal Richard (2018): The Corda Platform: An Introduction. Online verfügbar unter <https://www.corda.net/content/corda-platform-whitepaper.pdf>, zuletzt geprüft am 05.11.2019.
- BSI – Bundesamt für Sicherheit in der Informationstechnik: Blockchain sicher gestalten. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf;jsessionid=55E433DCBA85CB54AC8944321CB1706B.1_cid341?__blob=publicationFile&v=5, zuletzt geprüft am 06.08.2019.
- BTC-ECHO GmbH (2019a): 5 Stable Coins, die Anleger kennen sollten. Online verfügbar unter <https://www.btc-echo.de/5-stable-coins-die-anleger-kennen-sollten/>, zuletzt geprüft am 05.11.2019.
- BTC-ECHO GmbH (2019b): Bitcoin Cash führt erfolgreich Hard Fork zu 32-MegaByte-Blöcken durch. Online verfügbar unter <https://www.btc-echo.de/bitcoin-cash-fuehrt-erfolgreich-hard-fork-zu-32-megabyte-bloecken-durch/>, zuletzt geprüft am 29.11.2019.
- BTC-ECHO GmbH (2019c): IOTA: „Chronicle“ soll das Tangle durchsuchbar machen | BTC-ECHO. Online verfügbar unter <https://www.btc-echo.de/iota-chronicle-soll-das-tangle-durchsuchbar-machen/>, zuletzt geprüft am 15.10.2019.
- Bundesamt für Sicherheit in der Informationstechnik (2018): BSI TR-03116-1, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116.pdf?__blob=publicationFile&v=3, zuletzt geprüft am 11.10.2019.
- Bundesamt für Sicherheit in der Informationstechnik (BSI) (2019): Blockchain sicher gestalten. Bonn. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=5, zuletzt geprüft am 11.10.2019.
- Bundesministerium für Wirtschaft (2016): Fortschreibung der Anwendungsszenarien der Plattform Industrie 4.0. Berlin. Online verfügbar unter <https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/fortschreibung-anwendungsszenarien.html>.
- Bundesministerium für Wirtschaft und Energie/Plattform Industrie 4.0 (2016): Ergebnispapier - Aspekte der Forschungsroadmap in den Anwendungsprozessen. Bundesministerium für Wirtschaft und Energie/Plattform Industrie 4.0. Berlin. Online verfügbar unter <https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/fortschreibung-anwendungsszenarien.html>, zuletzt geprüft am 29.10.2019.

- Buntinx, J. P. (2017): What is Delegated Byzantine Fault Tolerance? Soquel, USA. Online verfügbar unter <https://themerke.com/what-is-delegated-byzantine-fault-tolerance/>, zuletzt geprüft am 11.10.2019.
- Buterin, Vitalik: Bitcoin Multisig Wallet: The Future of Bitcoin (2014). Online verfügbar unter <https://bitcoinmagazine.com/articles/multisig-future-bitcoin-1394686504>.
- Buterin, Vitalik: Chain Interoperability. R3 Reports. Online verfügbar unter https://www.r3.com/wp-content/uploads/2017/06/chain_interoperability_r3.pdf, zuletzt geprüft am 05.11.2019.
- Buterin, Vitalik (2013): A Next-Generation Smart Contract and Decentralized Application Platform. Online verfügbar unter <https://github.com/ethereum/wiki/wiki/White-Paper>, zuletzt geprüft am 29.08.2019.
- Camp, L. J.; Sirbu, M.; Tygar, J. D. (1995): Token and notational money in electronic commerce. First USENIX Workshop on Electronic Commerce New York. New York. Online verfügbar unter https://www.usenix.org/legacy/publications/library/proceedings/ec95/full_papers/camp.txt, zuletzt aktualisiert am 25.02.2019, zuletzt geprüft am 06.08.2019.
- Carson, Brent; Romanelli, Giulio; Zhumaev, Askhat; Walsh, Patricia (2018): Blockchain beyond the hype: What is the strategic business value? McKinsey & Company. Online verfügbar unter <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value>, zuletzt geprüft am 27.08.2019.
- Casey, Michael; Vigna, Paul (2015): Cryptocurrency. Wie virtuelles Geld unsere Gesellschaft verändert. Berlin: Econ.
- Casino, Fran; Dasaklis, Thomas K.; Patsakis, Constantinos (2019): A systematic literature review of blockchain-based applications: Current status, classification and open issues. In: *Telematics and Informatics* 36, S. 55–81. DOI: 10.1016/j.tele.2018.11.006.
- Castor, Amy (2017): A (Short) Guide to Blockchain Consensus Protocols. Online verfügbar unter <http://www.webcitation.org/6wgfJxwXJ>, zuletzt aktualisiert am 17.10.2017, zuletzt geprüft am 29.11.2019.
- Castro, Miguel; Liskov, Barbara (2002): Practical byzantine fault tolerance and proactive recovery. In: *ACM Trans. Comput. Syst.* 20 (4), S. 398–461. DOI: 10.1145/571637.571640.
- Chaum, David (1984a): A New Paradigm for Individuals in the Information Age. In: Security and Privacy, 1984 IEEE Symposium on. 1984 IEEE Symposium on Security and Privacy. Oakland, CA, USA, 4/29/1984 - 5/2/1984. Place of publication not identified: publisher not identified, S. 99.
- Chaum, David (Hg.) (1984b): Advances in Cryptology. Proceedings of Crypto 83. Boston, MA: Springer US.
- Christidis, Konstantinos; Devetsikiotis, Michael (2016): Blockchains and Smart Contracts for the Internet of Things. In: *IEEE Access* 4, S. 2292–2303. DOI: 10.1109/ACCESS.2016.2566339.
- Churyumov, Anton (o. J.): Byteball A Decentralized System for Storage and Transfer of Value. Obyte. Online verfügbar unter <https://obyte.org/Byteball.pdf>, zuletzt geprüft am 19.11.2019.
- Coinbase (2019): Ethereum (ETH / EUR) Preisdiagramm. Online verfügbar unter <https://www.coinbase.com/price/ethereum/eur?locale=de>, zuletzt geprüft am 08.11.2019.

- CoinMarketCap (2019): Kryptowährung Marktkapitalisierungen |. Online verfügbar unter <https://coinmarketcap.com/de/>, zuletzt geprüft am 11.10.2019.
- Cullen, Andrew; Ferraro, Pietro; King, Christopher; Shorten, Robert (2019): Distributed Ledger Technology for IoT: Parasite Chain Attacks. Online verfügbar unter <https://arxiv.org/pdf/1904.00996>, zuletzt geprüft am 29.11.2019.
- Dai, Hong-Ning; Zheng, Zibin; Zhang, Yan (2019): Blockchain for Internet of Things: A Survey. In: *IEEE Internet Things J.* 6 (5), S. 8076–8094. DOI: 10.1109/JIOT.2019.2920987.
- Decker, Christian; Seidel, Jochen; Wattenhofer, Roger (2014): Bitcoin Meets Strong Consistency. Online verfügbar unter <http://arxiv.org/pdf/1412.7935v1>, zuletzt geprüft am 29.11.2019.
- Deloitte (2017): Blockchain to blockchains: Broad adoption and integration enter the realm of the possible. Online verfügbar unter <https://www2.deloitte.com/us/en/insights/focus/tech-trends/2018/blockchain-integration-smart-contracts.html>, zuletzt geprüft am 13.12.2019.
- DEXON Foundation (2019): DEXON. Online verfügbar unter <https://dexon.org/>.
- Diemer, Moritz (2019): Blockchain – Implications Blockchain - Implications and Use Cases for Additive Manufacturing. Frankfurt School Blockchain Center. Online verfügbar unter http://explore-ip.com/2019_Blockchain-Additive-Manufacturing.pdf, zuletzt geprüft am 19.11.2019.
- Digiconomist (Hg.) (2019): Bitcoin Energy Consumption Index. Online verfügbar unter <https://digiconomist.net/bitcoin-energy-consumption>, zuletzt aktualisiert am 23.04.2019.
- Dilley, Johnny; Poelstra, Andrew; Wilkins, Jonathan; Piekarska, Marta; Gorlick, Ben; Friedenbach, Mark: Strong Federations: An Interoperable Blockchain Solution to Centralized Third-Party Risks. Online verfügbar unter <http://arxiv.org/pdf/1612.05491v3>, zuletzt geprüft am 29.11.2019.
- Dinh, Thang N.; Thai, My T. (2018): AI and Blockchain: A Disruptive Integration. In: *Computer* 51 (9), S. 48–53. DOI: 10.1109/MC.2018.3620971.
- Dong, Mo; Liang, Qingkai; Li, Xiaozhou; Liu, Junda (2018): Celer Network: Bring Internet Scale to Every Blockchain. Online verfügbar unter <https://arxiv.org/pdf/1810.00037.pdf>, zuletzt geprüft am 25.10.2019.
- Dorri, Ali; Kanhere, Salil S.; Jurdak, Raja; Gauravaram, Praveen (2019): LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. In: *Journal of Parallel and Distributed Computing* 134, S. 180–197. DOI: 10.1016/j.jpdc.2019.08.005.
- Drescher, Daniel (2017): Blockchain Basics. Berkeley, CA: Apress.
- Drobetz, Wolfgang; Momtaz, Paul P.; Schröder, Henning (2019): Investor Sentiment and Initial Coin Offerings. In: *JAI* 21 (4), S. 41–55. DOI: 10.3905/jai.2019.1.069.
- Du, Wenyu; Pan, Shan L.; Leidner, Dorothy E.; Ying, Wenchi (2019): Affordances, experimentation and actualization of FinTech: A blockchain implementation study. In: *The Journal of Strategic Information Systems* 28 (1), S. 50–65. DOI: 10.1016/j.jsis.2018.10.002.
- Duffield, Evan; Diaz, Daniel (2018): Dash: A Payments-Focused Cryptocurrency. Online verfügbar unter <https://github.com/dashpay/dash/wiki/Whitepaper>, zuletzt geprüft am 25.10.2019.

