WILHELM BÜCHNER HOCHSCHULE
Mobile University of Technology

Entwicklung der Blockchain 1.0 - 4.0

Chancen und Risiken

Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B. Sc.)“ im Studiengang Angewandte Informatik der Wilhelm Büchner Hochschule

vorgelegt von:	Christoph Huschenhöfer
Studienbereich:	Angewandte Informatik
Matrikelnummer:	860688
Erstgutachter und betreuender Hochschullehrer:	Dr. Mathias Scheiblich

Inhaltsverzeichnis

Abkürzungsverzeichnis

B2B	Business-2-Business
BC	Blockchain
DApp	Distributed Application
DLT	Distributed Ledger Technology
IoT	Internet of Things
M2M	Maschine zu Maschine
P2P	Peer-to-Peer
PoB	Proof of Burn
PoC	Proof of Concepts
PoI	Proof of Importance
PoS	Proof of Stake
PoW	Proof of Work
SCM	Supply Chain Management

Abbildungsverzeichnis

1 Einleitung

1.1 Motivation und Relevanz

Wir fahren auf dem Weg von der Arbeit an die Tankstelle, tanken und bezahlen per Karte an der Kasse. Nebenbei nutzen wir ein Treuepunkte Programm, sammeln Punkte und tauschen diese gegen einen Kaffee, Kaltgetränk oder Schokoriegel. Beim einsteigen in das Auto wird schon die Strecke nach Haus berechnet und die schnellste Route vorgeschlagen. Die Einfahrt in die Tiefgarage muss umständlich mit dem Schlüssel geöffnt werden, von der Haustür leider auch. Einfacher wäre schon ein automatisches System. Wir erkennen dies sofort und suchen über Google sofort nach einer Lösung. In den kommenden Wochen erhalten wir immerwieder Informationsangebote unserer Suche. Netterweise werden auch derzeitige Angebote zu günstigeren Lösungen angezeigt. Unser tägliches Leben ist so vielfältig, dass jede mögliche gefühlte Erleichterung dankend angenommen wird. Dass in diesem Fall mit Daten bezahlt wird ist dabei weniger bekannt oder wird schlicht hingenommen. Diese Daten nutzen Dritte auch in der oben beschriebenen Weise und im Rahmen des Marketing.

1.2 Zielsetzung und Aufbau

Ziel eines Konfliktes oder einer Auseinandersetzung soll nicht der Sieg, sondern der Fortschritt sein.
- Joseph Joubert (1754 - 1824) -

In diesem Sinne soll die Arbeit die fortwährende Entwicklung der Blockchain abbilden.

2 Theoretische Grundlagen der Blockchain

Das folgende Kapitel enthält eine ausführliche Erklärung der Begriffe Blockchain, Kryptowährung, Bitcoin, Ethereum, Smart Contracts, Distributed Application (DApp) und Internet of Things (IoT). Dieses dient dem Zweck ein ausreichendes und umfangreiches Basiswissen zu den Themen zu erhalten. Im Anschluss wird die Arbeitsweise einer Blockchain am Beispiel der Kryptowährung Bitcoin erklärt.

2.1 Begriffsklärung

2.1.1 Blockchain

Eine Blockchain ist eine vollständige und unveränderliche Transaktion-Historie zu allen Transaktionen einer dezentralen Community, der jeder, der ein Teil davon ist, zustimmt (Hosp 2018b, S. 45).

Blockchains sind fälschungssichere, verteilte Datenstrukturen, in denen Transaktionen in der Zeitfolge protokolliert, nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet sind (Finanzdienstleistungsaufsicht (BaFin) 2017, S. 16).

Bei der Blockchain handelt es sich vereinfacht dargestellt um eine Transaktionsliste. Einzelne Transaktionen wurden dabei zu Blöcken zusammengefasst, mit einem Zeitstempel versehen und durch ein kryptographisches Verfahren linear aneinandergehangen. Da es sich um ein verteiltes System handelt, handelt es sich nicht um eine einzelne Datei oder Datenbank, sondern um eine vollständige redundante Speicherung in einem Netzwerk. Neu erstellte Blöcke werden im Netzwerk verteilt, dort durch jeden Teilnehmer kontrolliert und an die dort vorliegende Blockchain angehängt.

Synonym für eine Blockchain steht die Distributed Ledger Technology (DLT). Dabei treten jedoch vereinzelte Unterschiede auf. So muss ein DLT aber nicht zwangsläufig in Form einer Kette vorliegen noch muss es zwangsläufig einen Proof of

Work (PoW) zur Bestätigung eines Konsens durchführen. Dies sollte nochmals kontrolliert werden.

2.1.2 Kryptowährung

Die Wortherkunft selbst stammt aus den Grundbegriffen Kryptografie und Währung.

Durch die Nutzung von kryptographischen Funktionen zur Erzeugung von Prüfwerten und die Nutzung eines asymetrischen Verschlüsselungsverfahrens zur Erstellung einer Signatur.

Als Währung muss die sie dabei die drei Geldfunktionen erfüllen. Dabei handelt es sich um die Funktionen als Zahlungsmittel-, Wertaufbewahrungs- und Wertmessfunktion.

Kryptowährungen sind als digitale Darstellung von Wert definiert, die weder von einer Zentralbank, noch einer Behörde geschaffen oder ausgestellt wird und auch keine Verbindung zu gesetzlichen Zahlungsmitteln haben muss. Kryptowährungen werden von natürlichen und juristischen Personen als Tauschmittel verwendet und können elektronischÜbertragen, gespeichert und gehandelt werden (*EBA Opinion on ‚virtual currencies'* 2014).

Technisch werden Kryptowährungen als digitale Währungen mit einem meist dezentralen, stets verteilten und kryptografisch abgesicherten Zahlungssystem beschrieben (Gabler 2018).

2.1.3 Bitcoin

Bei einem Bitcoin handelt es sich um eine dezentrale digitale Währung, als sogenannten Kryptowährung, auf der Blockchain. Da Bitcoin selbst die Blockchain-Technologie nutzt, greifen alle zuvor genannten Eigenschaften.

