Funktionsweise und Auswirkungen der Blockchain-Technologie auf den Wertpapierhandel

Bachelorarbeit

im Studiengang
Informationswirtschaft

vorgelegt von

René Zahrte

am 7. Oktober 2016
an der Technischen Hochschule Köln

Erstprüfer/in: Prof. Dr. Prokop
Zweitprüfer/in: Prof. Seidler-de Alwis, MBA.

Kurzfassung

Die vorliegende Bachelorarbeit gibt einen Überblick über die Funktionsweise und Auswirkungen der Blockchain-Technologie auf den Wertpapierhandel. Dabei werden zunächst die essentiellen, technischen Grundlagen der Kryptografie und Dezentralisierung am Beispiel der führenden Kryptowährung Bitcoin untersucht. Danach werden die gewonnenen Erkenntnisse mit einer SWOT-Analyse auf den Wertpapierhandelsprozess angewandt und es wird die Implementierung eines Distributed Ledgers auf Chancen und Risiken für die Finanzmärkte hin evaluiert. Als Essenz der Literaturauswertung ist festzustellen, dass die Stärken der DLT nur nach Einigung auf einen technischen Marktstandard voll abgeschöpft werden können. Die Basis der Bachelorarbeit sind aktuelle Studien und Arbeitspapiere von Regulierungsbehörden, Beratungsunternehmen und Finanzdienstleistern aus Europa und den USA zur Auswirkung der Distributed Ledger Technology auf den Wertpapierhandel sowie die Fachbücher und Arbeitspapiere von Narayanan (2016) und Nakamoto (2008) zur Funktionsweise der Blockchain-Technologie. Durch die Verknüpfung von Informationstechnologie und Finanzwirtschaft erhofft sich der Autor einen interdisziplinären Erkenntnisgewinn über aktuelle Entwicklungen auf den Finanzmärkten.

Schlagwörter: Bachelorarbeit, Blockchain, Bitcoin, Wertpapierhandel, DLT, Distributed Ledger Technology

Abstract

This bachelor thesis gives an overview of the mechanics and impact of the blockchain technology on securities trading. At first there is an introduction to the essential technical basics of cryptography and decentralization using the example of Bitcoin as the leading cryptocurrency. Afterwards these findings are applied on the securities trading process with a SWOT analysis to evaluate the chances and risks of an implementation of a distributed ledger in the financial markets. As a result of the literature evaluation it can be stated that the strengths of the DLT can only be fully utilized by an agreement on a technical market standard. The basis for this thesis are current studies and working papers by regulators, consultants and financial institutions from Europe and the United States on the impact of Distributed Ledger Technology on securities trading as well as the books and papers of Narayanan (2016) and Nakamoto (2008) on the mechanics of the blockchain technology. By combining information technology and finance, the author hopes to get an interdisciplinary insight into current developments in the financial markets.

Keywords: bachelor thesis, blockchain, Bitcoin, securities trading, DLT, distributed ledger technology

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

BTC	Bitcoin
CSD	Central Securities Depository
CCP	Central Counterparty
DLT	Distributed Ledger Technology
ECB	European Central Bank
ESMA	European Securities and Markets Authority
ISIN	International Securities Identification Number
NASDAQ	National Association of Securities Dealers Automated Quotations
P2P	Peer-to-Peer
SHA	Secure Hash Algorithm
SWIFT	Society for Worldwide Interbank Financial Telecommunication

1 Überblick

1.1 Begriffsabgrenzung

In der öffentlichen Diskussion um die Blockchain-Technologie, werden die Begriffe Blockchain und Distributed Ledger Technology *DLT* vielfach synonym verwendet. Strenggenommen ist die DLT der Überbegriff für die gesamte Technologie im Allgemeinen und die Blockchain ein spezieller Distributed Ledger für Kryptowährungen. Durch die außerordentlich große Bedeutung von Bitcoin als Technologieträger der DLT, wird allerdings auch außerhalb der Diskussion um virtuelle Währungen von der Blockchain-Technologie gesprochen.

1.2 Blockchain

Die Blockchain ist eine verteilte Datenbank, die es sich nicht vertrauenden Handelspartnern erlaubt, ohne einen Intermediär, sicher untereinander Transaktionen über ein Peer-to-Peer-Netzwerk abwickeln zu können.[1] Die Teilnehmer des Netzwerks werden als Nodes bezeichnet und sind für die Verifikation und das Speichern der Transaktionen zuständig. Ein weiteres wichtiges Merkmal ist der umfassende Einsatz von Kryptografie wie Public und Private Keys sowie Hash-Funktionen.[2] In der Blockchain wird gespeichert, wer welche Positionen oder Güter besitzt. Dabei werden die Besitzer nicht über ihren Namen identifiziert, sondern über ein eindeutiges und nicht fälschbares Schlüsselpaar.

1.3 Distributed Ledger Technology

Aus dem Englischen übersetzt bedeutet Distributed Ledger etwa soviel wie dezentralisiertes Konto. Die Besonderheit gegenüber einem klassischen Konto liegt darin, dass es

[1] Vgl. UCL, "Ucl Research Centre for Blockchain Technologies", University College London, http://blockchain.cs.ucl.ac.uk/.

[2] Vgl. ESMA, *The Distributed Ledger Technology Applied to Securities Markets* (Paris: European Securities and Markets Authority, 2016), S. 8. https://www.esma.europa.eu/file/18727/download?token=j_lKec2m.

nicht von einer zentralen Einheit verwaltet wird, sondern von einem verteilten Netzwerk, das Transaktionen verifiziert und einen Intermediär überflüssig macht.

Ihre bisher größte Verbreitung hat die DLT als öffentlicher Ledger für Transaktionen der virtuellen Währung Bitcoin erfahren. Die Idee, Distributed Ledger auch auf den Wertpapierhandel anzuwenden, ist hingegen noch relativ jung. Um die Chancen und Risiken einer Implementierung der Technologie im Wertpapierhandel näher zu untersuchen und ihr zum Durchbruch zu verhelfen, haben viele Marktteilnehmer und Behörden Arbeitsgruppen eingerichtet.[3]

Die Anwendung der DLT im Wertpapierhandel unterscheidet sich in einigen Eigenschaften von der Anwendung als Distributed Ledger für Bitcoin. Die Bitcoin Blockchain ist ein erlaubnisfreies System, an dem sich jeder beteiligen und Transaktionen verifizieren kann. Ein System für den Wertpapierhandel wird erlaubnispflichtig sein und autorisierten Teilnehmern wie Banken und Behörden vorbehalten bleiben.[4]

1.4 Bitcoin

Bitcoin *BTC* ist die weltweit erste und heute mit Abstand am weitesten verbreitete Kryptowährung und wurde Anfang 2009 von einem Entwickler oder Entwicklerteam unter dem Pseudonym *Satoshi Nakamoto* eingeführt. Im Gegensatz zu konventionellen Währungen wie Euro oder US-Dollar, wird Bitcoin nicht von einer Zentralbank verwaltet, sondern von einem dezentralisierten Netzwerk, an dem sich jeder beteiligen kann, der die frei verfügbare Bitcoin Software installiert hat.

Es können maximal 21 Millionen BTC erzeugt werden, was der Währung einen deflationären Charakter verleiht. Bitcoins selbst werden durch Mining erschaffen, wobei ausstehende Transaktionen in Blöcken zusammengefasst und von rechenintensiven Algorithmen auf ihre Richtigkeit überprüft werden. Für das Bereitstellen der Rechenleistung erhält der Miner, der als erstes einen neuen Block erfolgreich verifiziert hat, einen Block Reward in Höhe von derzeit 12,5 BTC. Der Block Reward von anfänglich 50 BTC wird alle 4 Jahre halbiert, bis im Jahr 2140 alle Bitcoins erstellt worden sein werden. Die Algorithmen sind so ausgelegt, dass das Netzwerk pro Block etwa 10 min Rechenzeit benötigt. Ein erfolgreich berechneter Block wird dann an die bestehende Kette

[3] Vgl. ebd.
[4] Vgl. ebd.

von Blöcken anhängt, wodurch die Technologie zu ihrem Namen *Blockchain* gekommen ist.[5]

Auch wenn es sich bei Bitcoin um eine Kryptowährung handelt, darf Kryptografie nicht mit Verschlüsselung verwechselt werden. In Bitcoin werden keine Daten verschlüsselt. Verschlüsselung ist lediglich eine mögliche Anwendung von Kryptografie. Die Blockchain-Technologie greift intensiv auf kryptografische Verfahren zurück, die in den folgenden Kapiteln genauer vorgestellt werden.[6]

Anders als bei herkömmlichen Währungen, gibt es bei Bitcoin keine fest notierten Einheiten wie Scheine und Münzen. Bitcoins sind rein virtuell und können bis auf die achte Nachkommastelle genau angegeben werden Der kleinstmögliche Wert sind 0,00000001 BTC, was auch 1 Satoshi genannt wird.[7]

[5] Vgl. Daniel Kerscher, *Handbuch Der Digitalen Währungen* (Dingolfing: Kemacon, 2014), S. 94.

[6] Vgl. Arvind Narayanan; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton: Princeton University Press, 2016), S. 19.

[7] Vgl. ebd., S. 46.

2 Ziele und Vorgehen

Die Blockchain-Technologie verspricht nicht weniger, als dass Banken ihre komplette Infrastruktur und die nachgelagerten Prozesse modernisieren können, um sie fit für das 21. Jahrhundert zu machen und Kunden einen sichtbaren Mehrwert bieten zu können, so die Zusammenfassung des Finanzberaters D+H.[8] Sie hat das Potenzial den Wertpapierhandelsprozess zu transformieren und eine entscheidende Weiterentwicklung im Wertpapierhandel darzustellen. Kryptografie und Dezentralisierung decken das gesteigerte Bedürfnis nach Informationssicherheit ab und verbessern die Geschwindigkeit der Handelsabwicklung von mehreren Tagen auf eine annähernd sofortige Ausführung, wodurch die Effizienz der Märkte deutlich gesteigert und Aufwendungen minimiert werden können. Eine Implementierung der Blockchain ist gleichzeitig aber auch mit tiefgreifenden Änderungen für die Akteure am Kapitalmarkt verbunden, weil sie etablierte Finanzinstitutionen aus den Bereichen Clearing und Settlement teilweise redundant werden lässt und Intermediäre durch Informationstechnik ersetzt.

Zielgruppe der Bachelorarbeit sind Beschäftigte aus allen Bereichen des Wertpapierhandels und an Finanztechnologie interessierte Studenten, die sich einen Überblick über die Blockchain-Technologie, ihre Funktionsweise und ihre Auswirkungen auf den Wertpapierhandel verschaffen möchten. Der Autor erhofft sich zudem, durch die Verknüpfung von Informationstechnologie und Finanzwirtschaft, einen interdisziplinären Erkenntnisgewinn über aktuelle Entwicklungen auf den Finanzmärkten.

Im ersten Schritt soll die grundlegende Funktionsweise der Blockchain-Technologie am Beispiel der Kryptowährung Bitcoin beschreiben werden. Auch wenn sich die Bitcoin Blockchain in einigen Punkten von einem Distributed Ledger für den Wertpapierhandel unterscheidet, ist die zu Grunde liegende Technologie dieselbe und für Bitcoin inzwischen durch die Literatur von Narayanan (2016) gut dokumentiert. Darauf aufbauend soll im zweiten Schritt im Rahmen einer SWOT-Analyse betrachtet werden, an welchen Stellen entlang des Wertpapierhandelsprozesses die DLT zum Einsatz kommen und die Märkte effizienter und sicherer gestalten kann und welche Herausforderungen bei einer

[8] Vgl. D+H, *Five Things Blockchain Must Get Right to Realize Its Full and Transformative Potential* (Toronto: D+H, 2016), S. 7. http://www.dh.com/resources/white-papers/five-things-blockchain-must-get-right-realize-its-full-and-transformative.

Einführung auftreten. Bei seiner Analyse stützt sich der Autor auf aktuelle Studien und Arbeitspapiere von Regulierungsbehörden, Beratungsunternehmen und Finanzdienstleistern aus Europa und den USA. Nicht Gegenstand dieser Bachelorarbeit ist die Analyse der juristischen Voraussetzungen für eine Implementierung der DLT im Wertpapierhandel.

3 Funktionsweise der Blockchain-Technologie

Im Folgenden sollen die technischen Grundlagen der Blockchain-Technologie erarbeitet werden, um darauf aufbauend in Abschnitt 4 die Chancen und Risiken der DLT für den Wertpapierhandel besser beurteilen zu können. Wegen ihres Charakters als Technologieträger der Blockchain und die gute Dokumentation, soll die Funktionsweise von Distributed Ledgern am Beispiel der Kryptowährung Bitcoin vorgestellt werden.

3.1 Kryptografie

Damit eine Währung funktioniert, ist es erforderlich, dass die verfügbare Geldmenge reguliert werden kann und eine Reihe von Sicherheitsmerkmalen erfüllt werden, um Betrug zu unterbinden und Vertrauen herzustellen.[9] Bei physischen Währungen fällt diese Aufgabe den Zentralbanken und Gesetzeshütern zu. Die gleichen Anforderungen müssen auch von virtuellen Währungen erfüllt werden. Falls beispielsweise eine Transaktion doppelt ausgeführt wird und unterschiedliche Empfänger aufweist, muss in einem Regelwerk definiert sein, welche Transaktion gültig und wer der korrekte Empfänger ist. Anders als bei physischen Währungen, übernimmt diese Aufgabe keine zentrale Behörde, sondern die Einhaltung des Regelwerks wird rein technologisch durchgesetzt. Zentrales Element dabei ist die Kryptografie. Über das Encodieren von Informationen werden Transaktionen betrugssicher gemacht und in Algorithmen ist hinterlegt, wie neue Einheiten der Währung erschaffen werden. Um das Funktionsprinzip von Kryptowährungen zu erschließen, ist es notwendig, die dahinterliegende Technologie genauer zu analysieren. Die Blockchain-Technologie basiert primär auf zwei kryptografischen Elementen: Hash-Funktionen und digitalen Signaturen. Erstere strukturieren die Transaktionen und Letztere ermöglichen den vertrauenswürdigen Austausch von Informationen zwischen den Handelsparteien.[10]

[9] Vgl. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (Online: Bitcoin.org, 2008), S. 1. https://bitcoin.org/bitcoin.pdf.

[10] Vgl. Narayanan, S. 1.

3.1.1 Hash-Funktionen

Eine Hash-Funktion ist eine mathematische Funktion, die im Wesentlichen die folgenden Eigenschaften aufweist:

- Der Eingabewert ist ein beliebiger String mit beliebiger Größe.
- Der Ausgabewert hat eine fest definierte Größe. Im Fall von Bitcoin beträgt diese 256-bit.
- Die Funktion ist deterministisch. Ein gleicher Eingabewert führt immer zum gleichen Ausgabewert.
- Die Funktion muss effizient zu berechnen sein und darf nicht zu rechenintensiv ausfallen.[11]

Hash-Funktionen mit den genannten Merkmalen lassen sich zum Aufbau einfacher Datenstrukturen verwenden. Der Eingabewert ist die *Nachricht* und der Ausgabewert der *Hash*. Dabei verrät der Hash nichts über die eingegebene Nachricht und auch nur geringe Änderungen der Nachricht haben einen völlig anderen Hash zum Ergebnis.

