Hochschule für Technik und Wirtschaft Dresden (FH)

Fachbereich Informatik/Mathematik

Bachelorarbeit

im Studiengang Allgemeine Informatik

Vergleich dezentraler elektronischer Währungen

Eingereicht von: Christian Pfnür

Eingereicht am: 07. Juli 2014

Betreuer: Prof. Dr.-Ing. Jörg Vogt
Prof. Dr.-Ing. Robert Baumgartl

Inhaltsverzeichnis

Abkürzungsverzeichnis

ASIC ..... Anwendungsspezifische integrierte Schaltung

BOINC ..... Berkeley Open Infrastructure for Network Computing

BTC ..... ISO 4217 Code für Bitcoin

CPU ..... Central Processing Unit

DNS ..... Domain Name System

ECDSA ..... Elliptic Curve Digital Signature Algorithm

GPU ..... Graphics Processing Unit

P2P ..... Peer to Peer

PoB ..... Proof of Burn

PoS ..... Proof of Stake

PoW ..... Proof of Work

TAN ..... Transaktionsnummer

Glossar

ASIC

ist eine anwendungsspezifische, integrierte Schaltung, die nur einem einzigen vorprogrammierten Zweck dienen soll. Im Zusammenhang mit Bitcoin berechnet ein ASIC ausschließlich möglichst viele SHA256 Hashwerte je Sekunde.

Block

Ein Block fasst Transaktionen innerhalb eines Netzwerkes zusammen und wird an das Ende der Blockchain angefügt.

Block Reward

Wird als Belohnung für seinen Beitrag zum Erhalt des Netzwerkes an den Erzeuger eines Blocks ausgezahlt.

Blockchain

Die Blockchain ist eine Datenbank über alle Blöcke einer dezentralen Währung. Blöcke werden der Reihenfolge ihrer Lösung nach miteinander verknüpft und enthalten Informationen über den jeweils vorangegangenen Block. In Blöcken werden Transaktionsdaten gespeichert..

Domain

Eine Domain beschreibt den Name einer Webseite wie z.B. “archlinux.org“.

Full Node

beschreibt einen Teilnehmer eines Netzwerkes, der die gesamte Blockchain vorhält und Transaktionshistorien prüfen kann.

Hash

ist eine Zeichenfolge, die eine große Eingabemenge unterschiedlicher Länge auf eine kleinere Zielmenge (die Hashwerte) abbildet.

Mailingliste

Eine Mailingliste bietet einer Gruppe von Menschen die Möglichkeit zum Nachrichtenaustausch per E-Mail. Die Nachrichten werden parallel im Internet veröffentlicht.

Mining Pools

ist eine Menge an Benutzern, die zusammen an der Lösung eines mathematischen Rätsels arbeitet, um Blöcke in einem dezentralen Währungssystem zu erstellen.

Minting

Das Minten ist ein Verfahren zur Erzeugung neuer Coins durch das Besitzen von Coins. Man kann es sich wie eine Verzinsung vorstellen, durch die Anleger nach einer gewissen Zeit neue Coins erhalten.

Off-Chain Transaktion

Ist eine Transaktion, die innerhalb einer Handelsplattform stattfindet und nicht als Transaktion auf der Blockchain verzeichnet wird. Vergleichbar mit einer Transaktion zwischen zwei Kunden der gleichen Bank wechselt Geld zwar den Besitzer, allerdings muss keine andere Partei involviert werden.

Overhead

Daten, die nicht primär zu den Nutzdaten zählen, sondern als Zusatzinformation zur Übermittlung oder Speicherung benötigt werden.

Proof Of Work

Ein Verfahren für den Beweis einer aufwändigen Arbeit um Blöcke für dezentrale Währungen zu erstellen. Im speziellen werden bei diesem Verfahren möglichst schnell sehr viele Hashes gebildet, um einen bestimmten Ziel-Hash zu finden.

Pruning

beschreibt das Löschen alter Transaktionen aus der Blockchain um Speicherplatz zu sparen.

Raspberry Pi

Ist ein Mini-Computer, der ohne Gehäuse vertrieben wird und einen geringen Stromverbrauch aufweist.

White Paper

bezeichnet eine Übersicht über Standards und Techniken einer IT-Thematik.

Tabellenverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Problemstellung

> "The man with a new idea is a Crank until the idea succeeds."
>
> Mark Twain (1835-1910)

Zum Jahreswechsel 2009 begann die praktische Umsetzung von Bitcoin (BTC) basierend auf der Idee eine Währung zu schaffen, die virtuell erzeugt und gehandelt wird[1]. Anfangs hatte die Währung keinen Wert und wurde vornehmlich erzeugt. Der Wert war tatsächlich so gering, dass ein Amerikaner 4 Tage gewartet hat, bis ihm jemand für sein Angebot über 10.000 Bitcoins (heute ca. €4.500.000) 2 große Pizzen hat liefern lassen[2]. Im Jahre 2011 erlangte die immer noch junge Währung einiges an Berühmtheit, als mit ihrer Hilfe ein pseudo-anonymer Zahlungsverkehr für die ehemalige Online-Drogenbörse Silk Road geschaffen wurde[3]. Zusätzlich etablierten sich Handelsplattformen wie Mt.Gox, auf der 2013 zwischenzeitlich 70% aller Bitcoins gehandelt wurden[4]. Auch Regierungen mussten sich mit der jungen Währung beschäftigen und begannen mögliche Gefahren zu diskutieren.

Die Währung entwickelte sich trotz Hackerangriffen auf Privatcomputer und Handelsplattformen[5] im Jahre 2013 sehr schnell. Während der europäischen Bankenkrise entstand eine Debatte darüber, ob auch die Kunden der Banken mit ihren Einlagen teilweise für diese Krise haften sollten[6], wodurch die Popularität der unregulierten Währung weiter wuchs. Vermehrt sahen auch Investoren das Potenzial in Bitcoin. Die für die Erzeugung von Bitcoins erforderliche Hardware wurde 2013 um enorm leistungsstarke anwendungsspezifische integrierte

[1] Nakamoto, Satoshi (2009), The Mail Archive
[2] Anonym (2010), bitcointalk.org
[3] Chen, Adrian (2011), Gawker.com
[4] Vigna, Paul (2011), Wall Street Journal
[5] Anonym (2014), Bitcointalk"
[6] Dörner, Stephan (2013), Wall Street Journal

Schaltungen (ASIC)[7] ergänzt. Die bisher verbreiteten Rechenmethoden mithilfe des Hauptprozessors (CPU) oder Grafikkarten (GPU) wurden dadurch unwirtschaftlich. In der Folge entstanden immer mehr Mining Pools, in denen sich einzelne Personen zusammenschließen um zusammen mehr Rechenleistung aufzubringen.

Mit der Entwicklung von alternativen, dezentralen Währungen begann auch eine fortlaufende Weiterentwicklung von neuen Ideen zur Verbesserung des Vorbildes Bitcoin. Parallel zu neuen Entwicklungen wurden immer mehr mögliche technische Schwachstellen offengelegt. Dennoch sahen Menschen zunehmend eine echte Alternative in Bitcoin. Durch die steigende Zahl der Teilnehmer und das wachsende Vertrauen in die Währung konnte der Bitcoin im Dezember 2013 auf seinen bisher höchsten Handelspreis von ca. 1200 USD/BTC steigen.[8]

Ihre konzeptionellen Schwachstellen und die Unbeständigkeit ihres gehandelten Wertes lassen den Erfolg dezentraler, elektronischer Währungen dennoch zweifelhaft erscheinen. Die Ideen der Entwickler neuer, alternativer Währungen sind wertvoll und tragen zu der Verbesserung des Gesamtkonzeptes dieser Form des elektronischen, dezentralen Geldes bei.

1.2 Aufbau und Zielsetzung der Arbeit

Das Ziel dieser Arbeit soll es sein ein Verständnis für die wichtigsten technischen Aspekte dezentraler, elektronischer Währungen zu vermitteln und zu untersuchen, wie zukunftsträchtig die Idee dieser Währungsform ist.

Dazu bietet der erste Teil der Arbeit zunächst einen Einblick in die Funktionsweise von Bitcoin als erste Umsetzung einer dezentralen, elektronischen Währung. Der zweite Teil schafft einen Vergleich zwischen den in der elektronischen Währung Bitcoin umgesetzten Prinzipien und ihren Weiterentwicklungen in alternativen elektronischen Währungen. Es wird erarbeitet, ob und in welcher Dimension sich die Verfahren jüngerer Währungen gegenüber Bitcoin behaupten können und inwiefern neue Ansätze für das noch relativ junge Prinzip elektronischen Geldes gebraucht werden.

Die Arbeit wird abgeschlossen mit einer Auswertung der verglichenen Kriterien und soll einen Schluss auf die zukünftige Entwicklung elektronischer Währungen zulassen.

[7] Gutekunst, Jürgen (2014), Elektronik für Ingenieure und Naturwissenschaftler

[8] Anonym (2013), bitcoincharts.com

1.3 Methodik und Vorgehensweise

Informationen zu dezentralen, elektronischen Währungen sind kurzlebig und werden erst relativ spät in wissenschaftlichen Arbeiten oder gar Veröffentlichungen in Buchform aufgegriffen. Um eine hohe Diversität bei den zugrundeliegenden Informationen zu gewährleisten, werden daher einige Beiträge aus Foren oder Artikel aus Blogs berücksichtigt. Auch wenn dort Pseudonyme verwendet werden, sind die Personen hinter den Beiträgen oft sehr eng in die Währungen und ihre zugrundeliegenden Mechanismen involviert. Neue Währungen und Ansätze werden meist direkt in Foren diskutiert. Der Informationsaustausch ist ein wichtiger Teil der Kultur dieser Währungen.

Teilweise sind die Verfasser von Dokumenten anonym. Vermutlich befürchten sie einen Angriff auf ihre Person, falls eine Schwachstelle in ihrer Währung oder Methodik gefunden wird und diese zu Millionenverlusten bei ihren Teilnehmern führt. Es mag durchaus sein, dass die Schöpfer auch andere Bedrohungen von Regierungen oder Gruppierungen befürchten müssen. Insbesondere aufgrund der Kanäle, in denen der Großteil der Informationen verbreitet wird, muss man mit einer Einschätzung des Wahrheitsgehaltes vorsichtig sein.

1.4 Überblick

Mit der Währung Bitcoin wurden 2009 durch seinen Gründer mit dem fiktiven Namen Satoshi Nakamoto erstmals die schon 1997 von Adam Back entwickelten Ansätze einer kryptografischen Funktion (Hashcash) zur Validierung von Informationen beim Datenaustausch umgesetzt.

Adam Back hat ursprünglich eine Methode zur Verhinderung großflächiger Spamverbreitung entwickeln wollen[9]. Mit einer moderaten Menge an Rechenaufwand sollte der Absender einen Hash erzeugen, der auf einer Zufallszahl basiert und im versteckten Kopfbereich (Header) einer E-Mail mitgesendet wird. Der Empfänger konnte diesen Hash schnell validieren und dadurch herausfinden, ob der Sender einen gewissen Aufwand in die Signierung dieser E-Mail investiert hat. Der Vorteil dieser Methode beruht nach Beck auf der Annahme, dass Spammer den Rechenaufwand für eine derart große Menge E-Mails nicht investieren könnten und in der Folge das globale Spamaufkommen zurückgehen würde.

Schon 1998 hatte Wei Dai mit B-money auf einer Mailingliste mögliche Protokolle auf Basis der Proof Of Work (PoW) Methode Hashcash vorgestellt[10]. Die erste Idee basierte auf

[9] Back, Adam (Unbekannt), Hashcash.org

[10] Dai, Wei (2013), weidai.com

der Annahme eines synchronen, nicht störbaren Broadcast-Netzes. Zur Umsetzung seiner zweiten Idee sollten eine gewisse Menge an auserwählten Servern aus dem Teilnehmer-Netz die Transaktionsinformationen speichern und untereinander austauschen. Ein Client sollte zur Verifizierung seines Guthabens mehrere Server abfragen, um dessen Betrag zu verifizieren.

Ebenfalls 1998 begann Nick Szabo mit der Entwicklung von "Bit gold", dessen Prinzip er 2005 präsentierte[11] und das als direkter Vorgänger des Bitcoins gesehen wird. Linguistischen Analysen zufolge[12] könnte er sogar der Erfinder von Bitcoin sein, da seine wissenschaftlichen Arbeiten stilistisch dem anonymen Bitcoin "White Paper"[13] ähneln, in welchem Bitcoin zum ersten Mal der Öffentlichkeit präsentiert wurde. Der Verfasser dieses Dokumentes versteckt sich hinter dem Pseudonym "Satoshi Nakamoto". Mit "Bit gold" hat Szabo bereits alle auch später in Bitcoin umgesetzten Prinzipien der Währung bedacht. Die dezentrale Generierung von Geld durch Lösungen kryptografischer Probleme sollte von allen Teilnehmern des Netzwerkes durchgeführt werden können. Der Teilnehmer mit der korrekten Lösung sollte die Hashkette der Lösung mit seinem öffentlichen Schlüssel verknüpfen. Wie bei der ursprünglichen Idee von Hashcash sollten alle Empfänger dieser Lösung sie ganz einfach überprüfen können.

Da der Wert dieser Währung einzig durch die Akzeptanz seiner Nutzer gemessen wird und keinen definierten Gegenwert in Rohstoffen hat, kann man die in dieser Arbeit aufgegriffenen Geldsysteme als Fiat-Währungen bezeichnen wie z.B. der US-Dollar eine ist. Das bedeutet, dass das Geld der Währung für sich wertlos los, es aber gegen Warengeld getauscht werden kann[14]. Warengeld umfasst Edelmetalle, aber auch Nahrungsmittel, Zigaretten und Alkohol. Mit der Lösung des ersten Blocks wurde 2009 die Währung Bitcoin geschaffen.

[11] Szabo, Nick (2008), Unenumerated Blog

[12] Grieve, Jack (2014), Aston University

[13] Nakamoto, Satoshi (2009), The Bitcoin Foundation

[14] Conway, Edmund (2011), 50 Schlüsselideen Wirtschaftswissenschaft

2 Funktionsweise von Bitcoin

Auf die digitale Welt übertragen funktionieren Bitcoins wie ein Bankkonto. Es gibt eine Liste an Bitcoin Konten, eine Liste an Transaktionen aller Teilnehmer und es gibt eine vertrauenswürdige Verwaltung der zur Verfügung stehenden Einheiten. Der erste grundlegende Unterschied zu konventionellen Bankkonten ist jedoch, dass alle Teilnehmer des Netzwerkes eine Kopie aller Konten und aller Transaktionen einsehen können. Der zweite Unterschied ist, dass alle Teilnehmer des Netzwerkes diese Liste speichern und selbst zur Verfügung stellen können. Und der dritte große Unterschied ist, dass keine absoluten Geldbeträge je Inhaber existieren, sondern der Besitz von Geldeinheiten anhand der kompletten Liste an Transaktionen zurückverfolgt[15] wird.

2.1 Wallets zur Guthabenverwaltung

Statt einer Kontonummer mit einer Transaktionsnummer (TAN) oder einem Zugangscode verwaltet im Bitcoin Netzwerk jeder aktive Teilnehmer Schlüsselpaare bestehend aus einem öffentlichen und einem privaten Schlüssel. Diese Schlüsselpaare werden in einer sogenannten Wallet Datei gespeichert.

