Kryptowährungen

Einführung und praktische Ansätze

Noah Lehmann
noah.lehmann@hof-university.de
Hochschule für Angewandte Wissenschaften
Hof, Deutschland

ZUSAMMENFASSUNG

In einer Zeit, in der das Finanzsystem wiederholt stark inflationäre Tendenzen entwickelt und das Konzept *Web 3.0* immer mehr an Bedeutung gewinnt, bedarf es einer neuen Technologie, die durch die Ideen des *Web 3.0* die Probleme des Finanzsystems zu lösen versucht. Hierfür entwickelte die nach wie vor anonyme Entität Satoshi Nakamoto 2008 erstmals ein funktionierendes Konzept für eine Kryptowährung namens *Bitcoin*. *Bitcoin* dezentralisiert sein Transaktionssystem und eliminiert somit alle Mittelmänner. Dadurch entsteht ein über die sogenannte *Blockchain* abgesichertes Peer-to-Peer-Bargeld.

KEYWORDS

Kryptowährungen, Bitcoin, Blockchain, Konsens-Protokoll, Dezentralität

ACM Reference Format:
Noah Lehmann. 2021. Kryptowährungen: Einführung und praktische Ansätze. In *Proceedings of Hochschule für Angewandte Wissenschaften Hof, 06.12.2021 (Aktuelle Themen der IT-Sicherheit WS21/22).* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 EINFÜHRUNG

Aktuelle Entwicklungen der Finanzsysteme weltweit übersteigen die regulären Wachstumsraten weit und tendieren immer mehr in Richtung hoher Inflationen. Zudem kommen seit Jahren immer mehr Fälle gezielter Manipulationen von Währungen auf. Genau diese Feststellungen waren schon zu Beginn des 21 Jahrhunderts Grundlage der Diskussion über die Möglichkeit der Umsetzung von dezentralen, möglichst digitalen Währungen, teils zu Zeiten, in denen das Internet noch großenteils auf Informationsdarstellung limitiert war. Diese Phase des Internets wird heute als Web 1.0 bezeichnet, das vom heute immer noch aktuellen Web 2.0 abgelöst wurde. Das Konzept des Web 2.0 ist die Erweiterung des statischen Internets der Informationen im Web 1.0 um die Teilnahme seiner Nutzer. Jedoch wurde diese Flut neuer Informationen ebenfalls von Unternehmen genutzt, die diese Daten Sammeln, weiter nutzen und vermarkten wollen. Daraus entstanden ist ein stark zentralisiertes Internet, welches von wenigen großen Firmen betrieben und bestimmt wird - ganz wie das Finanzsystem. Aus dem Bedürfnis heraus, sich der Kontrolle zentraler Instanzen zu entziehen und die Verantwortung der betroffenen Systeme wieder den Nutzern anzueignen ist die Idee des sogenannten Web 3.0 entstanden, das als völlig dezentrales Internet beschrieben wird, in dem sämtlicher Einfluss den Nutzern statt einigen wenigen zentralen Instanzen zusteht.

In genau diesem Zug sind erste Ideen für digitale Währungen entstanden, welche später durch ihren Bezug zur Kryptografie als Kryptowährungen bezeichnet wurden. Um kurz einzuschränken, was genau die Idee einer Kryptowährung beinhaltet wird im Folgenden kurz eine Definition zitiert:

> Kryptowährungen sind digitale (Quasi-)Währungen mit einem meist dezentralen, stets verteilten und kryptografisch abgesicherten Zahlungssystem [1].

Auf die genaue Bedeutung der einzelnen Punkte soll in den folgenden Kapiteln genauer eingegangen werden, jedoch sollte die in diesem Kapitel kurz angedeutete Geschichte der Finanzsysteme genauer dargestellt werden, um die Gründe für die Entwicklung von Kryptowährungen besser verstehen zu können.

2 BEKANNTE FINANZSYSTEME

Um zu verstehen, warum das Konzept von Kryptowährungen relevant sein könnten, müssen zuerst bekannte und veraltete Währungen nach ihren Schwachstellen analysiert werden. Im Folgenden werden einige bekannte Währungen und Bezahlsysteme kurz erläutert.

2.1 Einfache Wertgegenstände

Das grundlegende Konzept des Bezahlens ist das Tauschen zweier Gegenstände, die den jeweiligen Beteiligten den gleichen Mehrwert bieten. Um sich jedoch nicht auf das Tauschen von Gütern zu beschränken wurden früh Wertgegenstände als Währung eingeführt, die einen festgelegten Wert symbolisiert. Diese Wertgegenstände mussten schwer reproduzierbar sein, um Fälschungen vermeiden zu können. Zudem mussten sie leicht transportabel sein, um im täglichen Gebrauch praktikabel zu bleiben. Das bat den Währungen einen Vorteil gegenüber dem einfachen Tausch von Waren. Um eine Bezahlung bestätigen zu können, mussten diese Wertgegenstände leicht verifizierbar sein.

Beispiele hierfür sind Muscheln und Perlen. Im Falle der Perlen zeigt sich die Schwäche eines Wertgegenstandes im überregionalen oder sogar globalen Handel. So nutzten europäische Händler im Handel auf dem afrikanischen Kontinent Glasperlen, welche für sie relativ einfach zu reproduzieren waren, um sie dann gegen schwer zu reproduzierende Arbeitskraft in Form von afrikanischen Sklaven zu tauschen.

