JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN
PROFESSUR BWL – WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. AXEL SCHWICKERT

Graf von Plettenberg, Mariano; Schwickert, Axel;
Patzak, Maximilian

Blockchain – Grundlagen, Funktionsweise und Anwendungsbeispiele

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 1 / 2021
ISSN 1613-6667

Arbeitspapiere WI Nr. 1 / 2021

Autoren: Graf von Plettenberg, Mariano; Schwickert, Axel;
Patzak, Maximilian

Titel: Blockchain – Grundlagen, Funktionsweise und Anwendungsbeispiele

Zitation: Graf von Plettenberg, Mariano; Schwickert, Axel; Patzak, Maximilian: Blockchain – Grundlagen, Funktionsweise und Anwendungsbeispiele, in: Arbeitspapiere WI, Nr. 1/2021, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2021, 50 Seiten, ISSN 1613-6667.

Kurzfassung: In dem Arbeitspapier WI „Blockchain – Grundlagen, Funktionsweise und Anwendungsbeispiele“ (Nr. 01/2021) wird eine kompakte und einfach zu verstehende Einleitung in das Thema Blockchain gegeben. In diesem Zusammenhang wird zunächst die populärste Anwendung der Blockchain, die Kryptowährung Bitcoin, dargestellt und deren Funktionsprinzipien beschrieben. In einem weiteren Schritt werden charakteristische Eigenschaften von Smart Contracts und deren Funktionsweise sowie Anwendungsbeispiele dargelegt. Daraus abgeleitet werden die allgemeinen Grundlagen und die Funktionsweise der Blockchain-Technologie kompakt dargestellt und zukünftige Herausforderungen diskutiert.

Schlüsselwörter: Blockchain, Distributed-Ledger-Technology, Smart Contracts, Kryptowährungen, Bitcoin, Ethereum, Anwendungsbeispiele

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Seite

Abkürzungsverzeichnis

BaFin ..... Bundesanstalt für Finanzdienstleistungen
BTC ..... Bitcoin
DLT ..... Distributed-Ledger-Technology
IOTA ..... Internet of Things' Applications
PoS ..... Proof-of-Stake
PoW ..... Proof-of-Work
PKI ..... Privat Key Infrastructure
P2P-Netzwerk ..... Peer-to-Peer-Netzwerk

1 Problemstellung, Ziel und Aufbau

In den letzten Jahren haben sich mehrere digitale Währungen entwickelt. Darunter befindet sich auch die bekannte Kryptowährung „Bitcoin“, welche beispielsweise in Japan bereits als offizielles Zahlungsmittel akzeptiert wird.[1] Die Enthusiasten sprechen vom digitalen Gold und die Bitcoin-Gegner von einem reinen Spekulationsobjekt.[2] Fakt ist, dass die Kryptowährungen, im Speziellen Bitcoin, in den letzten Jahren für viele Schlagzeilen gesorgt haben. Kein Wunder, überstieg der Preis für einen Bitcoin im Jahr 2010 nicht einmal einen Euro, hatte dieser am 17. Dezember 2017 mit 16.679 Euro seinen bisherigen Höhepunkt erreicht.[3] Dabei stand die eigentliche technologische Innovation, die Blockchain-Technologie, lange Zeit im Schatten ihrer populärsten Anwendung, dem Bitcoin. Und dies, obwohl die Blockchain-Technologie die Abwicklung von Verträgen und Zahlungsströmen in ähnlichem Ausmaß revolutionieren kann, wie das World Wide Web unsere Mediennutzung verändert hat. Maßgeblich hierfür ist die technologische Beschaffenheit der Blockchain, Daten dezentral und unveränderlich zu speichern, ohne dabei eine zentrale Autorität einbinden zu müssen. Genauer gesagt, ermöglicht diese neue Technologie ein nicht manipulierbares globales Register, das Besitzverhältnisse unmissverständlich zuordnet und mit dessen Hilfe Werte bei Bedarf sekundenschnell transferiert werden können. Durch die weltweit dezentrale Speicherung der Datenbestände und automatisierte Konsensbildung werden Zwischeninstanzen wie Staaten oder Banken überflüssig. Visionäre sprechen von einer Zukunft, in der jeder mit jedem weltweit verlässlich Geschäfte abwickeln kann, ohne seinen Vertragspartner persönlich zu kennen. Die neue Technologie übernimmt die Validierung und Identifikation weitestgehend automatisiert über Rechnernetze.

Für Organisationen aus Wirtschaft, Verwaltung und Forschung stellt die Blockchain-Technologie eine neuartige Domäne dar. In dieser hat bisher nur eine begrenzte Anzahl von Experten tiefgreifendes Verständnis entwickelt und sich umfassend mit der Thematik auseinandergesetzt. Diese Experten sind sich allerdings einig, dass die Blockchain-Technologie das Potenzial hat, Bereiche in unserer Gesellschaft zu verändern, die weit über das Gebiet digitaler Währungen hinausgehen. Zahlreiche Startups und etablierte Unternehmen arbeiten an Blockchain-basierten Applikationen, um das technologische Fundament bestehender Geschäftsmodelle zu revolutionieren. Aufgrund der Popularität des Begriffs, der Komplexität der funktionalen Prinzipien und

1 Vgl. BTC-ECHO (Hrsg.): Das sind die 5 krypto-freundlichsten Länder der Welt, Online im Internet: https://www.btc-echo.de/dies-sind-die-5-krypto-freundlichsten-laender-der-welt/, 30.12.2018.

2 Vgl. Handelsblatt (Hrsg.): In Bitcoins investieren, Online im Internet: https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/sparen-in-der-digitalen-zukunft-in-bitcoins-investieren/19971882.html?ticket=ST-3252743-skOhWcVOWvTqBpa07dye-ap3, 25.06.2017.

3 Vgl. Blockchaincenter (Hrsg.): Bitcoin Kurs, Online im Internet: https://www.blockchaincenter.net/bitcoin/bitcoin/#kurs, 03.10.2020.

des technischen Fundaments soll die vorliegende Arbeit eine kompakte und einfach zu verstehende Einführung zur Blockchain bieten.

Um dieses Ziel zu erreichen, wird zunächst die populärste Anwendung der Blockchain, die Kryptowährung Bitcoin, dargestellt und deren Funktionsprinzipien beschrieben. Die Blockchain kann jedoch mehr: Sie kann neben Zahlungstransfers auch ganze Verträge abwickeln. Diese sog. „Smart Contracts“ werden in einem zweiten Schritt erläutert. Die Anwendungsbeispiele Kryptowährungen und Smart Contracts zeigen die wesentlichen Elemente und Funktionsprinzipien der Blockchain auf. Diese Elemente und Funktionsprinzipen werden abschließend zusammengefasst.

Die vorliegende Arbeit ist wie folgt aufgebaut: Nach dem einleitenden Kapitel 1 beschäftigt sich Kapitel 2 *„Kryptowährungen“* mit dem Bitcoin als populärste Anwendung. Zunächst wird dabei die Entstehung und Abgrenzung zu Fiatwährungen geschildert. Im Anschluss daran wird ein Transaktionsbeispiel durchexerziert, bevor im letzten Teil ein Überblick zu weiteren Kryptowährungen gegeben wird. Im 3. Kapitel *„Smart Contracts“* werden charakteristische Eigenschaften von Smart Contracts und deren Funktionsweise sowie Anwendungsbeispiele dargelegt. Daraus abgeleitet werden in Kapitel 4 die allgemeinen Grundlagen und die Funktionsweise der Blockchain-Technologie kompakt dargestellt. Daran anschließend werden neben einer Klassifikation der Blockchain weitere Anwendungsbeispiele vorgestellt und zukünftige Herausforderungen diskutiert. Das letzte Kapitel gibt einen Ausblick in die Zukunft der Blockchain.

2 Kryptowährungen

2.1 Blockchain und der Bitcoin

In diesem Kapitel 2 soll ein Grundverständnis für den Einsatz von Kryptowährungen vermittelt werden. Um dieses Ziel zu erreichen, werden Kryptowährungen definiert und zunächst gegenüber Fiatwährungen und Buchgeld abgegrenzt. Im Anschluss folgt die Erläuterung einer Beispieltransaktion auf Basis der Kryptowährung *Bitcoin*. Abschließend wird auf weitere Kryptowährungen – neben dem Bitcoin – eingegangen und der Funktionsumfang bzw. Einsatzgebiete dieser Kryptowährungen erläutert.

Die Begriffe „Bitcoin“ und „Blockchain“ werden oft miteinander in Verbindung gebracht und sind aus technisch-konzeptioneller Perspektive eng miteinander verbunden. Die Blockchain bildet die technische Grundlage für die Implementierung der Kryptowährung „Bitcoin“. Dabei kann die Blockchain vereinfacht als ein Transaktionsregister verstanden werden, das Bitcoin-Transaktionen dokumentiert und veröffentlicht. Die Transaktionen werden in „Blöcken“ zusammengefasst und chronologisch miteinander verkettet. Es entsteht eine Kette von Blöcken (engl. Blockchain), die sämtliche Bitcoin-Transaktionen abbildet.

Tatsächlich liegen die konzeptionellen Ursprünge der Blockchain-Technologie aber weit vor der Etablierung der Kryptowährungen. Bei der Blockchain-Technologie handelt es sich um eine Kombination aus mehreren Konzepten: Public-Key-Kryptografie bzw. digitale Signaturen, kryptografische Hash-Funktionen und Merkle Trees (dt. Hash-Baum).[4]

Haber und Stornetta erläutern bereits in ihrer Veröffentlichung von 1991 eine Software, die eine kryptografische Prüfsumme eines digitalen Dokuments generiert, in eine Datenbank lädt und das Dokument so mit einem eindeutigen Zeitstempel registriert.[5] Das Prinzip des Hash-Baums, welches das Zusammenfassen von mehreren Hashes zu einem Basis-Hash beschreibt, hat Ralph Merkle 1989 definiert.[6] Die Verwendung von öffentlichen Schlüsseln als anonyme bzw. pseudonyme Adressen wurde in den 80er-Jahren durch Chaum veröffentlicht.[7] Auch ist die Schaffung einer digitalen Währung kein ganz neuer Ansatz. Bereits 1998 veröffentlichte Wie Dai mit „B-Money“, und Nick Szabo, 2005, mit „Bit Gold“ jeweils Ansätze zu einer digitalen Währung.[8] Erst der „Bitcoin“ hat es allerdings geschafft, sich als Kryptowährung weltweit in etablierte Geschäftsmodelle und Geschäftsaktivitäten zu integrieren und die Abwicklung von Transaktionen auf Basis einer neuartigen Währung zu ermöglichen.

Am 31.10. 2008 veröffentlichte eine anonyme Person oder Gruppe unter dem Pseudonym Satoshi Nakamoto ein White Paper mit dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System“.[9] In diesem wird ein technisches Konzept erläutert, digitales Geld, Bitcoin genannt, in einem elektronischen Peer-To-Peer-Zahlungssystem direkt vom Sender an den Empfänger zu senden, ohne den Einbezug von Drittparteien als Intermediär. Der Begriff „Blockchain“ kommt dabei in der Veröffentlichung von Satoshi Nakamoto an keiner Stelle vor. Erst die Programmierer, die das Bitcoin-Konzept in einen Code übertrugen, nannten das entstandene Protokoll hinter der Kryptowährung „Blockchain“. Diese Blockchain war von Beginn an „open source“, bestand im Wesentlichen aus den oben genannten drei Konzepten und wurde in der Folge oft kopiert bzw. modifiziert. Dies ist auch eine Erklärung für die heutige große Anzahl an kryptografischen Währungen.[10]

---

4 Vgl. Böhme, Rainer; Christin, Nicolas; Edelman, Benjamin; Moore, Tyler: Bitcoin: Economics, Technology, and Governance, in: Journal of Economic Perspectives, 29(2)/2015, S. 216.

5 Vgl. Haber, Stuart; Stornetta, W. Scott: How to Time-Stamp a Digital Document, in: Journal of Cryptology, 3(2)/1991.

6 Vgl. Merkle, Ralph C.: A certified digital signature, in: CRYPTO ’89: Proceedings on Advances in Cryptology Lecture Notes in Computer Science, 435/1989.

7 Vgl. Chaum, David L.: Untraceable electronic mail, return addresses, and digital pseudonyms, in: Communication of ACM 24(2)/1981.

8 Vgl. Dai, Wie: B-Money, Online im Internet: http://www.weidai.com/bmoney.txt, 1998 und Szabo, Nick: Bit Gold, Online im Internet: https://nakamotoinstitute.org/bit-gold/, 29.12.2005.

9 Vgl. Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

10 Vgl. Crosby, Michael; Pattanayak, Pradan; Verma, Sanjeev; Kalyanaraman, Vignesh: BlockChain Technology: Beyond Bitcoin, in: Applied Innovation Review, 2/2016, S. 9.

Im Februar 2010 wurde mit *Bitcoin Market* die erste Handelsplattform eröffnet, auf der Blockchain-basiert Bitcoin gegen Landeswährung getauscht werden konnte. Drei Monate später, am 22.05.2010, erfolgte der erste dokumentierte Warenkauf mit der digitalen Währung Bitcoin. Der bitcointalk User Laszlo Hanyecz *(laszlo)* war die erste Person, die 10.000 Bitcoin für ein reales Gut, zwei Pizzen, eintauschte.[11] Der Tausch setzt einen historischen Preispunkt von 0,0025 US Dollar für einen Bitcoin fest. Zwei Monate später nahm die japanische Tauschbörse für Fantasy-Sammelspielkarten *Mt. Gox* ihre Geschäftstätigkeiten als Handelsplattform für Bitcoin auf. Dadurch wurde die Kryptowährung für eine breitere Masse sichtbar. In Folge dessen stieg am 01.04.2013 der Kurs eines Bitcoins auf 100 Euro und sieben Monate später auf über 1.000 Euro.[12] 2014 gaben mehrere namenhafte Unternehmen wie *Expedia*, *Dell* und *Microsoft* bekannt, Bitcoin als Zahlungsmittel zu akzeptieren.[13] Ein weiterer historisch entscheidender Moment war die Einführung von Bitcoin als offizielles Zahlungsmittel in Japan im April 2016.

Seit Bestehen ist der Bitcoin-Kurs von seiner hohen Volatilität geprägt. Im Oktober 2020 notiert er um 9.000 Euro. Die im Oktober 2020 im Umlauf befindlichen Bitcoins haben damit eine Marktkapitalisierung von rund 165 Mrd. Euro.[14] Während die Kryptowährung in ihren Anfängen häufig als Zahlungsmittel für Geschäfte im Darknet verwendet wurde, ist Bitcoin heute auf mehreren Plattformen frei handelbar und kann zum Kauf und Verkauf von Gütern und Dienstleistungen verwendet werden. Beispielsweise auf der Essenslieferplattform *Lieferando,* oder um lokale Steuern in der Schweizer Gemeinde Zug zu bezahlen.[15] Die zunehmende Etablierung und Nutzung des Bitcoins ist dabei jedoch auch mit einer rasant steigenden Rechenpower verbunden. Der weltweite Stromverbrauch pro Jahr für das Dokumentieren von Transaktionen in der Bitcoin-Blockchain übersteigt mittlerweile den kompletten jährlichen Stromverbrauch der Schweiz.[16]

11 Vgl. Bitcoin Wiki (Hrsg.): Laszlo Hanyecz, Online im Internet: https://en.bitcoin.it/wiki/Laszlo_ Hanyecz, 2010.

12 Vgl. Blockchaincenter (Hrsg.): Bitcoin Kurs, Online im Internet: https://www.blockchaincenter.net/bitcoin /#kurs, 03.10.2020.

13 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 87.

14 Vgl. CoinMarketCap (Hrsg.): Bitcoin, Online im Internet: https://coinmarketcap.com/de/currencies /bitcoin/, 03.10.2020.

15 Vgl. Krone Zeitung (Hrsg.): Zermatt akzeptiert Steuerzahlungen in Bitcoin, Online im Internet, https://www.krone.at/2087853, 29.01.2020 und Giga (Hrsg.): Mit Bitcoin Pizza bestellen und online liefern lassen – so geht's, Online im Internet: https://www.giga.de/downloads/bitcoin/specials/mit-bitcoin-pizza-bestellen-und-online-liefern-lasse n-so-gehts/, 02.02.2018.

16 Vgl. Finextra (Hrsg.): How to use technology to solve climate change and cloud waste, Online im Internet: https://www.finextra.com/newsarticle/35365/how-to-use-technology-to-solve-climate-change-and-cloud-waste, 27.02.2020.

Der aktuelle Entwicklungsstand der Blockchain-Technologie befindet sich jedoch noch am Anfang. Laut Experten ist es keine Frage, ob sich Blockchain-basierte Prozesse und Dienste in der realen Wirtschaft etablieren werden, sondern lediglich, wann und wo dies der Fall sein wird.[17]

2.2 Definition und Abgrenzung zu Fiatwährungen

Kryptowährungen, auch kryptografische, digitale oder virtuelle Währungen genannt, sind Währungen, deren Funktionsweise und Sicherheit auf Kryptografie basiert und die ausschließlich digital erzeugt und gehandelt werden.[18] Die Kryptowährung Bitcoin wurde mit dem Ziel entwickelt, eine neuartige Geldeinheit zu schaffen. Mit dem Bitcoin soll eine digitale Währung entstehen, die nicht von zentralen Institutionen wie Banken oder Staaten verwaltet wird und gleichzeitig die Anonymität von Bargeld beibehält. Um dieses Ziel zu erreichen, wurde der Bitcoin als eine reine „Peer-to-Peer-Version" von elektronischem Bargeld entworfen. Das bedeutet, Sender und Empfänger eines Bitcoins sind Teilnehmer eines Transaktionsnetzwerkes, das ohne den Einsatz einer zentralen Kontrollinstanz (z. B. Bank) auskommt. Überweisungen können durch die Teilnehmer selbst überprüft und genehmigt werden. Banken, die einzelne Transaktionen genehmigen, sind nicht notwendig.[19]

Die Blockchain dient als chronologisches Register in diesem Transaktionsnetzwerk und dokumentiert alle Überweisungen in einer Datenbank. Die Daten in dieser Datenbank werden in „Blöcken" zusammengefasst und sind unveränderlich miteinander verbunden.[20] „Bitcoins (BTC)" fungieren als Recheneinheit und werden in den einzelnen Blöcken gespeichert. Um Transaktionen in Bitcoin überprüfen zu können, halten die Netzwerkteilnehmer eine Kopie des Registers. Die Teilnehmer wissen also zu jeder Zeit, wer wie viel Bitcoins überwiesen und empfangen hat. Versucht ein Teilnehmer, sein Register zu manipulieren, fällt dies sofort den anderen Teilnehmern auf. Alle kopierten Register werden kontinuierlich miteinander verglichen. Weicht ein Register von allen anderen ab, wird das veränderte Register als fehlerhaft markiert und ausgeschlossen. Die Gemeinschaft der Teilnehmer stellt also sicher, dass das Guthaben und die Überweisungen Einzelner verlässlich dokumentiert werden. Eine zentrale Instanz, die für das Sicherstellen der Guthaben und Überweisungen eingesetzt wird, ist im Bitcoin-System nicht notwendig.

17 Vgl. Becker, Sebastian: Everything a Marketplace: Wie die Blockchain neue Geschäftsmodelle eröffnet, in: Die Zukunft ist dezentral, Hrsg.: Sandner, Philipp; Tumasjan, Andranik; Welpe, Isabelle, Norderstedt: BoD – Books on Demand 2020, S. 25.

18 Vgl. Bussac, Enée: Bitcoin, Ethereum & Co. Praxiswissen Kryptowährungen und Blockchain, Berlin: Erich Schmidt Verlag GmbH & CO. KG 2019, S. 15.

19 Vgl. Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, S. 1.

20 Vgl. Fraunhofer FIT (Hrsg.): Blockchain: Grundlagen, Anwendungen und Potenziale, White Paper 2016, S. 8.

Ergänzend zu diesem Vorteil bergen Kryptowährungen wie Bitcoin aber auch ein spezifisches Risiko. Während bei physischen Objekten, wie einem Geldschein, die Eigentumsverhältnisse zu jeder Zeit klar definiert sind, können virtuelle Objekte sehr einfach kopiert, vervielfältigt und in der Folge auch mehrfach ausgegeben werden. Bei digitalen Geldeinheiten muss also die „Seltenheit“ als essentielle monetäre Eigenschaft durch besondere Maßnahmen gewährleistet werden. Dieses Problem wird in der Literatur als „Double-Spend" bezeichnet.[21] Um das „Double-Spending“ zu verhindern, existieren zwei Lösungsansätze. Entweder wird eine zentrale Instanz, bspw. eine Bank, damit beauftragt, alle elektronischen Zahlungen zu überprüfen, bevor diese getätigt werden. Oder es wird der Ansatz aus dem Bitcoin-Kontext verfolgt, welcher ohne einen Intermediär auskommt. Dabei werden alle getätigten Zahlungen im o. g. öffentlichen Register vermerkt. Vor jeder neuen Transaktion wird darüber durch die Netzwerkteilnehmer der Besitz der benötigten Geldeinheiten verifiziert.

Im direkten Vergleich zwischen dem Bitcoin-Systems und den Fiatwährungen werden die Gemeinsamkeiten und Unterschiede deutlich. Der Begriff Fiatgeld hat seinen Ursprung im lateinischen „Fiat-Lux“ (dt. es werde Licht). Es beschreibt die Tatsache, dass Fiatgeld weder über einen Fundamentalwert – wie beispielsweise Gold – verfügt noch ein Zahlungsversprechen beinhaltet und somit gewissermaßen aus dem Nichts entsteht („es werde Geld“).[22] Grundsätzlich werden Landeswährungen wie der Euro oder der US-Dollar als Fiatwährungen bezeichnet und werden durch einen Staat oder eine Gruppe von Staaten künstlich erzeugt.[23] Der Marktwert von Fiatwährungen basiert dabei ausschließlich auf den Zukunftserwartungen und die Wertstabilität wird lediglich von der Zentralbank garantiert, welche die jeweilige Geldeinheit exklusiv emittiert.[24] Im Vergleich dazu werden Kryptowährungen bisher (Oktober 2020) nahezu ausschließlich von privaten Organisationen geschaffen und ein vorher festgelegter Algorithmus bestimmt den Verlauf der Schöpfung von neuen Blöcken und Coins.[25] Zusätzlich existieren Kryptowährungen nur in digitaler Form und sind nicht an ein bestimmtes Territorium gebunden. Allerdings besitzen auch Kryptowährungen keinen fundamentalen Wert. Der real-wirtschaftliche Gegenwert von Bitcoin-Einheiten wird über den Markt – Angebot und Nachfrage – bestimmt und

21 Vgl. Drescher, Daniel: Blockchain Basics: A Non-Technical Introduction in 25 Steps, Frankfurt am Main: Apress Media 2017, S. 50.