Jeder Teilnehmer kann unabhängig von anderen Teilnehmern neue Schlüsselpaare erzeugen und benutzen. Bei der Erstellung wird ein "Elliptic Curve Digital Signature Algorithm" (ECDSA) Schlüsselpaar erzeugt. Der öffentliche Teil dieses Paars wird mit der Hashfunktion RIPEMD-160 gehasht. Das Resultat ist eine öffentliche Adresse vergleichbar mit einer Kontonummer, da dieser Hash als Ziel bei Überweisungen verwendet wird. Teilnehmer können beliebig viele Schlüsselpaare erzeugen, um Transaktionen zu versenden und zu empfangen. Wer den passenden privaten Schlüssel zu einer öffentlichen Adresse verwaltet[16], kann über das Guthaben verfügen, das an diese Adresse übertragen wurde. Er ist demnach mit einer TAN vergleichbar. Die zeitgleiche Erzeugung eines exakt gleichen Schlüsselpaares ist nahezu unmöglich, da durch

[15] H. Cap, Clemens (2012), HMD Praxis der Wirtschaftsinformatik

[16] Anonym (Unbekannt), Bitcoin Wiki

Verwendung von RIPEMD-160 2^{160} verschiedene öffentliche Schlüssel erzeugbar sind. In dem ohnehin unwahrscheinlichen Fall, dass ein öffentlicher Schlüssel doppelt erzeugt wurde, gibt es für jeden einzelnen $2^{(256-160)}$ unterschiedliche Möglichkeiten des privaten Schlüssels. Um eine Transaktion auszulösen wird mithilfe des privaten Schlüssels eine Signatur erzeugt, die sich auf die Transaktionsinformationen bezieht (wie Abb. 2.1 zu entnehmen). Diese Signatur kann also nicht für andere Transaktionen wiederverwendet werden, da sie sich genau auf die Parameter einer Transaktion bezieht. Mit einem privaten Schlüssel können allerdings beliebig viele Transaktionen signiert werden. Die signierte Transaktion wird an das Netzwerk veröffentlicht und alle Teilnehmer können sie überprüfen. Dazu extrahieren sie aus der Signatur den öffentlichen Schlüssel des Absenders und prüfen mit selbigem die Gültigkeit der Signatur. Stimmt die Signatur mit der Transaktion überein, befinden die Teilnehmer sie für gültig.

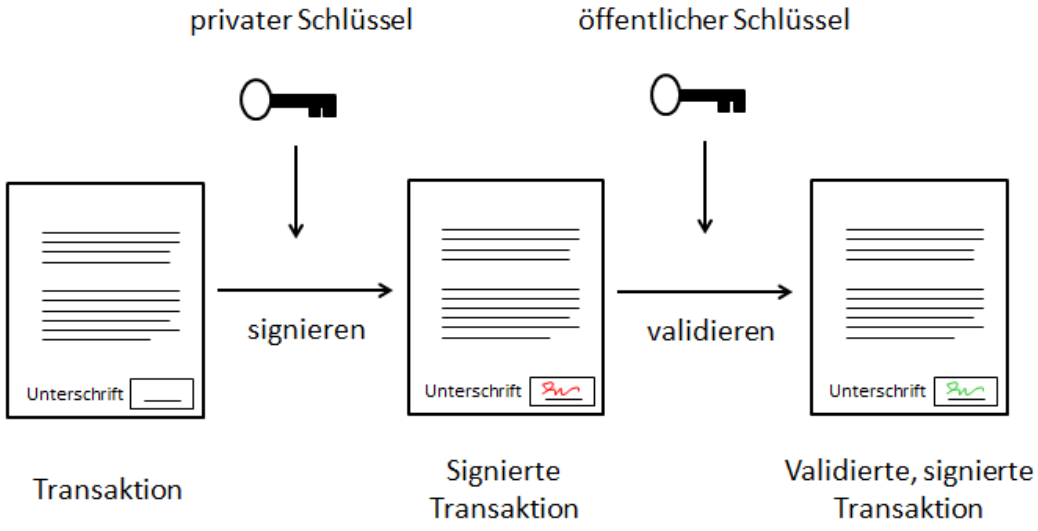

Abbildung 2.1: Digitales Signaturverfahren (eigene Darstellung)

In der Regel übernimmt die Erstellung und Verwaltung der Schlüsselpaare eine Wallet Software, die auf dem eigenen Computer oder als Webapplikation ausgeführt wird. In einer Wallet können beliebig viele Schlüsselpaare gespeichert werden, wobei es strategisch wichtig ist eine Kopie der Schlüssel-Datei sicher zu verwahren. Geht der private Schlüssel verloren, dann verliert sein Besitzer jede an den dazugehörigen öffentlichen Schlüssel gerichtete Transaktion. Für die Aufbewahrung des privaten Schlüssels wird üblicherweise das "Wallet Import Format" (WIF) verwendet. Im Wesentlichen ist das WIF Format ein base58 kodierter String des privaten Schlüssels[17], der zusätzlich um eine Prüfsumme ergänzt wurde. Mit der Prüfsumme kann zum Beispiel überprüft werden, ob ein gegebener Schlüssel gültig ist. Ein Vorteil der base58 Kodierung ergibt sich bei der Offline-Nutzung dieses Schlüssels, sollte man

[17] Sorge, Christoph; Krohn-Grimberghe, Artus (2012), Datenschutz und Datensicherheit

jemandem physischen Zugriff auf seine Transaktionen geben wollen. In base58 sind im Vergleich zu der Kodierungsart base64 weder Sonderzeichen noch die visuell schwer voneinander unterscheidbaren Zeichen Null (0) und der Buchstabe O bzw. die Buchstaben I (wie Ida) und l (wie Ludwig) enthalten, wie man in Abbildung 2.2 erkennen kann.

öffentlicher Schlüssel:

1CxsdkVhA5dCqLh85921vT27HdD4hrC8T8

privater Schlüssel:

0C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D

WIF Key:

5KgwtHbHNbpHoY34G5SoD8SxhZTFkBKbQzZQ4dyY9AwrUU5XBWc

Abbildung 2.2: Vergleich der Adresstypen (Quelle: bitaddress.org)

Zu dem digitalen, dateibasierten Lagern der Schlüsselpaare mithilfe von Computern gibt es auch Paper Wallets und Hardware Wallets. Diese besonderen Formen der Wallet-Speicherung ermöglichen die alltägliche Nutzung von Bitcoins zum Beispiel für den Kauf einer Mahlzeit. Man kann also ein Schlüsselpaar erzeugen, es auf ein Blatt Papier drucken und wie einen Scheck benutzen. Der Betrag dieses Schlüsselpaares hängt von der Menge an Geld ab, das man an die aufgedruckte Adresse geschickt hat.

Abbildung 2.3: Paperwallet erzeugt durch bitaddress.org

Zusätzlich gibt es Hardware Wallets, wie den TREZOR, der private Schlüssel ausschließlich auf dem Gerät selbst speichert und diese durch ein begrenztes USB Protokoll nicht herausgeben kann. Erst nach dem physischen bestätigen eines Knopfes am Gerät wird eine Transaktion durch das Gerät signiert. Die Signatur wird an den Rechner übergeben, mit dem die Zahlung durchgeführt wird[18].

2.2 Transaktionen

Im Bitcoin Netzwerk existieren Werte nicht als absolute Zahl in einem Konto, wie es bei einem konventionellen Bankkonto der Fall ist. Stattdessen setzt sich der verfügbare Wert eines Kontos aus der Historie aller zugrundeliegenden Transaktionen zusammen.

Möchte z.B. eine Teilnehmerin Alice an Teilnehmer Bob einen Betrag an Bitcoins versenden, dann muss sie nachweisen, dass sie zuvor bereits Transaktionen in mindestens gleicher Höhe erhalten hat. Dafür gibt sie Bob gegenüber alle Transaktionen an, die sie selbst erhalten hat. Diese Transaktionen heißen Inputs, werden im Allgemeinen allerdings als Coins beschrieben. Coins sind also die für einen Teilnehmer verfügbaren Inputs. Bob kann mithilfe der Blockchain (siehe Punkt 2.4) in der gesamten Transaktionshistorie nachsehen, wo die Inputs herkamen, wie viel Wert sie besitzen und ob Alice diese bereits ausgegeben hat. Für Alice ist die Übertragung an Bob ein Output, für Bob ist die Transaktion von Alice ein Input. Die schematische Darstellung in Abb. 2.4 zeigt die Transaktion von Alice an Bob unter Verwendung zweier Inputs. Die Transaktion "#13ab3..." ist die Transaktion an Bob. Für Bob ist sie ein Input, den er bei einer späteren Transaktion benutzen kann. Transaktionsgebühren werden in dieser Darstellung noch nicht berücksichtigt.

[18] Anonym (2014), SatoshiLabs

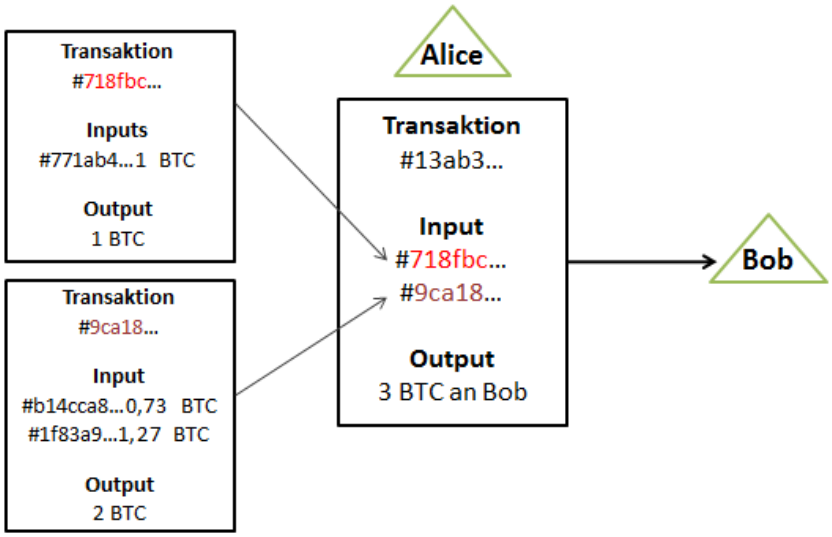

Abbildung 2.4: Transaktion mit Input-Nachweis von Alice an Bob (Eigene Darstellung)

Bei der in Bitcoin implementierten Form des ECDSA Verfahrens kann der öffentliche Schlüssel aus einer Signatur wiederhergestellt werden. Erst wenn sich ein Teilnehmer entscheidet Bitcoins zu verschicken wird auch sein öffentlicher Schlüssel offenbart. Vorher bleiben öffentlicher und privater Schlüssel unbekannt, wodurch die Sicherheit einzelner Teilnehmer vor Attacken gewährleistet wird. Der Empfänger kann seinen öffentlichen Schlüssel für den Empfang von Bitcoins trotzdem z.B. auf einer Webseite kommunizieren ohne eine Attacke auf selbigen zu befürchten. Offen kommuniziert wird nur der Hash des öffentlichen Schlüssels. Dadurch ist kein Rückschluss auf den öffentlichen Schlüssel in ursprünglicher Form möglich.

Sobald die Teilnehmer des Netzwerkes eine Transaktion erhalten haben, können sie diese Überprüfen. Für die Überprüfung gibt es zu jeder Transaktion eine Instruktionskette, die Script genannt wird. Diese Scripts enthalten eine detaillierte Anweisung zur Einlösung der Transaktion durch den Empfänger. Bei einer typischen Bitcoin Transaktion werden dem Empfänger 2 Voraussetzungen zur Einlösung gestellt. Der Empfänger muss:

1. einen öffentlichen Schlüssel nachweisen, dessen Hash dem angegebenen Ziel gleich ist.
2. Eine mit dem privaten Schlüssel erzeugte Signatur, die den vom Absender angegebenen Schlüssel als den eigenen identifiziert.

Die Anforderungen können allerdings auch erweiterte Anweisungen enthalten, sodass beispielsweise zwei private Schlüssel für die Erzeugung der Signatur erforderlich sind oder gar keiner. Die Verwendung mehrerer privater Schlüssel hat unter anderem eine Erhöhung der Sicherheit zur Folge, da bei Lagerung auf 2 voneinander getrennten Computern ein Angriff auf einen der

beiden den Angreifer noch nicht zu der Verwendung der Bitcoins befähigt[19].

2.3 Wechselgeld

Bei einer Transaktion von Bitcoins kann es vorkommen, dass die Werte der Inputs nicht exakt die benötigte Höhe des Transaktionsvolumens haben, das versendet werden soll. Sobald ein Teilnehmer z.B. 4 BTC Input zur Verfügung hat, jedoch einen geringeren Betrag ausgeben möchte, muss eine Art Wechselgeld eingeführt werden. Deshalb wird der Output grundsätzlich immer auf 2 Zieladressen aufgeteilt. Die erste ist die des eigentlichen Empfängers und trägt genau die zu versendende Summe. Die zweite Zieladresse ist die eigene Adresse, auf die der Gesamtbetrag der verwendeten Inputs abzüglich des versendeten Betrages und abzüglich einer Transaktionsgebühr übertragen wird[20]. Das Prinzip ist in etwa vergleichbar mit gestaffelt großen Werten von Banknoten. Kostet eine Ware in einem Ladengeschäft €5,50, dann kann entweder mit €5 und €0,50 passend bezahlt werden (mehrere Inputs, die zusammen exakt auf die Zielgröße kommen) oder man gibt €10 her um das Wechselgeld wieder an sich selbst ausgezahlt zu bekommen.

Inputs

Von Adresse	Betrag BTC
1E3FHSXSPx...	0,2194344
1E3FHSXSPx...	0,10179509
1E3FHSXSPx...	0,2242057
Gesamt	**0,54543519**

Outputs

Nach Adresse	Betrag BTC
1E2zmVJcW...	0,5
1E3FHSXSPx...	0,04533519
Gesamt	**0,54533519**
Gebühr	**- 0,0001**

Abbildung 2.5: Inputs und Outputs einer Transaktion (Eigene Darstellung

Aus Abb. 2.5 wird ersichtlich, wie ein Absender mit drei Input-Beträgen an einen Empfänger versendet und zusätzlich den Restbetrag an seine eigene Adresse zurück sendet. Die meisten Bitcoin Anwendungen legen für den Rücktransfer des Wechselgeldes automatisch eine neue Adresse an, anstatt sie auf der gleichen Adresse wie zuvor als neuen Input zu empfangen.

[19] Anonym (2014), Bitcoin Wiki

[20] Nakamoto, Satoshi (2008), Bitcoin Whitepaper (Abs. 9)

Die Erzeugung einer neuen Adresse verspricht mehr Sicherheit, da aus der Signatur einer Transaktion der öffentliche Schlüssel berechnet werden kann und damit "nur" noch ein Angriff auf den privaten Schlüssel erfolgen muss. Der zweite Grund für die Benutzung einer neuen Adresse für den Restbetrag ist die Anonymität bei der Benutzung von Bitcoin. Da alle Transaktionen für jeden einsehbar sind, ist es leicht bei einmal verknüpfter Identität eine Person anhand der Bitcoin-Adresse zu überwachen. Werden immer neue Adressen erzeugt, an die Restbeträge zurück gesendet werden, dann wird es zunehmend schwieriger alle Adressen einer Person zuzuordnen und diese zu überwachen.