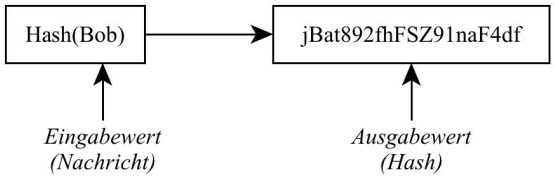

Abbildung 1: Hash-Funktion[12]

Damit sich die Hash-Funktion kryptografisch nutzen lässt, müssen drei weitere Merkmale erfüllt werden:

- Sie muss kollisionsresistent sein.
- Es muss sich um eine Einwegfunktion handeln.
- Sie muss puzzlefreundlich sein.[13]

[11] Vgl. ebd., S. 2.
[12] Eigene Darstellung
[13] Vgl. Narayanan, S. 2.

3.1.1.1 Kollisionsresistenz

Die erste zusätzliche Eigenschaft einer kryptografischen Hash-Funktion, ist die Notwendigkeit von Kollisionsresistenz. Von einer Kollision spricht man, wenn zwei unterschiedliche Eingabewerte zum gleichen Ausgabewert führen. Lässt sich für eine Hash-Funktion keine Kollision finden, gilt diese als kollisionsresistent. In Abbildung 2 wird eine Hash-Kollision dargestellt. Die unterschiedlichen Eingabewerte *x* und *y* haben das gleiche Hash-Ergebnis.

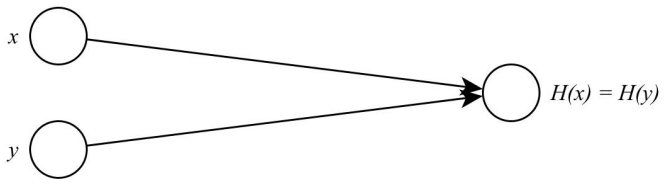

Abbildung 2: Hash-Kollision[14]

Kollisionsresistenz ist nicht zu verwechseln mit Kollisionsfreiheit und dass Kollisionen zwangsläufig existieren müssen, lässt sich einfach belegen: Da als Eingabewert ein beliebiger String mit beliebiger Größe gestattet ist, ist der Eingabewertebereich unendlich groß. Der Ausgabewertebereich hat hingegen eine fest definierte Größe und ist endlich. Folglich muss es Eingabewerte geben, die den identischen Ausgabewert haben, weil der Eingabewertebereich größer als der Ausgabewertebereich ist. Um eine Kollision für einen 256-bit Hash, wie von Bitcoin verwendet, zu finden, muss lediglich für $2^{256} + 1$ unterschiedliche Eingabewerte der Hash berechnet und das Ergebnis verglichen werden. Da die Anzahl der Eingabewerte höher als die mögliche Anzahl eindeutiger Ausgabewerte ist, werden mindestens zwei Hashwerte kollidieren. Bei der beschriebenen Methode ist eine Kollision garantiert. Mit hoher Wahrscheinlichkeit wird eine Kollision aber bereits deutlich vor dem Überschreiten des verfügbaren Hashwertebereichs eintreten. Für $2^{130} + 1$ zufällige Eingaben liegt die Wahrscheinlichkeit einer Kollision noch immer bei 99,8%. Dass grob angesetzt die Quadratwurzel an Eingaben aus dem gesamten Hashwertebereich ausreichend ist, um mit hoher Wahrscheinlichkeit eine Kollision

[14] Eigene Darstellung in Anlehnung an ebd., S. 3.

zu finden, liegt an einem statistischen Phänomen, das als *Geburtstagsparadoxon*[15] bekannt ist.[16]

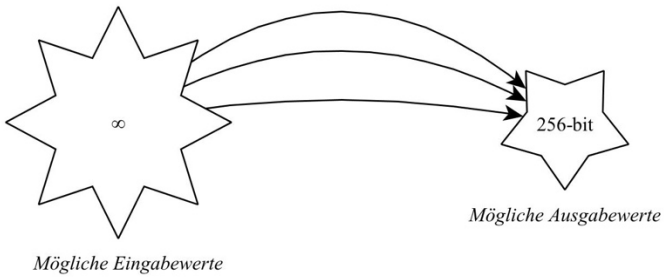

Abbildung 3: Unausweichlichkeit von Kollisionen[17]

Das Problem des vorgestellten Algorithmus zur Kollisionserkennung ist, dass die Berechnung aller Hashwerte äußert zeitaufwendig wäre. Unter der Annahme, dass ein Computer 10.000 Hashes pro Sekunde berechnen kann und dass im Durchschnitt alle 2^{128} Hashes eine Kollision gefunden wird, würde er 2^{27} Jahre für einen Durchlauf benötigen. Bildlich gesprochen heißt das, dass selbst wenn alle Computerchips der Menschheit seit Entstehung des Universums die Hash-Funktion berechnen würden, die Wahrscheinlichkeit, dass bis heute eine Kollision entdeckt worden wäre, noch immer infinitesimal gering ist. Solange für eine Hash-Funktion trotz großer Bemühungen noch keine Kollision nachgewiesen werden konnte, gilt diese als kollisionsresistent.[18]

In der Praxis wird die Eigenschaft der Kollisionsresistenz kryptografischer Hash-Funktionen bei der Berechnung von Prüfsummen ausgenutzt. Der Cloud Service-Anbieter *SecureBox* ermöglicht es beispielsweise, die Integrität selbst hochgeladener Dateien zu überprüfen. Angenommen die Benutzerin *Alice* möchte große Dateien online archivieren. Um bei erneutem Gebrauch überprüfen zu können, ob die online archivierten Dateien noch im Originalzustand sind, hätte *Alice* weiterhin lokale Kopien für einen Vergleich vorhalten müssen, was die Vorteile einer Archivierung unterlaufen würde. Hash-Funktionen bieten *Alice* die elegante Lösung, nur die Hashes der archivierten Dateien lokal speichern zu müssen. Für eine heruntergeladene Datei muss sie dann nur den

[15] Vgl. sciencebuddies, "Probability and the Birthday Paradox", Springer Nature, https://www.scientificamerican.com/article/bring-science-home-probability-birthday-paradox.

[16] Vgl. Narayanan, S. 3.

[17] Eigene Darstellung in Anlehnung an ebd.

[18] Vgl. ebd., S. 4f.

Hash berechnen lassen und diesen mit dem Gespeicherten vergleichen. Sind die Hashes identisch, entspricht die heruntergeladene Datei der Hochgeladenen. Unterscheiden sie sich hingegen, kann *Alice* den Rückschluss ziehen, dass die Datei entweder beim Upload beschädigt oder absichtlich manipuliert wurde. Kollisionsresistente Hash-Funktionen sind ein probates Mittel, um betrügerisches Verhalten aufzudecken und äußerst effektiv, wenn es darum geht, den Computer Dinge erkennen zu lassen, die er vorher schon einmal gesehen hat.[19] Gleichzeitig reduzieren sie den benötigten Speicherplatz erheblich.[20]

3.1.1.2 Einwegfunktionen

Einwegfunktionen sind die Grundlage asymmetrischer Kryptografie. Das bedeutet, wenn der Ausgabewert einer Hash-Funktion bekannt ist, dass keine Rückschlüsse auf den Eingabewert gezogen werden können. Damit diese Eigenschaft eingehalten werden kann, ist es notwendig, dass der Eingabewertebereich ausreichend groß und verteilt ist. Angenommen *Alice* wirft eine Münze und diese zeigt *Kopf*. Sie berechnet den Hashwert für *Kopf* und zeigt das Ergebnis *Bob*, der den Münzwurf nicht gesehen hat. Um herauszufinden, wie die Münze geworfen wurde, muss *Bob* lediglich selbst die Hashes für *Kopf* und *Zahl* berechnen und mit dem Hash von *Alice* vergleichen. Mit Hilfe eines Tricks, lassen sich die Eingaben *Kopf* und *Zahl* aber dennoch verschleiern. Dazu wird der Eingabewert mit einem weiteren, geheimen Zufallswert aus einem ausreichend großen und verteilten Wertebereich verkettet, so dass es nahezu unmöglich wird, die ursprüngliche Eingabe zu rekonstruieren.[21]

Die Eigenschaft der Einwegfunktion findet im Commitment-Verfahren Anwendung. Ein Commitment ist das digitale Gegenstück zu einem Brief, der in einem versiegelten Couvert sichtbar auf dem Schreibtisch liegt. Der Verfasser des Briefs bekennt sich automatisch zu dessen Inhalt. Er kann ihn nicht mehr ändern und nur ihm ist dieser bis zum Öffnen des Couverts bekannt.

Das Commitment-Verfahren besteht aus zwei Algorithmen:

- *commit(Nachricht, Nonce)* Die Commit-Funktion nimmt als Eingabe die Nachricht und verkettet diese mit einem zufälligen Wert, der *Nonce* genannt wird. Das Ergebnis der Funktion ist das Commitment.

[19] Vgl. ebd.
[20] Vgl. Nakamoto, S. 4.
[21] Vgl. Narayanan, S. 6–8.

- *verify(Commitment, Nachricht, Nonce)* Die Verify-Funktion nimmt als Eingaben das Commitment zur Nachricht, die Nachricht selbst und die Nonce. Das Ergebnis der Funktion ist wahr oder falsch.

Um die Nachricht des Commitments bekannt zu machen, ist es lediglich notwendig die Nonce zu verraten, so dass jeder den Inhalt verifizieren kann. Die beiden Algorithmen sind mit dem Versiegeln und Öffnen des Briefcouverts vergleichbar. Wichtig ist, dass für jedes Commitment eine neue Nonce gewählt wird. Die Nonce ist ein zufällig generierter Wert, der einmalig verwendet wird.[22]

Integriert man das Commitment-Verfahren in eine kryptografische Hash-Funktion, so wird eine 256-bit Nonce mit der Nachricht verkettet. Von diesem verketteten Wert wird dann der Hash als Commitment berechnet. Ohne Kenntnis von Nachricht und Nonce ist es unmöglich, Rückschlüsse vom Hashwert auf den Nachrichteninhalt zu ziehen. Für eine Verifikation müssen alle drei Parameter bekannt sein. Zudem verhindert die Kollisionsresistenz, dass es mehr als eine wahre Lösung bei der Verifikation geben kann.[23]

3.1.1.3 Puzzlefreundlichkeit

Die dritte Anforderung an eine kryptografische Hash-Funktion ist Puzzlefreundlichkeit. Ein Puzzle meint in diesem Fall ein mathematisches Problem, bei dem ein sehr großer Wertebereich zum Finden einer Lösung durchsucht werden muss und für das es keine Abkürzung gibt. Das Ergebnis kann nur durch Ausprobieren von Zufallswerten gefunden werden. Die Bestandteile eines Puzzles sind:

- Eine Hash-Funktion H mit 2^{256} möglichen Ausgabewerten.
- Eine zufällig gewählte Puzzle-ID *id* aus einem ausreichend großen und verteilten Wertebereich.
- Ein Zielwertebereich Y der kleiner als der Ausgabewertebereich von H ist.
- Der gesuchte Wert x.

$H(verkettet(id, x)) \in Y$ In dem Puzzle wird x gesucht, das mit einer zufälligen Puzzle-ID *id* verkettet ist. Der sich ergebende Hashwert muss dabei in den Zielwertebereich Y fallen. Definiert man den Zielwertebereich Y mit 2^{256} Möglichkeiten genau so groß wie den Ausgabewertebereich der Hash-Funktion, dann ist das Puzzle trivial und der Hash

[22] Vgl. ebd.
[23] Vgl. ebd.

für jeden Wert *x* würde in den Zielbereich *Y* fallen. Ist *Y* hingegen 1, dann ist das Puzzle maximal schwer zu lösen, weil es nur einen einzigen Hashwert gibt, der in den Zielwertebereich fällt. Mit der Wahl von *Y* ist es also möglich die Schwierigkeit eines Puzzles zu bestimmen. Diese Eigenschaft wird sich beim Bitcoin Mining zu Nutze gemacht.[24]

3.1.1.4 SHA-256

Nachdem die drei Eigenschaften kryptografischer Hash-Funktionen besprochen und an Beispielen veranschaulicht wurden, schauen wir uns die Hash-Funktion an, die Bitcoin im Speziellen nutzt und die unter dem Namen SHA-256 bekannt ist. SHA-256 setzt sich aus einer Kompressionsfunktion und der sogenannten Merkle-Damgård-Transformation zusammen. Dabei ist das Funktionsprinzip relativ einfach erklärt:

1. Jeder beliebige String wird von der Merkle-Damgård-Transformation in Blöcke von 512-bit Größe aufgeteilt.
2. Die 512-bit großen Blöcke werden mit dem 256-bit Hashwert des jeweils vorherigen Blocks verkettet, so dass sich eine Eingabegröße von 768-bit für die Kompressionsfunktion ergibt.
3. Die Kompressionsfunktion verarbeitet die 768-bit großen Eingaben und berechnet dafür den 256-bit großen Hashwert, der wiederum mit dem nächsten neuen 512-bit großen Block verkettet wird.
4. Der Rückgabewert der SHA-256-Hash-Funktion ist der 256-bit Hashwert des letzten berechneten Blocks.

Da der allererste Block nicht mit einem vorherigen Hashwert verkettet werden kann, wird stattdessen ein Initialisierungsvektor verwendet, der in SHA-256 fest hinterlegt ist.[25]

[24] Vgl. ebd., S. 8f.
[25] Vgl. ebd., S. 9f.

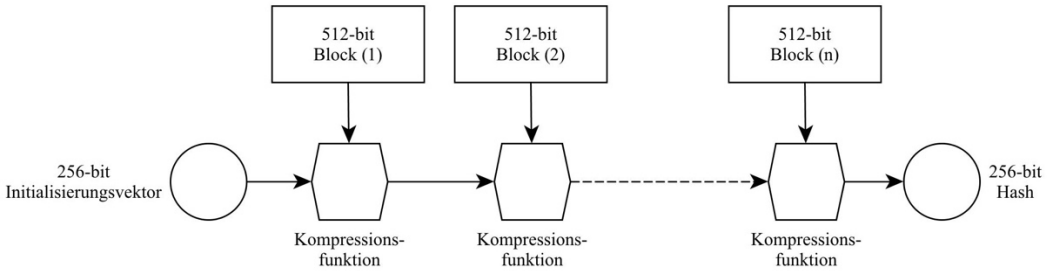

Abbildung 4: SHA-256-Hash-Funktion[26]

3.1.2 Hash Pointer

Hash Pointer sind ein Grundbaustein der Datenstruktur der Blockchain und zeigen an, wo eine Information gespeichert wurde. Zusätzlich halten sie den Hashwert der gespeicherten Information zur Verifikation bereit.

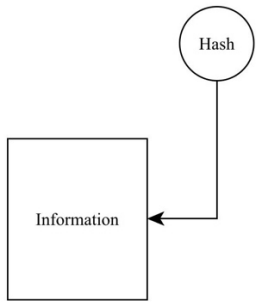

Abbildung 5: Hash Pointer[27]

3.1.2.1 Blockchain

Verlinkt man aufeinander aufbauende Informationen mit Hash Pointern untereinander, erhält man eine verlinkte Liste, die Blockchain genannt wird. Im Gegensatz zu einer, über einfache Pointer verlinkten Liste, hat die Blockchain den Mehrwert, dass jeder Block nicht nur verrät, wo der vorherige Block gespeichert wurde, sondern zusätzlich den Hash bereithält, um sicherzustellen, dass der vorherige Block nicht manipuliert worden ist. Um die gesamte Blockchain auslesen zu können, muss lediglich der Hash des letzten Blocks bekannt sein. Mit der Blockchain lassen sich beispielsweise fälschungssichere Logs erstellen.[28]

---

[26] Eigene Darstellung in Anlehnung an ebd., S. 10.