22 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 21.

23 Vgl. Rosenberger, Patrick: Bitcoin und Blockchain – Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik, Berlin: Springer Vieweg 2018, S. 118.

24 Vgl. Bussac, Enée: Bitcoin, Ethereum & Co. Praxiswissen Kryptowährungen und Blockchain, Berlin: Erich Schmidt Verlag GmbH & CO. KG 2019, S. 13.

25 Vgl. Sandner, Philipp; Gösele, Martin: Blockchain-Technologie, in: WISU – Das Wirtschaftsstudium (Hrsg.), 03/2018, S. 312.

repräsentiert folglich die Wertschätzung und Zahlungsbereitschaft der Marktakteure.[26] Darüber hinaus erfüllen Kryptowährungen die weiteren Hauptfunktionen einer Fiatwährung. Neben der Funktion als Tausch- und Zahlungsmittel können die Kryptowährungen auch als Recheneinheit und Wertaufbewahrungsmittel eingesetzt werden.[27] Ein klarer Unterscheid zwischen Fiat- und Kryptowährungen liegt in der Inflationseigenschaft. Im Gegensatz zu der Möglichkeit unendlich viele Euros oder Dollars neu zu schaffen, ist im Bitcoin-System durch eine mathematisch zwingende Vorgabe die Geldmenge auf 21 Millionen Bitcoin festgelegt und kann nicht erhöht werden[28].

Eine substantielle Innovation von Bitcoin liegt im bewussten Verzicht auf zentrale Instanzen. Innerhalb des traditionellen Systems von Fiatwährungen erfüllen Banken zum einen die Aufgabe der Verwahrung von Giralgeld und zum anderen die Autorisierung und Ausführung von Transaktionen. Beim Giralgeld handelt es sich um nichts anderes als die registerbasierte Digitalisierung von physischen Geldansprüchen. Somit besitzt das digitale Giralgeld, ebenso wie das Bitcoin-System, ein Register zur Buchhaltung von Geldflüssen. Im traditionellen System nutzen Banken ihr zentrales, exklusives Datenregister, um die Transaktionsfähigkeit, die Transaktionslegitimität und den Transaktionskonsens zu gewährleisten.[29] Ein solches zentrales Datenregister wird auch „general ledger“ (dt. Hauptkontenbuch) genannt. Im Gegensatz dazu ist die Bitcoin-Blockchain das dezentrale Datenregister, welches in unzähligen Kopien verteilt bei den Teilnehmern des Netzwerks abgespeichert ist. Dieses dezentral verteilte Datenregister wird deshalb „distributed ledger“ (dt. verteiltes Kontenbuch) genannt.[30] Die Transaktionsfähigkeit, die Transaktionslegitimität und der Transaktionskonsens wird im Bitcoin-System durch seine Netzwerkteilnehmer gewährleistet.[31]

2.3 Funktionsweise anhand eines Transaktionsbeispiels

Vor allem durch die mediale Aufmerksamkeit wird Bitcoin von vielen Menschen als reines Spekulationsobjekt angesehen. Primärer Sinn der Kryptowährung ist allerdings, diese als

26 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 79.

27 Vgl. Bussac, Enée: Bitcoin, Ethereum & Co. Praxiswissen Kryptowährungen und Blockchain, Berlin: Erich Schmidt Verlag GmbH & CO. KG 2019, S. 17.

28 Vgl. Rosenberger, Patrick: Bitcoin und Blockchain – Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik, Berlin: Springer Vieweg 2018, S. 67.

29 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 50.

30 Vgl. Drescher, Daniel: Blockchain Basics: A Non-Technical Introduction in 25 Steps, Frankfurt am Main: Apress Media 2017, S. 35.

31 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 50.

Zahlungsmittel zwischen zwei Personen (Peer-to-Peer) einzusetzen. Um das benötigte Vertrauen in die Transaktionsprozesse von Bitcoin herzustellen, existieren unterschiedliche Gruppen von Teilnehmern, die verschiedene Aufgaben in dem Transaktionsnetzwerk übernehmen. Dazu zählen die Anwender, die Bitcoin als Zahlungsmittel verwenden und für die Nutzung eine bestimmte Gebühr zahlen. Die Anwender müssen allerdings nicht eine Kopie der kompletten Blockchain heruntergeladen und abgespeichert haben, um die Kryptowährung als Zahlungsmittel zu nutzen. Nutzer, die dagegen die komplette Blockchain abspeichern, werden „Full Nodes" genannt und helfen bei der Validierung von Transaktionen. Daneben gibt es Teilnehmer, die als „Konsens-Kreierer" bezeichnet werden können und innerhalb der Kryptowährungen „Miner" oder „Masternode" genannt werden. Diese Masternodes bzw. Miner stellen sicher, dass alle Teilnehmer die gleiche Version des Blockchain-Datenregisters verwenden. Diese Aufgabe ist wesentlich für den Erhalt der Blockchain und wird den Minern durch eine Gebühr entlohnt.[32] Die Aufgabe der Miner soll im folgenden Transaktionsbeispiel verdeutlicht werden.

Für eine Transaktion im Bitcoin-Netzwerk gibt es verschiedene Voraussetzungen, die sowohl Sender als auch Empfänger von Bitcoins erfüllen müssen. Beide Parteien müssen über ein sog. Schlüsselpaar verfügen, welches jeweils aus einem privaten Schlüssel (Privat Key) besteht, dem ein öffentlicher Schlüssel (Public Key) fest zugewiesen ist.[33] Eine Transaktion, die mit dem öffentlicher Schlüssel verschlüsselt wurde, kann nur mit dem dazugehörigen privaten Schlüssel entschlüsselt werden. Zudem ist es mit einem privaten Schlüssel möglich, Nachrichten oder Transaktionen digital eindeutig zu signieren und sich damit als Sender oder Empfänger einer Transkation zu authentifizieren. Das Prinzip der asymmetrisch verschlüsselten Kommunikation durch ein mathematisch zusammenhängendes Schlüsselpaar wird „Privat Key Infrastructure" (PKI) genannt.[34] Die Bitcoin-Adresse ist ebenfalls einem privaten Schlüssel fest zugewiesen und stellt aufgrund ihrer unterschiedlichen mathematischen Berechnung eine andere Darstellungsform des öffentlichen Schlüssels dar. Die Bitcoin-Adresse soll bei Transaktionen mehr Anonymität der Sender und Empfänger garantieren. Im Vergleich zu einem traditionellen Bankkonto kann der private Schlüssel mit dem Pin für das Bankkonto und der öffentliche Schlüssel bzw. die Bitcoin-Adresse mit der IBAN verglichen werden. Die Empfänger einer Transaktion können daher die öffentliche Bitcoin-Adresse gefahrenlos weitergeben, ebenso wie den öffentlichen Schlüssel.[35]

32 Vgl. Mohanty, Debajani: Blockchain für Manager, Haar bei München: Franzis Verlag GmbH 2018, S. 27.

33 Vgl. Crosby, Michael; Pattanayak, Pradan; Verma, Sanjeev; Kalyanaraman, Vignesh: BlockChain Technology: Beyond Bitcoin, in: Applied Innovation Review, 2/2016, S. 9.

34 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Public Key Infrastrukturen (PKIen), Online im Internet: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/sicherPKI/sicherheitsmechanismenPKI.html, 05.10.2020.

35 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 182.

Zusätzlich zum Schlüsselpaar müssen Sender und Empfänger von Bitcoins über einen Bitcoin-Wallet verfügen. Der Bitcoin-Wallet ist ein digitaler Geldbeutel. Er wird durch eine Software realisiert, die sich Sender und Empfänger jeweils auf ihren Endgeräten installieren müssen. Die Wallet-Software hilft bei der benutzerfreundlichen Darstellung des Kontostandes. Dieser digitale Geldbeutel ist notwendig, da keine digitalen Coins (Geldeinheiten) im buchstäblichen Sinne existieren.[36] Um die Anzahl der zur Verfügung stehenden Bitcoins einer spezifischen Bitcoin-Adresse zu berechnen, muss ein Saldo der vergangenen Transaktionen dieser einen Adresse berechnet werden. Weiter werden durch das Bitcoin-Wallet die Schlüsselpaare automatisiert verwaltet und der digitale Geldbeutel hilft bei der Erstellung und Ausführen einer Transaktion.[37]

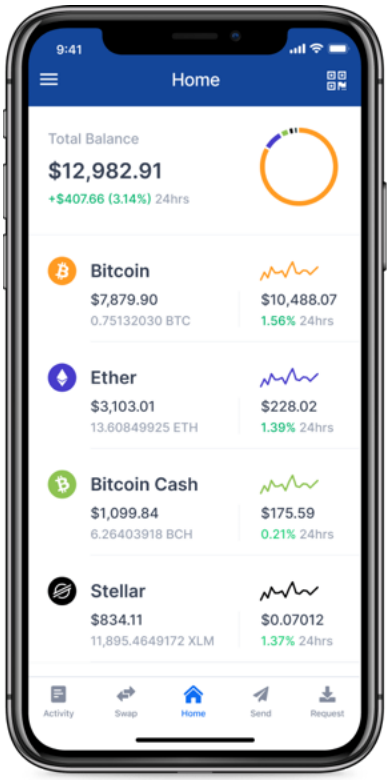

Abb. 1: Beispiel eines mobilen Krypto-Wallets[38]

Im Folgenden soll nun ein Beispiel für eine Transaktion Schritt für Schritt durchgeführt werden. Dafür wird in diesem Kapitel auf einer hohen Abstraktionsebene gestartet und technische Prozessdetails folgen in Kapitel 4. Im gewählten Beispiel ist der Student Tim sehr interessiert an

36 Vgl. Fraunhofer FIT (Hrsg.): Blockchain: Grundlagen, Anwendungen und Potenziale, White Paper 2016, S. 9.

37 Vgl. Brühl, Volker: Bitcoins, Blockchain und Distributed Ledgers, in: Wirtschaftsdienst, 97/2017, S. 136.

38 Blockchain-UK Ltd. (Hrsg.): https://www.blockchain.com.

einem gebrauchten Fernseher von Anna. Für den Fernseher verlangt Anna von Tim fünf Bitcoins. Die will Tim nun an Anna senden.

In den Grundzügen läuft die Bitcoin-Transaktion ähnlich einer Überweisung bei einer traditionellen Bank ab. Bei einer Überweisung muss durch den Sender angegeben werden, wer wie viele Geldeinheiten (Bitcoins) an wen versendet. Bezogen auf die Bitcoin-Transaktion bedeutet dies, dass Tim in seiner Wallet-Software entsprechende Informationen über die Transaktion eingeben muss:

- den zu versendenden Betrag an Bitcoin (Fünf Bitcoins),
- die Bitcoin-Adresse des Empfängers (Annas Bitcoin-Adresse),
- die Bitcoin-Adresse des Absenders (Tims Bitcoin-Adresse).[39]

Nach der Eingabe dieser Informationen in Tims Wallet-Software wird die gesamte Nachricht in das Transaktionsnetzwerk gesendet. Dort validieren die Netzwerkteilnehmer die Transaktion und Anna erhält in ihrer Wallet-Software einige Minuten später fünf Bitcoins von Tim gutgeschrieben.

In einem zentralen System würde der Prozess der Transaktionsvalidierung und Transaktionsauthentifizierung durch einen vertrauenswürdigen Intermediär, bspw. eine Bank, sichergestellt werden. In einem dezentralen System wie der Blockchain ist es die Aufgabe der Netzwerkteilnehmer, die Transaktionsinformationen auf ihre Richtigkeit zu prüfen und sowohl den Sender als auch den Empfänger zu authentifizieren. Bei diesem Verifikations-Prozess überprüfen die Miner zwei Dinge: Zum einen die Legitimität einer Transaktion und die damit verbundene Vermeidung von Doppelbuchungen.[40] Dabei prüfen die Miner, ob Tim als Sender tatsächlich über die Bitcoin-Einheiten verfügt, indem ein Saldo von allen vorhergehenden Transaktionen der Bitcoin-Adresse von Tim gebildet wird. Zum anderen prüfen die Miner die Autorisierung der Transaktion, das heißt, ob Tim auch wirklich Eigentümer der zu transferierenden Bitcoins ist.[41] Hierbei kommt erneut das Prinzip der PKI zum Einsatz. Der Absender der Bitcoins (hier Tim) signiert vor dem Versenden der Zahlungsnachricht die Transaktion mit seinem geheimen Privat Key. Diese Nachricht kann dann von den Minern mit dem vom Bitcoin-Sender (Tim) öffentlichen, zugehörigen Public Key entschlüsselt und somit auf ihre Echtheit überprüft werden (genauere Erläuterung in Kap. 4.3).[42] Bevor die Transaktionsnachricht versendet wird,

39 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 196.

40 Vgl. Mohanty, Debajani: Blockchain für Manager, Haar bei München: Franzis Verlag GmbH 2018, S. 28.

41 Vgl. Crosby, Michael; Pattanayak, Pradan; Verma, Sanjeev; Kalyanaraman, Vignesh: BlockChain Technology: Beyond Bitcoin, in: Applied Innovation Review, 2/2016, S. 10.

42 Vgl. Drescher, Daniel: Blockchain Basics: A Non-Technical Introduction in 25 Steps, Frankfurt am Main: Apress Media 2017, S. 119.

verschlüsselt der Versender (Tim) die Nachricht zusätzlich mit dem Public Key des Empfängers (Anna). Da nur Anna Zugriff auf ihren geheimen Privat Key hat, kann nur Anna die Nachricht entschlüsseln und auf die Bitcoins zugreifen. Anna ist nun neuer, eindeutiger Eigentümer der fünf Bitcoins.

Während das Senden und Empfangen einer Transaktion für den Anwender in seiner Wallet-Software sichtbar ist, passieren viele Abläufe in der Blockchain automatisiert im Hintergrund. Diese Art Blackbox soll nun in den folgenden Schritten sequentiell und chronologisch dargestellt werden.

1) Nach dem Signieren und Verschlüsseln der Transaktionsnachricht sendet Tim die Transaktionsnachricht von seiner Wallet-Software in das Bitcoin-Netzwerk. Tims Nachricht ist direkt für alle Teilnehmer im Netzwerk (Nodes) sichtbar.

2) Die Teilnehmer des Netzwerkes prüfen nun die Validität aller angefragten Transaktionen. Wird eine Transaktionsnachricht als korrekt verifiziert, wandert diese in das „Wartezimmer" (engl. Memory Pool bzw. Mempool) für alle unbestätigten Transaktionen im Bitcoin-Netzwerk.[43]

3) Aus dieser Art Warteschlange wählen die Miner zufällige Transaktionen aus und führen sie zu einem Block zusammen, der als nächstes geschürft (engl. minen) werden soll.

4) In einem mathematischen Wettbewerb versuchen alle Miner ihren individuellen Block an die Blockchain anzuhängen. Der Miner, der die mathematische Aufgabe auf seinem Rechner als erstes gelöst hat, fügt den neuen Block an seine Kopie der Blockchain an.

5) Danach versendet der schnellste Miner ein Update der Blockchain an alle Teilnehmer im Netzwerk. Die Bitcoins erscheinen in der Wallet-Software von Anna und die Transaktion ist abgeschlossen.

Für den erbrachten Rechenaufwand, der zum Lösen der mathematischen Aufgabe notwendig ist, wird der Miner mit einem bestimmten Bitcoin-Betrag belohnt. Die Entlohnung besteht aus einer bestimmten Anzahl an neu geschürften Bitcoins. Die zu lösende Rechenaufgabe wird zunehmend schwieriger, je mehr Bitcoins hergestellt werden. Zusätzlich wird die Belohnung der Miner alle 210.000 Blöcke in der Blockchain reduziert.

43 Vgl. Wenz, Daniel: Bitcoin Mempool – Einfach erklärt, Online im Internet: https://cryptomonday.de/bitcoin-mempool-einfach-erklaert/, 21.10.2019.

Die folgende Abbildung 2 visualisiert die oben erläuterte Beispieltransaktion.

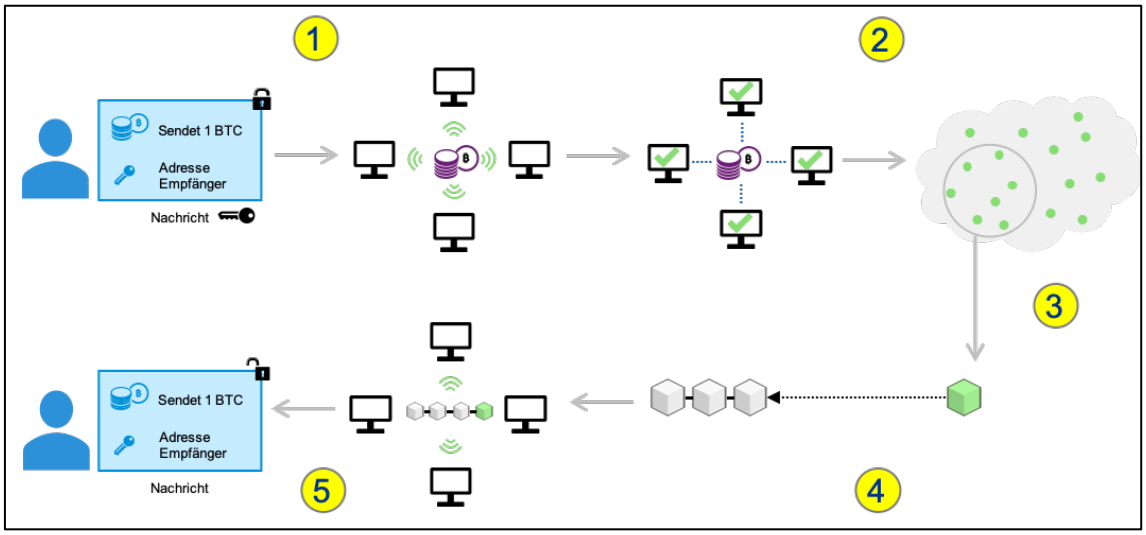

Abb. 2: Transaktionsbeispiel der Kryptowährung Bitcoin[44]

Zusammenfassend ist eine Bitcoin-Transaktion nichts anderes als ein durch digitale Signaturen gesicherter Informationsaustausch, welcher zwischen zwei Bitcoin-Wallets hin und her gesendet wird.[45] Dabei wird eine Transaktionseinheit (Bitcoin) versendet, indem der Eigentümer in einem öffentlich einsehbaren Register verändert wird.

2.4 Weitere Kryptowährungen

Die Offenlegung der gesamten Bitcoin-Technologie führt dazu, dass das Bitcoin-System von Interessierten weiterentwickelt und verwendet werden kann. Software-Entwickler haben die Möglichkeit, den originalen Quellcode zu übernehmen, beliebig anzupassen und eigene Variationen an Kryptowährungen und Transaktionsnetzwerken zu veröffentlichen. Bei den Variationen der Kryptowährungen handelt es sich um neue, klar abgetrennte Alternativsysteme, welche ein eigenes Register und eine eigene Kryptowährung besitzen.[46] Diese Klone werden „Alternative Coins“ bzw. „Altcoins“ genannt. Einen eigenen Altcoin zu erschaffen, ist für

44 Eigene Abbildung in Anlehnung an Tribowski, Christian: Blockchain: Die Technik hinter der Schlüsseltechnologie, Online im Internet: https://handelsblattintelligence.com/2019/08/02/ block chain-die-technik-hinter-derschluesseltech nologie/, 02.08.2019 und Vgl. Legder Academy (Hrsg.): What Are Public Keys and Private Keys?, Online im Internet: https://www.ledger.com/academy /blockchain/what-are-public-keys-and-private-keys, 23.10.2019.

45 Vgl. Böhme, Rainer; Christin, Nicolas; Edelman, Benjamin; Moore, Tyler: Bitcoin: Economics, Technology, and Governance, in: Journal of Economic Perspectives, 29(2)/2015, S. 216.

46 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 70.

erfahrene Entwickler relativ komplikationsfrei zu bewerkstelligen, weswegen mittlerweile mehr als fünftausend solcher Altcoins existieren (Oktober 2020).[47]

Während einige Altcoins nur identische Kopien des Bitcoin-Codes mit anderem Namen darstellen, haben andere einen erweiterten Funktionsumfang oder wesentliche Unter-schiede in der Parametrisierung (Gesamtanzahl der Coins, Transaktionsregeln, Konsens-mechanismus).[48] Trotz der unzähligen Vielfalt an Alternativen Coins ist bis heute Bitcoin die klare Nummer eins unter den Kryptowährungen. Während der Bitcoin allein eine Marktkapitalisierung von rund 165 Mrd. Euro (Oktober 2020) hat, kommen die anderen 5.450 gelisteten Altcoins zusammen gerade einmal auf eine Marktkapitalisierung von 120 Mrd. Dollar (Oktober 2020).[49]

Zusätzlich zum Klonen des ursprünglichen Quellcodes – die Klone werden auch „Soft-ware Forks“ genannt – können Altcoins auch noch in einem weiteren Fall entstehen. Dieser Fall tritt ein, wenn es innerhalb eines bestehenden Transaktionsnetzwerkes zu Unstimmigkeiten über die Konsensregeln kommt. Bei einer unvereinbaren Unstimmigkeit über die Ausrichtung der zukünftigen Validierungsregeln erfolgt eine Gabelung des Netzwerks. Ein sog. „Blockchain Fork“ entsteht. Dabei ordnen sich die Teilnehmer, je nachdem, welche Regeln sie befürworten, der alten oder der neuen Gruppe zu. Solche Gabelungen können als reine Updates passieren – Soft Fork – oder es entsteht als Folge ein neues Register, auf dem die jeweiligen Informationen zukünftig gespeichert werden – Hard Fork.[50] Bei letzterem gibt es eine Software-Änderung (= Änderung der Regeln), welche nicht rückwärtskompatibel ist. Dadurch entstehen zwei nebeneinander existierende Blockchains. Aufgrund einer Unstimmigkeit über die Skalierung bei Bitcoin entstand so am 01.08.2017 die neue „Bitcoin Cash-Blockchain“.[51] Das neue Register baut auf der Historie der originalen Bitcoin-Blockchain auf. Dadurch besitzt jeder Teilnehmer, der vor dem Fork Bitcoins gehalten hat, auch die gleiche Anzahl an Bitcoin Cash. Im Gegensatz zum Hard Fork verengt ein Soft Fork das Regelwerk und ist damit rückwärts-kompatibel.[52]

Ein Beispiel für einen Software Fork ist die Kryptowährung Litecoin. Mit dem Litecoin wird versucht, die Performance-Probleme von Bitcoin durch Optimierungen in der Funktionalität zu beheben. Ziel von Litecoin ist es, ein leichteres und schlankeres System zu gestalten und eine

47 Vgl. CoinMarketCap (Hrsg.): All Cryptocurrencies, Online im Internet: https://coinmarketcap.com/all/views/all/, 03.10.2020.

48 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 71.