Im Jahre 2008 veröffentlichte Satoshi Nakamoto unter dem Titel „Bitcoin: A peer-to-peer electronic cash system" ein Whitepaper, welches zugleich den Ursprung des Bitcoins, als auch die erste vollständige Umsetzung der Blockchain-Technologie beschreibt.

2.1.4 Ethereum

Während die Bitcoin-Blockchain eine Technologie ist, auf deren Basis es möglich ist, Zahlungen zwischen Transaktionspartnern per Bitcoin durchzuführen, stellt Ethereum primär das technische Fundament zur Verfügung, um Programmcodes, sogenannte DAPPs (decentralized applications) auszuführen (Rosenberg 2016, S. 54).

Der Vorteil von Ethereum gegenüber dem Bitcoin ist, dass es sich nicht lediglich um eine weitere Kryptowährung handelt. Ethereum kann durch die Währung namens Ether als Kryptowährung genutzt werden, erweitert diese Funktionalität um die Möglichkeit zur Nutzung sogenannter Smart Contracts.

2.1.5 Smart Contracts (Inteligente Verträge)

Smart Contracts sind rechtliche Vereinbarungen, die sich IT-Technologien bedienen, um die eigene Durchsetzbarkeit sicherzustellen. Es werden durch Smart Contracts autonome Handlungen initiiert, die zuvor durch die Parteien vertraglich vereinbart und signiert wurden. Beispielsweise können vereinbarte Zahlungen von Geldbeträgen selbsttätig veranlasst werden. Basieren Smart Contracts auf Blockchains, ergeben sich per se vertrauenswürdige Transaktionen. Eine dritte Instanz zur Sicherstellung einer korrekten Transaktion, beispielsweise eine Bank oder ein virtueller Marktplatz, wird nicht benötigt. Echte Peer-to-Peer-Verträge sind möglich. Ein weiterer Anwendungsfall von Smart Contracts ist denkbar. Smart Contracts könnten statt Vereinbarungen von Vertragsparteien gesetzliche Regelungen ausführen. Beispielsweise die Regelungen des Patentgesetzes könnten durch einen Smart Contract implementiert werden. Die Verwaltung von IPRs (Intellectual Property Rights) entsprechend den gesetzlichen Regelungen würde dadurch sichergestellt werden. Bislang werden Spezialisten, beispielsweise Patentanwälte, benötigt, um eine akkurate Administration von Schutzrechten zu gewährleisten. Smart Contracts könnten die Dienstleistungen dieser Spezialisten auf dem Gebiet des geistigen Eigentums obsolet werden lassen.

2.1.6 Destributed Application (Verteilte Anwendungen)

Verteilte Anwendungen (Distributed Applications) sind Software-Anwendungen, die in einem Netzwerk auf mehreren Computern ausgeführt und auf lokalen Servern

oder in der Cloud gespeichert werden. Im Gegensatz zu herkömmlichen Anwendungen, die auf einem einzigen System laufen, führen verteilte Anwendungen eine einzelne Aufgabe oder einen Job auf mehreren Systemen gleichzeitig aus.

2.1.7 Internet of Things

Der Begriff Internet of Things (zu Deutsch: Internet der Dinge) bezeichnet die zunehmende Vernetzung zwischen intelligenten Gegenständen sowohl untereinander als auch nach außen mit dem Internet. Verschiedene Objekte, Alltagsgegenstände oder Maschinen werden dabei mit Prozessoren und eingebetteten Sensoren ausgestattet, sodass sie in der Lage sind, via IP-Netz miteinander zu kommunizieren. So ist neben der heute bestehenden Mensch-Maschine-Kommunikation auch eine Maschine zu Maschine (M2M) möglich.

2.2 Technologien der Blockchain

Der vorangegangenen Darstellung liegen die hier folgenden Technologien zugrunde.

2.2.1 Konsensusmechanismus

Konsensus ist ein kooperativer Prozess mit dem Ziel einer Einigung. Eine Gruppe von Teilnehmern entwickelt und vereinbart diese Entscheidung über den Zustand/Status des Systems im Interesse aller.

Eine Blockchain ist ein dezentrales System, bestehend aus gleichberechtigten Teilnehmern. In einem zentralen System wird ein Zustand durch eine Instanz vorgegeben. Um nun in diesem dezentralen System eine Einigung zu erzeugen, wie der Zustand sich ändert, bedarf es eines kooperativen Prozess, bei dem eine Gruppe von Teilnehmern im Interesse aller eine Entscheidung entwickelt und vereinbart.

Glaser und Bezzenberger (2015) bezeichnen die zugehörigen Verwaltungssysteme als verteilte Konsenssysteme, bei denen durch die Kryptographie und einem Peer-to-Peer (P2P)-Netzwerk ein Konsens durch eine geschützte netzwerkweite Verifikation des Status des Systems erreicht wird .

Im weiteren Verlauf soll daher ein Einblick in die betreffenden Technologien Kryptographie, Proof-of-Work und P2P-Netzwerk gegeben werden.

2.2.2 Kryptographie

Wie beschrieben liegt der Blockchain-Technologie ein kryptografisches Verschlüsselungsverfahren zugrunde.

Bitcoin benutzt die kryptologische Hashfunktion SHA-256 (Claudio Brecht, 2017). Bei einer Hash-Funktion wird ein Input bestehend aus einer Information oder Datei in einen Hashwert als eine Buchstaben-Zahlen-Kombination überführt.

Bei einem Hash spricht man auch von einer Einwegfunktion. Man kann die Verschlüsselung nicht mehr umkehre beziehungsweise zu den Quelldaten decodieren. Der vom Hash-Algorithmus errechnete Code ist außerdem ein- zigartig und wird

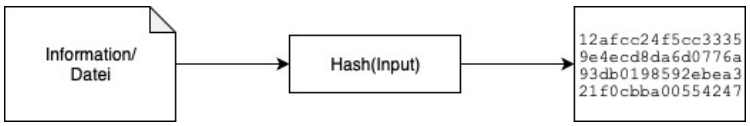

Abbildung 2.1: Hash-Funktion

aufgrund dieser Eigenschaft auch als digitaler Fingerabdruck bezeichnet (Chainthat, 2016). Durch diese komplexen mathematischen Berechnungen und der deterministischen Eigenschaft des Algorithmus wird aus einem Input stets der gleichen Hashwert erzeugen.