- Dwork, Cynthia; Lynch, Nancy; Stockmeyer, Larry (1988): Consensus in the presence of partial synchrony. In: *J. ACM* 35 (2), S. 288–323. DOI: 10.1145/42282.42283.
- Ellis, Steve; Juels, Ari; Nazarov, Sergey (2017): ChainLink A Decentralized Oracle Network. Online verfügbar unter <https://link.smartcontract.com/whitepaper>.
- Energy Web Foundation (o. J.): The Grid's New Digital DNA. Zug, Schweiz. Online verfügbar unter <https://www.energyweb.org/>, zuletzt geprüft am 29.11.2019.
- Ethereum Community (2019): Welcome to the Ethereum Wiki! Ethereum Foundation. Zug (Schweiz). Online verfügbar unter <https://github.com/ethereum/wiki/wiki>, zuletzt geprüft am 11.10.2019.
- EU Blockchain Observatory and Forum (o. J.): Initiative map | EUBlockchain. Online verfügbar unter <https://www.eublockchainforum.eu/initiative-map>, zuletzt aktualisiert am 19.11.2019, zuletzt geprüft am 19.11.2019.
- European Telecommunications Standards Institute (ETSI) (2018): Terms of Reference (ToR) for ETSI ISG 'Permissioned Distributed Ledger' (ISG PDL).
- EVEN Foundation (2019a): Analysis of crosschain platforms. Online verfügbar unter <https://evenfound.org/blog/analysis-of-crosschain-platforms>, zuletzt geprüft am 05.11.2019.
- EVEN Foundation (2019b): EVEN — Cross-chain Interaction Network. Online verfügbar unter <https://evenfound.org/>, zuletzt geprüft am 05.11.2019.
- Falkon, Samuel (2017): The Story of the DAO — Its History and Consequences. Medium. Online verfügbar unter <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee>, zuletzt aktualisiert am 22.04.2020, zuletzt geprüft am 22.04.2020.
- Firdaus, Ahmad; Razak, Mohd Faizal Ab; Feizollah, Ali; Hashem, Ibrahim Abaker Targio; Hazim, Mohamad; Anuar, Nor Badrul (2019): The rise of "blockchain": bibliometric analysis of blockchain study. In: *Scientometrics* 120 (3), S. 1289–1331. DOI: 10.1007/s11192-019-03170-4.
- Fischer, Michael J.; Lynch, Nancy A.; Paterson, Michael S. (1985): Impossibility of distributed consensus with one faulty process. In: *J. ACM* 32 (2), S. 374–382. DOI: 10.1145/3149.214121.
- Florian Tschorsch and Björn Scheuermann: Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. Online verfügbar unter <https://eprint.iacr.org/2015/464.pdf>, zuletzt geprüft am 13.08.2019.
- Foamspace Corp (2019): FOAM. Online verfügbar unter <https://foam.space/>, zuletzt aktualisiert am 29.09.2019, zuletzt geprüft am 12.11.2019.
- Fokusgruppe 5G (2015): 5G – Schlüsseltechnologie für die vernetzte Gesellschaft. Nationaler IT Gipfel Berlin 2015.
- Fraunhofer FIT: Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale. Online verfügbar unter https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf, zuletzt geprüft am 13.08.2019.
- Fraunhofer-Institut für Sichere Informationstechnologie (o. J.): Fraunhofer SIT. Online verfügbar unter <https://www.sit.fraunhofer.de/de/>, zuletzt geprüft am 05.11.2019.

- Fridgen, Gilbert; Guggenberger, Nikolas; Hoeren, Thomas; Prinz, Wolfgang; Urbach, Nils; Baur, Johannes et al. (2019): Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik. Hg. v. Bundesministerium für Verkehr und digitale Infrastruktur. Fraunhofer-Institut für Angewandte Informationstechnik FIT, zuletzt geprüft am 12.09.2019.
- Fridgen, Gilbert; Guggenmoos, Florian; Lockl, Jannik; Rieger, Alexander; Schweizer, Andre (2018a): Developing an Evaluation Framework for Blockchain in the Public Sector: The Example of the German Asylum Process. In: 2510-2591. Online verfügbar unter https://dl.eusset.eu/bitstream/20.500.12015/3157/1/blockchain2018_10.pdf, zuletzt geprüft am 29.11.2019.
- Fridgen, Gilbert; Lockl, Jannik; Radszuwill, Sven; Rieger, Alexander; Schweizer, André; Urbach, Nils (2018b): A Solution in Search of a Problem: A Method for the Development of Blockchain Use Cases. In: *AMCIS*. Online verfügbar unter <https://pdfs.semanticscholar.org/dec6/5673be121bb4d2818a2c9e74118ae45005ff.pdf>, zuletzt geprüft am 29.11.2019.
- Frost & Sullivan (2019): Global Mega Trends to 2030. Futurecasting Key Themes that will Shape Our Future Lives. Online verfügbar unter <https://store.frost.com/global-mega-trends-to-2030.html>, zuletzt geprüft am 19.11.2019.
- G7 Working Group on Stablecoins (2019): Investigating the impact of global stablecoins. Online verfügbar unter <https://www.bis.org/cpmi/publ/d187.pdf>, zuletzt geprüft am 25.10.2019.
- Gassmann, Oliver; Schmück, Kilian (2019): DLT/Blockchainbasierte Geschäftsmodelle. In: Oliver Gassmann und Philipp Sutter (Hg.): *Digitale Transformation gestalten. Geschäftsmodelle, Erfolgsfaktoren, Checklisten*. 2., überarbeitete und erweiterte Auflage, 61ff.
- Gassmann, Oliver; Sutter, Philipp (Hg.) (2019): *Digitale Transformation gestalten. Geschäftsmodelle, Erfolgsfaktoren, Checklisten*. 2., überarbeitete und erweiterte Auflage.
- Gatteschi, Valentina; Lamberti, Fabrizio; Demartini, Claudio; Pranteda, Chiara; Santamaria, Victor (2018): To Blockchain or Not to Blockchain: That Is the Question. In: *IT Prof.* 20 (2), S. 62–74. DOI: 10.1109/MITP.2018.021921652.
- Gavin Wood (2018): Polkadot: Vision for a heterogeneous Multi-chain Framework. Online verfügbar unter <https://polkadot.network/PolkaDotPaper.pdf>.
- Gehrke, Lars; Kühn, Arno T.; Rule, David; Moore, Paul; Bellmann, Christoph; Siemes, Sebastian et al. (2015): Industry 4.0 A Discussion of Qualifications and Skills in the Factory of the Future. VDI; ASME. Online verfügbar unter <https://pdfs.semanticscholar.org/e141/17c9f1b01b46d09afdb7d37c009098745b0d.pdf>, zuletzt geprüft am 08.11.2019.
- Genkin, Daniel; Papadopoulos, Dimitrios; Papamanthou, Charalampos (2018): Privacy in decentralized cryptocurrencies. In: *Commun. ACM* 61 (6), S. 78–88. DOI: 10.1145/3132696.
- Gentemann, Lukas (2019): Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen. Studienbericht 2019. Bitkom e.V. Online verfügbar unter https://www.bitkom.org/sites/default/files/2019-04/190410_bitkom_studie_blockchain_2019.pdf, zuletzt geprüft am 12.11.2019.
- Geschka, Horst; Schaufele, Jochen; Zimmer, Claudia (2017): Explorative Technologie-Roadmaps – Eine Methodik zur Erkundung technologischer Entwicklungslinien und Potenziale. In: Martin