49 Vgl. CoinMarketCap (Hrsg.): All Cryptocurrencies, Online im Internet: https://coinmarketcap.com/all/views/all/, 03.10.2020.

50 Vgl. Hosp, Julian: Blockchain 2.0: einfach erklärt – weit mehr als nur Bitcoin, 1. Auflage, München: Finanzbuch Verlag 2018, S. 62.

51 Vgl. Rosenberger, Patrick: Bitcoin und Blockchain – Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik, Berlin: Springer Vieweg 2018, S. 56.

52 Vgl. Blockchainwelt (Hrsg.): Hard Fork und Soft Fork – Definition und Erklärung, Online im Internet: https://blockchainwelt.de/hard-fork-und-soft-fork-blockchain-bitcoin/, 30.04.2019.

höhere Verarbeitungsgeschwindigkeit zu garantieren.[53] Während im Bitcoin-Netzwerk alle zehn Minuten ein Block entsteht, erzeugt das Litecoin-Netzwerk alle zweieinhalb Minuten einen neuen Block. Dies hat zur Folge, dass Litecoin in der Lage ist, viermal mehr Transaktionen in der gleichen Zeit durchzuführen. Weiter führt dies zu einer viermal so schnellen Generierung an neuen Währungseinheiten (Schürfprozess), was auch eine viermal so hohe Anzahl an Litecoins zur Folge hat – insgesamt 84 Millionen Einheiten. Zusätzlich benutzt Litecoin einen weniger rechenintensiven Konsens-Algorithmus. Indem der Algorithmus auf normale Computer zugeschnitten ist und keine enorme Rechenleistung bedarf, soll dies einer Zentralisierung des Minings vorbeugen.[54] Dadurch soll verhindert werden, dass ein einzelner oder wenige Miner eine Mehrheit der Gesamtrechenleistung des Netzwerks übernehmen. Der mehrheitliche Besitz von Gesamtrechenleistungen in einem Netzwerk führt zu einer erheblichen Mitgestaltung der Blöcke, was betrügerische Handlungen – z. B. doppelte Ausgaben (engl. double spending) – ermöglicht.[55]

Innerhalb des Litecoin-Netzwerks gab es ebenfalls einen Blockchain Fork und es entstand die Kryptowährung „Dash“. Diese will die Anonymität von Bitcoin erhöhen und die Performance von Litecoin erhalten. Die vermeintliche Anonymität von Bitcoin wird durch die Verwendung von alphanumerischen Adressen statt persönlichen Daten beim Versenden von Transaktionen gewährleistet. Diese Anonymität hält allerdings nur so lange an, bis einmalig die wahre Identität hinter der Adresse bekannt wird. Es wird daher argumentiert, dass Bitcoin streng genommen pseudonym, aber nicht anonym ist.[56] Die von Evan Duffield ins Leben gerufene Kryptowährung Dash versteht sich als neue Generation von Bargeld und soll absolute Anonymität garantieren. Dafür sammeln sog. Masternodes die Transaktionen der Teilnehmer und fassen sie zu Zahlungsströmen zusammen. Es gibt im Dash-Transaktionsnetzwerk keine Einzeltransaktionen, sondern lediglich Inputs und Outputs, die von den Knoten in die Zahlungsströme der Masternodes ein- und an ihrem Ziel wieder austreten.[57]

Weitere Alternative Coins versuchen nicht, einzelne Funktionalitäten des Bitcoin-Quellcodes zu verbessern, sondern wollen das Blockchain-Konzept umfassend neu entwickeln. So beispielsweise auch die Erfinder von „IOTA (Internet of Things’ Applications)“. Bei der Kryptowährung IOTA handelt es sich um ein System, welches ein sicheres Kommunikations- und

53 Vgl. Bussac, Enée: Bitcoin, Ethereum & Co. Praxiswissen Kryptowährungen und Blockchain, Berlin: Erich Schmidt Verlag GmbH & CO. KG 2019, S. 20.

54 Vgl. Cryptolist (Hrsg.): Was ist Litecoin?, Online im Internet: https://www.cryptolist.de/litecoin.

55 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 233.

56 Vgl. Bashir, Imran: Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2. Auflage, Birmingham: Packt Publishing 2018, S. 21.

57 Vgl. Rosenberger, Patrick: Bitcoin und Blockchain – Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik, Berlin: Springer Vieweg 2018, S. 57.

Zahlungsprotokoll zwischen Maschinen, Fahrzeugen und Geräten im Internet of Things ermöglichen soll. Durch die Kombination einer Kryptowährung mit Smart Contracts soll ermöglicht werden, dass Geräte miteinander kommunizieren und über eine Wenn-dann-Beziehung interagieren.[58] Statt in Blöcken werden Transaktionen im sog. Tangle-Ledger abgelegt. Dabei werden Transaktionen nicht in Blöcken, sondern in Form eines Gewirrs (engl. Tangle) direkt miteinander verbunden. Jede neue Transaktion verifiziert dabei automatisch zwei vorhergehende Transaktionen, wodurch das System nahezu unendlich skalierbar wird.[59]

Eine weitere Entwicklung innerhalb der Kryptowährungen spiegelt sich in den Stablecoins wider. Diese Kategorie an Kryptowährungen sind an einen bestimmten Vermögenswert, bspw. eine Fiatwährung, oder einen Korb an Vermögenswerten gebunden und dienen dazu, die bisher hohe Volatilität von Kryptowährung durch die Bindung an einen stabilen Vermögenswert zu minimeren.[60] Beispiele für die Stablecoins sind u. a. Libra oder Tether. Letzterer ist ein Coin, welcher den Wert des US-Dollars widerspiegelt. Dieser wird von einem Privatunternehmen ausgegeben, das durch den Kauf und Verkauf des eigenen Coins den Kurs möglichst nahe am zugrundeliegenden Vermögenswert hält.[61]

In diesem zweiten Kapitel wurden Kryptowährungen hauptsächlich mit dem Blickwinkel auf die Zahlungsfunktion betrachtet. Allerdings kann mithilfe der Blockchain-Technologie auch Software innerhalb der einzelnen Blöcke eingebunden werden. In Kapitel 3 wird deshalb Ethereum genauer betrachtet. Ethereum ist ein verteiltes System, welches das Anlegen, Verwalten und Ausführen von dezentralen Programmen bzw. Smart Contracts erlaubt.[62]

3 Smart Contracts

3.1 Blockchain und Ethereum

Bitcoin hat eine technologische Errungenschaft prominent sichtbar gemacht, die zur Abwicklung unterschiedlichster Geschäftsaktivitäten eingesetzt werden kann, die Blockchain. Die Blockchain bildet aber nicht nur das Grundgerüst zum Übertragen von Werteinheiten, sondern

58 Vgl. Rosenberger, Patrick: Bitcoin und Blockchain – Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik, Berlin: Springer Vieweg 2018, S. 50.

59 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 129.

60 Vgl. Bussac, Enée: Bitcoin, Ethereum & Co. Praxiswissen Kryptowährungen und Blockchain, Berlin: Erich Schmidt Verlag GmbH & CO. KG 2019, S. 32.

61 Vgl. Blockchainwelt (Hrsg.): Was ist Tether (USDT)? » Informationen und News, Online im Internet: https://blockchainwelt.de/tether/, 26.12.2019.

62 Vgl. Mohanty, Debajani: Blockchain für Manager, Haar bei München: Franzis Verlag GmbH 2018, S. 39.

kann auch Zustände von Geschäftsaktivitäten so abbilden, dass diese für alle Teilnehmer nachvollziehbar sind.[63]

Während die Bitcoin-Blockchain den Zweck der direkten Zahlungsabwicklung durch ein verteiltes Kontobuch verfolgt (engl. „single purpose Blockchain"), wird die „Ethereum-Blockchain" als Allzweck-Blockchain (engl. „general purpose Blockchain") bezeichnet.[64] Sie ist in der Lage, Software-Code innerhalb der Blöcke abzulegen und auszuführen. Dabei bildet die Ethereum-Blockchain selbst die Software-Infrastruktur bzw. Programmierplattform, auf der die jeweiligen Blockchain-basierten Anwendungen aufsetzen.[65] Die Ethereum-Blockchain ist als ein dezentrales Rechnernetzwerk konzipiert, auf dem jegliche Art von P2P-Werttausch – nicht nur Geldtransaktionen – ermöglicht wird.[66]

Vitalik Buterin, ehemaliger Bitcoin-Programmierer, war der Meinung, dass die Blockchain-Technologie viel mehr zu bieten hat, als die Basis für ein Zahlungssystem. Als Reaktion wurde Ethereum im Jahr 2013 von Vitalik Buterin und seinem Team entwickelt und im Whitepaper „Ethereum: A next Generation Smart Contract and Dencentralized Application Platform" erläutert.[67] Im Paper wird die Notwendigkeit eines verteilten Systems beschrieben, welches nicht nur dezentralisiertes Mining, sondern auch eine Plattform für die Entwicklung eigener Software bieten soll. Dabei soll Ethereum als ein dezentralisierter Supercomputer agieren, der gegen eine Gebühr Rechenleistung an die Entwickler von dezentralen Anwendungen vermietet.[68]

Nach einem Crowdfunding wurde 2015 die Ethereum-Plattform gelauncht. Der größte Unterschied zum Bitcoin besteht darin, dass die Ethereum-Blockchain nicht nur Transaktionen von Ether-Coins (ETH) ermöglicht, sondern auch eine Plattformfunktion umfasst. Diese Funktion befähigt die Anwender, Applikationen – wie bspw. Smart Contracts – dezentral zu speichern und auszuführen.[69] Smart Contracts sind Transaktionsprotokolle bzw. Programme, die

63 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 277.

64 Vgl. Wilkens, Robert; Falk, Richard: Smart Contracts – Grundlagen, Anwendungsfelder und rechtliche Aspekte, Wiesbaden: Springer Gabler 2019, S. 8.

65 Vgl. Mohanty, Debajani: Blockchain für Manager, Haar bei München: Franzis Verlag GmbH 2018, S. 39.

66 Vgl. Voshmgir, Shermin: Blockchains, Smart Contracts und das Dezentrale Web, Online im Internet: https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_Blockchain Studie.pdf, 30.01.2017, S. 15.

67 Vgl. Buterin, Vitalik: Ethereum: A next Generation Smart Contract and Dencentralized Application Platform, 2013.

68 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 116.

69 Vgl. Mukhopadhyay, Mayukh: Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity, Birmingham: Packt Publishing Ltd. 2018, S. 21.

automatisch und permanent die Bedingungen eines Vertrags kontrollieren und ggf. einzelne Bestimmungen eines Vertrags automatisiert ausführen (genauere Beschreibung in Kap. 3.3).[70]

Darüber hinaus bietet die Plattform die Möglichkeit, dezentrale Programme (engl. Decentralized Application, DApps) und dezentralisierte autonome Organisationen (engl. Decentralized Autonomous Organization, DAOs) anzulegen, zu verwalten und auszuführen.[71] Eine DApp bezeichnet eine dezentrale und sich selbstverwaltende Anwendung, die im Gegensatz zu heutigen Apps nicht von einer zentralen Instanz betrieben, gewartet oder weiterentwickelt wird. Eine DApp ist eine auf Smart Contracts basierende Applikation, mit welcher Benutzer interagieren können.[72] Buterin beschreibt das Konzept einer dezentralen autonomen Organisation (DAO) als System langfristiger Smart Contracts, welche Wirtschaftsgüter und kodierte Statuten eines ganzen Unternehmens beinhalten.[73] Dabei handelt es sich um voll digitale Unternehmen ohne Management und Firmensitz, die ausschließlich auf Basis von Smart Contracts auf der Ethereum-Blockchain existieren.[74] Dabei verfolgen die DAOs einen komplett basisdemokratischen Ansatz und nutzen die Schwarmintelligenz aller Teilhaber. In einem vorher festgelegten und nicht veränderbaren Programmcode ist die Geschäftsordnung festgelegt. Über Abstimmungen können die Teilhaber über zukünftige Entwicklungen des Unternehmens entscheiden. Die DAO entspricht somit einer Organisation, die demokratisch und dezentral über die Vorschläge ihrer Teilhaber abstimmt.[75]

Das Ethereum-Netzwerk besteht aus vielen, miteinander verbundenen Computern, die die Ethereum-Software betreiben. Diese werden Knoten (engl. Nodes) genannt. Zusammengeschlossen sollen alle Knoten eine Art „Weltcomputer“ bilden. Darauf aufbauend liegt das Hauptmerkmal von Ethereum, die „Ethereum Virtual Machine“ (EVM). Sie ist eine „virtuelle Maschine“ (engl. Virtual Machine, VM), die dezentral auf allen Computern der Knoten läuft.[76] Deren Ziel ist es, ein leistungsstarkes Computernetzwerk aufzubauen und den Benutzern der EVM zur Verfügung zu stellen. Dabei stellen Millionen von einzelnen Computern, die dem

70 Vgl. Wilkens, Robert; Falk, Richard: Smart Contracts – Grundlagen, Anwendungsfelder und rechtliche Aspekte, Wiesbaden: Springer Gabler 2019, S. 4.

71 Vgl. Buterin, Vitalik: Ethereum: A next Generation Smart Contract and Dencentralized Application Platform, 2013, S. 13.

72 Vgl. Bashir, Imran: Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2. Auflage, Birmingham: Packt Publishing 2018, S. 54.

73 Vgl. Buterin, Vitalik: Ethereum: A next Generation Smart Contract and Dencentralized Application Platform, 2013, S. 1.

74 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 124.

75 Vgl. Mohanty, Debajani: Ethereum for Architects and Developers: With Case Studies and Code Samples in Solidity, 1. Auflage, Berkeley, CA: Apress 2018, S. 40.

76 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 124.

Netzwerk angehören, ihre Rechenleistung gegen eine bestimmte Vergütung zur Verfügung.[77] Die VM bildet die Basis aller Arten von Smart Contracts. Sie ist von der Blockchain komplett isoliert und bildet einen eigenen Bereich. Dadurch können in der EVM Smart Contracts entwickelt und getestet werden ohne Änderungen in der Blockchain vorzunehmen. Die Programmierung von Smart Contracts auf der Ethereum-Plattform kann in drei Programmiersprachen erfolgen: Solidity, Vyper und LLL.[78]

Eine weitere Eigenschaft der Ethereum-Plattform ist die Möglichkeit, Smart Contracts jederzeit automatisch auf der EVM abzuwickeln. Das Netzwerk stellt den Benutzern für die Speicherung und Ausführung von Apps auf der EVM Speicherkapazität und Rechenleistung zur Verfügung. Für jede Speicherung und Ausführung von Applikationen auf der EVM muss der Benutzer eine festgelegte Menge an „Gas“ (= ein Bruchteil von einer Ether-Einheit) an das Netzwerk bezahlen.[79] Dabei verspricht Ethereum, dass die Applikationen und Smart Contracts jederzeit funktionstüchtig sind, solange es das Internet gibt. Denn die Smart Contracts sind auf der Ethereum-Blockchain abgespeichert. Dadurch liegen die Smart Contracts auf vielen Computern im Ethereum-Netzwerk verteilt, die ununterbrochen online sind.[80]

Zurzeit setzen viele größere Unternehmen sowie Startups auf die Ethereum-Blockchain. Das Ethereum-Projekt ist laut Experten die am weitesten entwickelte und am besten zugängliche Blockchain und damit führend in der Industrie im Bereich der Blockchain-Innovation.[81] Die Idee eine VM aufzubauen, auf der dezentralisierte Anwendungen kostengünstig und ohne Unterbrechung laufen, hat auch den Wettbewerber EOS hervorgebracht.

EOS wird von der privaten Firma block.one betrieben und versucht, durch verschiedene technische Verfahren und neue Ideen die Grundstruktur von Ethereum in einer verbesserten Form nachzuahmen.[82] Dabei will das Unternehmen hauptsächlich die Hauptmängel von Ethereum, die Gebühren und die geringe Skalierbarkeit (15-20 Transaktionen pro Sekunde) beheben. EOS

77 Vgl. Bussac, Enée: Bitcoin, Ethereum & Co. Praxiswissen Kryptowährungen und Blockchain, Berlin: Erich Schmidt Verlag GmbH & CO. KG 2019, S. 26.

78 Vgl. Mohanty, Debajani: Ethereum for Architects and Developers: With Case Studies and Code Samples in Solidity, 1. Auflage, Berkeley, CA: Apress 2018, S. 41.

79 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 122.

80 Vgl. Bussac, Enée: Bitcoin, Ethereum & Co. Praxiswissen Kryptowährungen und Blockchain, Berlin: Erich Schmidt Verlag GmbH & CO. KG 2019, S. 26.

81 Vgl. Voshmgir, Shermin: Blockchains, Smart Contracts und das Dezentrale Web, Online im Internet: https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_Blockchain Studie.pdf, 30.01.2017, S. 15.

82 Vgl. block.one (Hrsg.): EOS.IO Technical White Paper v2, Online im Internet: https://github.com /EOSIO/Documentation/blob/master/TechnicalWhitePaper.md#free-usage, 16.03.2018.

zielt darauf ab, die Gebühren für die Bereitstellung von dezentraler Speicherlösungen zu erlassen und die Skalierungsprobleme durch mehr Zentralisierung zu verbessern.[83]

3.2 Definition und Abgrenzung zu herkömmlichen Verträgen

Smart Contracts sind ein wichtiger Bestandteil im Blockchain-Framework von Ethereum. Sie erlauben es den Anwendern, Prozesse automatisch auszuführen, ohne einen Mittelsmann zu benötigen.[84] Der Begriff „Smart Contract" beschreibt dabei ein Konzept, welches jedoch schon vor der Blockchain-Technologie und dem Bitcoin entwickelt wurde. Der US-amerikanische Informatiker und Jurist Nick Szabo beschrieb erstmals Ende der 1990er Jahre das Konzept rechtsrelevanter Computerprogramme.[85] Durch webbasierte Computerprogramme sollen Verträge abgebildet und überprüft werden. Ebenso sollen Vertragsverhandlungen und -durchsetzungen technisch unterstützt werden.[86] In Kombination mit der Blockchain-Technologie lassen sich Smart Contracts in einer Vielzahl von Bereichen einsetzen.[87] Heute existieren für den Begriff „Smart Contract" (dt. intelligenter Vertrag) im Blockchain-Kontext eine große Anzahl an unterschiedlichen Definitionsansätzen und keine allgemeingültige Definition. Deswegen ist es notwendig, mehrere Definitionen zusammenzuführen, um die Eigenschaften und Funktionsweise von Smart Contracts weitreichend zu erläutern.

Smart Contracts sind Vereinbarungen über einen durchzuführenden Leistungsaustauch zwischen zwei Parteien.[88] Dabei bedienen sich die Smart Contracts der Informationstechnologie, um die Durchsetzung von Verträgen sicherzustellen, anstatt diese einer zentralen Einheit anzuvertrauen.[89] In einem intelligenten Vertrag definieren die beteiligten Parteien die Bedingungen, zu denen der Vertrag durchgeführt werden soll. Bei Erfüllung der festgelegten Bedingungen werden durch den Smart Contract automatisch autonome Handlungen initiiert, die ebenfalls vorher vertraglich vereinbart wurden.[90] Aus einem technischen Blickwinkel betrachtet,

83 Vgl. Bussac, Enée: Bitcoin, Ethereum & Co. Praxiswissen Kryptowährungen und Blockchain, Berlin: Erich Schmidt Verlag GmbH & CO. KG 2019, S. 29.

84 Vgl. Fraunhofer-Gesellschaft (Hrsg.): Blockchain und Smart Contracts: Technologien, Forschungsfragen und Anwendungen, 11.2017, S. 19.

85 Vgl. Szabo, Nick: Formalizing and Securing Relationships on Public Networks, Online im Internet: http://firstmonday.org/ojs/index.php/fm/article/view/548/469, 1.09.1997.

86 Vgl. Wilkens, Robert; Falk, Richard: Smart Contracts – Grundlagen, Anwendungsfelder und rechtliche Aspekte, Wiesbaden: Springer Gabler 2019, S. 3.

87 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 141.

88 Vgl. Kaulartz, Markus; Heckmann, Jörn: Smart Contracts – Anwendungen der Blockchain-Technologie; in Computer und Recht, 09/2016, S. 618.

89 Vgl. Meitinger, Thomas Heinz: Smart Contracts, in: Informatik_Spektrum, 40/2017, Nr. 4, S. 372.

90 Vgl. Hoffmann, Thomas; Skwarek, Volker: Blockchain, Smart Contracts und Recht, in: Informatik _Spektrum, 42/2019, Nr. 3, S. 198.

beschreiben Smart Contracts ein softwarebasiertes Protokoll (= Programmcode) auf Basis der Blockchain, welches in der Lage ist, vertragliche Logiken jeglicher Vereinbarung abzubilden.[91] Eingebettet in den Programmcode sind die Rahmenbedingungen unter denen die beteiligten Parteien den Vertrag eingehen.[92] Der Programmcode arbeitet auf Basis einer Wenn-dann-Logik. Bei Eintritt eins zuvor definierten Ereignisses (sog. Trigger-Ereignis) führt der digitale Vertrag automatisch eine ebenfalls zuvor festgelegte Aktion aus.[93] Der Smart Contract ist dabei auf einem verteilten Transaktionssystem – wie bspw. der Blockchain – gespeichert und erbt dessen Eigenschaften. Dadurch charakterisieren sich Smart Contracts durch folgende Eigenschaften:

- **Digital**: Smart Contracts sind nicht physisch an einem Ort gelagert, sondern liegen in elektronischer Form auf den Rechnern der Netzwerkteilnehmer.[94]
- **Dezentral**: Es existiert eine Vielzahl von Kopien der intelligenten Verträge, welche verteilt auf den Computern der Netzwerkteilnehmer abgespeichert sind.[95]
- **Autonom und selbstausführend**: Smart Contracts, die auf der Blockchain abgespeichert sind, prüfen stets autonom deren vordefinierte Bedingungen. Falls die Bedingungen erfüllt sind, werden automatisch die ebenfalls vordefinierten Handlungen initiiert. Dadurch ist keine zentrale Partei in die Ausführung und Durchsetzung involviert.[96]
- **Vertrauenswürdig**: Das P2P-Netzwerk kontrolliert sich jederzeit gegenseitig. Dadurch sorgt die Blockchain-Technologie für Vertrauen zwischen zwei – häufig unbekannten – Parteien, die ein Vertragsverhältnis eingehen wollen. Es wird kein vertrauenswürdiger Intermediär zur Kontrolle benötigt.[97]
- **Transparent und anonym:** Wenn Smart Contracts in einer öffentlichen Blockchain gespeichert werden, sind alle vergangenen Transaktionen protokolliert und für jeden Menschen einsehbar. Die Verwendung von Smart Contracts erfolgt über die PKI, weswegen nur anonyme Transaktionsdetails vorliegen.[98]

---

91 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Blockchain-Technologie, Online im Internet: https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html, 19.06.2017.

