Eine Einführung in das Themengebiet der Kryptowährungen

Oliver Kattwinkel
Fachbereich Informatik
Hochschule Bonn-Rhein-Sieg
Sankt Augustin, 15. Januar 2018
oliver.kattwinkel@smail.inf.h-brs.de

***Abstract*—Das Ziel dieser Arbeit ist es, dem Leser eine Einführung in das Themengebiet der Kryptowährungen zu ermöglichen. Dafür wird erläutert, aus welchen grundlegenden Bestandteilen dezentrale Kryptowährungen bestehen und wie sie funktionieren. Um eine Verständnisgrundlage zu bilden, werden dafür zunächst technologische sowie sicherheitsrelevante Konzepte thematisiert. Neben diesen Grundlagen folgen im weiteren Verlauf ausgewählte Aspekte und Funktionsweisen zur Vertiefung des Themas. Durch das damit erlangte Verständnis soll der Leser verschiedene Kryptowährungen und deren Anwendungsgebiete besser verstehen und bewerten können.**

1. Einleitung

1.1. Motivation

Der Handel von materiellen und immateriellen Gütern orientiert sich maßgeblich durch den einer Währung zugesprochenen und anerkannten Wert. Handel ohne Einsatz von Währungen ist aus heutiger Sicht kaum noch vorstellbar. Dies hängt mit der historischen Entwicklung früherer Währungsformen zusammen und liegt überwiegend daran, dass Währungen den Handel stark vereinfachen. Es ist weitaus angenehmer ein anerkanntes und beliebig skalierbares Tausch- und Zahlungsmittel als Gegenleistung für den Transfer von Waren und Dienstleistungen zu verwenden, als erneut auf Waren und Dienstleistungen zurückzugreifen, welche dann auch noch in ein adäquates Verhältnis übertragen werden müssen. Das für diesen Transfer verwendete anerkannte und skalierbare Tausch- und Zahlungsmittel ist aus Sicht des heutig üblichen Gebrauches Geld. Das Zahlungsmittel Geld besitzt wiederum seinen Wert durch eine damit verbundene Währung. Wenn also das Geld seinen Wert durch das Vertrauen in dessen zugrunde liegende Währung erhält, woher erhält dann eine Währung ihren Wert?

Grundlage einer stabilen und wertbehafteten Währung sind stabile wirtschaftliche Verhältnisse des der Währung umgebenden Währungsraumes. Dieser muss nicht ausschließlich aus nur einem Nationalstaat bestehen, sondern kann auch aus mehreren Mitgliedsstaaten eines Staatenverbundes wie bspw. die Europäische Union zusammengesetzt sein. Dadurch ist eine Währung innerhalb ihres Währungsraumes, welcher auf staatlicher Ebene festgelegt wird, ein anerkanntes Zahlungsmittel. Der Wert einer Währung ist folglich untrennbar von den währungspolitischen und somit auch wirtschaftspolitischen Entscheidungen eines Staates bzw. eines Staatenverbundes. Die Ausübung dieser währungspolitischen Entscheidungen und der damit einhergehenden Währungskontrolle erfolgt durch staatliche bzw. staatenübergreifende Zentralbanken. Diese Institutionen verfolgen als primäres Ziel die Geldwertstabilität des Währungsraumes zu wahren indem sie Zinshöhen steuern und die im Umlauf befindlichen Geldmengen regulieren. Es wirkt als könne eine Währung ohne Staat, somit folglich auch ohne auf staatlicher Ebene währungskontrollierender Institution, nicht existieren. Kann eine Währung, welche weder an zentraler Stelle definiert noch kontrolliert wird, überhaupt einen Wert besitzen?

Durch die vorangegangene Fragestellung wird deutlich, dass Währungsformen ohne zentrale und monopole Kontrollinstanz ein Problem besitzen. Woher soll eine Währung ihren Wert beziehen, wenn nicht durch das Vertrauen in eine zentrale währungskontrollierende Institution? Indem eine Währung keine zentrale Währungskontrolle benötigt. Um eine Währung von dieser Eigenschaft zu lösen muss nicht nur auf Zentralisierung verzichtet werden, sondern Dezentralisierung muss als maßgebende Haupteigenschaft gelten.

Ein dezentrales Währungsmodell hat die Absicht völlig ohne zentrale Kontrollinstanz zu funktionieren. Als direkte Konsequenz dieser Eigenschaft kann das Währungsmodell durch keine währungspolitisch aktive Zentralbank gesteuert werden. Für Geldwertstabilität muss innerhalb des Währungsmodells folglich mit anderen Mitteln gesorgt werden. Es kann im Gegensatz zu *normalen* Staatengeld auf einer endlichen Geldmenge basieren. Dies bewirkt Wertstabilität und hindert Inflation. Vergleichbar mit dem begrenzt verfügbaren Rohstoff Gold wird der Wert des Währungsmodells allein durch Angebot und Nachfrage bestimmt. Jedoch muss hierbei zwischen Warengeld und Fiatgeld unterschieden werden. Gold ist Warengeld und besitzt im Gegensatz zu Fiatgeld einen intrinsischen Wert. Es ist ein Edelmetall und besitzt wichtige physikalische Eigenschaften und benötigt dadurch kein wertschöpfendes Vertrauen. Das Geld des Währungsmodells hingegen ist Fiatgeld, welches auf das Vertrauen in eine Währung baut.

Durch Abwesenheit zentraler Währungskontrolle besitzt das Währungsmodell auch keinen speziellen Währungsraum. Ohne Währungsraum fallen staatliche Grenzen weg, wodurch theoretisch jeder über Staatsgrenzen hinweg eine solche staatenlose Währung uneingeschränkt nutzen kann. Jedoch ist nicht nur die zuvor genannte allgemeine Währungskontrolle per Definition ausgeschlossen, sondern auch diejenige, welche in einem bargeldlosen

Zahlungsprozess letztendlich die Transaktion zwischen zwei Parteien tätigt. Eine solche dritte verwaltende Partei, wie bspw. eine Geschäftsbank, ist mit dem Gedanken der Dezentralisierung nicht vereinbar, weil auch hier erneut zu viel Verantwortung auf einzelnen Knoten in einem Netzwerk aus Währungsnutzern liegt.

Um dem Anspruch der Dezentralisierung gerecht zu werden, dürfen also gar keine solcher Banken existieren. Doch mit welchen Mitteln werden dann bargeldlose Zahlungen bzw. Transaktionen durchgeführt und verwaltet? Um dieses Dilemma zu umgehen, besitzt jeder Währungsnutzer einen eigenen Zugang zu einem öffentlichen Transaktionsnetzwerk und verwaltet somit seine Transaktionen selbst. Folglich kann das Geld einer solchen Währung nicht physisch bzw. materiell zur Verfügung stehen, sondern kann nur als virtuelles Geld einer digitalen Währung existieren. Durch Ausschluss jeglicher Form der Zentralisierung besitzt das dezentrale Währungsmodell auch keinen *Single-Point-of-Failure*, welcher in diesem Zusammenhang eine nicht zu unterschätzende Gefahr darstellt.

Dennoch bleibt die Frage offen, woher das Währungsmodell sein Vertrauen und den daraus resultierenden Wert gewinnt. Dieses Vertrauen wird durch den abschließenden technologischen Aspekt geprägt. Das zuvor genannte Transaktionsnetzwerk ist ein öffentliches und transparentes Buchführungssystem mit hohem Maß an Transaktionssicherheit. Mathematische Gesetze und Beweisverfahren stellen die Korrektheit von Transaktionen sicher. Das System speichert alle Transaktionen frei zugänglich in sogenannten Blöcken und hängt alle bereits abgearbeiteten d. h. verifizierten Blöcke aneinander. Kontrolle über dieses System hat weder der Staat noch irgendeine zentrale Institution. Das System kontrolliert sich selbst indem die mehrheitliche Meinung aller Währungsnutzer einen allgemein anerkannten Konsens bildet. Dieses Blöcke verkettende System ist die namensgebende Technologie genannt *Blockchain* und das auf diese Blockchain basierende konstruierte Währungsmodell ist keine neue Erfindung sondern eine sogenannte kryptographische Währung, kurz *Kryptowährung*.[1] Zusammenfassend ist diese neue Art von Währung, allen voran die erste weltweit erfolgreiche dezentrale Kryptowährung *Bitcoin* [1], als Zahlungssystem digital, verteilt, fälschungs- und manipulationssicher und wird bereits in steigendem Umfang verwendet.