- G. Möhrle und Ralf Isenmann (Hg.): Technologie-Roadmapping, Bd. 40. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 83–102.
- Glaser, Florian: Hawaii International Conference on System Sciences 2017 (HICSS-50). Hilton Waikoloa Village, Hawaii, January 4-7, 2017. Online verfügbar unter <http://aisel.aisnet.org/hicss-50/>.
- Gnosis Ltd. (2017): Gnosis Whitepaper. Online verfügbar unter <https://gnosis.io/pdf/gnosis-whitepaper.pdf>, zuletzt geprüft am 29.11.2019.
- Goodkind, Andrew L.; Jones, Benjamin A.; Berrens, Robert P. (2020): Cryptodamages: Monetary value estimates of the air pollution and human health impacts of cryptocurrency mining. In: *Energy Research & Social Science* 59, S. 101281. DOI: 10.1016/j.erss.2019.101281.
- Goyal, Swati (2018): Blockchain Interoperability - The Importance of Cross Chain Technology. 101Blockchains. Online verfügbar unter <https://101blockchains.com/blockchain-interoperability/>, zuletzt geprüft am 05.11.2019.
- Graham, W. (2018): Building it Better: A Simple Guide to Blockchain Use Cases. Online verfügbar unter <https://medium.com/blockchain-at-berkeley/building-it-better-a-simple-guide-to-blockchain-use-cases-de494a8f5b60>, zuletzt geprüft am 13.12.2019.
- Greenspan, Gideon (2015a): Avoiding the pointless blockchain project. Coin Sciences Ltd. Online verfügbar unter <https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/>, zuletzt geprüft am 21.05.2019.
- Greenspan, Gideon (2015b): Private blockchains are more than “just” shared databases | MultiChain. Online verfügbar unter <https://www.multichain.com/blog/2015/10/private-blockchains-shared-databases/>, zuletzt geprüft am 21.05.2019.
- Greenspan, Gideon (2019): Ten Enterprise Blockchains. That Actually Work. | MultiChain. MultiChain. Online verfügbar unter <https://www.multichain.com/blog/2019/06/ten-enterprise-blockchains/>, zuletzt geprüft am 12.11.2019.
- Gross, Andrew; Barinov, Igor (o. J.): Welcome to POA. Online verfügbar unter <https://www.poa.network/>, zuletzt aktualisiert am 26.11.2019, zuletzt geprüft am 26.11.2019.
- Grover, Purva; Kar, Arpan Kumar; Vigneswara Ilavarasan, P. (2018): Blockchain for Businesses: A Systematic Literature Review. In: Salah A. Al-Sharhan, Antonis C. Simintiras, Yogesh K. Dwivedi, Marijn Janssen, Matti Mäntymäki, Luay Tahat et al. (Hg.): Challenges and Opportunities in the Digital Era. 17th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2018, Kuwait City, Kuwait, October 30 - November 1, 2018, Proceedings, Bd. 11195. Cham: Springer International Publishing (Theoretical Computer Science and General Issues, 11195), S. 325–336.
- Hadedy, Mohamed El; Gligoroski, Danilo; Knapskog, Svein J.; Margala, Martin (2010): Compact Implementation of BLUE MIDNIGHT WISH-256 Hash Function on Xilinx FPGA Platform. In: *IAS 2010*. Online verfügbar unter <https://pdfs.semanticscholar.org/a202/4b7bede04a273390a4c55a2baa8de11a9715.pdf>.
- Hahn, Christopher; Wons, Adrian (2018): Initial Coin Offering (ICO). Unternehmensfinanzierung auf Basis der Blockchain-Technologie. Wiesbaden: Springer Gabler (essentials).

- Hammerschmidt, Chris (2017): Consensus in Blockchain Systems. In Short. Medium. San Francisco, USA. Online verfügbar unter <https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe>, zuletzt geprüft am 11.10.2019.
- Handelsblatt Media Group GmbH & Co. KG (2017): Long Island Iced Tea: 500 Prozent plus durch Namensänderung in Long Blockchain. Online verfügbar unter <https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/long-island-iced-tea-500-prozent-plus-durch-namensaenderung-in-long-blockchain/20767496.html?ticket=ST-50132702-fjRhWGVUB1hab1tZVtHK-ap6>, zuletzt geprüft am 29.10.2019.
- Harris-Braun, Eric; Luck, Nicolas; Brock, Arthur (2018): Holochain. scalable agent-centric distributed computing.
- Hays, Demelza (2019): Blockchain 3.0 – Die Zukunft der DLT? Crypto Research Report. Online verfügbar unter <https://cryptoresearch.report/crypto-research/blockchain-3-0-die-zukunft-der-dlt/?lang=de>, zuletzt geprüft am 25.10.2019.
- Hebert, Cédric; Di Cerbo, Francesco (2019): Secure blockchain in the enterprise: A methodology. In: *Pervasive and Mobile Computing* 59, S. 101038. DOI: 10.1016/j.pmcj.2019.101038.
- Hedera Hashgraph (2018): Formal Methods: The Importance of Being ABFT in a World with Bad Actors |. Online verfügbar unter <https://www.hedera.com/blog/formal-methods-the-importance-of-being-abft-in-a-world-with-bad-actors>, zuletzt geprüft am 11.10.2019.
- Heinze, Nico (2019): Was kommt nach der Blockchain? Teil 3: Einführung in Hashgraph. iteratec GmbH. Online verfügbar unter <https://www.iteratec.de/tech-blog/artikel/was-kommt-nach-der-blockchain-teil-3-einfuehrung-in-hashgraph/>, zuletzt geprüft am 12.11.2019.
- Henke, Michael; Schulte, Axel T.; Jakob, Sabine (2015): Blockchain-basiertes Supply Chain Management. In: Birgit Vogel-Heuser, Thomas Bauernhansl und Michael ten Hompel (Hg.): Handbuch Industrie 4.0. Produktion, Automatisierung und Logistik. Wiesbaden: Springer Fachmedien Wiesbaden (Springer NachschlageWissen), S. 1–17.
- Herweijer, Celine; Waughray, Dominic; Warren, Sheila (Hg.) (2018): Building block(chain)s for a better planet. PwC. Online verfügbar unter <https://www.pwc.com/gx/en/sustainability/assets/blockchain-for-a-better-planet.pdf>, zuletzt geprüft am 19.11.2019.
- <https://www.facebook.com/bitcoinecho>: Was ist ein STO (Security Token Offering)? | BTC-ECHO. Online verfügbar unter <https://www.btc-echo.de/tutorial/security-token-offering-definition-was-sind-stos/>, zuletzt geprüft am 27.08.2019.
- Hughes, Laurie; Dwivedi, Yogesh K.; Misra, Santosh K.; Rana, Nripendra P.; Raghavan, Vishnupriya; Akella, Viswanadh (2019): Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. In: *International Journal of Information Management* 49, S. 114–129. DOI: 10.1016/j.ijinfomgt.2019.02.005.
- Hyperledger (2019a): A Blockchain Platform for the Enterprise. Online verfügbar unter <https://hyperledger-fabric.readthedocs.io/en/latest/blockchain.html>.
- Hyperledger (2019b): A Blockchain Platform for the Enterprise — hyperledger-fabricdocs master documentation. Online verfügbar unter <https://hyperledger-fabric.readthedocs.io/en/release-1.4/>, zuletzt aktualisiert am 28.10.2019, zuletzt geprüft am 29.10.2019.