[27] Eigene Darstellung in Anlehnung an ebd., S. 11.

[28] Vgl. ebd.

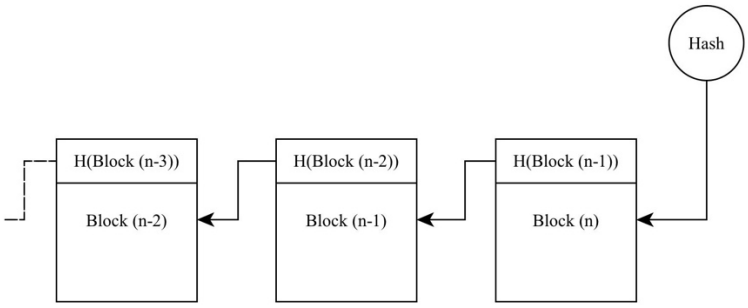

Abbildung 6: Blockchain[29]

Angenommen ein Angreifer manipuliert die Daten aus Block (n-1). Da die Daten jetzt nicht mehr mit dem in Block (n) gespeicherten Hash übereinstimmen, würde der Hash Pointer als Ergebnis *falsch* liefern und den Betrugsversuch sofort auffliegen lassen. Die Kollisionsresistenz garantiert uns, dass die geänderten Daten auf keinen Fall mit dem alten Hash übereinstimmen werden. Selbst wenn der Angreifer jeden einzelnen Block so anpasst, dass die Hash Pointer untereinander alle zu einem *wahren* Ergebnis kommen, würde die Manipulation direkt bei Block (n) auffallen, weil der uns bekannte Hash des Endes der Blockchain, den Block (n) nicht verifizieren würde (Abbildung 6).[30]

3.1.2.2 Merkle Tree

Eine weitere Datenstruktur, die sich mit Hilfe von Hash Pointern bauen lässt, ist ein, als Merkle Tree bekannter, binärer Baum. Die Blätter des Baums sind in Paaren angeordnete Datenblöcke. Die beiden Hashwerte eines Blockpaares sind in einem Elternknoten zusammengefasst. Dann werden jeweils zwei Elternknoten gruppiert und über einen Hash in einem neuen Elternknoten eine Ebene höher gespeichert. Die Äste des Baums werden immer enger zusammengeführt, bis man am Wurzelknoten angekommen ist.

[29] Eigene Darstellung in Anlehnung an ebd.
[30] Vgl. ebd., S. 11f.

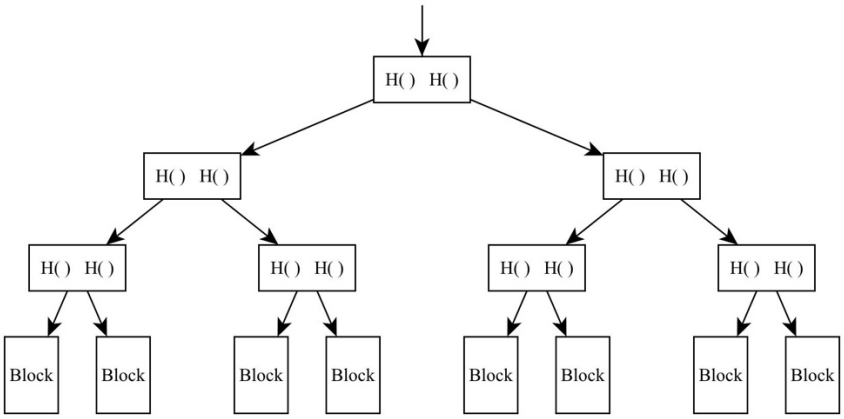

Abbildung 7: Merkle Tree[31]

Wie bei der Blockchain, ist es auch beim Merkle Tree ausreichend, immer nur den aktuellen Hash des Wurzelknotens zu kennen, um den gesamten Baum verifizieren zu können. Zusätzlich unterstützt der Merkle Tree das Konzept Proof of Membership. Ziel des Proof of Memberships ist es, den Beweis erbringen zu können, dass ein bestimmter Block gültiger Teil der Datenstruktur ist. Dafür genügt es, nur den Ast vom Wurzelknoten bis zum entsprechenden Block zu verifizieren. Die Anzahl der zu überprüfenden Knoten entspricht dabei dem Logarithmus der Gesamtanzahl an Knoten. Auch wenn die Blockchain ebenfalls grundsätzlich ein Proof of Membership zulässt, ist die Verifikation eines Blocks im Merkle Tree bei vielen Blöcken wesentlich effizienter möglich.[32]

[31] Eigene Darstellung in Anlehnung an ebd., S. 13.
[32] Vgl. ebd., S. 12–15.

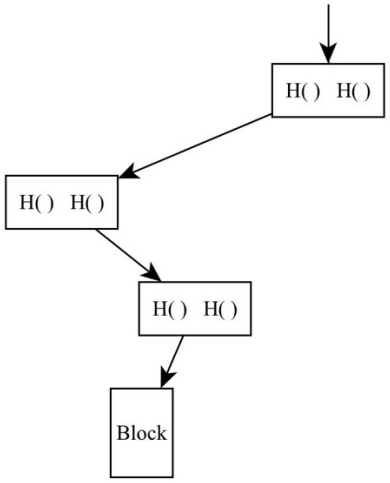

Abbildung 8: Proof of Membership[33]

3.1.3 Digitale Signaturen

Digitale Signaturen sind ein weiteres kryptografisches Werkzeug, das zum Erstellen einer Kryptowährung benötigt wird. Sie sind das digitale Gegenstück zu einer Unterschrift auf einem Brief und müssen vergleichbare Merkmale aufweisen:

- Nur man selbst kann mit seiner eigenen Signatur unterschreiben, aber jeder kann diese auf Echtheit verifizieren. Analog verhält es sich mit der händischen Unterschrift, die einen selbst identifiziert und nur schwer zu fälschen ist, aber von allen gelesen und bestätigt werden kann.
- Die Signatur ist an das unterschriebene Dokument gebunden und kann nicht auf ein anderes kopiert werden. Das heißt, jedes Dokument muss einzeln signiert werden. Auch beim analogen Pendant kann die Unterschrift nicht einfach ausgeschnitten und auf ein neues Dokument geklebt werden, ohne dass es auffallen würde.[34]

Digitale Signaturen authentifizieren also eine Nachricht zwischen Sender und Empfänger auf eine Weise, die den Empfänger und alle Benutzer der Blockchain verifizieren lässt, dass die Nachricht tatsächlich vom erwarteten Sender stammt und dass sie nicht manipuliert wurde. Gleichzeitig kann der Sender nicht abstreiten, dass er die Nachricht gesendet hat, weil sie mit seiner Signatur versehen ist. Daraus lässt sich ein Schema

[33] Eigene Darstellung in Anlehnung an ebd., S. 14.
[34] Vgl. ebd., S. 15–17.

ableiten, das digitale Signaturen erfüllen müssen und das auf drei einfachen Algorithmen beruht:

- g*enerateKeys(Schlüsselgröße)* Die Methode bekommt als Parameter die gewünschte Schlüsselgröße übergeben und erzeugt einen Public Key und einen Secret Key. Der Secret Key wird geheim gehalten und dient dem Signieren von Nachrichten. Er ist die eigene Unterschrift. Der Public Key wird hingegen der Öffentlichkeit bekannt gegeben. Er ermöglicht es anderen, die Signatur verifizieren zu können.
- *sign(Secret Key, Nachricht)* Mit *sign* wird eine Nachricht mit dem Secret Key unterschrieben und es wird eine Signatur für das unterschriebene Dokument generiert.
- *verify(Public Key, Nachricht, Signatur)* Die Verify-Methode ermöglicht das Verifizieren einer Nachricht, in dem diese mit dem Public Key und der Signatur des Senders verglichen wird. Das Ergebnis ist entweder wahr oder falsch.

Für die Sicherheit ist es wichtig, dass die Schlüsselpaare zufällig generiert werden. Auch gilt, dass ein großer Wertebereich für die Schlüsselgröße mehr Schlüsselpaare erlaubt und entsprechend schwieriger zu fälschen ist, als ein Schlüsselpaar aus einem kleinen Wertebereich. In der praktischen Anwendung wird oft nicht die Nachricht selbst signiert, sondern der Hash der Nachricht. Signiert man beispielsweise den Hash Pointer am Ende der Blockchain, dann gilt die gesamte Blockchain als signiert.[35]

3.1.4 Public Keys als Identität

Im echten Leben identifiziert die Unterschrift eine Person. Diesen Umstand macht man sich auch bei digitalen Signaturen zu Nutze, wo der Public Key einem Benutzer eindeutig zuzuordnen ist. Aus dieser Sicht verleiht der Public Key einer signierten Nachricht eine Identität. Das bedeutet, dass sich jeder Benutzer in der digitalen Welt beliebig viele neue Identitäten zulegen kann, in dem er einfach ein neues Schlüsselpaar generiert. Da die Schlüsselpaare zufällig generiert werden, lassen sich Public Keys auch nicht direkt einer Person zuordnen. Dennoch verschaffen viele Identitäten keine echte Anonymität, weil sich Verhaltensmuster im Netzwerk nach einiger Zeit oftmals einem Benutzer zuordnen lassen. Durch die Tatsache, dass jeder seine eigenen Schlüsselpaare erstellen

[35] Vgl. ebd.

kann, entsteht der attraktive Mehrwert einer dezentralisierten Verwaltung von Identitäten. Es ist keine zentrale Einheit mehr notwendig, um neue Benutzer zu registrieren. Jeder Benutzer registriert sich mit seinem Public Key automatisch selbst und kann selbst bestimmen, wie viele Identitäten er verwenden und wann oder ob er sie wechseln möchte. In Bitcoin und anderen Kryptowährungen werden diese Identitäten *Adresse* genannt.[36]

3.2 Dezentralisierung

Nachdem wir die grundlegenden kryptografischen Werkzeuge der Blockchain-Technologie vorgestellt haben, ist es an der Zeit zu analysieren, mit Hilfe welcher Mittel die Bitcoin Blockchain dezentralisiert wird. Um diese Frage beantworten zu können, müssen wir geeignete Untersuchungskriterien definieren:

- Wer pflegt den Ledger mit Transaktionen?
- Wer validiert die Transaktionen?
- Wer kann neue Bitcoins erstellen?

Grundsätzlich kann jeder die Bitcoin Software installieren und Teil des Peer-to-Peer-Netzwerks werden. Auch sind die Einstiegsbarrieren dafür relativ gering und ein handelsüblicher Computer ist ausreichend. Bitcoin Mining erfordert hingegen einen großen technischen Aufwand und hohe Investitionen. Das hat zu einer Bündelung und Zentralisierung von Mining-Ressourcen geführt, die von nur einer Hand voll Akteuren kontrolliert werden.[37]

3.2.1 Verteilter Konsens

Der Hauptgrund ein System zu dezentralisieren, ist das Erhöhen von Ausfallsicherheit und Zuverlässigkeit. Die zentrale Herausforderung eines dezentralisiert verwalteten Ledgers, ist das Herstellen eines Konsens zwischen den zahllosen Netzwerkteilnehmern, so dass alle Nodes synchronisiert sind. Auch Eingaben von fehlerhaften oder bösartigen Nodes müssen von den ehrlichen Teilnehmern abgelehnt werden können.

Angenommen *Alice* möchte eine Transaktion an *Bob* senden. Weil es sich um ein Peer-to-Peer-Netzwerk handelt, wird die Transaktion an alle Nodes im Netzwerk gesendet.

[36] Vgl. ebd., S. 18–21.
[37] Vgl. ebd., S. 27f.

Unsere Ausgangslage ist ein globaler Ledger über den Konsens im Netzwerk herrscht. Um die Transaktion zu empfangen, ist es nicht notwendig, dass *Bob* selbst eine Node bereitstellt, da das Netzwerk ohne sein Zutun entscheiden wird, ob die Transaktion gültig oder ungültig ist

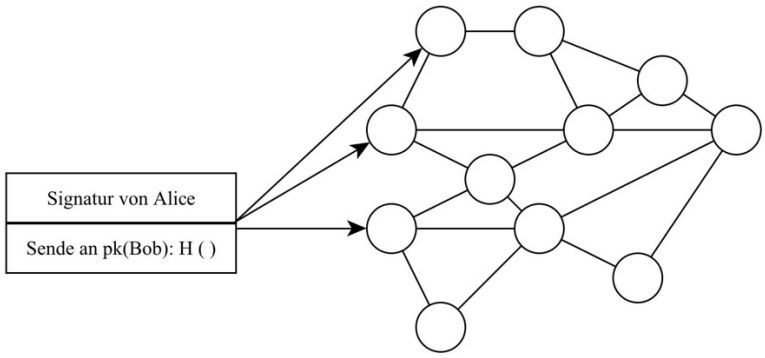

Abbildung 9: Senden einer Transaktion im P2P-Netz[38]

Die Schwierigkeit liegt darin, dass nicht nur *Alice* eine Transaktion senden wird, sondern unzählige Netzwerkteilnehmer gleichzeitig ihre Transaktionen senden. Diese müssen in eine Reihenfolge gebracht und dann validiert werden. Um das Verfahren übersichtlicher und effizienter zu gestalten, werden sie dazu in Blöcken zusammengefasst. Jede Node führt eine Liste mit ausstehenden Transaktionen, die an sie gesendet worden sind, die aber noch nicht in der Blockchain aufgenommen wurden. So hat jede Node eine etwas andere Sicht über den Stand der Transaktionen. Wir erinnern uns daran, dass in der Blockchain nur Blöcke geführt werden, über die Konsens im Peer-to-Peer-Netzwerk besteht. In einem Intervall von 10 min schlagen die Nodes ihren Block mit offenen Transaktionen dem gesamten Netzwerk vor und ein Konsens-Protokoll entscheidet und validiert, welcher Block als nächstes in die Blockchain aufgenommen wird. Gültige Transaktionen, die keinen Platz mehr in dem ausgesuchten Block hatten, werden im folgenden Block übernommen.[39]

In der Praxis müssen auf dem Weg dahin aber noch eine ganze Reihe von technischen Problemen gelöst werden. So gibt es Nodes, die bösartig sind und ungültige Transaktionen versenden, mache können abstürzen oder über eine schlechte Internetverbindung mit dem Netz verbunden sein und zuletzt ist das Peer-to-Peer-Netzwerk nicht vollver-

[38] Eigene Darstellung in Anlehnung an ebd., S. 30.
[39] Vgl. ebd., S. 28–32.