1.2. Zielsetzung und Aufbau

Das Ziel dieser Arbeit ist es, dem Leser eine Einführung in das Themengebiet der Kryptowährungen zu ermöglichen. Dafür werden zunächst technologische sowie sicherheitsrelevante Eigenschaften thematisiert, um eine Verständnisgrundlage für die zentralen Bestandteile dieses Themas zu bilden. Aufgrund der Vielfalt von derzeit mehr als 1300 unterschiedlichen Kryptowährungen bzw. Implementierungen [4] werden im Rahmen dieser Arbeit, um dem Zweck einer Einführung gerecht zu werden, zu großen Teilen nur diejenigen Konzepte dargestellt, auf welche die derzeit erfolgreichsten Kryptowährungen basieren. Verständnisunterstützend werden diese Konzepte insbesondere auf Basis der Implementierung von Bitcoin, der ersten und aktuell weltweit erfolgreichsten Kryptowährung mit einer Marktkapitalisierung von ca. 270 Milliarden USD [4], an geeigneten Stellen exemplarisch dargestellt. Zur Vertiefung des Themas folgen neben den technologischen und sicherheitsrelevanten Grundlagen ausgewählte Aspekte und Funktionsweisen von Kryptowährungen. Durch das damit erlangte Verständnis soll der Leser verschiedene Kryptowährungen und deren Anwendungsgebiete besser verstehen und bewerten können.

2. P2P-Netzwerk und Blockchain

Als Grundlage zur Dezentralisierung dient ein Peer-to-Peer-Netzwerk (P2P) auf Basis des Internets. Alle Netzwerkteilnehmer bilden in einem P2P-Netzwerk selbstständige Netzwerkknoten, welche Dienste sowohl konsumieren als auch zur Verfügungen stellen können. Datenbestände sind innerhalb des Netzwerks verteilt und teilweise redundant auf den Knoten gespeichert. Änderungen der Daten können Konsistenzverletzungen im Netzwerk durch abweichende Versionsstände hervorrufen. Im Rahmen von dezentralen Kryptowährungen dient ein solches Netzwerk der verteilten Verwaltung aller Transaktionsdaten durch ein öffentliches und transparentes Buchführungssystem. Daher ist es zwingend notwendig, dass propagierte Transaktionen von jedem Netzwerkteilnehmer ohne Konsistenzverletzungen anerkannt werden.

Zur Sicherstellung eines gemeinsamen Konsens unter allen Teilnehmern innerhalb des P2P-Netzwerks wird eine Blockchain genutzt. Eine Blockchain ist eine chronologische Aneinanderreihung bzw. Verkettung von gekapselten Daten innerhalb von Blöcken.[2] Ein geschlossener bzw. bestätigter und damit verifizierter Block wird mit einer Hashfunktion vor Veränderungen geschützt und mit dem Hashwert des vorherigen Blocks verbunden. Änderungen bereits bestätigter Blöcke bzw. Manipulationen der in Blöcken zusammengefassten Transaktionen sind, wie im weiteren Verlauf dieser Arbeit erläutert, durch verschiedene Konsensmechanismen ausgeschlossen [6]. Die Blockchain bildet durch ihre dezentrale Eigenschaft die Grundlage moderner Kryptowährungen.

3. Transaktionsabwicklung

In diesem Kapitel soll die Frage beantwortet werden, durch welche Mechanismen Transaktionen in Einheiten von Kryptowährungen abgewickelt werden. Wie in Kapitel 2 erläutert, ist auf der Blockchain jede einzelne Transaktion mit all ihren Eigenschaften öffentlich und transparent hinterlegt. Wie auch in anderen Währungsformen üblich besteht eine Transaktion dabei unter anderem aus den drei notwendigen Bestandteilen Sender, Empfänger und Betrag. Diese drei und weitere Bestandteile basieren bei Kryptowährungen jedoch auf völlig unterschiedlichen Konzepten. Ziel dieser Konzepte ist Realisierung von umfänglicher Transaktionssicherheit, sodass jede Transaktion autorisiert und nichtabstreitbar ist, nicht manipuliert wurde und anerkannt wird. Insbesondere die Begrifflichkeiten

1. Anzumerken ist hierbei, dass nicht jede dezentrale Kryptowährung auf einer Blockchain basieren muss. Alternativen sind z. B. *IOTA* [2] oder *Byteball* [3], welche auf einem gerichteten azyklischen Graphen (DAG) basieren.

2. Eine vollständige Ausarbeitung zum Thema Blockchain bildet [5].

Sender und *Empfänger* gelten dabei nur noch als Verständnis unterstützende Abstraktionen. Im Kern besteht eine Transaktionsabwicklung einer Kryptowährung aus Funktionen des der Mathematik zugeordneten Teilgebiets der asymmetrischen Kryptographie und wird im weiteren Verlauf dieses Kapitels in Einzelteilen erläutert.

3.1. Asymmetrische Kryptographie

Das erste Verfahren der asymmetrischen Kryptographie wurde in den 1970er Jahren entwickelt [7]. Die daraus resultierenden Public-Key-Verschlüsselungverfahren wurden über die Zeit hinsichtlich ihrer Sicherheit stark optimiert. Die dafür verwendeten mathematischen Funktionen besitzen die Eigenschaft praktisch irreversible zu sein, wodurch sie sehr einfach in die eine Richtung aber unmöglich in die rückwärtige Richtung berechnet werden können. Auf Basis dieser mathematischen Funktionen können mittels der Public-Key-Verschlüsselung digitale Geheimnisse und fälschungssichere digitale Signaturen erzeugt werden. Im Kontext von Kryptowährungen sind jedoch meist nur die Signaturen und nicht das Verschlüsseln von Daten relevant. Die für Signaturen verwendeten Schlüsselpaare, bestehend aus einem *Private* und *Public Key*, besitzen eine mathematische Beziehung, wodurch Nachrichten von einem Ersteller mit dem privaten Schlüssel digital signiert und mit dem öffentlichen Schlüssel anschließend durch den Empfänger oder dritte verifiziert werden können [8, S. 56f]. Dieses Schlüsselpaar, die daraus erzeugte Adresse und die damit erstellte Signatur werden in den folgenden Abschnitten genauer erläutert.

3.1.1. Private Key. Kurz gefasst ist ein Private Key lediglich eine zufällig ausgewählte geheime Nummer der Länge *n*. Diese Nummer könnte bereits mit nicht mehr als einer Münze, einem Stift und einem Stück Papier erstellt werden. Dafür würde die Münze n-mal geworfen und für jeden Wurf entsprechend mit null oder eins notiert. Da diese Variante sehr zeitaufwendig wäre, werden selbstverständlich Computer mit sicherer Entropiequelle zur Generierung von privaten Schlüsseln verwendet. Der Schlüssel ist insofern privat bzw. geheim, dass er nur von der Person welche ihn erstellt hat, gekannt werden darf. Denn es ist genau dieser Schlüssel, welcher zur Ausstellung der Signaturen verwendet wird und somit dem Besitzer uneingeschränkten Zugriff auf das Guthaben der damit verbundenen Adresse gibt.

Tabelle 1. BITCOIN PRIVATE-KEY-FORMATE

Format	Private Key
Hex	`268A2A761FFE6FBD8A32D0656D5E9BA9E1DA92F01E91F843926C8B5280C83AB8`
WIF	`5J7G2W2Py3hfNKovx848B2839PgfLN3xta8w1VYCpYhthxkJ4G7`
WIF-Compressed	`KxWdKd7ANNvUM8298J8nfDx4U384CTv5gdG1PAxjArwVDMgVwL1H`

Der Bitcoin Private Key besteht aus 256 Bits und kann folglich jede Zahl zwischen 1 und $2^{256} - 1$ annehmen [8, S. 58f]. Statt den Schlüssel mit 256 binären Zeichen abzubilden, wird er wie in Tabelle 1 veranschaulicht, entweder in hexadezimaler Notation mit 64 hexadezimalen Zeichen, als Base58Check-Kodierung im sogenannten *Wallet Import Format* (WIF) oder im WIF-Compressed Format mit ergänzendem `0x01` Suffix vor der angewandten Base58Check-Kodierung angegeben. Diese Kodierungen dienen zur Erhöhung der Lesbarkeit und reduzieren die Anzahl von Eingabefehlern. Anzumerken ist hierbei, dass das WIF-Compressed Format nicht selbst komprimiert ist, sondern zur Erzeugung von komprimierten Public Keys verwendet werden sollte und mit dem Suffix dafür gekennzeichnet ist [8, S. 70ff]. Welche Bedeutung dabei der Public Key hat, wird im folgenden Abschnitt erläutert.