92 Vgl. Mohanty, Debajani: Blockchain für Manager, Haar bei München: Franzis Verlag GmbH 2018, S. 40.

93 Vgl. Wilkens, Robert; Falk, Richard: Smart Contracts – Grundlagen, Anwendungsfelder und rechtliche Aspekte, Wiesbaden: Springer Gabler 2019, S. 4.

94 Vgl. Bussac, Enée: Bitcoin, Ethereum & Co. Praxiswissen Kryptowährungen und Blockchain, Berlin: Erich Schmidt Verlag GmbH & CO. KG 2019, S. 61.

95 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 142.

96 Vgl. Kaulartz, Markus; Heckmann, Jörn: Smart Contracts – Anwendungen der Blockchain-Technologie; in Computer und Recht, 09/2016, S. 620.

97 Vgl. Mohanty, Debajani: Blockchain für Manager, Haar bei München: Franzis Verlag GmbH 2018, S. 40.

98 Vgl. Wilkens, Robert; Falk, Richard: Smart Contracts – Grundlagen, Anwendungsfelder und rechtliche Aspekte, Wiesbaden: Springer Gabler 2019, S. 14.

- **Unveränderlich und sicher**: Ein einmal abgelegter Vertrag in der Blockchain kann nicht mehr verändert werden. Dadurch wird auch eine nachträgliche Manipulation von Vertragsbedingungen verhindert. Zudem sind alle Transaktionen an und von Smart Contracts in der Blockchain dauerhaft protokolliert. Eine nachträgliche Manipulation von Kontoständen ist daher ebenfalls unmöglich.[99]

Die Bezeichnung „Smart Contracts" ist dabei durchaus missverständlich von Vitalik Buterin formuliert. Es handelt sich weder um einen Vertrag (engl. contract) im Rechtssinne noch ist zwingend eine gewisse Intelligenz (engl. smart) notwendig.[100]

Im Vergleich zu „normalen" Verträgen wird bei Smart Contracts versucht, den Faktor Mensch so weit wie möglich auszuschließen. Informationstechnologien werden genutzt, um die vordefinierten Vereinbarungen in den programmierten Smart Contracts direkt durchzusetzen. Die intelligenten Verträge initiieren automatisiert und autonom Handlungen, die zuvor vertraglich vereinbart wurden.[101] Es bedarf weder eines Intermediäres zur Ausführung und Durchsetzung des Vertrages, noch müssen die Parteien in Kontakt miteinander bleiben. Das Ziel des Verzichts auf eine menschliche Instanz ist die Reduktion von Transaktionskosten und eine Maximierung der Vertragssicherheit durch einen hohen Grad an Unabhängigkeit. Die Gefahr der Manipulation durch Dritte wird verringert, da es sich um eine automatisierte Durchführung handelt, die durch die Blockchain-Mechanismen (Konsensmechanismus) verwaltet wird.[102] Zudem wird durch den Einsatz von Softwarecode die Abwicklungsgeschwindigkeit von Smart Contracts erhöht. Dies kann zur Automatisierung von Aufgaben und zur Vereinfachung von Geschäftsprozessen genutzt werden.[103] Alle Smart Contracts in der Ethereum-Blockchain werden auf der öffentlich zugänglichen, gemeinsam genutzten Blockchain verschlüsselt gespeichert. Die Smart Contracts sind somit fälschungssicher und nach ihrer Erstellung nicht veränderbar. Diese Eigenschaften sind nicht immer nur vorteilhaft. Risiken ergeben sich insbesondere auch aus dem Fehlen einer zentralen Instanz. Bei Fehlverhalten – beabsichtigt oder unbeabsichtigt – kann nicht korrigierend eingegriffen werden.[104] Folgen durch Fehler in den Programmcodes der Smart Contracts müssen somit von den Vertragsteilnehmern getragen werden.

---

99 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Blockchain-Technologie, Online im Internet: https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html, 19.06.2017.

100 Vgl. Kaulartz, Markus; Heckmann, Jörn: Smart Contracts – Anwendungen der Blockchain-Technologie; in Computer und Recht, 09/2016, S. 624.

101 Vgl. Meitinger, Thomas Heinz: Smart Contracts, in: Informatik_Spektrum, 40/2017, Nr. 4, S. 372.

102 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Blockchain-Technologie, Online im Internet: https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html, 19.06.2017.

103 Vgl. Fraunhofer-Gesellschaft (Hrsg.): Blockchain und Smart Contracts: Technologien, Forschungsfragen und Anwendungen, 11.2017, S. 21.

104 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 142.

Weitere Risiken bestehen in den Schnittstellen zwischen Inputs und Smart Contracts bzw. zwischen Smart Contracts und Outputs. Denn Smart Contracts sind meist von Drittquellen und deren Datenqualität abhängig. Solche Drittquellen, die Echtweltdaten der Blockchain zur Verfügung stellen, werden als „Orakel" (engl. Oracle) bezeichnet.[105] Diese sind beispielsweise Wetterdaten, die dem Computerprogramm als Input dienen. Die Verlässlichkeit solcher Informationen ist äußerst wichtig.[106]

Aus rechtlicher und regulatorischer Sicht bestehen ebenfalls gewisse Unsicherheiten. Aktuell besteht noch Unklarheit, ob Entscheidungen, die der Programmcode trifft, auch von Gerichten als verbindlich anerkannt werden.[107] Fraglich ist ebenfalls, ob Marktteilnehmer ein Verfahren akzeptieren werden, in der Gerichte bei illegitimen oder ineffizienten Entscheidungen keine Eingriffsrechte haben. Denn für Verbraucher oder Privatanleger ist der Programmcode mit den niedergeschriebenen Vertragsbedingungen meist nur schwer verständlich.[108] Zudem sind Verträge mit der Eigenschaft der Unveränderbarkeit bisher nicht in unserer Rechtskultur bekannt. Bei Smart Contracts ist weder ein Rücktritt vom Vertrag noch eine nachträgliche Anpassung des Vertrages möglich.[109] Ebenso ist ungeklärt, wer bei Betrugsfall eines Orakels die Haftung trägt.[110]

3.3 Funktionsweise anhand eines Versicherungsbeispiels

Bei der Kombination eines digitalen Vertrags mit der Blockchain-Technologie stellen die gesamten Netzwerk-Teilnehmer sicher, dass die Smart Contracts zwischen zwei Parteien garantiert ausgeführt werden. Dabei wird die Funktion einer neutralen, vertrauenswürdigen dritten Partei durch die Blockchain übernommen. Durch diese Kombination aus intelligenten Verträgen und der vertrauensschaffenden Blockchain-Technologie kann eine Vielzahl von Prozess-Automatisierungen ermöglicht werden. Die Eigenschaften der Smart Contracts (vgl. Kap. 3.2), die vor allem durch das Zusammenspiel mit den dezentralisierten Systemen aufkommen, bringen zahlreiche Vorteile. Beispielsweise können Transaktionskosten gesenkt, Abwicklungs-

105 Vgl. Skwarek, Volker: Eine kurze Geschichte der Blockchain, in: Informatik_Spektrum, 42/03. 2019, S. 163.

106 Vgl. Wilkens, Robert; Falk, Richard: Smart Contracts – Grundlagen, Anwendungsfelder und rechtliche Aspekte, Wiesbaden: Springer Gabler 2019, S. 14.

107 Vgl. Hoffmann, Thomas; Skwarek, Volker: Blockchain, Smart Contracts und Recht, in: Informatik _Spektrum, 42/2019, Nr. 3, S. 198.

108 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Blockchain-Technologie, Online im Internet: https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html, 19.06.2017.

109 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 164.

110 Vgl. Cap, Clemens H.: Grenzen der Blockchain, in: Informatik_Spektrum, 42/03. 2019, S. 194.

geschwindigkeiten erhöht und Vertragsrisiken der Parteien minimiert werden.[111] Durch die beschriebenen Vorteile entstehen viele neue Möglichkeiten, wie Geschäftsprozesse effizienter und sicherer gestaltet werden können. In Folge dessen können neue Geschäftsmodelle und Tarife entstehen, die wesentliche Vorteile für den Endkonsumenten bringen können.[112]

Vereinfacht kann auf technischer Ebene der Smart Contract als ein Programmcode betrachtet werden, der bei Eintritt eines Zustands oder Erfüllung einer Bedingung A automatisch Aktion B ausführt. Die vereinfachte Funktionsweise von Smart Contracts folgt somit dem Schema: Wenn A eintritt, dann führe B aus.[113] Das heißt, bei Eintritt einer zuvor im Smart Contract festgelegten Bedingung bzw. eines Ereignisses A (Input) führt der Vertrag automatisch die ebenfalls zuvor definierte Aktion B (Output) aus.[114] Folglich müssen beim Aufsetzen bzw. Programmieren von intelligenten Verträgen Inputs und Outputs vorab definiert werden. Diese werden auch als Rahmenbedingungen des Smart Contracts bezeichnet und gleichen den Vertragsbedingungen eines juristischen Vertrags.[115]

Das bekannteste Beispiel zur Beschreibung der Funktionsweise ist der Warenautomat (engl. vending machine) und stammt von Nick Szabo, dem Erfinder der Smart Contracts.[116] Werden in einen Warenautomaten ausreichend Geldeinheiten eingeworfen und wird eine Produktauswahl getroffen, erhält die anfragende Person die gewünschte Ware. Im Vergleich zu einem traditionellen Supermarkt ist bei der Warenautomat-Transaktion kein Mensch für die Abwicklung unmittelbar beteiligt. Stattdessen wird die Abwicklung voll automatisiert ausgeführt.[117] Das Prinzip dahinter ist eine einfache, oben beschriebene Wenn-dann-Funktion. Wenn genügend Geldeinheiten zur angefragten Ware in den Automaten eingeworfen werden, dann gibt der Automat automatisch die Ware frei. Auf digitaler Ebene funktioniert ein Smart Contract auf identische Weise. Dies wird in Tabelle 1 dargestellt.

111 Vgl. Finck, Michèle: Grundlagen und Technologie von Smart Contracts, in: Smart Contracts, Hrsg.: Fries, Martin; Paal, Boris P., Tübingen: Mohr Siebeck GmbH und Co. KG 2019, S. 6.

112 Vgl. Fraunhofer-Gesellschaft (Hrsg.): Blockchain und Smart Contracts: Technologien, Forschungsfragen und Anwendungen, 11.2017, S. 7.

113 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 141.

114 Vgl. Wilkens, Robert; Falk, Richard: Smart Contracts – Grundlagen, Anwendungsfelder und rechtliche Aspekte, Wiesbaden: Springer Gabler 2019, S. 4.

115 Vgl. Sillaber, Christian; Waltl, Bernhard: Life Cycle of Smart Contracts in Blockchain Ecosystems, in: Datenschutz und Datensicherheit (DuD), 41/2017, S. 498.

116 Vgl. Szabo, Nick: Formalizing and Securing Relationships on Public Networks, Online im Internet: http://firstmonday.org/ojs/index.php/fm/article/view/548/469, 1.09.1997.

117 Vgl. Borselli, Angelo: Smart Contracts in Insurance: A Law and Futurology Perspective, in: InsurTech: A Legal and Regulatory View, Hrsg. Marano, Pierpaolo; Noussia, Kyriaki, Cham: Springer Nature Switzerland AG 2020, S. 103.

	Beispiel Warenautomat	Smart Contract auf digitaler Ebene
Input / Trigger	Auslöser ist der Geldeinwurf und die Auswahl der Ware durch eine bestimmte Tastenkombination.	Auslöser für den intelligenten Vertrag ist ein digital prüfbares Ereignis.
Durch-führung	Abgleich und Prüfung der geforderten Ware mit den eingeworfenen Geldeinheiten.	Der Programmcode des Smart Contracts verarbeitet und prüft die vordefinierten Bedingungen.
Output	Ausgabe der Ware.	Auf Basis der erfüllten Bedingungen initiiert der Smart Contract einen Output.

Tab. 1: Vergleich eines Smart Contracts mit einem Warenautomaten[118]

Ein Smart Contract, der auf der Blockchain-Technologie basiert, kann in insgesamt vier Lebenszyklen unterteilt werden: Schaffung, Einfrieren, Ausführung und Beendigung (engl. Create, Freeze, Execute, Finalize).[119] Während der Schaffensphase werden die Rahmenbedingungen des Vertrags (online oder offline) definiert und in einen Code umgewandelt. Im nächsten Schritt wird der Softwarecode an die Teilnehmer der Blockchain versendet und nach der Verifizierung durch die Nodes der bestehenden Blockchain angehängt. Dieser Prozessschritt wird Einfrieren genannt, da ab diesem Zeitpunkt von niemandem mehr eine Veränderung im Vertrag bzw. Code vorgenommen werden kann. Während der Ausführungsphase kooperiert der Smart Contract mit den externen Datenquellen (Orakel) und überprüft automatisch die vorher definierten Bedingungen. Bei Erfüllung der Bedingungen werden die Outputs initiiert. Nachdem der Smart Contract ausgeführt wurde, wird in der letzten Phase der Smart Contract abgeschlossen. Dabei werden alle neuen Zustandsinformationen und Transaktionen in der Blockchain gespeichert.

Um die Funktionsweise von Smart Contracts verständlich aufzuzeigen, wird im folgenden Abschnitt das Anwendungspotenzial von Smart Contracts anhand eines Beispiels aus der Praxis erläutert. Bei dem gewählten Beispiel handelt es sich um eine intelligente Versicherung für Flugverspätungen und Flugannullierungen. Dabei schließt der Versicherungsnehmer mit der Versicherung einen Smart Contract ab. Dieser Vertrag ist auf einer Blockchain gespeichert und beinhaltet die Rahmenbedingungen der Versicherungspolice. Als Input dient eine öffentliche Datenquelle (Orakel), die Informationen über Verspätungen und Annullierungen protokolliert. Bei einer Verspätung oder Annullierung des versicherten Flugs gemäß den Rahmenbedingungen des Vertrags (Input), löst der Smart Contract automatisch die Auszahlung der versicherten Summe aus (Output). Dabei können nach Vertragsabschluss weder Versicherungsnehmer noch die Versicherung Einfluss auf den Prozess nehmen oder den Smart Contract im Nachhinein

118 Eigene Abbildung.

119 Vgl. Sillaber, Christian; Waltl, Bernhard: Life Cycle of Smart Contracts in Blockchain Ecosystems, in: Datenschutz und Datensicherheit (DuD), 41/2017, S. 499.

verändern. Dies bietet den Vorteil, dass die Vertragsparteien sich kein gegenseitiges Vertrauen entgegenbringen müssen, sondern lediglich die Rahmenbedingungen des Smart Contracts verstehen müssen.[120]

In diesem konkreten Beispiel wird von einer fiktiven Versicherungsgesellschaft „InsureFly" eine automatisierte Police für Flugverspätungen und Flugannullierungen „Pay When Delay" angeboten. Die Arbeitnehmerin Maria würde gerne für ihren Flug am 17. Oktober 2020 von Frankfurt am Main nach London (Flugnummer: LH 171020) eine Versicherung abschließen. Falls ihr Flug verspätet ist oder annulliert wird, würde Maria gerne einen Teil oder den gesamten Preis (300 €) erstattet haben.

Das Unternehmen InsureFly bietet der Versicherungsnehmerin Maria die folgenden Rahmenbedingungen an:

- Falls ihr Flug mehr als 2 Stunden verspätet ist, bekommt die Versicherungsnehmerin 50% des Flugpreises zurückerstattet. Unter der Bedingung, dass der Flug trotzdem ohne eine Annullierung durchgeführt wird.
- Bei einer Annullierung des Flugs wird 100% des Flugpreises an die Versicherungsnehmerin zurückerstattet.
- Die Input-Daten über die Flüge zur Messung der Verspätung bzw. Annullierung werden über eine externe Datenquelle (Orakel) bezogen. Hierfür werden Daten der Webseite www.flightradar24.com verwendet.
- Der Preis für die Versicherung beträgt 1% des Ticketpreises.

Die Versicherungsnehmerin Maria ist mit den Rahmenbedingungen einverstanden und will die Versicherungspolice für ihren Flug von Frankfurt am Main nach London am 17. Oktober 2020 (Flugnummer LH 171020) abschließen. Der genaue Ablauf und die Funktionsweise des Smart Contracts wird nun sequentiell dargestellt und in Abb. 3 visualisiert.

Einzige Voraussetzung für die Durchführung ist ein digitaler Gelbeutel in Form einer Wallet-Software bei allen Beteiligten, die mit der Blockchain kompatibel ist und auf der sich der Smart Contract befindet. Dies ist notwendig, um Transaktionen zwischen den Vertragsparteien durchzuführen. Der Smart Contract selbst besitzt ebenfalls einen digitalen Geldbeutel, um potentielle spätere Zahlungsforderungen von den Parteien im Vorhinein einzufordern.

120 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 142.

1. Die Versicherungsgesellschaft InsureFly stellt ihre Rahmenbedingungen der Versicherungsnehmerin Maria zur Verfügung. Diese ist mit den Konditionen einverstanden und gibt ihre Flugdaten für den zu versichernden Flug auf der Webseite des Unternehmens ein.
2. Die Rahmenbedingungen und die Flugdaten von Maria werden in einen Smart Contract (Programmcode) eingearbeitet. Die Versicherungsnehmerin und die Versicherungsgesellschaft schließen den Smart Contract mit den oben beschriebenen Rahmenbedingungen ab. Dies erfolgt über die Signatur des Smart Contracts mit dem geheimen Privat Key.
3. Der unterschriebene Smart Contract wird vom Netzwerk verifiziert und in der Blockchain abgelegt. Von nun an ist der Smart Contract von keiner Partei mehr veränderbar bzw. manipulierbar.
4. Der Smart Contract zieht nun automatisch die potentiell maximalen Zahlungsanforderungen der Gegenparteien ein. Bei einer Annullierung des Flugs muss InsureFly maximal 300 € an Maria zahlen. Maria muss in jedem Fall die Kosten in Höhe von 1% des Flugpreises (3 €) an die Versicherung zahlen. Durch das Einziehen der maximalen Zahlung wird eine spätere automatische Durchführung sichergestellt, ohne auf die zukünftige Zahlungsfähigkeit der Parteien vertrauen zu müssen.
5. Am geplanten Abflugdatum prüft der Smart Contract in regemäßigen Abständen selbst, ob die vordefinierten Bedingungen erfüllt sind. Dafür kooperiert der Smart Contract mit dem Orakel, um Informationen (Input) über den Flug von Maria zu erhalten. Die Webseite (Orakel) übermittelt dem Smart Contract die Daten, dass der Flug mit der Flugnummer LH 171020 annulliert wurde. Die Daten vom Orakel vergleicht der Smart Contract nun mit den festgelegten Rahmenbedingungen.
6. Output: Da der Flug von Maria annulliert wurde, sind die Bedingungen für eine 100%-Auszahlung des Flugpreises erfüllt. Die Wallet-Software des Smart Contracts initiiert eine Transaktion in Höhe von 300 € an den digitalen Geldbeutel von Maria.
7. In der Blockchain werden alle neuen Transaktionen und Informationen über den Ausgang der Versicherung festgehalten.

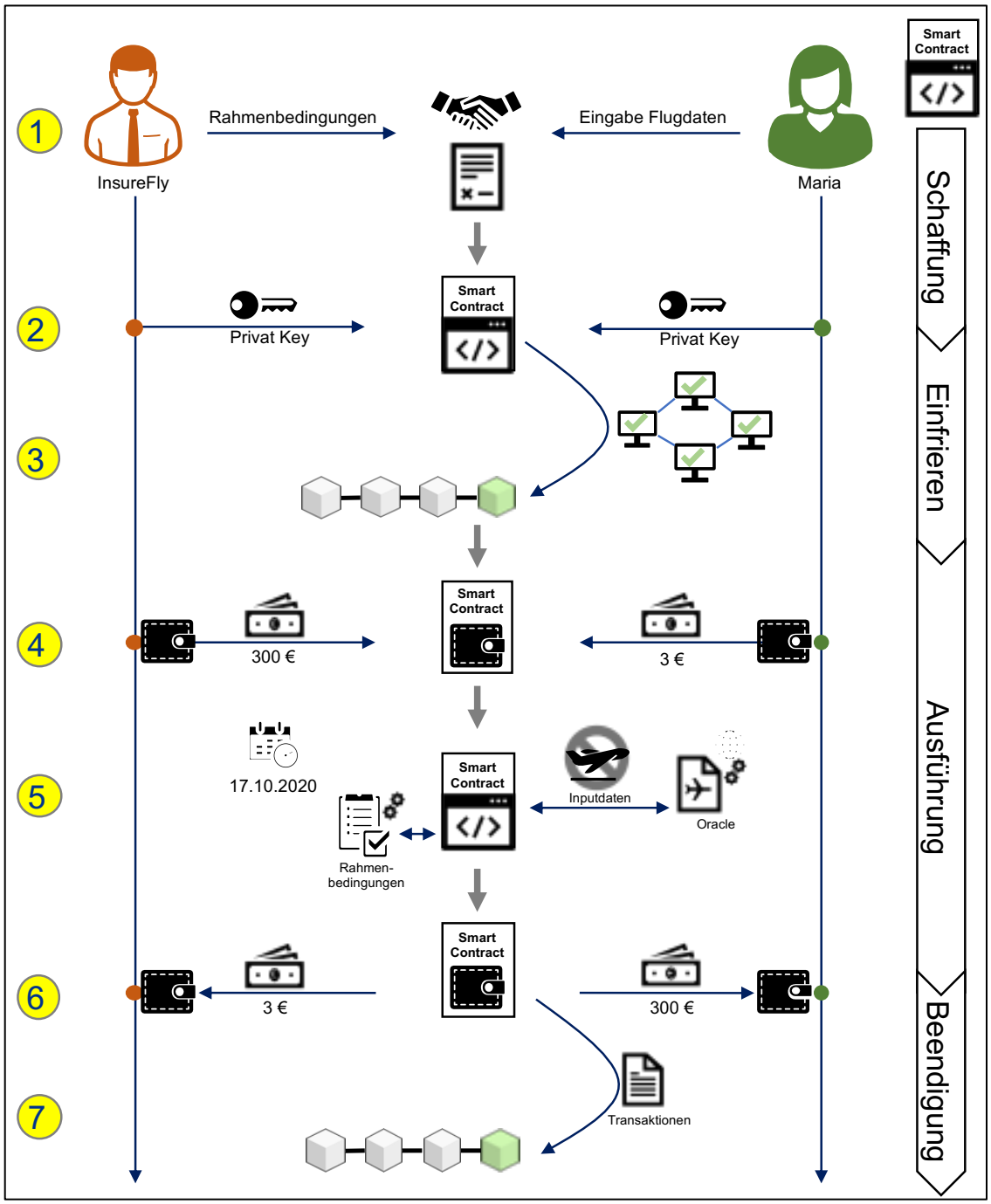

Abb. 3: Ablauf eines Smart Contracts anhand einer Versicherung[121]

3.4 Weitere Anwendungsgebiete und -beispiele

Beim Konzept der Smart Contracts handelt es sich nicht um Verträge im rechtlichen Sinne, dennoch ermöglicht ein Smart Contract, durch Regeln und Ausführungsanweisungen vorgegebene Prozesse auf der Blockchain zu automatisieren und dezentral auszuführen. Dadurch

121 Eigene Abbildung.

eröffnet sich ein enormes Automatisierungspotenzial.[122] Anwendungsmöglichkeiten finden sich von der Logistik über die Verwaltung bis hin zum Finanzsektor. Denn ein Smart Contract ist in der Lage, Berechnungen durchzuführen, Informationen abzuspeichern und automatisiert Transaktionen durchzuführen. Dadurch könnten ganze Branchen disruptiert werden, da intelligente Verträge das Marktplatzsystem automatisieren und es den Parteien ermöglichen, ohne gegenseitiges Vertrauen zwischen den beteiligten Parteien zusammenzuarbeiten.[123] Die Blockchain übernimmt dort die Funktion einer neutralen und vertrauenswürdigen dritten Partei. Dies führt zu Vorteilen, welche Kosten, Effizienz und Sicherheit beeinflussen.