mascht, das heißt nicht jede Node ist untereinander verbunden. Unter diesen Umständen ist es unmöglich, dass alle Nodes dem Konsens-Protokoll zustimmen können. Ebenso verhindern unterschiedliche Latenzzeiten, dass sich die Nodes auf eine verbindliche Reihenfolge der Transaktionen einigen können. Glücklicherweise konnte sich das Bitcoin Peer-to-Peer-Netzwerk trotz schlechter theoretischer Voraussetzungen in der Praxis bereits bewähren und funktioniert besser, als zu vermuten wäre. Das liegt insbesondere daran, dass Bitcoin mit vielen der traditionellen Annahmen bricht, die man in der Erforschung verteilter Netze als Grundvoraussetzung erachtet hat. In der Tat erbringt Bitcoin derzeit den Beweis, dass der verteilte Konsens so zuverlässig funktioniert, dass eine Anwendung der Blockchain-Technologie auch außerhalb von Kryptowährungen intensiv erforscht wird.[40]

An welchen Stellen bricht Bitcoin nun aber mit der Theorie? Ein zentraler Aspekt ist das Belohnen ehrlichen Verhaltens. Ehrliche Nodes erhalten einen Block Reward für das Validieren neuer Blöcke und ihnen ist zudem freigestellt, eine Transaktionsgebühr für eingehende Transaktionen zu erheben. Daneben spielt Zufälligkeit im Konsens-Protokoll eine große Rolle, wie wir im Folgenden untersuchen werden. Auch wird ein Konsens nicht sofort erreicht, sondern etwa eine Stunde nach Verarbeitung ihrer Transaktion, kann *Alice* davon ausgehen, dass ausreichend Nodes ihrer Transaktion zugestimmt haben und der Konsens darüber im Netzwerk so hoch ist, dass es als ausgeschlossen angenommen werden kann, dass das Netzwerk seine Meinung ändert und die Transaktion für ungültig erklärt.[41]

3.2.2 Konsens ohne Identität

Der verteilte Konsens ist in Bitcoin um die Eigenschaft erweitert, dass die Nodes über keine feste Identität verfügen. Der Grund dafür ist, dass Bitcoin auf einem Peer-to-Peer-Netzwerk basiert, wo es keine zentrale Verwaltungseinheit gibt, die neuen Nodes eine Identität zuweisen könnte. Ebenso ist eines der Design-Ziele von Bitcoin, die Pseudonymität seiner Nutzer zu wahren. Niemand soll gezwungen werden, seine wahre Identität offenbaren zu müssen. Ein Gegenbeispiel für ein verteiltes Netz mit zentraler Verwaltung und festen Identitäten wäre das Servernetz von Facebook, weil sich in dem Netz nicht einfach ein unbekannter Server anmelden kann. Identitäten helfen dabei, feh-

[40] Vgl. ebd.
[41] Vgl. ebd.

lerhafte Nodes zu identifizieren und die Last zu verteilen. Das Fehlen eben dieser in Bitcoin erschwert es deshalb, ein Protokoll zur Konsensfindung zu definieren. [42]

3.2.2.1 Impliziter Konsens

Die Lösung des Problems heißt impliziter Konsens. Die Nodes werden nach einem Zufallssystem selektiert und dürfen einen neuen Block für die Blockchain vorschlagen. Es kommt zu keinem klassischen Konsens und es findet keine Abstimmung zwischen den Nodes über den vorgeschlagenen Block statt. Die vom Protokoll bestimmte Node schlägt unilateral ihren Block vor. Was aber, wenn die Node sabotiert wurde? Jetzt kommt der implizite Konsens ins Spiel, denn die anderen Nodes entscheiden für sich selbst, ob der neue Block valide ist, in dem sie den Block in ihre Version der Blockchain aufnehmen und auf ihm aufbauen oder sie lehnen den Block ab, in dem sie auf dem zuletzt akzeptierten Block aufbauen und den neuen Block ignorieren. Da die Blöcke über Hash Pointer miteinander verknüpft sind, ist für jede Node sichtbar, auf welchem Block andere Nodes gerade aufbauen. In vereinfachter Version sieht die Konsensfindung in Bitcoin wie folgt aus:

1. Neue Transaktionen werden im Peer-to-Peer-Netzwerk verbreitet.
2. Jede Node bündelt die ausstehenden Transaktionen, von denen sie gehört hat, in einem Block.
3. In jeder Runde darf eine zufällig ausgewählte Node einen Block vorschlagen.
4. Die anderen Nodes akzeptieren diesen Block implizit, wenn alle darin enthaltenen Transaktionen valide sind.
5. Die Nodes machen ihr Einverständnis sichtbar, indem sie den Hash des neuen Blocks in ihrem nächsten neuen Block aufnehmen.

Um zu verstehen, warum der implizite Konsens funktioniert, betrachten wir ein paar typische Angriffsmuster, mit denen ein Angreifer versuchen könnte, das System zu hintergehen. Nennen wir unseren Angreifer in den nachfolgenden Beispielen *Alice*.[43]

3.2.2.2 Stehlen von Bitcoins

Alice, die tausende sabotierte Nodes im Peer-to-Peer-Netzwerk kontrolliert und daher gute Chancen hat, den nächsten Block vorschlagen zu dürfen, könnte beliebige Transak-

[42] Vgl. ebd., S. 32f.
[43] Vgl. ebd., S. 33f.

tionen kreieren und sich die Bitcoins unwissender Benutzer überweisen. Der Angriff wäre jedoch sinnlos, denn dafür müsste sie die Signaturen der Benutzer fälschen können, was nicht möglich ist, wie wir gelernt haben.[44]

3.2.2.3 Denial-of-Service Attack

Alice könnte im Streit mit Bob liegen und ihm deshalb den Service verweigern wollen. Sie nimmt keine der von Bob getätigten Transaktionen in ihren Block auf. Sollte Alice den nächsten Block vorschlagen dürfen, wäre der Angriff sogar erfolgreich, denn ihr Block an sich ist gültig und würde von den anderen Nodes akzeptiert werden. Jedoch ist es äußerst wahrscheinlich, dass den darauffolgenden Block eine nicht von Alice kontrollierte Node vorschlagen darf, welche die Transaktionen von Bob aufnehmen würde. Eine Denial-of-Service Attack ist also auch nicht zielführend.[45]

3.2.2.4 Double-Spend Attack

Als weiteres Angriffsmuster könnte Alice eine Double-Spend Attack unternehmen. Ein dafür denkbares Szenario wäre, dass Alice im Online Shop von Bob Waren einkauft. Beim Check Out bezahlt Alice regulär die Waren und die Transaktion an Bob wird von einer ehrlichen Node in den nächsten Block der Blockchain übernommen, was in Abbildung 10 von *Block (n+1)* dargestellt wird. Die Transaktion enthält Alices Signatur, die Zahlungsanweisung an den Public Key von Bob und einen Hash, der Auskunft darüber gibt, aus welcher ehemaligen Transaktion Alice die Bitcoins erhalten hat, die sie jetzt ausgibt. Nachdem Bob sieht, dass die Transaktion in der Blockchain aufgenommen wurde, verschickt der die Waren an Alice. Angenommen eine von Alice kontrollierte Node darf jetzt den nächsten Block vorschlagen, dann könnte sie den neuen Block mit der Transaktion an Bob ignorieren und auf *Block (n)* vor ihrer Transaktion aufbauen. Ihr eigener *Block (n+1)'* enthält dann eine Transaktion, die die ursprünglich an Bob geschickten Bitcoins, an eine weitere, von ihr selbst kontrollierte Adresse *Alice'* sendet. Es existieren jetzt zwei Versionen der Blockchain. Welche Transaktion gültig sein wird, hängt vom Langzeitkonsens der Nodes ab.[46]

---

[44] Vgl. ebd., S. 34.
[45] Vgl. ebd.
[46] Vgl. ebd., S. 35.

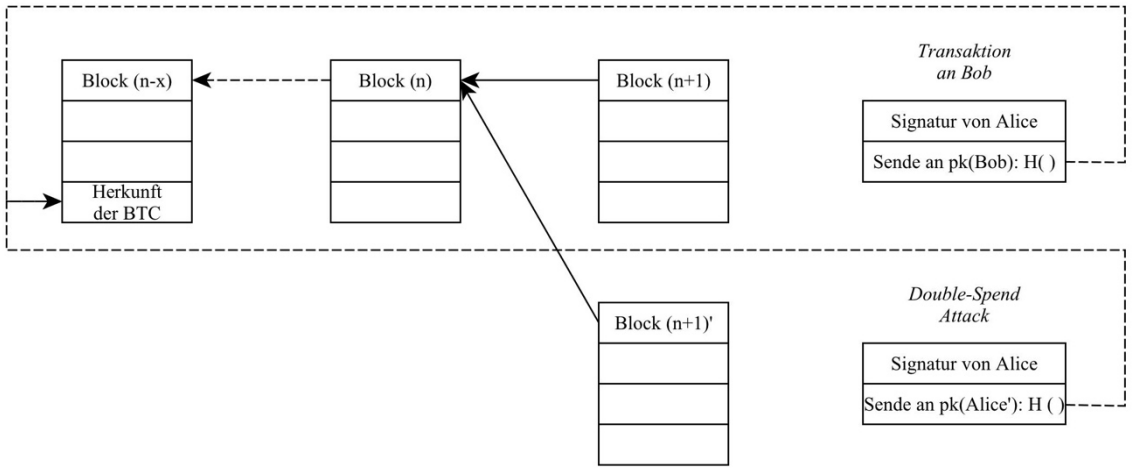

Abbildung 10: Double-Spend Attack[47]

In ihrem Protokoll ist verankert, dass ehrliche Nodes immer auf der längsten gültigen Kette der Blockchain aufbauen. In unserem Beispiel gibt es nach der Double-Spend Attack zwei gleichlange Ketten, die beide einen gültigen letzten Block haben. Moralisch gesehen müsste auf jeden Fall auf Block (n+1) aufgebaut werden, aber technisch gesehen sind die Transaktionen absolut gleichwertig zu behandeln. Normalerweise wählen Nodes bei Gleichstand den Block, der zuerst im Netzwerk verkündet wurde, aber durch Latenzzeiten und die nicht perfekte Vernetzung der Nodes untereinander, könnte das auch Block (n+1)' mit der Double-Spend Attack sein. Entscheidet sich die nächste Node also für Block (n+1)', dann steigt die Wahrscheinlichkeit, dass Alice mit ihrem Angriff erfolgreich war und ihre Version im Langzeitkonsens der Blockchain übernommen wird. Der Block des betrogenen Verkäufers Bob wird zum Waisenblock, weil die Kette nicht weiter verlängert wird und ihre Gültigkeit verliert.[48]

Sollte es sich bei Bob um einen extrem gutgläubigen Verkäufer handeln, könnte er die Ware bereits an Alice verschicken, sobald Alice ihre Transaktion an Bob im Netzwerk verbreitet ohne dass die Transaktion überhaupt schon in Block (n+1) übernommen wurde. Die Bezeichnung dafür heißt *Zero Confirmation Transaction*, weil die Transaktion noch von keiner einigen Node bestätigt wurde. Handelt es sich bei Bob hingegen um einen vorsichtigen Verkäufer, fällt es leicht die Sicherheitsmerkmale von Bitcoin Transaktionen im Nachfolgenden zu verstehen. Um nicht Opfer einer Double-Spend Attack zu werden, wartet Bob mit dem Versenden der Ware mehrere Bestätigungen der Trans-

[47] Eigene Darstellung in Anlehnung an ebd.
[48] Vgl. ebd., S. 34–38.

aktion von anderen Nodes ab (Abbildung 11). Je häufiger die Transaktion von Alice an ihn bestätigt wurde, umso sicherer kann er sich sein, nicht betrogen zu werden. Die Wahrscheinlichkeit, Opfer einer Double-Spend Attack zu werden, sinkt exponentiell mit der Anzahl an Bestätigungen der Transaktion. In der Praxis haben sich bei Bitcoin sechs Bestätigungen als guter Kompromiss zwischen Wartezeit und Sicherheit erwiesen.

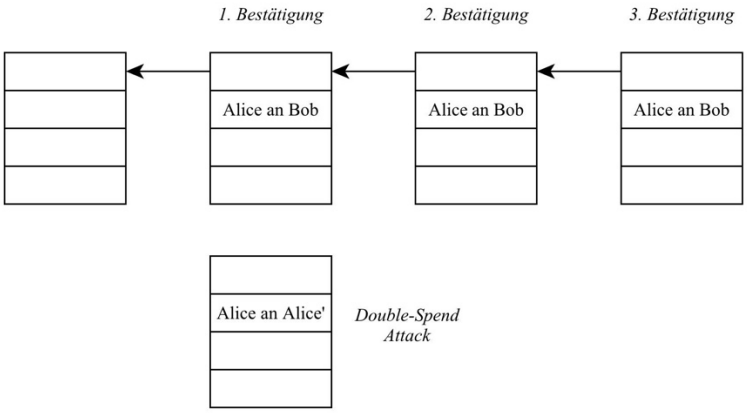

Abbildung 11: Transaktionsbestätigungen[49]

Zusammengefasst lässt sich sagen, dass der Schutz vor Betrug in der Blockchain-Technologie kryptografisch gelöst und über Konsensfindung durchgesetzt wird. Kryptografie schützt vor dem Stehlen von Bitcoins, weil es dem Angreifer unmöglich ist, die digitalen Signaturen zu fälschen. Das Finden des Langzeitkonsens macht Denial-of-Service Angriffe sinnlos, da ehrliche Nodes die Verifizierung von gültigen Transaktionen nicht verweigern und eine Double-Spend Attack endet für den Angreifer in einer Sackgasse, wenn sich das Ziel des Angriffs nicht naiv verhält und ausreichend Bestätigungen der Transaktion abwartet. Da die meisten Nodes ehrlich sind und immer auf der längsten Kette der Blockchain aufbauen, ist es ausgeschlossen, dass eine Transaktion mit ausreichend Bestätigungen im Nachhinein ungültig wird.[50]

3.2.3 Anreizsystem

Im vorangegangen Kapitel haben wir betrachtet, wie Blockchain-Transaktionen technisch sicher gemacht werden und sind davon ausgegangen, dass sich der Großteil der Nodes ehrlich verhält. Da sowohl bei Kryptowährungen, als auch im Wertpapierhandel

[49] Eigene Darstellung in Anlehnung an ebd., S. 37.
[50] Vgl. ebd., S. 34–38.

große Mengen an Geld bewegt werden, ist der Versuch für einen Angreifer besonders attraktiv, das System zu umgehen. Um dem entgegenzuwirken, ist in Bitcoin ein Anreizsystem implementiert, das ehrliches Verhalten belohnen soll.