Aktuelle Themen der IT-Sicherheit WS21/22, 06.12.2021, Hof, Deutschland

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Später nutzte man stabilere Ressourcen wie Silber und Gold zum Tausch gegen Waren, wobei die Vereinigten Staaten von Amerika sogar ihren gesamten Währungswert des Dollars mit Gold verknüpften. Da dies nicht flexibel genug war, löste man die Wertverknüpfung 1971, was zum aktuellen Stand des Dollars führte.

2.2 Fiat-Währungen

Fiat stammt vom lateinischen Wort *fieri* und bedeutet *Es werde* oder *Es soll*. In Verknüpfung mit Währungen bezeichnet *Fiat* somit die innere Wertlosigkeit der Währung. Der tatsächliche Wert wird von außen vorgegeben, was den Unterschied zu historischen Währungen darstellt, deren Wert maßgeblich vom Angebot abhing.

Fiat-Währungen werden zentral gesteuert, was einige Vorteile mit sich bringt. Die Einheiten der Währung, das Bargeld, kann leicht in Umlauf gebracht werden, getauscht werden und sehr einfach von Fälschungen Unterschieden werden. Zudem kann durch eine staatliche Steuerung der Währung ebenfalls die Wirtschaft gesteuert und manipuliert werden. Satoshi Nakamoto beschreibt den Stand der aktuellen Fiat-Währungen folgendermaßen:

> Der Zentralbank muss vertraut werden, dass sie die Währung nicht entwertet, aber die Geschichte der Fiat-Währungen ist voll von Verstößen gegen dieses Vertrauen[6].

Ein Beispiel für den Missbrauch der Währungen von Zentralbanken und Staaten zeigt die Entwertung des venezuelanischen Bolivars durch die korrupte Regierung in den anfängen des einundzwanzigsten Jahrhunderts. Auch die gezielte Manipulation des chinesischen Renminbi zur Senkung des Exportpreises der eigenen Waren ist ein Beleg des Missbrauchs.

Eine weitere Eigenschaft von Fiat-Währungen ist die zentralisierung der potenziellen Fehlerquellen. Fiat Währungen werden durch Banken verwaltet, welche sowohl große Mengen der Währung, als auch sensible Daten der Kunden halten und somit zu attraktiven Angriffszielen werden. Auch dieses Phänomen beschreibt Satoschi Nakamoto:

> Wir müssen ihnen unsere Privatsphäre anvertrauen und darauf hoffen, dass sie unsere Konten nicht von Betrügern leerräumen lassen[6].

Auch hierfür gibt es ein Beispiel. Der US-Amerikanische Finanzdienstleister *Equifax* wurde 2017 Opfer eines Angriffs, in dem über 140 Millionen Datensätze aktueller und vergangener Kunden offengelegt wurden.

2.3 Erste Ansätze für Kryptowährungen

Wei Dei veröffentlichte um die Jahrtausendwende ein Konzept namens *b-Money*, in welchem er ein anonymes, verteiltes und digitale Bargeld beschrieb. *B-Money* legte den Fokus des Geldes auf Dezentralität und ermöglichte das Ausführen von Transaktionen ohne Mittelsmänner.

Wenige Jahre später entwickelte Adam Back *Hashcash*, welches als DoS-Schutz für Mail-Server entwickelt wurde. Das Konzept beschreibt erstmals die Idee des *Proof of Work* oder Arbeitsnachweises. Mail Clients mussten hier eine relativ aufwändige Rechenaufgabe lösen, um eine Mail an den Server schicken zu können. Somit wurde eine Überflutung von Anfragen an den Server unterbunden.

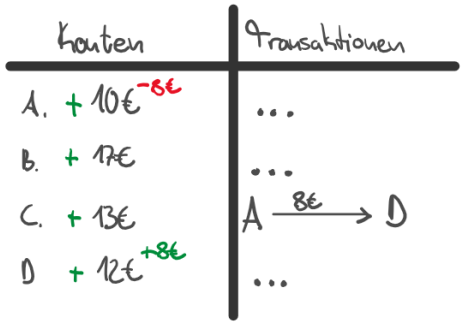

Abbildung 1: Zentrales Ledger

Der Server konnte die Lösung der Rechenaufgabe sehr leicht verifizieren. Dieses Konzept wurde später von Kryptowährungen wie *Bitcoin* adaptiert.

3 KRYPTOWÄHRUNGEN

Im vergangenen Kapitel wurden einige Probleme von vergangenen Währungen und den aktuellen Fiat-Währungen erläutert, darunter die Instabilität des Wertes, Manipulierbarkeit und die Zentralität der Fehlerquellen. Kryptowährungen versuchen diese Probleme zu eliminieren, erste Ansätze hierfür wurden ebenfalls im vorigen Kapitel gezeigt.

Um zu verstehen, wie Kryptowährungen funktionieren, wird im folgenden Kapitel auf die Ziele von Kryptowährungen eingegangen und auf die Ansätze, wie man diese Ziele erreichen kann. Folgende Ziele werden betrachtet:

- Dezentralisierung
- Verteilter Konsens
- Kein Vertrauen
- Inflationssicherheit
- Synchronisation
- Stabilität

Um diese Ziele und deren Lösungen erklären zu können, wird im folgenden Kapitel eine Währung aufgebaut, die sich stark an der Implementierung von Bitcoin [5] orientiert.

3.1 Dezentralisierung

Wie im Kapitel Fiat-Währungen bereits erläutert wurde, bieten zentralisierte Finanzsysteme einige Manipulationsmöglichkeiten, sowohl durch Angriffe als auch durch Einflussnahme Dritter. Beim Aufbau einer neuen Währung muss man somit als erstes die Dezentralität garantieren.