3.1.2. Public Key. Wie bereits zuvor erwähnt, besitzen Private und Public Key eine mathematische Beziehung zueinander. In dieser Beziehung bildet der zufällig generierte Private Key den Ursprung zur irreversiblen Berechnung eines Public Keys. Im Gegensatz zum Private Key muss der Public Key nicht geheim gehalten werden, sondern kann öffentlich zur Verifizierung von den mit dem Private Key ausgestellten Signaturen verwendet werden. Daraus ergibt sich im Rahmen von Kryptowährungen, dass Transaktionen nur von dem Inhaber des privaten Schlüssels autorisiert bzw. signiert werden können. Diese Autorisierung kann anschließend durch den Empfänger oder dritte ohne Enthüllung des privaten Schlüssels sondern nur mittels des öffentlichen Schlüssels auf Gültigkeit geprüft und somit anerkannt werden. Im Falle von Bitcoin wird der Public Key *K* durch Elliptische-Kurven-Kryptographie auf Basis des diskreten Logarithmus berechnet. Dafür wird ein für alle Bitcoin-Nutzer festgelegter Punkt *G* auf einer elliptischen Kurve gewählt und mit dem Private Key *k* multipliziert [8, S. 60ff].

$$K = k * G$$

Aus dieser Berechnung folgt ein Public Key, welcher wie in Tabelle 2 abgebildet entweder aus 130 oder 66 hexadezimalen Zeichen besteht. Der Schlüssel ist dann entweder als reines oder komprimiertes hexadezimales Format abgebildet. Das Public Key Hex-Compressed Format wird aus dem zuvor erläuterten WIF-Compressed Format berechnet. Die eingeführten Kompressionen der Public Keys dienen zur Größenreduzierung der Transaktionsdaten und damit letztendlich zur Entlastung der Blockchain [8, S. 73f]. Doch neben der Funktion zur Verifizierung von Transaktionen besitzt der Public Key eine weitere Aufgabe.

Tabelle 2. BITCOIN PUBLIC-KEY-FORMATE

Format	Public Key
Hex	`04B057083E32D101B69D81BEB381CA873992F26E5DB5ADFFC54DE5E0E35113979F7DB405E428F43D145E245F57F788C151CF179C9D72C9DD644B7E4D7CF06748EB`
Hex-Compressed	`03B057083E32D101B69D81BEB381CA873992F26E5DB5ADFFC54DE5E0E35113979F`

3.1.3. Adresse. Als weitere Funktion bildet der Public Key die Grundlage zur Generierung einer Sender- bzw. Empfängeradresse. Jedoch gelten *Sender* und *Empfänger* dabei nur noch als Verständnis unterstützende Abstraktionen und bieten im Rahmen von Kryptowährungen ein

gewisses Maß an Anonymität.[3] Eine Adresse repräsentiert den Besitzer eines Schlüsselpaares und berechnet sich durch eine Hashfunktion aus dem Public Key (somit folglich auch indirekt aus dem Private Key).

Eine Hashfunktion bildet eine beliebige Eingabemenge irreversibel auf eine kleinere Zielmenge konstanter Größe ab. Identische Eingabedaten erzeugen immer den selben Hashwert und jede auch noch so geringe Änderung der Eingabedaten erzeugt dabei einen völlig anderen Hashwert. Solche Hashfunktionen werden im Rahmen von Kryptowährungen exzessiv verwendet und im weiteren Verlauf dieser Arbeit thematisiert.

Zur Berechnung einer Bitcoin-Adresse *A* werden zwei verschiedene Hashfunktionen hintereinander auf einen Public Key *K* ausgeführt. Die Algorithmen dieser Funktionen sind, wie in folgender Gleichung angegeben, der *Secure Hash Algorithm* (SHA-256) und der *RACE Integrity Primitives Evaluation Message Digest* (RIPEMD-160) [8, S. 64ff].

$$A = \mathrm{RIPEMD160}(\mathrm{SHA256}(K))$$

Abschließend wird jede Bitcoin-Adresse analog zur Base58Check-Kodierung zur Erhöhung der Lesbarkeit und Reduzierung von Fehlern kodiert. Wie in Tabelle 3 abgebildet, ist das Ergebnis eine mit eins beginnende Bitcoin-Adresse. Diese kann in Abhängigkeit von dem Public-Key-Format entweder unkomprimiert oder komprimiert sein. Das bedeutet, dass ein einzelner privater Schlüssel zwei verschiedene Public-Key-Formate erzeugen kann, welche wiederum zwei unterschiedlich Bitcoin-Adressen erzeugen. Ein Problem ist dies jedoch nicht, weil beide Bitcoin-Adressen aus dem selben Private Key stammen [8, S. 74f]. Wie zuvor erläutert, dienen die eingeführten Kompressionen der Public Keys zur Größenreduzierung der Transaktionsdaten und damit letztendlich zur Entlastung der Blockchain.

Tabelle 3. BITCOIN-ADRESSFORMATE

Format	Adresse
Uncompressed	`17xREU6jPwcb4ZEfNqRtA7GEhtcDPezhR5`
Compressed	`19ucDdtiM22Yk3fxs5PGfTuNnn29wybBgS`

3.1.4. Signatur. In den vorherigen Abschnitten wurde bereits grob erläutert wofür eine digitale Signatur benötigt und wie sie erstellt wird. Wie zuvor beschrieben ermöglichen Signaturen im Rahmen von Kryptowährungen eine umfängliche Transaktionssicherheit, durch welche Transaktionen autorisiert und nichtabstreitbar sind, nicht manipuliert wurden und anschließend auch anerkannt werden. Damit werden die drei Schutzziele Authentizität, Nichtabstreitbarkeit und Integrität erfüllt. Dies geschieht am Beispiel von Bitcoin durch den Signaturalgorithmus *Elliptic Curve Digital Signature Algorithm* (ECDSA) [8, S. 138f]. ECDSA basiert auf der zuvor im Kontext der Public-Key-Erzeugung erläuterten Elliptische-Kurven-Kryptographie und benötigt zur Berechnung der Signatur *Sig*, wie in folgender Gleichung angegeben, den Hashwert der Transaktionsdaten m und den Private Key k.

$$Sig = \mathrm{ECDSA}(\mathrm{Hash}(m), k)$$

Durch den Gebrauch von digitalen Signaturen ergibt sich, dass Transaktionen nur von dem Inhaber des Private Keys autorisiert bzw. signiert werden können. Im Gegensatz zum Private Key muss der Public Key nicht geheim gehalten werden, sondern kann öffentlich zur Verifizierung von den mit dem privaten Schlüssel ausgestellten Signaturen verwendet werden. Zur Verifizierung wird die Signatur, der Hashwert der Transaktionsdaten und der Public Key benötigt. Der Verifizierungsprozess resultiert mit Erfolg, wenn die Signatur gültig für den Hashwert und Schlüssel ist und bestätigt, dass nur der Besitzer des privaten Schlüssels die Signatur der Transaktion erzeugt haben kann [8, S. 139].

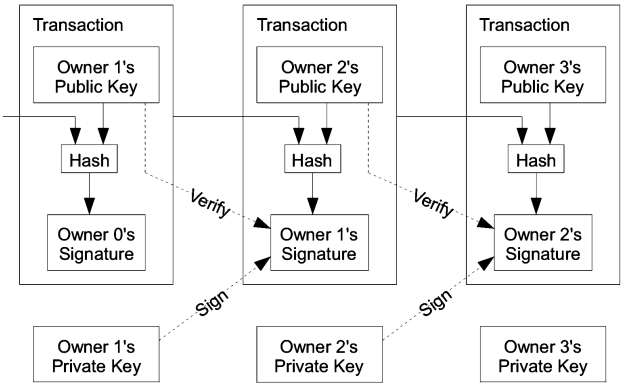

Abbildung 1. Transaktionsmodell [1, S. 2]

Wie in der in Abbildung 1 veranschaulichten Darstellung eines vereinfachten Transaktionsmodells, besteht der Hashwert der Transaktionsdaten aus einer vorherigen Transaktion und dem Public Key des Empfängers. Wenn nun *Owner 1* (Sender) eine Transaktion zu *Owner 2* (Empfänger) durchführt, ist diese vorherige Transaktion diejenige, in welcher *Owner 1's Public Key* als Empfänger vermerkt ist. Den öffentlichen Schlüssel des Empfängers bildet *Owner 2's Public Key*. Der Hashwert bildet zusammen mit *Owner 1's Private Key* die in der mittleren Transaktion aufgeführte Signatur *Owner 1's Signature*. Diese Signatur kann nun ohne Enthüllung des privaten Schlüssels, sondern nur mittels des öffentlichen Schlüssels von *Owner 1* verifiziert werden. Daraus geht hervor, dass nur *Owner 1* diese Transaktion hat ausstellen können. Selbiges gilt für die Transaktion von *Owner 2* zu *Owner 3* usw.