Betrachtet man die Double-Spend Attack, könnte man auf Idee kommen, bösartige Nodes zu sanktionieren oder auszuschließen. Im Falle von Bitcoin verfügen die Nodes jedoch über keine feste Identität, so dass Sanktionsmaßnahmen keine sinnvolle Lösung sind.[51]

3.2.3.1 Block Reward

Der erste Anreiz für ehrliches Verhalten in Bitcoin ist der sogenannte Block Reward. Für das Erstellen eines neuen Blocks, darf die Node eine Spezialtransaktion hinzufügen, die neue Bitcoins erstellt und deren Empfänger sich die Node selbst aussuchen darf. Im Grunde genommen wird die Node also einfach für ihre geleistete Arbeit bezahlt. Da auch die Spezialtransaktion im Langzeitkonsens der Blockchain von anderen Nodes bestätigt werden muss, wird eine bösartige Node, die einen neuen Block vorschlägt, keinen Block Reward erhalten, weil ihre Version der Blockchain verwaisen und nicht zur längsten Kette werden wird. Der Block Reward ist die einzige Art und Weise, wie neue Bitcoins erstellt werden können. Allerdings werden im Jahr 2140 alle 21 Millionen Bitcoins erstellt worden sein und es wird keinen Block Reward mehr geben können. Deshalb ist ein weiterer Anreiz implementiert.[52]

3.2.3.2 Transaction Fee

Das zweite Element ist die Transaction Fee. Diese gestattet es dem Ersteller einer Transaktion festzulegen, dass beim Empfänger weniger BTC ankommen, als er versendet hat. Die Differenz erhält die Node, die zuerst die Transaktion in ihren Block aufgenommen hat. Derzeit ist die Transaktion Fee freiwillig. Ihr wird mit sinkendem Block Reward aber eine immer höhere Bedeutung zukommen, um die Qualität des Services im Netzwerk zu sichern.[53]

---

[51] Vgl. ebd., S. 38.
[52] Vgl. ebd., S. 39.
[53] Vgl. ebd., S. 40.

3.2.3.3 Mining und Proof of Work

In unseren bisherigen Beispielen sind wir davon ausgegangen, dass die Nodes alle gleich sind und zufällig ausgewählt werden, um einen Block vorschlagen zu dürfen. Dadurch entsteht ein neues Problem, weil eine zufällige Auswahl der Nodes dazu führen würde, dass die Teilnehmer das Netzwerk mit Nodes überfluten, um eine möglichst hohe Chance auf den Block Reward und die Transaction Fee zu haben. Dem wird mit dem System Proof of Work entgegengewirkt. Die Idee dahinter ist, dass die Nodes anteilig nach der zur Verfügung gestellten Rechenkapazität ausgewählt werden, weil angenommen werden kann, dass die Rechenkapazität so weit verteilt ist, dass es nicht möglich ist, mit vertretbarem Aufwand ein Monopol darauf zu erhalten. Proof of Work wird in Bitcoin durch das Lösen von Hash-Puzzles erbracht.[54] Um einen Block vorschlagen zu dürfen, muss die Node zuerst den Zielwert des Puzzles finden, wie in Abschnitt 3.1.1.3 erläutert wurde. Weil es keine Abkürzung beim Finden des Zielwerts gibt, entscheidet automatisch die zur Verfügung stehende Rechenleistung darüber, welche Node die höchste Chance hat, den nächsten Block vorschlagen zu dürfen. Die Nodes befinden sich in einem permanenten Wettrennen untereinander, das Hash-Puzzle des nächsten Blocks als erstes zu lösen. Dadurch ist sichergestellt, dass der Auswahlprozess vollkommen dezentralisiert ist. Der gesamte Prozess wird als *Mining* bezeichnet und die daran teilnehmenden Nodes als *Miner*.[55]

Auch wenn theoretisch jeder am Mining teilnehmen kann, ist der notwendige Rechenaufwand, um ein Hash-Puzzle lösen zu können, inzwischen so hoch, dass sich nur noch Serverfarmen und Mining Gilden daran beteiligen, was zu einer Konzentration an Ressourcen geführt an. Der Zielwertebereich des Hash-Puzzles wird alle 2.016 Blöcke neu angepasst, um den Einfluss von besserer Hardware und eines sich verändernden Mining-Ökosystems eliminieren zu können, so dass immer nur etwa alle 10 min ein neuer Block erstellt werden kann. Das heißt, eine Anpassung findet alle zwei Wochen statt. Der Grund für die gewollte Latenz von 10 min ist die Aufrechterhaltung von Effizienz. Es ist effizienter, viele Transaktionen in einem großen Block zu berechnen und einen Konsens zu finden, als bei vielen kleinen Blöcken mit wenigen Transaktionen. Anderseits darf die Blockgröße auch nicht zu groß gewählt werden, weil Transaktionen dann nicht schnell genug bestätigt werden würden. Für Bitcoin hat sich eine zehnminütige

[54] Vgl. Nakamoto, S. 3.
[55] Vgl. Narayanan, S. 40–45.

Latenz als guter Kompromiss zwischen Effizienz und Geschwindigkeit erwiesen. Bei anderen Kryptowährungen oder der Anwendung als Ledger für Wertpapiertransaktionen, können sich andere Latenzzeiten als besser geeignet erweisen.[56]

Im Wissen um die Funktionsweise der Sicherheitsmerkmale der Blockchain-Technologie von Bitcoin, können wir unsere Annahme, dass sich der Großteil an Nodes ehrlich verhält – in einem Kontext, wo Nodes keine Identität haben – präzisieren. Ehrlichkeit bedeutet lediglich, dass sich die Nodes an das Protokoll halten und die bekannten Angriffsmuster nicht zielführend sind, solange sich der Großteil der Miner an das Protokoll hält. Die Miner sind dabei nach ihrer zur Verfügung gestellten Rechenleistung gewichtet, die auch als Hash Power bezeichnet wird. Solange über 50% Hash Power von ehrlichen Minern kontrolliert wird, werden betrügerische Transaktionen nicht in den Langzeitkonsens der Blockchain finden. Für den einzelnen Miner lässt sich mit einer einfachen Formel leicht berechnen, wie lange er im Durchschnitt benötigen wird, um einen Block zu finden:

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

Kontrolliert ein Miner also 0,1% der gesamten Hash Power des Netzwerks, so wird er alle 10.000 Minuten einen Block finden, was etwa einer Woche entspricht.[57]

Die letzte wichtige Eigenschaft des Proof of Work-Systems ist, dass einmal gefundene Blöcke trivial von anderen Nodes verifizierbar sind. Findet eine Node einen neuen Block, dann veröffentlicht sie im Netzwerk zusammen mit diesem die Lösung des Hash-Puzzles (Nonce). Der neue Block kann dann unmittelbar von anderen Minern verifiziert werden.[58]

3.2.4 Zusammenfassung der Merkmale

Wir haben jetzt eine gute Vorstellung davon entwickelt, wie die Blockchain dezentralisiert wird. Echte Identitäten werden nicht benötigt, um am Netzwerk teilnehmen zu können und jeder Teilnehmer kann beliebig viele Pseudonyme erstellen. Transaktionen sind im Grunde genommen Nachrichten, die im Peer-to-Peer-Netzwerk verbreitet werden und Anweisungen enthalten, Bitcoins von einer Adresse an eine andere zu senden.

[56] Vgl. ebd.
[57] Vgl. ebd.
[58] Vgl. ebd.

Die Sicherheit wird ausschließlich durch die Blockchain und das Protokoll zur Findung des Langzeitkonsens erzielt. Spricht man davon, dass eine Transaktion in der Blockchain aufgenommen wurde, heißt das, dass die Transaktion von ausreichend vielen Nodes bestätigt wurde. Es gibt keine fest vorgegebene Anzahl an Bestätigungen, die notwendig sind, dass die Transaktion Teil des Langzeitkonsens wird. Je häufiger die Transaktion bestätigt wird, umso sicherer kann sich der Empfänger sein, dass die Transaktion dauerhaft Teil der Blockchain bleiben wird und nicht mehr rückgängig gemacht werden kann. Blöcke, die nicht Teil des Langzeitkonsens werden, verwaisen. Diese *Orphan Blocks* können Ursache von ungültigen Transaktionen, Double-Spend Attacks oder Netzwerklatenz sein.[59]

Darüber hinaus haben wir Mining und Hash-Puzzles genauer betrachtet. Miner sind spezialisierte Nodes, die im Rennen, als erstes einen neuen Block zu finden, gegeneinander antreten ein Hash-Puzzle zu lösen. Dafür werden sie mit einem Block Reward belohnt und dürfen eine Transaktion Fee einstreichen, sofern diese von den Netzwerkteilnehmern gewährt wird. In der weiteren Entwicklung von Bitcoin ist es denkbar, dass die Transaktion Fee mit sinkendem Block Reward obligatorisch wird. Die Wahrscheinlichkeit, das Hash-Puzzle eines neuen Blocks als Erster zu lösen, ist prozentual zur gesamten Hash Power des Peer-to-Peer-Netzwerks verteilt. Hat Alice 100 Mal so viel Hash Power wie Bob, dann heißt das nicht, dass Alice immer gewinnen wird, sondern dass Bob im Durchschnitt nur 1% so viele Blöcke finden wird wie Alice. Das Konzept des verteilten Konsens zieht sich durch die gesamte Bitcoin Architektur. Bei traditionellen Währungen kommt es hauptsächlich beim Ermitteln des Wechselkurses zu einem Konsens. Das trifft natürlich auch auf Kryptowährungen zu. Darüber hinaus wird in Bitcoin aber auch der aktuelle Stand des Ledgers im Konsens bestimmt, was über die Blockchain realisiert wird. Das bedeutet, dass auch die Buchführung darüber, wer wie viele Bitcoins besitzt, im Konsens bestimmt wird. Der Besitz von Bitcoins ist nichts weiter, als der Konsens zwischen Nodes, dass einem bestimmten Nutzer die entsprechenden Bitcoins gehören.[60]

[59] Vgl. ebd., S. 45–47.

[60] Vgl. Joerg Platzer, *Bitcoin - Kurz & Gut* (Beijing: O'Reilly, 2014), S. 23–25.

3.2.5 Bootstrapping

Das Zusammenspiel der Merkmale führt zu einer Eigenschaft, die sich Bootstrapping nennt und in gewisser Weise das Henne-Ei-Problem beschreibt. Die Sicherheit der Blockchain, die Gesundheit des Mining-Ökosystems und der Wert von Bitcoin im Austausch mit traditionellen Währungen, stehen in gegenseitiger Abhängigkeit zueinander. Damit die Blockchain sicher ist, darf es einem Angreifer nicht möglich sein, das Konsens-Protokoll zu überlisten. Das wiederum erfordert, dass er nicht in der Lage sein darf, über 50% der Hash Power im Netzwerk zu kontrollieren. Dazu bedarf es eines gesunden Mining Ökosystems, in dem der Großteil der Nodes das Protokoll befolgt. Der wichtigste Anreiz für die Miner ist finanzieller Natur. Mining ist umso attraktiver, desto besser der Wechselkurs von Bitcoin zu US-Dollar oder Euro ist. Das liegt daran, dass Block Reward und Transaction Fee in BTC gewährt werden, wohingegen die Ausgaben für Mining Hardware und Elektrizität in herkömmlichen Währungen beglichen werden müssen.[61]

Es stellt sich die naheliegende Frage, wie ein stabiler Wechselkurs sichergestellt werden kann. Die Antwort darauf ist ebenso einfach wie vage: Die Benutzer von Bitcoin müssen in die Sicherheit der Blockchain vertrauen. Sollte nur geringes Vertrauen in die Technologie existieren, hätte die Währung nicht viel Wert. Als Bitcoin erstmalig eingeführt wurde, hat die Kryptowährung keines der Merkmale erfüllt. Es gab keine Miner, außer den Entwicklern selbst, die Währung hatte keinen Wert, weil sie gänzlich neu und unbekannt war und die Blockchain war unsicher, weil die Hash Power zu konzentriert war und man den Konsens leicht hätte manipulieren können. Es gibt keine konkrete Erklärung, wie Bitcoin es geschafft hat, im Laufe kurzer Zeit alle drei Kriterien zu erfüllen. Ein Grund ist die hohe Medienpräsenz, die Bitcoin als erste Kryptowährung der Welt erfahren hat. Je mehr Leute von Bitcoin hören, desto mehr Leute interessieren sich für Mining. Je mehr Leute sich mit Mining beschäftigen, desto mehr Vertrauen erfährt die Blockchain und umso stabiler wird die Währung.[62]

[61] Vgl. Narayanan, S. 47f.
[62] Vgl. ebd.

3.3 Ablauf einer Transaktion

Zum Abschluss des Kapitels zur Funktionsweise der Blockchain-Technologie, wollen wir zusammenfassen, in welchen Schritten eine Transaktion auf einem Distributed Ledger abläuft.

3.3.1 Initialisierung

Angenommen Alice möchte eine Transaktion durchführen und einen BTC an Bob senden. Dafür benötigen Alice und Bob Adressen in Form eines Public Keys, die wir *pk(Alice)* und *pk(Bob)* nennen. Dann sendet Alice eine Nachricht an das Peer-to-Peer-Netzwerk in der Form *pk(Alice) sendet an pk(Bob) die Transaktionsmenge von einem BTC*. Die Nachricht unterschreibt sie mit ihrem Secret Key, so dass jeder verifizieren kann, dass die Transaktionsanweisung von ihr stammt und nicht manipuliert wurde. Auch kann Alice nach dem Signieren der Nachricht nicht mehr abstreiten, dass sie die Verfasserin ist.

3.3.2 Verifizierung

Bevor die Transaktion ausgeführt wird, muss das Netzwerk folgende Aspekte überprüfen:

- Ist Alice der Sender der Transaktion?
- Hat Alice ausreichend Bitcoins, um die Transaktion ausführen zu können?

Die digitale Signatur garantiert, dass nur der Besitzer des dazugehörigen Secret Keys die Nachricht unterschrieben haben kann und weil die Transaktionen sequentiell abgearbeitet werden, wäre auch der Versuch einer Double-Spend Attack nicht erfolgreich.

3.3.3 Ausführung

Ist die initiale Verifikation erfolgreich, befinden sich die Nodes im Wettlauf, die Transaktion als erstes in einem neuen Block speichern zu können. Dazu gruppiert jede Node die offenen Transaktionen, von denen sie seit dem letzten Update der Blockchain gehört hat, in einem neuen Block. Ist der Block voll, beginnt der Wettlauf, als erstes das Hash-Puzzle zu lösen. Sobald der Gewinner feststeht, erhält dieser den Block Reward als Belohnung und die Transaktion wird mit dem neuen Block in der Blockchain gespeichert.

Das Peer-to-Peer-Netzwerk garantiert dabei, dass die Verifikation der Transaktion früher oder später von allen Nodes im Netzwerk vorgenommen wird, sobald diese den Block mit der Transaktion im Langzeitkonsens der Blockchain aufgenommen haben. Möchte Bob sich sicher sein, dass die Transaktion von Alice an ihn Bestand hat, dann wartet er mindestens sechs Bestätigungen des neuen Blocks ab.

4 Auswirkungen auf den Wertpapierhandel

Nachdem wir die technischen Grundlagen der Blockchain-Technologie kennengelernt haben und verstehen, wie die Elemente Kryptografie und Dezentralisierung zum Einsatz kommen, können wir nun analysieren, wie eine Anwendung der Blockchain-Technologie im Wertpapierhandel aussehen könnte. Dabei sollen im Rahmen einer SWOT-Analyse die Chancen und Risiken vorgestellt werden, die mit einer Einführung verbunden sind. Um die Auswirkungen auf den Wertpapierhandel besser verstehen zu können, wollen wir zunächst einmal betrachten, wie der Lebenszyklus eines Wertpapiers aussieht (Abbildung 12).