Um eine Währung betreiben zu können, benötigt man ein sogenanntes Hauptbuch - im Folgenden als *Ledger* bezeichnet. Dieses hält alle Informationen zu aktuellen Kontoständen und vergangenen Transaktionen. Somit lassen sich alle Änderungen nachvollziehen. Abbildung 1 zeigt eine mögliche Form eines Ledgers.

Hält man dieses Ledger nun nur zentral, ergeben sich alle Nachteile einer konventionellen Währung. Somit muss das Ledger an alle Beteiligten verteilt werden. Jede Änderung wird an alle Teilnehmer

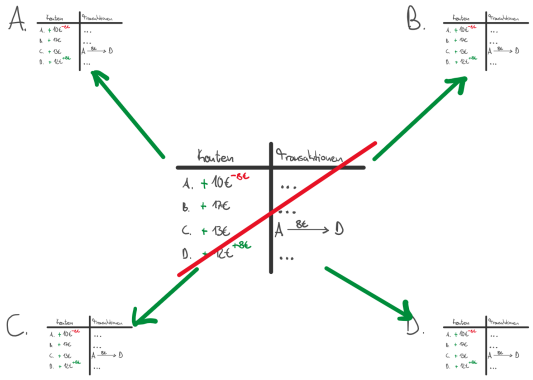

Abbildung 2: Verteiltes Ledger

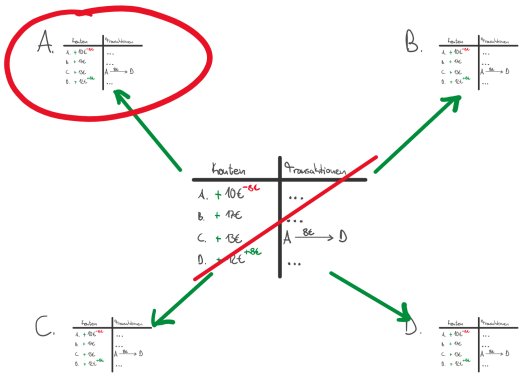

Abbildung 3: Vertrauenswürdiger Schreiber

der Währung bekannt gegeben und von allen geprüft. Somit lässt sich das Netzwerk wie in Abbildung Verteiltes Ledger beschreiben.

Durch die Verteilung des Ledgers wurden nun die Grundlagen einer dezentralen Währung bereitgestellt.

3.2 Verteilter Konsens

Die Verteilung des Ledgers funktioniert bei einem kleinen Netzwerk sehr gut. Sobald man aber skaliert und ein beliebig großes Netzwerk aufbaut, wird die Kommunikation immer ineffizienter und es bieten sich klare Angriffs- und Manipulationsmöglichkeiten. Einige Teilnehmer des Netzwerkes könnten so gefälschte Ausgaben in das Ledger schreiben und dieses an neue Teilnehmer kommunizieren. Eine naive Lösung dessen ist das Prüfen und Schreiben durch einen vertrauenswürdigen Teilnehmer, wie in Abbildung Vertrauenswürdiger Schreiber gezeigt.

Dieser vertrauenswürdige Schreiber prüft nun alle Änderungen, die an ihn kommuniziert werden, schreibt diese gegebenenfalls in das Ledger und kommuniziert dies an alle anderen Teilnehmer, die nur Änderungen des Schreibers annehmen. Dies bedarf ein grundlegendes Vertrauen in den Schreiber, bietet aber wiederum neue Angriffsmöglichkeiten. Der Schreiber könnte entweder manipuliert, bedroht oder durch Dritte ersetzt werden, ohne dass die restlichen

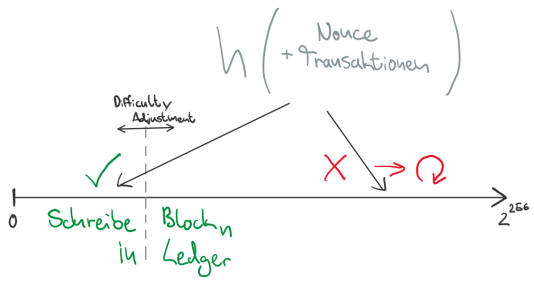

Abbildung 4: Einrichten einer Lotterie

Teilnehmer im Netzwerk etwas bemerken. In Kapitel Kein Vertrauen wird gezeigt, wie man einen einen vertrauenswürdigen Schreiber in einem dezentralen System festlegen kann, ohne ihn angreifbar zu machen.

3.3 Kein Vertrauen

Wie bereits beschrieben bietet ein einziger vertrauenswürdiger Schreiber eine Schwachstelle in einer neuen Währung. Da das große Ziel einer Kryptowährung die Gleichberechtigung aller Teilnehmer ist, muss man den Vertrauensaspekt beim Schreiben in das Ledger entfernen. Der Gleichberechtigung geschuldet müssen alle Teilnehmer im Netzwerk der Währung schreiben können. Hierfür kann man eine Lotterie erstellen, welche das Schreibrecht vergibt ud an der grundsätzlich alle Teilnehmer des Netzwerks teilnehmen können. Diese Lotterie muss mindestens folgende Bedingungen erfüllen:

- **Zufälligkeit der Schreibberechtigung** Gegenstand der Verlosung ist die Schreibberechtigung, welche vollkommen unvorhersehbar erteilt werden muss. Wie in Kapitel Verteilter Konsens bereits beschrieben bietet ein festgelegter Schreiber eine Schwachstelle. Legt man diesen Schreiber jedoch zufällig unter allen Teilnehmern fest, ist es Angreifern unmöglich, den richtigen Teilnehmer zu finden.
- **Kosten für Teilnahme** Um es Teilnehmern unmöglich zu machen, ihre Gewinnchancen zu weit zu erhöhen, muss die Teilnahme an der Lotterie etwas Kosten. Somit bleibt die Zufälligkeit des Schreibers und die Chancengleichheit garantiert.
- **Gewinner-Bestimmung ohne zentrale Lotterieleitung** Die Lotterie stellt sich den gleichen Herausforderungen wie die Währung selbst, sie muss völlig dezentral und somit nicht manipulierbar bleiben. Es muss eine Möglichkeit gefunden werden, den Gewinner dezentral zu bestimmen, so dass jeder Teilnehmer dies verifizieren und somit den Schreiber akzeptieren kann.

