HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Herr
Manuel Müller

Chancen und Risiken der Distributed Ledger Technologie im Finanzsektor mit Fokus auf die Anwendungsbereiche Zahlungsverkehr und Wertpapierhandel

Mittweida, 2018

Fakultät Wirtschaftsingenieurwesen

BACHELORARBEIT

Chancen und Risiken der Distributed Ledger Technologie im Finanzsektor mit Fokus auf die Anwendungsbereiche Zahlungsverkehr und Wertpapierhandel

Autor:
Herr

Manuel Müller

Studiengang:
Betriebswirtschaftslehre

Seminargruppe:
BW15w3-B

Erstprüfer:
Prof. Dr. rer. oec. Volker Tolkmitt

Zweitprüfer:
Prof. Dr. rer. oec. Serge Velesco

Einreichung:
Mittweida, 29.08.2018

Verteidigung/Bewertung:
Mittweida, 2018

Faculty Industrial Engineering

BACHELOR THESIS

Opportunities and risks of distributed ledger technology in the financial sector with focus on the applications payment transactions and securities trading

author:
Mr.

Manuel Müller

course of studies:
Business Administration

seminar group:
BW15w3-B

first examiner:
Prof. Dr. rer. oec. Volker Tolkmitt

second examiner:
Prof. Dr. rer. oec. Serge Velesco

submission:
Mittweida, 29.08.2018

defence/ evaluation:
Mittweida,2018

Bibliografische Beschreibung:

Müller, Manuel:
Chancen und Risiken der Distributed Ledger Technologie im Finanzsektor mit Fokus auf die Anwendungsbereiche Zahlungsverkehr und Wertpapierhandel. - 2018. - 9, 56 S. Mittweida, Hochschule Mittweida, Fakultät Wirtschaftsingenieurwesen, Bachelorarbeit, 2018

Referat:

Diese Arbeit befasst sich mit der sogenannten Distributed Ledger Technologie und ihrer bekanntesten Anwendungsform Blockchain. Dabei handelt es sich um eine neuartige, dezentrale Form von Datenbanken. Zunächst wird die Funktionsweise von Blockchain am Beispiel Bitcoin erläutert, um dann die Vorteile und Nachteile einer Anwendung im Finanzsektor bewerten zu können. Fokus liegt in dieser Arbeit auf den Bereichen Zahlungsverkehr und Wertpapierhandel. Zuletzt erfolgt dann noch ein Blick auf mögliche Verwendungsmöglichkeiten von Blockchain über die Finanzbranche hinaus.

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
Bzw.	Beziehungsweise
CEO	Chief Executive Officier
DLT	Distributed Ledger Technologie
FBI	Federal Bureau of Investigation
FinTech	Finanztechnologie
ICO	Initial Coin Offering
ILP	Inter-Ledger-Protokoll
IPO	Initial Public Offering
USN	Universal Sharing Network
Usw.	Und so weiter
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TWh	Terrawattstunde
z.B.	Zum Beispiel

1 Einleitung

1.1 Motivation und Problemstellung

„The first generation of the digital revolution brought us the Internet of information. The second generation-powered by Blockchain technology-is bringing us the Internet of value: a new, distributed platform that can help us reshape the world of business and transform the old order of human affairs for the better. “

Dieses Zitat von Don Tapscott, einem kanadischen Unternehmer, Professor und Buchautor beschreibt ziemlich treffend, in welchem digitalen Wandel wir uns momentan erneut befinden. Mit der Entwicklung des World Wide Web Ende der 80ger Jahre und deren allmählicher Verbreitung in den 90ger Jahre hätten wohl selbst die kühnsten Optimisten nicht damit gerechnet, in welcher Weise diese neuartige Technologie sämtliche Lebensbereiche des Menschen verändern und revolutionieren wird. War das Internet zunächst auf den digitalen Austausch von Informationen bedacht, gibt es heutzutage scheinbar unendlichen Nutzungsmöglichkeiten. Ob nun das Einkaufen sämtlicher Waren, Knüpfung neuer sozialer Kontakte, Abwicklung von Transaktionen oder das Buchen einer Urlaubsreise - nur einige Beispiele von Dingen, die im virtuellen Raum des Internets möglich sind.

Nun ist gut 30 Jahre nach Entwicklung des Internets eine neue Technologie auf dem Vormarsch und in Begriff, die zweite Generation der digitalen Revolution einzuleiten. Die Rede ist von der Distributed Ledger Technologie, eine dezentrale, transparente und kryptografisch gesicherte Art der Verwaltung von Daten. Mit dieser Technologie soll ein Internet der Werte geschaffen werden, bei dem es möglich ist, verschiedenste Werte fast in Echtzeit von einer Person zur anderen zu senden. Brachte die Einführung des Internets bereits vielfältigen Veränderungen in der Finanzwelt, wird der Distributed Ledger Technologie in diesem Bereich ein disruptives Potenzial zugeschrieben. Mit dem Aufkommen von Bitcoin, der digitalen Währung, deren Funktionsweise auf Distributed Ledger Technologie basiert, begannen immer mehr Finanzinstitute auf diesem Gebiet zu forschen und Anwendungsmöglichkeiten für ihren eigenen Markt zu entdecken.

Ein Großteil der Finanzsysteme wurde zwar im Wandel der Digitalisierung an die neuen Begebenheiten angepasst, dennoch gibt es akute Schwachstellen, die diese Systeme intransparent und aufgrund der Verantwortlichkeit einer zentralen Instanz zu einem Sicherheitsrisiko machen. Die Vielzahl an beteiligten Akteuren sorgen zudem für ineffiziente Prozesse mit unnötigen zeitlichen Verzögerungen und Abwicklungskosten. Die Distributed Ledger Technologie setzt an diesen Schwachstellen an und verspricht nicht nur diese zu beseitigen, sondern die Finanzwelt als Ganzes komplett umzukrempeln. Fraglich ist, ob das Potenzial einer

Revolution im Finanzsektor mithilfe dieser Technologie tatsächlich gegeben ist oder ob und wenn überhaupt nur Teilbereiche verbessert werden können?

Wie können der Zahlungsverkehr und der Wertpapierhandel, als große Geschäftsfelder für Finanzinstitute von dieser Technologie profitieren? Welche Herausforderungen sind zu berücksichtigen, bevor ein Einsatz überhaupt in Frage kommt? Neben dem Finanzsektor sollen auch andere Bereiche der Wirtschaft und des öffentlichen Sektors von Distributed Ledger Technologie profitieren können. Um welche Bereiche handelt es sich dabei und gibt es bereits Beispiele erfolgreicher Anwendung? All diese Fragen sollen in der folgenden Arbeit recherchiert um im Fazit beantwortet werden.

1.2 Zielsetzung und methodisches Vorgehen

Ziel dieser Arbeit ist es zunächst, eine begriffliche Abgrenzung der relevanten Schlagwörter vorzunehmen, da diese in der breiten Öffentlichkeit fälschlicherweise oftmals vermischt oder synonym verwendet werden. Nach einem kurzen geschichtlichen Abriss über die Vorgänger der Distributed Ledger Technologie soll dann ein grundlegendes Verständnis für die Funktionsweise dieser Technologie am Beispiel Blockchain vermittelt werden.

In den darauffolgenden Kapiteln 2 und 3 liegt der Fokus auf den für diese Arbeit ausgesuchten Anwendungsbereichen des Zahlungsverkehrs und des Wertpapierhandels. Ein Blick auf aktuelle Gegebenheiten und Probleme der beiden Geschäftsbereiche soll dabei die Grundlage für die weiterführende Erörterung sein. Die Betrachtung von ausgewählten Vorteilen und Herausforderungen ermöglicht es, abschließend ein Fazit zu ziehen und eine Bewertung vorzunehmen.

In Kapitel 5 geht es um weitere Verwendungsmöglichkeiten über die Finanzbranche hinaus, mit dem Ziel, dem Leser eine Auswahl an weiteren potenziellen Einsatzgebieten in der Wirtschaft und im öffentlichen Sektor mithilfe von Beispielen aus der Praxis näherzubringen.

2 Begriffliche und theoretische Grundlagen

In diesem Teil meiner Arbeit sollen nun die Grundlagen zum allgemeinen Verständnis des weiteren Textes geschaffen werden.

2.1 Begriffsabgrenzungen und Definitionen

Mit dem Aufstieg und der zunehmenden Bekanntheit von Bitcoin und Kryptowährungen im Allgemeinen in den letzten Jahren sowie der zunehmenden Diskussion zum Thema, tauchten auch Begriffe wie „Blockchain“ und „Distributed Ledger Technologie“ in den Schlagzeilen auf, die fälschlicherweise oftmals synonym verwendet werden. Um die Bedeutung und Unterschiede von DLT und Blockchain zu verstehen ist es wichtig, beide Begriffe auch im Hinblick auf den Anwendungsbereich von Kryptowährungen zu differenzieren. Weiterhin spielen die Begriffe Smart Contracts und ICOs, speziell für den Anwendungsbereich Finanzsektor, eine tragende Rolle.

2.1.1 Distributed Ledger Technologie

Übersetzt man Distributed Ledger aus dem Englischen bedeutet es so viel wie „Verteiltes Kontenbuch“. Im Gegensatz zu einem „klassischen“ Kontenbuch handelt es sich hierbei um eine dezentrale digitale Datenbank, welche keinen zentralen Intermediär zur Absicherung und Aktualisierung der Transaktionen mehr benötigt. Alle Teilnehmer dieses Netzwerks besitzen eine gemeinsame Schreib-, Speicher- und Leseberechtigung und es gibt wie eben schon erwähnt keine zentrale Instanz mit alleiniger Schreibberechtigung.[1] Eine Steigerung der Effizienz in Abwicklung von Datenaustausch und Kommunikation unter den Beteiligten ist die Folge und wird als einer der großen Vorteile dieser Technologie angesehen.

Die Informationen der Datenbank werden von allen Teilnehmern als richtig und unabänderlich angesehen, kommen neue Daten hinzu, müssen diese erst vom gesamten Netzwerk validiert werden. Abbildung 1 veranschaulicht die Funktionsweise eines Distributed Ledger`s im Vergleich zu einem Kontenbuch mit zentraler Instanz. Die gängigsten DLT-Anwendung basieren auf der Blockchain-Technologie, deren Einsatz vor allem bei der Abbildung von Transaktionen digitaler Währungen wie zum Beispiel Bitcoin Anwendung findet.

Im Falle der Blockchain besteht das Verteilte Kontenbuch aus einer zusammenhängenden Kette (Chain) von chronologisch aneinandergereihten Blöcken

[1] Vgl. Metzger, Jochen: Distributed Ledger Technologie (DLT).

(Block), welche eine oder mehrere Transaktionen enthalten.[2] Die Blockchain von Bitcoin ist das bekannteste Beispiel eines „unpermissioned“ Ledgers, also offen zugänglich für jedermann. Die Blockchain auf der die Kryptowährung Ripple basiert ist hingegen ein „permissioned“ Ledger, im Gegensatz zur offenen Datenbank nur einem beschränkten Teilnehmerkreis zugänglich.

Blockchain ist aber nur eine Anwendungsmöglichkeit von DLT. So verzichtet die Kryptowährung IOTA komplett auf eine Kettenstruktur und verwendet den sogenannten „Tangle-Ledger“. Dabei werden die Transaktionen nicht in Blöcke zusammengefasst, sondern von übergeordneten Transaktionen oder Knoten im Netzwerk bestätigt.[3] Weiterhin gibt es noch Hashgraph, eine Art DLT, die angibt, bis zu 250.000 Transaktionen pro Sekunde verarbeiten zu können und mithilfe von sogenanntem „Virtual Voting“ Übereinstimmung unter den Teilnehmern erreicht. Dabei ist ein Netzwerkteilnehmer dazu verpflichtet, alle bekannten Informationen zu Transaktionen mit anderen zufällig ausgewählten Teilnehmern zu teilen. Die Technologie dahinter ist patentiert und nicht öffentlich einsehbar. Der Fokus liegt in dieser Arbeit aufgrund der Bekanntheit und Praxiserprobung auf Blockchain als Anwendung von DLT.

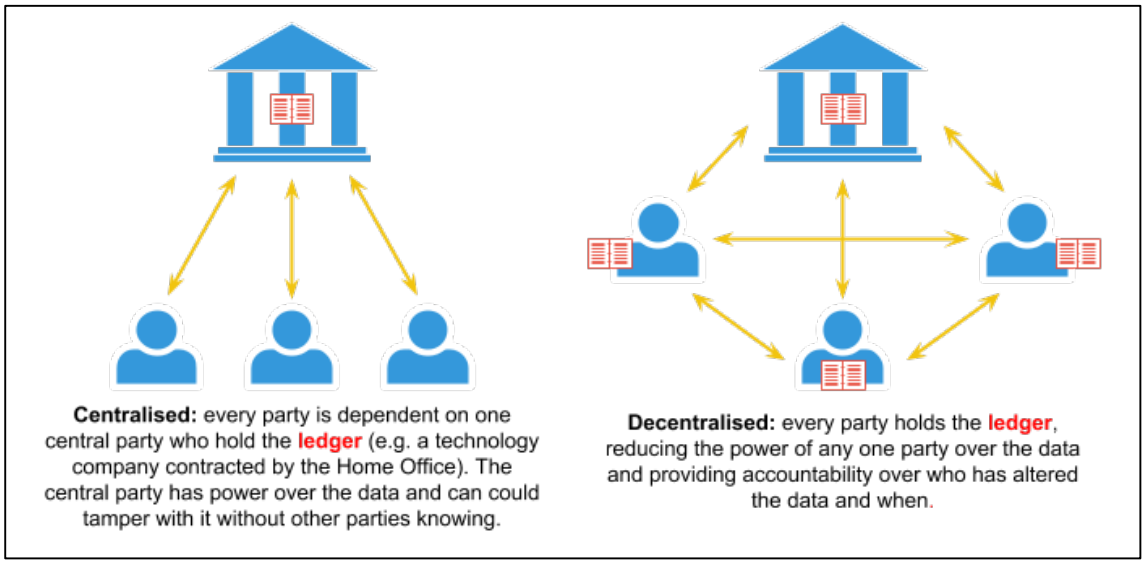

Abbildung 1: Distributed Ledger Technologie[4]

[2] Vgl. Deutsche Bundesbank (2017): Distributed-Ledger-Technologien, S.37.

[3] Vgl. Negin: IOTA | Kryptowährung für das IOT.

[4] Siehe: https://openinnovation.blog.gov.uk/2018/02/19/is-distributed-ledger-technology-the-answer/ vom 05.06.2018.

2.1.2 Blockchain

Häufigste Anwendungsform der DLT in der jetzigen Zeit, vor allem in Bezug auf digitale Währungen ist die Blockchain-Technologie. Diese verteilte Datenbank erlaubt es Teilnehmern des Netzwerks, direkt und ohne Intermediär, Transaktionsdaten peer-to-peer abzuwickeln. Mehrere Daten werden dabei in Blöcken zusammengefasst und mithilfe kryptografischer Verfahren in chronologischer Reihenfolge miteinander verkettet. Die Teilnehmer sind für die Verifikation der Blöcke und die Speicherung der kompletten Transaktionshistorie verantwortlich, es gibt keine zentrale Instanz, die diese Aufgaben übernimmt. Neue Blöcke enthalten stets gewisse Werte bzw. Informationen aus vergangen Blöcken und es ist dadurch praktisch unmöglich, vergangene Transaktionen nachträglich abzuändern und die Blockchain zu manipulieren. Das gesamte Netzwerk würde dies sofort merken.

Auf die genaue Funktionsweise der Blockchain wird im Punkt 2.3 noch genauer eingegangen, Abbildung 2 gibt aber bereits einen sehr guten Überblick.

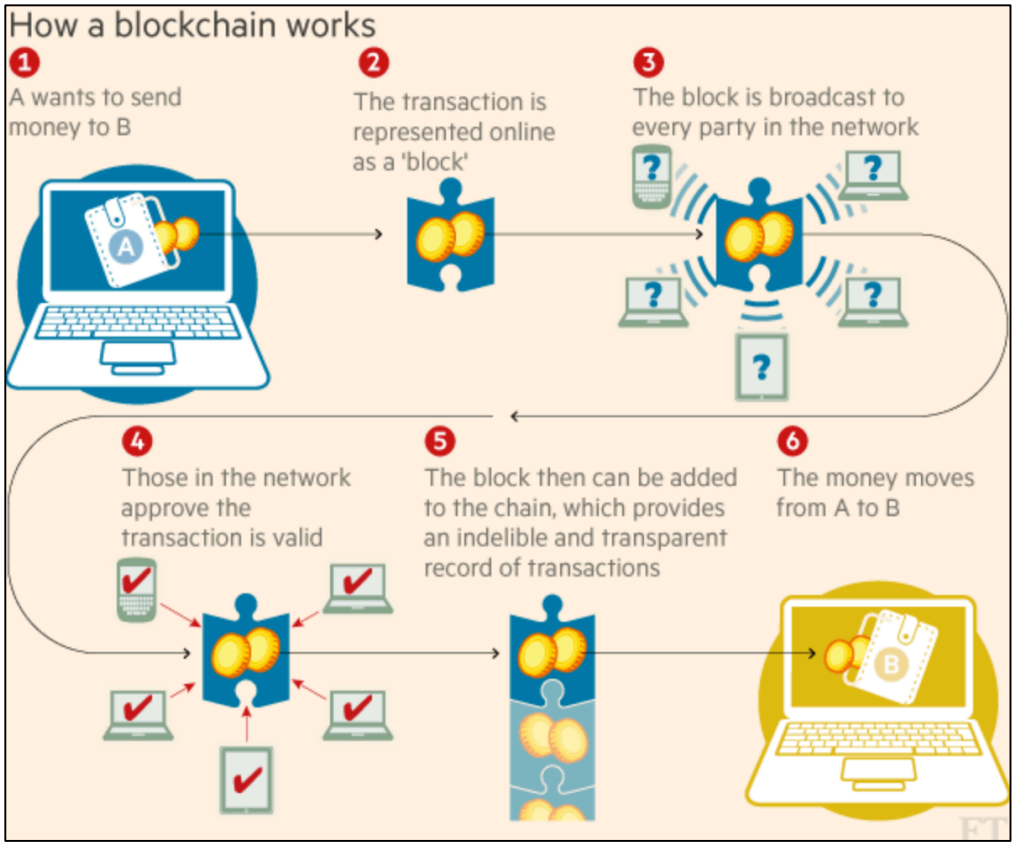

Abbildung 2: Funktionsweise einer Blockchain[5]

[5] Siehe: https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64 vom 07.06.2018.

2.1.3 Kryptowährungen

Weil Kryptowährungen, allen voran deren bekannteste Vertreter Bitcoin und Ethereum oft in einem Atemzug mit Blockchain und DLT genannt werden und teilweise auch vermischt beziehungsweise falsch interpretiert werden, möchte ich in diesem Punkt etwas Klarheit schaffen.

Kryptowährungen sind, wie es der Name schon sagt, digitale Zahlungsmittel welche auf den Grundlagen der Kryptografie erstellt werden. Im Gegensatz zu Fiatgeld (Euro, Dollar...), welches von den jeweiligen Zentralbanken gedruckt und ausgegeben wird, sind digitale Währungen dezentral organisiert und werden von der Gemeinschaft erschaffen und transferiert. Um digitales Geld von einer Person an die nächste zu versenden bedarf es der Distributed Ledger Technologie, bei vielen Kryptowährungen wird sich bis auf einige Ausnahmen der Blockchain als verteilte Datenbank bedient. Derzeit existieren insgesamt 1610 Kryptowährungen[6] (Stand: 12.06.18), allerdings verschwinden viele nach bestimmter Zeit wieder vom Markt und es kommen gleichzeitig auch neue hinzu.

2.1.4 Smart Contracts

Smart Contracts wird aufgrund ihres hohen Automatisierungspotenzials und Anwendbarkeit in verschiedenen Branchen hohe Bedeutung im Bereich der Distributed Ledger Technologie zugemessen. Es handelt sich dabei aber nicht um „Intelligente Verträge“, bzw. Verträge im rechtlichen Sinne, sondern vielmehr um automatisch ausführbare Programme, die bei einer Transaktion prüfen, welche Konditionen spezifiziert wurden und welche Folgeaktivitäten zu initiieren sind.[7]

Smart Contracts werden auf einer Blockchain gespeichert, sind daher unveränderlich, verteilt, sehr sicher und schaffen Vertrauen zwischen Parteien, die sich sonst nicht vertrauen würden. Smart Contracts machen die Notwendigkeit von zentralen Instanzen in bestimmten Anwendungsbereichen, wie zum Beispiel der Vergabe von Darlehen bei Banken oder die Inanspruchnahme von Leistungen bei Versicherungen, hinfällig. Ganz einfach lassen sich Smart Contracts am Beispiel Crowdfunding erklären. Bisher benötigte es immer noch eine dritte Partei, die Crowdfunding-Plattform, um sicherzustellen, dass das Geld der Unterstützer ordnungsgemäß gehandhabt und die Mittel nach Erreichen der Zielsumme auch tatsächlich an den Empfänger ausgezahlt werden. Ein Smart Contract könnte die Crowdfunding Plattform als Intermediär zwischen Unterstützer und Empfänger unbrauchbar machen. Das Programm bzw. der Code des Smart Contracts würde sicherstellen, dass die Gelder der Unterstützer bis zum Erreichen der Zielsumme ordnungsgemäß und sicher verwahrt und schließlich automatisch an den Empfänger ausgezahlt werden. Wird die Zielsumme nicht erreicht, fließen die eingezahlten Mittel automatisch wieder zurück an die Unterstützer.

---

[6] CoinMarketCap: All Cryptocurrencies.

[7] Vgl. Fraunhofer - Institut: BLOCKCHAIN UND SMART CONTRACTS, S.19.

2.1.5 Initial Coin Offering

Ein Initial Coin Offering ist ähnlich dem IPO (Initial Public Offering oder auch Börsengang) eine Methode zur Unternehmensfinanzierung. Im Gegensatz zum IPO ist diese Methode des Crowdfundings allerdings unreguliert und wird speziell von Firmen und Startups verwendet, deren Geschäftsmodell auf Kryptowährungen basiert. ICOs dienen einfach gesagt dazu, neue Kryptowährungen auf den Markt zu bringen und diese durch ein ICO zu finanzieren. Dabei wird beim sogenannten Token-Sale (Token = neu erzeugte digitale Währung) den Unterstützern und Investoren des Projekts die Möglichkeit gegeben, einen Anteil der neu emittierten Währung, meist im Tausch gegen andere Kryptowährungen wie z.B. Bitcoin oder Ethereum zu erwerben. [8]

Unterscheiden lassen sich grundsätzlich zwei Arten von Token: Der Utility Token soll nach Abschluss des Projekts als Zahlungsmittel genutzt werden, gibt dem Erwerber aber kein Mitbestimmungs- bzw. Teilhabrecht am Unternehmen - trägt also einen inhärenten Wert mit sich. Der Revenue Share Token lässt sich hingegen mit Aktien vergleichen und berechtigt den Besitzer zu Teilhabe und Dividende. Die einfachste und gängigste Methode, eine neue Kryptowährung zu emittieren erfolgt über die Ethereum Blockchain, bei der sogenannte ERC20 Token nach einem bestimmten Standard erstellt werden.

2.2 Geschichtlicher Hintergrund der Distributed Ledger Technologie

Um die Bedeutung und das Potenzial der Distributed Ledger Technologie und speziell von Blockchain zu verstehen ist es wichtig, den geschichtlichen Kontext und die Entstehung von Kontenbüchern zu kennen. Dieser Abschnitt soll einen kurzen geschichtlichen Abriss über die Entwicklungen der Buchführung von der Vergangenheit bis zur Gegenwart geben.