Wird der Input modifiziert, so erhält man mit der gleichen Hash-Funktion einen vollkommen anderen Hashwert. Somit folgt auf eine minimale Änderung des Inputs eine maximale Änderung des Output. Der Hashwert sichert somit die Integrität des Inputs. Es ist dabei jedoch nicht möglich von einem berechneten Hash zurück zum ursprünglichen Input zu gelangen.

Die Kryptografie sorgt für die Transparenz als auch für die Privatsphäre. Bei dem Prozess der Kryptographie im Zusammenhang mit der Blockchain wird ein geheimer Schlüssel in Form einer Zufallszahl generiert bzw. errechnet. Es werden somit alle Daten einer Transaktion verschlüsselt. (Claudio Brecht, 2017)

Aus diesem geheimen Schlüssel der in Form eines Hash vorliegt generiert man den öffentlichen Schlüssel.

Neben dem Hash nutzt eine Blockchain im Rahmen der Kryptographie ein weiteres Verfahren. Es handelt sich dabei um ein asymetrisches Verschlüsselungsverfahren.

Im Rahmen des asymetrische Verschlüsselungsverfahren verwenden ein Sender und ein Empfänger unterschiedliche Schlüssel. Man spricht bei diesen um mathematisch verbundene Schlüsselpaare aus einem öffentlichen Schlüssel und einem dazugehörigen geheimen Schlüssel. Die benannten Schlüssel werden im weiteren Schreiben auch als public-Key und private-Key bezeichnet.

Dieses Schlüsselpaar kann zur Erstellung einer digitalen Signatur verwendet werden (Stallings 2003). In das Literaturverzeichnis aufnehmen.

2.2.3 Proof of Work

Der bekannteste Konsensus-Mechanismus sieht so aus: Um einen Block (also ein Update) zu kreieren, muss ein Teilnehmer mit seinem Computer eine Rechenleistung erbringen, mit der ein zufälliger Hash zum Orginalergebnis rückgerechnet werden muss. Man spricht bei dieser Hashingpower (die Macht, Hashes durchzurechnen) vom Beweis durch Arbeitsleistung bzw. auf Englisch von Proof of Work (POW) (Hosp 2018a, S. 59).

Der PoW bezeichnet das gesamte Verfahren, welches sich als mathematisch kryptographische Aufgabe darstellt.

Der Teilnehmer, der diese Aufgabe durchführt wird als Miner bezeichnet. Wie im Kapitel 2.2.2 beschrieben wird hierbei jdeoch nicht aus einem bestimmten Input ein Hashwert erzeugt, sondern aus einem zufälligen Input versucht einen bestimmten Hashwert zu erzeugen.

Während die Aufgabe selbst einen erheblichen Rechenaufwand in Form von enormen Speicherbedarf oder CPU-Power einnimmt, erfolgt eine Kontrolle in nur Millisekunden.

Der Teilnehmer, der diese Aufgabe als erstes erfült, sammelt die Transaktionen, kreiert den Block, hängt diesen an die Blockchain und informiert das Netzwerk. Nounce und Dificulty beschreiben.

Neben dem PoW als Arbeitsnachweis, existieren noch Proof of Importance (PoI) als Nachweis der Wichtigkeit und Proof of Stake (PoS) als Geldnachweis.

Das Verfahren wird auch als Reverse Engeneering bezeichnet.

Adam Back erstellte ein ähnliches Hashcash-System.

2.2.4 P2P-System

Das P2P-System bildet die technische Grundlage der Blockchain. Dabei handelt es sich um eine System/Netzwerk-Architektur.

Ein Peer-to-Peer (P2P) Netzwerk beschreibt ein Computernetzwerk/ Rechnernetzwerk bei denen alle Rechner miteinander verbunden sind und gleichberechtigt miteinander arbeiten. Es gibt keinen zentralen Server (Bryan, 2005).

Bei einem P2P-System handelt es sich um Netzwerk von gleichberechtigten Teilnehmern. Das englische Wort „Peer“ wird zu deutsch auch als Gegenstück oder Gleichartiger übersetzt.

Peer-tp-Peer-Netzwerk grafisch darstellen.

2.3 Datenstruktur einer Blockchain

Eine Blockchain besteht als einer Struktur von Daten. Diese Datenstruktur besteht vereinfacht aus Blöcken, die linear aneinander gekettet sind.

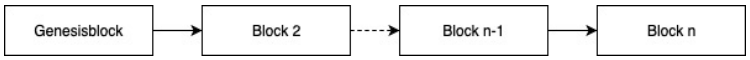

Abbildung 2.2: Vereinfachte Darstellung der Blockchain

Der erste Block der Blockchain wird als Genesisblock bezeichnet und wird durch den Entwickler der Blockchain vordefiniert.

Jeder weitere Block besteht dazu zum einen aus einem Block-Header, zum anderen der Transaktionsliste. Der Block-Header besteht aus Informationen zur Version, dem Nounce, Difficulty-Target, einer Prüfsumme des Block-Headers des Vorgängerblocks, einem Timestamp und einer Prüfsumme des Merkle-Tree. Diese benannten Prüfsummen werden im Folgenden als Hash bezeichnet.

Die Verkettung der Blöcke untereinander erfolgt in dem Block-Header. Dabei wird der Hash des Block-Headers des Vorgänger-Blocks erstellt und im aktuellen Block gespeichert. Durch dieses Verfahren enthält somit jeder Block den Hash des Headers des Vorgängerblocks und bestätigt den Block durch diese Art der Verkettung.