Für dieses Problem lässt sich das Hash-Verfahren nutzen, denn es bietet den Vorteil, dass das Ergebnis eines Hashes unabhängig von der Eingabe ist, jedoch bei mehrmaliger Ausführung immer dasselbe ist. Abbildung Einrichten einer Lotterie zeigt eine mögliche Nutzung des Hash-Verfahrens in der SHA-256 Implementierung, welche in der Umsetzung von Bitcoin an dieser Stelle verwendet wird. Die Lotterie läuft folgendermaßen ab:

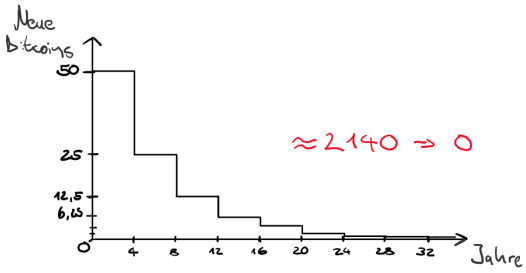

Abbildung 5: Verlauf der Coinbase-Transaktionen

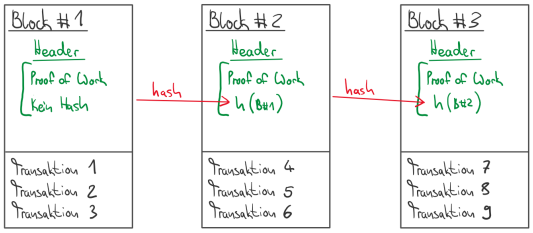

Abbildung 6: Schema einer Blockchain

(1) Vor dem Lotterie-Durchgang wird ein gültiger Teilbereich im Wertebereich des Hash-Verfahrens festgelegt
(2) Alle Transaktionen, die geschrieben werden müssen, werden von allen Teilnehmern gesammelt und verifiziert.
(3) Sobald eine Runde der Lotterie beginnt, werden alle gültigen Transaktionen mit einer zufällig gewählten Zahl - *Nonce* - gehashed.
(4) Liegt der resultierende Hash nicht im gültigen Wertebereich wird eine neue Nonce gewählt und Schritt 3 wiederholt
(5) Liegt der resultierende Hash im gültigen Wertebereich, so teilt der Teilnehmer seine Nonce an das Netzwerk mit.
(6) Alle anderen Teilnehmer im Netzwerk prüfen das Ergebnis und akzeptieren den Gewinner gegebenenfalls als Schreiber

Da das finden der korrekten Nonce beliebig viel Rechenkraft kosten kann, sind die Kosten für die Teilnahme garantiert. Die Unvorhersehbarkeit des Hash-Ergebnisses garantiert wiederum die Zufälligkeit der Schreibberechtigung und das einfache Prüfen des gültigen Hashes durch das einmalige Ausführen des Hashes mit der gültigen Nonce ermöglicht eine dezentrale Prüfung des Ergebnisses und macht somit eine zentrale Lotterieleitung überflüssig. Die Kosten des Hash-verfahrens bietet den weiteren Vorteil, dass eine Manipulation des Ledgers durch den Schreiber nicht rentabel ist. Die restlichen Teilnehmer können die Änderungen sehr einfach prüfen und notfalls ablehnen, womit der Schreiber sämtliche investierte Rechenkraft verschwendet hat.

3.4 Inflationssicherheit

Es wurde nun eine Lotterie eingerichtet, welche den Schreiber für das Ledger vollkommen unvorhersehbar bestimmt. Jedoch bedarf es für den Gewinner noch eine Art Belohnung, um ihn für die aufgewandte Rechenkraft zu entlohnen und einen Anreiz für die Teilnahme an der Lotterie zu schaffen.

Das kann durch die sogenannte *Coinbase*-Transaktion geschafft werden. Diese wird von allen Teilnehmern der Lotterie zusätzlich zu allen anderen Transaktionen einbezogen und beschreibt den Transfer eines Betrages der Währung an den Teilnehmer selbst. Diese Transaktion benötigt keinen Ursprung, da sie neue Einheiten der Währung produziert. Somit wird der Gewinner der Lotterie nicht nur entlohnt, es wird auch ein Weg festgelegt, wie neue Währung in den Umlauf gebracht wird.

Es muss nun nur der Wert dieser Coinbase-Transaktion festgelegt werden. Dieser darf auch nicht konstant bleiben, da die Währung sonst eine konstante Inflation erlebt und somit nicht stabil ist. Abbildung Verlauf der Coinbase-Transaktionen zeigt das sogenannte Halving, ein Mechanismus, der den Wert der Coinbase-Transaktion nach einer bestimmten Anzahl an Lotterie-Durchgängen halbiert, bis er den Wert 0 erreicht hat. Danach wird der Gewinner der Lotterie durch Transaktionsgebühren entlohnt, was einen weiteren Anreiz zur Teilnahme bietet. Somit ist die Menge der Währung finalisiert, was die Währung an sich von Inflationstendenzen befreit.