Im folgenden Abschnitt soll auf weitere Anwendungsbeispiele eingegangen werden, die durch Smart Contracts möglich werden. Dabei werden exklusiv Beispiele aus der Sharing Economy erläutert, da dort ein enormes Anwendungspotenzial besteht. Das Potenzial liegt vor allem in der großen Menschenmenge begründet, die durch die Sharing Economy verbunden wird und der Notwendigkeit, verbindliche Vereinbarungen zwischen unbekannten Parteien abzuschließen. In einer Studie des Fraunhofer Instituts wird die Sharing Economy beschrieben als ein Konzept „des Wirtschaftens basierend auf dem Teilen bzw. gemeinschaftlichen Nutzen vorhandener Ressourcen, das es Kunden ermöglicht, auf Güter, Produkte und Dienstleistungen bei Bedarf zuzugreifen“.[124] Dabei werden Ressourcen nicht mehr von einer alleinstehenden Person gekauft und genutzt, sondern gemeinsam gekauft, benutzt und verliehen. Typische Kennzeichen der Sharing Economy sind das gegenseitige Bereitstellen und Ausleihen von Gütern, Produkten, Dienstleistungen und Räumen bzw. Flächen wie bspw. Fahrräder, Autos, Kleider, Wohnungen oder ganze Häuser.

Die Sharing Economy kann in Zukunft maßgeblich von der Blockchain-Technologie profitieren. Zum einen durch die vertrauenswürdige und transparente Speicherung von Informationen. Zum anderen durch den automatisierten Leistungsaustausch mit Hilfe von Smart Contracts. Intelligente Verträge können beispielsweise bei der Vermietung von Autos oder Wohnungen, bei der Kommunikation, dem Datenaustausch sowie bei der selbstausführenden Zahlungsabwicklungen zwischen intelligenten Geräten, wie intelligente Schlösser oder intelligente

122 Vgl. Fraunhofer-Gesellschaft (Hrsg.): Blockchain und Smart Contracts: Technologien, Forschungsfragen und Anwendungen, 11.2017, S. 8.

123 Vgl. Patel, Dhiren; Shah, Keivan; Shanbhag, Sanket; Mistry, Vasu: Towards Legally Enforceable Smart Contracts, in: Blockchain – ICBC 2018, Hrsg: Goos, Gerhard; Hartmanis, Juris; van Leeuwen, Jan, Cham: Springer International Publishing AG 2018, S. 153.

124 Spindler, Helge; Martinetz, Simone; Friz, Daniel: Strukturstudie »BWSHARE« Gemeinschaftliche Nutzung von Ressourcen – Chancen und Herausforderungen der Sharing Economy für die etablierte Wirtschaft in Baden-Württemberg, Hrsg: Bauer, Wilhelm in: Fraunhofer Institute für Arbeitswirtschaft und Organisation IAO, 2015, S. 21.

Wassersensoren, helfen.[125] Dadurch sorgen intelligente Verträge unter anderem für geringere Transaktionskosten und eine gesteigerte Abwicklungsgeschwindigkeit.[126]

Durch den automatisierten Datenaustausch bietet vor allem die Vermietung von Wohnraum (bspw. einer Ferienwohnung) vielfältige Anwendungsmöglichkeiten von Smart Contracts. In Zukunft könnte der Smart Contract den Mietvertrag zwischen dem Vermieter und dem Mieter widerspiegeln.[127] Dabei ist innerhalb des programmierten intelligenten Vertrags festgelegt, welche Gebühr und Kaution vorab durch den Mieter zu bezahlen sind. Erst nach der Durchführung dieser Transaktion erhält der Mieter durch den Smart Contract die Berechtigung die Wohnung zu betreten. Durch die autonome Kommunikation zwischen digital gesteuerten Wohnungsschlössern und dem Smart Contract kann die Nutzung des Kunden erst freigeschaltet werden, wenn die entsprechenden Gebühren bezahlt sind. So kann der Smart Contract dem elektronisch gesicherten Schloss Anweisungen über die Dauer der Berechtigung erteilen. Physische Schlüsselübergaben könnten dadurch der Vergangenheit angehören. Darüber hinaus kann die Nutzung von Wasser, Strom und Gas durch den Smart Contract automatisch vom digitalen Geldbeutel des Mieters abgebucht werden. Daten hierfür stellen intelligente Wasser-, Strom- und Gaszähler zur Verfügung, die mit dem Internet verbunden sind. Alle Transaktionen zwischen den Beteiligten werden in der Blockchain protokolliert und sind, wie der Smart Contract selbst, transparent für die Beteiligten einsehbar.

Im direkten Beispiel des Carsharings zeigen sich sowohl Anwendungspotenziale auf privater Seite als auch auf Seiten der Autobauer. Private Haushalte können ihr Fahrzeug in der Zeit, in der sie dieses nicht nutzen, an andere Privatpersonen vermieten. Smart Contracts ermöglichen dabei eine einfache und sichere Vermietung durch direkte und automatisierte Zahlung der Nutzungsgebühren und weiteren Transaktionen wie Parkgebühren, Maut oder das Aufladen an der Ladestation. Vorteil ist der wegfallende Verwaltungsaufwand für den Vermieter.[128] Weiter sorgt die automatisierte Zahlungsabwicklung für einen sicheren und vertrauensvollen monetären Ausgleich zwischen den beiden Parteien. Für Hersteller von Fahrzeugen wird die Option ermöglicht, statt eines einmaligen Verkaufs einen langfristigen und regelmäßigen Cashflow durch das Vermieten oder das Leasen von Autos zu realisieren.[129] Bei der Vermietung schließt der

125 Vgl. Wilkens, Robert; Falk, Richard: Smart Contracts – Grundlagen, Anwendungsfelder und rechtliche Aspekte, Wiesbaden: Springer Gabler 2019, S. 19.

126 Vgl. Anzinger, Heribert M.: Smart Contracts in der Sharing Economy, in: Smart Contracts, Hrsg.: Fries, Martin; Paal, Boris P., Tübingen: Mohr Siebeck GmbH and Co. KG 2019 S. 35.

127 Vgl. Teuteberg, Frank; Tönnissen, Stefan: Smart Contracts, in: WISU-Kompakt – Das Wirtschaftsstudium (Hrsg.), 5/2017, S. 566-567.

128 Vgl. Wilkens, Robert; Falk, Richard: Smart Contracts – Grundlagen, Anwendungsfelder und rechtliche Aspekte, Wiesbaden: Springer Gabler 2019, S. 19.

129 Vgl. Kaulartz, Markus; Heckmann, Jörn: Smart Contracts – Anwendungen der Blockchain-Technologie; in Computer und Recht, 09/2016, S. 618.

Kunde kurz vor der Nutzung des Autos einen Smart Contract mit dem Auto ab. In dem intelligenten Vertrag sind die Rahmenbedingungen der Nutzung geregelt. Durch die autonome Kommunikation zwischen dem Smart Contract, der Wallet-Software des Kunden und dem Auto öffnet sich das Türschloss des Autos nach der Zahlung der Gebühren automatisch. Ebenso wären zukünftig Geschäftsmodelle denkbar, in denen autonom arbeitende Maschinen (bspw. selbstfahrende Fahrzeuge) Dienstleistungen wie Taxifahrten ohne die Interaktion mit einem Menschen anbieten. Die Fahrzeuge selbst würden dabei direkt ihr Geld durch den Personentransport verdienen, können bei Wartungsbedarf diesen selbständig melden und in beide Richtungen direkt abrechnen.[130]

Neben den Beispielen aus der Sharing Economy und der in Kapitel 3.4 vorgestellten Möglichkeit Versicherungen zu automatisieren, gibt es ebenso weitere vielversprechende Anwendungsbereiche in anderen Branchen. Selbst die Musikindustrie könnte von Smart Contracts profitieren. Denn vom Schreiben eines Songs bis zum Verkauf sind viele Anteilseigner beteiligt, die vom Verkauf des Songs profitieren. Die Nutzung von Smart Contracts würde die Bezahlmodalitäten transparent aufschlüsseln und Einnahmen automatisiert zu den vordefinierten Anteilen an die Beteiligten auszahlen.[131] Grundlegend bestehen Anwendungsmöglichkeiten überall dort, wo sich Abläufe und Prozesse digital eindeutig darstellen und überprüfen lassen. Diese Prozesse können mithilfe von Smart Contracts automatisiert werden. Vor allem in Situationen, in denen vorher eine vertrauenswürdige dritte Partei benötigt wurde, lassen sich mit Smart Contracts und der Blockchain-Technologie Vorteile erzielen. Allerdings muss zur vollen Ausnutzung des Potenzials in allen Anwendungsmöglichkeiten auf regulatorischer Ebene Klarheit geschaffen werden. Nur dann werden Unternehmen auf die neue Technologie zugreifen und diese in ihre Geschäftsprozesse und in neue Geschäftsmodelle einbauen.[132]

Im Kapitel 2 und 3 wurde ein Fokus auf die Anwendungen auf Blockchain-Basis gelegt. Kapitel 4 wird nun auf den Fokus auf die Blockchain-Technologie selbst richten. Dazu werden zunächst kryptografische Grundlagen erläutert. Aufbauend darauf erfolgt eine technische Einordnung und eine detaillierte Beschreibung der Funktionsweise der Blockchain-Technologie.

130 Vgl. Fraunhofer-Gesellschaft (Hrsg.): Blockchain und Smart Contracts: Technologien, Forschungsfragen und Anwendungen, 11.2017, S. 23.

131 Vgl. Rosenberger, Patrick: Bitcoin und Blockchain – Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik, Berlin: Springer Vieweg 2018, S. 99.

132 Vgl. Anzinger, Heribert M.: Smart Contracts in der Sharing Economy, in: Smart Contracts, Hrsg.: Fries, Martin; Paal, Boris P., Tübingen: Mohr Siebeck GmbH and Co. KG 2019, S. 53.

4 Die Blockchain-Technologie

4.1 Grundlagentechnologie der Blockchain

Daten werden heute zunehmend in elektronischer Form ausgetauscht. Dabei wird der Schutz vor unerlaubtem oder unerwünschtem Lesen sowie vor der Verfälschung dieser Daten immer wichtiger. Kryptografie wird daher mit dem Ziel eingesetzt Vertraulichkeit, Authentizität, Integrität und Anonymität zu erreichen und Daten vor ungewollter Manipulation zu schützen.[133] Das Blockchain-System basiert vor allem auf zwei kryptografischen Elementen. Zum einen wird eine Public Key Infrastructure (PKI) eingesetzt, um die Transaktion eines Assets von unberechtigten Personen auszuschließen. Zum anderen werden Hash-Funktionen benutzt, um Veränderung und Manipulation der Blockchain zu verhindern.

Public Key Infrastructure: Das Prinzip der PKI gehört zu den asymmetrischen Verschlüsselungsverfahren.[134] Bei den asymmetrischen Verschlüsselungsverfahren wird im Gegensatz zu den symmetrischen Verschlüsselungsverfahren nicht nur ein einziger Schlüssel zur Ver- und Entschlüsselung der Nachricht verwendet. Stattdessen wird ein Schlüsselpaar erzeugt, bestehend aus einem privaten Schlüssel (Privat Key) und einem öffentlichen Schlüssel (Public Key). Bei der Erstellung wird zunächst der geheime private Schlüssel erzeugt und durch eine mathematische Einwegfunktion ein zugehöriger öffentlicher Schlüssel.[135] Der öffentliche Schlüssel ist somit immer dem zugehörigen privaten Schlüssel logisch verbunden. Die Einwegfunktion ermöglicht es, sehr einfach ausgehend von dem privaten Schlüssel den öffentlichen Schlüssel zu berechnen. Es ist jedoch praktisch unmöglich, die Umkehrfunktion auszuführen, d. h., von einem öffentlichen Schlüssel auf den zugehörigen privaten Schlüssel zu schließen. Vorteil der asymmetrischen Verschlüsselung ist die einseitige Anwendung der Schlüssel des Schlüsselpaares entweder für die Verschlüsselung oder für die Entschlüsselung einer Nachricht. Eine Nachricht, welche mit einem der beiden Schüssel verschlüsselt wurde, kann somit nur mit dem jeweils anderen Schlüssel entschlüsselt werden und umgekehrt.[136] Weiter kann der private Schlüssel des asymmetrischen Schlüsselpaars zur Erstellung und Überprüfung einer digitalen Signatur verwendet werden. Bei der Autorisierung von Transaktionen sind digitale Signaturen essentiell,

133 Vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet, 4., überarbeitete und erweiterte Auflage, Wiesbaden: Springer Gabler 2014, S. 7 und Vgl. Bussac, Enée: Bitcoin, Ethereum & Co. Praxiswissen Kryptowährungen und Blockchain, Berlin: Erich Schmidt Verlag GmbH & CO. KG 2019, S. 14.

134 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Public Key Infrastrukturen (PKIen), Online im Internet: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/sicherPKI/sicherheitsmechanismenPKI.html, 05.10.2020.

135 Vgl. Hosp, Julian: Blockchain 2.0: einfach erklärt – weit mehr als nur Bitcoin, 1. Auflage, München: Finanzbuch Verlag 2018, S. 54.

136 Vgl. Vornberger, Oliver: Kryptografie und Bitcoin, in: WISU-Kompakt – Das Wirtschaftsstudium (Hrsg.), 6/2014, S. 744.

da diese nur vom Eigentümer des privaten Schlüssels erstellt werden können, aber von allen Teilnehmern mit Hilfe des öffentlichen Schlüssels verifiziert werden können.[137]

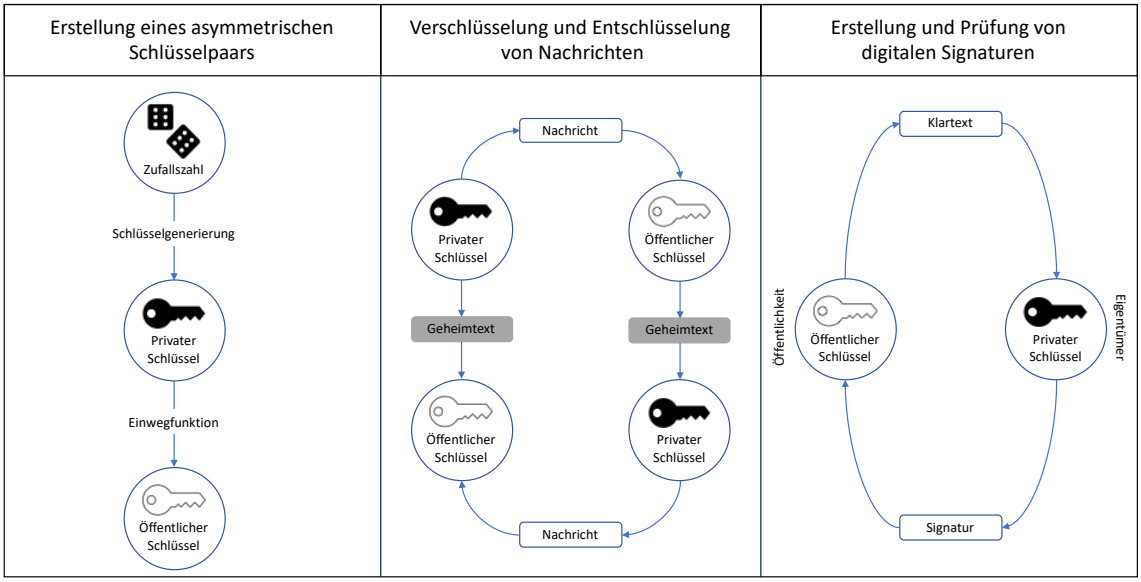

Abb. 4: Schematische Darstellung der asymmetrischen Verschlüsselung und der digitalen Signatur[138]

Innerhalb eines Blockchain-Netzwerkes gehört jedes Schlüsselpaar genau zu einer Person. Das Schlüsselpaar wird meist von einer Wallet-Software erstellt. Die Blockchain-Technologie nutzt asymmetrische Kryptografie für zwei Aspekte:

- Die Identifizierung von Konten: Bei den Kontonummern von Anwenderkonten in der Blockchain handelt es sich um öffentliche kryptografische Schlüssel. Dadurch kann eine Zuordnung von Eigentümer und Eigentum erfolgen.
- Die Autorisierung von Transaktionen: Mit Hilfe von digitalen Signaturen kann die Authentizität einer Transaktionsnachricht nachgewiesen werden.[139]

Weiterführende detailierte Erklärungen zu Verschlüsselungsverfahren finden Sie in den Arbeitspapieren der Professur für BWL und Wirtschaftsinformatik der Justus-Liebig-Universität Gießen.[140]

137 Vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet, 4., überarbeitete und erweiterte Auflage, Wiesbaden: Springer Gabler 2014, S. 17.

138 Eigene Abbildung in Anlehnung an Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 145.

139 Vgl. Drescher, Daniel: Blockchain Basics: A Non-Technical Introduction in 25 Steps, Frankfurt am Main: Apress Media 2017, S. 119.

140 Vgl. Schmoranz, Paul W.; Schick, Lukas; Schwickert, Axel: Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete, in: Arbeitspapiere WI, Nr. 2/2020 und Schwickert, Axel; Schick, Lukas: macOS – Verschlüsseln, Entschlüsseln und Signieren von E-Mails, in: Arbeitspapiere WI, Nr. 4/2019 und Schwickert, Axel C.; Schick; Lukas; Schramm, Laura; Hein, Melanie: Verschlüsseln,

Hashfunktionen und Hash-Baum (engl. Merkle-Tree): Eine Hashfunktion ist ein Algorithmus, der eine Zeichenfolge von beliebiger Länge in eine Zeichenfolge mit fixer Länge umwandelt. Dadurch erzeugen die kryptographischen Hashfunktionen für beliebige Daten einen eindeutigen digitalen Fingerabdruck, der Hashwert genannt wird.[141]

Die Hashfunktionen zeichnen sich durch die folgenden Eigenschaften aus:[142]

- *deterministisch:* Gleiche Eingabeinformationen enden immer im identischen Hashwert. Jede Diskrepanz im Hashwert wird durch eine Diskrepanz in den Eingabedaten verursacht. Eine Abweichung im Hashwert wird schon von einem Leerzeichen oder einer anderen Groß- und Kleinschreibung verursacht.
- *pseudozufällig:* Der von der Hashfunktion ausgegebene Hashwert verändert sich auf unvorhergesehene Weise, wenn die Eingabeinformationen abgeändert werden. Eine einzige kleine Änderung in den Eingabedaten resultiert in einem stark abweichenden unvorhersehbaren neuen Hashwert.
- *Einwegfunktionen:* Praktisch ist es unmöglich, mit Wissen über den Hashwert Rückschlüsse über die Ursprungsdaten zu ziehen. Anders ausgedrückt: Es existiert keine mathematische Umkehrfunktion, um von einem bestimmten Hashwert zurück zu den Eingabedaten zu gelangen.
- *kollisionsresistent:* Es ist praktisch unmöglich, einen zweiten Dateninput zu finden, der denselben Hashwert ausgibt. Folglich ist der Hashwert eine eindeutig identifizierbare Ausgabe des Dateninputs ähnlich eines Fingerabdrucks.

Die oben beschriebenen Eigenschaften werden in Tabelle 2 anhand des sicheren Hash-Algorithmus (engl. secure hash algorithm) SHA-256 visualisiert, welcher auch in der Bitcoin-Blockchain verwendet wird.

Entschlüsseln und Signieren von Dateien und E-Mails – Reader zur WBT-Serie, in: Arbeitspapiere WI, Nr. 1/2019, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2019.

141 Vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet, 4., überarbeitete und erweiterte Auflage, Wiesbaden: Springer Gabler 2014, S. 17.

142 Vgl. Drescher, Daniel: Blockchain Basics: A Non-Technical Introduction in 25 Steps, Frankfurt am Main: Apress Media 2017, S. 90 f.

Input	Output mit SHA-256
Wirtschaftsinformatik	7c00371c7b410ee6d5ef5cc3a05bfcf6b5f064b645ab28794af10d62d6739d24
wirtschaftsinformatik	29863e205fb571694de1d46488f20cb90c394fc2237ee806d189fc2675c79371
Professur für BWL und Wirtschaftsinformatik	54ab0ba93ddd6c67bcaf3d921a3f0a7478622b8bb3712d5ab6fc8f392d887d21

Tab. 2: Verschlüsselungsbeispiele mit dem SHA-256 Hash-Algorithmus[143]

Innerhalb der Blockchain-Technologie werden Hashfunktionen und Hashwerte für unterschiedliche Zwecke genutzt. In einem dezentralen Transaktionsnetzwerk fallen große Mengen an Transaktionsdaten an. Die Transaktionsdaten werden durch Hashfunktionen in ein standardisiertes Format gebracht und mit einer eindeutigen digitalen Signatur versehen.[144] Die Manipulationssicherheit wird ebenfalls durch Hashwerte und dem Konzept des Hash-Baums ermöglicht. Ziel ist es, einmal abgespeicherte Transaktionen in den Blöcken und ganze Datenblöcke innerhalb der Blockchain fälschungssicher zu halten. Dazu fasst der Hash-Baum innerhalb eines jeden Blocks die einzelnen Hashwerte der Transaktionen zu einem gesamthaften Hashwert zusammen, Wurzel des Hash-Baums (engl. Merkle-Root) genannt (vgl. Abb. 5). Da die kleinste Änderung in einer Transaktion eine Veränderung im Hashwert und somit in der Wurzel des Hash-Baums bedeutet, können mithilfe von Hash-Bäumen Daten veränderungssensitiv gespeichert werden. Jede Manipulation fällt direkt auf.