- IEEE COMMUNICATIONS SOCIETY (2019): Blockchain and AI for Beyond 5G Networks | IEEE Communications Society. Online verfügbar unter <https://www.comsoc.org/publications/magazines/ieee-network/cfp/blockchain-and-ai-beyond-5g-networks>, zuletzt aktualisiert am 28.10.2019, zuletzt geprüft am 29.10.2019.
- Ikeda, Kazuki (2017): qBitcoin: A Peer-to-Peer Quantum Cash System. Online verfügbar unter <http://arxiv.org/pdf/1708.04955v2>.
- Institute of Electrical and Electronics Engineers (2019): Standards - IEEE Blockchain Initiative. Online verfügbar unter <https://blockchain.ieee.org/standards>, zuletzt geprüft am 08.11.2019.
- International Organization for Standardization (2016): ISO/TC 307 - Blockchain and distributed ledger technologies. Online verfügbar unter <https://www.iso.org/committee/6266604.html>, zuletzt geprüft am 08.11.2019.
- Internet Research Task Force (2018): blockchain-federation – IRTF Wiki. Online verfügbar unter <https://trac.ietf.org/trac/irtf/wiki/blockchain-federation>, zuletzt geprüft am 08.11.2019.
- IOTA Foundation (2019): Academic Papers. Research undertaken on topics related to The Tangle and IOTA related technologies. Online verfügbar unter <https://www.iota.org/research/academic-papers>, zuletzt geprüft am 15.10.2019.
- Jae Kwon, Ethan Buchman: Cosmos. Online verfügbar unter <https://cosmos.network/cosmos-whitepaper.pdf>.
- Janssen, Marijn; Weerakkody, Vishanth; Ismagilova, Elvira; Sivarajah, Uthayasankar; Irani, Zahir (2020): A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. In: *International Journal of Information Management* 50, S. 302–309. Online verfügbar unter <https://doi.org/10.1016/j.ijinfomgt.2019.08.012>, zuletzt geprüft am 29.11.2019.
- Jin, Hai; Dai, Xiaohai; Xiao, Jiang (2018): Towards a Novel Architecture for Enabling Interoperability amongst Multiple Blockchains. In: 2018 IEEE 38th International Conference on Distributed Computing Systems. ICDCS 2018 : 2-5 July 2018, Vienna, Austria : proceedings. 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). Vienna, 7/2/2018 - 7/6/2018. IEEE International Conference on Distributed Computing Systems; Institute of Electrical and Electronics Engineers; ICDCS; International Workshop on Scalable Network Traffic Analytics; SNTA; Workshop on QoE-Based Analysis and Management of Data Communication Networks; Internet-QoE. Piscataway, NJ: IEEE, S. 1203–1211.
- Juniper Research Ltd (2018): IoT Connections to Grow 140% to Hit 50 Billion By 2022. Hampshire. Online verfügbar unter <https://www.juniperresearch.com/press/press-releases/iot-connections-to-grow-140pc-to-50-billion-2022>, zuletzt geprüft am 29.10.2019.
- Kannengiesser, Niclas; Lins, Sebastian; Dehling, Tobias; Sunyaev, Ali: What Does Not Fit Can be Made to Fit! Trade-Offs in Distributed Ledger Technology Designs.
- Keller, Stephen C. (2018): Hashgraph VS Blockchain. The Future of Cryptocurrency. Wrocław: Amazon Fulfillment Poland Sp. z o.o.
- Kerschbaum, Florian (o. J.): Privacy-Preserving Computation (Position Paper). SAP Research. Karlsruhe, Germany. Online verfügbar unter <http://www.fkerschbaum.org/apf12.pdf>, zuletzt geprüft am 19.11.2019.

- Keuper, Ralf (2018): Sicheres Identitäts- und Rechtemanagement mit ID-Chains – Interview mit Dr. Andreas Wilke (Bundesdruckerei GmbH). Online verfügbar unter <https://bankstil.de/sicheres-identitaets-und-rechtemanagement-mit-id-chains-interview-mit-dr-andreas-wilke-bundesdruckerei-gmbh>, zuletzt geprüft am 05.11.2019.
- Kiktenko, E. O.; Pozhar, N. O.; Anufriev, M. N.; Trushechkin, A. S.; Yunusov, R. R.; Kurochkin, Y. V. et al. (2018): Quantum-secured blockchain. In: *Quantum Sci. Technol.* 3 (3), S. 35004. DOI: 10.1088/2058-9565/aabc6b.
- Klein, Sandra; Prinz, Wolfgang; Gräther, Wolfgang (2018): A Use Case Identification Framework and Use Case Canvas for identifying and exploring relevant Blockchain opportunities. In: *European Society for Socially Embedded Technologies (EUSSET)*. DOI: 10.18420/BLOCKCHAIN2018_02.
- Kleinfurter, Friederike; Vengadasalam, Sandra; Lawton, James (2020): bloxberg The Trusted Research Infrastructure. Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V. Online verfügbar unter https://bloxberg.org/wp-content/uploads/2020/02/bloxberg_whitepaper_1.1.pdf.
- Koens, T.; Poll, E. (2019): Assessing interoperability solutions for distributed ledgers. In: *Pervasive and Mobile Computing* 59, S. 101079. DOI: 10.1016/j.pmcj.2019.101079.
- Kokoris-Kogias, Eleftherios; Jovanovic, Philipp; Gasser, Linus; Gailly, Nicolas; Syta, Ewa; Ford, Bryan (2018): OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding. In: 2018 IEEE Symposium on Security and Privacy. SP 2018 : 21-23 May 2018, San Francisco, California, USA : proceedings. 2018 IEEE Symposium on Security and Privacy (SP). San Francisco, CA, 5/20/2018 - 5/24/2018. IEEE Symposium on Security and Privacy; Institute of Electrical and Electronics Engineers; IEEE Computer Society; International Association for Cryptologic Research; SP; S & P. Piscataway, NJ: IEEE, S. 583–598.
- Kreutzer, Michael; Niederhagen, Ruben; Waidner, Michael (2018): EBERBACHER GESPRÄCH ON »NEXT GENERATION CRYPTO«. Ebersbacher Gespräche. FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGY.
- Kroll, Joshua A.; Davey, Ian C.; Felten, Edward W. (2013): The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. Online verfügbar unter <https://pdfs.semanticscholar.org/c55a/6c95b869938b817ed3fe3ea482bc65a7206b.pdf>, zuletzt geprüft am 29.11.2019.
- L., Raphael (2019): Brisante IOTA News im Interview mit Dominik Schiener - erste praktische Usecases 2020? - Kryptoszene.de. Kryptoszene.de. Online verfügbar unter <https://kryptoszene.de/brisante-iota-news-im-interview-mit-dominik-schiener-erste-praktische-usecases-2020/>, zuletzt geprüft am 19.11.2019.
- Lamport, Leslie; Shostak, Robert; Pease, Marshall (1982): The Byzantine Generals Problem. In: *ACM Trans. Program. Lang. Syst.* 4 (3), S. 382–401. DOI: 10.1145/357172.357176.
- Le Sève, Miriam Denis; Mason, Nathaniel; Nassiry, Darius (2018): Delivering blockchain's potential for environmental sustainability. ODI. Online verfügbar unter <https://www.odi.org/sites/odi.org.uk/files/resource-documents/12439.pdf>, zuletzt geprüft am 19.11.2019.
- Lerner, Sergio Demian (2015): RSK White Paper Overview. RSK Labs. Online verfügbar unter https://docs.rsk.co/RSK_White_Paper-Overview.pdf, zuletzt geprüft am 26.11.2019.

- Li, Songze; Yu, Mingchao; Yang, Chien-Sheng; Avestimehr, A. Salman; Kannan, Sreeram; Viswanath, Pramod (2018): PolyShard: Coded Sharding Achieves Linearly Scaling Efficiency and Security Simultaneously. Online verfügbar unter <https://arxiv.org/pdf/1809.10361>.
- Libra Association (2019): Einführung in Libra. Online verfügbar unter <https://libra.org/de-DE/white-paper/>, zuletzt geprüft am 18.09.2019.
- Lin, I.-C; Liao, T.-C (2017): A survey of blockchain security issues and challenges. In: *International Journal of Network Security* 19, S. 653–659. DOI: 10.6633/IJNS.201709.19(5).01.
- Loom Network (2019): What is Loom Network. Online verfügbar unter <https://loomx.io/developers/docs/en/intro-loom-sdk.html>, zuletzt aktualisiert am 11.04.2019, zuletzt geprüft am 26.11.2019.
- Lu, Yang (2018): Blockchain and the related issues: a review of current research topics. In: *Journal of Management Analytics* 5 (4), S. 231–255. DOI: 10.1080/23270012.2018.1516523.
- Lumb, Richard; Treat, David; Jelf, Owen (2016): Why distributed ledger technology must adapt to an imperfect world. Accenture. Online verfügbar unter https://www.accenture.com/_acnmedia/pdf-33/accenture-editing-uneditable-blockchain.pdf, zuletzt geprüft am 29.10.2019.
- Luongo, Matt; Pon, Corbin (2019): The Keep Network: A Privacy Layer for Public Blockchains. Online verfügbar unter <https://backend.keep.network/whitepaper>, zuletzt geprüft am 29.10.2019.
- Luu, Loi; Chu, Duc-Hiep; Olickel, Hrishikesh; Saxena, Prateek; Hobor, Aquinas (2016a): Making Smart Contracts Smarter. In: Stefan Katzenbeisser und Edgar Weippl (Hg.): Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. CCS'16 ; Oktober 24–28, 2016, Vienna, Austria. the 2016 ACM SIGSAC Conference. Vienna, Austria, 10/24/2016 - 10/28/2016. Association for Computing Machinery; ACM Conference on Computer and Communications Security; CCS. New York, NY: Association for Computing Machinery, S. 254–269.
- Luu, Loi; Narayanan, Viswesh; Zheng, Chaodong; Baweja, Kunal; Gilbert, Seth; Saxena, Prateek (2016b): A Secure Sharding Protocol For Open Blockchains. In: Stefan Katzenbeisser und Edgar Weippl (Hg.): Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. CCS'16 ; Oktober 24–28, 2016, Vienna, Austria. the 2016 ACM SIGSAC Conference. Vienna, Austria, 10/24/2016 - 10/28/2016. Association for Computing Machinery; ACM Conference on Computer and Communications Security; CCS. New York, NY: Association for Computing Machinery, S. 17–30.
- Madsen, Paul (2018): Hedera Technical Insights: Code is law, but what if the law needs to change? Hedera Hashgraph, LLC.
- Manning, Jim (2016): Proof-of-Work Vs. Proof-of-Stake Explained. ETHNews. Los Angeles. Online verfügbar unter <https://www.webcitation.org/6wpR55B4M>, zuletzt geprüft am 11.10.2019.
- Manyika, James; Chui, Michael (2015): By 2025, Internet of things applications could have \$11 trillion impact. McKinsey & Company. Online verfügbar unter <https://www.mckinsey.com/mgi/overview/in-the-news/by-2025-internet-of-things-applications-could-have-11-trillion-impact>, zuletzt geprüft am 12.11.2019.
- Masanet, Eric; Shehabi, Arman; Lei, Nuoa; Vranken, Harald; Koomey, Jonathan; Malmodin, Jens (2019): Implausible projections overestimate near-term Bitcoin CO2 emissions. Lawrence