3.5 Synchronisation

Es wurde nun eine Währung geschaffen, deren Ledger dezentral von allen Teilnehmern gehalten wird. Eine Sammlung von Transaktionen wird von einem durch die Lotterie zufällig gewählten Schreiber festgehalten und von allen Nutzern verifiziert. Die Manipulation des Ledgers wird durch die Kosten des Hash-Verfahrens unterbunden, die Kosten hingegen werden durch Transaktionsgebühren und die Coinbase-Transaktion gerechtfertigt.

Was noch nicht geklärt ist, ist wie genau das Ledger gesichert wird, denn neue Mitglieder im Netzwerk könnten nach wie vor mit korrumpierten Versionen manipuliert werden. Hier kommt die sogenannte *Blockchain* ins Spiel. Wie der Name vermuten lässt ist die Blockchain lediglich die Aneinanderreihung von Blöcken, wobei ein Block durch alle folgenden Blöcke abgesichert wird. Ein Block enthält die zu sichernden Informationen, im Falle der Kryptowährung die Transaktionen, den Hash des vorherigen Blockes und den Arbeitsnachweis des Schreibers, die sogenannte *Proof of Work*. Ausgenommen ist hier der erste Block der Blockchain, auch *Genesis-Block* genannt, welcher keine Informationen zum vorigen Block enthält[1].

Der Hash des vorigen Blockes garantiert die Unveränderbarkeit des Blockes, denn um nun einen älteren Block zu manipulieren, müsste ein Angreifer die Informationen in dem Block so manipulieren, dass derselbe Hash entsteht, also eine Kollision verursachen, was bei heutigen Hash-Verfahren quasi unmöglich ist.Eine Manipulation eines Blockes würde somit alle nachfolgenden Blöcke unbrauchbar machen. Somit muss die Hash-Eingabe in der Lotterie noch um den Hash des vorigen Blockes erweitert werden, dies ist in Abbildung 7 dargestellt.

Der Gewinner der Lotterie macht nun nicht einfach Einträge in ein Ledger, stattdessen schreibt er einen neuen Block in die Blockchain, welche fortan als Ledger angesehen werden kann.

[1] Siehe Abbildung 6

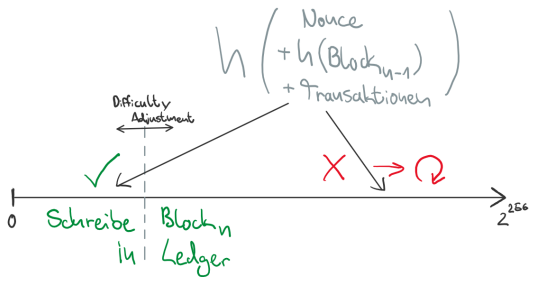

Abbildung 7: Einbinden der Blockchain in Lotterie

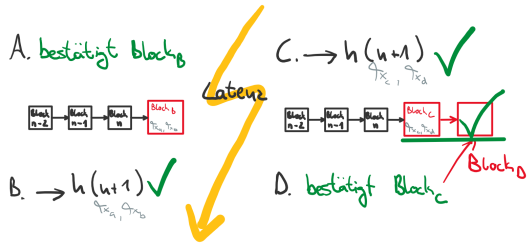

Abbildung 8: Nagamoto Konsens

3.6 Stabilität

Im Grunde ist die Währung nun komplett. Es wurde ein dezentrales Ledger durch die Blockchain erschaffen, welches nicht mehr manipuliert werden kann und in das neue Einträge - oder Blöcke - von zufällig gewählten Schreibern geschrieben werden. In diesem Ablauf wird die Skalierung jedoch noch nicht einbezogen, denn in einem beliebig großen Netzwerk von Teilnehmern, die ständig miteinander kommunizieren, muss die Latenz bei der Übertragung von Nachrichten mit beachtet werden.

Nimmt man also ein weltweites Netzwerk, so kann es in der Verlosung der Schreibrechte passieren, dass in unterschiedlichen Teilen des Netzwerkes unterschiedliche Blöcke gefunden werden, die alle gültig sind. Grund hierfür sind Transaktionen, die nähere Knoten im Netzwerk eher erreichen, als weiter entfernte. Verteilte Teilnehmer im Netzwerk starten ihren Versuch in der Lotterie also mit unterschiedlichen Transaktionen. Finden nun mehrere Teilnehmer im Netzwerk gleichzeitig gültige Blöcke, in denen unterschiedliche Transaktionen gehalten werden, bevor diese Transaktionen und die Blöcke von allen Teilnehmern akzeptiert oder gar empfangen wurden, so kommt es zu sogenannten *Blockkollisionen*. Hier akzeptieren alle Teilnehmer jeweils den gültigen Block, dessen Transaktionen sie bereits kannten und der sie als erstes erreicht hat. Es kann also zu Zeitpunkten kommen, in denen verschiedene Blöcke in der Blockchain akzeptiert werden. Um nun ein Spalten der Blockchain zu vermeiden und einen allgemeinen Konsens herzustellen muss ein weiteres Konsens- Verfahren eingeführt werden.