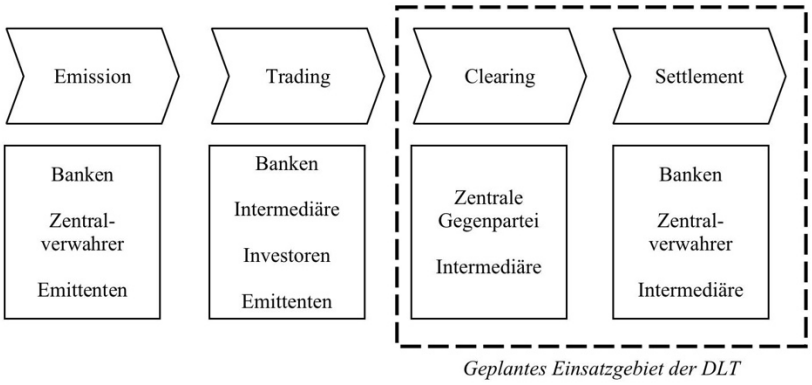

Abbildung 12: Lebenszyklus im Wertpapierhandel[63]

Am Anfang steht die Emission des Wertpapiers. Das kann zum Beispiel die Ausgabe von Aktien beim Börsengang eines Unternehmens sein. Das emittierte Wertpapier ist dann über eine Depotbank – an den Börsen an denen es notiert ist oder außerbörslich – handelbar. Nach dem Kauf fällt das Clearing an. Dabei tritt eine Clearingstelle als Gegenpartei zwischen Käufer und Verkäufer auf und stellt gegenseitige Forderungen und Verbindlichkeiten fest. Als Teil des Clearings werden diese gegebenenfalls noch beim Netting miteinander verrechnet, um Transaktionsgebühren und Sicherheitszahlungen zu reduzieren. Sinn und Zweck des Clearings ist es, einen Liefer- oder Zahlungsausfall zwischen den Handelspartnern zu verhindern. In Europa gibt es mit *Clearstream* in Luxemburg und *Euroclear* in Brüssel zwei große Clearingstellen. Das Clearing ist gleich-

[63] Eigene Darstellung in Anlehnung an ECB, *Distributed Ledger Technology* (Frankfurt: European Central Bank, 2016), S. 2. https://www.ecb.europa.eu/paym/pdf/infocus/20160422_infocus_dlt.pdf.

zeitig die Vorbereitung für das Settlement. Beim Settlement liefert der Verkäufer das Wertpapier an den Käufer und dieser bezahlt diesen dafür. Der Warenaustausch ist erfolgt und die Transaktion wurde erfolgreich abgeschlossen. Zwischen dem Tag des Handelsabschlusses und dem Tag der Geschäftserfüllung, dürfen bei Kassageschäften nicht mehr als zwei Tage liegen. In diesen zwei Tagen besteht die Gefahr eines Leistungsausfalls, indem beispielsweise der Verkäufer das Wertpapier zwar sofort ausliefert, der Käufer seiner Zahlungspflicht aber nicht nachkommt. Genau dieses Risiko sollen Clearingstellen als Intermediär verhindern. Für diesen Service werden natürlich zusätzliche Gebühren fällig und Sicherheitseinlagen notwendig. Eine technische Alternative dazu soll mit der DLT entwickelt werden. In einem Arbeitspapier hat die Europäische Wertpapier- und Marktaufsichtsbehörde *ESMA* untersuchen lassen, welche möglichen Auswirkungen die DLT auf den Wertpapierhandel haben könnte. Die Ergebnisse sind nachfolgend in einer SWOT-Analyse zusammengefasst.

4.1 Stärken und Chancen

4.1.1 Clearing und Settlement

Die DLT hat das Potenzial, die Bearbeitungszeit des Clearing- und Settlement-Prozesses deutlich zu verkürzen, in dem auf Intermediäre weitestgehend verzichtet werden kann. Weil es nur noch einen zentralen Ledger gibt, auf den alle Parteien zugreifen können und Transaktionen im verteilten Konsens bestätigt werden, wird es kaum noch sich widersprechende Informationen und Buchungen geben. Derzeit fließt ein nicht unerheblicher Teil der Arbeit in den sogenannten Reconciliation-Prozess. Dabei wird überprüft, ob die eingegangene Buchungsanweisung mit der vorgenommenen Buchung auf dem Konto des Kunden übereinstimmt. Es wird angenommen, dass Clearing und Settlement sogar zu einem Schritt verschmelzen und dann nahezu sofort ausgeführt werden können. Das würde, neben der verkürzten Bearbeitungszeit von Transaktionen, zudem das Counterparty Risk reduzieren, wodurch auch weniger Sicherheiten hinterlegt werden müssten. Das Counterparty Risk bezeichnet das Risiko bei einer Transaktion, dass der Geschäftspartner die getroffenen Vereinbarungen nicht erfüllt.[64]

[64] Vgl. ESMA, S. 10.

4.1.2 Depotführung und Smart Contracts

Einen weiteren Vorteil der DLT verspricht man sich in der vereinfachten Übertragung von Wertpapieren und einer erleichterten Depotführung. Zur Diskussion steht die Implementierung einer Referenzdatenbank, die jedes Wertpapier eindeutig identifiziert. Zwar gibt es bereits Standards wie die ISIN, allerdings wird diese nicht über alle Anlageklassen gleichermaßen verwendet und sie ist nicht ausreichend, um alle Wertpapiere eindeutig identifizierbar zu machen. So gibt es eine Vielzahl länder- und börsenspezifischer Kennnummern, die je nach Wertpapier Verwendung finden.[65]

Durch die rein digitale Transaktionsabwicklung auf einem Distributed Ledger, ließen sich auch digitale Wertpapiere erstellen und nutzen, was so bisher noch nicht möglich ist. Die sogenannten Smart Contracts sind intelligente Wertpapiere, bei denen die Vertragsbedingungen im Kontrakt selbst gespeichert werden. Ein Algorithmus überprüft dann permanent, ob vorher definierte Vertragsbedingungen eingetreten sind. Ist das der Fall, kann das Wertpapier automatisch entsprechende Instruktionen ausführen. Das kann zum Beispiel die Coupon-Zahlung einer Anleihe zu einem Fälligkeitsdatum sein. Der Smart Contract würde in dem Fall ohne manuelles Zutun eine Coupon-Zahlung an den Halter der Anleihe vornehmen.[66] Ein weiterer Vorteil digitaler Wertpapiere ist die Tatsache, dass der Besitzwechsel genau dokumentiert wird. Jedes einzelne Wertpapier ließe sich ab seiner Emission in seiner Transaktionshistorie im Distributed Ledger präzise nachverfolgen.[67]

4.1.3 Reporting

Spätestens seit der Finanzkrise im Jahr 2008 kommt dem Reporting, Risikomanagement und der Überwachung von Wertpapiergeschäften eine außerordentlich wichtige Bedeutung zu. Durch die Bündelung aller Transaktionen auf einem Ledger, erleichtert es die DLT sowohl den Regulierungsbehörden, als auch bankinternen Abteilungen, an Informationen zu kommen.[68]

---

[65] Vgl. ebd., S. 10f.

[66] Vgl. Andrea Pinna; Ruttenberg, Wiebe, *Distributed Ledger Technologies in Securities Post-Trading: Revolution or Evolution?* (Frankfurt: European Central Bank, 2016), S. 18. https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf.

[67] Vgl. ESMA, S. 10f.

[68] Vgl. ebd., S. 11.

So möchte die NASDAQ in ihren Distributed Ledger unterschiedliche Berechtigungsstufen und Leserechte einbauen, so dass alle Informationen einer Transaktion nur für die Parteien sichtbar sind, die darin direkt oder indirekt involviert sind. So könnte der Marktaufsicht voller Lesezugriff auf die Daten aller Transaktionen eingeräumt werden. Für alle weiteren Teilnehmer wären hingegen nur Basisinformationen wie der Ausführungspreis oder die Zeit der Orderausführung sichtbar. So erhofft man sich dem Missbrauch von vertraulichen Informationen vorbeugen zu können.[69]

4.1.4 Counterparty Risk

Durch die bereits angesprochene Verkürzung des Clearing- und Settlement-Prozesses, wären die Handelspartner untereinander einem deutlich verkürzten Counterparty Risk ausgesetzt. Viele Transaktionen könnten sofort abgeschlossen werden, was eine Clearingstelle als Intermediär überflüssig machen würde. Bisher ist es die klassische Aufgabe der Clearingstelle, das Counterparty Risk zu eliminieren. Sie führt Käufer und Verkäufer zusammen und übernimmt das Risiko eines Liefer- oder Zahlungsausfalls der Transaktionspartner. Für Termingeschäfte mit Zahlungs- und Liefertermin in der Zukunft wie Optionen und Futures, wäre aber nach wie vor eine Clearingstelle notwendig, weil das Counterparty Risk über die gesamte Laufzeit des Finanzinstruments aufrechterhalten bleibt. Das Geschäft kann und soll gar nicht sofort nach Erwerb des Terminkontrakts abgeschlossen werden.[70]

4.1.5 Verfügbarkeit und Sicherheit

Zwei sehr offensichtliche Vorteile der DLT sind die Verbesserung der Verfügbarkeit und Sicherheit der Kontoführung. Zu Beginn der Bachelorarbeit haben wir ausführlich die Sicherheitsmerkmale der Blockchain-Technologie besprochen. Durch die Verteilung des Ledgers auf alle teilnehmenden Finanzdienstleister und Behörden, gäbe es keinen zentralen Angriffspunkt mehr für einen Angreifer. Selbst wenn die Node einer Bank ausfallen würde, könnten die Kunden der Bank weiterhin ihre Geschäfte abwickeln, weil digitale Signaturen und der verteilte Konsens die Transaktionen verifizieren wür-

[69] Vgl. Anna Irrera, *Nasdaq: Our Plans with the Blockchain* (London: Financial News, 2015). http://www.efinancialnews.com/story/2015-08-20/nasdaq-our-plans-for-the-blockchain-fredrik-voss.

[70] Vgl. ESMA, S. 11f.

den. Dadurch könnten auch kostspielige Notfallpläne für Serverausfälle einfacher und kostengünstiger ausfallen.[71]

Ein weiterer Vorteil wäre ein rund um die Uhr möglicher Handel an sieben Tagen der Woche, weil kein zentraler Betreiber mehr notwendig ist. Das würde die Globalisierung der Finanzmärkte noch weiter vorantreiben.[72]

4.1.6 Kosteneinsparungen

Der vielleicht wichtigste Faktor bei der Begeisterung um die DLT sind schlichtergreifend Kosteneinsparungen. Die dem Handel nachgelagerten Prozesse wie Clearing, Settlement und Reporting können in vielen Punkten gebündelt und automatisiert werden. Durch die Nutzung eines Distributed Ledgers, ließe sich die Kontoführung firmeneigener Ledger eliminieren und kostspielige Notfallpläne bei Serverausfällen würden obsolet werden. Nicht zuletzt verspricht der Wegfall von Intermediären am Spotmarkt günstigere Transaktionskosten für die Kunden.[73] Stattet man den Distributed Ledger mit unterschiedlichen Leserechten aus, könnten Finanzdienstleister und Regulierungsbehörden, trotz unterschiedlicher Anforderungen, alle für sie relevanten Informationen von einer einzigen Datenbank beziehen.[74]

4.2 Schwächen und Risiken

Die Einführung der DLT würde für die Finanzmärkte mit fundamentalen Änderungen von lange etablierten Prozessen einhergehen und ist damit mit nicht zu unterschätzenden Herausforderungen für die Akteure verbunden. Dabei sind die Risiken nicht unbedingt größer, als bei der momentanen, zentralen Marktstruktur. Durch die Dezentralisierung und veränderte Transaktionsabwicklung muss vielmehr den sich veränderten Charakteristika korrekt begegnet werden.

4.2.1 Technische Hürden

Aktuell gibt es kein System an den Finanzmärkten, das die DLT bereits im großen Stil einsetzt. Auch wenn Bitcoin für Kryptowährungen beweist, dass die Technologie mas-

[71] Vgl. ebd., S. 12.
[72] Vgl. ECB, S. 5.
[73] Vgl. ESMA, S. 12.
[74] Vgl. Irrera.

sentauglich ist, herrscht noch viel Unsicherheit. Nach einer Studie von IBM gibt es vor allem Bedenken, dass sich der Erfolg einer Kryptowährung nicht direkt auf den Wertpapierhandel, mit seinen zahllosen unterschiedlichen Akteuren und Anforderungen, übertragen lässt.[75] Auch stellt sich die Frage, wie die DLT mit bestehenden Systemen zusammenarbeiten würde. Natürlich ist es unrealistisch, dass die Technologie simultan über alle Märkte und Prozesse eingeführt wird, weshalb es eine Übergangsphase geben wird, in der das bestehende System mit dem Distributed Ledger reibungslos kommunizieren können muss. Wie gut das funktionieren wird, hängt vor allem von den einzelnen Akteuren ab. Jeder wird ein individuelles Interface programmieren müssen, das den Distributed Ledger an das eigene, proprietäre System koppelt. Würden viele Marktteilnehmer eine abwartende Haltung einnehmen und die Entwicklung der Technologie nur beobachten anstatt sie direkt zu implementieren, dann könnten sich viele der Vorteile nicht richtig entfalten.[76]

Um alle Stärken ausspielen zu können, müssen die Transaktionen auf dem Distributed Ledger in einer Zentralbankwährung wie Euro oder US-Dollar gespeichert werden. Sollte stattdessen für die Wertpapierabrechnung eine eigene Kryptowährung entwickelt werden, müsste zusätzlich eine Schnittstelle zur Verrechnung zwischen der Kryptowährung und Zentralbankwährung implementiert werden.[77]

Bei Bitcoin sind einmal im Langzeitkonsens der Blockchain vorhandene Transaktionen irreversibel. Wertpapiertransaktionen haben aber wesentlich mehr Parameter und Fehlerquellen, als die Transaktion einer Kryptowährung, deren wichtigste Information lediglich aus Empfänger und Geldmenge besteht. Auch können Smart Contracts fehlerhaft programmiert worden sein und ungewollte Transaktionen ausführen. Das ist insbesondere wegen der deutlichen Beschleunigung von Clearing und Settlement entscheidend, weil es durch die sofortige Handelsabwicklung kein Zeitfenster für manuelle Korrekturen mehr gibt. Das wirft die Frage auf, wie mögliche Fehler korrigiert werden können.[78] Allerdings gibt es bereits mit dem Enigma-Projekt des MIT[79] eine Blockchain, die

[75] Vgl. IBM, *Banking on Blockchain: Charting the Progress of Distributed Ledger Technology in Financial Services* (London: Finextra, 2016), S. 7. https://www.ingwb.com/media/1609652/banking-on-blockchain.pdf.

[76] Vgl. ESMA, S. 14f.

[77] Vgl. ebd.

[78] Vgl. ebd.