- Berkeley National Laboratory. Online verfügbar unter <https://eta.lbl.gov/publications/implausible-projections-overestimate>.
- Mattila, Juri (2016): The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures. UNIVERSITY OF CALIFORNIA, BERKELEY. Online verfügbar unter https://www.researchgate.net/publication/313477689_The_Blockchain_Phenomenon_-_The_Disruptive_Potential_of_Distributed_Consensus_Architectures.
- Mearian, Lucas (2019): Sharding: What it is and why many blockchain protocols rely on it. IDG Communications, Inc. Online verfügbar unter <https://www.computerworld.com/article/3336187/sharding-what-it-is-and-why-so-many-blockchain-protocols-rely-on-it.html>, zuletzt aktualisiert am 28.01.2019, zuletzt geprüft am 08.11.2019.
- Meinel, Christoph; Gayvoronskaya, Tatiana; Schnjakin, Maxim (2018): Blockchain. Hype or innovation. Potsdam: Universitätsverlag Potsdam (Technische Berichte des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, Nr. 124). Online verfügbar unter <http://nbn-resolving.de/urn:nbn:de:kobv:517-opus4-414525>.
- Merkle, Ralph C. (1988): A Digital Signature Based on a Conventional Encryption Function. In: Carl Pomerance (Hg.): Advances in cryptology - CRYPTO '87. Proceedings, Bd. 293. Berlin: Springer (Advances in cryptology, 7.1987), S. 369–378.
- Merkle, Ralph C. (1990): One Way Hash Functions and DES. In: Gilles Brassard (Hg.): Advances in cryptology - CRYPTO '89. Proceedings, Bd. 435. New York: Springer (Lecture Notes in Computer Science, 435), S. 428–446.
- Meunier, S. (2018): When do you need blockchain? Decision models. Online verfügbar unter <https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1>, zuletzt geprüft am 13.12.2019.
- Miers, I.; Garman, C.; Green, M.; Rubin, A. D. (2013): Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In: 2013 IEEE Symposium on Security and Privacy (SP). 19 - 22 May 2013, San Francisco, California, USA. 2013 IEEE Symposium on Security and Privacy (SP) Conference. Berkeley, CA: IEEE, S. 397–411.
- MimbleWimbleCoin Whitepaper. Online verfügbar unter <https://github.com/mwcp/whitepaper/blob/master/whitepaper.pdf>, zuletzt geprüft am 31.12.2019.
- Mingxiao, Du; Xiaofeng, Ma; Zhe, Zhang; Xiangwei, Wang; Qijun, Chen (2017): A review on consensus algorithm of blockchain. In: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC). Banff Center, Banff, Canada, October 5-8, 2017. 2017 IEEE International Conference on Systems, Man and Cybernetics (SMC). Banff, AB, 10/5/2017 - 10/8/2017. IEEE International Conference on Systems, Man, and Cybernetics; Institute of Electrical and Electronics Engineers; IEEE Systems, Man, and Cybernetics Society; SMC. Piscataway, NJ: IEEE, S. 2567–2572.
- Momtaz, Paul P. (2018): Token Sales and Initial Coin Offerings: Introduction, 14.11.2018.
- Momtaz, Paul P.; Rennertseder, Kathrin; Schröder, Henning (2019): Token Offerings: A Revolution in Corporate Finance? In: *SSRN Journal*. DOI: 10.2139/ssrn.3346964.

- Mora, Camilo; Rollins, Randi L.; Taladay, Katie; Kantar, Michael B.; Chock, Mason K.; Shimada, Mio; Franklin, Erik C. (2019): Publisher Correction: Bitcoin emissions alone could push global warming above 2 °C. In: *Nature Clim Change* 9 (1), S. 80. DOI: 10.1038/s41558-018-0353-0.
- Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. Online verfügbar unter <https://bitcoin.org/bitcoin.pdf>, zuletzt geprüft am 06.06.2019.
- Nano (2019): Nano. Online verfügbar unter <https://nano.org/en>.
- Narayanan, Arvind; Clark, Jeremy (2017): Bitcoin's academic pedigree. In: *Commun. ACM* 60 (12), S. 36–45. DOI: 10.1145/3132259.
- NEAR (2019): The NEAR Whitepaper. Online verfügbar unter <https://near.org/papers/the-official-near-white-paper/>, zuletzt geprüft am 31.12.2019.
- NExT e.V. in Zusammenarbeit mit der Initiative "Blockchain in der Verwaltung Deutschland" (BiVD) und der Community of Practice Blockchain des NExT-Expertennetzwerks (2019): BLOCKCHAIN IN DER VERWALTUNG. ANWENDUNGSBEREICHE UND HERAUSFORDERUNGEN.
- Niemann, Christoph (2017): Orakel-Dienste speisen externe Informationen in die Blockchain. In: *JavaSpektrum*, S. 14–17. Online verfügbar unter https://www.maibornwolff.de/sites/default/files/news/files/javaspektrum_orakeldienste_blockchain_drchristophniemann.pdf, zuletzt geprüft am 08.11.2019.
- Nikolaev, Ilia (2019): Ethereum Dezentralität in Gefahr? - Blockgröße heimlich um 25% erhöht. Cryptomonday. Online verfügbar unter <https://cryptomonday.de/ethereum-dezentralitaet-in-gefahr-blockgroesse-heimlich-um-25-erhoeht/>, zuletzt geprüft am 25.10.2019.
- NIST (Hg.) (2017): SHA-3 Project - Hash Functions | CSRC. Online verfügbar unter <https://csrc.nist.gov/projects/hash-functions/sha-3-project>, zuletzt geprüft am 30.07.2019.
- Nofer, Michael; Gomber, Peter; Hinz, Oliver; Schiereck, Dirk (2017): Blockchain. In: *Bus Inf Syst Eng* 59 (3), S. 183–187. DOI: 10.1007/s12599-017-0467-3.
- Nomura Research Institute (2016): Survey on Blockchain Technologies and Related Services. Online verfügbar unter https://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf, zuletzt geprüft am 17.09.2019.
- o. A. (o. J.): ICO Watch List - Best ICO & Token Crowdsales List For Token Buyers. Hg. v. icowatchlist.com. Online verfügbar unter <https://icowatchlist.com>, zuletzt geprüft am 15.10.2019.
- O'Neal, Stephen (2019): Können Kryptobörsen jemals vollständig dezentralisiert sein? Cointelegraph. Online verfügbar unter <https://de.cointelegraph.com/news/can-crypto-exchanges-ever-be-truly-decentralized>, zuletzt geprüft am 25.10.2019.
- Osterwalder, Alexander; Pigneur, Yves (2010): Business model generation. A handbook for visionaries, game changers, and challengers. Hoboken, NJ: Wiley. Online verfügbar unter <http://proquest.safaribooksonline.com/9780470876411>.
- Otto, Boris; Jürjens, Jan; Schon, Jochen; Auer, Sören; Menz, Nadja; Wenzel, Sven; Cirullies, Jan (2016): Industrial Data Space - Digitale Souveränität über Daten. Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. München. Online verfügbar unter https://www.fraunhofer.de/content/dam/zv/de/Forschungsfelder/industrial-data-space/Industrial-Data-Space_whitepaper.pdf, zuletzt geprüft am 19.11.2019.