Im Falle von Bitcoin heißt dieser Konsens *Nakamoto-Konsens*. Dieser besagt, dass die Blockchain mit dem höchsten Arbeitsaufwand, *Proof of Work*, akzeptiert wird. Findet somit ein Teilnehmer einen weiteren Block und teilt ihn an alle anderen Teilnehmer mit, bevor jemand anderes einen Block findet, so wird dessen darunterliegende Blockchain als neue Grundlage akzeptiert, da in diese am meisten Aufwand geflossen ist. Alle anderen Blöcke werden verworfen. Abbildung 8 zeigt diesen Ablauf beispielhaft. Hier kollidieren die Blöcke *B* und *C*, wobei Block *D* Block *C* zuerst bestätigt. Block *B* wird nun verworfen. Verworfene Transaktionen gehen allerdings nicht verloren, sie werden in einem späteren Block neu aufgenommen und solange mit neuen Transaktionen im sogenannten *Transaktionspool* gehalten, den alle Nutzer bei sich halten.

Es wurde nun ein Protokoll geschaffen, welches ein dezentrales Ledger durch eine Blockchain realisiert, die jeder Nutzer der Währung halten und verifizieren kann. Alle Teilnehmer des Netzwerks sind gleichberechtigt und dürfen somit alle neue Blöcke schreiben, Voraussetzung für eine Schreibberechtigung ist jedoch das finden einer gültigen Zufallszahl, *Nonce*, welche, sobald sie gefunden wurde als Arbeitsnachweis, *Proof of Work*, von allen Teilnehmer akzeptiert wird. Die Kosten der Berechnung machen Manipulationsversuche unwirtschaftlich, da diese leicht erkannt und abgelehnt werden können. Für den Aufwand des Hashens wird der Schreiber mit der *Coinbase-Transaktion* und Transaktionsgebühren belohnt. Die *Coinbase-Transaktion* reguliert ebenfalls die Gesamtmenge der Währungseinheiten, da sie nach einer bestimmten Anzahl an geschriebenen Blöcken im Wert halbiert wird. Das verhinder eine Inflation der Währung. Sollten Blöcke durch die Größe des Netzwerks geschuldet kollidieren, so gilt die Blockchain mit dem höchsten Arbeitsaufwand als neue akzeptierte Blockchain. Alle anderen Blöcke werden verworfen, die Transaktionen werden in späteren Blöcken festgehalten.

4 WALLETS UND TRANSAKTIONEN

In Kapitel 3 wurde gezeigt, wie eine Kryptowährung aufgebaut werden kann, um einige Probleme von klassischen Währungen zu eliminieren. Im Folgenden sollen noch einmal kurz die Vorteile der Nutzung einer Kryptowährung gezeigt werden, um danach genauer auf die Nutzung einer solchen Währung einzugehen.

Grundsätzlich implementieren die meisten Kryptowährungen die grundlegenden Ideen des *web3*, konkret folgende:

- **Unabhängigkeit von zentralen Instanzen** Kryptowährungen geben die Verantwortung der Währung den Nutzern, statt sie zentralen Instanzen anzuvertrauen und sich Manipulationen durch diese und Angriffe auf diese auszusetzen.
- **Kryptografische Absicherung** Kryptowährungen basieren in keiner Form auf Vertrauen, sondern stets auf kryptografischer Absicherung und der quasi Unmöglichkeit, die Verfahren zu umgehen, um die Währung zu manipulieren.
- **Privatsphäre** Kryptowährungen verzichten in der regel auf Identifizierungen der Nutzer und verfolgen die Ansicht, dass die Nutzung einer Währung unter die zu schützende Privatsphäre einzuordnen ist. Durch den Verzicht der Speicherung von sensiblen Daten machen sich Kryptowährungen auch nicht im Sinne der Privatsphäre der Nutzer angreifbar.
- **Wertstabilität** Durch eine kontrollierte Ausschüttung der Währungseinheiten und die Limitierung dieser entziehen sich Kryptowährungen von jeglicher Inflation, Deflation oder

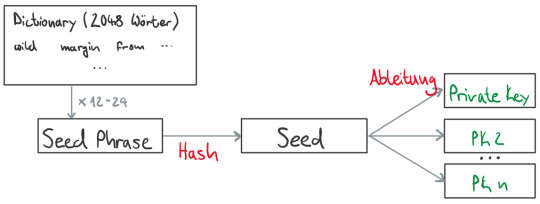

Abbildung 9: Erstellung eines Key-Pairs

vergleichbaren Wertinstabilitäten. Sie sind somit langfristig planbar, zuverlässig und vor Wertmanipulation geschützt.

Durch diese Eigenschaften heben sich Kryptowährungen von aktuellen *Fiat*-Währungen ab und bieten somit eine Alternative. Im Folgenden soll genauer darauf eingegangen werden, wie Kryptowährungen genutzt werden können und wie die Nutzung konkret implementiert sein könnte. Hierfür wird erneut die Kryptowährung *Bitcoin* als Beispiel verwendet.

4.1 Krypto-Wallets

Wie bereits angesprochen versuchen Kryptowährungen die Identifizierbarkeit aus der Währung zu entfernen. Primärer Fokus liegt hier bei der Eliminierung persönlicher Daten aus der Identifizierung des Nutzers. Die Herausforderung liegt also darin, eine Art Konto für eine Währung anzulegen, für das man sich nicht bei einer zentralen Bank identifizieren muss und das nicht von anderen Nutzern oder Angreifern manipuliert werden kann.

Auch hierfür bedienen sich gängige Kryptowährungen der Kryptografie, indem sie zur eindeutigen Identifizierung eines Nutzers asymmetrische Verschlüsselungsverfahren anwenden.