Bereits die frühen Hochkulturen im Zweistromland um Euphrat und Tigris benutzten ab ca. 3000 vor Christus einfache Tontafeln, um Angaben über Lieferungen wie Bier und Brot schriftlich festzuhalten. Diese einfachsten Formen zum Verzeichnis von Vermögen oder Besitz gewannen mit fortschreitender Entwicklung an Bedeutung und wurden zum Rückgrat der Wirtschaft. [9]

Die Technik der Papierherstellung, welche im 13. Jahrhundert bis nach Europa gelangte, setzte die Grundlage für laufende Aufzeichnungen von Transaktionen und Besitzverhältnissen. Ein weiterer Meilenstein der Konten- bzw. Buchführung, war die Entwicklung und Einführung der doppelten Buchführung nach dem Muster von Genua. Das Hauptbuch spiegelte nun erstmals in der Geschichte Einnahmen sowie Ausgaben wieder und ermöglichte eine lückenlose Dokumentation

[8] Vgl. BTC - ECHO: Was ist ein ICO?

[9] Vgl. Gabele/ Mayer (2015): Einführung in die Buchhaltung und Jahresabschlusserstellung, S.3-8.

von Transaktionen. Über das Zeitalter der Industrialisierung, mit einer zunehmenden Vereinheitlichung und Standardisierung von Prozessen und Abläufen, bis zur Entwicklung des Personal Computers Ende der 70ger Jahre des vergangenen Jahrhunderts wurden Ledger bzw. Kontenbücher zunehmend digitalisiert und man kehrte der klassischen Buchführung, mit Niederschrift auf Papier, den Rücken. Die Digitalisierung ermöglichte erst das komplexe wirtschaftliche System, in dem wir heute Leben. 2008 veröffentliche eine Person unter dem Synonym „Satoshi Nakamoto“ ein Whitepaper mit dem Thema „Bitcoin: A Peer-to-Peer electronic cash system“ deren Herzstück eine neuartige Ledger Technologie mit dem Namen Blockchain war. Es war der erste Ledger, der nicht von einer einzigen Person, Gruppe oder der Regierung kontrolliert wurde. Daraus entwickelte sich ein weltweites Netz von Computern, welches kryptografisch gesichert, schnell und dezentral organisiert ist. Die Zukunft dieser noch sehr jungen Technologie ist ungewiss, ihr wird aber bereits heute ein gleiches disruptives Potenzial, wie der des Internets zugesagt.

2.3 Funktionsweise der DLT am Beispiel der Blockchain von Bitcoin

Im nun folgenden Abschnitt soll auf die technischen Grundlagen der Distributed Ledger Technologie genauer eingegangen werden, um anschließend die Anwendungsbereiche Wertpapierhandel und Zahlungsverkehr nach Chancen und Risiken beurteilen zu können. Die Blockchain von Bitcoin bietet sich in diesem Fall besonders an, weil aufgrund der hohen medialen Dokumentation und Aufmerksamkeit entsprechend viele Informationsquellen und Daten vorliegen.

2.3.1 Kryptografie

Bis zum Jahr 2008, als Satoshi Nakamoto sein Modell eines peer-to-peer elektronischen Bezahlsystems vorstellte, beruhte der Handel im Internet fast vollständig darauf, dass Banken als Intermediäre dazu dienten, Vertrauen zwischen zwei Parteien zu schaffen und elektronische Zahlungen zu verarbeiten. Die größten Schwächen dieses Systems sind, dass es keine völlig unumkehrbaren Transaktionen geben kann, die Vermittlungskosten der Finanzinstitute die Transaktionskosten erhöhen und weil Transaktionen theoretisch rückgängig gemacht werden können, sich das Misstrauen zwischen Händler und Kunden erhöht. Um Sicherheit zu schaffen werden letztendlich mehr Informationen vom Kunden verlangt als eigentlich notwendig. Betrug, beziehungsweise ein gewisses Maß davon, wird dabei hingenommen und akzeptiert [10]

Die Vision von Satoshi Nakamoto, dessen Identität bis heute noch ungeklärt ist, war es also, ein elektronisches Zahlungssystem zu entwickeln, welches Vertrauen mithilfe von Kryptografie schafft und es zwei Parteien ermöglicht, Transaktionen direkt untereinander ohne eine dritte Partei durchzuführen. Durch das

[10] Vgl. Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, S.1.

Enkodieren von Informationen mittels Kryptografie wird es rechnerisch unmöglich, Transaktionen zu widerrufen und gleichzeitig schützt dieser Mechanismus die beteiligten Personen vor Betrug. Die Kryptografie der Blockchain von Bitcoin basiert auf drei wesentlichen Säulen: kryptografischen Hashfunktionen, einer Private und Public Key Infrastruktur und digitalen Signaturen. [11]

2.3.1.1 Hashfunktionen

Übersetzt man „to hash“ aus dem Englischen in das Deutsche bekommt man Ergebnisse wie hacken oder zerkleinern. Stark vereinfacht werden in dem Fall der kryptografischen Hashfunktionen der Blockchain von Bitcoin, eine beliebige Zeichenkette an Informationen, der sogenannte String, als Input in einen Output mit fest vorgeschriebener Länge umgewandelt beziehungsweise diese Informationen „zerkleinert“. Bei der Blockchain von Bitcoin handelt es sich konkret um 256 Bit. Wichtig dabei ist, dass diese mathematische Funktion deterministisch ist, also der gleiche Eingabewert immer zum gleichen Ausgabewert führt. Weiterhin muss die Funktion effizient und schnell berechenbar sein, also ohne großen Speicherverbrauch auskommen. [12]

Abbildung 1 verdeutlicht die Funktionsweise des SHA-256 Hashverfahrens an einem einfachen Beispiel.

Abbildung 3: Hashfunktion[13]

[11] Vgl. Ittner, Prof. Dr. - Ing. Andreas (2018): Grundlagen Blockchain, S.5.

[12] Vgl. Zahrte, René: Funktionsweise und Auswirkungen der Blockchain - Technologie auf den Wertpapierhandel, S.14.

[13] Eigene Darstellung.

Zur kryptografischen Nutzung der Hashfunktion, gibt es drei weitere Sicherheitsaspekte. Die Funktionen müssen:

- Kollisionsresistent
- Verborgen und
- Puzzlefreundlich sein

Die erste Eigenschaft ist, dass die Hashfunktion kollisionsresistent sein muss. Eine Kollision tritt ein, wenn zwei unterschiedliche Eingabewerte den gleichen Ausgabewert ergeben. Eine Hashfunktion H gilt als kollisionsresistent, wenn niemand eine Kollision finden kann, sodass Eingabewert x und Ausgabewert y den gleichen Hash H(x) = H(y) ergeben. Allerdings ist es sicher, dass es Kollisionen gibt, was sich ganz einfach beweisen lässt. Weil die Anzahl der Strings im Eingabebereich theoretisch bis ins Unendliche gehen kann, die Ausgabewerte allerdings Strings einer bestimmten, festgelegten Länge haben, muss es zwangsläufig zwei unterschiedliche Eingabewerte geben, die zu demselben Ausgabewert führen. Mit einer einfachen Berechnung lässt sich eine Kollision für einen 256 Bit Hash finden: man berechnet für $2^{256} + 1$ unterschiedliche Eingabewerte den Hash und prüft nach, ob zwei Ausgabewerte identisch sind. Weil wir in dieser Rechnung mehr Eingabe- als Ausgabewerte haben, muss ein Paar zwangsläufig kollidieren. Es bleibt aber festzustellen, dass die Berechnung aller Hashwerte äußert zeit- und energieaufwendig wäre. Selbst wenn man davon ausgeht, dass ein Computer 10.000 Hashes pro Sekunde berechnen kann und durchschnittlich alle 2^{128} eine Kollision gefunden wird, würde er dafür 10^{27} Jahre brauchen.[14]

Hypothetisch ist es wahrscheinlicher, dass die Erde in den nächsten Sekunden von einem Meteor getroffen wird, als dass eine Kollision von zwei Hashwerten gefunden wird. Solange für eine Hashfunktion also keine Kollision festgestellt bzw. berechnet werden kann, gilt diese als kollisionsresistent.

Als zweite entscheidende Eigenschaft, die auf kryptografische Hashfunktionen zutreffen muss, gilt die Verborgenheit. Diese Eigenschaft besagt, dass wenn man den Hash H(x) gegeben hat, es nicht möglich ist, daraus den Eingabewert x zu bestimmen. Um das zu gewährleisten muss man sicherstellen, dass der Eingabewert entsprechend groß und verteilt ist. Weil die einzugebende Nachricht diese Funktion nicht zwangsläufig erfüllt, wird der Eingabewert mit einer weiteren, zufällig gewählten und einmalig verwendbaren Variablen, der Nonce, verkettet. Diese Nonce wird aus einem ausreichend großem und verteilten Wertebereich gewählt, sodass es unmöglich ist, über den Hash auf den Eingabewert zu schließen, ohne die Nonce zu kennen. Zur Umsetzung bedient man sich des sogenannten Commitment-Verfahrens. [15] Dieses Verfahren besteht aus zwei verschiedenen Algorithmen:

[14] Vgl. Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven. Bitcoin and Cryptocurrency Technologies, S.25.

[15] Vgl. ebd., S.28.

1. Commit (msg/nonce) - Die Commit-Funktion bedient sich der Nachricht und einem geheimen, zufälligen Wert, der Nonce, als Eingabe und als Ergebnis erhält man das sogenannte Commitment.

2. Verify (com/ msg/ nonce) - Die Verify-Funktion nimmt als Eingabe das Commitment, die Nachricht und die Nonce. Das Ergebnis ist entweder richtig, wenn com = commit (msg/nonce) oder falsch, wenn dem nicht der Fall sein sollte.

Damit dieses Verfahren funktioniert ist es wichtig, dass für jedes Commitment eine neue Nonce gewählt wird und dieser zufällig gewählte Wert auch nur einmal verwendet wird. Wird das Commitment-Verfahren nun in eine kryptografische Hashfunktion integriert, wird eine Nachricht mit einer Nonce verkettet, die einen zufälligen 256 Bit Wert hat. Über die Verkettung von Nachricht und Nonce wird dann der Hash berechnet. Wie im Zuge der Verify-Funktion schon angedeutet ist es unmöglich, ohne Kenntnis über alle drei Parameter (Nonce, Nachricht und Hash) Rückschlüsse auf den Inhalt der eingegebenen Nachricht zu ziehen. Deshalb kann man davon ausgehen, dass wenn eine Hashfunktion kollisionsresistent und verborgen ist, dass Commitment-Verfahren in der Hinsicht funktionieren wird, weil es die nötigen Sicherheitseigenschaften hat.[16]

Die dritte wichtige Anforderung an kryptografische Hashfunktionen ist Puzzlefreundlichkeit. Genauer gesagt handelt es sich hierbei um ein mathematisches Problem, bei der ein sehr großer Wertebereich durchsucht werden muss, bevor man die richtige Lösung gefunden hat. Wichtig dabei: es gibt keine Abkürzung, das heißt man findet die gültige Lösung, also das letzte Stück des Puzzles nur, wenn man diesen großen Wertbereich durchsucht. Das richtige Ergebnis kann nur durch das Ausprobieren von Zufallswerten gefunden werden. Unser Suchrätsel besteht in diesem Fall aus:

1. Einer Hashfunktion H
2. Einem Wert id (Puzzle-id), aus einer Verteilung mit hoher Zufallszahl
3. Einen Zielwertebereich Y

Eine Lösung zu diesem Rätsel ist der gesuchte Wert x, so dass $H(id \parallel x) \in Y$. Der Gedanke dahinter ist, dass wenn H einen n-Bit Ausgabebereich hat, es nur einen von 2^n Werten annehmen kann. Um das Puzzle zu lösen muss der Hashwert in den Zielwertebereich Y fallen. Die Größe von Y entscheidet also, wie schwer das Puzzle ist. Zusammenfassend ist zu sagen, dass es keine bessere Strategie zur Lösung des Puzzles gibt, als das zufällige Ausprobieren von x-Werten. Die Eigenschaft der Puzzlefreundlichkeit wird im Punkt 2.3.2.3 Mining noch eine wichtige Rolle spielen.

[16] Vgl. ebd., S.29.

Nachdem wir uns die drei wichtigen Eigenschaften von Hashfunktionen angeschaut haben stellt sich die Frage, wie genau die Anwendung bei Bitcoin aussieht. Bei Bitcoin wird die sogenannte SHA-256 Funktion benutzt, welche sich aus einer Kompressionsfunktion und der Merkle - Damgard - Transformation zusammensetzt. Vereinfacht gesagt, wird bei SHA-256 Funktion mithilfe der Merkle-Damgard-Transformation eine kollisionsresistente Kompressionsfunktion mit bestimmter, festgeschriebener Länge an Eingabewerten in eine Hashfunktion umgewandelt, die willkürliche Längen als Eingabewert akzeptiert.

2.3.1.2 Digitale Signaturen

Als ein zweites wichtiges Werkzeug, welches zur Erstellung von Kryptowährungen benötigt wird, zählen digitale Signaturen. Diese verhalten sich ähnlich den Unterschriften auf einem Schriftstück und sind eine Möglichkeit, eine Nachricht zwischen Sender und Empfänger zu bestätigen. Digitale Signaturen haben zwei entscheidende Merkmale:

1. Nur man selbst kann digital unterschreiben, aber jeder Teilnehmer kann meine Unterschrift auf Echtheit verifizieren
2. Jede Signatur ist an ein bestimmtes Dokument gebunden und kann nur für dieses verwendet werden

Diese zwei Merkmale stellen sicher, dass (1.) der Empfänger bestätigen kann, dass die Nachricht auch tatsächlich vom Sender kam, (2.) der Sender nicht abstreiten kann, die Nachricht gesendet zu haben und (3.), dass die Nachricht nicht manipuliert wurde.[17]

Der Einsatz von digitalen Signaturen bedarf der sogenannten Public Key Verschlüsselung, bei der ein Set Schlüssel, der Private und Public Key, mit bestimmten Eigenschaften erzeugt werden. Mithilfe von Eliptic Curve Multiplication wird aus einem Private Key der Public Key erzeugt, man kann aber im Umkehrschluss als wichtiger Sicherheitsaspekt nicht von Public auf Private Key schließen. Der Private Key ist wichtig zum Signieren der jeweiligen Nachricht und wird geheim gehalten, der Public Key ist öffentlich und dient der Verifizierung.

Abbildung 4 veranschaulicht, wie das digitale Unterschreiben einer Nachricht abläuft. Die Signaturfunktion verbindet die Nachricht n mit dem Private Key (a) des Absenders zur Unterschrift (u). Um die Unterschrift (u) zur erhalten, muss der Sender der Nachricht diese mit seinem Private Key (a) unterschreiben. Der Empfänger erhält dann die unterschriebene Nachricht. Bevor die Nachricht allerdings akzeptiert wird, überprüft der Empfänger die Authentizität des Absenders, indem die Nachricht und der Public Key (b) verglichen werden. Das geschieht, indem die Verifizierungsfunktion die unterschriebene Nachricht und den Public Key (b)

[17] Vgl. Badev, Anton; Chen, Matthew (2014): Bitcoin: Technical Background and Data Analysis., S.8.

als Eingabewert nimmt und als Ausgabe eine binäre Antwort produziert: Annahme oder Abweisung.

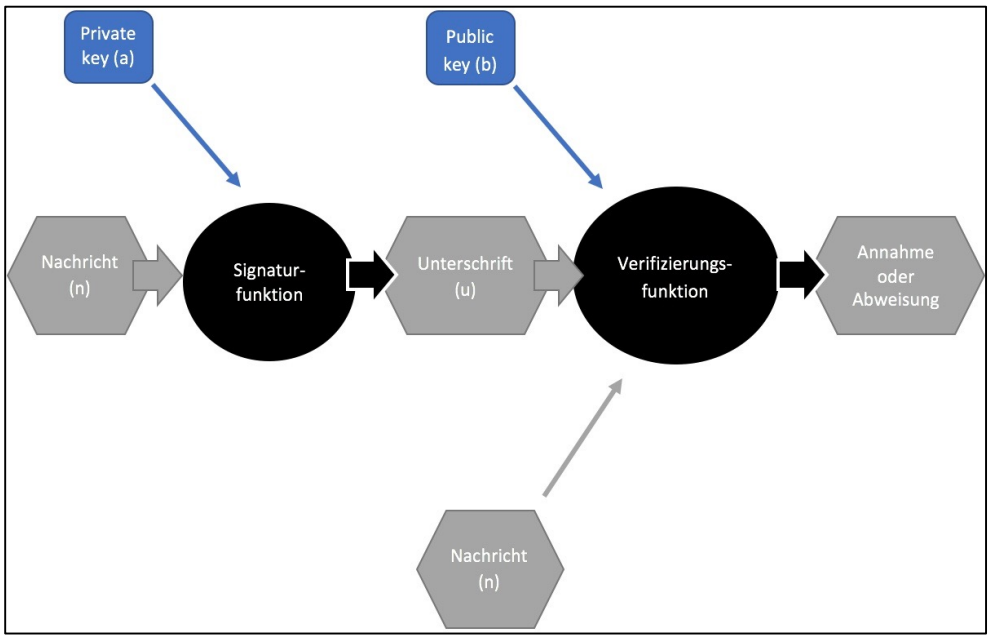

Abbildung 4: Digitale Signaturen via Private und Public Key[18]

Bei der Verwendung von digitalen Signaturen, bzw. Private und Public Keys auf der Blockchain von Bitcoin, werden Public Keys als Identitäten verwendet, Private Keys zum Unterschreiben der Nachricht. Jeder Benutzer kann zu jeder Zeit so viele digitale Identitäten erstellen wie er möchte, er muss dazu einfach ein neues Schlüsselpaar generieren. Es ist keine zentrale Institution dafür notwendig! Diese digitalen Identitäten sind nicht gekoppelt an Identitäten in der realen Welt. Bei Bitcoin und anderen Kryptowährungen werden diese Identitäten Adressen genannt.[19]

2.3.2 Dezentralisierung

Nachdem wir im letzten Abschnitt die kryptografischen Grundlagen untersucht haben, geht es nun darum, wie Dezentralisierung bei der Blockchain von Bitcoin erreicht wird. Zur Vereinfachung sollte man sich drei weitere, spezifischere Fragen stellen:

1. Wer ist für die Instandhaltung des Ledgers der Transaktion zuständig?
2. Wer hat die Entscheidungsgewalt darüber, welche Transaktionen gültig sind und welche nicht?
3. Wer erstellt neue Bitcoins?

[18] Eigene Darstellung.
[19] Vgl. Ittner, Prof. Dr. - Ing. Andreas (2018): Grundlagen Blockchain, S.23.

Das peer-to-peer Netzwerk bei Bitcoin ist fast vollständig dezentralisiert, weil grundsätzlich jeder Teil des Systems werden kann und die Eintrittsbarrieren relativ gering sind. Man muss ganz einfach über einen internetfähigen PC die Bitcoin - Software herunterladen und wird so ein sogenannter Node, wird Teil des Systems. Das Bitcoin-Mining, worüber im späteren Teil dieser Arbeit noch gesprochen wird, ist hingegen mit hohem technischen Aufwand und enormen Anfangsinvestitionen verbunden.

2.3.2.1 Verteilter Konsens

Eines der entscheidenden technischen Probleme, die bei einem verteilten, dezentralisierten Electronic-Cash-System gelöst werden müssen, ist die Erreichung von verteiltem Konsens. Verteilter Konsens ist bereits seit vielen Jahrzenten Bestandteil computerwissenschaftlicher Untersuchungen und wird traditionell dazu eingesetzt, um die Zuverlässigkeit von (Computer) -systemen zu verbessern. Bei dem verteilten Konsens - Protokoll gibt es n verschiedene Nodes, welche alle einen Eingabewert haben, beziehungsweise am System teilnehmen und wie in unserem Beispiel, Bitcoin an eine andere Adresse senden möchten. Herausforderung dabei ist, dass alle Nodes synchronisiert werden müssen und gleichzeitig, fehlerhafte und bösartige Nodes vom gesamten System erkannt und abgewiesen werden. Verdeutlichen lässt sich das an einem einfachen Beispiel: Gehen wir davon aus, dass Jaqueline eine Transaktion an Ronny senden möchte. Weil es sich bei Bitcoin um ein peer-to-peer-System handelt, wird die Transaktion, wie in Abbildung 5 zu sehen, an alle Nodes im Netzwerk gesendet.[20]

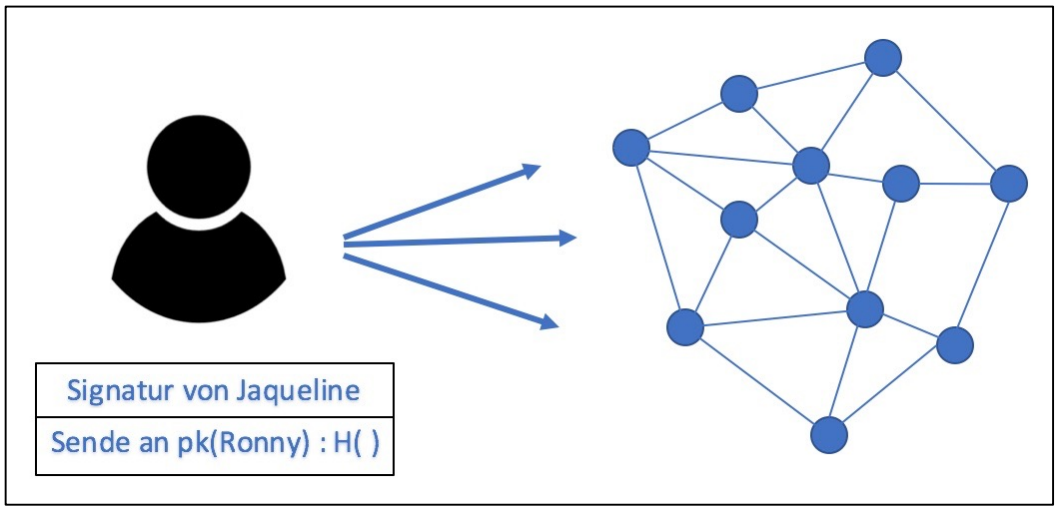

Abbildung 5: Übertragung einer Transaktion[21]

Damit Ronny die Transaktion empfängt ist es nicht notwendig, dass dieser selbst eine Node im System bereitstellt, er selbst hat keinen Einfluss darauf. Das gesamte System entscheidet, ob die Transaktion von Jaqueline an Ronny gültig ist

[20] Vgl. Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven. Bitcoin and Cryptocurrency Technologies, S.53.

[21] Eigene Darstellung.

oder nicht. Die Schwierigkeit besteht darin, dass eine Vielzahl von Nutzern gleichzeitig Transaktionen an das Netzwerk senden und von allen Nodes entschieden werden muss, welche Transaktionen stattfinden und in welcher Reihenfolge. Daraus resultiert ein globaler Ledger für das gesamte System. Zur Optimierung des Ablaufs werden die Transaktionen bei Bitcoin und anderen Kryptowährungen in Blöcken zusammengefasst.

Zu jeder Zeit besitzen alle Nodes im peer-to-peer Netzwerk einen Ledger bestehend aus einer Abfolge von Blöcken, bei denen Konsens erreicht wurde. Zusätzlich hat jede Node eine Liste an ausstehenden Transaktion, die an sie gesendet wurden, aber noch nicht zu einem Block zusammengefasst wurden. In einem zeitlichen Abstand von 10 Minuten schlagen die Nodes ihre Liste mit noch zu verarbeitenden Transaktionen dem gesamten Netzwerk vor und über ein Konsens-Protokoll wird entschieden, welcher Block welches Nodes als nächstes validiert und in die Blockchain aufgenommen wird. Noch ausstehende Transaktionen gehen nicht verloren, sondern werden einfach im nächsten Block inkludiert. Leider gibt es bei dieser Vorgehensweise noch einige technische Probleme, vor allem beim Protokoll von Bitcoin. Zum einen die Fehlerhaftigkeit im System, darunter fallen Dinge wie unvermeidbare Latenzzeiten oder abstürzende Nodes aufgrund schlechter Internetverbindung und zum anderen vorsätzliche Angriffe von Nodes auf das Netzwerk, um den Ablauf zu manipulieren.