3.2. Transaktionsbetrag

Nachdem im vorherigen Abschnitt die Konzepte zur Realisierung von Transaktionssicherheit und die daraus resultierende Implementierung von Sender und Empfänger erläutert wurden, wird nun der Transaktionsbetrag als weiterer obligatorischer Bestandteil einer Transaktion behandelt. Dieser Betrag besteht bei Kryptowährungen nicht ausschließlich aus dem Wert, welcher ausgehend von dem Sender den Empfänger erreichen soll, sondern

3. Anzumerken ist hierbei, dass nicht jede Kryptowährung vollständig anonym sein kann und daher meist als pseudo-anonym gilt. Das gewünschte Maß an Anonymität kann durch sog. *Mixing Services* maßgeblich erhöht werden [13]. Auf Anonymität ausgerichtete Kryptowährungen sind bspw. *Monero* [9], *Zcash* [10] oder *Verge* [11].

auch aus verfügbaren Mitteln, welche von dem Sender zunächst konsumiert werden müssen. Zusätzlich bildet die Differenz aus verfügbaren und ausgehenden Werten dabei eine Gebühr, welche für die Abwicklung der Transaktion einbehalten wird. Diese Details rund um den Transaktionsbetrag im Rahmen der Transaktionsabwicklung werden in den folgenden Abschnitten erläutert.

3.2.1. Inputs und Outputs. Jede währungsbasierte Transaktion hat den Anspruch nur aus zur Verfügung stehenden Mitteln heraus Zahlungen zu realisieren. Folglich muss eine Transaktion durch entsprechendes Guthaben des Senders gedeckt sein. Wann eine Transaktion gedeckt ist, wird bei Kryptowährungen nicht durch eine verwaltende Institution entschieden, sondern durch die Blockchain, welche jede einzelne Transaktion mit all ihren Eigenschaften transparent hinterlegt.

Am Beispiel von Bitcoin geschieht dies durch sogenannte *Inputs* (Eingangsadressen) und *Outputs* (Ausgangsadressen). Inputs gehen als Grundlage in eine neue Transaktion ein und bilden das für den Transaktionsbetrag konsumierbare Guthaben des Senders. Das Gesamtkapital eines Senders ist daher die Summe aller seiner Inputs. Outputs mindern das Guthaben und bilden die Zahlungsanweisung zu Gunsten eines oder mehrerer Empfänger. Folglich sind alle verfügbaren Inputs bereits empfangene Outputs aus vorherigen Transaktionen [8, S. 123].

Die zur Verfügung stehenden Inputs eines Senders werden aus dem durch die Blockchain ablesbaren Transaktionsfluss ermittelt. Dazu wird jedes zuvor empfangene Output verwendet, welches sich über die entsprechenden Schlüssel bzw. den Private Key konsumieren lässt. Diese und weitere Aufgaben übernimmt ein sogenanntes *Wallet* (digitale Geldbörse), welches in Kapitel 5 erläutert wird. Wenn bekannt ist welche Menge an Inputs dem Sender zur Verfügung stehen, können diese im Rahmen der Transaktion konsumiert und anschließend ausgegeben werden.

Abhängig vom angestrebten Transaktionsbetrag ist anzumerken, dass die Menge der Inputs innerhalb einer Transaktion variiert und das Wallet meist mehrere Inputs bündelt, um ein ausreichend hohes Guthaben zu erzeugen. Durch die Tatsache, dass Inputs diskrete und unteilbare Einheiten sind und somit nur als Ganzes verbraucht werden können, muss mit einer Art *Wechselgeld* (vgl. Bargeld) gearbeitet werden. Dies geschieht indem neben der Adresse der Empfänger auch die eigene Adresse als Output in die Transaktion eingetragen wird.

Tabelle 4. BITCOIN TRANSAKTIONSBETRAG

Art	Adresse	Betrag
Inputs	`19ucDdtiM2...nn29wybBgS`	1,000 BTC
$\sum$		1,000 BTC
Outputs	`1KrxGPMcsX...3ahbunPBZD`	0,200 BTC
	`19ucDdtiM2...nn29wybBgS`	0,795 BTC
$\sum$		0,995 BTC
Gebühr		0,005 BTC
Gesendet		0,200 BTC
Gesamt		0,205 BTC

Wie in Tabelle 4 beispielhaft dargestellt, besteht eine Transaktion von 0,200 BTC aus einem Input der Größe 1,000 BTC. Das Input ist der Adresse `19ucDdtiM2...` zugeordnet und kann daher nur von dem Inhaber des zugehörigen Private Keys konsumiert werden. Der zu zahlende Betrag von 0,200 BTC findet sich unter Outputs und wird an den Empfänger mit der Adresse `1KrxGPMcsX...` gesendet. Weil die Summe der Inputs den zu zahlenden Betrag überschreiten, muss die Transaktion die Differenz der Beträge als Wechselgeld zurück an eine Adresse des Senders ermöglichen. Diese Adresse ist in diesem Beispiel identisch mit der Adresse des Inputs und daher folglich auch in Kontrolle des Senders. Jedoch beträgt dieses Wechselgeld nicht die zu erwartenden Differenz von 0,800 BTC (1,000 BTC - 0,200 BTC), sondern den um 0,005 BTC geringeren Betrag von 0,795 BTC. Dies liegt daran, dass der Sender einer Transaktion auch immer die Transaktionsgebühr zu zahlen hat und ihm diese in diesem Beispiel direkt vom Wechselgeld abgezogen wird. Die Summe der Outputs beträgt somit 0,995 BTC. Dieser Berechnungsprozess wird von der Wallet Software automatisch durchgeführt. Der Sender muss dabei nur die Empfängeradresse, den zu zahlenden Betrag und die Gebühr wählen. Welche Bedeutung die angesprochene Transaktionsgebühr dabei hat, wird im folgenden Abschnitt erläutert.

3.2.2. Transaktionsgebühr. Wie im vorherigen Abschnitt dargestellt, besitzt jede Transaktion eine Transaktionsgebühr. Diese hat der Sender zu entrichten indem er zu jedem zu zahlenden Betrag eine Gebühr addiert. Der zu zahlende Gesamtbetrag liegt, wie beispielhaft in Tabelle 4 veranschaulicht, somit bei 0,205 BTC. Obwohl eine Wallet Software dem Sender die Möglichkeit zur Anpassung der Gebühr überlässt, entsteht die Gebühr nicht durch einen zuvor gewählten Wert, sondern durch die in der folgenden Gleichung angegebenen Differenz der Summe aller Inputs zu der Summe aller Outputs [8, S. 129f].

$$\text{Transaktionsgebuehr} = \sum(\text{Inputs}) - \sum(\text{Outputs})$$

Es ist zwingend notwendig das o. g. Wechselgeld als Output anzugeben sobald die Summe der Inputs den gewünschten Zahlungsbetrag überschreitet. Sonst könnte ein sogenannter *Miner*, der Transaktionen in Blöcke fasst und dafür mit einem kleinen Betrag entlohnt wird, die gesamte Differenz als Transaktionsgebühr einbeziehen. Neben diesem Prozess, welcher in Kapitel 4 weiter erläutert wird, ist die Sicherheit ein weiterer Grund für die Verwendung von Transaktionsgebühren. Durch die Gebühren ist es finanziell enorm erschwert das Netzwerk mit Transaktionen zu fluten. Somit gelten Transaktionsgebühren bei Kryptowährung auch als Schutz gegen *Denial-of-Service* (DOS) Angriffe [8, S. 126f].

4. Mining

Nachdem im Kapitel 3 Transaktionen, deren sicherheitsrelevante Aspekte und weitere essentielle Bestandteile erläutert wurden, soll in diesem Kapitel die Frage beantwortet werden, durch welchen Mechanismus Transaktionen ihre Gültigkeit erhalten und warum es lukrativ sein kann, die für diesen Prozess benötigten Ressourcen bereitzustellen. Transaktionsgebühren werden an transaktionsabwickelnde Miner zur Entlohnung für den Rechenaufwand zur Integration der Transaktionen in einen neuen Block der Blockchain ausgeschüttet. Neben den

Transaktionsgebühren erhält ein Miner durch die zur Verfügung gestellte Rechenleistung eine aufwandsentschädigende Neuemission der verarbeiteten Kryptowährung als weitere Belohnung. Analog zum Goldschürfen nennt sich dieser ebenfalls auf einen begrenzt verfügbaren *Rohstoff* basierender Prozess *Mining*.