Wie weiterhin in Abb. 2.5 ersichtlich ist, wurde in dem Beispiel eine Transaktionsgebühr von 0,0001 Bitcoins erhoben. Gebühren sind rein theoretisch nicht erforderlich, damit eine Transaktion bearbeitet wird. Allerdings dient die Gebühr als Anreiz für Miner, die Rechenleistung für die Validierung von Transaktionen aufwenden. Der Miner, der einen Block gelöst hat, erhält die gesamten Transaktionsgebühren und den "Block Reward". Es ist sehr wahrscheinlich, dass Transaktionen ohne Gebühr nicht in die Blockchain aufgenommen werden, doch das hängt vom jeweiligen Miner ab[21].

[21] Nakamoto, Satoshi (2008), Bitcoin Whitepaper (Abs. 4)

2.4 Blockchain als Prüfmechanismus

Nach der Validierung einer Transaktion muss sichergestellt werden, dass der Absender einen Input nicht erneut referenzieren kann. Aus diesem Grund gibt es die Blockchain, die als eine Datenbank über alle vergangenen Transaktionen dient. Die Blockchain besteht aus mehreren Blöcken, wobei jeder Block jeweils eine Referenz auf den vorherigen Block enthält. In diesen Blöcken werden Transaktionen gesammelt, die von den Teilnehmern des Netzwerkes überprüft und für valide befunden wurden. Neue Blöcke können nur von Minern gebildet werden, da die Erstellung eines Blocks das Lösen eines mathematischen Rätsels erfordert.

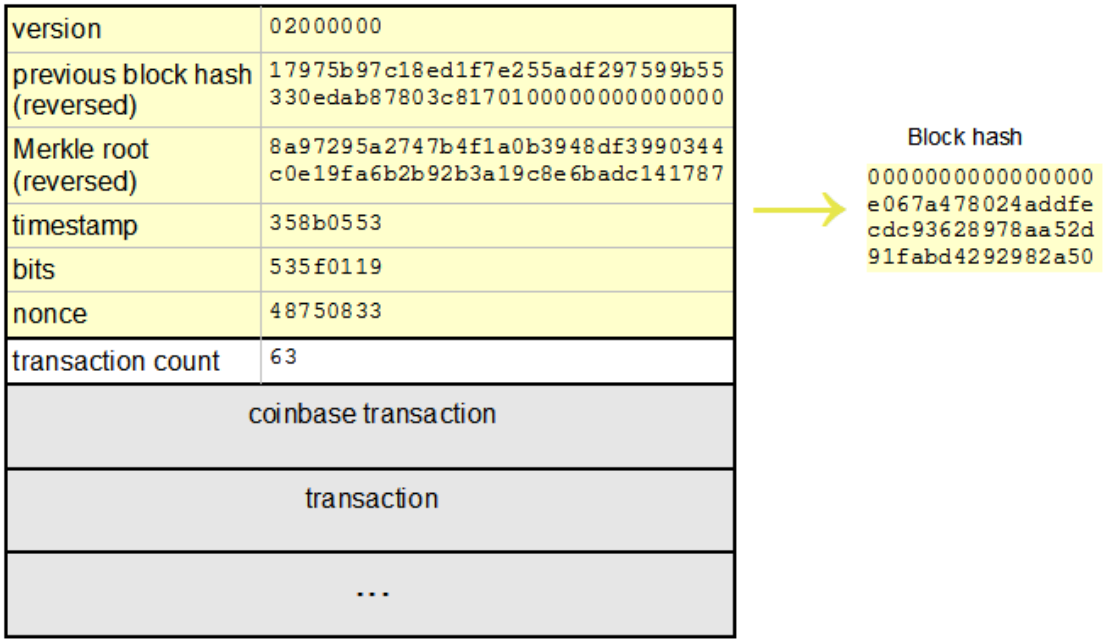

Abbildung 2.6: Headerstruktur eines Blocks (Quelle: Ken Shirriff - righto.com)

In dem Block am Ende der Kette befindet sich die Vorgabe eines bestimmten Schwellwertes, den die Lösung des nachfolgend erzeugten Hashes unterschreiten muss. Der Hash wird aus den in Abb. 2.6 ersichtlichen Header-Informationen gebildet. Veränderliche sind neben der Versionsnummer vor allem der "Merkle root", der einen Hash aus den bisher gesammelten Transaktionen enthält, der Timestamp und ein Nonce. Ein Nonce ist ein ansteigender Wert, der lediglich dazu dient, die Nachricht und damit auch ihren Hash zu verändern. Der Wert “bits“ aus Abb. 2.6 beschreibt den Schwellwert und damit den aktuellen Schwierigkeitsgrad. Miner werden nie parallel die gleichen Hashes berechnen, da sie in der Blocklösung, an der sie Arbeiten jeweils ihre eigene Adresse für “coinbase transaction“ angeben und sich dadurch der individuelle Hash der Gesamtlösung verändert. Das Feld “coinbase transaction“ beschreibt an

welche Adresse die Belohnung für den Block geschickt werden soll[22].

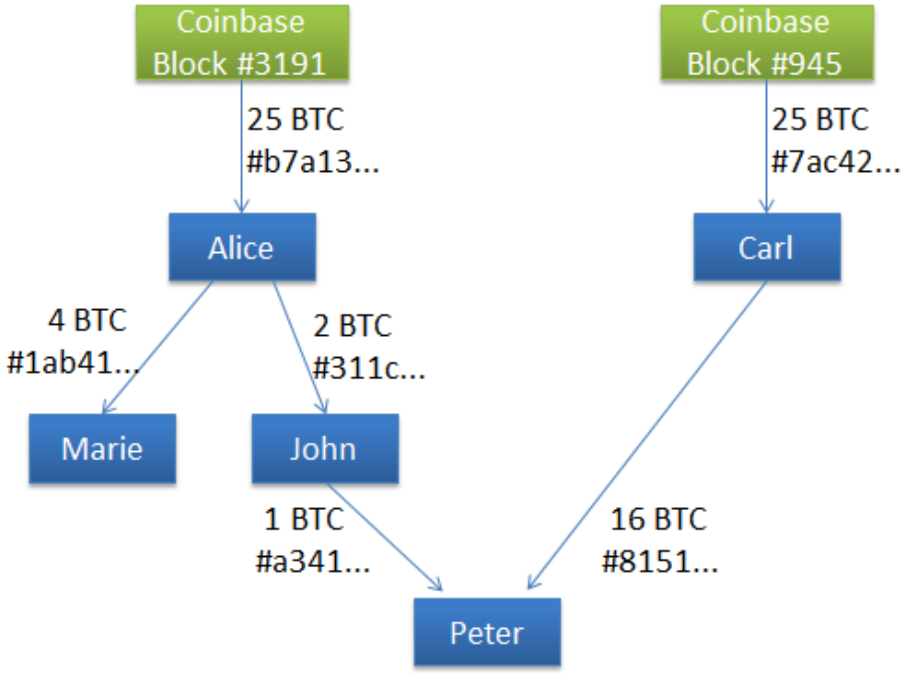

Abbildung 2.7: Verlauf der Transaktionen ab Coinbase

Diese Transaktion, die Belohnung für die Blocklösung, ist immer der Ausgangspunkt für alle folgenden Transaktionen. Hier werden Coins ursprünglich geschaffen. Anders ausgedrückt ist die Coinbase immer der erste Input in einer Kette von Transaktionen. Wie in Abb. 2.7 abgebildet werden Inputs in einer Baumstruktur bis zu ihrer Coinbase zurückverfolgt. Ist die Kette aller Transaktionen bis zur Coinbase zurück valide, so zählt ein Input als gültig und kann für eine weitere Transaktion verwendet werden.

Die Blockchain ist das Herz von Bitcoin und auch anderer dezentraler Währungen, weshalb deren fortlaufende Generierung essenziell für den Erhalt der Währung ist. Um den Minern einen Anreiz zu geben ihre Ressourcen für die Verarbeitung von Transaktionen zur Aufnahme in die Blockchain zu verwenden, wird für einen Block eine fest definierte Anzahl Bitcoins ausgeschüttet. Diese Belohnung nennt sich "Block Reward" und wird in Form der initialen Transaktion, der Coinbase, ausgeschüttet. Diese Anzahl lag zu Beginn bei 50 BTC, liegt derzeit bei 25 BTC und soll im Mittel alle 4 Jahre halbiert werden bis rechnerisch im Jahr 2140 der letzte vergütete Block die Nummer 6.929.999 tragen wird. Auch danach werden weiterhin Blöcke erzeugt, der Anreiz wird dann jedoch durch die Ausschüttung der

[22] Shirriff, Ken (2014), Righto.com

Transaktionsgebühren geschaffen. Derzeit werden diese ebenfalls ausgeschüttet, allerdings summieren sie sich auf vergleichsweise geringe 0,05 bis 0,2 BTC je nach Menge der im Block enthaltenen Transaktionen.

Mit steigender Rechenleistung der Miner steigt auch die Schwierigkeit zur Berechnung der Blöcke. Das Konzept von Bitcoin sieht eine mittlere Lösungszeit von 10 Minuten pro Block vor, um langfristig die Stabilität des Netzes zu gewährleisten. Deshalb wird der Schwellwert alle 2016 Blöcke oder bei Einhaltung der 10-minütigen Blocklösungszeit alle 2 Wochen nach oben oder unten angepasst.

2.5 Erzeugung von BTC

Wie bereits beschrieben dient das Erzeugen von Bitcoins gleichzeitig dem Erhalt der Währung. In den Anfängen war die Anzahl Teilnehmer und deren Rechenleistung noch gering, sodass jeder mit einem gewöhnlichen Computer mit recht hoher Wahrscheinlichkeit einen korrekten Hash finden und damit Bitcoins verdienen und das Bitcoin Netz sichern konnte.

Mit der steigenden Anzahl an Teilnehmern wuchs auch die Rechenleistung stark an. Berechnungen wurden auf GPUs ausgelagert und später gar auf ASICs, die nichts anderes tun als Hashes zu berechnen. Heutzutage ist es selbst mit mehreren GPUs oder kleinen ASICs so enorm unwahrscheinlich einen Block zu lösen, dass sich viele Miner einem Mining Pool anschließen. In einem Mining Pool werden die Berechnungen verteilt, sodass jeder nur eine gewisse Menge Berechnungen durchführt, damit aber schlussendlich zur Lösung beiträgt und durch den Pool anteilig entlohnt wird.

```
[2014-08-15 21:10:03] thread 0: 3932 hashes, 2.02 khash/s
[2014-08-15 21:10:03] thread 1: 1180 hashes, 2.21 khash/s
[2014-08-15 21:10:03] Stratum requested work restart
[2014-08-15 21:10:26] thread 1: 45032 hashes, 2.07 khash/s
[2014-08-15 21:10:26] accepted: 2/2 (100.00%), 4.09 khash/s (yay!!!)
[2014-08-15 21:11:01] thread 0: 120968 hashes, 2.13 khash/s
[2014-08-15 21:11:23] thread 1: 124496 hashes, 2.17 khash/s
[2014-08-15 21:12:00] thread 0: 128060 hashes, 2.17 khash/s
```

Abbildung 2.8: Mining mit erhaltenem Share (eigene Abb.)

Als Grundlage für die Anteilige Beteiligung an dem Gewinn eines Mining Pools dient die Anzahl Shares (siehe Abb. 2.8), die ein Miner entdeckt. Wenn also im Netzwerk zur Lösung eines Blocks aktuell ein Hash unter einem Schwellwert von 00000007 gesucht wird, akzeptiert ein Mining Pool bereits Hashes mit einem höheren Schwellwert ab z.B. 00001. Durch den Fund

dieser Hashes beweist ein Miner gegenüber den Mining Pool seinen Arbeitseinsatz und der Pool kann anhand der Shares eines Miners den Gewinnanteil eines einzelnen bestimmen ohne jeden einzelnen Hash zu überprüfen. Wenn der übermittelte Hash mit dem höheren Schwellwert zusätzlich auch den schwereren Schwellwert des aktuellen Blocks unterschreitet hat der Pool den Block gefunden bzw. das Rätsel gelöst. Der Pool bekommt die volle Belohnung inklusive Transaktionsgebühren anderer Miner und schüttet diesen nach seinen Regeln an die Teilnehmer des Pools aus[23].

2.6 Netzwerk

Das Bitcoin Netzwerk basiert auf dem Peer-to-Peer (P2P) Prinzip, was bedeutet, dass Teilnehmer untereinander direkt kommunizieren. Teilnehmer schicken via Broadcast allen ihnen bekannten Teilnehmern die Information über ihre Transaktion. Diese senden die Informationen wiederum an alle ihnen bekannten Teilnehmer. Um direkt bei dem erstem Start der Software Teilnehmer kennen zu lernen, wurden in Bitcoin verschiedene Techniken umgesetzt. Da die Kommunikation mit anderen Teilnehmern die wichtigste Komponente von Bitcoin und allen anderen dezentralen Währungen ist, gibt es zahlreiche Möglichkeiten IP-Adressen von anderen Teilnehmern in Erfahrung zu bringen.

Die einfachste Form der Bekanntmachung anderer Teilnehmer ist das direkte Hinzufügen der IP-Adressen anderer Teilnehmer über einen Kommandozeilen-Parameter bei Aufruf der Software. Hierzu kann der Bitcoin-Client IP-Adressen über den Parameter "-addnode <ip>" ansprechen. IP-Adressen anderer Teilnehmer lassen sich auch aus einer Liste laden, indem eine Datei namens "addr.txt" im Bitcoin-Verzeichnis abgelegt wird. Der Bitcoin Client sucht bei Start nach dieser und läd die Adressen automatisch.

Wenn Teilnehmer keine direkten IP-Adressen von anderen Teilnehmern angeben können, werden fest im Programmcode hinterlegte "Domain Name System" (DNS) Server angefragt. Die übliche Aufgabe der Namensauflösung von Internetadressen macht sich Bitcoin hier zunutze, indem es DNS Server mit einer Liste an passenden Adressen für einen Namen antworten lässt.

Wie in Abb. 2.9 ersichtlich antwortet die Domain "bitseed.xf2.org" mit einer Liste an IP-Adressen. Der Betreiber dieser Domain prüft regelmäßig, ob die IP-Adressen tatsächlich noch ansprechbare Bitcoin Teilnehmer sind und hält diese aktuell. Derzeit werden sieben verschiedene DNS-Server verwendet[24].

[23] Goetz, Philipp (2011), pensan's Blog

[24] Anonym (2014), Github

```
;; QUESTION SECTION:
;bitseed.xf2.org.               IN      A

;; ANSWER SECTION:
bitseed.xf2.org.        1310    IN      A       24.52.35.44
bitseed.xf2.org.        1310    IN      A       50.177.196.160
bitseed.xf2.org.        1310    IN      A       68.48.214.241
bitseed.xf2.org.        1310    IN      A       76.111.96.126
bitseed.xf2.org.        1310    IN      A       85.214.90.1
bitseed.xf2.org.        1310    IN      A       94.226.111.26
bitseed.xf2.org.        1310    IN      A       96.2.103.25
bitseed.xf2.org.        1310    IN      A       97.117.255.48
bitseed.xf2.org.        1310    IN      A       99.242.230.163
bitseed.xf2.org.        1310    IN      A       162.243.194.210
```

Abbildung 2.9: Anfrage an bitseed.xf2.org gibt IP-Adressen zurück (eigene Abb.)