Ironischerweise funktioniert Konsens in der Realität besser als in der Theorie, zumindest nach aktuellem Stand der Forschung. Das liegt vor allem daran, dass Bitcoin mit vielen traditionellen Annahmen zu Konsens bricht. Bitcoin hat das Anreizsystem eingeführt, was eine Neuheit bei verteilten Konsensprotokollen ist. Ehrliches Verhalten der Nodes wird belohnt, weil Nodes für das Validieren neuer Blöcke einen sogenannten Block-Reward bekommen und zusätzlich Transaktionsgebühren erheben können. Das funktioniert allerdings nur, weil Bitcoin eine digitale Währung ist. [22]

Zweitens nutzt Bitcoins Konsensalgorithmus in großem Maße die Idee der Zufälligkeit. Anders als in der Theorie gibt es für das Erreichen von Konsens, keinen bestimmten Start- oder Endpunkt. Stattdessen findet Konsens über einen längeren Zeitraum statt, bei Bitcoin dauert es normalerweise etwa eine Stunde bis Konsens erreicht wurde. Weil das Modell des verteilten Konsenses in der Praxis bei Bitcoin so gut funktioniert, wird schon seit geraumer Zeit die Anwendung von Blockchain-Technologie auch außerhalb von Kryptowährungen intensiv erforscht.

2.3.2.2 Konsens ohne Identität

Zurückblickend haben wir bereits festgestellt, dass die Bitcoin-Nodes keine beständigen, langanhaltenden Identitäten haben. Ein Grund dafür sind das Fehlen einer zentralen Instanz in einem peer-to-peer System wie Bitcoin. Der zweite

[22] Vgl.ebd., S.55.

Grund ist, dass Pseudonymität ein grundlegendes Ziel von Bitcoin ist. Als wichtige Eigenschaft von Bitcoin soll kein Nutzer dazu gezwungen werden, seine echte Identität im realen Leben offenzulegen um am System teilzunehmen.

Es bleibt allerdings festzustellen, dass das Fehlen von Identitäten einige Probleme für das Konsens-Protokoll von Bitcoin mit sich bringt. Hätten die Nodes Identitäten, wäre einerseits das Design einfacher und andererseits, die Sicherheit wesentlich höher bzw. einfacher zu realisieren. Das Fehlen von Identitäten kann man bei Bitcoin kompensieren, indem man eine schwächere Annahme anstellt, was uns zum nächsten Punkt bringt: impliziter Konsens.

Beim Bitcoin-Protokoll gibt es verschiedene Runden, die jeweils mit einem Block in der Blockchain korrespondieren. In jeder Runde wird nach dem Zufallssystem eine Node ausgewählt, die den nächsten Block vorschlagen darf. Was passiert, wenn die ausgewählte Node bösartig oder fehlerhaft ist? Nun kommt der implizite Konsens zur Anwendung. Die anderen Nodes entscheiden selbst, ob sie den Block akzeptieren oder ablehnen indem sie auf diesem draufbauen oder nicht. Wird der Block abgelehnt, dann wird auf dem zuletzt akzeptierten Block gebaut und der nicht valide Block ignoriert. Zurückschauend haben wir gelernt, dass jeder Block den Hash des vorherigen Blocks enthält und daher jede Node erkennt, auf welchem Block andere Nodes gerade aufbauen.[23]

Vereinfacht sieht der Bitcoin Konsens Algorithmus also folgendermaßen aus:

1. Die neue Transaktion wird an alle Nodes übertragen
2. Jede Node ordnet die neuen Transaktion in einem Block an
3. In jeder Runde des Protokolls darf eine zufällig ausgewählte Node einen neuen Block vorschlagen
4. Die anderen Nodes akzeptieren den neuen Block nur, wenn alle, in dem Block enthaltenen Transaktionen gültig sind
5. Die Nodes akzeptieren den Block, indem sie dessen Hash im nächst erstellten Block inkludieren

Um zu verstehen, wie und warum dieser Konsens Algorithmus funktioniert, hier ein paar Beispiele, wie mögliche Angreifer versuchen könnten, das System zu manipulieren.

Beispiel a: Das Stehlen von Bitcoins

Könnte man Bitcoins, die anderen Benutzern gehören und deren Adressen nicht vom Angreifer kontrolliert werden einfach stehlen? Nein, denn dazu müsste der Angreifer eine gültige Transaktion erstellen, die diese zu stehlenden Coins auch ausgibt. Dazu müsste der Angreifer die Signatur des Besitzers fälschen, was allerdings unmöglich ist, solang das vorhin erklärte Modell der digitalen Signaturen verwendet wird.

[23] Vgl.ebd., S.57.

Beispiel b: Denial-of-Service Angriff

Gehen wir davon aus, dass eine Node die Transaktionen eines anderen Nutzers aus welchem Grund auch immer, nicht mit in den Block einbinden will, den diese Node als nächstes vorschlägt. Wie der Name schon sagt, verweigert diese Node einem anderen Benutzer ihren Dienst (Denial of Service). Glücklicherweise ist solch eine Attacke nur ein geringfügiges Problem, denn Transaktionen, die es nicht mehr in den Block schaffen, die eine bestimmte Node vorschlägt, werden einfach in den nächsten Block einer ehrlichen Node aufgenommen.

Beispiel c: Double-Spending-Angriff

Das sogenannte Double-Spending Problem ist ein signifikantes Ärgernis der digitalen Welt im Bereich Zahlungsabwicklung, welches Satoshi Nakamoto in seiner Bitcoin Whitepaper speziell anspricht und mit seinem Modell eines elektronischen peer-to-peer Bezahlsystems lösen will. Doch wie funktioniert ein Double-Spending-Angriff nun im Detail? Zur Verdeutlichung bedienen wir uns eines Beispiels mit den zuvor verwendeten fiktionalen Charakteren Jaqueline und Ronny. Angenommen Jaqueline kauft in einem von Ronny betriebenen Onlineshop Leistungen im Tausch gegen Bitcoin ein. Diese Transaktion wird von einer ehrlichen Node in den nächsten Block der Blockchain aufgenommen. Erinnern wir uns daran, dass diese Transaktion die digitale Signatur von Jaqueline, die Zahlungsanweisung an die Public Address von Ronny sowie einen Hash, mit dem Hinweis auf eine vergangene Transaktion bei der Jaqueline die Bitcoins erhalten hat, die sie jetzt ausgibt, enthält. Nachdem Ronny gesehen hat, dass die Transaktion in die Blockchain aufgenommen wurde, wird die von Jaqueline erworbene Leistung freigegeben und an sie übertragen. Nehmen wir nun an, dass eine von Jaqueline kontrollierte Node in der nächsten Runde des Protokolls an der Reihe ist und den nächsten Block vorschlagen darf. Dann könnte sie einen neuen Block vorschlagen, der die Information zur Transaktion zwischen ihr und Ronny ignoriert und auf den Hash des vorherigen Blocks aufbaut. Zudem könnte Jaqueline in dem von ihr vorgeschlagenen Block eine Transaktion inkludieren, die die von ihr bereits an Ronny geschickten Bitcoins an eine von ihr kontrollierte Adresse schickt. Ein klassisches Beispiel, bei dem versucht wird, ein und das selbe digitale Geld zweifach zu verwenden. So bleibt festzustellen, dass weil bei beiden Transaktionen die gleichen Bitcoins verwendet wurden, nur eine der Transaktionen in die Blockchain aufgenommen werden können. [24] Verdeutlicht wird das eben Erklärte in Abbildung 6.

[24] Vgl.ebd., S.59.

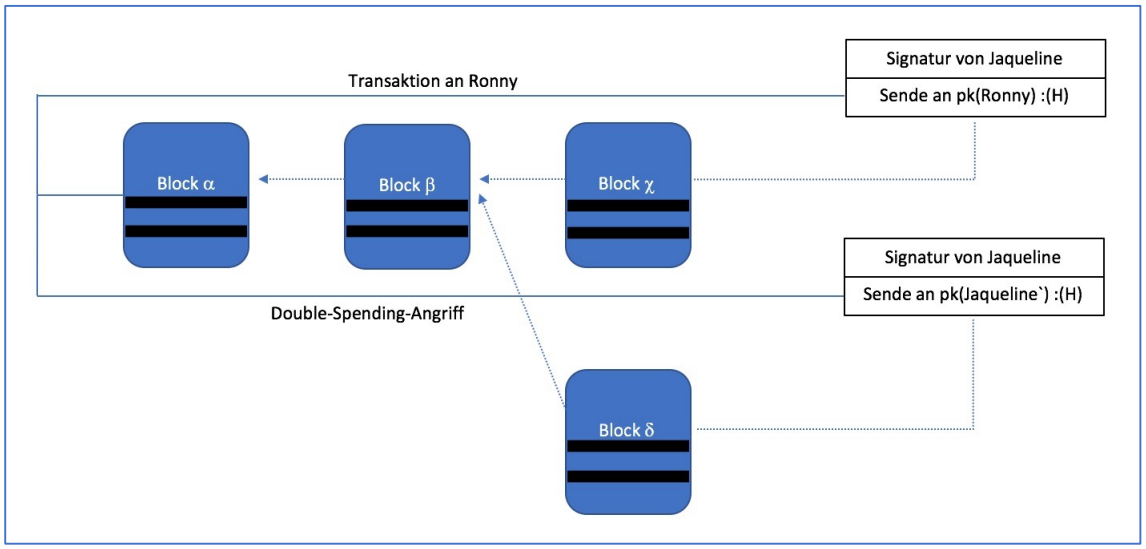

Abbildung 6: Double-Spending-Angriff[25]

Im Protokoll von Bitcoin ist verankert, dass ehrliche Nodes immer auf dem längsten, vorhandenen Zweig der Blockchain aufbauen. Weil aber zu diesem Zeitpunkt beide Ketten gleichlang sind, hängt es von der Node, die den nächsten Block vorschlägt ab, auf welchen Block aufgebaut wird und ob der Double-Spending-Angriff von Jaqueline erfolgreich ist oder nicht. Aus technischer Sicht sind beide Blöcke völlig identisch, wohingegen es von einem moralischen Gesichtspunkt her natürlich einen klaren Unterscheid zwischen beiden Blöcken gibt. Normalerweise folgen Nodes immer dem Block, welcher zeitlich gesehen als Erstes im Netzwerk verkündet wurde, was aber aufgrund von Latenzzeiten auch Block δ sein kann. Entscheidet sich die nächste Node also, auf diesem Block aufzubauen, dann steigt die Wahrscheinlichkeit, dass dieser in den Langzeitkonsens der Blockchain aufgenommen wird und Jaqueline mit ihrem Angriff erfolgreich war. Der Block, der die Transaktion an Ronny enthält, wird auf der anderen Seite vom Netzwerk ignoriert und Orphan-Block genannt. Die Blockchain wird an dieser Stelle nicht weiter verlängert, verliert ihre Gültigkeit und verwaist.

Ob der Angriff in unserem Beispiel Erfolg hat, hängt viel von der Verhaltensweise des Verkäufers, in unserem Fall also Ronny, ab. Handelt es sich um einen gutgläubigen Verkäufer, dann könnte er die Leistung bereits an Jaqueline freigegeben, sobald sich die Transaktion von Jaqueline an Ronny im Netzwerk verbreitet hat, aber noch bevor diese in Block χ aufgenommen wurde. Dabei handelt es sich um eine sogenannte Zero-Confirmation-Transaction, welche es dem Angreifer relativ leichtmacht, einen Double-Spending-Angriff durchzuführen.

Ein vorsichtiger Verkäufer würde die Leistung erst freigeben, nachdem die Transaktion von Jaqueline an Ronny von mehreren Nodes bestätigt wurde, denn allgemein gilt: je öfter eine Transaktion bestätigt wurde, umso höher ist die Wahrscheinlichkeit, dass diese in den langfristigen Konsens der Blockchain aufgenommen wird und umso unwahrscheinlicher wird es, dass Ronny Opfer einer Double-Spending-Attacke wird und betrogen werden kann. Für gewöhnlich sind es sechs

[25] Eigene Darstellung.

Bestätigungen, bevor man sichergehen kann, dass die Transaktion als sicher gilt und tatsächlich auf der Blockchain mit dem größten Konsens landet.

Abschließend kann man sagen, dass der nötige Schutz gegenüber ungültigen Transaktionen vollständig von der verwendeten Kryptografie abhängt, aber mithilfe von Konsensbildung bei Bitcoin umgesetzt wird. Das Stehlen von Bitcoins ist nicht möglich, weil die digitalen Signaturen nicht fälschbar sind. Denial-of Service Angriffe sind ebenfalls wenig erfolgversprechend, weil die Mehrheit der Nodes im System ehrlich sind und eine gültige Transaktion auf kurz oder lang verifiziert und in den Langzeitkonsens der Blockchain übernommen werden. Schutz gegenüber Double-Spending-Angriffen hängt vollständig vom Konsens ab. Man kann aber davon ausgehen, dass nach sechs Bestätigungen, die jeweilige Transaktion im Nachhinein nicht mehr ungültig gemacht werden kann.

2.3.2.3 Anreizsystem und Proof of Work

Nachdem wir in den vorherigen Kapiteln eine technische Sicht auf den Bitcoin-Konsens-Algorithmus geworfen haben, dreht sich 2.3.2.3 nun um das bei Bitcoin verwendete Anreizsystem. Weil sich im Bitcoin-Netzwerk viel Geld im Umlauf befindet ist die Versuchung groß, Nodes zu manipulieren und das System zu umgehen. Aufgrund der Tatsache, dass die Nodes keine Real-Life Identitäten haben ist es schwer, diese bei Fehlverhalten zu bestrafen. Was wäre aber, wenn man die Frage umdreht und Nodes für ihr ehrliches Verhalten, also das Erstellen von Blöcken, die im Langzeit-Konsens der Blockchain verankert werden, belohnt? [26]

a) Block-Reward

Der erste Anreiz für ehrliches Verhalten ist der sogenannte Block-Reward, bei der die Node, welche einen Block erstellt hat, diesem eine Spezial-Transaktion hinzufügen darf. Diese Spezial-Transaktion ist nichts weiter als eine Erschaffung neuer Bitcoins, die von der Node an eine Adresse seiner Wahl geschickt wird. Dabei handelt es sich also um eine Bezahlung für den Aufwand, einen neuen Block zu erstellen. Aktuell beläuft sich der Block-Reward auf 12,5 Bitcoins pro Block, was sich aber alle 210.000 Blöcke halbiert. Daraus ergibt sich, dass es eine endliche Anzahl an Bicoins gibt, nämlich 21 Millionen. Das bedeutet, dass ab 2140 kein Block-Reward mehr ausgezahlt wird, weil zu diesem Zeitpunkt alle 21 Mio. Bitcoin im Umlauf sein werden. Könnten aber theoretisch auch manipulierte und fehlerhafte Nodes diesen Block-Reward erhalten? Nein, denn auch die Spezial-Transaktion zur Erschaffung neuer Bitcoins wird in den Langzeitkonsens der Bitcoin aufgenommen und muss von anderen Nodes bestätigt werden. Der vorgeschlagene Block der bösartigen Node wird hingegen nicht Teil der längsten Kette der Blockchain und verwaist zu einem Orphan Block.

[26] Vgl.ebd., S.61.

b) Transaction Fee

Ab 2140 wird es keinen Block-Reward mehr geben - bedeutet das, dass ab diesem Zeitpunkt das System aufhört zu funktionieren und es für die Nodes keinen Anreiz mehr gibt, sich ehrlich zu verhalten? Nein, denn als zweiten Anreiz gibt es die Transaction Fee. Diese erlaubt dem Ersteller einer beliebigen Transaktion, dass beim Empfänger weniger Bitcoin ankommen als gesendet. Die Differenz erhält die Node, welche die Transaktion zuerst in ihrem Block aufgenommen hat. Die Transaction Fee ist freiwillig, ihr wird aber mit abnehmendem Block-Reward immer größere Bedeutung zukommen, wenn die Anwender des Systems auch in Zukunft eine vernünftige Qualität des Service erhalten wollen.

c) Mining und Proof of Work

Bisher sind wir davon ausgegangen, dass alle Nodes gleich sind und per Zufall die Node ausgewählt wird, die den nächsten Block vorschlagen darf. Dadurch entsteht das Problem, dass aufgrund des Anreizsystems unser Netzwerk von Nodes überflutet und instabil wird, weil jeder ein Stück vom Block-Reward abhaben will. Zusätzlich dazu gibt es noch das Problem, dass ein Angreifer eine große Anzahl von manipulierten Nodes erstellen könnte um damit das Konsens-Protokoll zu untergraben. Die Lösung dazu nennt sich Proof-of-Work. Der Gedanke dahinter ist, dass Nodes nicht zufällig, sondern im Verhältnis zur bereitgestellten Rechenleistung ausgewählt werden. Genauer gesagt stehen die Nodes im Wettstreit gegeneinander wer am schnellsten sogenannte Hash-Puzzles lösen kann. Um einen neuen Block zu erstellen, muss die Node erst den Zielwert des Puzzles, eine Nonce, finden. Der Block ist erst vollständig und kann zur Blockchain hinzugefügt werden, wenn diese Nonce, zusammen mit dem Hash des vorherigen Blocks und der Liste von Transaktionen komplettiert ist. Diese zu findende Nonce erfüllt die Eigenschaft der Puzzlefreundlichkeit wie in Punkt 2.3.1.1 bereits beschrieben. Das Puzzle kann also nur durch mehrmaliges Probieren gelöst werden. Je mehr Rechenleistung eine Node hat, umso schneller ist das fehlende Puzzleteil gefunden und der Block-Reward sowie mögliche Transaction Fees werden als Belohnung ausgezahlt. Dieser Prozess nennt sich Mining und die am Mining beteiligten Nodes heißen entsprechend Miner. Drei Eigenschaften der Hash-Puzzles haben darauf Einfluss, welchen der Nodes am Mining-Prozess teilnehmen und welche nicht. Erstens müssen Hash-Puzzles schwer zu berechnen sein. Heutzutage ist der Rechenaufwand so hoch, dass nur noch Miningfarmen und Mininggilden mit tausenden Servern rentabel Bitcoin schürfen. Via Cloudmining, bei dem die notwendige Soft- und Hardware von einem externen Unternehmen gegen Bezahlung in einer Cloud vermietet wird, können aber auch Menschen ohne großen Aufwand am Bitcoin-Mining teilhaben.[27]

Die zweite Eigenschaft ist, dass die Kosten parametrierbar sein müssen. Das bedeutet, dass der Zielwertbereich des Hash-puzzles alle 2.016 Blöcke neu angepasst wird. Damit wird der Veränderung des Mining-Ökosystems und der Ver-

[27] Vgl. BTC - ECHO: Wie funktioniert Bitcoin-Mining?

fügbarkeit von besserer Hardware Rechnung getragen, damit sichergestellt werden kann, dass nur alle 10 Minuten ein neuer Block erstellt wird. Doch warum gerade 10 Minuten? Der Grund für diese Latenzzeiten ist ganze einfach Effizienz. Es ist deutlich effizienter, viele Transaktionen in einem großen Block zusammenzuführen, als viele kleine Blöcke mit weniger Transaktionen. Für Bitcoin hat sich eine Latenzzeit von 10 Minuten als am effizientesten erwiesen, dass kann aber bei anderen Kryptowährungen oder Anwendungsbereichen deutlich abweichen und variieren.

Mit dem bis jetzt gesammelten Wissen über die Funktionsweise des Bitcoin-Protokolls in Bezug auf die notwendige Sicherheit, müssen wir unsere Annahmen neu formulieren. Der Großteil der Angriffe ist impraktikabel solang die Mehrheit der Miner, gewichtet an der zur Verfügung gestellten Rechenleistung (Hash-Power), dem Protokoll folgen oder ehrlich sind. Aufgrund des Wettstreits der Miner untereinander, den nächsten Block vorschlagen zu dürfen, wird sichergestellt, dass mit einer Wahrscheinlichkeit von mindestens 50% der nächste Block von einer ehrlichen Node vorgeschlagen wird. [28]

Das Lösen der Hash-Puzzles erfolgt der Wahrscheinlichkeit nach, weil niemand vorhersagen kann welche Nonce zur Lösung des Hash-Puzzles führt. Für den einzelnen Miner ergibt sich folgenden Berechnung, wie lange im Durchschnitt benötigt wird, um einen neuen Block zu finden:

$$\text{Mittlere Zeit bis zum nächsten Block} = \frac{10\ Minuten}{Anteil\ an\ der\ gesamten\ Hash\ Power}$$

Die dritte wichtige Eigenschaft der Proof of Work-Funktion ist, dass es trivial zu verifizieren ist, dass eine Node Proof of Work richtig berechnet hat. Weil die Nonce als Teil des Blocks im Netzwerk veröffentlicht werden muss ist es nicht wichtig, dass andere Nodes sich die Inhalte des Blocks anschauen und alles in einem Hash vereinen um zu sehen, ob dieser in den benötigten Zielwertbereich fällt. Eine wichtige Eigenschaft, die ohne Mithilfe einer zentralen Instanz sicherstellt, dass die Miner ihre Arbeit korrekt erledigen. [29]

2.3.3 Ablauf einer Transaktion

Wir haben jetzt bereits eine gute Vorstellung davon, wie eine Blockchain dezentralisiert wird und welche kryptografischen Verfahren dabei eine wichtige Rolle spielen. All diese Erkenntnisse sollen nun abschließend zusammengefasst werden, indem erklärt wird, wie der Ablauf einer Transaktion bei Bitcoin aussieht.

[28] Vgl. Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven. Bitcoin and Cryptocurrency Technologies, S.66.

[29] Vgl.ebd., S.68.

Schritt 1: Initialisierung

Wir bedienen uns zur Verdeutlichung wieder unserer fiktionalen Charaktere Ronny und Jaqueline aus den vorherigen Beispielen. Angenommen Jaqueline möchte Ronny 10 Bitcoin senden. Dazu nutzt Jaqueline ihren Private Key um eine Nachricht mit dem Input, welcher die Herkunft der Bitcoin aus vorherigen Transaktionen beschreibt, der Anzahl an Bitcoins an Ronny und dem Output, in dem Fall Ronny's Public Address, zu signieren. Diese digitale Signatur belegt, dass die Bitcoins tatsächlich von ihr stammen. Die Nachricht über diese Transaktion wird dann an das gesamte peer-to-peer Netzwerk gesendet und muss von allen Teilnehmern des Netzwerks, den Nodes, verifiziert werden. Mögliche Änderungen an der Transaktion von Jaqueline im Nachhinein sind nicht möglich und würden von der Gesamtheit aller Nodes sofort bemerkt.

Schritt 2: Validierung

Bevor die Transaktion ausgeführt werden kann, wird vom gesamten Netzwerk geprüft, ob Jaqueline tatsächlich der Sender ist und ob sie überhaupt ausreichend Bitcoins zur Verfügung hat um diese Transaktion durchzuführen. Damit soll Missbrauch und Fälschung verhindert werden, wie zum Beispiel einer mehrfachen Ausgabe bereits verwendeter Bitcoin durch Jaqueline. Ist mit der Transaktion etwas nicht in Ordnung schlägt das System sofort Alarm und es ist unmöglich, dass diese mit in den Langzeitkonsens der Blockchain aufgenommen wird.