In Abbildung 9 wird anschaulich dargestellt, wie Nutzer beliebig viele Schlüsselpaare erzeugen können, aus denen dann Adressen zur Identifizierung erzeugt werden können.

(1) Erstellen einer *Seed-Phrase* aus menschenlesbaren Wörtern
(2) Hashing der Seed-Phrase zum Erstellen des Seeds
(3) Ableitung beliebig vieler Schlüsselpaare zur Adressgenerierung und weiteren Nutzung

Hierbei wird Schritt 1 in vielen gängigen Kryptowährungen angewandt, um das Merken des Seeds zu vereinfachen. Ein Nutzer kann somit alle seine Schlüsselpaare regenerieren, indem er sich die Wörter der Seed-Phrase merkt.

Aus einem Schlüsselpaar kann nun eine Adresse erzeugt werden, wie Abbildung 10 zeigt. Diese Adresse können nun der Nutzer und alle anderen Teilnehmer nutzen, um aus der Blockchain alle Transaktionen mit dieser Adresse auszulesen. Durch diese Transaktionen kann dann der Kontostand des Nutzers ermittelt werden, wodurch spätere Transaktionen validiert werden können. Abbildung 10 zeigt in folgenden Schritten, wie eine Bitcoin Adresse aus einem Schlüsselpaar generiert werden kann:

(1) Doppel-Hash des Public-Keys zur Verkleinerung dessen auf einen Wertebereich von 160 Bit
(2) Kodierung des Hashes zu Base58

Der Doppel-Hash in Schritt 1 ist in diesem konkreten Fall eine Vorsichtsmaßnahme, um die Wahrscheinlichkeit von Kollisionen

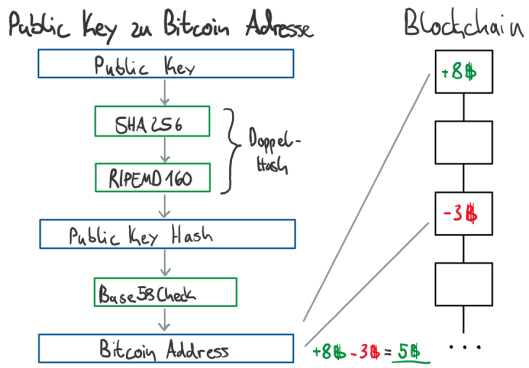

Abbildung 10: Erstellung einer Adresse

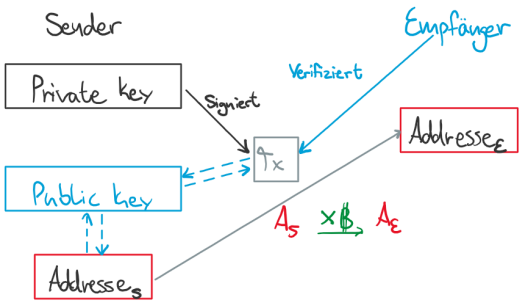

Abbildung 11: Transaktionsablauf

weiter zu verhindern. Das eigentliche Ziel des Hashes ist es, den Public-Key deutlich zu verkleinern, um die Nutzung der späteren Adresse zu vereinfachen. Auch Schritt 2 dient lediglich der einfacheren Nutzung, da Base58 ähnlich scheinende Zeichen aus dem Zeichensatz entfernt. Somit sollen Verwechslungen vermieden werden. Im Grunde kann also der Public-Key zur Identifizierung eines Nutzers genutzt werden, in der Praxis wandelt man diesen zur einfacheren Nutzung allerdings etwas ab. Daraus resultiert die Adresse.

Wie bei asymmetrischen Verschlüsselungsverfahren gängig kann nun der Public-Key des Schlüsselpaars an alle Nutzer im Netzwerk weitergegeben werden. Der Private-Key sollte dabei nie Preis gegeben werden.

Führt man nun eine Transaktion aus, so signiert der Sender die Transaktion mit seinem Private-Key. Somit ist garantiert, dass die Transaktion definitiv vom entsprechenden Nutzer angestoßen wurde. Der Empfänger ubd alle anderen Teilnehmer im Netzwerk können diese Transaktion verifizieren, indem sie sie mit dem Public-Key des Senders entschlüsseln. Der Inhalt einer Transaktion besteht somit nur aus zwei Adressen, der des Senders und der des Empfängers und des Betrages, der transferiert werden soll. Somit die Datenmenge, die an alle Nutzer bekannt gegeben werden muss ebenfalls auf ein Minimum beschränkt. Abbildung 11 zeigt diesen Ablauf schematisch.

Hot Wallets	Cold Wallets
Web-Anwendung Mobile-Anwendung Desktop-Anwendung	Hardware Digital Papier
+ einfach kostenfrei	+ sehr sicher
– unsicher	– teuer schwerer Einstieg

Tabelle 1: Arten von Krypto-Wallets

4.2 Arten von Wallets

Wie in Kapitel 4.1 beschrieben ist eine Wallet nichts anderes als ein Werkzeug, welches für einen Nutzer die Adressen, Schlüsselpaare und Transaktionsabläufe betreut. Dabei limitieren sich Wallets keineswegs auf die Nutzung für nur eine Kryptowährung, stattdessen können sie beliebig komplex ausfallen und verschiedene Kryptowährungen für einen Nutzer halten. Tabelle 1 zeigt verschiedene Implementierungsarten von Wallets für Kryptowährungen. Wallets kann man grundsätzlich in zwei Arten unterscheiden, Cold-Wallets und Hot-Wallets. Man betrachtet Hot-Wallets im Allgemeinen als einfacher zu Nutzen und günstiger in der Anschaffung. Da sie jedoch, wie der Name impliziert, immer am Netzwerk hängen, machen Hot Wallets sich leicht angreifbar und sind für die Nutzung mit großen Beträgen nicht zu empfehlen.