Neben dem genannten Hash wird ein zweiter Hashwert unter dem Namen Merkle-Root im Block-Header gespeichert.

Hier folgt ein Übergang.

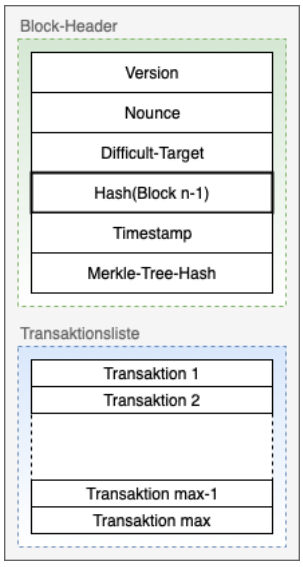

Abbildung 2.3: Block n

Wie beschrieben besteht ein jeder Block aus dem Block-Header und der Transaktionsliste. Diese Transaktionsliste beinhaltet alle verifizierten Transaktionen. Auf jede Transaktion des Blockes wird eine Hash-Funktion angewandt. Die erstellten Hashwerte werden daraufhin paarweise in einen neuen Hashwert überführt. So bildet sich ein Graph, dessen Wurzel als

Merkle-Root-Hash bezeichnet wird. Der Merkle-Root-Hash speichert demnach die Prüfsumme der Transaktionsliste und bestätigt sie.

Ein Zeitstempel dokumentiert den Zeitpunkt der Verifikation der Transaktionen.

In der Verkettung der Blöcke wird neben dem Hashwert des Block-Headers auch der Merkle-Root-Hash und somit alle enthaltenen Transaktionen bestätigt. Aufgrund der Verkettung der Blöcke und der in diesen hinterlegten Hashwerte des Vorgängerblock und Merkle-Tree, ist eine Modifikation bestätigter Blöcke nicht möglich, ohne auch die darauf aufbauenden Folgeblöcke neu zu berechnen.

Die Netzwerkknoten berechnen in regelmäßigen Abständen die Hashwerte eines jeden Blockes nach und bestätigen dadurch die Blockchain.

2.4 Arbeitsweise einer Blockchain

Die Arbeitsweise einer Blockchain soll am Beispiel einer Bitcoin-Transaktion erfolgen.

„Bitcoins werden von einer inzwischen endlosen Zahl von Computern auf der ganzen Welt erzeugt, die alle versuchen, das gleiche mathematische Rätsel zu lösen. Etwa alle 10 Minuten löst ein Computer dieses Rätsel und wird dafür mit Bitcoins belohnt. Ein neues Rätsel wird erzeugt und der Kreislauf beginnt von vorne.“ (Rosenberg 2016, S. 121)

Dieser Mechanismus soll im Folgenden näher erklärt werden.

Eine Transaktion sollte grafisch dargestellt und beschrieben werden.

Soll eine Transaktion durchgeführt werden, so wird der Public-Key des Empfängers als seine Adresse angegeben. Der Sender „signied“ diese Transaktion mit seinem Private-Key. Somit bestätigt er, dass diese Transaktion durch ihn ausgeführt werden soll. Diese Transaktion wird dann an den für den Sender zuständigen Knotenpunkt im Netzwerk gesand, welcher automatisch die weitere Verteilung im Netzwerk vornimmt. Die Transaktion ist mit der Verteilung dieser im Netzwerk zu diesem Zeitpunkt nicht verifiziert. Erst mit der Aufnahme in einem Block und dem Anfügen an die Blockchain gilt sie als verifiziert. Jeder Teilnehmer im Netzwerk prüft mit dem erhalt die Transaktion. Dabei erfolgt eine Kontrolle ob die Transaktion des Senders mit der Adresse des Public-Key und mit dem Private-Key „gesigned“ wurde, die Adresse des Empfängers als Public-Key korrekt ist und der Sender über genügend Coins verfügt. Schlussendlich wird die Transaktion in einen „Pool of unconfirmed Transactions“ aufgenommen.

Zirca alle 10 Minuten erfolgt das Reverse Engeneering zur Erzeugung eines zuteils vorgegebenen Hashwert.

Ist die Aufgabe durch den PoW erfüllt, wird der gesuchte Hash als Beweis veröffentlicht. Für die Lösung der Aufgabe erhält der Miner eine Belohnung in Form der Transaktionsgebühr. Der erstellte Block wird dann an die Blockchain gehängt.

3 Anwendung und Entwicklung der Blockchain

Vorgeschichte

Sein anbeginn der Menschheit, sieht der Mensch neben bestehenden Problemen auch Herausvorderungen und versucht diesen aus dem Weg zu gehen oder diese zu beseitigen. Mit der Erfindung des Computers hat sich dies in keinster Art und Weise geändert. Ein unbekannter Autor gab mit dem Zitat: „Der Computer hilft uns, Probleme zu lösen, die wir ohne ihn gar nicht hätten.“ den Hinweis darauf, dass allein mit der Technologisierung und Digitalisierung die bereits bestehenden Probleme nicht einfach in Luft auflösen. Einige bestehende Probleme wurden gelöst, andere sind daraus erst entstanden.

An dieser Stelle könnte die entstehung des Computers und des Internets kurz beschrieben werden. Von der Standallone Rechenmaschine, die Daten einfach speichert und wiedergeben kann, folgte schnell ein Netzwerk (Mehrwert).

Auch die Blockchain-Technologie entstand demnach natürlich nicht einfach aus dem Nichts. Es bedarfte einige findige Köpfe, die zu diesem Zeitpunkt bestehende Probleme erkannten und versuchten diese nach und nach auch mit der Hilfe des Computers zu lösen.

Hier muss ein übergang zu den offenen Fragen: Hashing, Dezentralisierung (P2P-Netzwerk), Kryptografie,... geschaffen werden. Ziel ist es mithilfe der Komponenten eine Blockchain als dezentralen Datenspeicher zu erzeugen der durch Art und Weise ein Vertrauen enthielt.