Schritt 3: Ausführung

Ist die Validierung erfolgreich verlaufen, kommt es zu Schritt 3: der Ausführung. Jetzt befinden sich eine spezielle Art der Nodes, die Miner, im Wettstreit gegeneinander, die Transaktion von Jaqueline gemeinsam mit allen anderen noch ausstehenden Transaktionen seit der letzten Aktualisierung der Blockchain in einem neuen Block zu speichern. Zur Vervollständigung des Blocks muss neben dem Hash des vorherigen Blocks auch das fehlende Stück eines Hash-puzzles durch Probieren gefunden und gesichert werden. Der Miner, welcher als erstes den Block komplettiert hat erhält eine Belohnung, den Block-Reward, sowie mögliche Transaktionsgebühren. Der Block wird nun abgespeichert und der Blockchain hinzugefügt. Die gesamte Blockchain wird von allen Nodes abgespeichert und Transaktionen, die einmal in den Langzeitkonsens aufgenommen wurden, gelten nach mindestens sechs Bestätigungen als sicher und nicht mehr umkehrbar. Zusammengefasst und veranschaulicht wird der gesamte Vorgang in Abbildung 7.

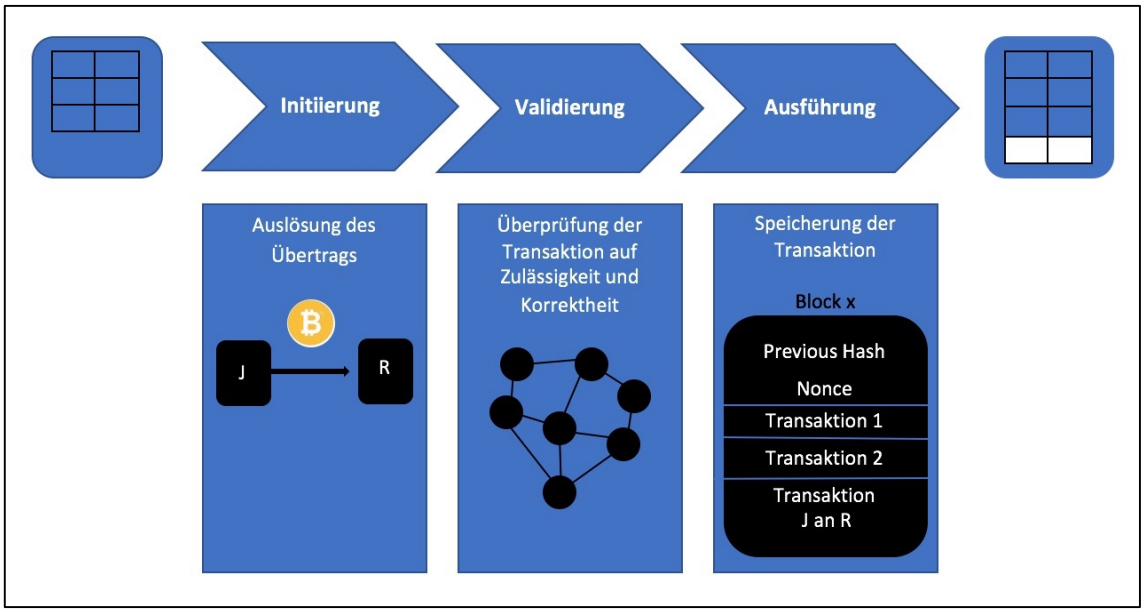

Abbildung 7: Ablauf einer Transaktion[30]

[30] Eigene Darstellung.

3 Einsatz von Blockchain im Zahlungsverkehr

Nachdem wir uns in Punkt 2 die theoretischen Grundlagen der Distributed Ledger Technologie angeschaut haben, folgt nun die Frage nach der Anwendung in der Praxis. Das Augenmerk liegt dabei auf der Blockchain-Technologie im Bereich Zahlungsverkehr.

3.1 Zahlungsverkehr heute

Um das Potenzial aber auch die Herausforderungen der Anwendung von Blockchain im Bereich Zahlungsverkehr zu erkennen ist es wichtig zu verstehen, was den Zahlungsverkehr wie wir ihn heute kennen ausmacht und welche Probleme es zu lösen gilt.

3.1.1 Überblick

Was ist Zahlungsverkehr? Laut Bundesbank „die Übertragung von Zahlungsmitteln innerhalb einer Volkswirtschaft im baren und unbaren Zahlungsverkehr.“[31] Selbst, wenn das Bargeld in bestimmten Bevölkerungsschichten noch sehr beliebt ist, wird der Großteil des Zahlungsverkehrs heutzutage von Banken, Unternehmen und Privatpersonen bargeldlos erledigt. Täglich fließen viele Milliarden Euro hin und her und für einen bestmöglichen wirtschaftlichen Austausch erfordert es effiziente, sichere und günstige Zahlungsmittel. [32]

Ist das Online-Banking heutzutage schon fest etabliert, drängen immer neue Innovationen wie kontaktloses Bezahlen, neue Bezahlverfahren wie zum Beispiel clickandbuy für den Einkauf im Internet, Bezahlung via Apps mit Mobiltelefonen oder auch die rasante Abwicklung von Bezahlungen von Konto zu Konto auf den Markt und gewinnen zunehmend an Interesse. Selbst wenn sich viele dieser Innovationen noch in der Wachstumsphase befinden, wird diesen Entwicklungen bereits großes Potenzial zugeschrieben. Besonders Banken befinden sich momentan in einer Umbruchphase, weil befürchtet wird, dass mithilfe der neuen Technologien, darunter auch Blockchain, ihre Rolle als Intermediäre wegfällt und damit ein traditioneller Geschäftsbereich wegbrechen könnte. Der Wettbewerb verstärkt sich auch dadurch, weil Nichtbanken wie Internethändler mit ihrer technologischen Kompetenz in das Marktgeschehen eingreifen und deren Angebote immer größeren Anklang finden.

[31] Deutsche Bundesbank: Zahlungsverkehr.

[32] Vgl. Deutsche Bundesbank (2016): Die Deutsche Bundesbank, S.172.

Wesentliche Erfolgsfaktoren für die Durchsetzung der angesprochenen Innovationen im Zahlungsverkehr sind neben der technischen Entwicklung das Nutzerverhalten, der bisher in vielen Bereichen noch unklare regulatorische Rahmen, der Grad an Standardisierung und Kooperation, die Preisentwicklung und letztendlich als einer der wichtigsten Faktoren die Sicherheit. [33]

3.1.2 Aktuelle Probleme

Das bestehende Finanzsystem zeichnet sich im Hinblick auf den Zahlungsverkehr vor allem durch die große Anzahl an Intermediären, die zwischen Sender und Empfänger liegen, aus. Sind zwei Personen einer Transaktion (innerhalb Deutschlands) beispielsweise Kunden von zwei unterschiedlichen Banken, dann gibt es mit den zwei Hausbanken der Kunden mindestens zwei Intermediäre, eventuell noch ein Clearinghaus. Im internationalen Zahlungsverkehr kommen ausländische Zahlungsverkehrssysteme oder Korrespondenzbanken hinzu.[34] Aufgrund der dabei stattfindenden komplexen Prozesse, dauern Überweisungen oftmals mehrere Tage, vor allem bei internationalen Überweisungen zwischen verschiedenen Kreditinstituten. Selbst, wenn Überweisungen im Euroraum mit Einführung des SEPA-Verfahrens vereinheitlicht wurden, können bei internationalen Transaktionen signifikante Kosten anfallen. So kostet ein bargeldloser Transfer in die USA über 1000€ bei der Berliner Sparkasse online und mit dem von der Sparkasse festgelegten Wechselkurs 32,50 € an Gebühren.[35]

Ein weiteres Problem ist die Tatsache, dass der Einsatz der verschiedenen Intermediäre sehr ressourcenintensiv, aber wenig effizient ist. Es gibt bisher weltweit kein einheitliches Zahlungssystem das es Privatpersonen, Unternehmen und Banken ermöglicht, auch große Geldmengen schnell, kostengünstig und sicher zu transferieren.

3.2 Erwartete Vorteile durch die Implementierung von Blockchain

Der Bereich Zahlungsverkehr stellt für viele Banken weltweit ein wichtiges Geschäftsfeld dar. So ist die Anzahl der Transaktionen im bargeldlosen Zahlungsverkehr weltweit von 282 Mrd. im Jahr 2010 auf voraussichtlich 522,4 Mrd. im Jahr 2017 gewachsen.[36] Prognosen sagen zudem für die nächsten Jahre ein weiteres Wachstum voraus.

Es wird erwartet, dass die Blockchain aufgrund ihrer Netzwerkstruktur und der Möglichkeit des gleichzeitigen Zugriffs auf eine gemeinsame Datenbank sehr

[33] Vgl. Deutsche Bundesbank (2012): Innovationen im Zahlungsverkehr, S.49.

[34] Vgl. Deutsche Bundesbank (2017): Distributed-Ledger-Technologien, S.39.

[35] Vgl. TransferWise: Auslandsüberweisung Sparkasse.

[36] Statista (2018): Anzahl der Transaktionen im bargeldlosen Zahlungsverkehr weltweit von 2010 bis 2020 (in Milliarden).

gute Voraussetzungen für einen effektiven Einsatz im Zahlungsverkehr schafft und dadurch ein höherer Grad an Transparenz, Sicherheit und Resilienz, Unabhängigkeit von Intermediären und Automatisierung in der Abwicklung erreicht werden kann.

3.2.1 Schnellere Übertragungsgeschwindigkeit

Wie in 3.1.2 bereits angesprochen ist das Thema Übertragungsdauer von Transaktionen immer noch ein leidiges Thema im Bankenbereich, welches mithilfe der Blockchain-Technologie nun endlich gelöst werden könnte. Hier hat sich das Zahlungsnetzwerk Ripple mit seiner geschlossenen Blockchain bereits einen Namen gemacht. Als weltweit erstes kommerziell operierendes Blockchain-Netzwerk konnte Ripple bereits über 100 Banken- und Zahlungsanbieter gewinnen, darunter Branchengrößen wie BBVA, Santander und UBS.

Wie funktioniert nun aber Ripple und inwiefern kann die Übertragungsgeschwindigkeit verkürzt werden? Die dezentrale Datenbank bei Ripple beinhaltet ein Register mit allen Kontoständen, welches jeder Teilnehmer des Netzwerks einsehen kann und damit sämtliche Aufzeichnungen und Vorgänge komplett transparent sind. Innerhalb weniger Sekunden kann sich gemeinsam auf Veränderungen geeinigt werden und Transaktionen können ohne eine zentrale Verrechnungsstelle gehandelt werden.

Dass dieses System nicht nur in der Theorie, sondern auch in der Praxis funktioniert zeigte sich bereits 2016. Während der Zahlungsverkehrskonferenz „Payments Panorama 2016“ in Kanada wurde live ein Bargeld-zu-Konto und Konto-zu-Bargeld-Blockchain Transfer vorgenommen. Bei dieser Transaktion zwischen der ATB Financial Bank in Kanada und der Reisebank AG in Frankfurt am Main wechselten 1000 kanadische Dollar innerhalb von 8 Sekunden den Besitzer. Mit dem zurzeit noch gängigen SWIFT-System hätte solch eine Transaktion mehrere Tage gedauert.

Ein Merkmal der Blockchain-Technologie ist der gleichzeitige Ablauf von Zahlungsnachricht und Settlement, also Abschluss der Zahlung. Weiterhin ist ein Clearing nicht mehr notwendig, weil die Einzelzahlungen in der dezentralen Datenbank mithilfe von mathematischen Algorithmen automatisch verbucht werden. Die Ausführung und Finalität von internationalen Zahlungen könnte somit von mehreren Tagen bis auf wenige Sekunden schrumpfen und hat dadurch natürlich ein enormes Kosten- und Ressourceneinsparungspotenzial.[37]

Die nachfolgende Abbildung verdeutlicht noch einmal das eben beschriebene Beispiel.

[37] Vgl. Boberach, Frank: Transatlantischer Zahlungsverkehr auf der Basis von Blockchain – Erfahrungen der Reise-Bank, S.34.

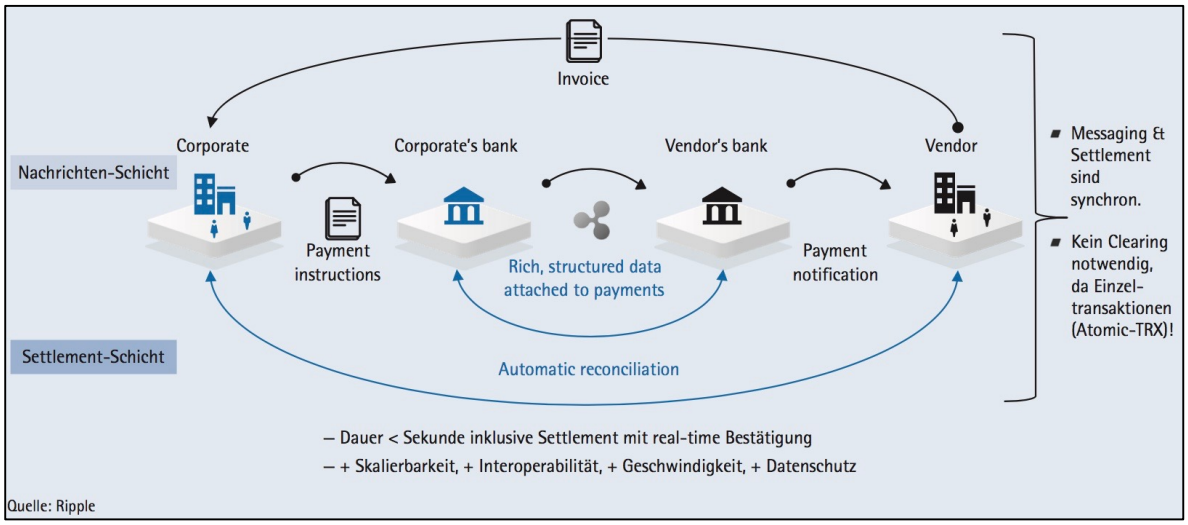

Abbildung 8: Der Zahlungsverkehr von morgen mithilfe der Ripple-Blockchain[38]

3.2.2 Skalierbarkeit und Transparenz

Einzelne Transaktionen sind leicht darstellbar, doch wie verhält sich das System bei der Abwicklung von hunderten oder gar tausenden Transaktionen in der Sekunde? Grundsätzlich ist die Technologie für eine große Anzahl an Transaktionen skalierungsfähig. So ist das Ripple-Zahlungssystem in der Lage, aktuell bis zu 1.500 Transaktionen in der Sekunde abzuwickeln und das zu jeder Zeit, quasi 24/7. Zudem ist das System bis auf 50.000 Transaktionen pro Sekunde skalierungsfähig, was dem Volumen von VISA entspricht.[39]

Zusätzlich dazu ist wie im vorherigen Punkt 3.2.1 schon angeschnitten, das Ripple Konsensus Ledger ein öffentliches Kontenbuch, welches prinzipiell von jedem öffentlich im Netz nachverfolgt werden kann und damit die notwendige Transparenz gewährleistet ist. Dieser Umstand birgt in der Praxis vor allem für Banken auch Herausforderungen, weil eine Transaktion zwar immer nachzuverfolgen, aber nicht zwangsläufig für jedermann sichtbar sein muss.

Ripple hat sich zur Lösung dieses Problems und auch um die Skalierbarkeit gewährleisten zu können, das Inter-Ledger-Protokoll überlegt. Dabei wird auf die bestehende Korrespondenzbanken-Infrastruktur zurückgegriffen und diese mit dem ILP kombiniert, was man sich als eine Kombination aus SWIFT und Blockchain vorstellen kann. Dadurch sollen internationale Fremdwährungszahlungen effizienter und schneller abgewickelt werden, weil Nachrichtenaustausch und Settlement synchron verlaufen. Zusätzlich dazu sind die jeweiligen Zahlungen einer Bank nur noch für eben diese und den nächsten Korrespondenzpartner sichtbar, weil die Kontenbücher beim ILP wieder hinter die Firewall der Banken

[38] Siehe Boberach, Frank: Transatlantischer Zahlungsverkehr auf der Basis von Blockchain – Erfahrungen der Reise-Bank, S.35.

[39] Ripple (o.J. (b)): XRP - The digital asset for payments.

verlegt werden, quasi privatisiert und nicht mehr öffentlich sichtbar für jedermann sind.[40]

In puncto Skalierbarkeit kommt die veränderte Kryptografie beim ILP zum Tragen, weil bei diesem auf den bei einer Blockchain sonst notwendige Konsensmechanismus zur Validierung neuer Blöcke verzichtet werden kann. Bei ILP wird Konsens über eine Software, dem sogenannten „Validator" erreicht. Nicht zuletzt ermöglicht ILP die Vernetzung bestehender Zahlungsverkehrssysteme, verschiedene Arten von Kontenbüchern und Netzwerken können adressiert und angebunden werden.

3.2.3 Unabhängigkeit von Intermediären

Das heutige Bankensystem im Bereich des internationalen Zahlungsverkehrs zeichnet sich durch eine Vielzahl von Intermediären aus, bevor ein Wert von Person A zu Person B transferiert werden kann. So tragen Korrespondenzbanken, Clearing- und Settlement-Stellen der Tatsache Rechnung, dass es aufgrund der verschiedenen internationalen Währungen und von Land zu Land unterschiedlichen Regularien bezüglich des Zahlungsverkehrs, sogenannte Cross-Border-Payments sehr kosten- und ressourcenaufwendig sind. Aufgrund der peer-to-peer Netzwerkstruktur der Blockchain ist es möglich, Transaktionen zwischen Teilnehmern intermediationsfrei auszutauschen.[41]

Mithilfe der Ripple-Blockchain und des in Punkt 3.2.2 erwähnten Inter-Ledger-Protokolls soll es Banken möglich gemacht werden, die gewöhnlichen Intermediäre in der Zahlungsverkehrsbranche zu ersetzen. Die dabei gesparten Kosten können dann an Partner-Banken und letztendlich an den Kunden weitergegeben werden. Laut Ripple soll eine Ersparnis von bis zu 60% der Transaktionsgebühren im Bereich des Machbaren liegen.[42]

Aber nicht nur Banken können von den Ripple angebotenen Produkten profitieren. So ermöglicht die Software xRapid es Zahlungsanbietern ihre Liquiditätskosten und den Kapitalbedarf für Liquidität drastisch zu senken. Dann ist es nicht mehr nötig, vorfinanzierte Konten in der ganzen Welt bei Zahlungen in Schwellenländer zu unterhalten - das Liquiditätsrisiko sinkt stark und Zahlungsanbieter werden unabhängiger von den Finanzinstituten in anderen Ländern. Möglich wird das durch den Einsatz von XRP, welche in unserem Fall als Brückenwährung im Handel mit anderen Währungen dient und eine zuverlässige Liquiditätsoption für grenzüberschreitende Zahlungen bietet. [43]

[40] Vgl. Boberach, Frank: Transatlantischer Zahlungsverkehr auf der Basis von Blockchain – Erfahrungen der Reise-Bank, S.35.

[41] Vgl. Deutsche Bundesbank (2017): Distributed-Ledger-Technologien, S.41.

[42] Vgl. Ripple (o.J. (b)): Solution Overview, S.17.

[43] Vgl. Ripple (o.J. (c)): Source Liquidity – xRapid.

3.2.4 Umsetzung von Micro-und Nanopayments

Bei Micro- bzw. Nanopayments handelt es sich um „die Zahlung von Kleinbeträgen im E-Commerce. Aufgrund der geringen Beträge sind für die zugrundeliegenden
Geschäfte Kreditkartenzahlungen wegen der hohen Transaktionskosten unwirtschaftlich.“[44] Die meisten Zahlungsanbieter sind heutzutage nicht in der Lage diese Art von Bezahlungen für geringe Summen zwischen einem Cent und fünf Euro für beispielsweise digitale Musikstücke oder Zeitungsartikel wirtschaftlich abzuwickeln, weil die Kosten für die Zahlungsabwicklung oftmals den Warenwert übersteigen.

Noch deutlicher wird diese Problematik, wenn man bedenkt, dass fast die Hälfte der Menschen weltweit von weniger als 2,5 $ am Tag auskommen müssen. Für Menschen in den Entwicklungsländern, wo ein Dollar einen großen Unterschied machen kann, bedeutet das eine wirkliches Hindernis. Für diese Personengruppe ist es unmöglich, Kleinstzahlungen zu senden oder zu empfangen.

Mithilfe von Blockchain soll es in Zukunft möglich sein, Micro-Transaktionen mit einem Bruchteil der jetzigen Transaktionskosten durchzuführen. Ein Unternehmen, das sich dieses Vorhaben auf die Fahne geschrieben hat ist das 2014 in Berlin gegründete Start-up SatoshiPay. SatoshiPay bietet eine Bezahl-Plattform an, die es möglich macht, dass Anbieter von journalistischen Inhalten im Internet wie Autoren, Lektoren oder Grafiker ihren Kunden Kleinstbeträge für das Lesen von Artikeln, Ansehen von Videos oder Hören von Musiktiteln berechnen. Diese Plattform erlaubt es, Nanopayments von 5 Cent oder weniger abzuwickeln, mit Transaktionskosten so niedrig wie dem Bruchteil eines Cents. Setzte das Unternehmen anfangs noch auf die Blockchain von Bitcoin, um die Micropayments vom Endnutzer direkt zum Herausgeber zu schicken, änderte sich das Ende 2017. Die Wirtschaftlichkeit des Bitcoin-Netzwerks hatte sich im Laufe der Jahre verändert und auch aufgrund des zunehmenden öffentlichen Interesses schossen die Transaktionsgebühren förmlich durch die Decke, von anfangs 0,02 $ bis heutzutage 3 $ im Durchschnitt, mit Spitzen von bis zu 5 $ pro Transaktion. Aus diesem Grund wechselte man Ende 2017 auf die Stellar-Blockchain, bei der nun StellarLumen anstelle von Bitcoin zur Abwicklung der Zahlungen verwendet werden. Die Vorteile dabei sind schnellere Transaktionen (ca. 5 Sekunden bis zur finalen Bestätigung) und extrem niedrige Gebühren (aktuell nur 0,00003 Cent pro Vorgang). Außerdem basiert die Stellar-Blockchain nicht auf einem Proof of Work, sondern einem Proof of Stake Konzept, bei dem Konsens nicht über die Rechenleistung, sondern über die Teilnahmedauer und/oder das Vermögen der Teilnehmer erreicht wird. Dieser Umstand hat die Energiekosten deutlich reduziert.[45]

[44] Kollmann, Prof. Dr. Tobias: Micropayment.

[45] Vgl. Schmidt, Tobias: Was ist eigentlich aus SatoshiPay geworden?

3.3 Herausforderungen

Die Distributed Ledger Technologie und die Blockchain-Technologie im Speziellen birgt im digitalen Zeitalter des 21. Jahrhunderts wie eben beschrieben ein enormes, bisweilen disruptives Potenzial im Sektor des Zahlungsverkehrs. Die Übertragung von Blockchain von einem ursprünglich für eine virtuelle Währung geschaffenen System hin zur Anwendung im realen Finanzsystem ist eine große Herausforderung. So benötigt es an vielen Stellen Anpassungen und Veränderungen um den Ansprüchen des Marktes gerecht zu werden, ohne dabei die strengen Regeln und Regularien außer Acht zu lassen, die im Finanzsystem eine so große Rolle spielen.