4.1. Funktionsweise

Dauerhaft fließen neue Transaktionen in das Netzwerk einer Kryptowährung ein. Im Falle von Bitcoin sind dies aktuell ca. 300.000 bestätigte Transaktionen pro Tag [12]. Doch bevor Transaktionen als bestätigt gelten, werden diese zunächst in einem sogenannten *Memory Pool*, kurz Mempool, gesammelt. Dort angekommen sind sie dem Netzwerk zwar bekannt, aber noch nicht durch Integration in einen Block der Blockchain bestätigt. Zur Bestätigung der Transaktionen werden die profitabelsten Transaktionen, d. h. diejenigen mit höchster Transaktionsgebühr, priorisiert aus dem Mempool ausgewählt und in einem neuen Block gesammelt. Die Menge an ausgewählten Transaktion ist dabei durch die Blockgöße begrenzt und beträgt bei Bitcoin aus Sicherheitsgründen 1 MB [13] [14]. Der Block gilt jedoch zunächst als unbestätigt und muss anschließend durch den Prozess des Minings von allen Minern bestätigt werden. Das Mining dient als Mechanismus, um innerhalb des P2P-Netzwerks einen gemeinsamen Konsens unter allen Netzwerkteilnehmern zu erzielen.

Am Beispiel von Bitcoin wird dieser Prozess durch zwei unterschiedliche Schritte durchgeführt. Zum einen ist dies die Verifizierung aller im Block befindlichen Transaktionen durch ein gemeinsames Konsensregelwerk, durch welches fehlerhafte Transaktionen als ungültig erklärt und abgelehnt werden. Und zum anderen ist dies die Berechnung einer komplex zu lösenden Aufgabe, welche eine starke Asymmetrie zwischen dem Aufwand zum Erzeugen einer zulässigen Lösung gegenüber dem Aufwand zum Überprüfen einer bereits gefundenen Lösung aufweist und in jedem Block unterschiedlich ist [6]. Alle Miner beteiligen sich zeitgleich an der Suche nach dieser Lösung und führen den Wettkampf wiederholt solange aus, bis eine gültige Lösung für den aktuellen Block gefunden ist. Derjenige Miner, dem dies gelingt, erhält sowohl alle Transaktionsgebühren innerhalb des geschlossenen Blockes sowie eine zusätzliche aufwandsentschädigende Neuemission als Belohnung und treibt so die Aktualisierung der Blockchain voran [8, S. 26ff].

4.1.1. Algorithmus. Der globale Wettkampf der Bitcoin Miner besteht aus der Anwendung einer irreversiblen Hashfunktion zur Berechnung eines streng definierten Hashwerts. Die Berechnung eines gültigen Hashwerts erfordert ein gewaltiges Maß an Rechenkapazität. Aktuell besitzt das Bitcoin-Netzwerk eine Hashrate von ca. 14 EH/s [15]. Das bedeutet, dass ca. 14.000 Billiarden ($14 * 10^{18}$) Berechnungen von Hashwerten pro Sekunde durchgeführt werden. Jede einzelne dieser Berechnungen erfolgt durch einen sogenannten *Proof-of-Work* (POW) Algorithmus, welcher sicherstellt, dass durch genügend Zeit und Rechenleistung ein Block geschlossen und damit als gültig erklärt werden darf und gilt damit als Nachweis für die geleistete Arbeit.

Anzumerken ist, dass Mining auch ohne Arbeitsnachweis funktionieren kann. Die Wahrscheinlichkeit einen Block erfolgreich zu minen, ist bei POW durch den Anteil der Rechenkapazität im Netzwerk bedingt. Eine weiterer Konsensmechanismus ist bspw. *Proof-of-Stake* (POS). Durch POS ist der Anteil der Einheiten einer Kryptowährung im Netzwerk ausschlaggebend für die Wahrscheinlichkeit einen Block zu minen [16].[4]

Der durch den POW Algorithmus berechnete Hashwert, erfolgt bei Bitcoin auf Basis der SHA-256 Hashfunktion und erhält folgende drei Eingabewerte, welche wie in Abbildung 2 vereinfacht dargestellt, den sogenannten *Block Header* bilden. Der erste Wert ist ein Hashwert aller Transaktionsdaten, welcher mit Hilfe eines sogenannten Hashbaums berechnet wird. Hiermit wird sichergestellt, dass Transaktionen nicht manipuliert werden können nachdem sie durch Schließung des Blocks bestätigt sind [13].

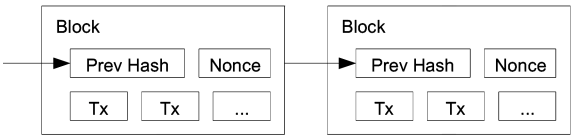

Abbildung 2. Proof-of-Work Mining [1, S. 3]

Der zweite Wert ist der Hashwert des vorherigen Blocks. Wie in Kaptitel 2 beschrieben, sind alle Blöcke durch ihren Hashwert miteinander verkettet. Damit werden durch den POW Algorithmus zusätzlich alle vorherigen Blöcke weiter abgesichert. Änderungen in vorherigen Blöcken würden weitere Änderungen in folgenden Blöcken erzeugen. Folglich müssten alle Blöcke neu berechnet werden. Der dafür benötigte Rechenaufwand steigert sich exponentiell und reduziert somit das Risiko einer Blockmanipulation wie bspw. Rückabwicklungen von Transaktionen [17]. Daher gelten Transaktionen offiziell nach dem fünften darauf folgendem Block als unumkehrbar und vollständig bestätigt [18].

Der dritte Eingabewert der SHA-256 Hashfunktion ist eine sogenannte *Nonce*. Die Nonce hat eine Größe von 32 Bit und dient dem Zweck zur Anpassung der Eingabewerte ohne die zuvor genannten Eingabewerte ändern zu müssen. Eine Änderung des Hashwerts der Transaktionsdaten oder des Hashwerts des vorherigen Blocks ist ohne Verletzung der geforderten Konzepte nicht möglich. Daher gelten sie als unveränderliche Eingabewerte. Das Ziel ist, dass der aus dem Block Header produzierte Hashwert der SHA-256 Hashfunktion kleiner oder gleich einem streng definierten Schwellenwert ist. Dafür wird die Nonce solange inkrementiert bis der Hashwert dem Schwellenwert unterliegt. Der Schwellenwert legt fest mit wie vielen Nullen der berechnete Hashwert beginnen muss und definiert die sogenannte *Mining Difficulty* (Schwierigkeitsgrad des Minings).

Die Mining Difficulty ist als künstlicher Schwierigkeitsgrad ein variables Maß und passt sich alle 2016 Blöcke (d. h. alle zwei Wochen) selbst an, sodass die durchschnittliche Berechnungszeit pro Block bei zehn Minuten liegt. Dieser Vorgang ist zwingend notwendig, weil die Rechenkapazität des Bitcoin-Netzwerks von der

4. Weitere Konsensmechanismen können aus [5] entnommen werden.

Rechenleistung der Miner abhängig ist und somit schwanken kann. So kann durch das Hinzukommen weiterer Miner die Rechenkapazität des Netzwerks steigen und die Berechnungszeit pro Block sinken. Um dies zu verhindern wird der Schwierigkeitsgrad zur Berechnung des geforderten Hashwerts durch den Schwellenwert angepasst, wodurch die festgelegte Zeitspanne von zehn Minuten weiter gewährleistet werden kann [19].

Als Beispiel für diesen Vorgang eignet sich der Vergleich mit einem Sudoku-Rätsel. Wenn eine einzelne Person in durchschnittlich zehn Minuten ein neun mal neun großes Rätsel löst, dann können statistisch betrachtet mehrere Personen dieses Rätsel in weniger Zeit lösen. Um nun die geforderten zehn Minuten weiterhin einzuhalten, kann das Rätsel um weitere Zeilen und Spalten erweitert und somit beliebig erschwert werden. Diese variabel gesteuerte Schwierigkeit entspricht der Mining Difficulty und passt sich an der Menge der zur einer Lösung eines Problems verwendeten Ressourcen an. Eine weitere Gemeinsamkeit ist, dass berechnete Lösungen einfach zu verifizieren sind, obwohl das Problem asymmetrisch schwierig zu lösen ist [8, S. 26f].