Eine reguläre einfache Client-Server-Datenbankarchitektur ist zentralisiert. Sie besitzt also viele Clients, die alle mit einem Server kommunizieren. Die Dezentralisierung folgte daraufhin.

1991 erarbeiteten die Forscher Stuart Haber und W. Scott Stornetta eine Konzeption mit dem Titel „How to Timestamp a Digital Document“ (zu Deutsch: Wie man digitale Dokumente zeitstempelt). In ihrer Konzeption beschreiben sie, wie festgestellt werden kann, wann ein Dokument erstellt und wann es zuletzt bearbeitet wurde.

Darauf aufbauend beschreiben sie eine „rechnerisch praktikable Lösung zur Zeitstempelung digitaler Dokumente, die nicht rückwirkend veränderbar sind.“(Stuart Haber 1991) Aus dieser Lösung erging das Hashing, eine Datei in einen unverwechselbaren Hash umzuwandeln. Diesen zusammen mit einen Zeitstempel zu unwiederruflich zu speichern.

1992 wurde dann ein Merkle-Tree hinzugefügt, der die Effiziens der Speicherung optimiertte, indem durch diesen mehrere Dokumente in einen Block integriert werden konnten. Die beschriebene Technologie wurde jedoch nicht weiter erprobt und das Patent zu dieser erlosch im Jahre 2004.

Ab 2004 griff Hal Finney diese Technologien erneut auf und entwickelte ein wiederverwendbaren Proof-of-Work (RPoW). Dieses Verfahren erstellte einen nicht austauschbaren Token und einen RSA-signierten Token, der den Besitz einer Person zugeordnet und übertragbar war. Das Problem der Doppelausgabe (Double-Spending) konnte durch einen zentralen „vertrauenswürdigen“ Server behoben werden, der den Besitz der Token registrierte.

Parallel zu dieser Entwicklung entstand „in den 90er Jahren unter der Cyberpunk-Bewegung ein erstes Konzept zu einem dezentralen System, das Werte anonym und verschlüsselt zwischen zwei Parteien transferieren konnte.“

Probleme

Die Technologien bestanden alle allein für sich bereits. Niemand jedoch kombinierte diese. Eine Kombination der Zeitstempelung von Dokumenten in Verbindung mit dem Merkle-Tree unter einem dezentralen System ohne ein sogenanntes Double-Spendung wurde bis dato jedoch nicht realisiert.

Entwicklung

Die grundlegendsten Ideen die zur Entwicklung einer Blockchain führten, war die Unabhängigkeit von Dritten, ein implementieren von Vertrauen durch eine manipulationsresistente, unveränderliche, dezentral verteilte und transparente Datenbasis.

Double Spending

Dabei muss gelten, dass die erste Transaktion, die im Ledger aufge- nommen wird, die einzig gültige ist und nicht im Nachhinein verändert oder aus dem Ledger entfernt werden kann (Roßbach, 2016). Diese Problemstellung löste Bitcoin mit der Blockchain. Bei dieser werden ausste- hende und als korrekt eingestufte Transaktionen in Blöcken gesammelt und als Gruppe in den Einigungsprozess eingebracht und dem Ledger sequentiell angehängt - diese Kette von Blöcken ist die Blockchain. Die Problematik ergibt sich dabei in erster Linie dadurch, dass in einem verteilten P2P-Netzwerk neu auftretende Informationen nicht zum exakt selben Zeitpunkt auf allen Knoten zur Verfügung stehen, sondern sich erst im Netz verteilen müssen. Sie werden an einer Stelle, genauer gesagt an einem Knoten, dem Netzwerk zugefügt und verbreiten sich von dort aus auf das gesamte Netz, was Zeit in Anspruch nimmt. Schickt nun ein Knoten eine Transaktion mit einem Asset in eine Richtung des Netzwerks und eine zweite Transaktion mit demselben Asset in eine andere, würde dies das Netz in einen inkonsistenten Zustand bringen, da die Teilnehmer über unterschiedliche Informationen verfügen (Roßbach, 2016).(Johannes Scherk B.Sc. 2017)

3.1 Blockchain 1.0 - Bitcoin als Beginn der Blockchain

3.1.1 Geschichte

Die Idee einer Kryptowährung wurde bereits 1998-2000 mehrfach beschrieben, jedoch nie umgesetzt.

„[...] war es Nakamoto, der ein zentrales Problem digitaler Währungen in einem dezentralen Umfeld als erstes lösen konnte: die Möglichkeit, eine digitale Münze zweimal auszugeben. Das war bislang nur Banken in ihrem zentralen Umfeld gelungen.“ (Rosenberg 2016, S. 25)

Unter dem Pseudonym Satoshi Nakamoto wurde im Jahr 2008 das Bitcoin Whitepaper - Bitcoin: A Peer-to-Peer Electronic Cash System (zu Deutsch: Bitcoin: Ein elektronisches Peer-to-Peer-Bezahlsystem) publiziert. Dieses Dokument gilt als Grundlage des Bitcoin und ersten Umsetzung einer Blockchain im Anwendungsgebiet der Kryptowährungen und beho bdas bis zu diesem Zeitpunkt weiter auftretende Problem der doppelten Ausgabe (Double-Spending).

Aufgrund der Komplexität einer Blockchain (Kryptografie, Entwicklung, Programmierung, Konzeption eines Systems) und benötigter Kompetenzen im Bereich der Finanzwirtschaft kommen Zweifel auf, dass ein Mensch all diese Kenntnisse besitzt und Bitcoin und somit der Ursprung der Blockchain allein durch einen Menschen erschaffen wurde. So besteht die Möglichkeit, dass es sich bei Satoshi Nakamoto auch um eine Personengruppe handelt.

3.1.2 Probleme

- Der Proof-of-Work ist zu energielastig, ohne nachhaltigen Inhalt, usw.
- Es wurde nur das Anwendungsfeld der Kryptowährung bedient, dich die Idee der Blockchain kann noch viel größer werden.
- Die Art der Skallierung ist begrenzt und kann durch eine neue Blockchain erweitert werden.
- die Speicherintensität steigt und nicht jeder Client muss die gesamte Blockchain speichern.
- Die Anzahl von Transaktionen einer Blockchain erreicht nicht den Wert, der heutzutage durchgeführten Transaktionen.