3.3.1 Technische Hürden

Die Blockchain-Technologie steckt bekanntermaßen noch in den Kinderschuhen und es ist schwer zu erahnen, welche Ausmaße das Ganze noch annehmen könnte. Schenkt man einer Potenzialanalyse von Sopra Steria Consulting vom September 2017 Glauben, so halten 76% der befragten Unternehmen die Technologie noch für experimentell oder nur probeweise einsetzbar und gar 11% sprechen ihr die Praxistauglichkeit ab.[46] Auf dem jetzigen Stand der Dinge ist eine der großen Schwachstellen der enorme Rechenaufwand und die damit verbundenen Energiekosten. Betrachten wir die Bitcoin-Blockchain, so kommt der jährliche Gesamtverbrauch an Strom, dem eines mittelgroßen Landes wie beispielsweise Österreich nahe. So beläuft sich laut digiconomist.net der aktuelle, jährliche Stromverbrauch allein für Bitcoin auf 73,12 TWh, was dem jährlichen Verbrauch von etwa 6.770.506 Haushalten in den USA entspricht.[47]

Je umfangreicher die Blockchain wird, also je mehr Teilnehmer und Transaktionen beteiligt sind, umso höher wird der Rechenaufwand und entsprechend der Stromverbrauch. Jede Information auf der Blockchain bleibt für immer erhalten und Veränderungen mit neuen oder aktualisierten Informationen werden in Form von neuen Blöcken hinzugefügt. Das Volumen der gesamten Blockchain wächst also exponentiell mit jeder Transaktion, was ein weiteres Problem zum Vorschein bringt: die enorme Menge an Speicherplatz, die auf den Rechnern der Netzwerkteilnehmer bereitgestellt werden muss. Ein weiterer Kritikpunkt ist die Zeitdauer je Transaktion, denn bisher benötigt die Blockchain von Bitcoin mehr als 10 Minuten für die Bestätigung eben dieser. Selbst wenn wie in den vorherigen Punkten die theoretische Möglichkeit der Skalierbarkeit gegeben ist, enthielten die bisherigen Pilotprojekte der Banken nur geringe Datenmengen und es muss sich erst zeigen, ob diese Technologie auch das gesamte Zahlungsmanagement eines Großkonzerns bewältigen könnte. [48]

[46] Vgl. SopraSteria: Blockchain 2017 - Spannende Technologien für morgen.

[47] Vgl. Digiconomist: Bitcoin Energy Consumption Index.

[48] Vgl. Metzner, Thomas: Techniktrend Blockchain, S.40.

Ein weiterer Kritikpunkt der an der Blockchain-Technologie ist, dass diese eine höhere Komplexität für die IT-Infrastruktur bedeutet. Weil das System auf mehreren Servern verteilt ist, ist es komplizierter und zeitaufwändiger Fehler zu lokalisieren und die Stabilität des Systems zu gewährleisten. Im schlimmsten Fall kann das zu einem Totalausfall der Blockchain führen.[49]

3.3.2 Fehlende Vertraulichkeit

Das Thema Vertraulichkeit spielt eine entscheidende Rolle, denn einerseits haben viele Finanzdienstleister aufgrund der Bankenkrise einen enormen Vertrauensverlust von Seiten der Kunden hinnehmen müssen und es wird sicherlich keine leichte Aufgabe, das Vertrauen der Kunden in diese neuartige Technologie aufzubauen.

Zum anderen ist die Idee hinter Blockchain so ausgerichtet, dass jeder Teilnehmer des Netzwerks prinzipiell die Möglichkeit hat, die komplette Transaktionshistorie einzusehen. Speziell bei Finanztransaktionen und dem Zahlungsverkehr ist es enorm wichtig, dass die Abwicklung vertraulich erfolgt, was ohne kryptografische Verschlüsselung allerdings unmöglich ist. Der rasante technische Fortschritt im Bereich Hardware- und Softwareentwicklung könnte es in Zukunft möglich machen, dass auch verschlüsselt abgespeicherte Daten über Transaktionen von allen Netzwerkteilnehmern wieder lesbar werden und damit die nötige Sicherheit und Vertraulichkeit nicht gegeben ist.

Die Methode der Perfect Forward Secrecy könnte diesem Problem Abhilfe schaffen, weil bei diesem Verfahren die nachträgliche Entschlüsselung selbst bei Bekanntwerden des Hauptschlüssels verhindert wird und es unmöglich wird, die ursprüngliche Transaktion zu entschlüsseln. Allerdings führt dieser Schutzmechanismus zu einer starken Abweichung von den Grundprinzipen von DLT. Nachvollziehbarkeit und vollständige Offenheit bzw. Transparenz einer dezentral verteilten Datenbank sind nicht mehr zu 100% gegeben und die Manipulationssicherheit des Systems kann bisweilen nicht mehr garantiert werden, wenn der ursprüngliche Code unbekannt und nicht mehr entschlüsselt werden kann.

3.3.3 Problem der Identifizierbarkeit

Denken wir zurück an die in Punkt 2 beschriebenen Grundlagen von DLT am Beispiel der Blockchain von Bitcoin, dann haben wir bereits festgestellt, dass die Public Keys jeder Node zwar öffentlich und für jeden sichtbar, aber nicht mit einer Identität in der realen Welt verknüpfbar sind.

Anders als bei den aktuellen Bezahlsystemen ist Blockchain also ein öffentliches Netzwerk bei den anonym, Werteinheiten übertragen werden. Das führt zu Herausforderungen beim Einsatz in der komplexen Infrastruktur von Zahlungssystemen. Laut §11 des Geldwäschegesetzes heißt es zum Thema Identifizierung:

[49] Vgl. Klaptor, Dr. Martin: Chancen und Herausforderungen der Blockchain.

„(1) Verpflichtete haben Vertragspartner, gegebenenfalls für diese auftretenden Personen und wirtschaftlich Berechtigte vor Begründung der Geschäftsbeziehung oder vor Durchführung der Transaktion zu identifizieren.“ [50]

Das bedeutet also, dass im Zahlungsverkehr beteiligte natürlich und juristische Personen eindeutig identifizierbar sein müssen. Dabei reicht als Identifizierung natürlich nicht der Public Key der Teilnehmer, sondern es werden der vollständige Name, die Adresse, Staatsangehörigkeit usw. benötigt. Bei Banken als Know Your Customer Prinzip bekannt setzt es voraus, dass die Teilnehmer an Transaktionen sich einer Legitimationsprüfung unterziehen. Unter diesen Regelungen könnte die anonyme Übertragung im P2P Netzwerk nicht mehr gewährleistet werden.

Ein weiterer Problempunkt im Hinblick auf Identifizierbarkeit von Blockchain ist das Anwendungsfeld Darknet. So ist dieser Bereich des Internets darauf ausgelegt, nicht oder nur schwer nachvollziehbare Kommunikation, Datenaustausch und Handel zu ermöglichen. Diese Orte bergen natürlich auch Gefahr, von Kriminellen für ihre Geschäfte missbraucht zu werden. Als bekanntester Marktplatz für Drogen, Waffen, Geldwäsche und illegale Geschäfte im Darknet galt bis zur Auflösung 2013 Silk Road. Auf dem Höhepunkt von Silk Road im Oktober 2013 hatte die Webseite 13.756 Notierungen in Bitcoin und die Plattform war überhaupt eine der ersten, die Bitcoin als Zahlungsmittel akzeptierte. Die Eigenschaft der anonymen Abwicklung von Geschäften ohne Verbindung zu realen Identitäten spielten Silk Road dabei in die Hände. Als dass FBI die Seite beschlagnahmte und deren Gründer Ross Ulbricht verhaftete, brach der Bitcoin-Kurs drastisch ein und Bitcoin und auch andere Kryptowährungen bekamen den Ruf, prädestiniert für kriminelle Handlungen und Geschäfte im Web zu sein. [51] Somit steht das Darknet „im gesellschaftlichen Interesseausgleich zwischen freiem und unbeobachteten Informations- und Güteraustausch und den Interessen der Strafverfolgung.“ [52]

Es ist dennoch unbestritten, dass es auch im Darknet völlig legale und nachvollziehbare Nutzungsformen gibt, die ausschließlich aus Gründen der Anonymität das Prinzip des unbeobachteten Informationsaustauschs verfolgen. Im Hinblick auf den Finanzsektor und speziell den Zahlungsverkehr kämen für Anwendungen der DLT keine öffentlichen Ledger, sondern in diesem Fall nur private Blockchain-Netzwerke in Frage. Diese wären dann nur für einen ausgewählten Teilnehmerkreis zugänglich und einsehbar. Die Durchführbarkeit solcher Netzwerke auf einem globalen Level muss allerdings zuerst noch geprüft und bewertet werden.

[50] GwG (idF v. 13.08.2008) § 11 Abs.I.

[51] Vgl. Tapscott, Don; Tapscott, Alex: Die Blockchain Revolution S.352.

[52] Fraunhofer - Institut (2017b): BLOCKCHAIN - Technologien, Forschungsfragen und Anwendungen, S. 28.

4 Wertpapierhandel der Zukunft mittels Blockchain

Bei dem Einsatz von Blockchain in Anwendungsbereichen der Finanzbranche wird neben dem Zahlungsverkehr, der Wertpapierabwicklung das größte Potenzial zugeschrieben.

Blythe Masters, eine bekannte Investmentbankerin und Größe an der Wall Street wechselte nach jahrelanger Tätigkeit für JPMorgan 2015 als CEO zum New Yorker Start-up Digital Asset Holdings, ein Fin Tech Unternehmen, dass sich auf DLT-basierte Produkte für Finanzdienstleister spezialisiert hat. Auf die Bedeutung von Blockchain für die Finanzwelt angesprochen sagte sie Folgendes: „Ich nahm das ebenso ernst, wie man das Konzept des Internets in den 1990er - Jahren hätte ernstnehmen sollen. Das ist eine ganz große Sache, die die Funktionsweise unserer Finanzwelt verändern wird.“[53]

Ob es tatsächlich möglich ist, die Abwicklung von Wertpapieren in der Zukunft mittels DLT durchzuführen und welche Herausforderungen auf dem Weg dahin zu bewältigen sind, soll in den folgenden Abschnitten geklärt werden.

4.1 Wertpapierhandel heute

Was zeichnet die Emission von Wertpapieren heutzutage aus und welche aktuellen Probleme sind der Grund, worum der Einsatz von Blockchain gerade auf diesem Gebiet Sinn macht? Diese Fragen sollen nun in den nächsten beiden Unterpunkten geklärt werden.

4.1.1 Überblick

Zunächst stellen wir uns wieder der Frage, was ist ein Wertpapier und wie kann damit gehandelt werden? Laut Gabler beschreibt ein Wertpapier ein „in Form einer Urkunde verbrieftes Vermögensrecht, zu dessen Ausübung der Besitz der Urkunde nötig ist“[54]

Zu den bekanntesten Wertpapieren zählen Aktien, Devisen, Zertifikaten, Futures sowie Waren und Rohstoffe. Die Plattformen, auf denen diese Wertpapiere gehandelt werden sind zum einen Börsen-und Handelsplätze wie die bekannte New York Stock Exchange oder in Deutschland die Frankfurter Wertpapierbörse, aber

[53] Vgl. Tapscott, Don; Tapscott, Alex: Die Blockchain Revolution, S. 93.

[54] Heldt, Dr. Cordula (2018): Wertpapier.

auch elektronische Handelssysteme, über die der sogenannte außerbörsliche Direkthandel abgewickelt wird. Möchte man selbst mit Wertpapieren handeln so geht das nur über ein Wertpapierdepot bei einer Bank oder einem Broker.

Um zu verstehen, wie Blockchain die Abläufe und Prozesse beim Handel von Wertpapieren beeinflussen und verbessern kann ist es wichtig zu wissen, wie der Lebenszyklus eines Wertpapiers aussieht und welche Parteien involviert sind. Abbildung 9 auf der nächsten Seite stellt die folgenden vier Schritte bildlich da.

Schritt eins ist die Ausgabe bzw. Emission des Wertpapiers. Als gängigstes Beispiel kann man hier die Ausgabe von Aktien beim Börsengang eines Unternehmens nennen. Daran beteiligt sind der Emittent, in unserem Fall das Unternehmen, eine Depotbank, über die das Wertpapier ausgegeben wird und schließlich ein Zentralverwahrer, welcher die Wertpapiere in zentraler Stelle aufbewahrt.

Als nächstes folgt der Handel des Wertpapiers. Der Emittent verkauft Firmenanteile an Investoren über eine Depotbank. Intermediäre haben dabei eine Art Vermittlerfunktion. Schritt drei ist das Clearing, bei der ein Zentraler Kontrahent (aus dem Englischen von Central Counterparty Clearing House) die gegenseitigen Forderungen und Verbindlichkeiten von Käufer und Verkäufer feststellt. Intermediäre haben dabei wieder eine Vermittlerfunktion zwischen den beteiligten Parteien. Durch das Clearing sollen Liefer- und Zahlungsausfälle vermieden werden.

Abschließend erfolgt das Settlement, der Prozess, bei dem der Emittent das Wertpapier an den Käufer liefert und dieser dafür bezahlt. An diesem letzten Schritt sind die Depotbank, der Zentralverwahrer und Intermediäre beteiligt. Handelt es sich wie bei unserem Beispiel um den Verkauf einer Aktie, also ein Kassageschäft, dann muss spätestens zwei Handelstage nach Geschäftsabschluss Zahlung und Lieferung erfüllt sein. Diese zwei Tage bergen natürlich das Risiko eines Leistungsausfalls, indem beispielsweise der Käufer zwar bezahlt, der Verkäufer aber seiner Pflicht der Lieferung nicht nachkommt. Clearingstellen sollen dieses Risiko minimieren, was aber im Umkehrschluss den Emittenten wieder Gebühren und Sicherheitseinlagen kostet. [55]

Der Einsatz von Blockchain soll im Bereich Clearing und Settlement erfolgen, weil diese beiden Punkte mithilfe der neuen Technologie das größte Potenzial auf Verbesserung haben.

[55] Vgl. Zahrte, René: Funktionsweise und Auswirkungen der Blockchain - Technologie auf den Wertpapierhandel, S. 39-40.

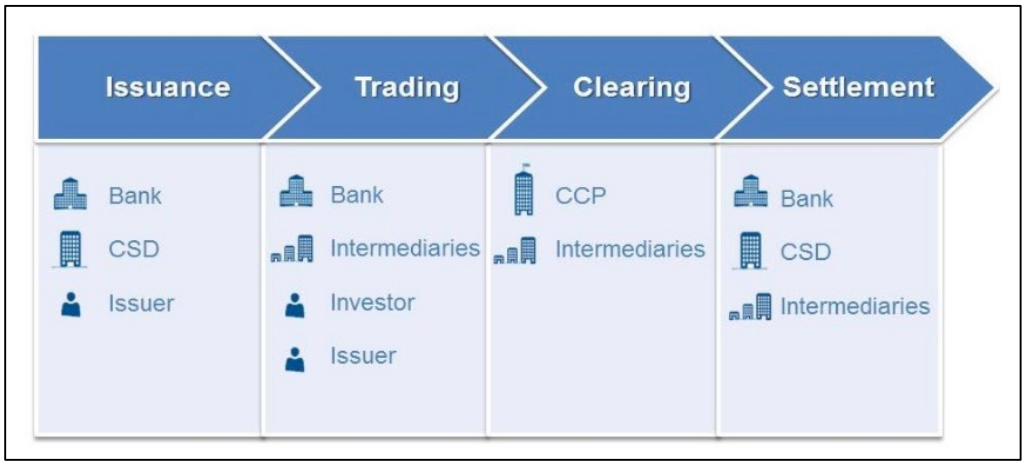

Abbildung 9: Lebenszyklus eines Wertpapiers[56]

4.1.2 Aktuelle Probleme

Auch beim Wertpapierhandel fällt wie beim Zahlungsverkehr auf, dass es eine Vielzahl von Intermediären gibt, die als Teil des Prozesses von der Ausgabe eines Wertpapiers bis zum Abschluss der Transaktion mitwirken. Allerdings ist deren Anzahl, wie im vorherigen Punkt beschrieben, ungleich höher. Depotbanken, Zentralverwahrer, Börsen, Zentrale Kontrahenten sowie Clearing- und Settlement - Häuser sind Teil des Lebenszyklus von Wertpapieren und machen die Abwicklung zeitintensiv, aufwändig, teuer und risikobehaftet. So benötigt man für den gesamten Prozess der Abwicklung eines Wertpapiers mehrere Tage, was neben dem enormen Zeitaufwand, aufgrund der anfallenden Gebühren und Transaktionskosten ebenfalls ein kostenintensives Geschäft für den Emittenten ist. Die Komplexität der Prozesse und gleichermaßen die Anfälligkeit für Fehler ist hoch und bedeutet ein hohes Maß an Abstimmung und Koordination unter den beteiligten Parteien. Selbst, wenn mit Einführung der TARGET2-Securities Plattform im Zuge der Europäischen Währungsunion der Wertpapierhandel innerhalb Europas kosteneffizienter und attraktiver gestaltet wurde, gibt es weltweit noch kein einheitliches System, das den globalen Wertpapierhandel zu vernünftigen Konditionen ermöglicht. International haben viele Länder ihr eigenes rechtliches und regulatorisches Instrumentarium. Das führt dazu, dass das Handelsvolumen der einzelnen Länder unter dem eigentlich möglichen liegt und es eine geringere Liquidität an individuellem Aktienkapital gibt.[57]

Eine weitere Herausforderung, welche ebenfalls der Vielzahl an beteiligten Intermediären geschuldet ist, beschreibt die zum Teil unzureichende Transparenz und Möglichkeit der Nachverfolgung, wer Eigentümer welches Wertpapiers ist. Die nationalen Zentralverwahrer haben zum Beispiel Datenbanken von enormen Ausmaß um

[56]Siehe https://www.ecb.europa.eu/paym/pdf/infocus/20160422_infocus_dlt.pdf, S.3.

[57] Vgl. Federal Reserve Bank of New York: Securities Trading and Settlement in Europe: Issues and Outlook, S.1.

die korrekten Besitzverhältnisse der einzelnen Wertpapiere sicherzustellen. Ein riesiger Aufwand an Speicherplatz und Personal ist die Folge.

4.2 Erwartete Vorteile durch Implementierung von Blockchain

Der Einsatz von Blockchain im Bereich der Wertpapierabwicklung wird mit verschiedenen Erwartungen und Hoffnungen verbunden. Es wird vermutet, dass Blockchain ähnliche Effizienzgewinne schaffen kann, wie die Einführung des elektronischen Handels auf dem Sekundärmarkt in jüngster Vergangenheit. So gab es in der Vergangenheit weltweit bereits verschiedene Pilotprojekte, bei denen der Einsatz von Blockchain von Marktteilnehmern auf globaler Ebene getestet wurde. Aus deutscher Sicht haben hier die Landesbank Baden-Württemberg und die Daimler AG eine Vorreiterrolle übernommen, indem sie 2017 ein Schuldscheindarlehen über 100 Mio. € mittels einer Blockchain platziert haben. Vielversprechendes Potenzial bieten zudem die kontrovers diskutierten Initial Coin Offerings, als eine Möglichkeit zur Kapitaleinsammlung in der digitalen Welt.

4.2.1 Verschlankung von Prozessen im Bereich Wertpapierabwicklung

Denken wir an den Lebenszyklus eines Wertpapiers zurück und schauen uns die vier Schritte an, dann hat Blockchain das Potenzial, das Clearing und Settlement bestimmter Wertpapiergeschäfte deutlich zu beschleunigen. Der gesamte Prozess wäre damit deutlich schlanker und effizienter. Theoretisch ist es möglich, dass mit dem Einsatz von Blockchain, Clearing und Settlement unmittelbar und fast in real-time durchgeführt werden könnten. Handelsbestätigung, Affirmation, Zuteilung und Settlement könnten in einem Schritt durchgeführt werden und den Reconcilliation – Prozess praktisch überflüssig machen. Das würde in eine Reihe von Vorteilen resultieren, darunter ein reduziertes Counterparty Risk (Risiko, dass die Gegenpartei ihren vertraglichen Verpflichtungen nicht nachkommt) und ebenfalls geringere Misserfolge und Strafen beim Settlement.

Eine weitere Verbesserung, die dem Einsatz von Blockchain in diesem Bereich zugeschrieben wird, ist die verbesserte Aufzeichnung der Besitzverhältnisse bei einer Vielzahl von Wertpapieren und der Verwahrung von bestimmten Vermögenswerten. Aufgrund des hohen Grades an Transparenz und der Netzwerkstruktur mit zentraler, für jeden Teilnehmer zugänglicher Datenbank bei einer Blockchain, könnte es die Rückverfolgbarkeit von Transaktionen verbessern und die Besitzverhältnisse während des gesamten Lebenszyklus eines Wertpapiers transparenter gestalten. So gibt es bereits einige Unternehmen, die DLT zur Ausgabe von privaten Aktien und zur Aufbewahrung der Aktionärsdaten benutzen. Die Verwendung von Smart Contracts könnte außerdem die Durchsetzung von Vertragsbedingungen erhöhen und für eine Automatisierung bestimmter Prozesse im Bereich des Back Office sorgen. Dies kommt vor allem bei Ge

schäften, die Rückbestätigungen oder Garantien von Geschäftspartnern benötigen, zum Tragen. Ein einfaches Beispiel ist hier die Auszahlung von Zinsen oder Dividenden, die dadurch völlig automatisiert erfolgen würden, solang bestimmte Bedingungen erfüllt sind. Diese Prozessoptimierung könnte zu einer Reduzierung von Fehlern und rechtlichen Streitigkeiten führen. [58]

Als letzter Punkt in Bezug auf die Verschlankung von Prozessen ist die Möglichkeit der Verarbeitung von Transaktionen auf dem Wertpapiermarkt und speziell in der Wertpapierabwicklung quasi rund um die Uhr, 24 Stunden am Tag und 7 Tage in der Woche. Weil keine zentrale Instanz wie bisher Börsen oder andere Handelsplätze benötigt werden und der Ledger rund um die Uhr geöffnet sein könnte, würde dieser Umstand die Globalisierung des Wertpapierhandels weiter vorantreiben.

4.2.2 Reduziertes Counterparty Risk

Wie im vorherigen Punkt schon kurz angeschnitten, bedeuten kürzere Clearing- und Settlement-Prozesse ein geringeres Counterparty Risk für die beteiligten Akteure, weil die Zeitspanne der Transaktionsabrechnung reduziert wird und diese damit einem geringeren Ausfallrisiko ausgesetzt sind. Ein Großteil der Transaktionen würde sofort abgeschlossen und könnte eine Clearingstelle als Intermediär überflüssig machen. Die Clearingstelle hat als Hauptaufgabe, das Counterparty Risk zu eliminieren und übernimmt das Risiko eines Zahlungs- oder Lieferausfalls der Transaktionspartner. In Zukunft könnte dies automatisiert via Blockchain erfolgen. Für bestimmte Transaktionen ist es notwendig, dass Sicherheiten von den Transaktionsteilnehmern hinterlegt werden, um das Counterparty Risk abzudecken. Bei einem verkürzten Settlement-Prozess reduziert sich logischerweise auch die benötigte Anzahl an Sicherheiten die beim Settlement benötigt werden. Das bedeutet auch, dass die verpfändeten Sicherheiten schließlich viel schneller wieder auf dem Markt verfügbar wären. Eine verbesserte Marktliquidität wäre als Folge dessen denkbar.

4.2.3 Vereinfachtes regulatorisches Reporting

Es wird davon ausgegangen, dass mithilfe von Blockchain die Funktionen des Reporting sowohl bei den Finanzinstituten als auch bei den Aufsichtsbehörden verbessert werden können, indem die Prozesse der Sammlung, Konsolidierung und Verbreitung von Daten zum Zwecke des Risikomanagements und des Reporting erleichtert werden. Weil sich nun alle relevanten Informationen bezüglich des regulatorischen Meldewesens bzw. Reportings auf einem einzigen, überprüfbarem Ledger befinden, könnten Organisationen ihre vorgeschriebenen regulatorischen Meldepflichten auf viel effizientere Weise durchführen.[59]

[58] Vgl. ESMA: The Distributed Ledger Technology Applied to Securities Markets, 5-6.

[59] Vgl. ECB: Distributed Ledger Technology, S.4.