Als letzten Ausweg verwendet die Bitcoin Software eine integrierte Liste an IP-Adressen von besonders zuverlässigen Teilnehmern. Diese werden allerdings erst nach mehreren erfolglosen Anfragen an DNS-Server verwendet, um die einzelnen Teilnehmer nicht zu überlasten.

Nachdem die ersten Teilnehmer bekannt sind, tauscht der Bitcoin-Client Informationen über weitere aktive Teilnehmer direkt mit den bekannten Teilnehmern aus. Dabei werden ganze Listen an qualifizierten Teilnehmern weitergegeben. Qualifizierte Teilnehmer zeichnen sich durch eine aktuelle Version des Bitcoin-Clients und durch eine regelmäßige Antwort auf Anfragen aus.

3 Vergleich zu anderen Währungen

Neben Bitcoin haben sich mittlerweile viele andere Währungen etabliert, die umgangssprachlich Altcoins, also alternative Coins genannt werden. Obgleich alle Währungen in ihren Grundeigenschaften ähnlich konzipiert sind, unterscheiden sie sich teilweise in den Details ihrer Umsetzung und haben ihre eigenen Vor- und Nachteile gegenüber Bitcoin.

Rang	Währung	Marktkapitalisierung in USD	Preis pro Coin in USD
1	Bitcoin	7,469,159,907	568.78
2	Litecoin	178,115,849	5.73
3	Ripple	41,750,154	0.005059
4	Nxt	32,457,906	0.032458
5	Darkcoin	22,494,249	4.94
6	Peercoin	17,453,937	0.806843
7	BitSharesX	17,303,474	0.008653
8	Dogecoin	12,829,356	0.000143
9	Namecoin	12,151,123	1.27
10	MaidSafeCoin	11,569,050	0.025564

Tabelle 3.1: Marktkapitalisierung beliebter Coins am 12.08.2014 (coinmarketcap.com)

Die Betrachtung Ihrer Unterschiede soll eine kritische Einschätzung der Zukunft dezentraler, elektronischer Währungen ermöglichen. Da mittlerweile weit über 100 alternative Währungen existieren und wöchentlich neue hinzukommen, wird sich der Vergleich hauptsächlich auf die Währungen beziehen, die bereits eine höhere Marktkapitalisierung (Tab. 3.1) erreicht und damit ein gewisses Vertrauen ihrer Nutzer erlangt haben.

Die Anforderungen an elektronische Zahlungssysteme wurden durch verschiedene Personen

schon vor der Entstehung dezentraler Systeme formuliert. Diesen Anforderungen folgend gab es zunächst zentrale, elektronische Währungen mit Namen wie E-Cash oder CyberCash, bei denen es nur einen vertrauenswürdigen Akteur gibt, der Transaktionen absichern kann. Die wichtigsten sechs Anforderungen nach Okamoto und Ohta[25] sind hierbei Unabhängigkeit, Sicherheit, Anonymität, Offline-Verwendbarkeit, Transferierbarkeit und die Wechselgeldfähigkeit. Diese Kriterien gelten auch heute noch und sind sicher auch gute Grundkriterien für dezentrale, elektronische Geldsysteme.

Bei der in dieser Arbeit behandelten speziellen Form des elektronischen Geldes findet der gesamte Prozess der Erzeugung und des Austausches der Währung im Internet statt, weshalb einige zusätzliche Kriterien Beachtung finden müssen. Hierzu gehören Quantität der Währungseinheiten, Transaktionsgeschwindigkeit, Erzeugung, Stabilität des Netzes und die ökonomische Stabilität der Währungen. Da sich die verschiedenen Währungen in ihrem Kernkonzept stark an Bitcoin anlehnen gibt es einige Aspekte wie z.B. die Benutzung von Schlüsselpaaren für das Signieren und Validieren von Transaktionen, die sich durch alle Währungen durchziehen und somit im Vergleich keine Beachtung finden. Allerdings gibt es unter den alternativen Systemen zahlreiche Abwandlungen, die sie von ihrem Vorbild unterscheiden. Diese gilt es zu untersuchen und eine Tendenz für die Gesamtheit aller dezentralen Währungen abzuleiten.

3.1 Stabilität des Netzes

Eingangs wurde beschrieben, dass Teilnehmer untereinander via Broadcast Informationen über neue Blöcke und Transaktionen austauschen, um zusammen die Blockchain zu verwalten. Allerdings sind nur die Teilnehmer in der Lage diese Informationen zu verwerten, die "Full Nodes" betreiben. Das bedeutet, dass nur Teilnehmer, die die gesamte Blockchain vorhalten, in der Lage sind Informationen auszutauschen. Nur so können Transaktionen in ihrer Historie bis zur ihrer ursprünglichen Coinbase-Transaktion zurückverfolgt und validiert werden (Abb. 2.7).

Ein Benutzer betreibt unter Verwendung der offiziellen Wallet-Software meist automatisch einen Full Node. Startet man die Software erstmalig wird zunächst eine initiale Synchronisation mit anderen Teilnehmern erfolgen, um alle historischen Blöcke der Blockchain zu laden. Je nach Gesamtanzahl der getätigten Transaktionen in der Währung kann der Prozess mehrere Tage dauern und viel Speicherplatz in Anspruch nehmen (siehe Tab. 3.2).

Ist die Blockchain erst einmal synchronisiert benötigt der Betrieb der Software nahezu keine Ressourcen. Selbst auf einem Mini-Computer wie der "Raspberry Pi" ist der Betrieb ohne

[25] Okamoto, Tatsuaki; Ohta, Kazuo (1991), Advances in Cryptology

Währung	Datum 1. Block	Speicherverbrauch in Gigabyte
Bitcoin	09.01.2009	26,08
Dogecoin	08.12.2013	5.82
Litecoin	08.10.2011	3,81
Namecoin	19.04.2011	1.90
Nxt	24.11.2013	1,4
Darkcoin	19.01.2014	0.34
Peercoin	19.08.2012	0.31

Tabelle 3.2: Einige Blockchain Speichergrößen - Stand 08/2014 (Eigene Messung)

weiteres möglich. Die Größe der Blockchain ist von der Anzahl Transaktionen im Netzwerk abhängig, da mit jeder Transaktion eine gewisse Menge Daten gespeichert werden müssen. Für den Erhalt der Dezentralität elektronischer Währungen ist es äußerst wichtig, dass viele Teilnehmer einen Full Node betreiben. Das hat 3 einfache Gründe:[26]

1. Full Nodes dienen der Synchronisierung neuer Nodes.

2. Full Nodes bieten die Möglichkeit Transaktionen im "Simplified Payment Verification" (SPV) Verfahren zu validieren.

3. Full Nodes validieren Blöcke und Transaktionen und leiten sie weiter.

Während diese Eigenschaften scheinbar trivial wirken, sind sie doch äußerst wichtig für die Stabilität des Netzes. Von diesen Handlungen hängt die Sicherheit, das Vertrauen und letztendlich der Wert der Währung ab. Bei der SPV Methode wird eine Transaktion validiert, indem einer oder mehrere vertrauenswürdige Full Nodes gefragt werden, in welchem Block eine Transaktion enthalten ist. Wenn die Transaktion bereits in einem Block enthalten ist geht der Client davon aus, dass die Transaktion bereits bis an ihren Ursprung zurückverfolgt und damit validiert wurde. Der Client vertraut bei dieser Variante also den Full Nodes[27].

Es gibt derzeit allerdings trotz ihres hohen Nutzens keine unmittelbare Belohnung für das Betreiben eines Full Nodes. Man könnte das Betreiben eines Full Nodes im Proof of Stake

[26] Lopp, Jameson (2014), Medium

[27] Nakamoto, Satoshi (2009), The Bitcoin Foundation

Verfahren (Abschnitt 3.2) als reizvoll betrachten, da der geöffnete Client Voraussetzung für das Minen ist. Allerdings ist zusätzlich der Besitz von Coins Voraussetzung, womit sich die Belohnung nicht auf das Betreiben des Nodes selbst bezieht. Die Transaktionsgebühren und der Block Reward wird einzig den Minern zugeschrieben. In den meisten Fällen sind Miner in Mining Pools organisiert, um schneller einen gewissen Anteil an der Belohnung für die Blockerstellung zu erhalten. Das bedeutet allerdings, dass die hohe Anzahl Miner selbst keinen Full Node betreiben, sondern lediglich der Server, dem sie ihre Berechnungen übermitteln. Nur dieser muss andere Transaktionen annehmen und in einen Block integrieren, wenn die Lösung gefunden wird. Das hat zur Folge, dass die Anzahl der Full Nodes immer weiter zurückgeht wie in Abb. 3.1 zu sehen ist. Die Grafik zeigt die Anzahl an Full Nodes im Zeitraum von Anfang März bis Anfang Mai, wobei im März ca. 9300 Nodes erfasst wurden und im Mai nur noch knapp 7700 Nodes. Zum jetzigen Zeitpunkt (08/2014) liegt die Anzahl bereits knapp unter 7000 Nodes.

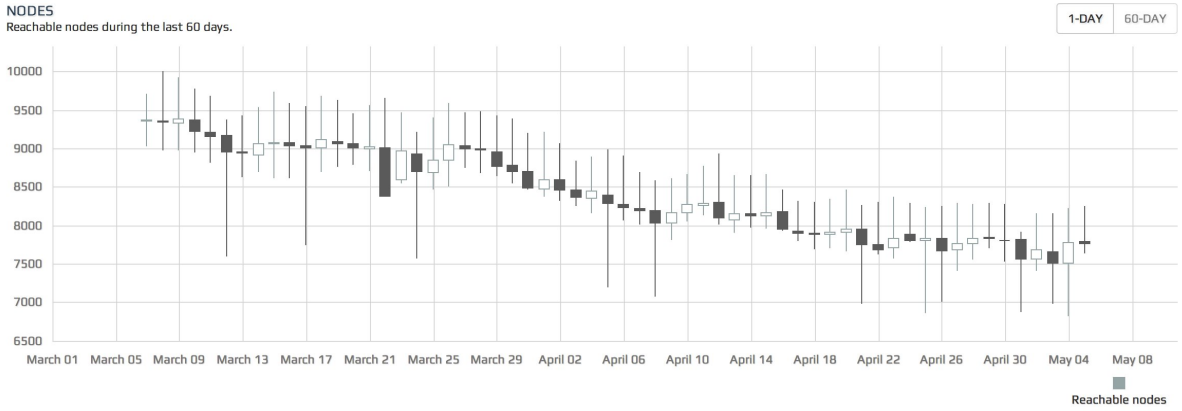

Abbildung 3.1: Anzahl Full Nodes ist stark rückläufig (Quelle: getaddr.bitnodes.io)

Hinzu kommt, dass die Verteilung der Betreiberländer sehr ungleich ist und ein hoher Schwerpunkt auf den Ländern USA, Deutschland und dem Vereinigtes Königreich liegt.

Weil momentan noch nicht vollständig geklärt ist wie das Bitcoin Netzwerk mit einer großen Menge Transaktionen umgehen soll, gibt es derzeit ein Limit von ca. 7 Transaktionen pro Sekunde bzw. darf ein Block der Blockchain nur bis zu 1 Megabyte groß sein[28]. Dieses Limit gilt zwar auch für alternative Währungen wie Litecoin, allerdings wird z.B im Litecoin Netzwerk alle 2,5 Minuten ein Block erzeugt während im Bitcoin Netzwerk alle 10 Minuten ein Block erzeugt wird. Obwohl also die Blockgröße auch bei Litecoin auf 1 Megabyte begrenzt ist, kann durch kürzere Blockerzeugungs-Intervalle eine bis zu vierfache Menge Transaktionen je Sekunde verarbeitet werden.

Es gibt verschiedene Ansätze zur Reduzierung des Speicherbedarfs der Blockchains von elek-

[28] Lee, Timothy B. (2013), The Washington Post

tronischen Währungen. Eine von ihnen ist das "Pruning", also das Bereinigen der Blockchain. Hierbei sollen alte Inputs, deren Betrag komplett aufgebraucht wurde, gelöscht werden, wenn sie lange genug existieren. Die Idee ist, dass in einem Netzwerk weitestgehend nur die Inputs vorgehalten werden, die noch ungenutzte Coinbeträge enthalten und ihre Vorgeschichte als bestätigt gelten soll. Betrachtet man nur diese sollte die Größe der Blockchain dramatisch sinken. Kritiker befürchten, dass mit dem Löschen der Vorgeschichte unter Umständen Lücken in der Nachvollziehbarkeit entstehen. Sie schlagen 2 Typen von Nodes vor, 1. die "Archiv Nodes" und 2. die "Light Nodes". Erstere sollen weiterhin alle Transaktionen archivieren, damit sie für einen späteren Zugriff zur Verfügung stehen. Letztere sollen nur die Inputs vorhalten, die noch nicht verwendet wurden[29].

Die zweite Methode, mit der Transaktionen gar nicht erst in die Blockchain gelangen, sind Off-Chain Transaktionen. Hierbei tauschen Benutzer Coins untereinander auf Handelsplattformen. Die Coins wechseln somit zwar den Besitzer, jedoch bleibt dabei immer der Betreiber der Plattform der eigentliche Besitzer gegenüber dem Bitcoin Netzwerk, da er die Inputs seiner Benutzer verwaltet.

3.2 Erzeugung von Coins

Für ihren Erhalt und zur Sicherung der Dezentralität ist allen Währungen gemein, dass Teilnehmer des Netzes die innerhalb des Netzwerks getätigten Transaktionen verifizieren und speichern müssen. Für die Strukturierung in Blöcken müssen sich alle Teilnehmer darüber einig sein, wer den jeweils nächsten Block löst. Weil es für die Lösung eines Blocks eine Belohnung gibt muss es schwer genug sein eine Lösung zu finden. Deshalb muss eine Voraussetzung existieren, die alle Teilnehmer als aufwändig akzeptieren. Für diesen Prozess gibt es verschiedene Ansätze unter den Währungssystemen. Neben Proof of Work (PoW) wird Proof of Stake (PoS, s. 3.1.2) als Beweisverfahren immer populärer, da nur jemand mit einer gewissen Menge an Coins und ohne großen Aufwand von Rechenleistung Transaktionen verarbeiten kann. Es gibt daneben auch noch weniger populäre Verfahren wie Proof of Burn (PoB) oder sogar bei der Währung Unitas[30] Proof of Learn, bei dem der Beweis einer Leistung aus dem Konsumieren oder Erschaffen von Texten bzw. Medien besteht. Häufiger werden auch hybride Verfahren genutzt, sodass bei der Generierung bis zu einer bestimmten Menge an Coins PoW zum Einsatz kommt, die Währung anschließend allerdings mit PoS weiter betrieben wird.

[29] Lee, Timothy B. (2013), The Washington Post

[30] M., Ernest (2014), LightCode Inc

Beweisverfahren	Währungen
PoW	Bitcoin, Litecoin, Dogecoin, Namecoin, Primecoin, Vertcoin, Feathercoin
PoS	Nxt, Blackcoin
PoB	Counterparty
PoB + PoS	Slimcoin
PoW + PoS	Peercoin, Darkcoin

Tabelle 3.3: Übersicht einiger Währungen und verwendetem Beweisverfahren

3.2.1 Proof of Work

Das eingangs erwähnte Proof of Work Verfahren kommt nicht nur bei Bitcoin, sondern auch bei Litecoin, Dodgecoin, Primecoin, Worldcoin, Feathercoin und den vielen weiteren Währungen zum Einsatz.