Wie einzelne Aspekte nun behoben werden konnten wird im folgenden Unterkapitel beschrieben.

3.1.3 Entwicklung

Warum kam es zu dieser Entwicklung:

Die voranngegengene Idee der Vorgeschichte der Blockchain wurde durch Bitcoin als Blockchain 1.0 umgesetzt. Und doch war die Entwicklung nicht abgeschlossen. Es ergaben sich andere Probleme:

Patrick Rosenberg beschrieb in seinem Buch Bitcoin und Blockchain die Arbeitsweise wie folgt: „Bitcoins werden von einer inzwischen endlosen Zahl von Computern auf der ganzen Welt erzeugt, die alle versuchen, das gleiche mathematische Rätsel zu lösen. Etwa alle 10 Minuten löst ein Computer dieses Rätsel und wird dafür mit Bitcoins belohnt. Ein neues Rätsel wird erzeugt und der Kreislauf beginnt von vorne.“ (Rosenberg 2016, S. 121)

Aus dieser Aussage gehen mehrere Probleme hervor! (mathematisches Rätzel ohne Sinn, nur alle 10 Minuten, mit Bitcoin belohnt, endlose Zahl von Computern, ...) Dieses Zitat kann als Einstieg in die Problematiken der Blockchain 1.0 genutzt werden.

Skalierungsprobleme -> SegWit-Update (Softfork) Das Problem der Skalierung wurde durch Update zumindest entschärft. Dieses Update beinhaltete SegWit. Mit dem Update namens Segregates Witness (kurz: SegWit, zu Deutsch segereiter Zeuge) wurde die Skalierung des Bitcoin verbessert. Mögliche Lösungen von Skalierungs-Problemen sind folgende: - Blockgröße vergrößern, - Transaktionsgröße veringern, - ...

Das SegWit-Update verringerte die Transaktionsgröße. Der benötigte Speicherplatz einer Transaktion besteht zur einen Hälfte aus Informationen zur Transaktion, zur anderen aus der Signatur per Private-Key. Durch das Update konnte die hälfte des Speicherplatzes eingespart werden und so die Anzahl von Transaktionen pro Block von 4200 Transaktionen auf 8400 Transaktionen erhöht, ohne den Speicherplatz zu erhöhen. Die Signatur wird nun wie nach dem Update benannt durch einen Zeugen bestätigt.

3.2 Blockchain 2.0 - Ethereum

3.2.1 Geschichte

Etherium

verfügt über eine eigene Programmiersprache -> Solidity,

Was bezweckte Vitalik Buterin damit, was versprach er sich davon

Bei Bitcoin handelte es sich um die erste digitale Währung, die eine Blockchain-Technologie nutzte. Ihr Anwendungsfeld blieb jedoch auf den Bereich der Kryptowährungen beschränkt.

Ethereum wurde 2013 durch Vitalik Buterin konzipiert und nicht lediglich auf ein Anwendungsfeld beschränkt. So kann mittels Ethereum nicht nur Transaktionen mit einem Zeitstempel versehen und in einen Block integriert werden. Ethereum kann ganze Klassen oder so genannten Smart Contracts in einen Block integrieren. So wird die Umgebung von Ethereum als Ethereum Virtual Machine bezeichnet und bietet die Funktionalität eines dezentralen Computers. Ethereum stellte zum ersten Mal die Möglichkeiten von Smart Contracts zur Verfügung.

Smart Contracts

Schon vor der erfolgreichen Entwicklung der Blockchain-Technologie skizzierte Nick Szabo das Konzept eines Smart Contract. Dazu definierte er bereits 1997 in seiner Arbeit Formalizing and Securing Relationships on Public Networks Smart Contracts erstmalig als automatisch ausführbare Verträge, die kryptografisch gesicherte Beziehungen zwischen den Knoten eines Rechnernetzes darstellen und eine Kombination von Protokollen und Benutzerschnittstellen nutzen.(Szabo 1997, S. 65)

Nick Szabo war 1994 der Erste, der den Begriff Smart Contract einführte und damit einen Ablauf beschrieb, bei dem ein Vertrag durch ein digitales Programm mit dem Rückhalt einer Gemeinschaft umgesetzt wird. Die Blockchain übernimmt damit die Funktion einer neutralen dritten Partei.(Hosp 2018a, S. 122)

„Schickst du mir Datei X, dann bekommst du Summe Y.“(Hosp 2018a, S. 123)

Blockchains sind programmierbar: In den Blöcken können Anweisungen einge- bettet sein, die zu entsprechende Aktionen führen, falls bestimmte Kriterien er- füllt werden, sowie weiterführende Daten zu Transkationen o.ä. enthalten. Gerade die Programmierbarkeit der Blockchain macht diese interessant: D.h. die Blockchain kann nicht nur für Transaktionen verwendet werden, sondern für alle denkbaren Anwendungen, die auf digitalen Daten basieren. Die Blockchain kann damit als sichere und transparente Datenbank für Informationen aller Art, zur Kommunikation zwischen den Teilnehmern im Netzwerk und oder als Instrument zur Nachverfolgung von Daten und Aktionen verwendet werden. Das größte Po- tenzial der Blockchain könnte jedoch darin liegen, selbstausführende Verpflichtungen - sog. „Smart Contracts“ - zu ermöglichen, die eine automatische Ausführung von Handlungen bei der Erfüllung festgelegter Kriterien erlauben. Solche Smart Contracts könnten insb. im Kontext des Internets der Dinge für die Kommunikati- on, den Austausch von Daten sowie die Selbstorganisation intelligenter, vernetzter Geräte eingesetzt werden. Eine Reihe von möglichen Anwendungsfeldern der Blockchain wird im nachfolgenden Kapitel vorgestellt.