[79] Mehr zum Enigma-Projekt: http://enigma.media.mit.edu/

es erlaubt, Datensätze im Nachhinein zu korrigieren und Sichtbarkeitseinstellungen zum Datenschutz leicht vorzunehmen zu können.[80]

Zuletzt bietet die DLT derzeit noch keine technische Möglichkeit, Positionen aus Derivategeschäften zu netten, Leerverkäufe zu tätigen oder mit Fremdkapital zu handeln. Beim Netting werden die offenen Positionen der Vertragspartner gegeneinander verrechnet, um Risiken zu minimieren und Gebühren zu sparen. Kauft beispielsweise ein Kunde 100 DAX-Futures und verkauft davon vor Fälligkeit wieder 40 Stück, dann werden die beiden Positionen von der Clearingstelle genettet und der Kunde hat nur noch eine offene Position über 60 DAX-Futures. Dadurch muss er auch nur für eine Position Gebühren bezahlen. Durch die sofortige Transaktionsabwicklung bei der DLT, wäre die erste Gebühr direkt beim Kauf der 100 Futures fällig und die zweite Gebühr beim Verkauf. Im Gegensatz zu Kassageschäften ist es bei Termingeschäften unerwünscht und unsinnig, dass Transaktionen sofort abgewickelt werden.[81]

Auch Leerverkäufe lassen sich nicht technisch reflektieren. Die Idee von Leerverkäufen ist, dass man Wertpapiere verkauft, die man selbst nicht besitzt, sondern sich nur geliehen hat. Damit sind Spekulationen auf sinkende Kurse möglich. Weil bei der DLT vor einem Verkauf aber überprüft wird, ob man das entsprechende Instrument überhaupt besitzt, ist ein Leerverkauf technisch ausgeschlossen. Das gleiche gilt für fremdkapitalfinanzierte Wertpapiergeschäfte, die es ermöglichen, überproportional an Kursschwankungen zu partizipieren und Gewinne zu hebeln. Durch die vorherige Überprüfung des Ledgers ist es unmöglich, Transaktionen mit geliehenem Kapital zu tätigen, weil man nur Kapital investieren kann, das man selbst besitzt.[82]

Ungeeignet erscheint die Technologie derzeit auch für die Live-Aufzeichnung von Quotes. Dabei handelt es sich um verbindlich gestellte Kurse an den Börsen, von denen Millionen pro Sekunde quotiert werden. Die Geschwindigkeitsanforderungen und das Volumen wären zu hoch.[83]

---

[80] Vgl. Gareth W. Peters; Panayi, Efstathios, *Understanding Modern Banking Ledgers through Blockchain Technologies* (London: University College London, 2015), S. 17f. http://www.digibib.net/permalink/832/EDS/edsbas:edsbas.ftarxivpreprints.oai.arXiv.org.1511.05740.

[81] Vgl. ESMA, S. 14f.

[82] Vgl. ebd.

[83] Vgl. Irrera.

4.2.2 Datenschutzbedenken

Bei der Beschreibung der Bitcoin Blockchain haben wir gelernt, dass sich jeder an dem Peer-to-Peer-Netzwerk beteiligen kann. Die Beteiligung vieler Nutzer ist sogar die Grundvoraussetzung, dass die Blockchain sicher und effizient funktioniert und die Währung stabil bleibt. Das heißt aber auch, dass jeder den Distributed Ledger vollständig auslesen kann. Ein genehmigungsfreier Distributed Ledger ist im Wertpapierhandel hingegen aus datenschutzrechtlichen Gründen undenkbar. Das System wäre genehmigungspflichtig und auf autorisierte Teilnehmer beschränkt, deren Identität bekannt ist. Das ist ein fundamentaler Unterschied zu dem Konsens ohne Identität von Bitcoin, den wir in Kapitel 3.2.2 kennengelernt haben.[84] Das bedeutet, dass ein Regelwerk geschaffen werden muss, das festlegt, welche Anforderungen an einen autorisierten Teilnehmer gestellt werden. Das können zum Beispiel ein erforderliches Mindestkapital, die Einhaltung von Risikomanagementprozessen und Regeln zur Führung von Geschäften sein. Die Herausforderung wird darin bestehen, eine Balance in den Aufnahmekriterien herzustellen, die einerseits eine Beteiligung am Distributed Ledger nicht zu schwierig gestaltet, anderseits das System aber nicht zu komplex werden lässt. Auch müssen Zuständigkeiten geklärt, Verhaltensregeln aufgestellt und Sanktionsmaßnahmen für den Fall definiert werden, dass sich autorisierte Teilnehmer regelwidrig verhalten.[85]

4.2.3 Regulatorische Hürden

Als größte Hürde auf dem Weg zur Einführung der DLT könnten sich regulatorische und juristische Anforderungen erweisen. Der Wertpapierhandel wird von zahllosen nationalen und internationalen Gesetzen reguliert, die alle unterschiedlich liberal oder restriktiv formuliert sind. Momentan herrschen zentral organisierte Marktstrukturen. Ein Distributed Ledger würde diese dezentralisieren und die Nodes des Peer-to-Peer-Netzwerks würden sich in vielen Ländern mit unterschiedlicher Rechtsprechung befinden, so dass eine gemeinsame Linie in Themen wie Datenschutz gefunden werden muss.[86]

---

[84] Vgl. GOS, *Distributed Ledger Technology: Beyond Blockchain* (London: UK Government Office for Science, 2016), S. 10. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[85] Vgl. ESMA, S. 15f.

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

4.2.4 Akzeptanz

Die DLT verspricht sehr überzeugende Vorteile, die damit einhergehend aber eine ganze Reihe von Intermediären wie Clearingstellen überflüssig machen würde. Insbesondere die betroffenen Dienstleister könnten vehement Widerstand gegen die Technologie leisten. Daher wird der richtigen Einführungsstrategie und Sensibilisierung gegenüber der Technologie eine wichtige Rolle zukommen. Um eine so radikale Änderung einführen zu können, muss die Finanzwelt davon überzeugt werden, dass die neue Welt besser ist, als die Alte. Das funktioniert nur, in dem man die versprochenen Vorteile an lauffähigen Prototypen demonstrieren kann. Dabei müssen die Marktteilnehmer auch gezeigt bekommen, wie der Wechsel von der alten Welt in die Neue aussehen wird. Die Zeit, in der beide Welten parallel laufen, sollte auf ein notwendiges Minimum reduziert werden können, um redundante IT-Systeme und hohe Ausgaben zu vermeiden.[87]

4.2.5 IT-Sicherheit

Durch die Verteilung des Ledgers auf viele Nodes, gibt es keinen zentralen Angriffspunkt mehr für Hacker. Sollte aber wider Erwarten doch noch ein Fehler in der Blockchain-Technologie entdeckt werden oder das kryptografische Verfahren geknackt werden, hätte ein Angreifer nicht nur Zugriff auf die Daten der gehackten Node, sondern potenziell auf die Daten aller Teilnehmer. Zudem steigt die Gefahr eines Hackerangriffs, weil die DLT nicht nur im Wertpapierhandel und für Kryptowährungen interessant ist, sondern auch in vielen anderen Bereichen wie zum Beispiel zur Autovermietung als Teil einer Sharing Economy diskutiert wird und zum Einsatz kommen könnte. Mit zunehmender Verbreitung steigt die Gefahr, dass Sicherheitslücken der Technologie entdeckt und ausgenutzt werden können.[88]

In Kapitel 3.1.4 haben wir das Konzept von Public Keys eingeführt. Sollte ein Kunde sein Schlüsselpaar verlieren, hat er keine Chance mehr an sein Kapital zu kommen und es wäre unwiederbringlich verloren. Auch bei Diebstahl der digitalen Signatur durch einen Angreifer wären getätigte Transaktionen irreversibel, wenn es kein verlässliches Regelwerk für Missbrauchs- und Verlustszenarien gibt.[89]

---

[87] Vgl. Irrera.
[88] Vgl. ESMA, S. 17.
[89] Vgl. ebd.

Zuletzt erleichtert die Verwendung von Schlüsselpaaren als Pseudonym, statt wie bisher echter Kundennamen, die Verschleierung von Geldwäsche und Terrorismus-Finanzierung.[90]

4.2.6 Operationelle Risiken

Als vielversprechender Vorteil der DLT gilt die weitgehende Automatisierung von Clearing und Settlement, was menschliche Fehler reduziert. Sollte es jedoch eine Anomalie im Distributed Ledger geben, so wären die Konsequenzen äußerst weitrechend und würden alle Marktteilnehmer betreffen, die das System nutzen. Das gleiche gilt für Smart Contracts, die einen hohen Grad an Automatisierung versprechen. Wird aber kein ausreichendes Kontrollsystem etabliert, könnten fehlerhaft programmierte Algorithmen zusätzliche Risiken schaffen. Das operationelle Risiko der DLT lässt sich so zusammenfassen, dass durch die Automatisierung die Anzahl der Fehler sinken wird, ihre Auswirkungen potenziell aber weiterreichender sein werden.[91]

4.2.7 Marktvolatilität

Die unter den Marktteilnehmern angepassten Prozesse und der hohe Grad an Automatisierung, können ein Herdenverhalten begünstigen und die Volatilität am Markt erhöhen. Insbesondere steht eine beschleunigte Verbreitung von Schocks durch die sofortige Handelsabwicklung zu befürchten. Noch nicht ausreichend erforscht ist zudem, ob derzeit stark regulierte und deshalb unattraktive Marktsegmente mit Einführung der DLT und einer damit einhergehenden erleichterten Handelsabwicklung, einen Boom erleben könnten. Das könnte bedeuten, dass neue Risikopositionen unkontrolliert aufgebaut werden können, welche die Marktschwankung erhöhen würden.[92]

4.2.8 Ungleicher Wettbewerb

Als letztes Risiko wird die Sorge betrachtet, dass es nach Einführung der DLT zu Wettbewerbsverzerrung kommen könnte. Die am Distributed Ledger beteiligten Akteure könnten neue Interessenten daran hintern, sich mit einer eigenen Node zu beteiligen oder die Konditionen so formulieren, dass eine Beteiligung wirtschaftlich nicht mehr

[90] Vgl. ebd.
[91] Vgl. ebd., S. 18.
[92] Vgl. ebd.

lukrativ ist. Das würde zu einer Monopolbildung führen und könnte die Märkte destabilisieren. Auch wird befürchtet, dass sich manche Teilnehmer am Distributed Ledger nicht an aufgestellte Nutzungsrichtlinien halten und Informationen zu ihrem Vorteil ausnutzen. Da die Trades aller Marktteilnehmer im Distributed Ledger gespeichert sind, ließen sich die Depots und Handelsstrategien der Konkurrenz eventuell rekonstruieren. Mit diesen Informationen wäre es möglich, die Märkte zu manipulieren und Front Running zu betreiben.[93]

[93] Vgl. ebd.

5 Fazit und Ausblick

Als eine der bedeutendsten Börsen der Welt, entwickelt auch die NASDAQ intensiv Konzepte zur Einführung der DLT. Aktuell werden Prototypen entwickelt, um den Beweis erbringen zu können, dass der Distributed Ledger ausgereift und bereit für eine schrittweise Einführung auf den Finanzmärkten ist. Die NASDAQ sieht in der DLT gleich zwei Chancen auf einmal: Zum einen verspricht man sich eine Verbesserung des eigenen Clearings und Settlements, zum anderen hofft man – als weltgrößter Anbieter von Börsentechnologie und Dienstleistungen – den selbstentwickelten Distributed Ledger auch an andere Börsen und Banken verkaufen zu können.[94]

5.1 Szenarien

Nach eingängiger Analyse der DLT durch die Europäische Zentralbank, wurden drei Szenarien entwickelt, wie die Zukunft des Wertpapierhandels aussehen könnte:

1. Fragmentierung: Die etablierten Institutionen nutzen die neue Technologie, um interne Prozesse zu verbessern, aber die bankübergreifende Einführung eines Distributed Ledgers bleibt aus. Weil viele Akteure auf Eigenlösungen setzen und der europäische Clearing- und Settlementmarkt unverändert bleibt, koexistieren mehr Systeme als bisher, was zu Fragmentierung führt (Abbildung 13). Da die DLT viele ihrer Stärken erst im Verbund der Teilnehmer ausspielen kann, handelt es sich hierbei um eine Art Worst-Case-Szenario.[95]

[94] Vgl. Irrera.
[95] Vgl. ECB, S. 6.

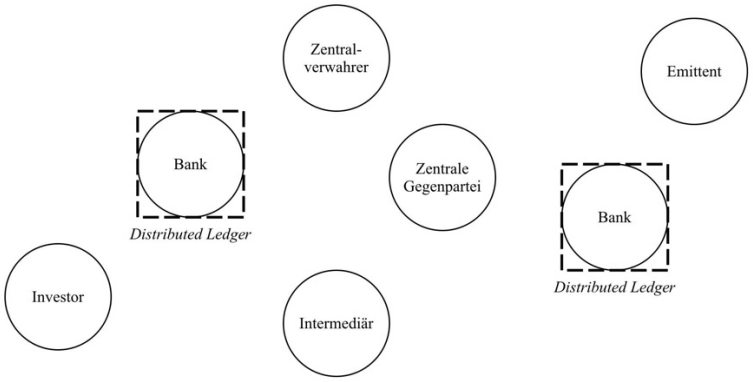

Abbildung 13: Fragmentierung der DLT[96]

2. Adaptierung: Zentrale Institutionen des Wertpapierhandels wie Zentralverwahrer und Zentrale Gegenparteien einigen sich auf einen gemeinsamen Standard und implementieren einen marktweiten Distributed Ledger, dem sich die Banken anschließen. In Folge dessen werden einige Intermediäre redundant. In diesem Szenario könnten Services wie Clearing, Settlement und Depotführung über einen Distributed Ledger abgewickelt werden. Auch das Reporting an die Regulierungsbehörden könnte ohne zusätzliche Kosten und in Echtzeit erfolgen und der Einsatz von Smart Contracts ist denkbar (Abbildung 14). Allerdings könnte eine neutrale Partei notwendig sein, um die Einführung eines industrieweiten Standards zu leiten, da redundante Intermediäre das Projekt blockieren könnten.[97]

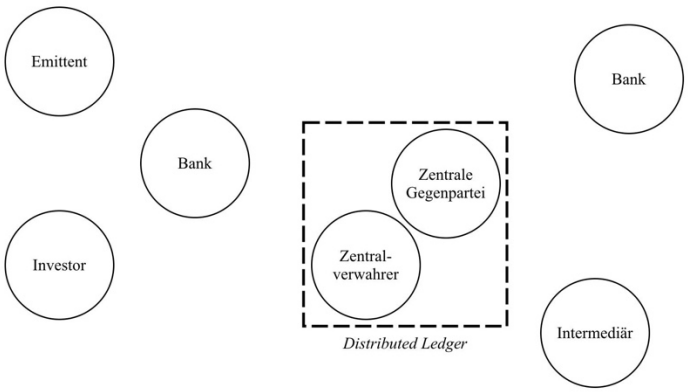

Abbildung 14: Adaptierung eines Standards[98]

[96] Eigene Darstellung in Anlehnung an ebd.
[97] Vgl. ebd., S. 6f.
[98] Eigene Darstellung in Anlehnung an ebd., S. 7.