4.1.2. Block Reward. Alle Miner konkurrieren bei der Berechnung eines neuen Blocks miteinander. Sie beteiligen sich zeitgleich an der Suche nach einer gültigen Lösung und führen den globalen Wettkampf wiederholt solange aus, bis ein korrekter Hashwert zur Schließung des Blocks gefunden ist. Derjenige Miner dem dies gelingt, erhält sowohl alle Transaktionsgebühren innerhalb des geschlossenen Blocks sowie eine zusätzliche aufwandsentschädigende Neuemission, der sogenannte *Block* bzw. *Coinbase Reward*, als Belohnung. Diese Neuemissionen sind Einheiten einer endlichen Kryptowährung. Folglich können sie nicht unbegrenzt zur Verfügung gestellt werden.

Bitcoin realisiert die begrenzte Verfügbarkeit, indem sich die Menge der ausgeschütteten Bitcoins alle 210.000 Blöcke (d. h. ca. alle vier Jahre) durch das sogenannte *Bitcoin Halving* halbiert [19] [21]. Folglich wird sich die Gesamtmenge aller Bitcoins an einen nicht überschreitbaren Wert annähern, welcher bei 21.000.000 Bitcoins liegt. Die kleinste ausgeschüttete Neuemission wird bei einer Menge von 10^{-8} Bitcoins liegen. Dieser Wert, ein sogenannter *Satoshi*, entspricht der kleinsten Bitcoin-Einheit. Nach diesem Zeitpunkt entfällt der Block Reward und Miner werden nur noch durch die Transaktionsgebühren entlohnt [13].

Mit dem Anreizsystem auf Basis des Wettkampfs um den Block Reward wird das Mining, das die Transaktionsabwicklung aufrecht erhält, lukrativ belohnt. Die steigende Zunahme der Rechenleistung und der damit wachsenden Schwierigkeitsgrad zur Berechnung eines Blocks ist dem Umstand des hohen finanziellen Wertes dieser Belohnung geschuldet. Derzeit liegt der Block Reward bei einer Menge von 12,5 Bitcoins und entspricht bei einem Kurs von ca. 16.000 USD pro Bitcoin einem Wert von ca. 200.000 USD [4]. Die Höhe des Block Rewards und die Menge der Transaktionsgebühren gepaart mit dem Wert einer Kryptowährung sind abzüglich der Betriebskosten die maßgeblichen Faktoren für die Lukrativität des Minings.

4.2. Hardware und Anwendung

Der globale Wettkampf des Minings führt zu hoher Nachfrage an effizienter Mining Hardware. Am Beispiel von Bitcoin ist der durch die Zunahme der Rechenleistung vorangetriebene Wandel der eingesetzten Hardware deutlich zu erkennen. Bitcoin Mining kann in Abhängigkeit des Schwierigkeitsgrades auch mit relativ wenig Rechenleistung betrieben werden. Vor dem Jahr 2010 war es noch finanziell lukrativ mit handelsüblichen CPUs zu minen. Durch Zunahme der Rechenkapazität des Netzwerks waren CPUs bereits im folgenden Jahr nicht mehr effizient genug und verbrauchten mehr Kosten an Energie als sie durch Mining der Kryptowährung erzeugten [19]. Es folgte der Einsatz von GPUs, welche für diesen Verwendungszweck wesentlich schneller und effizienter arbeiteten. Doch diese wurden ebenfalls rasch durch sogenannte *Field Programmable Gate Arrays* (FPGAs) abgelöst. Ein Mining FPGA ist ein integrierter Schaltkreis mit logischer Schaltung zur Berechnung des geforderten Hashwerts. Dessen Leistungsfähigkeit ist insbesondere durch geringen Stromverbrauch und hohen Taktzyklus definiert. Dadurch sind FPGAs weitaus effizienter als GPUs und unvergleichbar mit CPUs. Doch auch diese Technologie wurde durch stetig steigende Rechenleistung des Netzwerks zügig abgelöst.

Bereits im Jahr 2013 wurden die ersten *Application Specific Integrated Circuits* (ASICs) veröffentlicht und erzeugten einen weiteren massiven Zuwachs der Rechenkapazität. Die ersten Mining ASICs konnten mehr Rechenleistung erzeugen als das gesamte Netzwerk drei Jahre zuvor besaß [8, S. 247]. Ein Mining ASIC ist ebenfalls ein integrierter Schaltkreis, jedoch nicht mit logischer sondern elektronischer Schaltung zur Berechnung des geforderten Hashwerts. Die Vorteile gegenüber einem FPGA sind noch höhere Taktraten und damit eine weiter gesteigerte Effizienz durch Kosten- und Leitungsoptimierung. ASICs sind die derzeit effizienteste Bitcoin Mining Hardware [19]. Ein weiterer Sprung der Rechenleistung, wie er in der Vergangenheit statt fand, ist nicht zu erwarten. Die Integrationsdichte der industrielle gefertigten Hardware hat bereits ein Maß erreicht, welches durch das mooresche Gesetz begrenzt wird [8, S. 249]. Neben der Entwicklung der Hardware sind zusätzlich verschiedene Arten der Anwendung des Minings entstanden, welche in folgenden Absätzen erläutert werden.

Zu dem Zeitpunkt, als sich Mining noch durch CPUs und GPUs lohnte, konnte jeder Miner als einzelner Knoten im Netzwerk selbstständig Minen. Diese sogenannten *Solo Miner* verkörpern den Grundgedanken der Dezentralisierung der Kryptowährung Bitcoin. Durch sie ist das Maß der Dezentralisierung maximiert und Rechenleistung innerhalb des Netzwerks heterogen verteilt. Dezentralisierung schützt vor fehlerhaften Daten, denn jeder Miner kann Blockinhalte manipulieren und anschließend im Netzwerk propagieren. Wenn die Mehrheit der Miner die korrupten Daten als fehlerhaft anerkennt, würden sie durch das Netzwerk abgelehnt. Wenn jedoch mehr als 50% der Miner diese Inhalte als korrekt bezeichnen, gelten sie als gültig und werden fest in die Blockchain integriert. Folglich könnte ein einzelner Miner durch genügend konzentrierte Rechenleistung einen Angriff durchführen und bspw. Transaktionsdaten zu seinen Gunsten manipulie-

ren und Guthaben mehrfach ausgeben. Damit würde er das sogenannte *Double Spending* durch eine *51%-Attacke* durchführen, welche durch genügend Dezentralisierung im P2P-Netzwerk verhindert werden kann [13] [20].

Wie in Abschnitt 4.1.2 erläutert, erhält ein Miner nach erfolgreicher Berechnung eines Blocks eine Belohnung. Ein Solo Miner kann diese Belohnung vollständig für sich behalten. Doch im Zuge der Entwicklung der Hardware und dem Anstieg der Rechenleistung haben Solo Miner die Möglichkeit verloren, sich in dem globalen Wettkampf zu behaupten. Der Anteil der Rechenleistung eines Solo Miners ist im Verhältnis zur Gesamtkapazität des Netzwerks so gering, dass die Wahrscheinlichkeit zur Berechnung eines Blocks eher auf einen unregelmäßigen Glücksspiel basierten Zufall basiert. Auch die schnellsten ASIC Miner, welche immerhin ein Verhältnis von $1/1.000.000$ erreichen[5], können nicht mit kommerziellen Mining-Betrieben mithalten.

Aus diesem Grund haben sich sogenannte *Mining Pools* entwickelt, bei denen sich mehrere Miner zusammenschließen, um Rechenleistung zu bündeln und Erträge zu teilen. Dafür wird die Mining Hardware einzelner Miner mit dem Pool verbunden und intern synchronisiert. Dieser gemeinsame Prozess des Minings führt zu einer regelmäßigeren aber auch geringeren Belohnung. Denn sofern ein Miner einen Block berechnet, erhält zunächst nicht der Miner sondern der Pool die Belohnung. Diese wird anschließend unter allen Minern im Pool anteilsmäßig zu der zur Verfügung gestellten Rechenleistung aufgeteilt und ausgezahlt [8, S. 250f]. Durch Pool Mining kann mit festen Einnahmen innerhalb einer Kryptowährung kalkuliert werden. Zur Deckung der laufenden Betriebskosten der Hardware eignet sich diese Art des Minings besonders gut und hat das Solo Mining nahezu verdrängt.

Neben dem auf den Besitzt von Hardware basierenden Mining, existiert noch eine weitere Art des Minings. Bei dem sogenannten *Cloud Mining* investieren Anleger in Mining-Verträge und mieten externe Hardware. Kunden erwerben vertraglich festgelegt, meist über einen gewissen Zeitraum, eine bestimmte Menge an Rechenleistung. Der dadurch generierte Ertrag wird durch die Cloud-Mining-Anbieter regelmäßig separat an die einzelnen Kunden ausgezahlt. Vorteilhaft ist bei dieser Art des Minings, dass finanziellen Hürden gering sind, weil keine teure Hardware gekauft und betrieben werden muss. Anbieter verwenden jedoch häufig untransparente Mining-Systeme und besitzen jederzeit das Recht, Verträge vorzeitig kündigen und Auszahlungen blockieren zu dürfen [23].