Solch ein Smart Contract funktioniert sehr gut, da die Abmachung digital nachvollziehbar ist. Anders sieht es aus, wenn eine Vermischung mit der analogen/realen Welt vollzogen wird. Ob nun die Sache wirklich übergeben worden ist kann nicht nachvollzogen werden. Bestätigen beide Parteien der Blockchain, dass es zu einer übergabe kam, ist dies zu akzeptieren oder bedarf noch immer eines Dritten.

Alternativen zu Smart Contracts gibt es in soweit nicht, als dass Dritte mit einbezogen werden müssen. In der Praxis nutzen viele Personen gern Paypal (als Dritten), um in einem Falle das Geld zurückzuhalten. Internetanbieter/Onlineversandhäuser wie Amazon, Ebay oder Alibaba können Smart Contracts nutzen und in verbindung mit der Lieferung einen Erhalt zu bestätigen.

3.2.2 Probleme

3.2.3 Entwicklung

Anders als im Bitcoin, welcher sehr statisch ist und Anpassungen recht träge erfolgen, entwickelt sich Ethereum ständig weiter.

„Wenn man Bitcoin als eine Blockchain der ersten Generation betrachtet, so verdient Ethereum es definitiv, als Blockchain der zweiten Generation bezeichnet zu werden, da hier weit mehr Funktionen möglich sind.“(Hosp 2018b, S. 144)

Vorteile einer Blockchain allgemein: - geringe Unterhaltskosten (entgegen Versicherungsunternehmen, ...) - transparenz, da SC und die BC vollkommen transparent für alle ist,

Nachteile: - Verbindung der BC oder SC zur physischen Umwelt (nur durch Oracle oder andere BC möglich),

3.3 Blockchain 3.0 - Dezentralisierte Applikationen

3.3.1 Geschichte

Die Blockchain 3.0 entwickelte sich zwangsläufig aus der Blockchain 2.0, indem man die Entwicklung dieser vorantrieb, um ganze Applikationen auf die Blockchain zu speichern.

3.3.2 Probleme

3.3.3 Entwicklung

3.4 Blockchain 4.0 - Internet of Things

3.4.1 Geschichte

Internet of Things

IoT (zu Deutsch: „Internet der Dinge“)

Anwendungsfeld - Supply Chain Management

Eine mögliche Anwendung der Blockchain-Technologie in Verbindung mit dem IoT ist das Supply Chain Management (SCM). In einer Studie der Frauenhofer-Gesellschaft zu dem Thema Blockchain und Smart Contracts erläuterten die Autoren die Verwendung der Blockchain-Technologie und Smart Contracts unter anderem im Anwendungsfeld des SCM.

Aufgrund der Vielzahl von Wertschöpfungspartnern, beschrieben als Lieferanten, Hersteller, Händler, Logistik- und Finanzdienstleister, besteht der Bedarf an einem freizugänglichen Datenspeicher, in welchen die jeweiligen Beteiligten eine übergabe und übernahme eines physischen Produktes mit einem Zeitstempel unwiderruflich und für alle transparent speichert. Diese logistischen Prozesse können dabei automatisiert werden. (Prinz 2017)

Zur Umsetzung einer smarten Prozessteuerung im Bereich des SCM nutzt man das IoT.

Im Rahmen der logistischen Prozesse des IoT kommunizieren dabei Menschen zu Maschinen und umgekehrt oder aber M2M. Die benannte Automatisierung als Folge einer korrekten Kommunikation M2M ist in den vergangenen Jahren weit fortgeschritten.

Betrachtet man nun jedoch nicht die Automatisierung der physischen Abwicklung der Logistik, sondern eine damit verbundene Automatisierung der Finanzprozesse, so ist zu erkennen, dass die Abrechnung von Business-2-Business (B2B)-Transaktionen gemäß der Studie der Frauenhofer-Gesellschaft noch immer zu 60 Prozent durch Papierrechnungen durchgeführt werden. (Prinz 2017)

An dieser Stelle können auch weitere Anwendungsfelder/Anwendungsfälle definiert werden.

3.4.2 Probleme

Nachteile: Der private-Key muss sicher auf dem Gerät gespeichert und kryptografisch gesichert werden. (Christoph Meinel 2018)

Wie wird dabei die Abwicklung mittels der Blockchain und Smart Contracts durchgeführt? Wo liegen darin die Vor- und Nachteile?

Gartner sagt 6.4 Bil. Connected Things in 2016 (www.gartner.com/newsroom/id/3165317)

Daraus ergeben sich weitere Skalierungsprobleme...

Eine Möglichkeit für ein standardisiertes IoT-Protokoll, das diese Faktoren priorisiert, ist IOTA, ein völlig vertreiltes Datenbanksystem, das der sicheren und vollständig skalierbaren Kommunikation dient.(Hüls 2017)

3.4.3 Entwicklung

4 Die Entwicklung - Chancen mit Risiko

4.1 Der Hype als Ursprung der Entwicklung

Aus dem Hype entwickelten sich schnell Ideen, die einer Lösung bedarfen.