So wäre es auch denkbar, dass die Aufsichtsbehörden spezielle Zugangsrechte zum Ledger der jeweiligen Organisation bekommen, um erforderliche Daten abzurufen und zu überprüfen. Dass diese Möglichkeit nicht nur theoretisch gut klingt, sondern auch in der Praxis umsetzbar ist, bewies eine Interessegruppe aus der Finanzbranche bereits 2016. Die Firmen Irish Funds, Deloitte, Northern Trust und State Street konnten den Einsatz von Blockchain zum Verwalten und Überwachen von regulatorischem Reporting erfolgreich testen. Die Kollaboration erschuf ein Proof-of-Concept für regulatorisches Reporting, bei der die Blockchain genutzt wurde um Transaktionen zu erfassen, das Reporting mit der Fähigkeit von Smart Contracts zu managen und ebenfalls die Compliance zu verbessern. Die sogenannte „RegChain" bedient sich Smart Contracts um die Anforderungen an das Reporting automatisch auszuführen und jegliche Änderungen der Daten durch autorisierte Beteiligte zu prüfen. Dadurch wird die sichere Verwahrung, Integrität und Qualität der Daten gesichert und außerdem das gesamte Management im Bereich Reporting vereinfacht, weil neue regulatorische Anforderungen oder Bestimmungen einmal als Code auf der Blockchain programmiert werden und schließlich über das gesamte Netzwerk an alle Teilnehmer verbreitet werden. Selbst wenn die Studie von Irish Funds und co. auf den Bereich Investment Fonds ausgerichtet war, so ist die Vereinigung von anderen regulatorischen Reports im Bereich des Möglichen. [60]

4.2.4 Kapitalaufnahme mithilfe von ICOs

Weil BaFin und auch das Pendant in den USA, die Securities and Exchange Comission, im Einzelfall entscheiden können, dass Token als Finanzinstrumente im Sinne des Wertpapierhandelsgesetztes oder der europäischen Finanzmarktrichtlinie (MiFID II) ein Wertpapier im Sinne des Wertpapierprospektgesetzes sind, wird dieser Punkt mit im Bereich Wertpapierabwicklung erfasst. [61] Besonders für Klein- und mittelständische Unternehmen ohne die Möglichkeit eines Börsengangs bieten ICOs eine gute Möglichkeit, sich abseits des traditionellen und regulierten Kapitalmarkts zu finanzieren. Auch wenn der Token-Sale bisweilen für Unternehmen ausgelegt ist, deren Geschäftsmodell auf Kryptowährungen basiert, so ist es auch denkbar, dass Unternehmen in anderen Geschäftsbereichen Wertpapiere direkt auf dem Ledger ausgeben, damit Zugang zu einem größeren Pool an Investoren erhalten und ihre Finanzierungsmöglichkeiten erweitern.

Die Vorteile für Emittenten des Tokens als auch für die Investoren sind dabei vielfältig. Für die Emittenten des Tokens kann zum einen eine innovative Geschäftsidee ohne die regulatorischen Hürden und die hohen Transaktionskosten eines IPOs in die Tat umgesetzt werden. Hat das Unternehmen, welches den Token ausgibt wirtschaftlichen Erfolg, dann hat das eine enorme Wertsteigerung zur Folge und Investoren werden entweder am Erfolg beteiligt oder die erworbenen Tokens haben entsprechend einen hohen Wiederverkaufswert.

[60] Vgl. Irish Funds: Regulatory Reporting Blockchain, S.2-3.

[61] Vgl. BaFin (2018): Initial Coin Offerings.

Weil Tokens nur digital veräußert werden besteht für die potenziellen Investoren auch die Möglichkeit der frühzeitigen Teilhabe am Projekt und zukünftigen Produkten. Ein weiterer Vorteil für sowohl den Emittenten als auch den Investor ist die mit der Ausgabe des Tokens erhaltene Liquidität, die gegen andere Kryptowährungen oder Fiatgeld eingetauscht werden kann und die Möglichkeit für den Emittenten über nicht veräußerte Tokens zusätzlich wirtschaftliche Mittel zu erhalten. Dieses letzte Ereignis wird auch als Double-Fundraising bezeichnet.[62]

Dass ICOs international, vor allem in den Hubs USA, Schweiz und Singapur als Alternative zur Risikokapitalfinanzierung (Venture Capital) weiterhin Konkurrenz machen, zeigen aktuelle Zahlen vom Juni 2018: so wurden in den ersten fünf Monaten 2018 insgesamt 537 ICOs mit einem Gesamtvolumen von 13,7 Mrd. USD durchgeführt, was mehr als alle ICOs im vorherigen Jahren zusammengerechnet ist.[63] Im Vergleich dazu gab es in den USA im ersten Halbjahr 2018 Börsengänge mit einem Emissionsvolumen von insgesamt 28,6 Mrd. USD.[64]

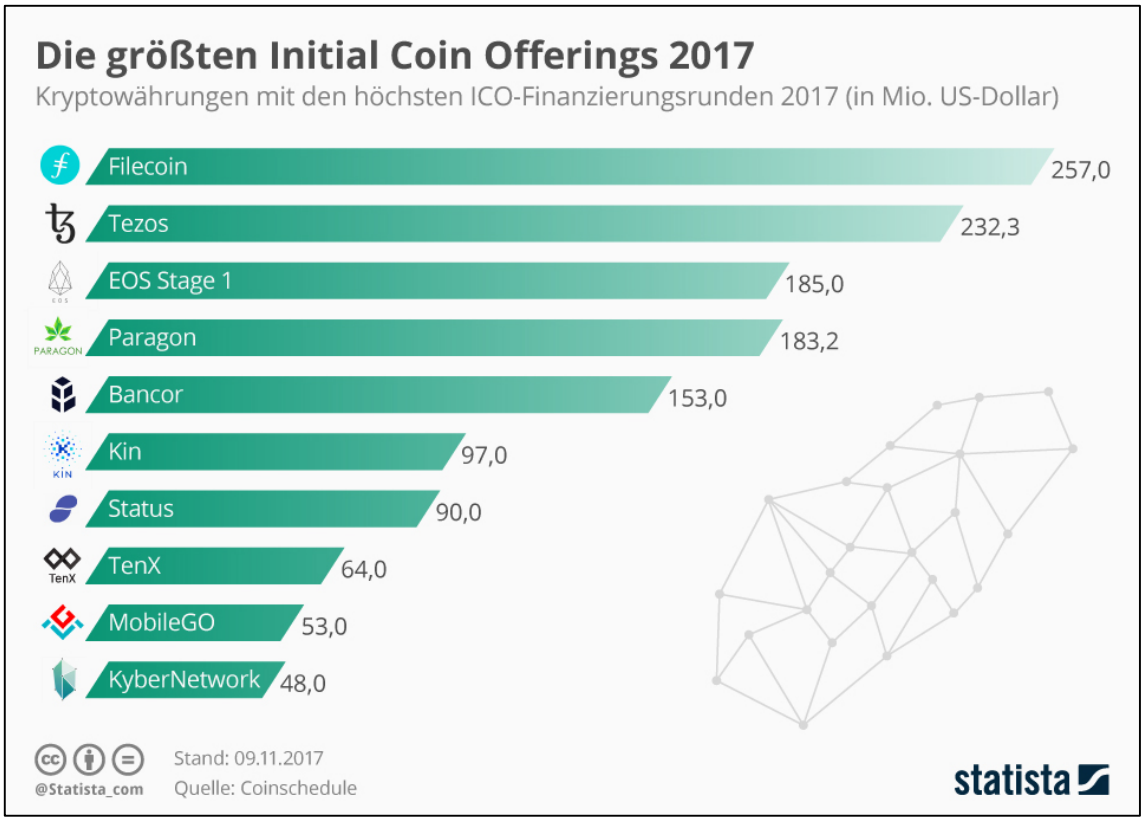

Abbildung 10: Die größten Initial Coin Offerings 2017[65]

[62] Vgl. Hahn, Christopher; Wohns, Adrian: Initial Coin Offering (ICO), S.3.

[63] Vgl. Strategy&/pwc: Initial Coin Offerings - Eine strategische Perspektive, S.1.

[64] Statista (2018b): Emissionsvolumen der Börsengänge in den USA von 1999 bis zum 1. Halbjahr 2018 (in Milliarden US-Dollar).

[65] Siehe https://de.statista.com/infografik/11763/kryptowaehrungen-mit-den-hoechsten-ico-finanzierungsrunden/.

Betrachtet man sich die Übersicht in Abbildung 10, dann sind im Bereich der Finanzwirtschaft vor allem zwei ICOs besonders interessant: Bancor und TenX. Bancor beschreibt ein dezentrales Liquiditätsnetzwerk mithilfe dessen man jeglichen Token halten und in andere Token umsetzten kann, ohne dabei eine Gegenpartei zu benötigen. Ein Modell, das auch für den Wertpapierhandel in Zukunft von Interesse sein könnte. Zum zweiten TenX, ein Unternehmen, welches Krypto-Debitkarten und -wallets ausgibt, mit dem Ziel, damit für Einkäufe in Bitcoin und sämtlichen anderen Kryptowährungen zu bezahlen. Ein System, welches im Bereich des internationalen Zahlungsverkehrs definitiv Zukunftspotenzial hat.

4.3 Herausforderungen

Auch im Bereich Wertpapierabwicklung ist es unstrittig, dass der Einsatz von Blockchain Vorteile und Verbesserungen bringen kann. Allerdings müssen dazu bestimmte Bedingungen und Voraussetzungen erfüllt werden. Zum einen wird bei allen Vorteilen der Technologie davon ausgegangen, dass diese von einem Großteil der Marktteilnehmer akzeptiert wird. Daraus resultieren dann weitere Fragen hinsichtlich der Zusammenarbeit von verschiedenen Organisationen und Systemen, inwiefern Standardisierung eine Rolle spielt und natürlich auch die technische Umsetzung. Zum anderen muss geklärt werden, wie Datenschutz und Privatsphäre von Benutzern der Blockchain und deren Kunden mithilfe entsprechender Sicherheitsmaßnahmen sichergestellt werden kann. Außerdem müssen regulatorische und rechtliche Fragestellungen zum Einsatz von Blockchain im Bereich Wertpapierabwicklung beantwortet werden.

4.3.1 Probleme in Hinblick auf Governance und Privatsphäre

Netzwerke von vertrauenswürdigen Parteien mit einem stabilen Governance-System bilden die Grundlage der heutigen Wertpapiermärkte. Im Gegensatz zu einem DLT Netzwerk, bei dem es kein zentrales Leitungsgremium gibt und kein alleiniges Mitglied für die ordnungsgemäße Operation des Systems verantwortlich ist, basiert der jetzige Wertpapierhandel auf Governance, vorgeschrieben durch Regulierungen oder Vereinbarungen zwischen Teilnehmern. Einsatz von öffentlichen Ledgers stellt im Hinblick auf einen reibungslosen Ablauf und effektives Management also Risiken für Märkte und Investoren da. Um dieses Problem zu umgehen untersuchen viele Organisationen die Möglichkeit, ein privates DLT Netzwerk zu verwenden, dass eine Governance-Struktur enthält, die berücksichtigt, dass sich die Teilnehmer innerhalb des Netzwerks kennen und untereinander vertrauen. Handelt es sich wie beim Wertpapiergeschäft um eine private Blockchain, bei der mehrere Organisationen eines gesamten Industriezweiges beteiligt sind, stellen sich weitere Fragen im Hinblick auf die Funktionsweise des Netzwerkes und wer welche Verantwortlichkeiten trägt. Dabei müsste geklärt werden, wer welche Rolle bei der Erstellung der Governance-Struktur innerhalb des Netzwerks spielt, welche Partei für die Einhaltung der festgelegten Regeln sorgt und inwieweit Teilnehmer bei Missachtung dieser Regeln zur Rechenschaft gezogen werden. Es müsste festgelegt werden, wer für die tägliche Abwicklung verantwortlich ist und wie mit Notfällen zum Beispiel technischen Problemen oder

ernsthaften Störungen des Geschäftsablaufs umgegangen wird. Ein weiterer Punkt wäre, wie mit Interessenskonflikten unter den Teilnehmern in Bezug auf die Abwicklung oder Teilhabe des Systems umgegangen wird. All diese Probleme und Fragestellungen müssten geklärt werden, bevor man damit beginnen kann, die speziellen Anforderungen des Wertpapiergeschäfts auf die Eigenschaften und Funktionen von Blockchain anzupassen. [66]

Die Geheimhaltung von bestimmten Informationen ist eine weiter charakteristische Eigenschaft im Wertpapiergeschäft. So ist die Identität der Teilnehmer einer bestimmten Transaktion in den meisten Fällen nicht öffentlich, außer es sei denn, dass rechtliche oder regulatorische Bestimmungen es verlangen. Selbst wenn es mithilfe von Kryptografie bereits möglich ist, dass über spezielle, geheime Zugänge (Private Keys) nur die Teilhabenden der Transaktion Zugang zu den vertraulichen Daten bekommen ist es noch unklar, inwieweit die Transaktionen dann validiert werden können, wenn andere Teilnehmer des Netzwerks keine öffentlichen Informationen dazu besitzen. Aus diesen Gründen ist es wichtig, dass private Ledgers beim Einsatz im Wertpapierhandel so entworfen werden, dass die Privatsphäre der Teilnehmer, wenn nötig, entsprechend geschützt ist.[67]

4.3.2 Regulatorische Bedenken

Denken wir zurück an den Punkt 4.2.4, dann wurde bereits erwähnt, dass Initial Coin Offerings eine unregulierte Art der Kapitalaufnahme und im Grunde nichts Anderes als Crowdfunding sind. Ein unreguliertes Finanzmarktgeschäft wie dieses birgt aber auch enorme Risiken. So bietet die Anonymität und nicht stattfindende staatliche Kontrolle Kriminellen die Möglichkeit, unter dem Vorwand, eine innovative Geschäftsidee zu verkaufen, Investoren zu betrügen. Dieser Umstand und das Fehlen eines festen Ordnungsrahmens weckt bei potenziellen Investoren nicht gerade Vertrauen. Immer wieder werden Anleger mit der Aussicht auf hohe Erträge gelockt und fallen auf Betrüger, zum Teil organisierte Kriminelle herein und es droht ein Totalverlust der Investition. BaFin warnt dabei vor zahlreichen Risiken und stellt fest, dass ein ICO zwar an den Börsengang angelehnt ist, das aber weder technisch noch rechtlich in der Realität der Fall ist. Zudem unterliegen die im Rahmen des ICOs erworbenen Token häufig großen Preisschwankungen, weil sich zum einen die Vorhaben noch in einem experimentellen Stadium befinden und Entwicklung sowie Geschäftsmodell wenig erprobt sind und zum anderen sind oftmals die „Whitepaper“ und Vertragsbedingungen unzureichend, unverständlich und bisweilen irreführend. Weil es keine gesetzlichen Vorschriften und Vorgaben gibt ist der Verbraucher oftmals auf sich selbst gestellt herauszufinden ob Identität, Seriosität und Bonität des Verkäufers vertrauenserweckend genug sind, um in dessen Projekt zu investieren. [68]

[66] Vgl. FINRA: Distributed Ledger Technology: Implications of Blockchains for the Securities Industry, S. 7-8.

[67] Vgl. ESMA: The Distributed Ledger Technology Applied to Securities Markets, S.9-10.

[68] Vgl. BaFin (2017): Verbraucherwarnung: Risiken von Initial Coin Offerings (ICOs).

Im Jahr 2017 hat BaFin bei insgesamt 36 ICOs geprüft, ob alles mit rechten Dingen zugeht und bei vier Verfahren wurde den beteiligten Unternehmen ihre Tätigkeiten sogar untersagt und die zuständigen Strafverfolgungsbehörden eingeschaltet.[69]

Ein weiterer Beweis, dass Initial Coin Offerings von vielen Finanzexperten als eine extrem risikoreiche Art der Investition angesehen wird, lieferte kürzlich eine Studie von einem College aus Boston, nach dem ca. 56 % der Startups die Gelder mittels Token-Sale einsammeln, innerhalb von vier Monaten nach dem Initial Coin Offering vom Markt verschwinden.[70]

Um weiteres Vertrauen der breiten Öffentlichkeit in ICOs zu schaffen wird es in Zukunft wichtig sein, dass internationale Absprachen bezüglich der Regulierung und rechtlichen Einordnung getroffen werden. Bisher gibt es weltweit noch keinen einheitlichen Konsens unter den Ländern und jeweiligen Finanzbehörden, inwieweit ICOs reguliert werden sollen. Nicht nur im Bereich der ICOs gibt es Bedenken zum Thema Regulierung, unzählige andere Bereiche im Wertpapierhandel sind mithilfe von zahllosen nationalen und internationalen Regeln und Gesetzten reguliert, die alle auf zentral organisierten Marktstrukturen basieren. Ein Beispiel ist die Art und Weise, wie Geldanlagen und Wertpapiere aktuell aufbewahrt beziehungsweise mit diesen umgangen wird. Die verantwortlichen Börsenmakler unterliegen in ihrem Aufgabenbereich einer Anzahl von Anforderungen wie beispielsweise der Regel 15c3-3 aus dem amerikanischen Wertpapierbörsengesetz bei dem es heißt: „the broker-dealer must maintain physical possession or control over customers' fully paid and excess margin securities." [71]

Ein DLT Netzwerk würde eine neue Möglichkeit schaffen, wie Geldanalagen und Wertpapiere aufbewahrt werden, bestehende Regulierungen müssten aber auf die neue Technologie angepasst werden um auch in Zukunft die sichere Verwahrung und den Schutz dieser Geldmittel für den Kunden garantieren zu können.

Ein weiteres Beispiel verdeutlicht die Regel 15c3-1 des amerikanischen Wertpapierbörsengesetzes in Bezug auf die Verpflichtungen der Firmen in Sachen Eigenkapitalanforderungen. Darunter heißt es, dass Börsenmakler zu jeder Zeit einen Mindestbestand an aus hochliquiden Vermögenswerten bestehendem Nettokapital unterhalten müssen. Handeln Firmen nun mit Token, digitalen Währungen oder anderen auf Kryptografie basierenden Wertpapieren wird zu überlegen sein, inwieweit diese die Regel der Nettokapitalberechnung 15c3-1 beeinflussen und gleichfalls inwieweit diese anrechenbar sind. [72]

[69] Vgl. Krempl, Stefan: ICO: Bafin hat 2017 vier Crowdfundings mit Kryptogeld untersagt.

[70] Vgl. Kharif, Olga: Half of ICOs Die Within Four Months After Token Sales Finalized.

[71] SEC Securities Exchange Act Release No. 70073 (Idf. v. 30.07.2013) Regel 15c3-3.

[72] Vgl. FINRA: Distributed Ledger Technology: Implications of Blockchains for the Securities Industry, S. 13.

4.3.3 Netzwerk – Sicherheit

Sicherheit ist eines der entscheidenden Themen die bei der Anwendung von Blockchain bedacht werden muss, speziell im Hinblick auf die verteilte Netzwerkstruktur und die mögliche Teilnahme von Parteien aus der ganzen Welt. Selbst wenn es nach dem heutigen Stand nahezu unmöglich scheint, dass ein verteilter Ledger bzw. eine Blockchain erfolgreich gehackt werden kann, sollte man dennoch vorsichtig sein, ob und wie die DLT die Gefahr von Cyber-Angriffen in bedeutender Weise reduzieren kann.

Es ist unbestritten, dass sich die Technologie noch in einer frühen Entwicklungsphase befindet und in weiten Teilen unerprobt ist. Markteilnehmer versuchen immer noch festzustellen, welchen Umfang potenzielle Sicherheitsrisiken von dieser neuen Technologie ausgehen und wie mit diesen Risiken umzugehen ist. So kann es in Zukunft aufgrund fortschreitender technologischer Entwicklungen wie zum Beispiel Quanten-Computern möglich sein, dass die jetzigen Sicherheitsvorkehrungen von Blockchain im Laufe der Zeit bedeutungslos werden und die kryptografischen Algorithmen, welche Blockchain zugrunde liegen, geknackt werden. Es stellt sich zudem die Frage nach dem „schwächsten Glied“ in der Kette. Wenn nur ein Code im gesamten Netz fehlerhaft ist oder ein Teilnehmer etwa Opfer einer Cyber-Attacke wird, könnten manipulierte Informationen eindringen und für eine signifikante Störung des gesamten DLT-Netzwerks sorgen.

Dringt ein Angreifer in ein privates Netzwerk von Banken und Finanzunternehmen einen, die sich zum Zwecke des Wertpapierhandels zusammengeschlossen haben, hätte dieser potenziell Zugriff auf allen sich im Netzwerk befindlichen Daten. Schäden im Umfang von mehreren Milliarden Euro wären denkbar. Daran angeknüpft stellt sich die Frage, wer trägt den Schaden eines solchen Betruges und welche Entschädigungsrechte haben Kunden und Investoren, wenn deren Vermögenswerte gestohlen oder manipuliert wurden. [73] Diese und weitere Fragestellungen müssen geklärt und beantwortet werden, bevor ein globaler und massentauglicher Einsatz von Blockchain nicht nur im Bereich Wertpapierhandel in Frage kommt und die Sicherheit der Daten aller Netzwerkteilnehmer gewährleistet werden kann.

[73] Vgl. ebd. S.10.

5 Verwendung von Blockchain über die Finanzbranche hinaus

Die Anwendungsmöglichkeiten von Distributed Ledger Technologie und Blockchain im Speziellen sind nicht nur auf den Finanzsektor beschränkt. Zahlreiche weitere Geschäftsbereiche und Institutionen erhoffen sich durch den Einsatz von DLT Verbesserungen und Einsparungen. Ob nun im Bereich Immobilien, zur Vereinfachung der Verkaufsabwicklung, über das Supply Chain Management mit dem Potenzial, die Wertschöpfungskette transparenter und fairer zu gestalten bis hin zur sogenannten Share Economy, bei der es in Zukunft mithilfe von Blockchain-Technologie viel einfacher möglich sein soll, ganz oder nur teilweise genutzte Ressourcen wie z.B. das eigene Auto oder die eigene Wohnung geteilt zu nutzen. Ein weiterer vielversprechender Anwendungsbereich ist der öffentliche Sektor. So ist es vorstellbar, dass mithilfe einer Blockchain-Lösung die Identitäten von Personen verifiziert werden könnten und Ausweisdokumente viel einfacher aufstellbar und fälschungssicher gemacht werden. Zudem ist es denkbar, dass die Blockchain als riesige Datenbank mit allen relevanten Informationen die Steuerabrechnung und -bezahlung der Zukunft sein könnte. Im Bereich Rechtswesen hat DLT das Potenzial die Prozesse der Verifikation von Urheberschaft und Dokumenteninhalten sowie die Übertragung von Eigentumsrechten zu revolutionieren. [74] Um den Rahmen dieser Arbeit nicht zu sprengen, wird sich im Punkt 5 auf jeweils zwei Anwendungsbeispiele aus dem Bereich Wirtschaft und öffentlicher Sektor beschränkt.

5.1 Weitere Anwendungsmöglichkeiten in der Wirtschaft

Führende Wirtschaftsunternehmen befassen sich schon seit geraumer Zeit mit der Blockchain-Technologie und in zahlreichende Pilotprojekten konnte die Praxistauglichkeit bereits bewiesen werden. Wie genau die Anwendungsmöglichkeiten in den Bereichen Supply Chain Management und Sharing Economy aussieht, soll in den folgenden zwei Punkten geklärt werden.