- Panetta, Kasey (2019): 5 Trends Appear on the Gartner Hype Cycle for Emerging Technologies, 2019. Gartner, Inc. Online verfügbar unter <https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019/>, zuletzt geprüft am 29.10.2019.
- Peck, M. (2017): Do You Need a Blockchain? Online verfügbar unter <https://spectrum.ieee.org/computing/net-works/do-you-need-a-blockchain>, zuletzt geprüft am 13.12.2019.
- Perard, Doriane; Lacan, Jérôme; Bachy, Yann; Detchart, Jonathan (2018): Erasure code-based low storage blockchain node. Online verfügbar unter <http://arxiv.org/pdf/1805.00860v1>.
- Perera, Srinath; Leymann, Frank; Fremantle, Paul (2019): A use case centric survey of Blockchain: status quo and future directions.
- Peters, Gareth W.; Panayi, Efstathios (2015): Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. In: *undefined*. Online verfügbar unter <https://arxiv.org/pdf/1511.05740.pdf>, zuletzt geprüft am 29.11.2019.
- Peterson, Jack; Krug, Joseph; Zoltu, Micah; Williams, Austin K.; Alexander, Stephanie (2018): Augur: a Decentralized Oracle and Prediction Market Platform. Online verfügbar unter <https://www.augur.net/whitepaper.pdf>, zuletzt geprüft am 29.11.2019.
- Peyrin, Thomas; Galbraith, Steven; Boneh, Dan; Drijvers, Manu; Neven, Gregory (Hg.) (2018): Compact Multi-signatures for Smaller Blockchains. Advances in Cryptology – ASIACRYPT 2018. Cham: Springer International Publishing. Online verfügbar unter <https://eprint.iacr.org/2018/483.pdf>.
- Pisa, M. (2018): Reassessing Expectations for Blockchain and Development. Online verfügbar unter <https://www.cgdev.org/publication/reassessing-expectations-blockchain-and-development-cost-complexity>, zuletzt geprüft am 13.12.2019.
- Polyzos, George C.; Fotiou, Nikos (2017): Blockchain-Assisted Information Distribution for the Internet of Things. In: Chengcui Zhang (Hg.): 2017 IEEE International Conference on Information Reuse and Integration. IRI 2017 : San Diego, CA, USA, 4-6 August 2017 : proceedings. 2017 IEEE International Conference on Information Reuse and Integration (IRI). San Diego, CA: IEEE, S. 75–78. Online verfügbar unter <https://ieeexplore.ieee.org/ielx7/8100855/8102895/08102921.pdf?tp=&arnumber=8102921&isnumber=8102895&ref=aHR0cHM6Ly9pZWVleHBsb3JlLmlZlZWUub3JnL2Fic3RyYWNOL2RvY3VtZW50LzgxMDI5MjE=>, zuletzt geprüft am 27.08.2019.
- Poon, Joseph; Dryja, Thaddeus (2016): The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Online verfügbar unter <https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf>, zuletzt geprüft am 25.10.2019.
- Popov, Serguei (2018): The Tangle. Online verfügbar unter https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvslqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf, zuletzt geprüft am 15.10.2019.
- Pournader, Mehrdokht; Shi, Yangyan; Seuring, Stefan; Koh, S. LennyC. (2019): Blockchain applications in supply chains, transport and logistics: a systematic review of the literature. In: *International Journal of Production Research* 2 (1), S. 1–19. DOI: 10.1080/00207543.2019.1650976.

- Presse- und Informationsamt der Bundesregierung (2019): Blockchain-Strategie. Online verfügbar unter <https://www.bundesregierung.de/breg-de/themen/digital-made-in-de/blockchain-strategie-1546662>, zuletzt geprüft am 25.10.2019.
- Prinz (2019): Die Idee hinter Libra ist wichtig für Deutschland. In: *Frankfurter Allgemeine*, 10.12.2019 (10.12.2019). Online verfügbar unter <https://www.faz.net/aktuell/finanzen/facebook-plant-eine-weltumspannende-digitale-waehrung-16522969.html>, zuletzt geprüft am 13.12.2019.
- Prinz, Eduard (2018): Unterschied Bitcoin, Multichain und Ethereum. BITFANTASTIC. Online verfügbar unter <https://www.bitfantastic.com/unterschied-bitcoin-multichain-und-ethereum/#Multichain>, zuletzt geprüft am 12.11.2019.
- Provable Things Limited (o. J.): oraclize A Scalable Architecture for On-Demand,. Online verfügbar unter https://provable.xyz/papers/random_datasource-rev1.pdf.
- Prusty, Narayan (2017): Building blockchain projects. Building decentralized blockchain applications with Ethereum and Solidity. Birmingham, Mumbai: Packt.
- Quant Network (o.J.): Overledger - Quant Network. Online verfügbar unter <https://www.quant.network/technology/overledger/>, zuletzt geprüft am 08.11.2019.
- Raikwar, Mayank; Gligoroski, Danilo; Kravlevska, Katina (2019): SoK of Used Cryptography in Blockchain. Online verfügbar unter <http://arxiv.org/pdf/1906.08609v3>.
- Rajan, Del; Visser, Matt (2019): Quantum Blockchain Using Entanglement in Time. In: *Quantum Reports* 1 (1), S. 3–11. DOI: 10.3390/quantum1010002.
- Rajasingham, Dilan (2017): Welcome to the machine-to-machine economy. Opportunities and challenges in a connected world. Commonwealth Bank of Australia. Online verfügbar unter <https://www.commbank.com.au/content/dam/caas/newsroom/docs/Commbank-Whitepaper-Machine-to-Machine-economy.pdf>, zuletzt geprüft am 08.11.2019.
- Raval, Siraj (2016): Decentralized applications. Harnessing Bitcoin's blockchain technology. Beijing, Boston: O'Reilly. Online verfügbar unter <http://kddlab.zjgsu.edu.cn:7200/research/blockchain/OReilly.Decentralized.Applications.Harnessing.Bitcoins.Blockchain.Technology.pdf>, zuletzt geprüft am 29.08.2019.
- Renz, Alexander (2019): IOTA and Qubic - The Start of New Era (and the Fulfillment of a Long Time Dream) | IOTA News. Online verfügbar unter <https://iota-news.com/iota-and-qubic-the-start-of-new-era-and-the-fulfillment-of-a-long-time-dream/>, zuletzt geprüft am 05.11.2019.
- Rogers, Everett M. (2003): Diffusion of innovations. Fifth edition, Free Press trade paperback edition. New York, London, Toronto, Sydney: Free Press (Social science). Online verfügbar unter <http://www.loc.gov/catdir/bios/simon052/2003049022.html>.
- RSK (2019): RSK - Home. RSK Labs. Online verfügbar unter <https://www.rsk.co/>, zuletzt aktualisiert am 21.11.2019, zuletzt geprüft am 26.11.2019.
- Sabine Jakob; Dr. Axel T. Schulte; Dominik Sparer; Roman Koller; Prof. Dr. Michael Henke (2018): Blockchain und Smart Contracts: Effiziente und sichere Wertschoepfungsnetzwerke. Hg. v. Michael ten Hompel, Michael Henke und Uwe Clausen. Dortmund. Online verfügbar unter https://www.iml.fraunhofer.de/content/dam/iml/de/documents/OE260/10_Whitepaper_BlockchainSmart-Contracts_Ausgabe_10_WEB.pdf, zuletzt geprüft am 19.11.2019.