3. Neue Welt: Emittenten, Investoren und FinTech-Unternehmen umgehen die etablierten Finanzinstitutionen und Schaffen von Grund auf ein neues Peer-to-Peer-System für Wertpapiertransaktionen. Smart Contracts und eine vollautomatisierte Handelsabwicklung spielen in diesem Extrem-Szenario eine besonders wichtige Rolle (Abbildung 15). Rein technisch betrachtet sind hier die Parallelen zu Bitcoin am ähnlichsten. Gleichzeitig stellt sich die identische Frage wie aktuell bei Kryptowährungen, denn es ist unklar, wer die Autorität und die Möglichkeit hätte, die neue Finanzwelt regulieren und kontrollieren zu können.[99]

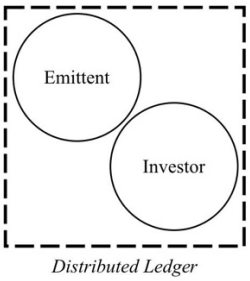

Abbildung 15: Neue Welt ohne Finanzinstitutionen[100]

5.2 Entwicklungsstand

Für das Finanzsystem ist es von hoher Wichtigkeit, dass die DLT nicht zu Fragmentierung führt und die Märkte intransparent macht, was zur Kumulierung unkalkulierbarer Risiken führen könnte (Szenario 1). Ebenso ist es bei den hohen regulatorischen Anforderungen unwahrscheinlich, dass die DLT den Wertpapierhandelsprozess von Grund auf revolutionieren wird (Szenario 3), so dass dem aktuellen Entwicklungsstand nach Szenario 2 als am Wahrscheinlichsten angesehen werden kann. Es ist offensichtlich, dass der Erfolg der DLT von der Kooperation aller Marktteilnehmer abhängig ist, auch wenn das bedeutet, dass einige Teilnehmer ihr Geschäftsmodell überarbeiten müssen, um nicht redundant zu werden. Ein Paradebeispiel dafür ist die NASDAQ, die selbst u.a. als Zentrale Gegenpartei agiert und mit der DLT eigene Geschäftsbereiche überflüssig machen würde. Gleichzeitig wird aber auch das außergewöhnlich große Potenzial der Blockchain-Technologie mit neuen und renditeträchtigen Geschäftsbereichen erkannt, so dass die NASDAQ eine führende Rolle in der Entwicklung einnimmt und

[99] Vgl. ebd., S. 7f.
[100] Eigene Darstellung in Anlehnung an ebd., S. 8.

durch ihre Marktmacht auch die Möglichkeit hätte, einen Standard zu etablieren. Eine zentrale Bedeutung bei der Transformation der Handelsabwicklung kommt demnach den zentralen Finanzinstitutionen zu. Dennoch ist eine Einführung im großen Stil nicht von heute auf morgen denkbar. Den aktuellen Entwicklungsstand der Blockchain-Technologie fasst die SWIFT anschaulich in der nachfolgenden Grafik zusammen (Abbildung 16). Es wird vor allem deutlich, dass insbesondere regulatorische Fragen geklärt und ein gemeinsamer Standard gefunden werden müssen. Auf technischer Seite ist die Forschung – nicht zuletzt dank der Erfahrungen mit Bitcoin – für die kurze Entwicklungszeit schon relativ weit fortgeschritten. Es sei noch einmal in Erinnerung gerufen, dass es Bitcoin erst seit dem Jahr 2009 gibt und die Forschungsausgaben für die DLT in der Finanzwelt vor wenigen Jahren noch bei null lagen.

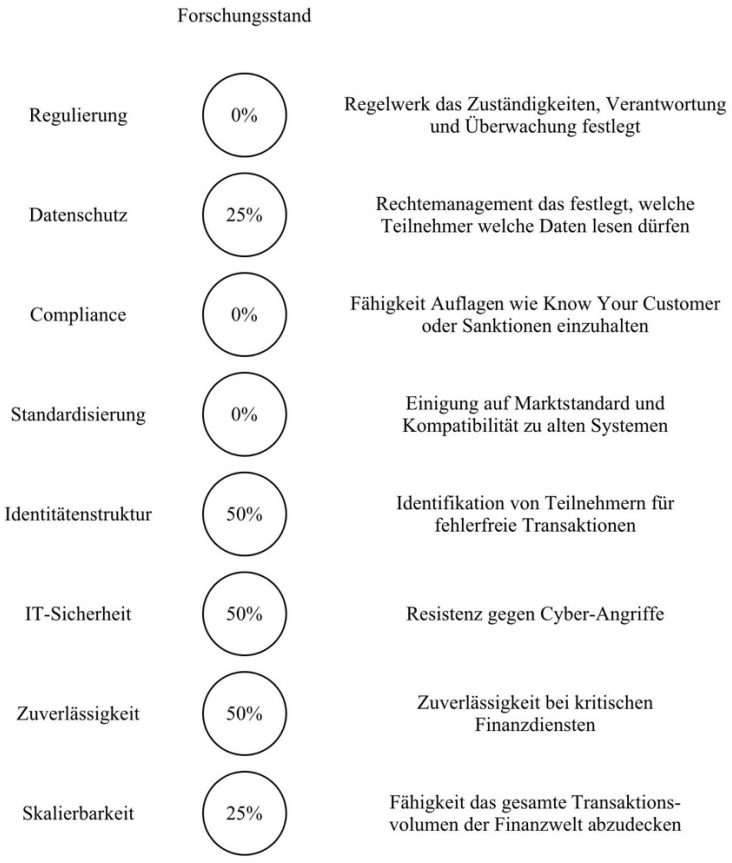

Abbildung 16: Entwicklungsstand der DLT[101]

[101] Eigene Darstellung in Anlehnung an SWIFT, *Swift on Distributed Ledger Technologies* (London: SWIFT, 2016), S. 15. https://www.swift.com/insights/press-releases/swift-and-accenture-outline-path-to-distributed-ledger-technology-adoption-within-financial-services.

Am Potenzial der Blockchain-Technologie gibt es nach Meinung von Analysten der Europäischen Zentralbank keine Zweifel mehr.[102] Allein 2015 wurden knapp eine halbe Milliarde US-Dollar in die Weiterentwicklung der Technologie investiert.[103] Bereits 2017 sollen die Investitionen laut einer Studie von Magister Advisors eine Milliarde US-Dollar erreichen.[104] So wird es nur noch eine Frage der Zeit sein, bis die DLT im großen Stil in der Finanzwelt zur Anwendung kommen wird. Die derzeit noch existierenden Herausforderungen sind alle lösbar und wie für Bitcoin, gilt auch für einen Distributed Ledger im Wertpapierhandel, dass die Technologie *bootstrapped* ist (Absatz 3.2.5). Das heißt, erst beim Zusammenspiel von Finanzdienstleistern und Regulierungsbehörden wird die DLT ein Erfolg werden können. Wann es soweit ist, wird auch eine politische Entscheidung sein. Das größte Blockchain-Konsortium wird derzeit vom FinTech-Unternehmen R3[105] geführt, welches die Entwicklung eines technischen Standards vorantreibt. Dem Konsortium gehören inzwischen 45 Finanzdienstleister an, darunter auch nahezu alle großen Investmentbanken und Vermögensverwalter.

[102] Vgl. Pinna, S. 5.

[103] Vgl. DB, *Future of Fintech in Captial Markets* (Frankfurt: Deutsche Börse AG, 2016), S. 9. http://deutsche-boerse.com/blob/2621702/ed055219caeb553f43950609d29e1bb3/data/future-of-fintech-in-capital-markets_en.pdf.

[104] Vgl. MA, *Blockchain & Bitcoin in 2016: A Survey of Global Leaders* (London: Magister Advisors, 2015), S. 32. http://de.slideshare.net/jeremysmillar/magister-advisors-blockchain-bitcoin-in-2016-a-survey-of-global-leaders.

[105] Mehr zum R3-Konsortium: https://r3cev.com/

Glossar

Bitcoin Erste und am weitesten verbreitete Kryptowährung. Wurde 2009 vom Entwickler Satoshi Nakamoto eingeführt.

Blockchain Dezentralisierte Datenbank, die Datensätze in Blöcken zusammenfasst und deren Integrität durch Verkettung von Hashwerten gewährleistet wird.

Block Reward Belohnung für die Node, die als erstes das Hash-Puzzle für einen neuen Block löst und die Blockchain verlängern darf.

Clearing Feststellen von Forderungen und Verbindlichkeiten zwischen zwei Handelspartnern durch eine Clearingstelle als Intermediär.

Distributed Ledger Auf ein Peer-to-Peer-Netzwerk verteiltes Konto, das von seinen Teilnehmern gemeinsam im Konsens verwaltet wird.

Front Running Das Ausnutzen von Insider-Informationen im Börsenhandel zum eigenen Vorteil. Front Running ist in den meisten Ländern illegal.

Hash Prüfsumme zur Überprüfung der Integrität von Daten.

ISIN International verwendete, zwölfstellige Nummer zur Identifizierung von Wertpapieren. Beispiel: DE000A1EWWW0 (Adidas AG).

Kassamarkt Markt, wo vornehmlich Aktien, Devisen und Rohstoffe gehandelt werden. Ein am Kassamarkt erfolgtes Geschäft, muss innerhalb von zwei Börsentagen erfüllt werden.

Kryptowährung Virtuelle Währung, die auf den Prinzipien der Kryptografie und Dezentralisierung aufbaut.

Ledger In der Finanzwelt gängige Bezeichnung für ein Konto.

Merkle Tree Baumförmige Hash-Datenstruktur, um effizient die Integrität großer Datenmengen überprüfen zu können.

Mining Vorgang, der durch Lösen eines Hash-Puzzles neue Blöcke erzeugt, die an die Blockchain angehängt werden.

Nakamoto, Satoshi Erfinder von Bitcoin. Die Identität von Satoshi Nakamoto ist nicht geklärt. Es ist unklar, ob sich hinter dem Pseudonym eine Einzelperson oder Entwicklergruppe verbirgt.

Node Teilnehmer am Bitcoin-Netzwerk, der Transaktionen und Blöcke durch Mining validiert.

Nonce Zufallswert, der nur einmal genutzt wird.

Peer-to-Peer Vernetzung von gleichgestellten Rechnern ohne zentralen Server. Jeder Rechner ist Client und Server zugleich.

Pointer Zeigt den Speicherort eines Objekts an.

Proof of Work Siehe Mining.

Quote Verbindliches Stellen eines Ankauf- und Verkauf-Kurses an der Börse.

Settlement Geschäftserfüllung einer Wertpapiertransaktion durch Austausch von Wertpapier gegen Bezahlung.

SHA-256 Von Bitcoin verwendete, kryptografische Hash-Funktion.

Signatur Digitale Unterschrift.

Smart Contract Intelligentes Wertpapier, das seine eigenen Vertragsbedingungen lesen und bei Eintritt vorher definierter Ereignisse automatisch ausführen kann.

Spotmarkt Siehe Kassamarkt.

String Bezeichnung für eine beliebige Zeichenkette.

Transaction Fee Transaktionsgebühr, die im Bitcoin-Netzwerk für die Ausführung einer Transaktion von einer Node erhoben werden kann.

Zentrale Gegenpartei Im englischen Central Counterparty genannt. Zentrale Clearingstelle, der Banken als Clearing Member angehören können.

Zentralverwahrer Im englischen Central Securities Depository genannt. Verwahrt im Auftrag von depotführenden Banken die Wertpapierdepots. Kann Wertpapiere zwischen unterschiedlichen Depotbanken verbuchen.

Literaturverzeichnis

D+H. *Five Things Blockchain Must Get Right to Realize Its Full and Transformative Potential*. Toronto: D+H, 2016. http://www.dh.com/resources/white-papers/five-things-blockchain-must-get-right-realize-its-full-and-transformative (Zugriff: 07.10.2016).

DB. *Future of Fintech in Captial Markets*. Frankfurt: Deutsche Börse AG, 2016. http://deutsche-boerse.com/blob/2621702/ed055219caeb553f43950609d29e1bb3/data/future-of-fintech-in-capital-markets_en.pdf (Zugriff: 07.10.2016).

ECB. *Distributed Ledger Technology*. Frankfurt: European Central Bank, 2016. https://www.ecb.europa.eu/paym/pdf/infocus/20160422_infocus_dlt.pdf (Zugriff: 07.10.2016).

ESMA. *The Distributed Ledger Technology Applied to Securities Markets*. Paris: European Securities and Markets Authority, 2016. https://www.esma.europa.eu/file/18727/download?token=j_lKec2m (Zugriff: 07.10.2016).

GOS. *Distributed Ledger Technology: Beyond Blockchain*. London: UK Government Office for Science, 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (Zugriff: 07.10.2016).

IBM. *Banking on Blockchain: Charting the Progress of Distributed Ledger Technology in Financial Services*. London: Finextra, 2016. https://www.ingwb.com/media/1609652/banking-on-blockchain.pdf (Zugriff: 07.10.2016).

Irrera, Anna. *Nasdaq: Our Plans with the Blockchain*. London: Financial News, 2015. http://www.efinancialnews.com/story/2015-08-20/nasdaq-our-plans-for-the-blockchain-fredrik-voss (Zugriff: 07.10.2016).

Kerscher, Daniel. *Handbuch Der Digitalen Währungen*. Dingolfing: Kemacon, 2014.

MA. *Blockchain & Bitcoin in 2016: A Survey of Global Leaders*. London: Magister Advisors, 2015. http://de.slideshare.net/jeremysmillar/magister-advisors-blockchain-bitcoin-in-2016-a-survey-of-global-leaders (Zugriff: 07.10.2016).

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Online: Bitcoin.org, 2008. https://bitcoin.org/bitcoin.pdf (Zugriff: 07.10.2016).

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

Peters, Gareth W.; Panayi, Efstathios. *Understanding Modern Banking Ledgers through Blockchain Technologies*. London: University College London, 2015. http://www.digibib.net/permalink/832/EDS/edsbas:edsbas.ftarxivpreprints.oai.arXiv.org.1511.05740 (Zugriff: 07.10.2016).

Pinna, Andrea; Ruttenberg, Wiebe. *Distributed Ledger Technologies in Securities Post-Trading: Revolution or Evolution?* Frankfurt: European Central Bank, 2016. https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf (Zugriff: 07.10.2016).

Platzer, Joerg. *Bitcoin - Kurz & Gut*. Beijing: O'Reilly, 2014.

sciencebuddies. "Probability and the Birthday Paradox." Springer Nature, https://www.scientificamerican.com/article/bring-science-home-probability-birthday-paradox (Zugriff: 07.10.2016).

SWIFT. *Swift on Distributed Ledger Technologies*. London: SWIFT, 2016. https://www.swift.com/insights/press-releases/swift-and-accenture-outline-path-to-distributed-ledger-technology-adoption-within-financial-services (Zugriff: 07.10.2016).

UCL. "Ucl Research Centre for Blockchain Technologies." University College London, http://blockchain.cs.ucl.ac.uk/ (Zugriff: 07.10.2016).

Eidesstattliche Versicherung

Name:	Zahrte	Vorname:	René
Matrikel-Nr.:	11089981	Studiengang:	Informationswirtschaft

Hiermit versichere ich, René Zahrte, an Eides statt, dass ich die vorliegende Bachelorarbeit mit dem Titel *Funktionsweise und Auswirkungen der Blockchain-Technologie auf den Wertpapierhandel* selbständig und ohne fremde Hilfe verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Arbeit, die dem Wortlaut oder dem Sinne nach anderen Werken entnommen wurden, sind in jedem Fall unter Angabe der Quelle kenntlich gemacht. Die Arbeit ist noch nicht veröffentlicht oder in anderer Form als Prüfungsleistung vorgelegt worden.

Ich habe die Bedeutung der eidesstattlichen Versicherung und prüfungsrechtlichen Folgen sowie die strafrechtlichen Folgen einer unrichtigen oder unvollständigen eidesstattlichen Versicherung zur Kenntnis genommen.

Köln, 07.10.2016 René Zahrte

Ort, Datum Unterschrift