5. Wallets

Jedes beliebige Zahlungssystem benötigt eine Möglichkeit zur Aufbewahrung und Verwaltung von persönlichem Guthaben. Auf Basis einer physischen bzw. materiellen Währung ist dies nicht weiter schwierig und wird z. B. durch eine Geldbörse oder ein Bankkonto realisiert. Eine digitale Kryptowährung bestehend aus virtuellem Geld, nutzt diese Konzepte als Abstraktion und verwendet zur Verwaltung des Guthabens ein sogenanntes *Wallet* (digitale Geldbörse). Ein Wallet kontrolliert den Zugang zu dem verfügbaren Guthaben, indem es die aus Kapitel 3 erläuterten Schlüssel und Adressen verwaltet.

Am Beispiel von Bitcoin wird das zugrunde liegende Guthaben dabei nicht durch gespeicherte Einheiten einer Kryptowährung, sondern durch Abfrage nach konsumierbaren Inputs durch die Blockchain ermittelt. Wie in Abschnitt 3.2.1 erläutert, bilden die entsprechenden Schlüssel die notwendige Grundlage. Verständnisfördernd kann neben der Bezeichnung als Geldbörse daher ebenfalls von einem Schlüsselbund gesprochen werden. Außerdem übernimmt ein Wallet die Aufgabe Transaktionen zu signieren und diese im Netzwerk zu propagieren, wodurch Guthaben autorisiert ausgegeben bzw. transferiert werden kann [8, S. 93].

5.1. Kategorien

Die primäre Aufgabe eines Wallets ist die sichere Speicherung des Schlüsselmaterials. Die Private Keys innerhalb eines Wallets werden meist ausgehend durch einen sogenannten *Seed* (Samen) deterministisch berechnet. Der Seed ist eine zufällig generierte Zahl kombiniert mit weiteren Daten. Solche deterministischen Wallets besitzen die Möglichkeit allein durch den Seed wiederhergestellt zu werden [8, S.95ff]. Um Anwendern diese Backup-Funktionalität weiter zu vereinfachen und der nicht geringen Menge an bereits verlorenen Schlüsseln entgegen zu wirken, wurde zusätzlich der *Mnemonic Code BIP-39* Standard entwickelt [24]. Durch diesen Standard wird der Seed und damit auch das gesamte Schlüsselmaterial aus einer leicht ablesbaren nummerierten Sequenz von natürlichsprachlichen Wörtern gebildet [17]. Diese Eigenschaft teilen sich die meisten Wallets. Dennoch gibt es unterschiedliche Wallet-Typen, welche in den folgenden Abschnitten zusammengefasst in drei Hauptkategorien erläutert werden.

5.1.1. Software Wallets. In die Kategorie der *Software Wallets* fallen die auf der eigenen Hardware, wie bspw. Desktop Computer oder Smartphone, installierbaren Wallets. Analog der Anwendung nennen sie sich *Desktop* und *Mobile Wallet* und verwalten die Schlüssel auf den jeweiligen Endgeräten. Im Falle von Bitcoin propagieren sie Transaktionen meist als sogenanntes *Full Service Wallet* mit direkter Anbindung an das P2P-Netzwerk. Damit basieren sie entweder auf vollwertigen Netzwerkknoten, den sogenannten *Full Nodes*, welche die gesamte Blockchain herunterladen und redundant speichern. Oder auf dem alternativen Verfahren genannt *Simplified Payment Verification* (SPV), durch welches anstatt alle Blockdaten nur die Block Header heruntergeladen werden, um die Datenmenge möglichst gering zu halten [1, S. 5] [17]. Insbesondere für auf Smartphone betriebenen Mobile Wallets, welche meist von einem begrenzt verfügbarem Datenvolumen abhängig sind, eignet sich letzteres.

Für den schnellen mobilen Zahlungseinsatz sind Mobile Wallets unersetzbar. Durch Zugriff auf Smartphone-Komponenten wie Kamera oder NFC-Schnittstelle können sie Transaktionen autorisieren ohne die Notwendigkeit manuelle Eingaben tätigen zu müssen [25]. Wie in Abbildung 3 beispielhaft dargestellt, können QR-Codes

5. 14 TH/s ASIC SHA-256 Miner (*Bitmain Technologies Antminer S9*) [22] im Verhältnis zur gesamten Rechenleistung des Bitcoin-Netzwerks mit 14 EH/s (14.000.000 TH/s) [15]

Abbildung 3. QR-Code einer Bitcoin-Adresse

zur Kodierung von Transaktionsdaten wie bspw. Empfängeradresse oder Betrag genutzt werden. Mobile Wallets können diese QR-Codes einscannen und bei Bedarf sofort den Zahlungsprozess einleiten.

5.1.2. Online Wallets. Webbasierte Wallets, kurz *Web Wallets*, sind vergleichbar mit Software Wallets, welche nicht auf eigener sondern externer Hardware betrieben werden. Sie fallen in die Kategorie der *Online Wallets*, weil die Transaktionsabwicklung dabei durch einen Server des Anbieters online erfolgt. Über ein Benutzerkonto kann auf verfügbares Guthaben durch das Internet zugegriffen werden. Diese Wallets besitzen ein hohes Maß an Verfügbarkeit weil sie durch das Internet von überall aus erreichbar sind. Dies führt jedoch auch zu dem durch diverse Angriffe mehrfach bestätigten Nachteil, besonders verwundbar zu sein [24].

Zusätzlich ist bei Online Wallets anzumerken, dass die Verwaltung des gesamten Schlüsselmaterials allein durch den Anbieter erfolgt und somit kein physischer Besitz besteht. Neben klassischen Web Wallets, welche lediglich Guthaben aufbewahren und verwalten, gehören im Rahmen von Kryptowährungen Handelsplätze, Mining-Pool- und Cloud-Mining-Anbieter ebenfalls in die Kategorie der Online Wallets.

5.1.3. Hardware Wallets. Die sicherste Kategorie zur Speicherung des Schlüsselmaterials bilden die *Hardware Wallets* ohne Internetanbindung durch sogenannte *Cold Storage*. Dazu gehören Hochsicherheitsgeräte mit besonderem Fokus auf Malware-Resistenz. Dies wird dadurch realisiert, dass die Private Keys niemals das Gerät verlassen und Transaktionen ausschließlich intern in kontrollierter Umgebung signiert werden. Sie gelten daher auch als sogenannte *Signing Only Wallets*, welche lediglich Signaturen von Transaktionen erzeugen [17]. Die Trennung von Schlüsselmaterial und verwundbarer Umgebung, wie bspw. das Internet, reduziert das Diebstahlrisiko auf unsicheren bzw. nicht vertrauenswürdigen Systemen [24]. Diese Art von Wallets benötigen jedoch eine Schnittstelle zur Anbindung an das P2P-Netzwerk, um Transaktionen zu propagieren. Für diese Interaktion muss eine meist eingeschränkte Spezialform eines Software Wallets zusätzlich verwendet werden.

Tabelle 5. EINFACHSTE FORM EINES BITCOIN PAPER WALLETS

Adresse	`17xREU6jPwcb4ZEfNqRtA7GEhtcDPezhR5`
Private Key (WIF)	`5J7G2W2Py3hfNKovx848B2839PgfLN3xta 8w1VYCpYhthxkJ4G7`

Eine Sonderform der Hardware Wallets sind *Paper Wallets* oder jegliche Form der lokalen Aufbewahrung von Schlüsselmaterial. Paper Wallets können keine Transaktionen abwickeln und dienen daher ausschließlich dem Zweck, Schlüsselmaterial ohne Verwendung von Software offline zu sichern. Wie in Tabelle 5 veranschaulicht, besteht die einfachste Form eines Bitcoin Paper Wallets aus lediglich einem Private Key und einer daraus abgeleiteten Adresse. Solange ein Paper Wallet nur für den Währungsempfang genutzt wird und sicher erstellt wurde, ist es kein ausnutzbares Ziel für Cyberangriffe [25]. Sofern Guthaben ausgegeben werden muss, benötigt ein Paper Wallet ebenfalls eine Schnittstelle zur Anbindung an das P2P-Netzwerk um Transaktionen zu propagieren. Dafür können sowohl Software Wallets als auch Online Wallets mit Importfunktion für Private Keys verwendet werden. Die Erstellung sowie der Gebrauch von Paper Wallets ist jedoch nur erfahrenen Anwendern zu empfehlen [24].