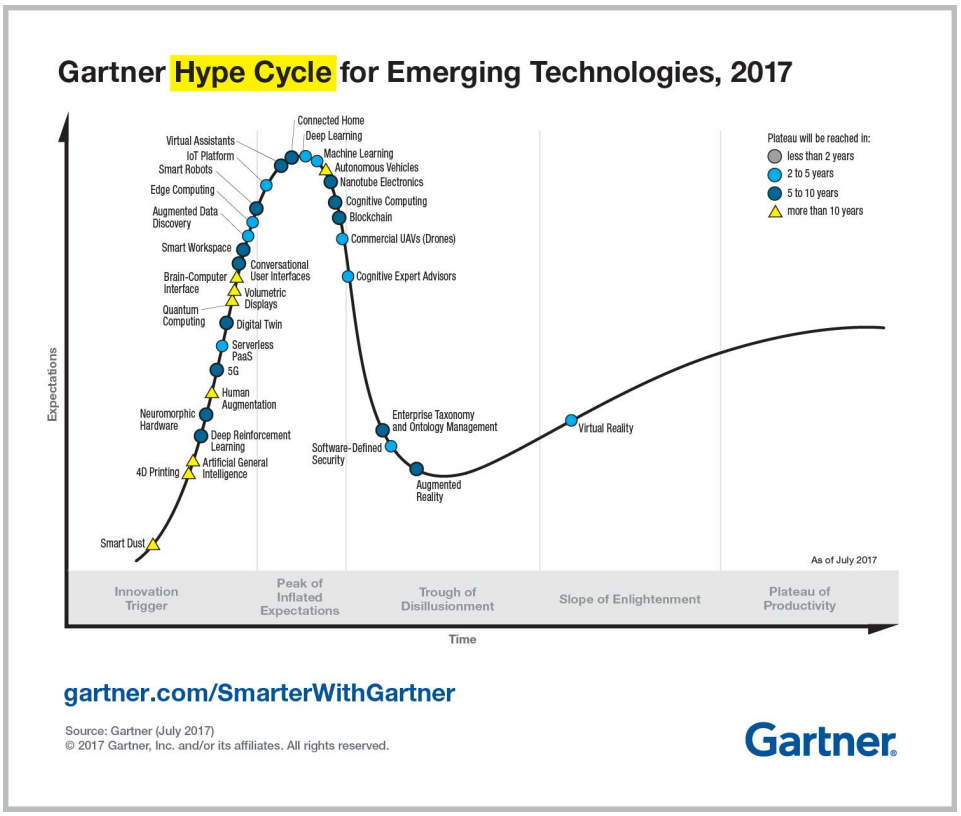

Abbildung 4.1: Gartner Hype Cicle

Der Gartner Hype Cycle wird in der Studie des HPI behandelt: (Christoph Meinel 2018)

4.2 Das Nutzungspotential

4.3 Der Hype

4.4 Alternativen

Tangle und Hashgraph https://cryptoresearch.report/crypto-research/blockchain-3-0-die-zukunft-der-dlt/?lang=de

5 Fazit

5.1 Zusammenfassung

Ziel dieser Arbeit war es die Entwicklung der Blockchain in erkennbare Phasen einzuteilen und zu klären, welchedie Gründezu der Teilung führten. Dazu wurden die folgenden Sachen durchgeführt:

5.2 Ergebnisse und Ausblick

Im Ergebnis erfolgte die Entwicklung der Blockchain trotz der doch jungen Technologie in 4 Schritten. Begonnen bei der Erfindung des Bitcoin im Whitepaper durch Satoshi Nakamoto, bis zur einbettung in die Industrie 4.0.

Bezogen auf die Umsetzung mancher Blockchains, die heutzutage in der Hand der öffentlichen Verwaltung liegen, äußerte sich Hosp wie folgt: “Ich glaube fast, dass eine solche Innovation von Regierungen selbst kommen muss, um einen Standard festzulegen.“ (Hosp 2018a, S. 111) Es ist also an der jeweiligen Regierung sich diser Technologie zu öffnen und ihren Nutzen zu erkennen. Dann kann die Blockchain selbst zu etwas Großem werden.

Erste wenn Blockchains untereinander kommunizieren können, werden Probleme mit der physischen Umwelt beseitigt werden können. Solang verlässt man sich auf Oracle oder die Bestätigung der Teilnehmer. Diese Blockchain könnten als Vertrauensketten fungieren.

Literaturverzeichnis

Christoph Meinel Tatiana Gayvoronskaya, Maxim Schnjakin (2018). *Blockchain: Hype oder Innovation*. Studie. Potsdam: Hasso-Plattner-Instituts.

EBA Opinion on ‚virtual currencies' (2014). European Banking Authority. URL: http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (besucht am 13. 01. 2019).

Finanzdienstleistungsaufsicht (BaFin), Bundesanstalt fuÌr (2017). „Initial Coin Offerings". In: *BaFin Journal* November 2017.

Gabler (2018). *Kryptowährungen*. Gabler Wirtschaftslexikon. URL: https://wirtschaftslexikon.gabler.de/definition/kryptowaehrung-54160 (besucht am 13. 01. 2019).

Glaser, Florian und Luis Bezzenberger (2015). „Beyond Cryptocurrencies - A Taxonomy of Decentralized Consensus Systems". Englisch. In: Munster: Universität Münster, Münster.

Hosp, Dr. Julian (2018a). *Blockchain 2.0*. München: Finanz Buch Verlag.

– (2018b). *Kryptowährungen*. München: Finanz Buch Verlag.

Hüls, Jannik (2017). *Tangle â Eine Einführung*. codecentric Blog. URL: https://wirtschaftslexikon.gabler.de/definition/kryptowaehrung-54160 (besucht am 13. 11. 2017).

Johannes Scherk B.Sc., Mag. Gerlinde PoÌchhacker-TroÌscher (2017). *Die Blockchain â Technologiefeld und wirtschaftliche Anwendungsbereiche*. Linz: BNVIT.

Prinz, Wolfgang (2017). *Blockchain und Smart Contracts - Technologien, Forschungsfragen und Anwendungen*. Studie. Fraunhofer-Gesellschaft.

Rosenberg, Patrick (2016). *Bitcoin und Blockchain*. Berlin: Springer Verlag.

Stuart Haber, W. Scott Stornetta (1991). *How to Timestamp a Digital Document*.

Szabo, Nick (1997). „Formalizing and Securing Relationships on Public Networks". In: *First Monday* 2.

Glossar

Smart Contracts Smart Contracts verstehen sich als intelligente Verträge auf Software-Basis, die im Code hinterlegte Regeln überwachen und vordefinierte Aktionen ausführt, sobald ein bestimmter Event eintritt.

Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit eigenständig und ohne fremde Hilfe angefertigt habe. Textpassagen, die wörtlich oder dem Sinn nach auf Publikationen oder Vorträgen anderer Autoren beruhen, sind als solche kenntlich gemacht. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Hennigsdorf, den 20.02.2019

_____

Christoph Huschenhöfer