Bestandteile eines Blocks: Jede Blockchain besteht aus einzelnen Bausteinen, die Blocks genannt werden. Jeder Block innerhalb der Blockchain besteht wiederum aus einem Block-Header (dt. Kopf eines Blocks) und einem Block-Body (dt. Körper eines Blocks) (vgl. Abb. 5). Die wesentlichen Bestandteile des Block-Headers sind:[145]

- *Referenz:* Innerhalb der Referenz wird der Hashwert des vorherigen Blocks eingetragen. Der Hashwert des vorherigen Blocks ist der Hashwert aller Bestandteile aus dem Header des vorherigen Blocks. Dieses Referenzieren bildet die Grundlage der Kettenstruktur (engl. chain) der Blockchain.
- *Zeitstempel:* Der Zeitstempel beinhaltet Angaben zum Zeitpunkt der Blockerstellung.
- *Nonce:* Die Abkürzung steht für einen Einmal-Code (engl. number only used once) und ist eine Zufallszahl, die die Einzigartigkeit der Transaktionen garantiert.

143 Eigene Abbildung, Output berechnet mit: Thesing, Henrik: Hashgenerator, Online im Internet: https://hashgenerator.de, 15.09.2020.

144 Vgl. Fraunhofer-Gesellschaft (Hrsg.): Blockchain und Smart Contracts: Technologien, Forschungsfragen und Anwendungen, 11.2017, S. 10.

145 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 197 f.

- *Merkle-Root:* Die Wurzel des Hash-Baums repräsentiert die Gesamtheit aller Transaktionen des Blocks.

Die einzelnen Transaktionen sind nicht Bestandteil des Block-Headers. Die einzelnen Transaktionen inklusive ihrer Hashwerte und dem Hash-Baum befinden sich im Block-Body. Die Merkle-Root kann als Bindeglied zwischen dem Kopf und dem Körper des Blocks gesehen werden. Diese garantiert, dass keine Transaktionsdaten unbemerkt verändert werden können.

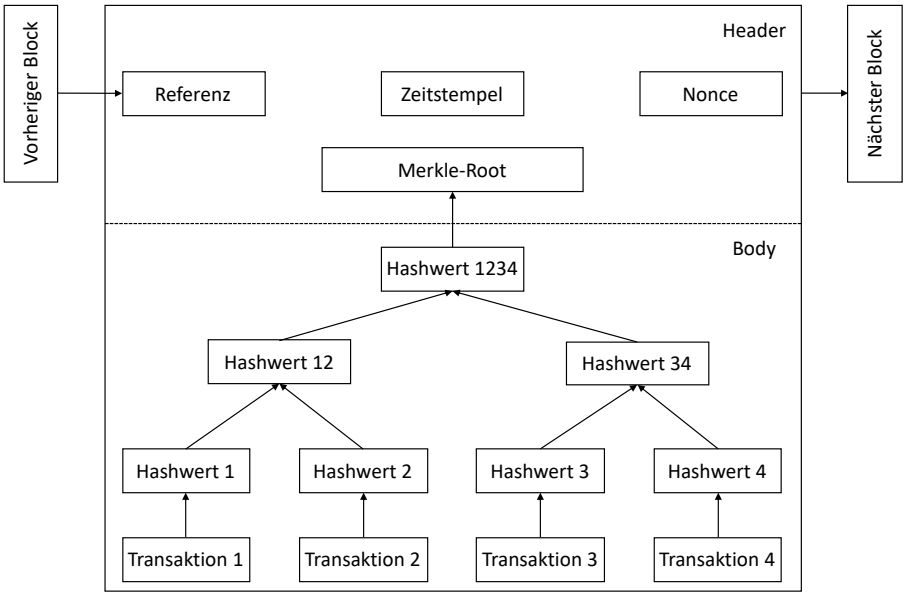

Abb. 5: Die interne Struktur eines Blocks[146]

4.2 Definition und Abgrenzung zur Distributed-Ledger-Technology

Bevor in die Definitionen der Blockchain-Technologie eingestiegen wird, sollte zunächst die Frage beantwortet werden, welches Problem die Blockchain-Technologie überhaupt lösen will bzw. mit welchem Hintergrund dieses Technologie-Konzept entwickelt wurde. Die Blockchain-Technologie löst das Problem, wie digitale Informationen (bspw. Transaktionsdaten) vertrauenswürdig ohne eine zentrale Verwaltungsstelle unveränderbar abgespeichert werden können und auf die jeder Teilnehmer des Netzwerkes Zugriff hat.[147] Das Problem, einen vertrauensvollen Informationsaustausch zwischen unbekannten Parteien in einem dezentralen System zu schaffen, ist bekannt als das Problem der byzantinsichen Generäle.[148] Korrumpierte

146 Vgl. Wang, Bozhi; Chen, Shiping; Yao, Lina; Liu, Bin; Xu, Xiwei; Zhu, Liming: A Simulation Approach for Studying Behavior and Quality of Blockchain Networks, in: Blockchain – ICBC 2018, Hrsg. Chen, Shiping; Zhang, Liang-Jie; Wang, Harry, Cham, Switzerland: Springer International Publishing AG 2018, S. 20.

147 Vgl. Hosp, Julian: Blockchain 2.0: einfach erklärt – weit mehr als nur Bitcoin, 1. Auflage, München: Finanzbuch Verlag 2018, S. 54.

148 Vgl. Rosenberger, Patrick: Bitcoin und Blockchain – Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik, Berlin: Springer Vieweg 2018, S. 66.

Teilnehmer können falsche Informationen verbreiten und dadurch Widersprüche hervorrufen. In einem zentralen System gibt es nur eine einzige Autoritätspartei, die dies verhindert. Die Blockchain-Technologie löst dieses Problem mit Hilfe des Konsensverfahrens (vgl. Kap. 4.3) und einem offenen, universell zugänglichen Register. Die Konsensverfahren helfen dem Netzwerk, sich gemeinsam auf eine einzige für alle Teilnehmer identische Version der Blockchain zu einigen.[149]

Da sich die Blockchain erst am Anfang ihrer Entwicklung befindet, haben sich bisher keine einheitlichen Definitionen durchgesetzt. Der Überblick über die populärsten Definitionen soll einen Einblick über die unterschiedlichen Betrachtungsweisen und Fokussetzungen der Blockchain-Technologie geben. Anschließend werden die wesentlichen Merkmale der Technologie herausgearbeitet und erläutert.

Imran Bashier definiert eine Blockchain als ein „ständig wachsendes, sicheres, gemeinsam genutztes Aufzeichnungssystem“[150], welches durch die Teilnehmer eines verteilten Rechnernetzes verwaltet und aktualisiert wird. Den Fokus auf die Anordnung der Daten setzt Walport in seiner Definition. Walport beschreibt die Blockchain als eine Art Datenbank, in der Einträge in Blöcken gruppiert werden.[151] Diese Blöcke sind in chronologischer Reihenfolge über eine kryptografische Signatur miteinander verknüpft. Die BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht), die vor allem für die Regulierung von Kryptowährungen und Kryptowerten im Deutschen Finanzsektor zuständig ist, definiert die Blockchain als „fälschungssichere, verteilte Datenstrukturen, in denen Transaktionen in der Zeitfolge protokolliert, nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet sind.“[152] Eine weitaus technischere Definition für die Blockchain wird von Julian Hosp benutzt: Eine Blockchain ist eine „dezentrale und meist öffentliche Datenbank, in der Vorgänge durch kryptografische Hashes als Merkel Tree (dt. Hash-Baum) über viele Computer hinweg aufgezeichnet werden, sodass die Datensätze nicht rückwirkend geändert werden können.“[153] Aus den genannten Definitionen gehen die Folgenden wesentlichen technischen Merkmale und deren Auswirkungen hervor.

149 Vgl. Teuteberg, Frank; Tönnissen, Stefan: Blockchains, in: WISU-Kompakt – Das Wirtschaftsstudium (Hrsg.), 3/2017, S. 287.

150 Bashir, Imran: Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2. Auflage, Birmingham: Packt Publishing 2018, S. 16.

151 Vgl. Walport, Mark: Distributed Ledger Technology: beyond blockchain – A report by the UK Government Chief Scientific Adviser, Online im Internet: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, 19.01.2016.

152 Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Blockchain-Technologie, Online im Internet: https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html, 19.06.2017.

153 Hosp, Julian: Blockchain 2.0: einfach erklärt – weit mehr als nur Bitcoin, 1. Auflage, München: Finanzbuch Verlag 2018, S. 50.

Dezentrales P2P-System: Peer-to-Peer-Netze (dt. Rechner-Rechner-Verbindungen) sind Rechnernetze, bei denen alle Rechner im Netz gleichberechtigt zusammenarbeiten. Im dezentralen P2P-Konzept gibt es keinen zentralen Server und alle Teilnehmer kommunizieren direkt miteinander. Diese Eigenschaft ermöglicht es, Transaktionen direkt zw. den Peers (dt. Gleichgestellter) auszutauschen, ohne dass ein Dritter involviert ist.[154] Die Blockchain ist eine dezentral verteilte Transaktionsdatenbank zur Speicherung und zum Transfer von Daten und Werten. Spezifikum eines dezentralisierten P2P-Systems wie der Blockchain ist die Verteilung der Steuerung und der Datenhaltung auf viele Knoten im Netzwerk, anstatt einer Abhängigkeit zu einem einzigen Master-Knoten. Dabei sind alle Teilnehmer des Netzwerkes (full nodes) gleichberechtigt und besitzen eine vollständige Kopie der kompletten Blockchain. Die unabhängigen Rechner (Netzwerkknoten) kommunizieren direkt miteinander und synchronisieren sich in regelmäßigen Abständen selbst, ohne einen zentralen Intermediär zu benötigen. Der Ausfall einzelner Rechner beeinflusst dabei weder die anderen Rechner noch führt es zu einem Informationsverlust, da die Daten von den Netzwerk-Teilnehmern redundant gespeichert werden. Dadurch gibt es keinen Single-Point of Failure (dt. einzelner Ausfallpunkt) und ein Totalausfall der Blockchain ist sehr unwahrscheinlich.[155]

Unveränderbarkeit der Aufzeichnungen (engl. immutable): Unveränderbarkeit im Zusammenhang mit der Blockchain bedeutet, dass einmal in der Blockchain aufgenommene Daten nicht mehr im Nachhinein manipuliert oder verändert werden können.[156] Durch die „Nur-Anfügen-Regel“ (engl. append-only rule) können neue Datenblöcke jeweils nur angehängt, aber keine schon bestehenden verändert werden.[157] Die Blockchain bietet dadurch ein lückenloses, chronologisch angeordnetes, permanent nachvollziehbares und im Nachhinein nicht veränderbares Register von Transaktionen. Diese Eigenschaft der Unveränderbarkeit wird durch die kryptografischen Konzepte gewährleistet (vgl. Kap. 4.1). Die Unveränderbarkeit von Daten trägt maßgeblich zur Integrität im dezentralen System bei. Die Blockchain kann deshalb die Rolle des vertrauenswürdigen Intermediärs übernehmen.[158]

Kryptografisch sichere Speicherung (engl. cryptographically secure): Alle Transaktionsdaten werden innerhalb der Blockchain kryptographisch sicher abgespeichert. Für die sichere

154 Vgl. Bashir, Imran: Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2. Auflage, Birmingham: Packt Publishing 2018, S. 16.

155 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 28.

156 Vgl. Drescher, Daniel: Blockchain Basics: A Non-Technical Introduction in 25 Steps, Frankfurt am Main: Apress Media 2017, S. 153.

157 Vgl. Bashir, Imran: Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2. Auflage, Birmingham: Packt Publishing 2018, S. 17.

158 Vgl. Tapscott, Don; Tapscott, Alex: Die Blockchain Revolution – Wie die Technologie hinter Bitcoin nicht nur das Finanzsystem, sondern die ganze Welt verändert, 5. Auflage, Kulmbach: Börsenmedien AG 2018, S. 52.

Speicherung der Daten kommen unterschiedliche Protokolle und Algorithmen zum Einsatz. Durch die Verwendung von Hash-Funktionen und Hash-Bäumen kann die Sicherheit der Daten innerhalb der Blockchain gegenüber Manipulation und Missbrauch gewährleistet werden.[159] Zur Eigentumssicherung und Eigentumsübertragung werden asymmetrische Schlüssel eingesetzt. Die Konsensmechanismen der Blockchain überprüfen und verifizieren die zu verarbeitenden Transaktionen der Netzwerkteilnehmer und sorgen für eine identische Version des digitalen Registers auf allen Netzwerkknoten.[160]

Transparenz und Vertrauen: Innerhalb des Blockchain-Systems ist jede Transaktion für alle Teilnehmer sichtbar. Die Teilnehmer des verteilten Transaktionssystems werden durch eine individuelle Zeichenfolge – dem öffentlichen Schlüssel (Public Key) oder dem Hashwert des öffentlichen Schlüssels – repräsentiert.[161] Dadurch werden keine personenbezogenen Daten an andere Nutzer weitergegeben und alle Teilnehmer bleiben trotz der Transparenz pseudonym. Durch die vollkommene Transparenz jeglicher Transaktionen bei gleichzeitiger Privatsphäre wird das Vertrauen in das jeweilige Blockchain-System gestärkt.[162] Zudem sorgen die kryptografischen Konzepte zur fälschungssicheren Speicherung der Daten sowie die redundante dezentrale Speicherung für Vertrauen in die Blockchain. Neben den öffentlichen Blockchains (engl. Public Blockchains) – welche bisher in dieser Arbeit betrachtet wurden – existieren zudem private Blockchains (engl. Privat Blockchains), die teilweise Lese- und Schreibrechte beschränken. Die vier Klassifikationen von Blockchains werden in Tab. 3 erläutert.

159 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 69.

160 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Blockchain-Technologie, Online im Internet: https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html, 19.06.2017.

161 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 127.

162 Vgl. Bashir, Imran: Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2. Auflage, Birmingham: Packt Publishing 2018, S. 24.

	Berechtigung notwendig	berechtigungsfrei
Öffentliche Blockchain	Öffentlich einsehbar, um als Teilnehmer beizutreten, ist eine Berechtigung notwendig. Beispiel: Logistik- und Transport-Blockchain.	Jeder kann der Blockchain beitreten und die komplette Blockchain kann von außen eingesehen werden. Beispiel: Blockchain für Kryptowährungen wie Bitcoin.
Private Blockchain	Diese Blockchains sind öffentlich nicht einsehbar und es wird eine Genehmigung benötigt, um ihnen beizutreten. Beispiel: Firmeneigene Blockchain.	Öffentlich nicht einsehbar, zugleich ist aber jedem der Zutritt erlaubt. Beispiel: Blockchain zur Nutzeridentifizierung (Know Your Customer - KYC).

Tab. 3: Blockchain-Kategorien[163]

Die Begriffe „Distributed Ledger (dt. verteilte Hauptbücher / Register)“ bzw. „Distributed-Ledger-Technology (DLT)“ und „Blockchain“ werden heutzutage häufig synonym verwendet. Dies ist allerdings nicht ganz zutreffend. Zunächst einmal dient der Begriff „Distributed-Ledger-Technology“ als Überbegriff für alle Technologien, die verteilte Transaktionssysteme darstellen. Der Begriff „Distributed Ledger“ steht für ein verteiltes Register, welches lediglich die gemeinsame Nutzung einer verteilten Datenbank beschreibt.[164] Daher fallen technisch gesehen alle Blockchain-Systeme unter die Kategorie DLT, während nicht unbedingt alle verteilten Register automatisch eine Blockchain abbilden.

Ein kritischer Unterschied zwischen der Blockhain-Technologie und der DLT besteht darin, dass ein verteiltes Register nicht notwendigerweise aus einer Kette von digitalen Blöcken bestehen muss. Die Blockchain ist vielmehr ein spezifischer Typ einer gemeinsam genutzten Datenbank, die aus Transaktionsblöcken besteht, welche stetig neu angehängt und durch Hash-Algorithmen verknüpft werden.[165] Es gibt allerdings auch verteilte Register, die keine Transaktionsblöcke verwenden. Ein Beispiel dafür ist R3’s Corda oder Ripple. Diese beiden verfolgen den Ansatz einer zusammenhängenden Speicherung der Datensätze, anstatt sie in Blöcken zu sortieren.[166] Da Blockchain eine Datenstruktur der Kategorie DLT ist, weisen beide ebenfalls Gemeinsamkeiten auf. Das jeweilige Register wird unter seinen Teilnehmern über mehrere Standorte oder Organisationen verteilt und bei jedem Teilnehmer redundant gespeichert. Darüber hinaus können sowohl Blockchains als auch andere Unterkategorien der DLT privat oder

163 Vgl. Drescher, Daniel: Blockchain Basics: A Non-Technical Introduction in 25 Steps, Frankfurt am Main: Apress Media 2017, S. 227 f.

164 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 31.

165 Vgl. Brühl, Volker: Bitcoins, Blockchain und Distributed Ledgers, in: Wirtschaftsdienst, 97/2017, S. 140.

166 Vgl. Bashir, Imran: Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2. Auflage, Birmingham: Packt Publishing 2018, S. 31.

auch öffentlich sein. Dies hängt jeweils vom spezifischen Anwendungszweck ab. Zudem verwenden sowohl die Blockchain-Technologie als auch DLT kryptografische Methoden wie die PKI und Hashing-Algorithmen, um die Sicherheit der Daten und die Integrität der kompletten Datenbank zu gewährleisten. Beide Technologien bauen ebenso auf einem P2P-Modell für eine direkte Kommunikation der Teilnehmer auf.[167] Die Blockchain-Technologie ist aktuell die populärste und am weitesten verbreitete DLT-Variante. Allerdings steckt die Entwicklung der Blockchain-Technologie noch in den Anfängen und es ist davon auszugehen, dass noch weitere konkurrenzfähige Alternativen auf den Markt kommen.

4.3 Technische Funktionsweise einer Blockchain

Die Nutzung von Blockchains beschränkt sich nicht nur auf Kryptowährungen und Smart Contracts. In diesem Kapitel soll daher – anknüpfend an das Kapitel 2.3 – eine allgemeine technische Funktionsweise der Blockchain-Technologie in vier Schritten erläutert werden. Der Fokus liegt dabei auf den Regeln und den unterschiedlichen Verfahren bei der Erstellung neuer Blöcke, „Mining“ genannt.

Jedes Blockchain-Netzwerk muss eine Entscheidung darüber treffen, wie festgelegt wird, wann welcher Netzwerkteilnehmer (Mining-Knoten) den nächsten Block an die Blockchain anhängen darf. Diese Entscheidung wird mittels eines Konsensverfahrens bzw. Konsensmechansimus getroffen. Dieser legt fest, auf welche Weise die Blockchain-Teilnehmer eine Einigung über Transaktionen und den neusten Zustand der Blockchain finden.[168] Im Gegensatz zu einer Bank, die z. B. die Transaktion ihrer Kunden zentral verifiziert und validiert, soll mit dem Konsensverfahren eine dezentrale, von einzelnen Organisationseinheiten unabhängige Validierung und Verifizierung der Transaktion erfolgen. Teilnehmer, die sich nicht kennen, können verlässlich Transaktionen bestätigen oder ablehnen. Die Konsensverfahren ermöglichen dabei vor allem auch einen Schutz vor Manipulation und missbräuchlicher Verwendung der Blockchain. Jede DLT arbeitet mit einem eigenen Konsensfindungsmechanismus, von denen zwei in diesem Kapitel näher betrachtet werden.

Erster Schritt – Transaktionsdefinition: Im ersten Schritt werden zunächst in jeder Blockchain-Transaktion digitale Informationen, wie bspw. eine Bitcoin-Überweisung, von einem Sender definiert und als Nachricht verpackt. Diese Transaktionsnachricht signiert der Absender

167 Vgl. Teuteberg, Frank; Tönnissen, Stefan: Blockchains, in: WISU-Kompakt – Das Wirtschaftsstudium (Hrsg.), 3/2017, S. 287.

168 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Blockchain-Technologie, Online im Internet: https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html, 19.06.2017.

mit seinem geheimen privaten Schlüssel. Im Anschluss daran wird die signierte Transaktionsnachricht an das jeweilige Blockchain-Netzwerk bzw. an die beteiligten Knoten gesendet.[169]

Zweiter Schritt – Transaktionsverifizierung: Jede neue Blockchain-Transaktion muss im Anschluss vom jeweiligen Blockchain-Netzwerk auf seine Richtigkeit überprüft werden. Bei diesem Verifikations-Prozess werden zwei Dinge überprüft: Zum einen die Legitimität der Transaktion. Die Netzwerkknoten gleichen die Informationen aus der Nachricht mit der Transaktionshistorie ab, um bspw. den Kontostand zu überprüfen. Zum anderen wird die Autorisierung der Transaktion überprüft. Das heißt, die digitale Signatur des Absenders wird auf ihre Gültigkeit geprüft und somit der Absender als wahrer Eigentümer autorisiert.[170] Die Erstellung der digitalen Signatur des Absenders und Autorisierung durch die Netzwerk-Teilnehmer wird im nächsten Abschnitt kurz erläutert und in Abb. 6 dargestellt:

Der Absender hasht seine Transaktionsnachricht, um diese in eine einheitliche Form zu bringen. Den entstandenen Hashwert verschlüsselt der Absender mit seinem geheimen privaten Schlüssel. Resultat ist eine digitale Signatur für diese spezifische Transaktionsnachricht, ohne den geheimen privaten Schlüssel freizugeben. Zur Verifizierung der Transaktion müssen die überprüfenden Netzwerkknoten die Schritte in umgekehrter Reihenfolge durchführen. Dazu nehmen die Netzwerkknoten (Nodes) die digitale Signatur und entschlüsseln sie mit dem bekannten öffentlichen Schlüssel des Absenders. Gleichzeitig hashen auch die überprüfenden Netzwerkknoten die Transaktionsnachricht und erhalten einen Hashwert. Stimmt der Hashwert der Transaktion und die entschlüsselte Signatur überein, hat der Absender bewiesen die Berechtigung zur Ausführung der Transaktion zu besitzen.[171]

169 Vgl. Fraunhofer-Gesellschaft (Hrsg.): Blockchain und Smart Contracts: Technologien, Forschungsfragen und Anwendungen, 11.2017, S. 10.

170 Vgl. Crosby, Michael; Pattanayak, Pradan; Verma, Sanjeev; Kalyanaraman, Vignesh: BlockChain Technology: Beyond Bitcoin, in: Applied Innovation Review, 2/2016, S. 10.

171 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 145 f.