Dabei wird ein mathematisches Problem ausgeschrieben, das schwer zu lösen ist, dessen Lösung aber sehr leicht durch alle Teilnehmer überprüft werden kann. Dieses mathematische Problem verfolgt in fast allen Fällen keine wissenschaftliche Zielstellung, da die Komplexität der Aufgabe steuerbar hoch bleiben und damit in etwa vorhersagbar sein muss. Weiterhin muss die Überprüfung der Lösung sehr einfach für jeden Teilnehmer mithilfe von gewöhnlicher Hardware möglich sein. Wäre die Dauer der Lösung einer Aufgabe vollständig dem Zufall überlassen, wäre nicht absehbar wann der nächste Block an Transaktionen bestätigt werden würde. Dadurch würde ein Währungssystem instabil werden. Die Möglichkeiten eines wissenschaftlichen Nutzens dieser Systeme sind daher äußerst begrenzt.

SHA256

Bitcoin, Namecoin, Peercoin, Bytecoin und viele weitere setzen auf die Generierung von SHA256 Hashes. Die Komplexität der Hashes kann einfach gesteuert werden, indem der Schwellwert des Hashes hoch- bzw. heruntergesetzt wird. Moderne ASIC Miner können problemlos nicht nur für den Erhalt von Bitcoin, sondern auch allen anderen SHA256 basierten Währungen eingesetzt werden. Durch Ihre enorme Rechenleistung, die die Leistung moderner Grafikkarten um ein vielfaches übersteigt, machen sie gewöhnliche Hardware untauglich für das Minen und damit für den Erhalt der Währung. Insbesondere dieser Fakt erschwert den

Einstieg in SHA256-basierte Coinsysteme für eine breite Masse, da der Schwellwert für die zu findenden Hashes bereits zu Beginn recht niedrig ist, damit die Schwierigkeit hoch liegt und CPU-basierte Systeme eine sehr geringe Chance haben einen Block zu lösen.

Das Spitzenmodell des Grafikkarten-Herstellers ATI, "Radeon HD 7970", erreicht 825 Megahashes je Sekunde[31]. Das "The Monarch" genannte Modell des ASIC-Herstellers Butterflylabs, erzeugt im Vergleich 600.000 Megahashes je Sekunde bei gleichem Stromverbrauch. Es scheint ein Wettrennen der Ressourcen zu sein, an dem nur diejenigen teilnehmen können, die bereit und in der Lage sind viel Geld zu investieren. Die Hashraten der ASICs erhöhen sich unterdessen immer weiter. Das genannte Modell des Grafikkarten-Herstellers würde bedeutend mehr Strom verbrauchen als es Bitcoins mit entsprechendem Gegenwert erschaffen würde.

316111 (Main Chain)	2014-08-17 16:55:09	GHash.IO
316110 (Main Chain)	2014-08-17 16:46:08	GHash.IO
316109 (Main Chain)	2014-08-17 16:29:37	GHash.IO
316108 (Main Chain)	2014-08-17 16:21:51	P2Pool
316107 (Main Chain)	2014-08-17 16:22:06	Polmine
316106 (Main Chain)	2014-08-17 16:14:14	AntPool
316105 (Main Chain)	2014-08-17 16:09:11	Discus Fish
316104 (Main Chain)	2014-08-17 16:05:35	Discus Fish

Abbildung 3.2: Durch Pools gelöste Bitcoin Blöcke (Quelle: blockchain.info)

In der Folge steigen viele Teilnehmer aus dem Mining-Prozess aus und übrig bleiben verhältnismäßig wenig Personen, die für den Erhalt der Stabilität der Währungen sorgen müssen. Da nahezu niemand seine Chance als einzelner sieht ist die Nutzung von Mining Pools sehr verbreitet. Wie in Punkt 3.3.2 weiter vertieft, ist es äußerst gefährlich für eine dezentrale Währung, wenn mehrere Blöcke hintereinander durch einen Akteur erzeugt werden. In Abb. 3.2 ist ersichtlich, dass für den gewählten Zeitraum ausschließlich Mining Pools an der Erzeugung von Blöcken beteiligt waren.

Eine potenzielle Lösung ist die Benutzung sogenannter "P2Pools"[32]. In diesen dezentral organisierten Pools kommunizieren die Teilnehmer eines Pools nicht mit einem bestimmten Server eines einzigen Betreibers sondern direkt untereinander. Dabei wird unter den P2Pool

[31] Anonym (2014), Bitcoin Wiki
[32] Anonym (2014), P2Pool.in

Minern eine eigene Blockchain geführt, die “share chain“. In dieser Kette wird vermerkt, wie viele Shares ein Miner innerhalb eines Pools erhalten hat und wie hoch damit sein Anteil am Block Reward sein wird. Da jeder Miner die Blocklösung finden könnte, muss jeder Miner die komplette Blockchain vorhalten, um alle in den Block zu inkludierenden Transaktionen überprüfen zu können. “P2Pools“ haben demnach auch einen positiven Effekt auf die Verteilung von Full Nodes und erhöhen stärken die Dezentralität. Ein weiterer Vorteil ist auch, dass die Belohnung Transparent und direkt verteilt wird. Bei regulären Mining Pools muss man in der Regel eine gewisse Auszahlungshöhe erreichen, um überhaupt Coins zu erhalten.

Scrypt

Litecoin, die ihrer Marktkapitalisierung nach derzeit zweitgrößte dezentrale, elektronische Währung (siehe Tab. 3.1), verfolgt ebenfalls den PoW Ansatz zur Bestätigung von Transaktionen. Allerdings wird für die Hashberechnung statt SHA256 das Scrypt-Verfahren verwendet. Im Unterschied zu den rein rechenlastigen SHA256 Operationen, wird bei Verwendung von Scrypt der Ansatz verfolgt, dass sich der Speicherbedarf pro Rechenoperation asymptotisch verhalten soll um ein vernünftiges Verhältnis zu wahren. Je mehr Rechenoperationen durchgeführt werden sollen, desto größere Adressbereiche des Arbeitsspeichers werden erfordert. Das Ziel dieses Ansatzes ist es, ASIC Mining abzuwehren und eine größere Chancengleichheit unter den Minern zu schaffen, um letztendlich die Dezentralität der Währung zu erhalten.

ASIC Mining fördert den Zusammenschluss der Teilnehmer in Mining Pools, wobei langfristig alle den vielversprechendsten Pool wählen und die Dezentralität mehr und mehr gefährdet wird. Viele weitere Coins wie Novacoin, FeatherCoin, WorldCoin und Bitmark benutzen Scrypt als Mechanismus für Proof of Work. Im April 2014 wurden durch das Unternehmen Zeusminer erste ASIC Miner für das Scrypt Mining angekündigt. Die Hashrate ist zwar aufgrund der hohen Anforderungen an Arbeitsspeicher nicht mit ASIC für die SHA256 Erzeugung vergleichbar, allerdings stieg die Schwierigkeit zur Lösung eines Blocks daraufhin rapide an (siehe Abb. 3.3).

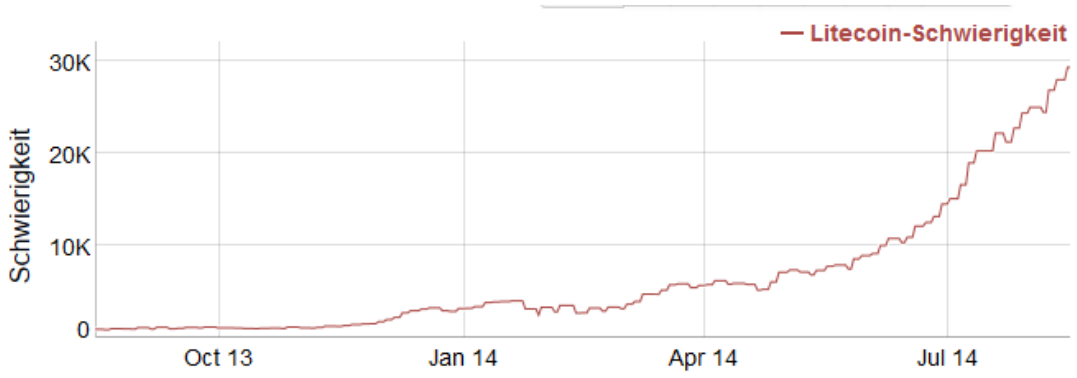

Abbildung 3.3: Anstieg des Schwierigkeitsgrades zur Erzeugung von Litecoin bei Veröffentlichung von Scrypt ASISs (Quelle: bitinfocharts.com)

Kurz vor Ankündigung der ersten ASIC Miner haben die Litecoin-Entwickler verkündet von dem herannahenden Problem zu wissen, jedoch hätten sie noch keine akzeptable Lösung des Problems gefunden und lehnen einen "Hard Fork" deshalb zur Zeit ab[33].

Ein Hard Fork einer Währung bedeutet, dass eine radikale Änderung des Programmcodes

[33] Anonym (2014), Litecointalk

stattfindet z.B. in Bezug auf die Art und Weise wie Coins generiert werden. In der Folge werden älteren Versionen der Anwendung nicht unterstützt, wodurch alle Teilnehmer auf die geänderte Version umsteigen müssen. Wenn die alte Version weiter betrieben wird entsteht eine parallele Version der Blockchain. Deshalb sollte ein Hard Fork lang genug vorher angekündigt und von allen Teilnehmern möglichst zur gleichen Zeit durchgeführt werden. Vor allem Händler müssen bei solch einer Umstellung äußerst vorsichtig vorgehen[34].

Mit Vertcoin gibt es einen Ansatz, der ebenfalls auf Scrypt basiert, bei dem aber der Speicherbedarf je Operation mit der Zeit automatisch angepasst wird. Eine Entwicklung von ASICs soll damit unwirtschaftlich gemacht werden, da die Hashrate nach Anschaffung eines ASICs schnell zu sinken droht und schnell immer leistungsfähigere Hardware erforderlich wird, um aus dem Mining Profit zu erzielen. Das Konzept basiert auf dem mooreschen Gesetz, das besagt, dass die Leistung von Computern sich zu gleich bleibenden Preisen regelmäßig verdoppelt[35].

Die Verfahren, bei denen der Speicherbedarf pro Rechenoperation über die Zeit automatisch erhöht wird, nennen sich Scrypt-Progressive-N Verfahren. "N" beschreibt die Größe des erforderlichen Speicherbereichs und soll regelmäßig steigen. Execoin verfolgt den gleichen Ansatz wie Vertcoin, wobei die Intervalle für die Erhöhung des Speicherbedarfes noch kürzer sind und die Entwertung von ASICs noch wirkungsvoller umgesetzt wird. Derzeit ist die Erhöhung des Speicherbedarfs pro Rechenoperation einer der wenigen wirksamen Hebel gegen die Entwicklung von ASIC Minern, da die Entwicklungskosten im Verhältnis zu der voraussichtlichen Nutzungsdauer zu hoch sind.

X11, X12, X13, X14, X15, X17

Neben den genannten, eher weit verbreiteten Ansätzen gibt es auch viele weitere PoW Methoden, um einen gesuchten Hashwert zu bilden. X11 kam erstmals bei Darkcoin zum Einsatz und beschreibt einen kombinierten Hash aus vielen verschiedenen Hashmethoden. Die Zahl nach dem X beschreibt die Anzahl der verwendeten Hashmethoden. Die Idee dieses Verfahrens beruht auf der Annahme, dass ein Verfahren wie z.B. SHA256 kompromittiert werden könnte. Sollte das passieren könnte jeder zielgerichtet einen Hash erzeugen, der den aktuellen Schwellwert unterschreitet und das Verfahren wäre als Beweis für eine Leistung nutzlos. Ein Hard Fork müsste stattfinden, das Vertrauen in die Währung würde drastisch abnehmen. Falls eine oder mehrere der Hashmethoden von X11 bzw. noch zahlreicher verketteten Techniken "geknackt" würden, könnten die übrigen Methoden in der Kette weiterhin Sicherheit gewährleisten.

[34] Kirk, David (2014), Tech-Recipes

[35] Anonym (2013), Encyclopedia Britannica

Während mit Software-Implementierungen und mit Hilfe von GPUs effizient X11 und andere gemischte Hashes berechnet werden können, gibt es derzeit noch keine ASICs für diese Form von Hashes, auch wenn deren Entwicklung theoretisch möglich wäre. Durch den hohen Implementierungsaufwand und die vergleichsweise geringe Marktkapitalisierung der Währungen, die diese Technik verwenden, ist die Entwicklung derzeit unwirtschaftlich.

Weitere PoW Mechanismen

Es gibt noch weitere Methoden um den Proof of Work zu erbringen, wie das recht junge bei Talkcoin zum Einsatz kommende NIST (SHA-3) oder die Berechnung von Cunningham-Ketten aus Primzahlen bei Primecoin zeigen. Letzteres ist das erste Geldsystem, das wissenschaftlich nutzbare Ergebnisse erzeugt, während gleichzeitig die Blockchain gesichert wird. Das Verfahren der Primzahlberechnung ist nicht besonders gut auf GPUs übertragbar, sodass ihr Vorteil gegenüber dem CPU Mining nicht hoch ist[36].

3.2.2 Proof of Stake

Der zweite populäre Mechanismus eine Leistung zu beweisen, um Coins initial zu erschaffen, ist der Proof of Stake Mechanismus. Stake bedeutet übersetzt Anteil und tatsächlich ist ein Anteil an der jeweiligen Währung Voraussetzung für das Verarbeiten eines Blockes mit seinen Transaktionen und dem Gewinn neuer Coins. Weil sich dieses Verfahren von dem rechenintensiven Mining stark unterscheidet, wird diese Form der Coinerzeugung auch Minting genannt.

Da das PoS Verfahren nicht auf der aufwändigen Berechnung künstlicher Hashwerte beruht ist es weniger auf leistungsstarke Hardware und damit hohe Stromverbräuche angewiesen. Stattdessen gilt z.B. bei der PoS Umsetzung von Peercoin, wer mindestens einen Peercoin (PPC) besitzt und diesen mindestens 30 Tage lang nicht in Transaktionen verwendet, also nicht bewegt hat, kann an dem Verfahren teilnehmen. Für die Teilnahme ist es weiterhin erforderlich die Wallet-Software geöffnet zu haben und mit dem Netzwerk verbunden zu sein.

Wenn die genannten Voraussetzungen erfüllt sind, wird der gleiche Mechanismus wie bei Bitcoin angewendet. Ein Hash des Blockheaders wird gebildet und der resultierende Hash muss einen Schwellwert unterschreiten, um akzeptiert zu werden. Der Unterschied hierbei

[36] King, Sunny (2014), primecoin.io

ist allerdings, dass nur das Alter des entsprechenden Inputs eine Rolle spielt, um Hashes zu bilden. Bei dem PoW Verfahren wird hier ein Nonce schrittweise erhöht, um so viele Hashes wie möglich zu erzeugen. Bei PoS kann hingegen nur ein Hash je Input je Sekunde gebildet werden. Die Höhe des Schwellwertes ist dabei abhängig von dem Alter des Inputs, sodass mit steigendem Input-Alter die Wahrscheinlichkeit zur Lösung zusätzlich steigt. Das Verfahren schont die Rechenleistung enorm, sodass sogar mobile Umsetzungen einer Software denkbar wären. Wenn ein Teilnehmer einen validen Hash findet und einen Block erstellen darf, übermittelt er die gesamte Höhe des Inputs, der zu dem Fund des Hashes beigetragen hat, zusätzlich einer Belohnung an sich selbst.