5.1.1 Supply Chain Management

Die Verwaltung von Lieferketten in der heutigen Zeit ist, unabhängig ob es sich dabei um Informationen, Produkte, Dienstleitungen oder Geld handelt, extrem komplex und vielschichtig. Selbst im Zeitalter der Digitalisierung ist das Verwalten

[74] Vgl. Fraunhofer - Institut (2016): BLOCKCHAIN: GRUNDLAGEN, ANWENDUNGEN UND POTENZIALE, S.31.

der Prozesse im Supply Chain Management schriftlich auf Papier noch weit verbreitet. Eingeschränkte Transparenz und Möglichkeit der Zusammenarbeit verschiedener Netzwerke ist die Folge. Für Kunden oder Käufer eines beliebigen Produktes ist es beispielsweise unheimlich schwer dessen wahren Wert aufgrund der nichtvorhandenen Möglichkeit der Nachprüfbarkeit festzustellen. Ein weiterer Schwachpunkt im aktuellen System betrifft den Punkt Compliance. Steht der Verdacht von illegalen oder unethischen Praktiken im Raum ist es so gut wie unmöglich herauszufinden, an welcher Stelle der Lieferkette die Schwachstelle liegt und gleichermaßen, ob alle beteiligten Parteien die vorgegebenen Standards und Regeln einhalten. Zudem bieten bestehende Strukturen der Lieferkette nur schwer die Möglichkeit, sich an unerwartete Ereignisse oder auftretende Probleme, ohne eine signifikante Erhöhung der Betriebskosten, anzupassen. Eingeschränkte Flexibilität und geringe Effizienz machen es Lieferanten und Anbietern schwer, sich untereinander abzustimmen [75]

Der Einsatz von Blockchain Technologie hat das Potenzial, die jetzigen Schwachpunkte der Lieferkette inklusive Nachverfolgbarkeit, Compliance und Flexibilität zu korrigieren. In einer Studie aus dem Jahr 2017 hat Deloitte, ein international führendes Unternehmen in den Branchen der Wirtschaftsprüfung und Beratung, drei große Anwendungsfälle im Bereich Supply Chain Management identifiziert. Dabei handelt es sich um die Nachverfolgbarkeit von Produkten im pharmazeutischen Sektor, den Warenkauf im Automobilbereich und das sogenannte „Know Your Supplier“ Problem in der Lebensmittelindustrie.

Exemplarisch möchte ich in dieser Arbeit auf das „Know Your Supplier“ Problem genauen eingehen. Dabei geht es um die Fähigkeit, jedes Mitglied der Lieferkette bzw. jeden Lieferanten zu identifizieren, überprüfen und bestätigen zu können, um dann die Entscheidung zu treffen, ob man mit diesem eine Geschäftsbeziehung aufbauen oder weiterführen möchte. Doch wie könnte das Ganze in der Praxis funktionieren? Grundlage ist der Aufbau einer industrieweiten Plattform, mithilfe dessen die Akteure der Lebensmittelversorgungskette die Beziehungen zu ihren Lieferanten verwalten und die Qualität der Lebensmittel entlang der ganzen Kette überprüfen könnten. Mit solche einer Plattform hätten beispielsweise Restaurants und Großhändler durchgehende Sichtbarkeit über alle Lieferantenbeziehungen und könnten diese in Echtzeit überwachen und managen. Alle Teilnehmer der Plattform hätten eine vollständige Buchungskontrolle über sämtliche Nahrungsmittelbestandteile, welche vom damit verbundenen Lieferanten gekauft werden. Gleichzeitig könnte sichergestellt und bewiesen werden, dass Produkte der vorgeschriebenen Qualität entsprechen, indem die Qualitätszertifikate jedes Bestandteils von der zuständigen Regulierungsbehörde hochgeladen und abgeglichen werden. Weil alle Informationen mit einem Zeitstempel versehen werden, hätte jeder Netzwerkteilnehmer eine komplette und 100% transparente Übersicht über alle Lieferanten sowie deren Beziehungen und Aktivitäten. Es gäbe einen natürlichen Anreiz für Lieferanten die Qualität ihrer Produkte auf einem hohen Niveau zu halten um zum einen neue Geschäftsbeziehungen aufzubauen und

[75] Vgl. Deloitte: When two chains combine - supply chain meets Blockchain, S.2.

zum anderen zu vermeiden, dass die Regierungsbehörden Qualitätszertifikate für Produkte zurücknimmt und jeden im Netzwerk darüber informiert, der entweder direkt oder indirekt mit diesem Lieferanten eine Beziehung hat. Updates über die Qualität von Lebenszutaten in Echtzeit soll es Teilnehmern im vorgelagerten Prozess ermöglichen, bessere Entscheidungen beim Beschaffen und Einkauf zu machen und zudem das Risiko eines Imageschadens zu minimieren. Zuletzt wäre es mit dieser Plattform erstmalig möglich, dass alle Teilnehmer einer Lieferkette sich direkt untereinander austauschen und Bewertungen über bestimmte Lebensmittel und deren Bestandteile teilen könnten.[76] Abbildung 1 auf der folgenden Seite verdeutlicht wie die Lebensmittelversorgungskette heute aussieht und wie eben beschrieben die Zukunft von morgen mithilfe von Blockchain aussehen könnte.

Allerdings sind mit dem Einsatz von Blockchain im Bereich Supply Chain Management, wie auch in jedem anderen Bereich, gewisse Risiken verbunden. Speziell in diesem Bereich gibt es Bedenken, dass Wettbewerber die Beschaffungsdetails der Supply Chain einsehen könnten, Dritte auf irgendeinem Weg in Besitz der Daten kommen könnten oder Wettbewerber feststellen könnten, in welchem Umfang Waren in einer bestimmten Supply Chain in Bewegung sind. Eine genaue Abwägung der Vorteile und Risiken sowie die Ausarbeitung einer Blockchain-Strategie wird über den Erfolg oder Misserfolg bestimmen.

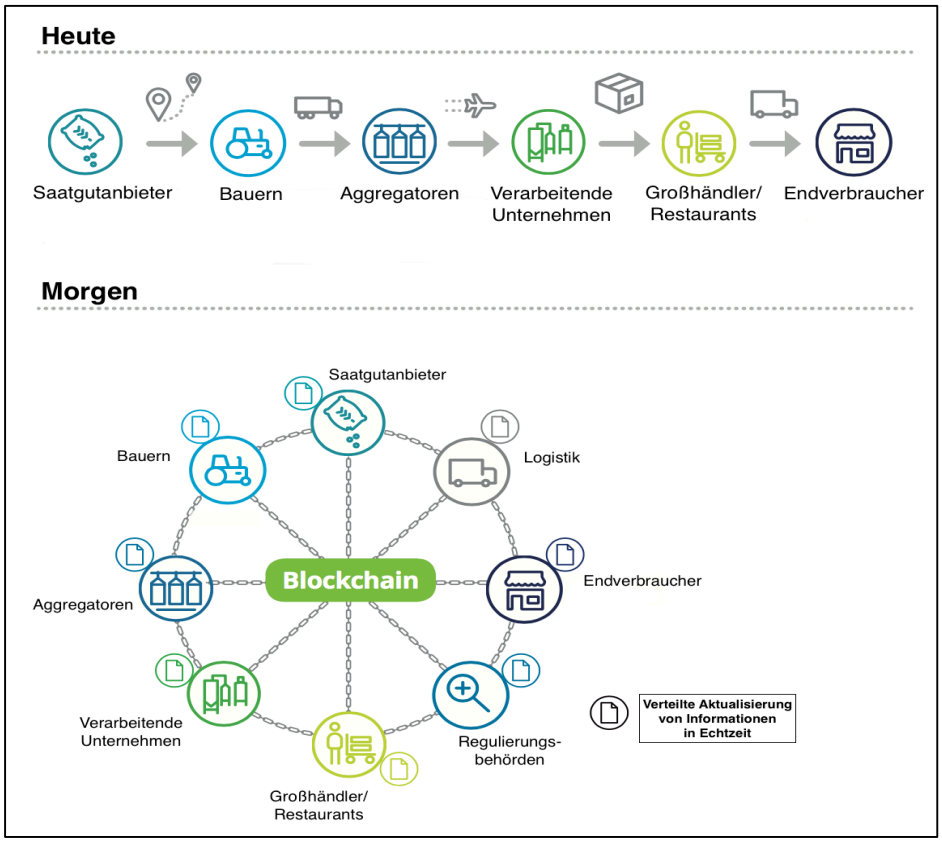

Abbildung 11: Lebensmittelversorgungskette heute und morgen[77]

[76] Vgl. Deloitte: When two chains combine - supply chain meets Blockchain, S.11-12.

[77] Siehe Deloitte: When two chains combine - supply chain meets Blockchain, S.14.

5.1.2 Sharing Economy

Die Sharing Economy ist eines der am schnellsten wachsenden Geschäftsfelder und erlaubt es Menschen ihr Eigentum zu vermieten, damit andere Personen es gegen entsprechende Bezahlung benutzen können. Laut einer weltweiten Umfrage von Nielsen, sind 68% der Befragten dazu bereit, ihre ungenutzten oder nur teilweise genutzten Vermögenswerte gegen einen finanziellen Ertrag mit anderen zu teilen.[78]

Bekannte Erfolgsmodelle sind zum Beispiel Airbnb, bei dem Reisende private Appartements oder Häuser mieten können, Uber als Ersatz für die klassischen Taxen oder car2go, bei dem man Autos von Privatpersonen stunden- oder tageweise ausleihen kann. Allerdings hat diese traditionelle Art der Sharing Economy auch ihre Schwachstellen. So wird von den Betreibern der Plattformen oft eine hohe Gebühr zur Nutzung dieser verlangt, die zentrale Ausrichtung vieler, aktuell auf dem Markt anzutreffender Plattformen berücksichtigt nur in bedingtem Maß die Interessen der Benutzer und außerdem gibt es auch Beispiele von Unternehmen, die ihre Macht ausgenutzt haben und sich ohne Wissen der Kunden Zugang zu deren privaten Daten verschafft haben. So stand Uber unter Verdacht, mithilfe einer Spionage-Software genannt „God View“ Fahrzeuge aufzuspüren und persönliche Informationen der Fahrer in den Autos sichtbar machen zu können. [79]

Um diese eben angesprochenen Probleme zu lösen, arbeiten mehrere Firmen an Sharing Economy Plattformen basierend auf Blockchain-Technologie. Diese neu entwickelten Plattformen sind um ein Vielfaches kostengünstiger in der Benutzung und bieten die bisher nur schwer herzustellende Transparenz. In den meisten Fällen gibt es keine Notwendigkeit mehr für einen Mittelmann, was die Kosten für Transaktionen, die bei zentral organisierten Plattformen 20-30% betragen, stark reduzieren bzw. eliminieren kann. Direkte peer-to-peer Transaktionen, die auf der Blockchain abgespeichert werden und so jedem Teilnehmer des Netzwerks die Möglichkeit geben, sämtliche Abläufe zu überprüfen und zu kontrollieren.

Eine Vorreiterrolle übernimmt auf diesem Gebiet das in Mittweida gegründete Startup slock.it der beiden Brüder Christoph und Simon Jentzsch. Anfangs bestand das Geschäftsmodell noch ausschließlich aus smarten Schlössern, die über programmierbare Schnittstellen mit der Ethereum-Blockchain verbunden sind. Mithilfe von Smart Contracts sollen die Schlösser dann bezahlt, geöffnet und wieder geschlossen werden. Nach dem Scheitern des ersten großen autonomen Fundings-Projekts in Ethereum wurde der Fokus auf die Entwicklung einer Sharing Economy Plattform gelegt. Nach einem erfolgreichen Seed sicherte sich das Unternehmen ein Funding von 2 Mio. $ und konnte zudem den deutschen Energieriesen Innogy sowie Siemens als Kooperationspartner gewinnen. Nach langer Arbeit wurde dann schließlich im November 2017 auf der Ethereum-

[78] Nielsen: Is Sharing the new Buying?

[79] Vgl. Taylor, Kate: 40 of the biggest scandals in Uber's history.

Developer-Conference in Mexiko das Universal Sharing Network (USN) vorgestellt. [80]

Laut Stephan Tual, einem der Mitbegründer von slock.it, wird es die Sharing Economy in der Weise revolutionieren, dass sowohl Firmen als auch einzelne Personen in der Lage sind, jedes beliebige verbundene und smarte Objekt an andere zu verleihen oder zu verkaufen. Aufbauend auf der öffentlichen Ethereum-Blockchain, soll es wie in Abbildung 2 vereinfacht dargestellt, Nutzern mithilfe von Apps auf Mobiltelefonen oder Computern die Möglichkeit geben, von überall auf der Welt aus jegliche smarte Objekte zu finden, zu lokalisieren und auszuleihen. Die Abwicklung findet dabei mittels Smart Contracts statt. Das Smartphone dient als Zugangsschlüssel und es bedarf keiner vorherigen Registrierung oder eines Logins. Die Verwendung von Blockchain offenbart dabei, inwieweit die Benutzererfahrung bei dieser Art von Plattformen vereinfacht werden kann:

1. App öffnen
2. Objekt in der Nähe finden
3. Bezahlung
4. Benutzung

Im Detail bietet das USN ein großes Potenzial der Kosteneinsparung, weil aufgrund der öffentlichen Netzinfrastruktur keine horrenden Kosten mehr für die Rechenzentren anfallen. Ein weiterer Vorteil ist die Möglichkeit der Interoperabilität, denn das Netzwerk mit dem man ein Auto ausleiht erlaubt ohne die Notwendigkeit von zusätzlicher Hard- oder Software, dass zum Beispiel das Auto gleichzeitig für anfallende Parkgebühren bezahlt. Aufgrund der kryptografischen Verschlüsselung und der Tatsache, dass es sich bei Ethereum um eine öffentliche Blockchain handelt, sind Sicherheit und Transparenz keine Schwachpunkte mehr.[81]

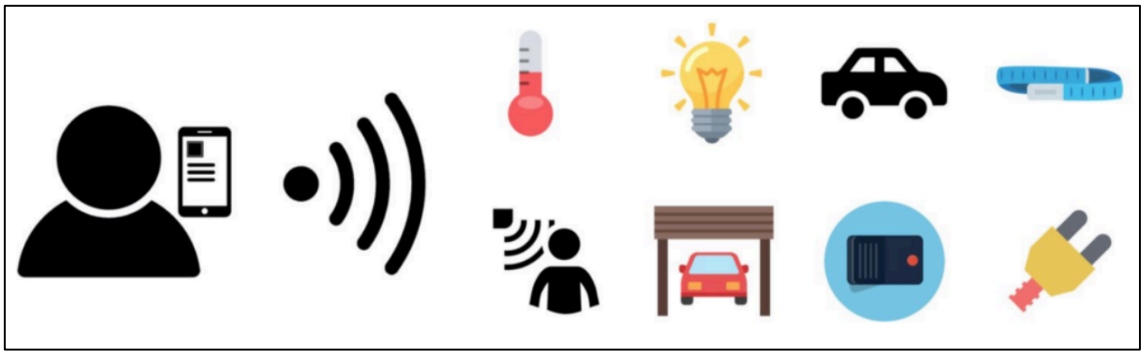

Abbildung 12: Das Universal Sharing Network[82]

[80] Vgl. Schmidt, Tobias: Was ist eigentlich aus Slock.it geworden?

[81] Vgl. Tual, Stephan: Slock.it secures $2 million USD seed funding to build next-generation Sharing Economy Platform.

[82] Siehe https://blog.slock.it/slock-it-secures-2-million-usd-seed-funding-to-build-next-generation-sharing-economy-platform-b795c6d1a92d.

5.2 Anwendungsbereich öffentlicher Sektor

Auch im öffentlichen Sektor haben die Versuche mit Blockchain-Anwendungen in den letzten Jahren rasant zugenommen. So gibt es bereits Projekte in über 20 Ländern weltweit, die sich mit der Architektur der Blockchain zur Bereitstellung und Beschaffung öffentlicher Dienstleistungen beschäftigen und eigene, individuelle Anwendungen basierend auf Blockchain entwickeln. [83]

5.2.1 Identitätsmanagement

Die Idee hinter DLT und Blockchain basiert auf einer eindeutigen Identifizierung der am Netzwerk teilnehmenden Parteien und ist aber gleichermaßen einer der kompliziertesten Vorgänge. Identitätsmanagement in der Vergangenheit bis ins heutige Zeitalter als Weg der Identifizierung von Personen in einem System zum Beispiel bei der Einreise in ein anderes Land via Personalausweis oder Reisepass, der Bereitstellung der Krankengeschichte mittels Krankenkassenkarte oder der Anspruch auf Sozialleistungen mittels Sozialversicherungsausweis ist in allen Fällen verbunden mit einem enormen bürokratischen Aufwand, langen Wartezeiten und der nicht mehr zeitgemäßen Speicherung sämtlicher Daten auf Papier. Außerdem bedeuten die eben beschriebenen Beispiele auch, dass die eigene Identität bei verschiedenen Institutionen mehrfach nachgewiesen werden muss. Weitere Schwachpunkte der aktuellen Systeme sind, wie in vielen zuvor beschriebenen Fällen auch, das Vorhandensein von verschiedenen zentralen Instanzen bzw. Datenbanken, die oftmals nicht in der Lage sind, auf effiziente Weise miteinander zu kommunizieren und Informationen auszutauschen. Risiken des Betrugs und Verlust von Daten gibt es aufgrund der Abwicklung von Prozessen auf Papierbasis. [84]

Wie kann Blockchain nun dabei helfen, die eben angesprochenen Probleme im Bereich Identitätsmanagement zu lösen? Es beginnt damit, dass alle personenbezogenen Daten auf der Blockchain gespeichert werden. Die abgespeicherten Datensätze sind untrennbar mit der Identität einer Person verbunden, sind jederzeit verfügbar und können nicht verloren gehen. Jede Person entscheidet, welche Organisationen Zugriffsrecht auf die eigenen Daten haben und aufgrund der kryptografischen Verschlüsselung sind die Daten außerdem vor Manipulation und Diebstahl gesichert. Eine einmalige Authentifizierung reicht aus, um der mehrmaligen Abfrage und Bestätigung von Daten vorzubeugen.

Estland ist weltweit eines der führenden Länder und gewissermaßen ein Pionier, wenn es zum Einsatz von Blockchain nicht nur im öffentlichen Sektor und der Anpassung von Regierung und Gesellschaft an den digitalen Wandel im 21. Jahrhundert kommt. Bereits seit 2002 gibt es in Estland den Digital ID, eine Art natio-

[83] Vgl. Deloitte: Blockchain in Public Sector - Transforming government services through exponential technologies, S.8.

[84] Vgl. Joshi, Prasad: Identitäts-Management mit der Blockchain.

naler Ausweiskarte mit eingebautem Chip, die kryptografisch verschlüsselt, Zugriff auf verschiedenste Daten erlaubt und als eindeutiger Verifizierungsnachweis in einer elektronischen Umgebung dient. Gut 98% aller Esten besitzen eine solche Karte und nutzen diese mehr als nur einen einfachen Personalausweis für Reisen innerhalb der EU. Die Karte funktioniert gleichermaßen als Krankenversicherungskarte, ermöglicht verifizierten Zugang zu Bankkonten, kann für digitale Signaturen verwendet werden, ermöglicht das Wählen via Internet und bietet zudem Zugriff auf die Krankenakte und kann für die Steuererklärung benutzt werden. Alle Funktionen vereint auf einer einzigen Karte.

Mit dem Auftreten der Blockchain-Technologie 2008 begann auch Estland diese zu testen und seit 2012 wird Blockchain in estnischen Registern operativ genutzt. Somit werden nicht nur die Daten der Digital ID Karten auf der Blockchain gespeichert, sondern beispielsweise auch sämtliche Patientenakten der verschiedenen Dienstleister im Gesundheitswesen. Eine gemeinsame Datenbank die es Patienten erlaubt, die komplette Krankenakte online einzusehen. Auch sämtliche Daten und Aufzeichnungen der Bereiche Judikative, Exekutive und Legislative sind in Registern elektronisch auf der Blockchain gespeichert. Mithilfe des e-Law Systems ist es für die Öffentlichkeit möglich, jeden Gesetzesentwurf seit Februar 2003 online einzusehen. Sichtbar sind Informationen zum aktuellen Status, möglichen Abänderungen im Laufe des parlamentarischen Prozesses und Angaben dazu, wer den Entwurf eingebracht hat. Im Bereich der Exekutive setzt Estland auf effektive Kommunikation und Koordination unter den einzelnen Polizeieinheiten. [85]So ist in jedem Polizeiauto eine mobile Arbeitsstation und ein Positioniersystem installiert, welche den Standort und Status jeder Polizeieinheit angeben.

Estland hat eigens dafür die sogenannte KSI Blockchain entwickelt, die noch bessere Datensicherheit und Schutz vor Cyber - Attacken bieten soll. KSI steht dabei für Keyless Signature Infrastructure, ein weltweit verteiltes System, dass Zeitstempel und digitale Signaturen als Leistungen anbietet. Keyless bedeutet im Vergleich zu Signaturen mit Public Keys nicht, dass keine kryptografischen Schlüssel verwendet werden, sondern vielmehr, dass die Signaturen zuverlässig verifiziert werden können auch ohne, dass man von einer fortwährenden Geheimhaltung des Schlüssels ausgeht. Mithilfe von KSI ist es den verantwortlichen Beamten möglich zu überwachen, welche Änderungen an den Aufzeichnungen zu welcher Zeit und von welcher Person vorgenommen worden. Jegliche Manipulationen an der Blockchain, ob nun von Hackern oder selbst von internen Systemadministratoren oder der Regierung würden sofort entdeckt.[86]

Estlands ehrgeizige Zukunftsvision eines e-Estonia wird weiterhin ein Prozess des Experimentierens und Lernen aus Fehlern sein. Betrachten wir das Identitätsmanagement als Teil der möglichen Blockchain-Anwendungen, dann besteht

[85] Vgl. e-Estonia: Building blocks of e-Estonia.

[86] Vgl. Buldas, Ahto ; Kroonmaa, Andres; Laanoja, Risto: Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees, S.1.

das Potenzial, aktuelle Problemstellungen zu lösen. Die Integration aller Marktteilnehmer auf einer Plattform ermöglicht schnellere und effizientere Prozesse mit dem Fokus auf die Bedürfnisse des Einzelnen, der zu jederzeit die vollständige Kontrolle über seine eigenen Daten hat.

5.2.2 Verarbeitung von Steuerzahlungen

Laut einer Befragung von 816 IT-Experten im Rahmen des Weltwirtschaftsforums 2015 gaben 73% an, dass die Einziehung von Steuern durch eine Regierung mithilfe eines Blockchain-Systems innerhalb der nächsten 10 Jahre im Rahmen des Möglichen liegt. [87]

Blockchain wird die Fähigkeit zugesagt, den Bereich Buchführung und die Abwicklung von Steuerzahlungen grundlegend zu verändern. Die dazu nötigen Veränderungen für Steuerbehörden bedeuten eine Revolution für die Art und Weise wie Regierungen zur jetzigen Zeit Datenbanken und Netzwerksysteme steuern. Außerdem wird es nötig sein, das Rechtssystem in Bezug auf gesetzliche Bestimmungen für Datenbanken, geistiges Eigentum und gesetzmäßige Identitäten zu reformieren. Die Zukunft verspricht automatisierte Steuerprozesse in Echtzeit für sowohl einzelne Individuen als auch kleine und große Unternehmen. Aufgrund der Komplexität des Steuersystems möchte ich mich in dieser Arbeit auf die Umsatzsteuer und die Einkommenssteuer beschränken. Der Bereich Zoll, Kapitalertragssteuer, Berechnung von Verrechnungspreisen und Betriebsprüfung sind weitere mögliche Anwendungsfälle.

Einkommenssteuer: Auch, wenn in einem Großteil der Industrieländer Angelegenheiten in Verbindung mit Einkommensteuer bereits digitalisiert sind, gibt es aufgrund der Vielzahl an beteiligten staatlichen Institutionen immer noch eine große Schwachstelle: mehrere Register der verschiedenen Institutionen, die im Grunde alle die gleichen Informationen wiedergeben. Zudem gibt es mit dem Arbeitgeber noch einen Mittelmann, der für die Berechnung und den Transfer der Steuern und Sozialabgaben zu den staatlichen Institutionen verantwortlich ist. Nur bedingte Transparenz und hohe administrative Kosten sind die Folgen. Blockchain-Lösungen bieten eine Alternative zur traditionellen Art der Abwicklung.