Cold-Wallets hingegen sind oft komplizierter in der Nutzung und oftmals auch teuer in der Anschaffung, sind aber deutlich sicherer als Hot-Wallets, insofern sie korrekt genutzt werden. Wie der Name schon impliziert, hängen Cold-Wallets nicht permanent am Netzwerk und sind somit in der Zeit, in der sie physisch getrennt sind, nicht über das Netzwerk angreifbar.

4.3 Arten von Kryptowährungen

Da *Bitcoin* allgemein als die erste funktionierende und tatsächlich implementierte Kryptowährung gilt unterteilt man den Begriff Kryptowährung allgemein in zwei Unterbereiche: *Bitcoin* und *Altcoin*. Altcoin beschreibt alle Währungen außer *Bitcoin* und wird selbst noch einmal in zwei Unterkategorien geteilt: Bitcoin-Abwandlungen und Kryptowährungen mit nativen Blockchains. Bitcoin-Abwandlungen sind hierbei Währungen, welche lediglich Teile der Bitcoin Implementierung abgewandelt haben und deren Blockchain in den frühen Blöcken identisch mit der von Bitcoin ist. Währungen mit einer nativen oder eigenen Blockchain sind seit Beginn ihrer Blockchain unabhängig von Bitcoin entwickelt worden. Abbildung 12 zeigt die Unterteilung von Kryptowährungen und gibt einige Beispiele für die Unterkategorien an.

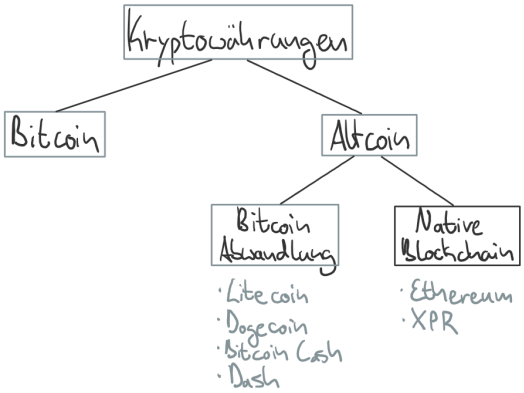

Abbildung 12: Kryptowährungen

5 FAZIT

Die große Anzahl der konkreten Kryptowährungen deutet darauf hin, dass die Konzepte und Implementierungen dieser auch funktionieren und von der Allgemeinheit akzeptiert werden. Stand jetzt bieten die größten drei Währungen einen umgewandelten Wert von ?Euro und sind somit eine echte Alternative zu klassischen Währungen geworden. Auch die Akzeptanz der Währung bei Dienstleistern wächst immer weiter. Und neben den konzeptuellen Erfolgen von Kryptowährungen bieten sie ebenfalls Sicherheit für Menschen weltweit, die in der Nutzung ihrer gängigen Fiat-Währung eingeschränkt sind, sei es durch Wertmanipulation oder Unterdrückung, da das Halten von Kryptowährungen lediglich das Merken der Seed-Phrase aus Kapitel 4.1 erfordert und somit im Extremfall kaum nachverfolgbar ist. Jedoch sollte man sich immer bewusst sein, dass physischer Zugriff auf Wallets oder deren Benutzer immer ein großes Problem sein kann. Auch sollte man nie einem System vertrauen, dass man nicht versteht oder nicht geprüft hat, was die Einstiegshürde für Kryptowährung deutlich erhöht. Dennoch sind sie eine vielversprechende Alternative zu klassischen Systemen und fügen sich der Idee des Web 3.0 nahtlos an. Die Entwicklung von Kryptowährungen sollte in den kommenden Jahren mit Spannung weiterverfolgt werden.

LITERATUR

[1] Prof. Dr. Oliver Bendel. 2021. *Definition: Was ist Kryptowährung.* https://wirtschaftslexikon.gabler.de/definition/kryptowaehrung-54160/version-384589 [Online; aufgerufen 15.10.2021].
[2] Bitcoin. 2021. *Wie funktioniert Bitcoin.* https://bitcoin.org/de/wie-es-funktioniert [Online; aufgerufen 26.11.2021].
[3] coindiligent.com. 2021. *Five Dollar Wrench Attack.* https://nitrocdn.com/RRxvRrLqWvYnbMLxaKtfoREJNlVTTpII/assets/static/optimized/rev-15a4122/wp-content/uploads/2018/12/xkcd-security.png [Online; aufgerufen 25.11.2021].
[4] Bitcoin cummunity. 2021. *Bitcoin Wiki.* https://en.bitcoin.it/wiki [Online; zuletzt aufgerufen 30.11.2021].
[5] Satoshi Nakamoto. 2009. *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf [Online; aufgerufen 12.10.2021].
[6] Satoshi Nakamoto. 2009. *Bitcoin open source implementation of P2P currency.* https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source [Online; aufgerufen 09.11.2021].
[7] Yan Pritzker. 2020. *Bitcoin entdecken.* Aprycot Media - Held & Troendle GbR.
[8] Maarten Zuidhoorn. 2020. *The Journey from Mnemonic Phrase to Address.* https://medium.com/mycrypto/the-journey-from-mnemonic-phrase-to-address-6c5e86e11e14 [Online; aufgerufen 25.11.2021].