Jährlich wird 1% der verfügbaren Menge Coins in Form von Belohnungen durch PoS ausgelost. Dabei richtet sich die Höhe der Belohnung nach der Menge der Coins/Inputs, die man besitzt. Besitzt man 5% aller Coins und löst den Hash zu einem Block nach einem halben Jahr erhält man seine anteiligen 50% an den 5%, die man besitzt.

Während Peercoin einen gemischten Ansatz aus PoW für die initiale Verteilung von Coinbeträgen und PoS für die Aufrechterhaltung des Netzwerks bei geringem Ressourcenverbrauch verfolgt, gibt es mit Nextcoin (NXT) auch einen vollständig auf dem PoS Verfahren basierenden Coin mit hoher Marktkapitalisierung (Tab. 3.1). Neue Coins können nur gekauft, nicht erzeugt werden, Transaktionen untereinander werden durch PoS in Blöcke zusammengefasst und bestätigt.

Es ist schwer schätzbar wie viel Watt Strom je Gigahertz Hashleistung für die Berechnung PoW-basierter Währungen verwendet wird, aber Schätzungen gehen von dem Verbrauch einer kleineren Stadt aus. Es gibt immer wieder kritische Diskussionen über die Energieverschwendung durch Bitcoin und andere PoW basierte Währungen. PoS ist deutlich sparsamer und es gibt keine sinnvollen Möglichkeiten Mining Pools zu bilden, wodurch die Dezentralität des Netzwerks geschützt ist. Zudem wird der Anreiz zum Betreiben eines "Full Nodes" erhöht, da es Voraussetzung zum Minting ist.

3.2.3 Proof of Burn

Als dritten nennenswerten Mechanismus für den Nachweis einer Arbeit kann das Proof of Burn (PoB) Verfahren genannt werden. Im Falle von "Counterparty" gibt es einen Coin, der auf dem Bitcoin Protokoll und seiner Blockchain aufsetzt. Um Coins in der Counterparty Währung XCP zu erstellen, müssen Bitcoins an die öffentliche Adresse mit dem Prefix "1Counterparty-XXXXXXXXXXXXXXX" gefolgt von einem Prüfcode gesendet werden. Diese Überweisungen gelten, da der private Schlüssel zu diesen Adressen so gut wie nicht wiederherstellbar ist, als

"verbrannt". Damit ist der Beweis eine Leistung erbracht zu haben abgeschlossen[37].

Im Prinzip ist der Mechanismus vergleichbar mit dem Verbrennen eines Kraftstoffes für die Erzeugung von Strom, der zur Generierung von Bitcoins gebraucht wird. Damit und weil Counterparty auf dem Bitcoin Netzwerk aufsetzt, muss zu einem früheren Zeitpunkt zur Erzeugung der zu verbrennenden Bitcoins ebenfalls das PoW Verfahren zum Einsatz gekommen sein. Das Verfahren wird stark kritisiert, da das Unverständnis über die Vernichtung groß ist. Stattdessen wünschen sich Nutzer eine Möglichkeit die Bitcoins weiterhin in Umlauf behalten bzw. spenden zu können, was allerdings schlussendlich dazu führen würde, dass Bitcoins unendlich viele Male gegen Counterparty Coins getauscht werden können. Dadurch würde die Währung eine inflationäre Entwicklung durchlaufen.

Obwohl Proof of Burn kontrovers diskutiert wird, erfüllt es die konzeptionellen Anforderungen an ein Beweisverfahren. Bei allen Verfahren muss es eine Aufgabe geben, die alle Teilnehmer als schwierig empfinden und deren Lösung für alle Teilnehmer als leicht überprüfbar gilt. Bei Proof of Burn entstehen vergleichbar mit der Anschaffung eines ASIC Miners zwar ebenfalls Kosten, diese implizieren allerdings nicht unmittelbar eine Verschwendung von Rohstoffen.

3.3 Sicherheit

Bei allen dezentralen, elektronischen Währungen handelt es sich um unregulierte Systeme ohne zentrales Organ für Beschwerden, Hilfe bei Anwenderproblemen und ohne einen verantwortlichen Ansprechpartner im Falle eines Sicherheitslecks. Verwaltet man große Mengen an Coins, so muss auch das Risiko bedacht werden, das mit ihrem Besitz einhergeht. Die verschiedenen Währungen haben aufgrund ihrer Mechanismen zur Erzeugung und Verbreitung von Währungseinheiten jeweils potenzielle Angriffspunkte, die das Netzwerk und deren Teilnehmer mehr oder weniger gefährden können.

3.3.1 Wallet

Die Wallet als zentrale Speicherstelle für die privaten Schlüssel zum Signieren von Transaktionen ist eine der schützenswertesten Elemente der Coin-Netzwerke.

Da die meisten Wallet-Programme Adaptionen der Bitcoin Wallet sind, profitieren sie von der

[37] Anonym (2014), Counterparty.co

Möglichkeit die Wallet-Datei zu verschlüsseln. Dafür wird in der ersten Runde AES-256-CBC verwendet, um die Wallet mit einem zufälligen Masterpasswort zu verschlüsseln. In der zweiten Runde wird das verschlüsselte Masterpasswort mit AES-256-CBC verschlüsselt. Hierfür wird ein Schlüssel aus dem Nutzerpasswort mithilfe eines SHA512 Hashs und der BytesToKey Funktion der kryptografischen Funktionen von OpenSSL erstellt[38].

In der Vergangenheit ist es vorgekommen, dass durch gezielte Angriffen auf Computer die Wallet Dateien ihrer Nutzer kopiert wurden. Gegen diese Form eines Angriffs können sich Nutzer durch die Vergabe eines sicheren Passworts schützen. Sobald ein Benutzer allerdings eine Überweisung auslöst, muss das Passwort zur Entschlüsselung eingegeben werden. Hat der Angreifer die Kontrolle über den Computer seines Opfers, könnte er nun das Passwort mitlesen, die öffentlichen und privaten Schlüssel für die Inputs des Opfers erbeuten und sie ausgeben. Wie bereits erklärt gibt es in diesem Fall keine Möglichkeit die gestohlenen Inputs zurück zu erlangen, da die Teilnehmer des Netzwerkes nach Angabe einer validen Signatur die Korrektheit der Transaktionen bestätigen und nach Aufnehmen in die Blockchain selbige irreversibel machen.

Die Walletverschlüsselung funktioniert grundsätzlich bei allen Coin-Systemen und ist lediglich von der Client-Software abhängig. Es gibt jedoch konzeptionell eine Besonderheit bei der Verwendung des Proof of Stake Mechanismus zum Minten. Da der Nachweis des Besitzes an einem Input für das Minten zwingend erforderlich ist, muss der Zugriff auf den privaten Schlüssel gegeben, die Wallet also für diese Funktionalität unverschlüsselt sein.

Diese entsperrte Wallet wird “Hot Wallet“ genannt, da sie ungesichert an dem Netzwerk hängt und ein relativ leichter Zugriff auf die Schlüsselpaare für die eigenen Inputs möglich ist. Auch Wallets bei Onlinediensten oder Guthaben bei Wechseldiensten zählen zu den Hot Wallets, da man auch dort in der Regel keine Kontrolle über seine Schlüssel hat. Im Gegenzug dazu nennt man den Ablageort offline gespeicherter Schlüsselpaare “Cold Storage“. Zu den Varianten von “Cold Storage“ gehören auch andere Methoden, wie die Lagerung auf USB Sticks, Papier Wallets, Münzen (auf denen ein privater Schlüssel vermerkt ist) oder Hardware Wallets.

Es gibt eine erweiterte Sicherheitsform von “Cold Storage“, die sich “Deep Cold Storage“ nennt. Bei dieser Form werden die Schlüsselpaare für Inputs verschlüsselt auf mehreren USB Sticks z.B. in Bankschließfächern gelagert. Dieses Verfahren wird für besonders hohe Vermögenssummen genutzt. Der öffentliche Schlüssel wird vom Eigentümer vorgehalten, wodurch er einfach an diese Adresse Geld senden kann. Der physische Zugriff ist allerdings mit einem gewissen Aufwand verbunden.

[38] Anonym (2014), Bitcoin Wiki

3.3.2 Strukturelle Mehrheits-Attacken

Da alle dezentralen Währungen ohne das Vertrauen in seine einzelnen Teilnehmer funktionieren müssen, ist es wichtig, dass alle unabhängigen Teilnehmer einen gemeinsamen Konsens haben. Ein Konsens z.B. über den letzten Block der Blockchain wird gefunden, indem alle Teilnehmer immer die längste Kette akzeptieren. Je nach verwendeter Methode des Arbeitsbeweises sind Angriffe möglich, indem eine künstliche Mehrheit geschaffen wird, die einen anderen Konsens hat, als der ehrliche Rest des Netzwerkes. Diese Angriffsform wird daher 51% Attacke genannt, auch wenn es durchaus möglich ist, mit einem deutlich geringeren Anteil Angriffe an einem Netzwerk durchzuführen[39].

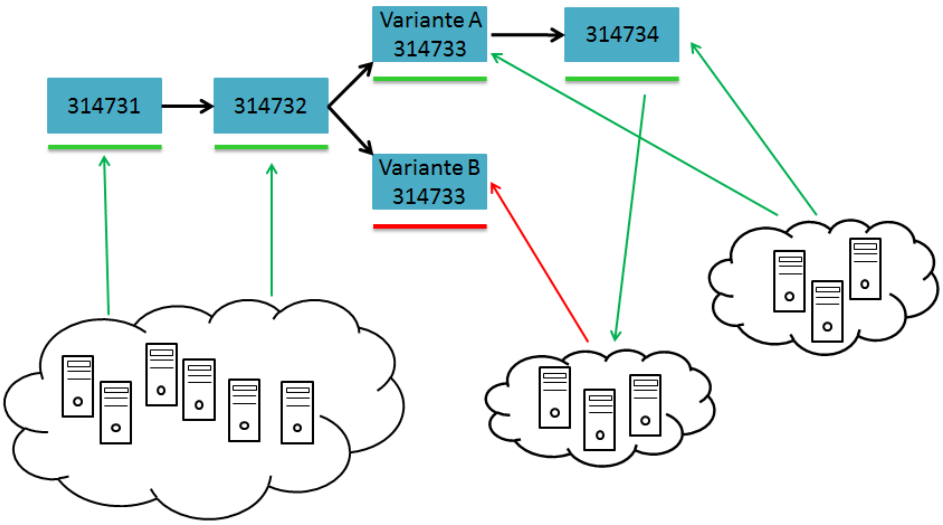

Abbildung 3.4: Blockchain mit zwei Zweigen. Längste Kette gewinnt immer. (eigene Abb.

Tritt der Fall ein, dass zufällig zwei Miner zeitgleich einen Block lösen, wird ein Teil der Teilnehmer und insbesondere Miner, die zuerst von der Blockvariante A wissen, diesen für den korrekten halten und der andere Teil Variante B (Abb 3.1). Es entscheidet sich mit der Gruppe, die schneller den nächsten Block löst, welche Kette fortgeführt wird. Es wird bei Lösung jeweils die Variante fortgesetzt, die die schnellere Gruppe zuerst kannte. Alle anderen Teilnehmer werden diese ebenfalls als die längste Kette akzeptieren. In der Folge wird Variante B des Blocks verwaisen und alle weiteren Berechnungen werden auf Variante A und seinem Folgeblock aufbauen.

In dem skizzierten Fall veröffentlichen beide Miner ihre zeitgleich gefundene Version des Blockes für alle anderen Miner. Bei einem Angriff bzw. würden böswillige Miner sogenanntes

[39] Berkman, Fran (2014), The Daily Dot

"Selfish Mining" praktizieren, dann würden sie ihren Fund zurückhalten und ohne Wissen der anderen Miner anfangen den nächsten Block zu errechnen. Eine 51% Attacke besagt, dass ein Miner oder ein Mining Pool knapp über die Hälfte der Rechenleistung kontrolliert und damit neue Blöcke statistisch immer ein wenig schneller als der Rest lösen kann.

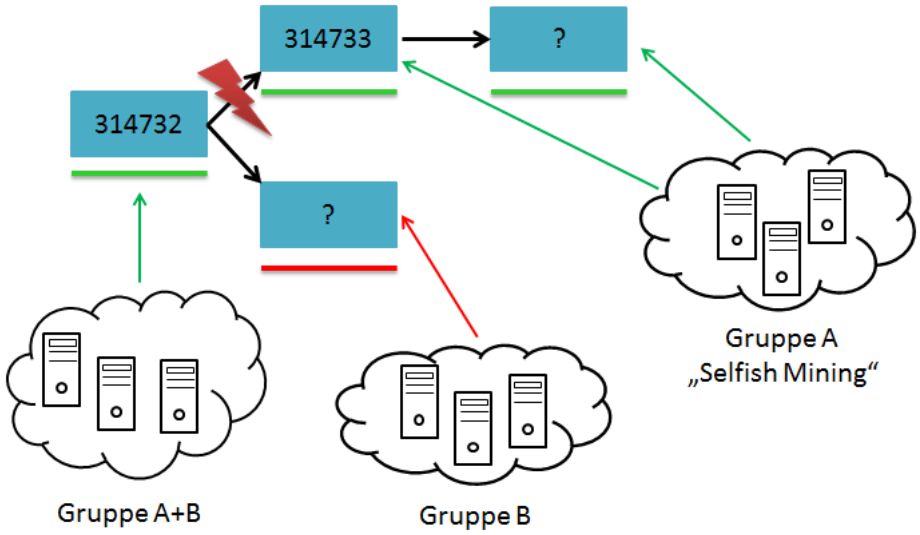

Abbildung 3.5: "Selfish Mining", mit Zeitvorteil gegenüber anderen Minern (Eigene Darstellung)

Durch das Zurückhalten von Blöcken verschaffen sie sich zunächst einen Zeitvorteil wie in Abb. 3.5 ersichtlich. Ab dem Moment, in dem Gruppe A einen Block geheim fertiggestellt hat, kann sie exklusiv an dem nächsten Block rechnen. Löst B nun vor A den nächsten Block, dann ist B wieder gleichauf mit A. Wenn A nun den nächsten Block vor B findet und zusammen mit dem ersten Block (Block 314733 in Abb 3.5) publiziert, hat A die durch B errechnete Version 314733 invalide gemacht, weil A's Version der Kette nachweislich länger ist. Der Block von B wird in der Folge verwaisen.

Durch diese Strategie kann der Angreifer mehrere potenzielle Ziele verfolgen. Er kann sich einerseits einen zeitlichen Vorteil in der Lösung eines neuen Blocks verschaffen. Im Bitcoin Netzwerk ist 1 BTC derzeit ca. €450 wert, was bei einer Belohnung (Block Reward) von 25 BTC €11250 pro gelöstem Block entspricht. Neue Blöcke werden durchschnittlich alle 10 Minuten gelöst, wodurch sich die Einnahmen bei längerer Laufzeit also deutlich aufsummieren und eventuell sogar eine Investition in sehr teure Hardware rechtfertigen können.

Des Weiteren kann der Angreifer allerdings auch entscheiden, welche Transaktionen in die Blöcke für die Blockchain gelangen. Ein Angreifer könnte also nur seine eigenen, nur bestimmte oder gar keine Transaktionen in den erzeugten Blöcken inkludieren und damit das Netzwerk für

eine bestimmte Zeit blockieren. Bezahlungen in Shops oder Zahlungen an andere Teilnehmer könnten zurückgehalten werden.