Der Einsatz von Smart Contracts zum Beispiel, könnte den Prozess der Einkommenssteuerberechnung und -abwicklung automatisieren. Nachdem der Arbeitgeber den Bruttobetrag des Angestellten in das System eingegeben hat, wird über Smart Contracts der exakte Betrag an zu zahlender Einkommenssteuer und Sozialabgeben berechnet. Das Nettogehalt wird automatisch auf das Konto des Arbeitnehmers überwiesen und der Staat erhält die zuvor berechneten Steuerabgaben. Zugang zur Blockchain haben natürlich nur die Steuerbehörden, Banken,

[87] Vgl. Fraunhofer - Institut (2016): BLOCKCHAIN: GRUNDLAGEN, ANWENDUNGEN UND POTENZIALE, S.30.

Arbeitgeber und sonstige, am Prozess beteiligte Institutionen. Als Ergebnis gestaltet sich die Abwicklung der Einkommenssteuer um ein vielfaches schneller und kostengünstiger. Das System ist vollkommen transparent gestaltet und kann von den Arbeitnehmern jederzeit eingesehen werden. [88]

Umsatzsteuer: Die Umsatzsteuer ist die Haupteinnahmequelle der Regierungen weltweit und aus diesem Grund sind die Steuerbehörden auf der Suche nach effektiveren und schnelleren Möglichkeiten zur Erhebung dieser Steuer. Auch wenn es sowohl innerhalb der EU mit einer geplanten Reform des EU-Umsatzsteuersystems in den nächsten Jahren, als auch international wie zum Beispiel in Brasilien mit einem elektronischen Abrechnungssystem in Echtzeit, bereits große Fortschritte gibt, ist das aktuelle System doch immer noch mit zahlreichen Problemen behaftet. So besteht eine große Abhängigkeit den Unternehmen gegenüber, welche den Umfang der Umsatzsteuer selbst korrekt zu berechnen und den Steuerbehörden einzureichen haben. Außerdem macht es das System den Regierungen schwer, Umsatzsteuerzahlungen nachzuverfolgen, was zum Steuerbetrug ausgenutzt wird. Verschiedene Ledger bzw. Datenbanken in den einzelnen Ländern weltweit erschweren es, einheitliche Daten über die Bewegungen von Umsatzsteuer zu erhalten.

Betrachtet man Abbildung 13, dann zeigt der obere Teil wie umständlich die Abwicklung von Transaktionen mit Umsatzsteuer aktuell ist. [89] In Schritt 1 wird vom Unternehmen eine Umsatzsteuerrechnung ausgestellt, die der Kunde in Schritt 2 zusammen mit dem Nettobetrag bezahlt. In Schritt 3 werden Informationen zur Zahlung im System des Unternehmens gespeichert. Das Unternehmen bezahlt in Schritt 4 die Lieferantenrechnung und muss im letzten Schritt je nach zeitlicher Vorgabe die fällige Höhe an Umsatzsteuer berechnen und eine Steuererklärung abgeben.

Mithilfe von Blockchain könnte man diesen Prozess auf zwei Schritte zusammenfassen. Schritt 1 wäre die Zahlung der Rechnung an das Unternehmen. Smart Contracts auf der Blockchain berechnen in der gleichen Zeit automatisch die Umsatzsteuer und den Nettobetrag. Die Umsatzsteuer wird via Smart Contract nun direkt an Steuerbehörde bezahlt und der Nettobetrag landet beim Unternehmen. Der Schritt 2, bei dem das Unternehmen eine Lieferantenrechnung begleicht läuft ähnlich ab: der benötigte Betrag wird vom Unternehmen eingegeben und Smart Contracts senden den fälligen Betrag an den Lieferanten und gleichzeitig wird die fällige Umsatzsteuer an die Steuerbehörden überwiesen. Die Vorteile, die diese Art der Steuerabrechnung bietet ist immens. Der Verwaltungsaufwand für Unternehmen und staatliche Einrichtungen ist beachtlich reduziert und führt zu Kosteinsparungen im Bereich der Buchhaltung. Der gesamte Prozess läuft in Echtzeit ab und ist aufgrund der Verwendung von Smart Contracts manipulationssicher und transparent. Die Verwendung von Blockchain ermöglicht den zuständigen Finanzbehörden einen direkten Einblick in die Finanzen der Unternehmen und die Durchführung von rechtlichen Prüfungen und Untersuchungen aller

[88] Vgl. Deloitte (2017b): Blockchain technology and its potential in taxes, S.11.

[89] Vgl. ebd., S.12-13.

steuerrelevanten Transaktionen. Das Risiko von Steuerbetrug und Fehlern bei der Berechnung von Umsatzsteuer kann um ein Vielfaches reduziert werden.

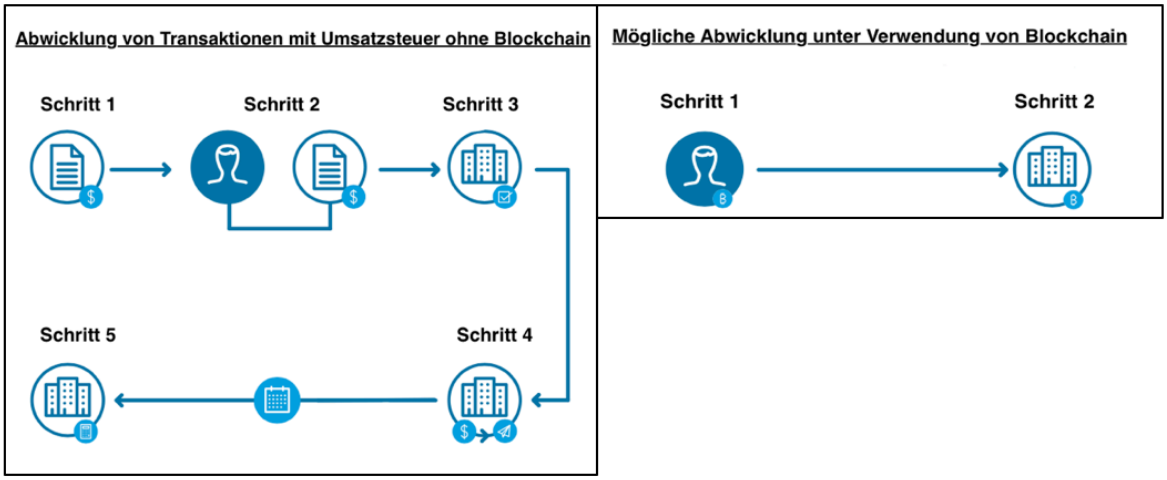

Abbildung 13: Abwicklung von Umsatzsteuer mit und ohne Blockchain[90]

[90] Siehe Deloitte (2017b): Blockchain technology and its potential in taxes, S.13.

6 Fazit und Ausblick

Der Einsatz von Distributed Ledger Technologie im Finanzsektor kann unter Abwägung der vorhandenen Risiken zu enormen Vorteilen für die beteiligten Institutionen führen. Teilbereiche der Finanzbranche können durch die Verwendung von Blockchain in vielerlei Hinsicht profitieren, ob die gesamte Finanzwelt grundlegend revolutioniert wird, ist aus heutiger Sicht noch nicht vorhersehbar. Die breite Akzeptanz und die Erforschung des wahren Potenzials von Blockchain spielen dabei eine große Rolle.

Der Zahlungsverkehr kann von Blockchain in dem Maße profitieren, dass die dezentrale, offene Struktur des Systems für mehr Transparenz und geringere Übertragungszeiten und Transaktionskosten führt. Zahlungen mit Werten von weniger als 5€ spielen in der digitalen Welt bereits eine große Rolle und können mithilfe von Blockchain zu einem Bruchteil der jetzigen Gebühren abgewickelt werden. Fraglich ist dennoch, wie die technische Umsetzung aussieht bzw. aussehen kann und wie die nicht mögliche Verknüpfung der digitalen zu realen Identitäten die nötige Vertraulichkeit zwischen den Parteien schaffen kann.

Im streng regulierten Bereich des Wertpapierhandels bedarf es einer Menge an regulatorischen und rechtlichen Anpassungen, bevor ein Einsatz von Blockchain in großem Umfang überhaupt in Frage kommt. Governance als zentraler Bestandteil des bestehenden Systems müsste überdacht und umstrukturiert werden. Außerdem ist es heute nicht klar, ob die Sicherheit eines Blockchain-Netzwerks und die Integrität derer Mitglieder und ihrer Daten auch in Zukunft mit dem Aufkommen neuer Technologien zu 100% gesichert ist. Dem gegenüber steht die Möglichkeit der effektiveren Gestaltung von Prozessen, vor allem in den Bereichen Clearing und Settlement. Das Counterparty Risk kann durch die Verwendung von Smart Contracts reduziert werden und ICOs bieten einen neuartigen Weg der Kapitalaufnahme.

Nicht nur die Finanzbranche kann von Blockchain profitieren, die Anwendungsmöglichkeiten gehen weit darüber hinaus. Im Bereich der Wirtschaft kann das Supply Chain Management transparenter und effektiver gestaltet werden. Die Möglichkeit, sämtliche ungenutzte Gegenstände mit anderen zu teilen und bei der Abwicklung dieser Geschäfte auf DLT zurückzugreifen ist ein Konzept, dass in Zeiten von AirBnb und Uber noch kostengünstiger und unabhängiger von jeglichen Intermediären gemacht werden kann. Der öffentliche Sektor wird ebenfalls von dieser neuartigen Technologie profitieren können. Der klassische Ausweis könnte durch einen digitalen Pass ersetzt werden, der nicht nur fälschungssicher ist, sondern auch andere personenbezogene Informationen enthalten könnte. Der Bereich Steuerabwicklung könnte von einem Prozess mit vielen Schritten und administrativ anspruchsvoller Verwaltung zu einem System mit wenigen Aktionen vereinfacht werden.

Derzeit ist es noch sehr schwer, einen aussagekräftigen Ausblick in Bezug auf die Zukunft von DLT in der Finanzbranche zu geben. Selbst wenn das Interesse der beteiligten Institutionen mit Aussicht auf die zu erwartenden Vorteile groß ist und bereits mehrere Pilotprojekte gestartet wurden, ist diese Technologie noch viel zu wenig erforscht um überhaupt ansatzweise von einer Revolution sprechen zu können. Geht man davon aus, dass sich der Entwicklungsstand von Blockchain ähnlich der des Internets Anfang der 90ger Jahre noch im Anfangsstadium befindet und vergleichbar gut entwickelt, stehen nicht nur der Finanzwelt goldene Zeiten bevor. Die Zukunft von Blockchain wird auch davon abhängen, ob es möglich sein wird, eine entsprechende IT-Infrastruktur mit adäquaten Kapazitäten zu schaffen, rechtliche und regulatorische Rahmenbedingungen zu etablieren und den Anforderungen entsprechende Sicherheitsstandards festzulegen.

Eines steht auf jeden Fall fest: Satoshi Nakamoto hat mit seinem Bitcoin-Whitepaper 2008 einen Stein ins Rollen gebracht, mit dessen Idee sich nur 10 Jahre nach Veröffentlichung Großunternehmen und Staaten auf der ganzen Welt beschäftigen. Die Erwartungen und Hoffnungen in das Potenzial dieser Technologie sind dabei genauso groß, wie die möglichen Risiken.

Literatur- und Quellenverzeichnis

Badev, Anton; **Chen**, Matthew (2014): Bitcoin: Technical Background and Data Analysis.
URL: https://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf, verfügbar am 15.06.2018.

BaFin (2017): Verbraucherwarnung: Risiken von Initial Coin Offerings (ICOs).
URL: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171109_ICOs.html, verfügbar am 16.07.2018, verfügbar am 18.07.2018.

BaFin (2018): Initial Coin Offerings: BaFin veröffentlicht Hinweisschreiben zur Einordnung als Finanzinstrumente. URL: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2018/fa_bj_1803_ICOs.html, verfügbar am 10.07.2018.

Boberach, Frank: Transatlantischer Zahlungsverkehr auf der Basis von Blockchain – Erfahrungen der Reise-Bank. In: Zeitschrift für das gesamte Kreditwesen: 2017, Nr. 11, S. 34 - 35. - ISSN 0341-4019.

BTC - ECHO (o.J.(a)): Was ist ein ICO? URL: https://www.btc-echo.de/tutorial/was-ist-ein-ico-und-wie-funktionieren-tokensales/, verfügbar am 12.06.2018.

BTC - ECHO (o.J. (b)): Wie funktioniert Bitcoin-Mining? URL: https://www.btc-echo.de/tutorial/wie-kann-ich-bitcoins-minen/, verfügbar am 20.06.2018.

Buldas, Ahto ; **Kroonmaa**, Andres; **Laanoja**, Risto: Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees. - 1. Auflage Berlin/Heidelberg: Springer - Verlag, 2013.

CoinMarketCap (2018): All Cryptocurrencies
URL: https://coinmarketcap.com/all/views/all/, verfügbar am 12.06.2018.

Deloitte (2017a): When two chains combine - supply chain meets blockchain.
URL: https://www2.deloitte.com/content/dam/Deloitte/pt/Documents/blockchain-supplychain/IE_C_TL_Supplychain_meets_blockchain_.pdf, verfügbar am 20.07.2018.

Deloitte (2017b): Blockchain technology and its potential in taxes. URL: https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Blockchain-technology-and-its-potential-in-taxes-2017-EN.PDF, verfügbar am 14.08.2018.

Deloitte (2018): Blockchain in Public Sector - Transforming government services through exponential technologies. URL: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/public-sector/in-ps-blockchain-noexp.pdf, verfügbar am 26.07.2018.

Deutsche Bundesbank (o.J.): Zahlungsverkehr: https://www.bundesbank.de/Redaktion/DE/Glossareintraege/Z/zahlungsverkehr.html, verfügbar am 20.06.2018.

Deutsche Bundesbank (2012): Innovationen im Zahlungsverkehr im Monatsbericht 09/12.
URL: https://www.bundesbank.de/Redaktion/DE/Downloads/Veroeffentlichungen/Monatsberichtsaufsaetze/2012/2012_09_innovationen_zahlungsverkehr.pdf?__blob=publicationFile, verfügbar am 21.06.2018.

Deutsche Bundesbank (2016): Die Deutsche Bundesbank – Notenbank für Deutschland. URL: https://www.bundesbank.de/Redaktion/DE/Downloads/Veroeffentlichungen/Bundesbank/die_deutsche_bundesbank.pdf?__blob=publicationFile, verfügbar 20.06.2018.

Deutsche Bundesbank (2017): Distributed-Ledger-Technologien im Zahlungsverkehr und in der Wertpapierabwicklung: Potenziale und Risiken im Monatsbericht 09/17.
URL: https://www.bundesbank.de/Redaktion/DE/Downloads/Veroeffentlichungen/Monatsberichtsaufsaetze/2017/2017_09_distributed_ledger_technologien.pdf?__blob=publicationFile, verfügbar am 10.06.2018.

Digiconomist (2018): Bitcoin Energy Consumption Index. URL: https://digiconomist.net/bitcoin-energy-consumption, verfügbar am 02.07.2018.

ECB (2016): Distributed Ledger Technology. URL: https://www.ecb.europa.eu/paym/pdf/infocus/20160422_infocus_dlt.pdf, verfügbar am 09.07.2018.

e-Estonia (o.J.): Building blocks of e-Estonia. URL: https://e-estonia.com/solutions/, verfügbar am 02.08.2018.

ESMA (2017): The Distributed Ledger Technology Applied to Securities Markets. URL: https://www.esma.europa.eu/system/files_force/library/dlt_report_-_esma50-1121423017-285.pdf, verfügbar am 08.07.2018.

Federal Reserve Bank of New York (2002): Securities Trading and Settlement in Europe: Issues and Outlook. URL: https://www.newyorkfed.org/medialibrary/media/research/current_issues/ci8-4.pdf, verfügbar am 05.07.2018.

FINRA (2017): Distributed Ledger Technology: Implications of Blockchains for the Securities Industry. URL: https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf, verfügbar am 15.07.2018.

Fraunhofer - Institut (2016): BLOCKCHAIN: GRUNDLAGEN, ANWENDUNGEN UND POTENZIALE - Whitepaper. URL: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf, verfügbar am 20.07.2018.

Fraunhofer - Institut (2017a): BLOCKCHAIN UND SMART CONTRACTS - Technologien, Forschungsfragen und Anwendungen. URL: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts.pdf?_=1516641660, S.19, verfügbar am 12.06.2018.

Fraunhofer - Institut (2017b): BLOCKCHAIN - Technologien, Forschungsfragen und Anwendungen. URL: https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/deutsch/FhG-Positionspapier-Blockchain.pdf, verfügbar am 05.07.2018.

Gabele, Eduard; **Mayer**, Horst: Einführung in die Buchhaltung und Jahresabschlusserstellung. - 8. Auflage Berlin: De Gruyter Verlag, 2015.

GwG (idF v. 13.08.2008) § 11 Abs.I.

Hahn, Christopher; **Wohns**, Adrian: Initial Coin Offering (ICO). - 1.Auflage Wiesbaden: Springer - Verlag, 2018.

Heldt, Dr. Cordula (2018): Wertpapier. In: Springer Gabler Verlag (Hg.), Gabler Wirtschaftslexikon.
URL: https://wirtschaftslexikon.gabler.de/definition/wertpapier-48640, verügbar am 05.07.2018.

Irish Funds (2016): Regulatory Reporting Blockchain. URL: https://files.irish-funds.ie/1488968245-Regulatory-Reporting-Blockchain-POC-Factsheet..pd, verfügbar am 09.07.2018.

Ittner, Prof. Dr. - Ing. Andreas (2018): Grundlagen Blockchain als Vorlesung im Rahmen der Blockchain Springschool 2018.

Joshi, Prasad (2018): Identitäts-Management mit der Blockchain auf www.egovernment-computing.de. URL: https://www.egovernment-computing.de/identitaets-management-mit-der-blockchain-a-705805/, verfügbar am 01.08.2018.

Kharif, Olga (2018): Half of ICOs Die Within Four Months After Token Sales Finalized auf www.bloomberg.com. URL: https://www.bloomberg.com/news/articles/2018-07-09/half-of-icos-die-within-four-months-after-token-sales-finalized, verfügbar am 20.07.2018.

Klaptor, Dr. Martin (2017): Chancen und Herausforderungen der Blockchain. URL: https://digitaleweltmagazin.de/2017/11/28/chancen-und-herausforderungen-der-blockchain/, verfügbar am 03.07.2018.

Kollmann, Prof. Dr. Tobias (2018): Micropayment. In: Springer Gabler Verlag (Hg.), Gabler Wirtschaftslexikon.
URL: https://wirtschaftslexikon.gabler.de/definition/micropayment-37916/version-261345, verügbar am 01.07.2018.

Krempl, Stefan (2018): ICO: Bafin hat 2017 vier Crowdfundings mit Kryptogeld untersagt auf www.heise.de. URL: https://www.heise.de/newsticker/meldung/ICO-Bafin-hat-2017-vier-Crowdfundings-mit-Kryptogeld-untersagt-3986942.html, verfügbar am 18.07.2018.

Metzger, Jochen (2018): Distributed Ledger Technologie (DLT). In: Springer Gabler Verlag (Hg.), Gabler Wirtschaftslexikon.
URL: https://wirtschaftslexikon.gabler.de/definition/distributed-ledger-technologie-dlt-54410/version-277444, verfügbar am 05.06.2018.

Metzner, Thomas: Techniktrend Blockchain - ausgewählte Handlungsfelder von Banken. In: Zeitschrift für das gesamte Kreditwesen: 2018, Nr. 6, S. 37 - 40. - ISSN 0341-4019.

Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf, verfügbar am 13.06.2018.

Narayanan, Arvind; **Bonneau**, Joseph; **Felten**, Edward; **Miller**, Andrew; **Goldfeder**, Steven. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. – 1. Auflage Princeton: Princeton University Press, 2016.

Negin (2018): IOTA | Kryptowährung für das IOT. URL: https://blockchain-welt.de/iota-tangle-kryptowaehrung-fuer-iot/, verfügbar am 10.06.2018.

Nielsen (2014): Is Sharing the new Buying? URL: http://www.nielsen.com/us/en/insights/reports/2014/is-sharing-the-new-buying.html, verfügbar am 20.07.2018.

Ripple (o.J. (a)): XRP – The digital asset for payments. URL: https://ripple.com/xrp/, verfügbar am 23.06.2018.

Ripple (o.J. (b)): Solution Overview. URL: https://ripple.com/files/ripple_solutions_guide.pdf, verfügbar am 23.06.2018.

Ripple (o.J. (c)): Source Liquidity - xRapid. URL: https://ripple.com/solutions/source-liquidity/, verfügbar am 23.06.2018.

Schmidt, Tobias (2018a): Was ist eigentlich aus SatoshiPay geworden? In: BTC-ECHO. URL: https://www.btc-echo.de/was-ist-eigentlich-aus-satoshipay-geworden/, verfügbar am 01.07.2018.

Schmidt, Tobias (2018b): Was ist eigentlich aus Slock.it geworden? Auf www.btc-echo.de.URL: https://www.btc-echo.de/was-ist-eigentlich-aus-slock-it-geworden/, verfügbar am 23.07.2018.

SEC Securities Exchange Act Release No. 70073 (Idf. v. 30.07.2013) Regel 15c3-3.

SopraSteria (2017): Blockchain 2017 - Spannende Technologien für morgen. URL: https://www.soprasteria.de/docs/librariesprovider33/infografiken/infografik-managementkompass-blockchain.pdf?sfvrsn=2, verfügbar am 01.07.2018.

Statista (2018a): Anzahl der Transaktionen im bargeldlosen Zahlungsverkehr weltweit in den Jahren von 2010 bis 2020 (in Milliarden). URL: https://de.statista.com/statistik/daten/studie/71256/umfrage/anzahl-bargeldloser-transaktionen-weltweit/, verfügbar am 23.06.2018.

Statista (2018b): Emissionsvolumen der Börsengänge in den USA von 1999 bis zum 1. Halbjahr 2018 (in Milliarden US-Dollar). URL: https://de.statista.com/statistik/daten/studie/36981/umfrage/volumen-der-boersengaenge-in-den-usa/, verfügbar am 13.07.2018.

Strategy&/pwc (2018): Initial Coin Offerings - Eine strategische Perspektive. URL: https://www.pwc.ch/de/publications/2018/20180628_PwC%20S&%20CVA%20ICO%20Report_DE.pdf, verfügbar am 12.07.2018.

Tapscott, Don; **Tapscott**, Alex: Die Blockchain Revolution. - 3. Auflage Kulmbach: Börsenbuchverlag, 2017.

Taylor, Kate (2017): 40 of the biggest scandals in Uber's history auf www.businessinsider.de- URL: https://www.businessinsider.de/uber-company-scandals-and-controversies-2017-11?op=1, verfügbar am 23.07.2018.

TransferWise (2017): Auslandsüberweisung Sparkasse: Kosten, Gebühren & Dauer
URL: https://transferwise.com/de/blog/auslandsueberweisung-sparkasse, verfügbar am 21.06.2018.

Tual, Stephan (2017): Slock.it secures $2 million USD seed funding to build next-generation Sharing Economy Platform. URL: https://blog.slock.it/slock-it-secures-2-million-usd-seed-funding-to-build-next-generation-sharing-economy-platform-b795c6d1a92d, verfügbar am 23.07.2018.

Zahrte, René: Funktionsweise und Auswirkungen der Blockchain - Technologie auf den Wertpapierhandel. - 2016. - 54 S. Köl, Technische Universität, Informations- und Kommunikationswissenschaften, Bachelorarbeit, 2017.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Mittweida, den 29.08.2018

Manuel Müller