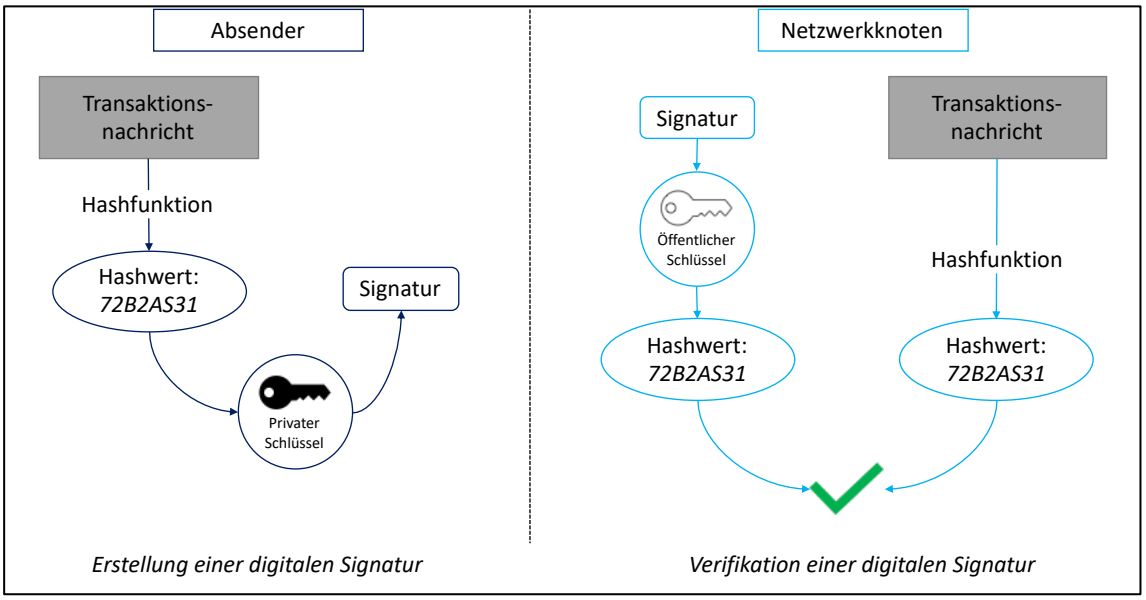

Abb. 6: Schematische Darstellung der Erstellung und Verifikation einer digitalen Signatur[172]

Nachdem eine Transaktion von den Nodes als korrekt verifiziert wurde, wandert die Transaktion in das Wartezimmer für alle unbestätigten Transaktionen (Memory Pool).

Dritter Schritt – Block-Validierung: Die Block-Validierung spiegelt die eigentliche Durchführung der Transaktion wider. Während „passive Knoten“ oder auch Validierungs-Knoten (engl. validation nodes) lediglich in der Lage sind, Transaktionen – wie im zweiten Schritt beschrieben – zu überprüfen, können Mining-Netzknoten (engl. mining nodes) auch Transaktionen in eine Blockchain aufnehmen.[173] Jeder Mining-Knoten wählt dafür beliebige, unbestätigte Transaktionen aus dem Memory Pool aus und fügt diese in einem Block zusammen, der als nächste geschürft (engl. gemined) werden soll. Dieser Prozess erfolgt aufgrund der Dezentralität des Netzwerkes bei jedem Mining-Knoten parallel, wobei sich die Transaktionen in den jeweiligen Blöcken der Miner unterscheiden. Ziel jedes einzelnen Miners ist es, ihren eigenen Block als Erster an die vorhandene Blockchain zu hängen, wodurch ein Wettbewerb zwischen den Mining-Netzknoten entsteht.[174] Wesentlicher Bestandteil des Mining-Prozesses ist der Konsensmechanismus. Mit Hilfe des Konsensmechanismus wird die missbräuchliche Verwendung der Blockchain verhindert und Einigung über die aktuelle Version der Blockchain erzielt. Somit werden beispielsweise Mehrfachausgaben (Double Spendings) durch falsche Informationen von korrumpierten Teilnehmern verhindert. Im Falle der Blockchain, die der Kryptowährung

172 Vgl. Drescher, Daniel: Blockchain Basics: A Non-Technical Introduction in 25 Steps, Frankfurt am Main: Apress Media 2017, S. 124.

173 Vgl. Sandner, Philipp; Gösele, Martin: Blockchain-Technologie, in: WISU – Das Wirtschaftsstudium (Hrsg.), 03/2018, S. 310.

174 Vgl. Vigliotti, Maria Grazia; Jones, Haydn: The Executive Guide to Blockchain – Using Smart Con-tracts and Digital Currencies in your Business, Cham: Springer Nature Switzerland AG 2020, S. 48.

Bitcoin zugrunde liegt, wird der Proof-of-Work-Konsensmechanismus verwendet. Proof-of-Work gewährleistet die Sicherheit des Bitcoin-Systems durch ressourcenintensives Versenden und Validieren zwischen den Nutzern eines Blockchain-Systems. Dabei müssen die Mining-Netzknoten einen Arbeitsnachweis erbringen, um ihren eigenen Block an die bisherige Blockchain anzuhängen.[175] Der Arbeitsnachweis für die Fertigstellung eines Blocks definiert sich durch das Lösen eines sehr rechenintensiven mathematischen Problems. Dazu muss eine beliebige Zeichenfolge im Block-Header (Nonce) so lange verändert werden, bis der Hash-Wert des Block-Headers einen vorgegebenen Zielwert unterschreitet.[176] Der Miner, der als erstes das Rätsel gelöst hat, hängt seinen Block an die bisherige Blockchain an. Das Mining neuer Blöcke in der Bitcoin-Blockchain ist bewusst ressourcenintensiv – schwierig im Ansatz und einfach in der Überprüfung – gestaltet, sodass die Anzahl der Blöcke, die täglich durch das Mining entstehen, konstant bleibt und Spam-Angriffen entgegengewirkt wird.[177]

Vierter Schritt - Block-Update: Die neuen Blöcke werden durch eine Verkettung mit der bereits bestehenden Historie der Blöcke verbunden. Die neue komplette Blockchain wird dann vom Miner als Update in das Netzwerk versendet. Beim Mining-Prozess, bestehend aus dem Validieren der Transaktion, der Aufnahme von Transaktionen in einem Block und dem Hinzufügen des neuen Blocks an die bestehende Blockchain, wird mit kryptografischen Hashfunktionen und der hierarchischen Verdichtung als Hash-Baum gearbeitet (vgl. Kap. 4.1). Dadurch lassen sich Transaktionen eindeutig in einem Block identifizieren und repräsentieren.[178]

Neben dem erläuterten Proof-of-Work Konsensmechanismus gibt es noch weitere alternative Konsensverfahren. Denn der Arbeitsnachweis (PoW), das von der Bitcoin-Blockchain eingesetzte Konsensverfahren, ist kostspielig, zeitaufwendig und verbraucht viel Energie.[179] Beim Proof-of-Stake (PoS, dt. Einsatznachweis) wird ein Konsens erzielt, wenn die Mehrheit der Inhaber aller Coins zum gleichen Ergebnis kommt.[180] Das PoS-Konsensverfahren geht davon aus, dass ein Nutzer, welcher einen Anteil (engl. stake) am System hält und somit in das System investiert ist, jeden böswilligen Manipulationsversuch verhindern will. Deshalb steigt die Wahrscheinlichkeit der Blockerzeugung durch einen Teilnehmer mit seinem wertmäßigen

175 Vgl. Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

176 Vgl. Brühl, Volker: Bitcoins, Blockchain und Distributed Ledgers, in: Wirtschaftsdienst, 97/2017, S. 137.

177 Vgl. Mohanty, Debajani: Blockchain für Manager, Haar bei München: Franzis Verlag GmbH 2018, S. 28.

178 Vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet, 4., überarbeitete und erweiterte Auflage, Wiesbaden: Springer Gabler 2014, S. 17.

179 Vgl. Egloff, Pascal; Turnes, Ernesto: Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019, S. 82.

180 Vgl. Fraunhofer-Gesellschaft (Hrsg.): Blockchain und Smart Contracts: Technologien, Forschungsfragen und Anwendungen, 11.2017, S. 11.

Anteil am gesamten Netzwerk und dem Alter der gehaltenen Coins.[181] PoS wird zum Beispiel in der Ethereum-Blockchain verwendet. DieVorteile des PoS-Mechanismus sind die geringere Rechenleistung, die benötigt wird, und die höhere Transaktionsgeschwindigkeit.[182]

4.4 Anwendungsbeispiele der Blockchain

Die Blockchain ist eine System-Infrastruktur, die eine dezentrale, transparente und unveränderbare Speicherung von Transaktionen ermöglicht.[183] Die damit verbundenen Möglichkeiten können Auswirkungen auf alle Wirtschafts- und Gesellschaftsbereiche haben. [184] Im Folgenden sollen vor allem die Bereiche Logistik, Finanzen und der öffentliche Sektor betrachtet werden. Dort sieht die Fachliteratur die meisten Potentiale.

Logistik: Der Bereich Logistik und Lieferketten gilt als einer der Bereiche, die von Blockchain-Anwendungen am meisten profitieren könnten.[185] Bei einheitlichen Daten- und Transaktionsstandards werden sich viele logistische Prozesse durch die Blockchain-Technologie automatisieren und optimieren lassen.[186] Denn die Blockchain gewährleistet eine sichere, verteilte und fehlerresistente Speicherung von Daten. Darüber hinaus kann sie das Vertrauensproblem zwischen Wertschöpfungspartnern in Bezug auf Transaktionen von monetären Werten, Vertragsabwicklungen und den Austausch von Daten lösen.[187] In einer global vernetzten Welt bestehen die Wertschöpfungsketten aus einer Vielzahl an Wertschöpfungspartnern, zwischen denen verschiedene Leistungsvereinbarungen existieren. Dabei scheint das Potential der Finanzprozesse in der Supply Chain durch den Einsatz von Smart Contracts enorm zu sein. Transaktionen können durch den Einsatz der Blockchains unabhängig von Rechnungen über Smart Contracts abgewickelt werden. Somit erlaubt die Technologie eine einfache Integration und sichere Vernetzung von verschiedenen Wertschöpfungspartnern. Insbesondere, wenn die Pläne der EZB zu einem programmierbaren Euro (engl. Central Bank Digital Currency, CBDC) umgesetzt

181 Vgl. Bashir, Imran: Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2. Auflage, Birmingham: Packt Publishing 2018, S. 37.

182 Vgl. Bussac, Enée: Bitcoin, Ethereum & Co. Praxiswissen Kryptowährungen und Blockchain, Berlin: Erich Schmidt Verlag GmbH & CO. KG 2019, S. 56.

183 Vgl. Hasan, Haya R.; Salah, Khaled: Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters, in: IEEE Access, 6/2018, S. 46781.

184 Vgl. Bullmann, Dirk: Bezahlen mit der Blockchain – wo Potentiale und Herausforderungen liegen, in: Die Zukunft ist dezentral, Hrsg.: Sandner, Philipp; Tumasjan, Andranik; Welpe, Isabelle, Norderstedt: BoD – Books on Demand 2020, S. 97.

185 Vgl. Bundesministerium für Wirtschaft und Energie; Bundesministerium für Finanzen (Hrsg.): Blockchain-Strategie der Bundesregierung – Wir stellen die Weichen für die Token-Ökonomie, 18.09.2019, S. 11.

186 Vgl. Voshmgir, Shermin: Blockchains, Smart Contracts und das Dezentrale Web, Online im Internet: https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_Blockchain Studie.pdf, 30.01.2017, S. 22.

187 Vgl. Fraunhofer (Hrsg.): Blockchain: Technologien, Forschungsfragen und Anwendungen, Positionspapier, 20.03.2017, S. 19.

werden, steht automatisierten Überweisung mit hoher Zahlungssicherheit und geringen Transaktionskosten nichts mehr im Weg.[188] Die Blockchain kann ebenso dabei helfen, Bewegungen von Objekten zuverlässig nachverfolgen zu können. Zum Beispiel wollen Konsumenten von Bio-zertifizierten Lebensmittel zunehmend Kenntnis über Produktions- und Lieferbedingungen haben. Verteilte Datenbanken bieten eine optimale Möglichkeit, transparent mit den Produktions- und Lieferinformationen umzugehen.

Finanzbereich: Die Blockchain-Technologie besitzt ebenfalls ein hohes Disruptionspotential für unterschiedliche Bereiche des Bankensektors**.** Innerhalb der Finanzbranche zeichnen sich daher aktuell die größten Aktivitäten im Bereich der Blockchain ab. Dies ist nicht verwunderlich vor dem Hintergrund, dass Banken eigentlich nur Finanzintermediäre beim Zahlungsverkehr und im Kapitalmarkthandel sind.[189] Ein heutiger Zahlungsprozess involviert mehrere Intermediäre wie Banken, Zentralbanken und Clearing-Stellen. Zahlungsprozesse – insbesondere internationale Transaktionen – sind daher kosten- und zeitintensiv. Die Blockchain könnte zu sinkenden Gebühren bei Überweisungen sowie einem geringerem Wechselkursrisiko durch eine reduzierte Abwicklungszeit führen. Kryptowährung versprechen zudem, von jedem verwendet werden zu können – bei weltweit 1,7 Mrd. Erwachsenen ohne Bankkonto ein Potential, welches nicht zu unterschätzen ist.[190]

Bei Transaktionsprozessen im Kapitalmarkt ist ebenfalls eine große Anzahl an Akteuren involviert. Dort müssen Daten kontinuierlich abgeglichen und validiert werden, weshalb hohe Kosten und lange Transaktionszeiten auftreten.[191] Intermediäre bei einer normalen Wertpapierorder wie Broker, Börsen und Clearingstellen sind eingebunden, um Sicherheit und Nachvollziehbarkeit der Transaktionen zu gewährleisten. Dies geht jedoch zu Lasten von Effizienz und Geschwindigkeit.[192] Die Blockchain-Technologie kann entsprechend vor allem bei der Abwicklung von Wertpapiertransaktionen eingesetzt werden. Kosten und Komplexität können durch

188 Vgl. Bindseil, Ulrich: Tiered CBDC and the financial system, in: ECB Working Paper Series No 2351, 01/2020, S.5.

189 Vgl. Beinke, Jan Heinrich; Tönnissen, Stefan; Samuel, Julia; Teuteberg, Frank: Blockchain im Bankensektor – Chancen, Herausforderungen, Handlungsempfehlungen und Vorgehensmodell, in: Blockchain Grundlagen, Anwendungsszenarien und Nutzungspotenziale, Hrsg.: Fill, Hans-Georg; Meier, Andreas, Wiesbaden: Springer Vieweg 2020, S. 137.

190 Vgl. The World Bank (Hrsg.): The Global Findex Database 2017 – Measuring Financial Inclusion and the Fintech Revolution, Online im Internet: https://globalfindex.worldbank.org/sites/globalfindex /files/2018-04/2017%20Findex%20full%20report_0.pdf, 2017.

191 Vgl. Fraunhofer (Hrsg.): Blockchain: Technologien, Forschungsfragen und Anwendungen, Positionspapier, 20.03.2017, S. 22.

192 Vgl. Höptner, Alexander: Neue Märkte, neue Rollen: Wie die Blockchain die Finanzwelt verändert, in: Die Zukunft ist dezentral, Hrsg.: Sandner, Philipp; Tumasjan, Andranik; Welpe, Isabelle, Norderstedt: BoD – Books on Demand 2020, S. 59.

den direkten Handel zwischen zwei Parteien (Peer-to-Peer) ohne den Einsatz von Vermittlern verringert werden.

Öffentlicher Sektor: Die Blockchain-Technologie bietet das Potential, Transparenz und Vertrauenswürdigkeit in Verwaltungsprozesse zu stärken. Innerhalb der verwaltungsinternen Kommunikation bietet die Technologie Chancen, Abläufe zu vereinfachen, insbesondere bei Verwaltungs übergreifenden Prozessen.[193] Akteure im öffentlichen Sektor treten heute wesentlich als Intermediäre auf. Bei der Registrierung und Dokumentierung von Eigentumsverhältnissen gelten bspw. Notare als vertrauenswürdige Stelle. Die Eigenschaft, Transaktionen nachweisbar, transparent und unveränderbar zu dokumentieren, bietet die Möglichkeit, Notare in Zukunft bei der Eigentumsübertragung und -dokumentierung abzulösen.[194] Die Einsatzmöglichkeiten der Blockchain-Technologie im öffentlichen Sektor sind aber weitaus vielseitiger und in einigen Ländern schon im Einsatz. Estland bietet mit dem „E-Residency-Programm“ einen Notardienst auf Blockchain-Basis an.[195] Aber auch im E-Payment Bereich, z. B. zur Bezahlung von Verwaltungsgebühren oder Studiengebühren, bietet sich die Blockchain-Technologie an.

Die Anwendungsfälle hören hier allerdings nicht auf. Die Verwendung von Tokens als Abbildung eines Inhaberrechts kann auf unterschiedlichste Bereiche eingesetzt werden, u. a. Gaming Token, Immobilien Token oder Wertpapier Token. Die Transparenz und Integrität der Blockchain-Technologie öffnet ebenfalls neue Geschäftsfelder für den Echtheitsnachweis von Zeugnissen und Zertifikaten. Weiter kann im Bereich Medizin der Datenschutz und die Sicherheit von Patientendaten enorm gesteigert werden. Wie auch in vielen anderen Bereichen der Wirtschaft und Gesellschaft stellt sich nicht die Frage wo, sondern wann die Blockchain-Technologie Einzug erhält.

5 Ausblick

Der Zukunftsforscher Roy Amara hat bereits 1960 beschrieben, wie wir Menschen den Effekt einer Technologie kurzfristig überschätzen und die langfristigen Auswirkungen einer innovativen Technologie unterschätzen.[196] Die Entwicklung des Internets mit seinen Folgen für unsere Gesellschaft bestätigt diese Erkenntnis. Gleichzeitig zeigt es, wie schwierig es ist, Vorhersagen

193 Vgl. Voshmgir, Shermin: Blockchains, Smart Contracts und das Dezentrale Web, Online im Internet: https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_Blockchain Studie.pdf, 30.01.2017, S. 21.

194 Vgl. Meitinger, Thomas Heinz: Smart Contracts, in: Informatik_Spektrum, 40/2017, Nr. 4, S. 373.

195 Vgl. Fraunhofer (Hrsg.): Blockchain: Technologien, Forschungsfragen und Anwendungen, Positionspapier, 20.03.2017, S. 25.

196 Vgl. Ratcliffe, Susan: Oxford Essential Quotations, Online im Internet: https://www.oxfordreference.com/view/10.1093/acref/9780191866692.001.0001/q-oro-ed6-00018679?rskey=O6r8bT&result=93, 12.08.2020.

über die langfristigen Effekte einer technologischen Innovation zu machen. Mehrere Aspekte weisen aber darauf hin, dass die Blockchain-Technologie – ähnlich dem Internet – viele Geschäftsbereiche beeinflussen wird: Die Blockchain-Technologie als Disintermediator löst die Rolle von vermittelnden Instanzen durch eine digitale und streng regeltreue Protokoll-basierte Variante ab.[197] Zusätzlich bietet die Technologie die Möglichkeit, weitreichende Automatisierungen und Prozessoptimierungen zu ermöglichen. Dazu müssen allerdings in Zukunft steigende Standardisierung und Regulierung im Bereich der Blockchain-Technologie Einzug erhalten. Darüber hinaus ist bedingungsloses Vertrauen in den letzten Jahren zu einem wertvollen Gut geworden. Insbesondere Datenskandale von großen Technologieunternehmen zeigen dies evident auf. Eine Technologie, die dieses wertvolle Gut als „Massenware" zu geringem Preis anbietet, sollte als sehr aussichtsreich betrachtet werden.[198]

Die Betrachtung der Blockchain-Technologie anhand des Gartner Hype Cycles (vgl. Abb. 7) gibt einen fundamentierten Überblick, in welcher Phase der Entwicklung und öffentlichen Aufmerksamkeit die Blockchain-Technologie sich aktuell befindet.[199] Positiv aus Sicht der Blockchain-Technologie ist der Fakt, dass die Blockchain-Technologie nicht mehr als nur ein einzelner Kreis dargestellt wird, sondern in unterschiedliche technologische Konzepte aufgeteilt ist (vgl. Abb. 7). Dies bestätigt die großen Chancen und Potentiale, die sich durch die Blockchain-Technologie in unterschiedlichsten Bereichen ergeben. Kritisch zu beurteilen sind jedoch die einzelnen Entwicklungsstände. Viele technologische Konzepte befinden sich noch am Anfang ihrer Entwicklung und die vollständigen Risiken sowie die Potentiale sind noch nicht umfassend bekannt. Somit stimmt der Gartner Hype Cycle mit den Meinungen vieler Experten überein, welche die Blockchain-Technologie noch ziemlich am Anfang ihrer Entwicklung sehen. Dennoch sind sich viele Experten einig, dass es keine Frage ist, ob sich Blockchain-basierte

197 Vgl. Brühl, Volker: Bitcoins, Blockchain und Distributed Ledgers, in: Wirtschaftsdienst, 97/2017, S. 140.

198 Vgl. Drescher, Daniel: Blockchain Basics: A Non-Technical Introduction in 25 Steps, Frankfurt am Main: Apress Media 2017, S. 253.

199 Vgl. Gartner (Hrsg.): Gartner Hype Cycle, Online im Internet: https://www.gartner.com/en/inform ation-technology/research/hype-cycle, 12.08.2020.