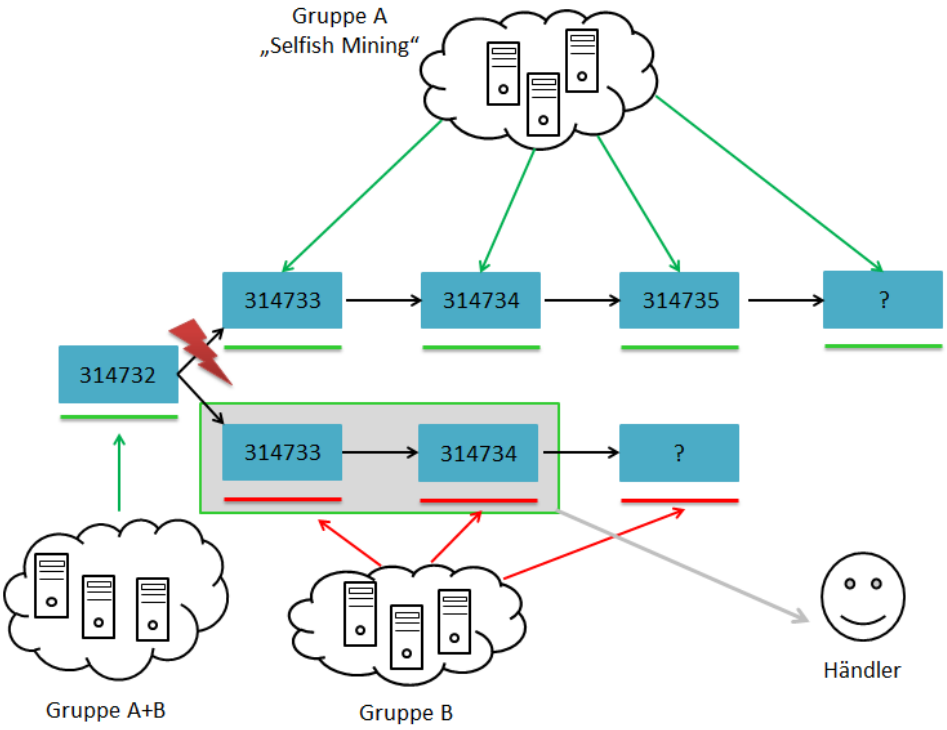

Abbildung 3.6: Double Spend Attacke. Transaktionen an Dritte zurücknehmen.

Ein Angreifer könnte eine Zahlung an einen Dienstleister oder Versandhandel über das reguläre öffentliche Netzwerk auslösen, wenn er weiß, dass er einen entsprechenden Vorsprung bei der Berechnung von Blöcken hat (siehe Gruppe A in Abb. 3.6). Wie in Abb. 3.6 angenommen, benötigt ein Händler, nachdem die an ihn gerichtete Transaktion in Block 314733 aufgenommen wurde, nur einen weiteren darauffolgenden Block, der diese Bestätigung absichert. Wenn der Block 314734 veröffentlicht wird und der Händler die Zahlung für hinreichend gesichert betrachtet, kann der Angreifer die gesamte Blockchain bis Block 314735 veröffentlichen und alle Teilnehmer werden auf diese Kette umsteigen, da immer die längste Kette akzeptiert wird. Der Angreifer kann in seine Version der Blockchain nun eine Transaktion an sich selbst inkludieren. In dieser muss er nur die Inputs, die er normalerweise an den Händler geschickt hätte, an sich selbst senden. Andere Teilnehmer halten diese Transaktion für die schnellere und verwerfen die zweite Transaktion an den Händler. Auch die Belohnung für die Miner, die an der ehrlichen, öffentlichen Variante der Blockchain gearbeitet haben, fällt nun an den Angreifer.

Aus dieser Vorgehensweise ergibt sich eine weitere mögliche Handlung eines Angreifers. Er könnte eine Parallelkette berechnen und wenn er sie - von allen anderen Teilnehmern unerwartet

- veröffentlicht, in den Blöcken keine einzige Transaktion aufnehmen. Da alle Teilnehmer die längste Kette akzeptieren fallen die Transaktionen aus dem bisher öffentlich bekannten Block in einen Pool aus unbestätigten Transaktionen zurück und gelten plötzlich als potenziell unsicher, da sie keine einzige Bestätigung mehr haben. Der Angreifer hat davon unmittelbar nichts, da er in keinem Fall Transaktionen im Namen Fremder auslösen kann. Dennoch kann er damit Transaktionen mit einem sehr großen Gesamthandelsvolumen auf eine Risikostufe zurücksetzen. Womöglich werden einige Transaktionen sogar verworfen bevor sie ihren Weg in den nächsten Block eines ehrlichen Miners finden. Händler haben eventuell schon Waren versandt und müssen nun plötzlich wieder um die Bezahlung fürchten. In dem Zustand könnte jeder Teilnehmer eine neue Transaktion an sich selbst mit höherer Transaktionsgebühr auslösen. Es ist dann sehr wahrscheinlich, dass der ehrliche Miner des nächsten Blockes die Transaktion mit der höheren Gebühr aufnimmt und die ursprüngliche Transaktion an den Händler verwirft.

Wenn man das Angriffsszenario etwas weiterführt, werden sich bei längeren, durch nur einen Miner gebildeten Ketten, andere Miner die Kosten für die Hardware und den Stromverbrauch nicht leisten können und aussteigen. Auch der Angreifer kann dadurch seine Ressourcen reduzieren und trotzdem weiterhin die Macht über das Netzwerk behalten. Das Vertrauen in die Währung würde rapide sinken und die erwirtschafteten Coins hätten für den Angreifer keinen hohen Gegenwert mehr. Ein Angriff muss nicht zwangsweise monetäre Ziele haben. Ein Gegner der Währung könnte sie durch eine relativ überschaubare Investition schädigen.

Das Szenario wurde hier für den Prozess des Minens nach dem Proof of Work Verfahren skizziert. Allerdings ist das Szenario auch bei Proof of Stake umsetzbar. Die Kosten sind allerdings je nach Marktkapitalisierung ungleich höher, da erst der Besitz von Coins das Minen ermöglicht und 51% der Menge aller Coins erforderlich sind, um über einen längeren Zeitraum eine alternative Variante der Blockchain zu berechnen und damit das Netzwerk anzugreifen.

3.4 Transaktionsgeschwindigkeit

Eine häufig an Bitcoin kritisierte Eigenschaft ist die durchschnittliche Zeit je berechnetem Block, die bei 10 Minuten liegt. Das heißt, dass alle 10 Minuten ein Block an die Blockchain angehangen wird und damit Transaktionen validiert werden. Unter Berücksichtigung der Angriffsmöglichkeiten aus Abschnitt 3.3.2 und der auffällig hohen Konzentration von Rechenkraft (Abb. 3.2) sollte ein Händler von mittel- bis hochpreisigen Waren einige Blöcke abwarten, um Gewissheit über die erfolgreiche Zahlung zu haben. Da die lange Wartezeit in vielen Situation unpraktisch ist, haben die meisten alternativen kürzere durchschnittliche Blockbildungszeiten.

Währung	Bitcoin	Peercoin	Namecoin	Litecoin	Darkcoin	Vertcoin
Blockbildungszeit	10 Min.	10 Min.	10 Min.	2.5 Min.	2.5 Min.	1.5 Min.
Währung	Dogecoin	Nxt	FeatherCoin	BlackCoin	BitSharesX	Hashcoin
Blockbildungszeit	1 Min.	1 Min.	1 Min.	1 Min.	25 Sek.	10 Sek.

Tabelle 3.4: Blockbildungszeiten einiger Währungen

Die Blockbildungszeiten haben verschiedene Auswirkungen auf die Sicherheit einer Währung und sollten daher vorsichtig gewählt werden. Wenn sie wie bei HashCoin sehr kurz gewählt wird kommt es schnell zu unbeabsichtigtem "Selfish Mining", da der Löser eines Blockes weiterarbeitet, bevor eine größere Menge Teilnehmer davon in Kenntnis gesetzt wurde. Auch andere Miner können eine parallele Kette entwickeln und unter Umständen erst nach 2 bis 3 neuen Blöcken von der jeweils anderen Kette erfahren. Die Folge sind viele verwaiste Blöcke und erhebliche Sicherheitseinbußen. Ein Händler kann schwer einschätzen, ab welchem Zeitpunkt er eine Transaktion akzeptiert, obwohl die Blockbildungszeit gering ist.

Ein weiterer Nebeneffekt ist die Erhöhung der Blockchain-Größe. Ein Block selbst hat zwar einen relativ geringen "Overhead", doch summiert sich die Größe bei einer sehr geringen Blockbildungszeit unnötig schnell. In Kombination mit den Sicherheitsmängeln gibt es keinen nachvollziehbaren Grund für eine sehr kurze Blockbildungszeit. Des Weiteren wird eine Transaktion auch ohne Aufnahme in einen Block beim Empfänger bekannt, gilt jedoch als unsicher. Die Aufnahme in eine Blockchain, in der mit hoher Wahrscheinlichkeit häufig verwaiste Blöcke erzeugt werden, ist auch unter diesem Aspekt nicht praktikabel. Nicht zuletzt bedeuten viele verwaiste Blöcke auch, dass viele Ressourcen mehrfach aufgewendet werden und damit ineffizient gearbeitet wird[40].

3.5 Ökonomische Aspekte

Neben all den technischen Aspekten dezentraler, elektronischer Währungen gibt es den nur bedingt direkt beeinflussbaren Aspekt der Währungsentwicklung. Hierzu zählen die Einordnung der Währungen in den Geldbegriff, aber vor allem auch die über eine Zukunft entscheidende Akzeptanz.

[40] Demian Lerner, Sergio (2014), Bitslog

3.5.1 Einordnung von Coin-Systemen in den Geldbegriff

Bevor das Verhalten von dezentralen Währungen wie Bitcoin untersucht werden kann, ist vorab der Begriff des Geldes in Zusammenhang mit Coin-Währungen zu klären. Nach Mankiw[41] muss Geld 3 Funktionen erfüllen.

1. Es muss ein Tausch- bzw. Zahlungsmittel sein
2. Es muss als Wertanlage fungieren können
3. Es muss eine Einheit sein, in der Menschen rechnen

Die erste Anforderung erfüllen Coin-Währungen zweifellos, da sowohl Internetshops, als auch reguläre Geschäfte wie z.B viele Cafés Bitcoin und/oder andere Währungen akzeptieren. Der zweite Punkt ist etwas weniger leicht zu bestätigen. Die aktuelle Entwicklung der meisten dezentralen Währungen ist mit einer sehr hohen Instabilität verbunden. Nicht selten schwanken Kurse um 10-40% innerhalb weniger Tage nach oben oder unten je nach Marktkapitalisierung der Währung.

Abbildung 3.7: Handelskurs von Bitcoin in Euro (ariva.de)

Da der Bitcoin Kurs sich im Vergleich zu anderen Währungen zeitweise relativ stabil verhält könnte man großzügig argumentieren, dass in einem gewissen Zeitraum die Bedingung erfüllt ist.

[41] Mankiw, N. Gregory (2007), Macroeconomics

Der dritte Punkt jedoch könnte die Einordnung von Coinsystemen als Geld nach Mankiw's Definition verhindern. Die Währung Bitcoin wird von keiner Personengruppe als primäre Recheneinheit verwendet, wie es bei etablierten Hartgeld-Währungen der Fall ist. Stattdessen werden Währungen wie Bitcoin derzeit von der Majorität als spekulative Objekte genutzt, aus deren Kurs sich unter Umständen Profit schlagen lässt. Der Aufwand, der in das Minen neuer Coins investiert wird und die hohe Verbreitung von Handelsbörsen bestätigen diese Vermutung. Sicherlich ist nicht zuletzt der stark schwankende Kurs mitverantwortlich für den Ruf dieser Währungen.

Die Mehrheit der Bitcoin-Nutzer vertraut der Währung nicht wie der offiziellen jeweiligen Landeswährung und betrachtet die Investition eher als Anlageform. Das Kriterium könnte sich mit der Zeit allerdings selbstständig erfüllen. Sobald eine Vielzahl an Personen bereit ist, etwas für einen virtuellen Gegenwert zu erschaffen und eine virtuelle Währung für eine Ware auszugeben, ist die dritte Bedingung ebenfalls erfüllt.

Es ist nicht vorhersehbar wann ein Großteil der Menschen einen digitalen Wert als ähnlich wertvoll wie einen Geldschein empfindt.

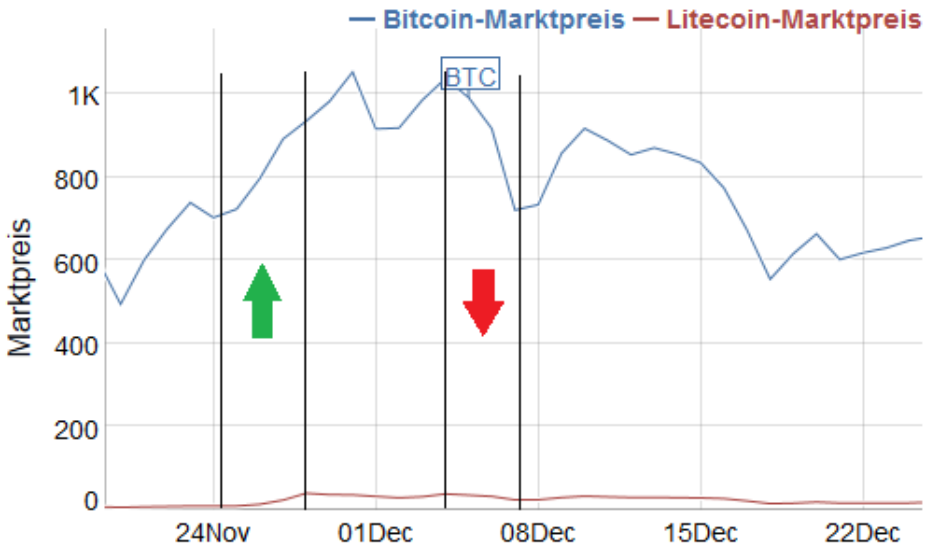

Abbildung 3.8: Marktpreis von Bitcoin und Litecoin in USD (bitinfocharts.com)

Betrachtet man die Marktkapitalisierung anderer Währungen, dann dürfte ihr Weg zu einem echten Geldverständnis sogar weitaus länger sein. Des Weiteren verhält sich Bitcoin als eine Art Referenz-Währung stellvertretend für die Art der dezentralen Währungen. Fällt das Vertrauen in die Art Währungen, dann fällt es für alle Währungen zur gleichen Zeit wie man anschaulich in einem Vergleich der beiden größten Währungen Bitcoin und Litecoin erkennen kann (Abb. 3.8). Ob der Auslöser des Vertrauensverlusts nur ein Problem einer bestimmten Währung

oder ein allgemeines Problem darstellt, spielt keine Rolle für die letztendlichen Auswirkungen auf alle Währungen. Aufgrund der hohen Komplexität des Themas sind medienwirksame, negative Schlagzeilen eine regelmäßige Gefahr für die Stabilität. Die Möglichkeit einzelne, technische Details zu überprüfen ist gering.