- Saini, Vaibhav (2019): 10 State Channel Projects Every Blockchain Developer Should Know About. Hackernoon. Online verfügbar unter <https://hackernoon.com/10-state-channel-projects-every-blockchain-developer-should-know-about-293514a516fd>, zuletzt geprüft am 15.10.2019.
- Salah, Khaled; Rehman, M. Habib Ur; Nizamuddin, Nishara; Al-Fuqaha, Ala (2019): Blockchain for AI: Review and Open Research Challenges. In: *IEEE Access* 7, S. 10127–10149. DOI: 10.1109/ACCESS.2018.2890507.
- Schiener, Dominik (o. J.): IOTA Deepdive · IOTA Guide. Online verfügbar unter <https://domschiener.gitbooks.io/iota-guide/content/chapter1.html>, zuletzt geprüft am 15.10.2019.
- Schiller, Kai (2018): Die Ethereum Roadmap | Der Weg zum Internet 3.0 | Blockchainwelt. Lunik Pro UG. Online verfügbar unter <https://blockchainwelt.de/ethereum-roadmap-zum-internet-3-0/>, zuletzt geprüft am 29.10.2019.
- Schiller, Kai (2019): Plasma: Skalierbare Ethereum Smart Contracts | Blockchainwelt. Lunik Pro UG. Online verfügbar unter <https://blockchainwelt.de/plasma-skalierbare-ethereum-smart-contracts/>, zuletzt geprüft am 05.11.2019.
- Schlatt, Vincent; Schweizer, André; Urbach, Nils; Fridgen, Gilbert (2016): Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT.
- Schneider, David (2019): Die 5 größten Bitcoin Mining Pools, sortiert nach Hash Rate. BTC-ECHO GmbH. Online verfügbar unter <https://www.btc-echo.de/die-5-groessten-bitcoin-mining-pools-sortiert-nach-hash-rate/>, zuletzt geprüft am 08.11.2019.
- Sclavounis, Odysseas (2017): Understanding Public Blockchain Governance — Oxford Internet Institute. Oxford Internet Institute. Online verfügbar unter <https://www.oii.ox.ac.uk/blog/understanding-public-blockchain-governance/>, zuletzt geprüft am 20.08.2019.
- Shen, Charles; Pena-Mora, Feniosky (2018): Blockchain for Cities—A Systematic Literature Review. In: *IEEE Access* 6, S. 76787–76819. DOI: 10.1109/ACCESS.2018.2880744.
- Sheth, Amit P. (1999): Changing Focus on Interoperability in Information Systems: From System, Syntax, Structure to Semantics. In: Michael Goodchild, Max Egenhofer, Robin Fegeas und Cliff Kottman (Hg.): *Interoperating Geographic Information Systems*. Boston, MA: Springer (The Springer International Series in Engineering and Computer Science, 495), S. 5–29. Online verfügbar unter https://doi.org/10.1007/978-1-4615-5189-8_2, zuletzt geprüft am 29.11.2019.
- Singh, Amritraj; Click, Kelly; Parizi, Reza M.; Zhang, Qi; Dehghantanha, Ali; Choo, Kim-Kwang Raymond (2020): Sidechain technologies in blockchain networks: An examination and state-of-the-art review. In: *Journal of Network and Computer Applications* 149, S. 102471. DOI: 10.1016/j.jnca.2019.102471.
- Singh, Nitish (2018): Real World Blockchain Use Cases - 46 Blockchain Applications. 101 Blockchains. Online verfügbar unter <https://101blockchains.com/blockchain-applications/#prettyPhoto>, zuletzt aktualisiert am 25.10.2019, zuletzt geprüft am 25.10.2019.
- Skidanov (2018): Unsolved Problems in Blockchain Sharding. Online verfügbar unter <https://medium.com/nearprotocol/unsolved-problems-in-blockchain-sharding-2327d6517f43>, zuletzt geprüft am 31.12.2019.

- Skwarek, Volker (2019): Eine kurze Geschichte der Blockchain. In: *Informatik Spektrum* 42 (3), S. 161–165. DOI: 10.1007/s00287-019-01175-0.
- Smith + Crown (2019): Smith + Crown Home. Online verfügbar unter <https://www.smithandcrown.com/>, zuletzt geprüft am 15.10.2019.
- Social Minds Inc (KK) (o. J.): Realitio - Crowd-sourced verification for smart contracts. Online verfügbar unter <https://realit.io/>, zuletzt geprüft am 29.11.2019.
- Sompolinsky, Yonatan; Zohar, Aviv (2013): Secure High_rate Transaction Processing in Bitcoin. Online verfügbar unter <https://eprint.iacr.org/eprint-bin/print.pl>.
- Steffen Schwalm; Ulrike Korte; Tomasz Kusber; Christian Berghoff (2018): LANGFRISTIGE BEWEISWERTERHALTUNG UND DATENSCHUTZ IN DER BLOCKCHAIN.
- Stockschläger, Tim (2019): Krypto-Boom: Security Token liegen im Trend - Biallo.de. Biallo & Team GmbH. Online verfügbar unter <https://new.biallo.de/geldanlage/ratgeber/krypto-boom-security-token-liegen-im-trend/?#>, zuletzt geprüft am 25.10.2019.
- Strinati, Emilio Calvanese; Barbarossa, Sergio; Gonzalez-Jimenez, José Luis; Kténas, Dimitri; Cassiau, Nicolas; Dehos, Cédric (2019): 6G: The Next Frontier. Online verfügbar unter <http://arxiv.org/pdf/1901.03239v2>.
- Suichies, B. (2015): Why Blockchain must die in 2016. Online verfügbar unter <https://medium.com/block-chain/why-blockchain-must-die-in-2016-e992774c03b4>, zuletzt geprüft am 13.12.2019.
- Surowiecki, James (2004): The wisdom of crowds. Why the many are smarter than the few and how collective wisdom shapes business, economies, societies, and nations. 1. ed. New York, NY: Doubleday. Online verfügbar unter <http://www.loc.gov/catdir/bios/random055/2003070095.html>.
- Swan, Melanie (2015): Blockchain. Blueprint for a new economy. 1. ed. Beijing: O'Reilly (Safari Tech Books Online). Online verfügbar unter <http://proquest.safaribooksonline.com/9781491920480>.
- Szabo, Nick (1998): Secure Property Titles with Owner Authority. Satoshi Nakamoto Institute. Online verfügbar unter <https://nakamotoinstitute.org/secure-property-titles/>, zuletzt aktualisiert am 03.03.2020, zuletzt geprüft am 03.03.2020.
- Tasca, Paolo; Tessone, Claudio J. (2017): Taxonomy of Blockchain Technologies. Principles of Identification and Classification. Online verfügbar unter <https://arxiv.org/pdf/1708.04872.pdf>, zuletzt geprüft am 17.07.2019.
- Tavares, Bruno; Correia, Filipe Figueiredo; Restivo, André; Faria, João Pascoal; Aguiar, Ademar (2019): A survey of blockchain frameworks and applications, 24.03.2019. Online verfügbar unter <https://arxiv.org/pdf/1903.12553>.
- The Economist (2015): The trust machine. Online verfügbar unter <https://www.economist.com/leaders/2015/10/31/the-trust-machine>, zuletzt geprüft am 25.10.2019.
- Trauth, Daniel (2018a): Manufacturing Economy. Online verfügbar unter <https://medium.com/industrial-iota-lab-aachen-wzl-of-rwth-aachen/manufacturing-economy-e541066889ee>, zuletzt geprüft am 08.11.2019.

- Trauth, Daniel (2018b): WZL x GCX x IOTA—Status Report 05. Online verfügbar unter <https://medium.com/industrial-iota-lab-aachen-wzl-of-rwth-aachen/wzl-x-gcx-x-iota-status-report-05-bd73734eac2b>, zuletzt geprüft am 08.11.2019.
- Turan, Meltem Sonmez; Perlner, Ray; Bassham, Lawrence E.; Burr, William; Chang, Donghoon; Chang, Shu-jen et al. (2011): Status report on the second round of the SHA-3 cryptographic hash algorithm competition. Gaithersburg, MD.
- Universität Paderborn (o. J.): Codes und Kryptographie - Paarungsbasierte Kryptographie (Universität Paderborn). Online verfügbar unter <https://cs.uni-paderborn.de/cuk/forschung/paarungsbasierte-kryptographie/>, zuletzt geprüft am 05.11.2019.
- Vavilov, Valery; Kikvadze, George; Mariani, Nicola; Sewell, Jeremy; Petrov, Alex (2015): Proof of Stake versus Proof of Work. Bitfury Group Limited. Online verfügbar unter <https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf>, zuletzt geprüft am 11.10.2019.
- Visa Inc. (2015): Visa Inc. at a Glance. Online verfügbar unter <https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf>, zuletzt geprüft am 25.10.2019.
- Vitalik Non-giver of Ether on Twitter. Online verfügbar unter <https://twitter.com/vitalikbuterin/status/1051160932699770882>, zuletzt geprüft am 31.07.2019.
- Voshmgir, Shermin: Blockchains, Smart Contracts und Dezentrale Web. Technologie Stiftung Berlin. Online verfügbar unter https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf, zuletzt geprüft am 29.08.2019.
- Voshmgir, Shermin (2019): Token economy. How blockchains and smart contracts revolutionize the economy. 1st edition, 2nd amended printing.
- Vyjayanti, Desai; Diofasi, Anna; Lu, Jing (2018): The global identification challenge: Who are the 1 billion people without proof of identity? Online verfügbar unter <https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity>, zuletzt geprüft am 25.10.2019.
- W3C (2019): Blockchain | W3C Blog. Online verfügbar unter <https://www.w3.org/blog/category/technology/blockchain/>, zuletzt geprüft am 08.11.2019.
- WANCHAIN FOUNDATION LTD (2019): Wanchain - Decentralized Finance Interoperability - Wanchain. Online verfügbar unter <https://www.wanchain.org/>, zuletzt geprüft am 29.10.2019.
- Wang, Licheng; Shen, Xiaoying; Li, Jing; Shao, Jun; Yang, Yixian (2019a): Cryptographic primitives in blockchains. In: *Journal of Network and Computer Applications* 127, S. 43–58. DOI: 10.1016/j.jnca.2018.11.003.
- Wang, Wenbo; Hoang, Dinh Thai; Hu, Peizhao; Xiong, Zehui; Niyato, Dusit; Wang, Ping et al. (2019b): A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. In: *IEEE Access* 7, S. 22328–22370. DOI: 10.1109/ACCESS.2019.2896108.
- Wei, Dai (1998): B-Money. Online verfügbar unter <http://www.weidai.com/bmoney.txt>, zuletzt aktualisiert am 03.03.2020, zuletzt geprüft am 03.03.2020.