Prozesse und Dienste in der realen Wirtschaft etablieren werden, sondern lediglich, wann und wie dies der Fall sein wird.[200]

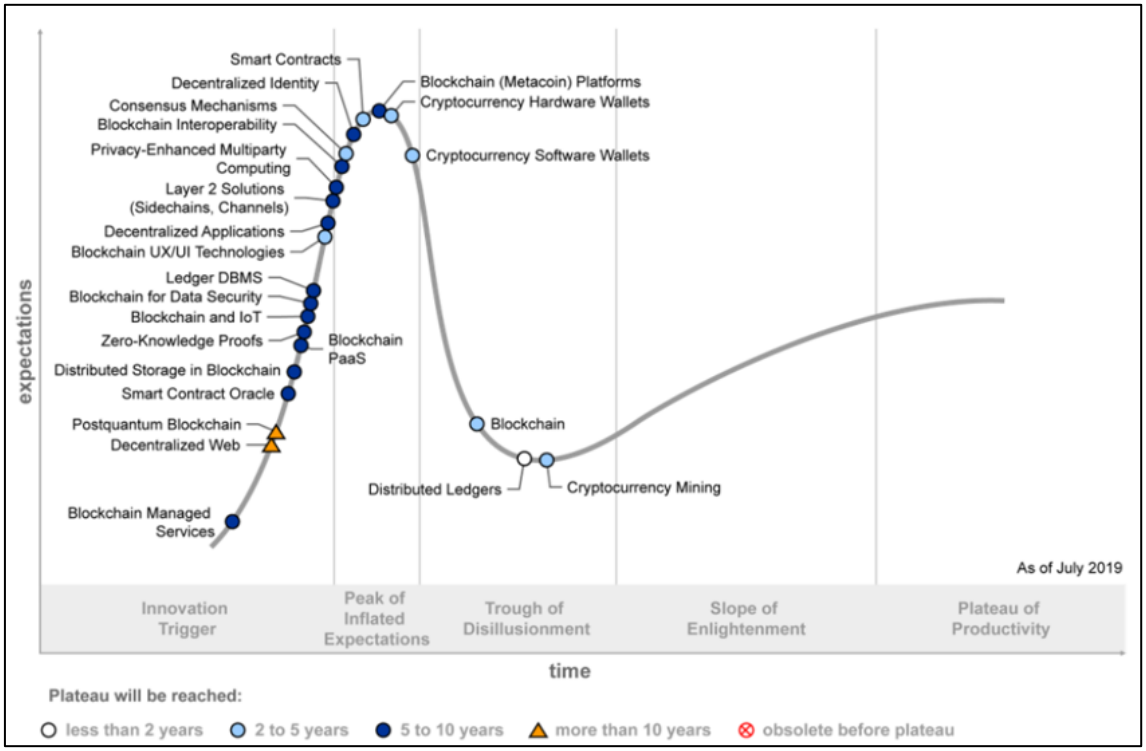

Abb. 7: Gartner Hype Cycle für die Blockchain-Technologien[201]

Die Blockchain-Technologie begründet ihre Daseinsberechtigung hauptsächlich im fehlenden Vertrauen von uns Menschen in zentralisierte Systeme. Gäbe es ein zentralisiertes System, welchem absolutes Vertrauen entgegengebracht werden könnte, wäre die Blockchain-Technologie einschließlich ihrer Anwendungen praktisch nicht notwendig. Denn ein dezentralisiertes System ist nicht unbedingt besser als ein zentralisiertes System – dies sollte nicht vergessen werden. Ein dezentralisiertes System ist mit höheren Kosten und Ressourcenverschwendung durch die benötigte Konsensbildung in dezentralen Systemen verbunden. Dazu kommen weitere technische Herausforderungen wie die fehlende Skalierbarkeit. Während der Kreditkartendienstleister Visa mehr als 50.000 Transaktionen pro Sekunde verarbeiten kann, ist die Bitcoin-

200 Vgl. Becker, Sebastian: Everything a Marketplace: Wie die Blockchain neue Geschäftsmodelle eröffnet, in: Die Zukunft ist dezentral, Hrsg.: Sandner, Philipp; Tumasjan, Andranik; Welpe, Isabelle, Norderstedt: BoD – Books on Demand 2020, S. 25.

201 Vgl. Gartner (Hrsg.): Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact, Online im Internet: https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies -are-still-five-to-10-years-away-from-transformational-impact, 08.10.2019.

Blockchain nur in der Lage ca. sieben Transaktionen pro Sekunde zu verarbeiten. Die Ethereum-Blockchain kommt immerhin auf bis zu 20 Transaktionen pro Sekunde.[202]

Eine weitere Herausforderung auf dem Weg zu etablierten Anwendungen ist die bisher fehlende Standardisierung. Es existieren über 6.500 Blockchain-Netzwerke mit verschiedensten Protokollen, Programmiersprachen und Konsensmechanismen.[203] Ebenso darf bei Anwendungen für den Endkonsumenten auch nicht die Nutzerfreundlichkeit vergessen werden und die Frage, wer den Kundensupport in einer dezentralen Gesellschaft, in der alle gleichberechtigt sein sollen, sicherstellt.

Öffentliche und genehmigungsfreie Blockchains bieten aufgrund ihrer begrenzten Skalierbarkeit und ihrer geringen Nutzerfreundlichkeit nur wenige Möglichkeiten der Kommerzialisierung für Unternehmen. Experten gehen deshalb zurzeit davon aus, dass kommerzielle Blockchain-Anwendungen in Zukunft auf private und genehmigungspflichtige Blockchain-Netzwerke setzen werden. Dafür werden sich führende Unternehmen aus einem bestimmten Sektor oder einer Branche zusammenschließen. Vorteile wie Standardisierung, Automatisierung, Prozessoptimierung und Kostensenkung werden die Unternehmen dazu motivieren.[204]

Die Blockchain-Technologie ist zwar aktuell die bekannteste, aber trotzdem nur eine einzige Kategorie im Bereich der DLT. Aktuell wird neben der Blockchain-Technologie an weiteren dezentralen Alternativen wie der Directed Acyclic Graphs (DAG), die beispielsweise bei IOTA eingesetzt wird, gearbeitet und geforscht.[205] Welches dezentrale Transaktionssystem sich in Zukunft durchsetzen wird, kann heute noch nicht mit Bestimmtheit gesagt werden.

Werden die Vor- und Nachteile sowie die Chancen und Risiken der Blockchain-Technologie gegenübergestellt, bleibt die Zukunft abhängig von mehreren Punkten. Unternehmen müssen sich auf gleiche Standards einigen und der Rechtsrahmen muss schnellstmöglich vom Gesetzgeber festgelegt werden. Nur so kann durch die Blockchain-Technologie in Zusammenspiel mit bspw. Smart Contracts Automatisierungspotentiale realisieren und zu wirklichen Effizienzgewinnen führen. Nebenbei bleibt die Frage offen, ob die Wirtschaft oder die Forschung technisch überlegenere DLT Lösungen findet oder es nur innerhalb der Blockchain-Technologie zu evolutionären Fortschritten kommt. Kleinere technische Verbesserungen und Variationen beziehen

202 Vgl. Berentsen, Aleksander; Schär, Fabian: Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017, S. 251.

203 Vgl. Finextra (Hrsg.): Remaining challenges of blockchain adoption and possible solutions, Online im Internet: https://www.finextra.com/blogposting/18496/remaining-challenges-of-blockchain-adoption-and-possible-solutions, 29.02.2020.

204 Vgl. Drescher, Daniel: Blockchain Basics: A Non-Technical Introduction in 25 Steps, Frankfurt am Main: Apress Media 2017, S. 256 f.

205 Vgl. Bashir, Imran: Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2. Auflage, Birmingham: Packt Publishing 2018, S. 591.

sich dabei auf die Vielzahl an Konzepten und Grundlagen aus der Softwareentwicklung und Informatik, darunter Hashfunktionen, Hashreferenzen, Kryptografie und Berechnungsaufgaben wie PoW. Jedes dieser Konzepte und jede dieser Technologien ist weiterhin ein Bereich der aktiven Forschung und kann Auswirkung auf die Funktionsweise der Blockchain haben.

Literaturverzeichnis

1. **Anzinger, Heribert M.:** Smart Contracts in der Sharing Economy, in: Smart Contracts, Hrsg.: Fries, Martin; Paal, Boris P., Tübingen: Mohr Siebeck GmbH and Co. KG 2019, S. 34-72.
2. **Bashir, Imran:** Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2. Auflage, Birmingham: Packt Publishing 2018.
3. **Becker, Sebastian:** Everything a Marketplace: Wie die Blockchain neue Geschäftsmodelle eröffnet, in: Die Zukunft ist dezentral, Hrsg.: Sandner, Philipp; Tumasjan, Andranik; Welpe, Isabelle, Norderstedt: BoD – Books on Demand 2020, S. 21-36.
4. **Beinke, Jan Heinrich; Tönnissen, Stefan; Samuel, Julia; Teuteberg, Frank:** Blockchain im Bankensektor – Chancen, Herausforderungen, Handlungsempfehlungen und Vorgehensmodell, in: Blockchain Grundlagen, Anwendungsszenarien und Nutzungspotenziale, Hrsg.: Fill, Hans-Georg; Meier, Andreas, Wiesbaden: Springer Vieweg 2020, S. 135-146.
5. **Berentsen, Aleksander; Schär, Fabian:** Bitcoin, Blockchain und Kryptoassets, 1. Auflage, Norderstedt: BoD – Books on Demand 2017.
6. **Bindseil, Ulrich:** Tiered CBDC and the financial system, in: ECB Working Paper Series No 2351, 01/2020.
7. **Bitcoin Wiki (Hrsg.):** Laszlo Hanyecz, Online im Internet: https://en.bitcoin.it/wiki /Laszlo_Hanyecz, 2010.
8. **block.one (Hrsg.):** EOS.IO Technical White Paper v2, Online im Internet: https:// github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md#free-usage, 16.03.2018.
9. **Blockchain-UK Ltd. (Hrsg.):** https://www.blockchain.com.
10. **Blockchaincenter (Hrsg.):** Bitcoin Kurs, Online im Internet: https://www.block chaincenter.net/ bitcoin/#kurs, 03.10.2020.
11. **Blockchainwelt (Hrsg.):** Hard Fork und Soft Fork – Definition und Erklärung, Online im Internet: https://blockchainwelt.de/hard-fork-und-soft-fork-blockchain-bitcoin/, 30.04.2019.
12. **Blockchainwelt (Hrsg.):** Was ist Tether (USDT)? » Informationen und News, Online im Internet: https://blockchainwelt.de/tether/, 26.12.2019.
13. **Böhme, Rainer; Christin, Nicolas; Edelman, Benjamin; Moore, Tyler:** Bitcoin: Economics, Technology, and Governance, in: Journal of Economic Perspectives, 29(2)/2015, S. 213-238.

14. **Borselli, Angelo:** Smart Contracts in Insurance: A Law and Futurology Perspective, in: InsurTech: A Legal and Regulatory View, Hrsg. Marano, Pierpaolo; Noussia, Kyriaki, Cham: Springer Nature Switzerland AG 2020, S. 101-127.

15. **Brühl, Volker:** Bitcoins, Blockchain und Distributed Ledgers, in: Wirtschaftsdienst, 97/2017.

16. **BTC-ECHO (Hrsg.):** Das sind die 5 krypto-freundlichsten Länder der Welt, Online im Internet: https://www.btc-echo.de/dies-sind-die-5-krypto-freundlichsten-laender-der-welt/, 30.12.2018.

17. **Bullmann, Dirk:** Bezahlen mit der Blockchain – wo Potentiale und Herausforderungen liegen, in: Die Zukunft ist dezentral, Hrsg.: Sandner, Philipp; Tumasjan, Andranik; Welpe, Isabelle, Norderstedt: BoD – Books on Demand 2020, S. 91-108.

18. **Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):** Public Key Infrastrukturen (PKIen), Online im Internet: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/sicherPKI/sicherheitsmechanismenPKI.html, 05.10.2020.

19. **Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.):** Blockchain-Technologie, Online im Internet: https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html, 19.06.2017.

20. **Bundesministerium für Wirtschaft und Energie; Bundesministerium für Finanzen (Hrsg.):** Blockchain-Strategie der Bundesregierung – Wir stellen die Weichen für die Token-Ökonomie, 18.09.2019.

21. **Bussac, Enée:** Bitcoin, Ethereum & Co. Praxiswissen Kryptowährungen und Blockchain, Berlin: Erich Schmidt Verlag GmbH & CO. KG 2019.

22. **Buterin, Vitalik:** Ethereum: A next Generation Smart Contract and Dencentralized Application Platform, 2013.

23. **Cap, Clemens H.:** Grenzen der Blockchain, in: Informatik_Spektrum, 42/03. 2019, S. 191-196.

24. **Chaum, David L.:** Untraceable electronic mail, return addresses, and digital pseudonyms, in: Communication of ACM 24(2)/1981, S. 84-88.

25. **CoinMarketCap (Hrsg.):** All Cryptocurrencies, Online im Internet: https://coinmarketcap.com/all /views/all/, 03.10.2020.

26. **CoinMarketCap (Hrsg.):** Bitcoin, Online im Internet: https://coinmarketcap.com/de/currencies /bitcoin/, 03.10.2020.

27. **Crosby, Michael; Pattanayak, Pradan; Verma, Sanjeev; Kalyanaraman, Vignesh:** BlockChain Technology: Beyond Bitcoin, in: Applied Innovation Review, 2/2016, S. 6-19.

28. **Cryptolist (Hrsg.):** Was ist Litecoin?, Online im Internet: https://www.cryptolist.de/litecoin.

29. **Dai, Wie:** B-Money, Online im Internet: http://www.wei dai.com/bmoney.txt, 1998.

30. **Drescher, Daniel:** Blockchain Basics: A Non-Technical Introduction in 25 Steps, Frankfurt am Main: Apress Media 2017.

31. **Egloff, Pascal; Turnes, Ernesto:** Blockchain für die Praxis: Kryptowährungen, Smart Contracts, ICOs und Tokens, 1. Auflage, Zürich: Verlag SKV 2019.

32. **Finck, Michèle:** Grundlagen und Technologie von Smart Contracts, in: Smart Contracts, Hrsg.: Fries, Martin; Paal, Boris P., Tübingen: Mohr Siebeck GmbH und Co. KG 2019, S. 1-12.

33. **Finextra (Hrsg.):** How to use technology to solve climate change and cloud waste, Online im Internet: https://www.finextra.com/newsarticle/35365/how-to-use-technology-to-solve-climate-change-and-cloud-waste, 27.02.2020.

34. **Finextra (Hrsg.):** Remaining challenges of blockchain adoption and possible solutions, Online im Internet: https://www.finextra.com/blogposting/18496/remaining-challenges-of-blockchain-adoption-and-possible-solutions, 29.02.2020.

35. **Fraunhofer (Hrsg.):** Blockchain: Technologien, Forschungsfragen und Anwendungen, Positionspapier, 20.03.2017.

36. **Fraunhofer FIT (Hrsg.):** Blockchain: Grundlagen, Anwendungen und Potenziale, White Paper 2016.

37. **Fraunhofer-Gesellschaft (Hrsg.):** Blockchain und Smart Contracts: Technologien, Forschungsfragen und Anwendungen, 11.2017.

38. **Gartner (Hrsg.):** Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact, Online im Internet: https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-from-transformational-impact, 08.10.2019.

39. **Gartner (Hrsg.):** Gartner Hype Cycle, Online im Internet: https://www.gartner.com/en/information-technology/research/hype-cycle, 12.08.2020.

40. **Giga (Hrsg.):** Mit Bitcoin Pizza bestellen und online liefern lassen – so geht's, Online im Internet: https://www.giga.de/downloads/bitcoin/specials/mit-bitcoin-pizza-bestellen-und-online-liefern-lassen-so-gehts/, 02.02.2018.

41. **Haber, Stuart; Stornetta, W. Scott:** How to Time-Stamp a Digital Document, in: Journal of Cryptology, 3(2)/1991, S. 99-111.

42. **Handelsblatt (Hrsg.):** In Bitcoins investieren, Online im Internet: https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/sparen-in-der-digitalen-zukunft-in-bitcoins-investieren/19971882.html?ticket=ST-3252743-skOhWcVOWvTqBpa07dye-ap3, 25.06.2017.

43. **Hasan, Haya R.; Salah, Khaled:** Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters, in: IEEE Access, 6/2018, S. 46781-46793.

44. **Hoffmann, Thomas; Skwarek, Volker:** Blockchain, Smart Contracts und Recht, in: Informatik _Spektrum, 42/2019, Nr. 3, S. 197-204.

45. **Höptner, Alexander:** Neue Märkte, neue Rollen: Wie die Blockchain die Finanzwelt verändert, in: Die Zukunft ist dezentral, Hrsg.: Sandner, Philipp; Tumasjan, Andranik; Welpe, Isabelle, Norderstedt: BoD – Books on Demand 2020, S. 57-71.

46. **Hosp, Annan:** Blockchain 2.0: einfach erklärt – weit mehr als nur Bitcoin, 1. Auflage, München: Finanzbuch Verlag 2018.

47. **Kaulartz, Markus; Heckmann, Jörn:** Smart Contracts – Anwendungen der Blockchain-Technologie; in Computer und Recht, 09/2016, S. 618-624.

48. **Krone Zeitung (Hrsg.):** Zermatt akzeptiert Steuerzahlungen in Bitcoin, Online im Internet: https://www.krone.at/2087853, 29.01.2020.

49. **Legder Academy (Hrsg.):** What Are Public Keys and Private Keys?, Online im Internet: https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys, 23.10.2019.

50. **Meitinger, Thomas Heinz:** Smart Contracts, in: Informatik_Spektrum, 40/2017, Nr. 4, S. 371-375.

51. **Merkle, Ralph C.:** A certified digital signature, in: CRYPTO ’89: Proceedings on Advances in Cryptology Lecture Notes in Computer Science, 435/1989, S. 218–238.

52. **Mohanty, Debajani:** Blockchain für Manager, Haar bei München: Franzis Verlag GmbH 2018.

53. **Mohanty, Debajani:** Ethereum for Architects and Developers: With Case Studies and Code Samples in Solidity, 1. Auflage, Berkeley, CA: Apress 2018.

54. **Mukhopadhyay, Mayukh:** Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity, Birmingham: Packt Publishing Ltd. 2018.

55. **Nakamoto, Satoshi:** Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

56. **Patel, Dhiren; Shah, Keivan; Shanbhag, Sanket; Mistry, Vasu:** Towards Legally Enforceable Smart Contracts, in: Blockchain – ICBC 2018, Hrsg: Goos, Gerhard; Hartmanis, Juris; van Leeuwen, Jan, Cham: Springer International Publishing AG 2018, S. 153-166.

57. **Ratcliffe, Susan:** Oxford Essential Quotations, Online im Internet: https://www.oxfordreference.com/view/10.1093/acref/9780191866692.001.0001/q-oro-ed6000 18679?rskey=O6r8bT&result=93, 12.08.2020.

58. **Rosenberger, Patrick:** Bitcoin und Blockchain – Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik, Berlin: Springer Vieweg 2018.

59. **Sandner, Philipp; Gösele, Martin:** Blockchain-Technologie, in: WISU – Das Wirtschaftsstudium (Hrsg.), 03/2018, S. 309-314.

60. **Schmoranz, Paul W.; Schick, Lukas; Schwickert, Axel:** Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete, in: Arbeits-papiere WI, Nr. 2/2020, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2020.

61. **Schwenk, Jörg:** Sicherheit und Kryptographie im Internet, 4., überarbeitete und erweiterte Auflage, Wiesbaden: Springer Gabler 2014.

62. **Schwickert, Axel; Schick, Lukas**: macOS – Verschlüsseln, Entschlüsseln und Signieren von E-Mails, in: Arbeitspapiere WI, Nr. 4/2019, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2019.

63. **Schwickert, Axel C.; Schick; Lukas; Schramm, Laura; Hein, Melanie:** Verschlüsseln, Entschlüsseln und Signieren von Dateien und E-Mails – Reader zur WBT-Serie, in: Arbeitspapiere WI, Nr. 1/2019, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2019.

64. **Sillaber, Christian; Waltl, Bernhard:** Life Cycle of Smart Contracts in Blockchain Ecosystems, in: Datenschutz und Datensicherheit (DuD), 41/2017, S. 497-500.

65. **Skwarek, Volker:** Eine kurze Geschichte der Blockchain, in: Informatik _Spektrum, 42/2019, Nr. 3, S. 161-165.

66. **Spindler, Helge; Martinetz, Simone; Friz, Daniel:** Strukturstudie »BW SHARE« Gemeinschaftliche Nutzung von Ressourcen – Chancen und Herausforderungen der

Sharing Economy für die etablierte Wirtschaft in Baden-Württemberg, Hrsg: Bauer, Wilhelm in: Fraunhofer Institute für Arbeitswirtschaft und Organisation IAO, 2015.

67. **Szabo, Nick:** Bit Gold, Online im Internet: https://nakamotoinstitute.org/bit-gold/, 29.12.2005.

68. **Szabo, Nick:** Formalizing and Securing Relationships on Public Networks, Online im Internet: http://firstmonday.org/ojs/index.php/fm/article/view/548/469, 1.09.1997.

69. **Tapscott, Don; Tapscott, Alex:** Die Blockchain Revolution – Wie die Technologie hinter Bitcoin nicht nur das Finanzsystem, sondern die ganze Welt verändert, 5. Auflage, Kulmbach: Börsenmedien AG 2018.

70. **Teuteberg, Frank; Tönnissen, Stefan:** Blockchains, in: WISU-Kompakt – Das Wirtschaftsstudium (Hrsg.), 3/2017, S. 286-288.

71. **Teuteberg, Frank; Tönnissen, Stefan:** Smart Contracts, in: WISU-Kompakt – Das Wirtschaftsstudium (Hrsg.), 5/2017, S. 566-567.

72. **The World Bank (Hrsg.):** The Global Findex Database 2017 – Measuring Financial Inclusion and the Fintech Revolution, Online im Internet: https://globalfindex.worldbank.org/sites/globalfindex/files/2018-04/2017%20Findex%20full%20report_0.pdf, 2017.

73. **Thesing, Henrik:** Hashgenerator, Online im Internet: https://hashgenerator.de, 15.09.2020.

74. **Vigliotti, Maria Grazia; Jones, Haydn:** The Executive Guide to Blockchain – Using Smart Contracts and Digital Currencies in your Business, Cham: Springer Nature Switzerland AG 2020.

75. **Vornberger, Oliver:** Kryptografie und Bitcoin, in: WISU-Kompakt – Das Wirtschaftsstudium (Hrsg.), 6/2014, S. 744-745.

76. **Voshmgir, Shermin:** Blockchains, Smart Contracts und das Dezentrale Web, Online im Internet: https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf, 30.01.2017.

77. **Walport, Mark:** Distributed Ledger Technology: beyond blockchain – A report by the UK Government Chief Scientific Adviser, Online im Internet: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, 19.01.2016.

78. **Wang, Bozhi; Chen, Shiping; Yao, Lina; Liu, Bin; Xu, Xiwei; Zhu, Liming:** A Simulation Approach for Studying Behavior and Quality of Blockchain Networks, in:

Blockchain – ICBC 2018, Hrsg. Chen, Shiping; Zhang, Liang-Jie; Wang, Harry, Cham, Switzerland: Springer International Publishing AG 2018, S. 18-31.

79. **Wenz, Daniel:** Bitcoin Mempool – Einfach erklärt, Online im Internet: https:// cryptomonday.de /bitcoin-mempool-einfach-erklaert/, 21.10.2019.

80. **Wilkens, Robert; Falk, Richard:** Smart Contracts – Grundlagen, Anwendungs-felder und rechtliche Aspekte, Wiesbaden: Springer Gabler 2019.

Impressum

Reihe: **Arbeitspapiere Wirtschaftsinformatik** (ISSN 1613-6667)

Bezug: http://wi.uni-giessen.de

Herausgeber: Prof. Dr. Axel Schwickert
Prof. Dr. Bernhard Ostheimer

c/o Professur BWL – Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IT-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstehen aus Forschungs-, Abschluss-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr-, Vortrags- und Kolloquiumsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Prof. Dr. Axel Schwickert, Justus-Liebig-Universität Gießen sowie der Professur für Wirtschaftsinformatik, insbes. medienorientierte Wirtschaftsinformatik, Prof. Dr. Bernhard Ostheimer, Fachbereich Wirtschaft, Hochschule Mainz.

Hinweise: Wir nehmen Ihre Anregungen zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.

Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit einem der Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe erhalten Sie unter der Web-Adresse
http://wi.uni-giessen.de/