6. Fazit und Ausblick

Mit dieser Arbeit wurde erläutert, aus welchen grundlegenden Bestandteilen dezentrale Kryptowährungen bestehen und wie sie funktionieren. Um eine Verständnisgrundlage zu bilden, wurden dafür zunächst technologische sowie sicherheitsrelevante Konzepte thematisiert. Neben diesen Grundlagen folgten zur Vertiefung des Themas ausgewählte Aspekte und Funktionsweisen von Kryptowährungen. Dafür wurden insbesondere die Eigenschaften von Bitcoin genutzt und an geeigneten Stellen exemplarisch dargestellt. Bitcoin ist die erste und aktuell weltweit erfolgreichste Kryptowährung und stellt durch ihre Konzepte die Grundlage vieler weiterer Kryptowährungen dar.

Kryptowährungen werden in steigendem Umfang verwendet. Das zeigt sich unter anderem durch die Kursentwicklungen vieler Kryptowährungen sowie durch eine gesamte Marktkapitalisierung von ca. 800 Milliarden USD [4]. Die ansteigende Verwendung basiert auf mehreren Faktoren. Dazu gehören bspw. zunehmende Akzeptanz und Interesse an staatenlosen dezentralen Währungen, wachsendes Vertrauen auf technologischer Ebene oder schlicht Kapitalmaximierung aus ökonomischer Sichtweise. Insbesondere letzteres führt durch Spekulationen zu ständigen Kursbewegungen und diskreditiert den Ruf von Kryptowährungen. Durch die hohe Lukrativität des Bitcoin Minings und der daraus folgenden Zunahme an Rechenkapazität und Energieverbrauch, ist in der Vergangenheit vermehrt Kritik an Proof-of-Work basierten Kryptowährungen aufgekommen. Das Problem ist dabei weniger das Anreizsystem auf Basis des Wettkampfs um den Block Reward, sondern eher ein Resultat von menschlicher Gier.

Neben Bitcoin existieren viele alternative Kryptowährungen mit teils stark unterschiedlichen Implementierungskonzepten und Anwendungsgebieten. Sie bieten als Zahlungsmittel großes Potential und basieren auf innovativen Technologien. Die dezentrale Plattform *Ethereum* mit der eigenen Kryptowährung *Ether* bietet durch ein verteiltes System die Möglichkeit, turingmächtige Programme auszuführen. Im Gegensatz zum klassischen Client-Server-Modell werden durch Ethereum die Programme, sogenannte *Smart Contracts* und *DApps*, innerhalb eines P2P-Netzwerks dezentral ausgeführt.[6] Systeme wie diese

6. Ein vollständige Ausarbeitung zum Thema Ethereum und Smart Contracts bildet [26].

schaffen neben der durch Kryptowährungen angestrebten Währungsunabhängigkeit neue Lösungen für bestehende Probleme.

Es bleibt daher spannend, inwieweit sich einzelne Kryptowährungen und deren Basistechnologien in einem aktuell unübersichtlichen Markt durchsetzen. Für dezentrale Kryptowährungen, welche in Zukunft als alltägliches Zahlungsmittel verwendet werden sollen, ist es notwendig aktuell aufkommende Probleme der Skalierbarkeit zu lösen. Dabei gilt jedoch zu beachten die grundlegende Eigenschaft der Dezentralisierung nicht zu verletzen. Insbesondere Bitcoin stößt derzeit immer wieder an eigene technische Kapazitätsgrenzen und bedarf gemäß des ursprünglich gewählten Leitgedankens, *purely Peer-to-Peer Electronic Cash* [1, S. 1], leistungsfähigen Weiterentwicklungen.

Literatur

[1] **Nakamoto, Satoshi**: *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, URL: https://bitcoin.org/bitcoin.pdf (Stand: 01.11.2017)

[2] **Popov, Serguei**: *The Tangle*, Version 1.3, 01.10.2017, URL: https://iota.org/IOTA_Whitepaper.pdf (Stand: 13.11.2017)

[3] **Churyumov, Anton**: *Byteball: A Decentralized System for Storage and Transfer of Value*, (o.J.), URL: https://byteball.org/Byteball.pdf (Stand: 13.11.2017)

[4] **CoinMarketCap**: *Cryptocurrency Market Capitalizations*, 07.01.2018, URL: https://coinmarketcap.com (Stand: 07.01.2018)

[5] **Kaucher, Alexander**: *Blockchain: Funktionsweise und Applikationsmöglichkeiten*, Hochschule Bonn-Rhein-Sieg, 2018

[6] **Bitkom**: *Blockchain Banking: Ein Leitfaden zum Ansatz des Distributed Ledger und Anwendungsszenarien*, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., 2016, URL: http://www.digitalestadt.org/bitkom/org/noindex/Publikationen/2016/Leitfaden/Blockchain/161104-LF-Blockchain-final-2.pdf (Stand: 28.12.2017)

[7] **Merkle, Ralph & Hellman, Martin**: *Hiding information and signatures in trapdoor knapsacks*, In: IEEE Transactions on Information Theory, Volume: 24, Issue: 5, Sep. 1978

[8] **Antonopoulos, Andreas**: *Mastering Bitcoin: Programming the Open Blockchain*, Second Edition, O'Reilly Media, 01.07.2017, ISBN: 978-1491954386

[9] **Monero Project**: *Monero*, (o. J.), URL: https://getmonero.org (Stand: 13.11.2017)

[10] **Zerocoin Electronic Coin Company**: *Zcash*, (o. J.), URL: https://z.cash (Stand: 13.11.2017)

[11] **Verge**: *Verge*, (o. J.), URL: https://vergecurrency.com/langs/de/ (Stand: 13.11.2017)

[12] **Blockchain Luxembourg S.A.**: *Confirmed Transactions Per Day*, (o. J.), URL: https://blockchain.info/de/charts/n-transactions (Stand: 27.12.2017)

[13] **Tschorsch, Florian & Scheuermann, Björn**: *Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies*, In: IEEE Communications Surveys & Tutorials, Vol. 18, Issue 3, S. 2084-2123, 02.03.2016, URL: http://ieeexplore.ieee.org/document/7423672 (Stand: 28.12.2017)

[14] **Bitcoin Wiki**: *Block*, 08.08.2014, URL: https://de.bitcoin.it/wiki/Block (Stand: 31.12.2017)

[15] **Blockchain Luxembourg S.A.**: *Hash Rate*, (o. J.), URL: https://blockchain.info/de/charts/hash-rate (Stand: 27.12.2017)

[16] **BTC-Echo**: *Was ist Proof-of-Stake?*, (o. J.), URL: https://www.btc-echo.de/tutorial/was-ist-proof-of-stake (Stand: 29.12.2017)

[17] **Bitcoin Project**: *Bitcoin Developer Guide*, (o. J.), URL: https://bitcoin.org/en/developer-guide (Stand: 30.12.2017)

[18] **Bitcoin Wiki**: *Erste Schritte*, 08.05.2016, URL: https://de.bitcoin.it/wiki/Erste_Schritte (Stand: 28.12.2017)

[19] **Bitcoin Wiki**: *Mining*, 22.10.2017, URL: https://en.bitcoin.it/wiki/Mining (Stand: 28.12.2017)

[20] **Bitcoin Wiki**: *Majority attack*, 10.08.2017, URL: https://en.bitcoin.it/wiki/Majority_attack (Stand: 28.12.2017)

[21] **Preuss, Mark**: *Bitcoin Block Halving – Das solltest du wissen*, BTC-Echo, 15.05.2016, URL: https://www.btc-echo.de/bitcoin-block-halving-faq (Stand: 29.12.2017)

[22] **Bitmain**: *Bitmain Antminer*, (o. J.), URL: https://shop.bitmain.com/main.htm?lang=en (Stand: 29.12.2017)

[23] **Kops, Max**: *Bitcoin Cloudmining – Was ist dran am Mythos?*, BTC-Echo, 02.06.2016, URL: https://www.btc-echo.de/geld-verdienen-mit-cloudmining-072016 (Stand: 29.12.2017)

[24] **Bitcoin Wiki**: *Storing bitcoins*, 29.12.2017, URL: https://en.bitcoin.it/wiki/Storing_bitcoins (Stand: 30.12.2017)

[25] **BTC-Echo**: *Digitale Währungen aufbewahren*, (o. J.), URL: https://www.btc-echo.de/tutorial/wallet-bitcoins-sicher-aufbewahren (Stand: 30.12.2017)

[26] **Müller, Rene**: *Ethereum und Smart Contracts*, Hochschule Bonn-Rhein-Sieg, 2018