- Wei, Songjie; Li, Shuai; Liu, Peilong; Liu, Meilin (2018): BAVP: Blockchain-Based Access Verification Protocol in LEO Constellation Using IBE Keys. In: *Security and Communication Networks* 2018 (4), S. 1–14. DOI: 10.1155/2018/7202806.
- Weizsäcker, Franz von; Meier-Hahn, Uta; Wannemacher, Lars (2019): Libra vs. Regierungen - Der Wettlauf um eine offene globale Zahlungsinfrastruktur. netzpolitik.org. Online verfügbar unter <https://netzpolitik.org/2019/libra-vs-regierungen-der-wettlauf-um-eine-offene-globale-zahlungsinfrastruktur/>, zuletzt geprüft am 25.10.2019.
- Wilke, Andreas (2017): Blockchain - Verbesserungspotential der Technologie. Bundesdruckerei GmbH. Online verfügbar unter https://www.bafin.de/SharedDocs/Downloads/DE/Veranstaltung/dl_180410_BaFinTech_2018_WS3_2.pdf?__blob=publicationFile&v=3, zuletzt geprüft am 05.11.2019.
- Will Martino, Stuart Popejoy (2019): The Kadena Public Blockchain. Online verfügbar unter https://d31d887a-c1e0-47c2-aa51-c69f9f998b07.filesusr.com/ugd/86a16f_1e25e5ac5db44fb7b7e4eb2fe845ce2d.pdf, zuletzt geprüft am 31.12.2019.
- Wobst, Reinhard (2019): Märchenkette. In: *iX* (9), S. 98–103. Online verfügbar unter <https://www.heise.de/select/ix/2019/9/1914809440002427567>, zuletzt geprüft am 15.10.2019.
- Wolmarans, Tiaan (2019): Sharding and Scaling On Blockchain. Hackernoon. Online verfügbar unter <https://hackernoon.com/sharding-and-the-scaling-of-a-blockchain-xz1kq30j0>, zuletzt aktualisiert am 29.10.2019, zuletzt geprüft am 08.11.2019.
- Wood, Garvin: Ethereum: a secure decentralised generalised transaction ledger (EIP-150 REVISION). 2014 (2014). Online verfügbar unter <https://gavwood.com/paper.pdf>, zuletzt geprüft am 29.11.2019.
- Wood, Gavin (2017): ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. Online verfügbar unter <https://gavwood.com/paper.pdf>, zuletzt geprüft am 11.10.2019.
- World Economic Forum (2015): Deep Shift: Technology Tipping Points and Societal Impact. Online verfügbar unter <https://www.weforum.org/reports/deep-shift-technology-tipping-points-and-societal-impact>, zuletzt geprüft am 29.11.2019.
- World Economic Forum (2019): Global risks 2019. 14th Edition. 14th Edition. Geneva.
- Wüst, Karl; Gervais, Arthur (2018 - 2018): Do you Need a Blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). Zug, 20.06.2018 - 22.06.2018: IEEE, S. 45–54.
- Xiao, David (2016): The Four Layers of the Blockchain. Medium. San Francisco, USA. Online verfügbar unter <https://medium.com/@coriacetic/the-four-layers-of-the-blockchain-dc1376efa10f>, zuletzt geprüft am 15.10.2019.
- Yaffe, Lior (2017): Using the Blockchain to Bridge Data Silos. Online verfügbar unter <https://medium.com/@lyaffe/using-the-blockchain-to-bridge-data-silos-852aa82d84eb>, zuletzt geprüft am 08.11.2019.

- Yaga, Dylan; Mell, Peter; Roby, Nik; Scarfone, Karen (2018): Blockchain Technology Overview. NIST. Online verfügbar unter <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf>, zuletzt geprüft am 06.08.2019.
- Yli-Huomo, Jesse; Ko, Deokyoong; Choi, Sujin; Park, Sooyong; Smolander, Kari (2016): Where Is Current Research on Blockchain Technology?-A Systematic Review. In: *PloS one* 11 (10), e0163477. DOI: 10.1371/journal.pone.0163477.
- Yuan, Yong; Wang, Fei-Yue (2018): Blockchain and Cryptocurrencies: Model, Techniques, and Applications. In: *IEEE Trans. Syst. Man Cybern, Syst.* 48 (9), S. 1421–1428. DOI: 10.1109/TSMC.2018.2854904.
- Z_punkt GmbH (2019): Die Blockchain als Internet der Werte | Z_punkt. Online verfügbar unter <http://www.z-punkt.de/de/themen/artikel/blockchain/472>, zuletzt geprüft am 17.09.2019.
- Zamani, Mahdi; Movahedi, Mahnush; Raykova, Mariana (2018): RapidChain. In: David Lie und Mohammad Mannan (Hg.): CCS'18. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security ; October 15-19, 2018, Toronto, ON, Canada. the 2018 ACM SIGSAC Conference. Toronto, Canada, 10/15/2018 - 10/19/2018. Association for Computing Machinery; ACM Conference on Computer and Communications Security; CCS. New York, NY: Association for Computing Machinery, S. 931–948.
- Zamfir, Vlad (2015): Introducing Casper “the Friendly Ghost”. Foundation, Ethereum. Online verfügbar unter <https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/>, zuletzt aktualisiert am 07.10.2019, zuletzt geprüft am 11.10.2019.
- Zhang, Fangguo; Kim, Kwangjo (2002): ID-Based Blind Signature and Ring Signature from Pairings. In: Yuliang Zheng (Hg.): Advances in Cryptology - ASIACRYPT 2002. 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown, New Zealand, December 1-5, 2002 Proceedings, Bd. 2501. Berlin, Heidelberg: Springer (Lecture Notes in Computer Science, 2501), S. 533–547.
- Zhang, Shijie; Lee, Jong-Hyouk (2019): Analysis of the main consensus protocols of blockchain. In: *ICT Express*. DOI: 10.1016/j.icte.2019.08.001.
- Zheng, Zibin; Xie, Shaoan; Dai, Hong Ning; Chen, Xiangping; Wang, Huaimin (2018): Blockchain challenges and opportunities: a survey. In: *IJWGS* 14 (4), S. 352. DOI: 10.1504/IJWGS.2018.095647.
- Zheng, Zibin; Xie, Shaoan; Dai, Hongning; Chen, Xiangping; Wang, Huaimin (2017): An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: George Karypis und Jia Zhang (Hg.): 2017 IEEE International Congress on Big Data - BigData Congress 2017. 25-30 June 2017, Honolulu, Hawaii, USA : proceedings. 2017 IEEE International Congress on Big Data (BigData Congress). Honolulu, HI, USA: IEEE, S. 557–564. Online verfügbar unter <https://ieeexplore.ieee.org/ielx7/8027154/8029291/08029379.pdf?tp=&arnumber=8029379&isnumber=8029291&ref=aHR0cHM6Ly9pZWVleHBsb3JlLmlZSWUub3JnL2Fic3RyYWNOL2RvY3VtZW50LzgwMjkzNzk=>, zuletzt geprüft am 23.07.2019.
- Zilliqa (2019): Zilliqa - Home. Online verfügbar unter <https://zilliqa.com/>, zuletzt aktualisiert am 11.11.2019.