3.5.2 Inflationäres/Deflationäres Verhalten

Die Kurssprünge dezentraler Währungen, insbesondere von Bitcoin, haben schon oft für Aufsehen gesorgt. Bitcoins sind auf 21 Mio Stück begrenzt, wobei der letzte Block im Jahr 2140 erzeugt werden wird. Anschließend werden weiterhin Blöcke erzeugt, allerdings sollen diese ausschließlich durch Gebühren für Transaktionen bezahlt werden.

Betrachtet man die Entwicklung von Coin-Währungen, stellt sich die Frage nach ihrem tatsächlichen Wert und ob die derzeitige Entwicklung nicht eher bedenklich instabil verläuft. Immer, wenn die Nachfrage nach Bitcoins zunimmt, werden trotzdem nicht mehr Coins erzeugt und der Preis steigt in der Folge.

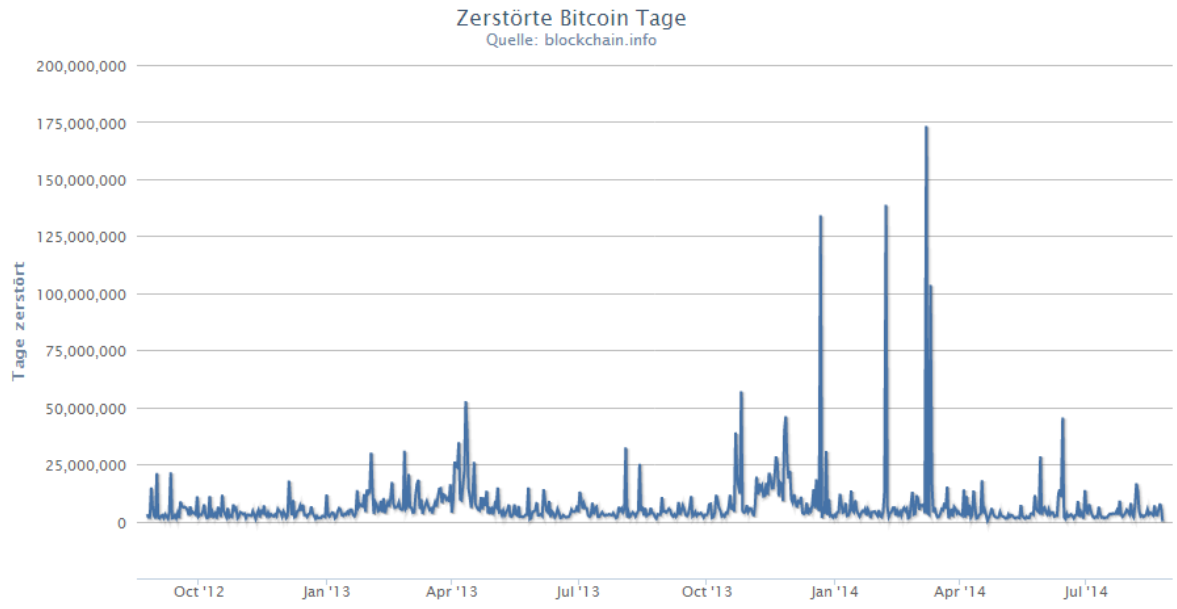

Abbildung 3.9: Umlaufgeschwindigkeit der letzten 2 Jahre visualisiert durch vernichtete Tage je Zeit (blockchain.info)

Nach Engelkamp und Sell "gibt die Umlaufgeschwindigkeit an, wie oft jede Geldeinheit im

Durchschnitt der betrachteten Periode die Kasse gewechselt hat“[42]. Unabhängig davon, ob Bitcoin als Geld anerkannt werden kann, wird in Abb. 3.9 ersichtlich, dass die Umlaufgeschwindigkeit von Bitcoin über zwei Jahre im Schnitt nicht gestiegen ist. Die Ausschläge in der Grafik zeigen, dass vor allem dann Handel stattfindet, wenn der Wert der Währung steigt. Das Grundniveau allerdings bleibt gleich. Eine echte Wertsteigerung kann allerdings nur erfolgen, wenn eine Währung tatsächlich mehr gehandelt wird. Die genannte Entwicklung bestätigt indes einen spekulativen Umgang mit Bitcoin.

Abbildung 3.10: Handelspreis der letzten 2 Jahre in USD (blockchain.info)

Vergleicht man die Umlaufgeschwindigkeit mit der Entwicklung des Marktpreises der letzten zwei Jahre, so kann man feststellen, dass der Marktwert von Bitcoins steigt. Jedoch steigt die Umlaufgeschwindigkeit nicht proportional an. Da sich die Umlaufgeschwindigkeit einer Währung ähnlich deren Wert entwickeln sollte, kann man hier von einer künstlichen Blase ausgehen, die durch Investitionen und den deflationären Charakter von Bitcoin verursacht wird[43].

Grundsätzlich dürfte dieser Effekt bei allen elektronischen, dezentralen Währungen verbreitet sein. Dennoch gibt es grundlegende Unterschiede in der Anzahl an Coins der jeweiligen Währungen und der damit verbundenen geplanten Inflationsrate. So hat eine Währung mit einer unbegrenzten Geldmenge grundsätzlich eine gewisse inflationäre Entwicklung in Höhe der neu erzeugten Coins im Vergleich zu den vorhandenen Coins.

[42] Engelkamp, Paul; L. Sell, Friedrich (2005), Einführung in die Volkswirtschaftslehre

[43] P. Schmidt, Artur (2013), Heise Telepolis

Währung	Bitcoin	Peercoin	Namecoin	Litecoin	Darkcoin	Vertcoin
Anzahl Coins	21 Mio.	Unbegrenzt	21 Mio.	84 Mio.	22 Mio.	84 Mio.
Währung	Dogecoin	Nxt	FeatherCoin	BlackCoin	Primecoin	Freicoin
Anzahl Coins	Unbegrenzt	1 Mrd.	336 Mio.	100 Mio.	Unbegrenzt.	100 Mio.

Tabelle 3.5: Maximalanzahl Coins von verschiedenen Währungen

Die ursprünglich als Parodie auf Bitcoin gedachte Währung Dogecoin hat erst ein Limit bei 100 Mrd. Coins gehabt, was im Februar 2014 gänzlich aufgehoben wurde (Tab. 3.5). Ende 2014 werden voraussichtlich die 98 Mrd. Coins vergeben worden sein und ab 2015 wird es jährlich eine fixe Anzahl von 5,2 Mrd. neuer Coins geben. Sollte diese Anzahl stabil bleiben entspräche das einer Inflationsrate von 5,3% in 2015, 5,04% in 2016 usw. Der Reiz diese Währung vorzuhalten sollte entsprechend geringer sein, da der Wertverlust die Währung als Anlage unattraktiv macht. Die Auswirkungen kann man bisher kaum messen, da weder Handelswert noch Umlaufgeschwindigkeit zugenommen haben.

Einen interessanten Effekt ruft die Währung Primecoin hervor. Die Höhe der Belohnung bei Fund einer korrekten Cunningham-Kette entspricht 999/Schwierigkeitsgrad^2. Wenn die Nachfrage steigt und der Schwierigkeitsgrad durch die steigende Rechenleistung erhöht wird, reduziert sich die Anzahl ausgeschütteter Primecoins. Es wird dabei jedoch die gleiche Anzahl an Blöcken pro Tag verarbeitet. Wenn die Nachfrage sinkt steigt die Belohnung hingegen wieder an. Durch die hohe Menge an Primecoins und die sehr wechselhafte Nachfrage ist dieses Geldsystem zu einem beliebten Handelsobjekt geworden, konnte bisher aber noch keine Stabilität erreichen.

Freicoin verfolgt unter den Währungen einen radikaleren Ansatz, um die Umlaufgeschwindigkeit der Währung zu beschleunigen. Die Währung entstand aus der Protestbewegung “Occupy“ und setzt sich als Ziel, hauptsächlich die Interessen von 99% der “normalen“ Bevölkerung zu vertreten und den Erhalt des Reichtums der übrigen 1% nicht direkt zu fördern. Das Modell dieser Idee wird bereits länger diskutiert und nennt sich "demurrage currency". Der Begriff beschreibt eine Währung, die eine Liegegebühr auf Geld vorsieht. Man könnte diese Gebühr also auch als Umlaufsicherungsgebühr bezeichnen, da es nicht belohnt wird Geld in großen Mengen anzuhäufen. Die Höhe des Liegegeldes liegt bei 4,4% im Jahr, es werden also 4,4% des gesamten Guthabens aller Teilnehmer jährlich eingezogen[44]. Die Inflationsrate Deutschlands lag im Jahr 2013 bei 1,5%[45]. Der wesentliche Unterschied in der Umsetzung von Freicoin ist, dass das so eingezogene Geld umverteilt und wieder den Minern zugeschrieben

[44] Anonym (2012), Bitcointalk

[45] Anonym (2014), Statistisches Bundesamt

wird.

Durch diese Umverteilung sollen vor allem Investitionen gefördert und das Anhäufen von Geld nicht belohnt werden. Wie Tab. 3.5 zu entnehmen ist, liegt das Limit an gesamten Freicoins bei 100 Mio.

3.6 Nutzen

Die etablierten Coin-Währungen bauen, wie in 3.2 beschrieben, auf der Berechnung von möglichst vielen Hashes je Sekunde auf. Es ist schwer tatsächlich sinnvolle Berechnungen zu wählen, da die Schwierigkeit der Berechnungen je nach Rechenleistung des Netzwerkes angepasst werden muss. Dennoch gibt es einige Ansätze, die mit der Rechenleistung einen sinnvollen Zweck erfüllen wollen.

3.6.1 Primzahlenberechnungen

Primecoin z.B. nutzt die Rechenleistung der Teilnehmer für die Suche nach Primzahlen, konkret Cunningham Ketten. Die Formel $a_0 = p$ mit $a_{n+1} = 2 \cdot a_n + 1$ ergibt eine Cunningham Kette erster Art, wohingegen $a_0 = p$ mit $a_{n+1} = 2 \cdot a_n - 1$ eine Cunningham-Kette zweiter Art beschreibt. Wenn beide Arten zutreffen und sich die Mitte der Ketten jeweils verdoppeln, nennt man die Kette eine doppelte Cunningham-Kette. Ist 5 z.B. Cunningham-Kette erster Art und 7 die Cunningham-Kette zweiter Art, dann ist 6 ihr Mittelpunkt. Verdoppelt man 6 erhält man 12, was der Mittelpunkt von 11, der Cunningham-Kette erster Art und 13, der Cunningham-Kette zweiter Art ist. Damit ist 5,7,11,13 eine doppelte Cunningham-Kette der Länge 4[46].

Auch die Wiederverwendbarkeit einer Cunningham-Kette ist in Primecoin ausgeschlossen. Hierfür wird ein Quotient aus dem Block Header und der Cunningham-Kette genutzt, um ein Zertifikat, eine Art Prüfwert, zu erschaffen. Das Ergebnis des Prüfwerts wird in Kombination mit dem Block Header betrachtet.

Die Anpassung des Schwierigkeitsgrades ist den Entwicklern zufolge nicht so einfach zu bewältigen wie z.B bei dem SHA256-Verfahren. Wie in Abb. 3.9 ersichtlich, funktioniert allerdings die Anpassung der Schwierigkeit gut, sodass die Stabilität der Blockbildungszeiten

[46] King, Sunny (2014), primecoin.io

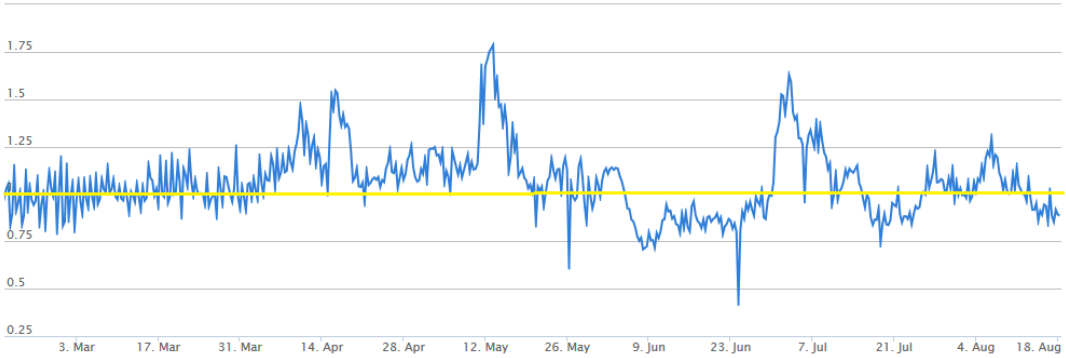

Abbildung 3.11: Mittlere Blocklösungs-Zeiten von Primecoin (xpm.muuttuja.org)

nicht gefährdet ist. Die gelbe Linie repräsentiert die angestrebten 60 Sekunden je erzeugtem Block.

Der unmittelbare Nutzen dieser Art von Primzahlen mag nicht besonders hoch sein, jedoch sind die Ergebnisse im Vergleich zu SHA256 oder Scrypt in einer bestimmten Weise überhaupt verwertbar und liefern Erkenntnisse über mathematische Zusammenhänge. Außerdem können hohe Primzahlen für Verschlüsselungsverfahren wie z.B. RSA benutzt werden, bei denen der öffentliche Schlüssel aus dem Produkt zweier besonders hoher Primzahlen erzeugt wird[47].

3.6.2 Humanitäre Einsatzzwecke

Neben der Primzahlensuche gibt es zwei Coins namens Gridcoin und Curecoin, die eine Unterstützung wissenschaftlicher Interessen vertreten.

Für Gridcoin ist die Teilnahme an dem Berkeley Open Infrastructure for Network Computing (BOINC) Netzwerk Voraussetzung. Über die BOINC-Plattform stellen freiwillige ihre ungenutzte Rechenleistung zur Verfügung und können an diversen Projekten teilnehmen. Es gibt von Voraussagen zur Klimaentwicklung über 3D-Berechnungen der Milchstraße bis zur Simulation von Proteinfaltungen zur Erforschung von Krankheiten verschiedene Möglichkeiten des Einsatzes.

Grundvoraussetzung ist die kostenfreie Mitgliedschaft in der Gridcoin Gruppe des jeweiligen Projektes. Innerhalb der Projekte werden Berechnungen durchgeführt, die an das Projekt zurückgeschickt werden. Die jeweiligen Projekte zählen einen individuellen Punktewert für die

[47] Johnston, Casey (2013), Arstechnica

durchgeführten Berechnungen und ermitteln die jüngste, durchschnittliche Punkte-Anzahl aus den Projekten. Ein Teilnehmer kann nach einer durch das Netzwerk festgelegten Zeit einen Block erzeugen, in dem er seinen öffentlichen Schlüssel, seine gehashte E-Mail Adresse und die "Cross-project identification" (CPID) von BOINC in dem Block vermerkt. In der Projektbeschreibung ist von "Proof of Boinc" die Rede. Die Coins, die der Teilnehmer in Gridcoin erhält, hängen von der Anzahl seiner Punkte aus dem Projekt ab. Die Schwierigkeit wird über die Zeit festgelegt, nach der ein Teilnehmer erneut einen Block erschaffen darf. Mit steigender Teilnehmerzahl erhöht sich demnach die Zeit bis zur nächsten Chance auf einen Block[48].

Curecoin arbeitet nach dem gleichen Prinzip, verwendet allerdings "Folding@Home" für die wissenschaftlichen Berechnungen. Dieses Projekt der Uni Standford beschäftigt sich ausschließlich mit dem Falten von Proteinen zur Suche nach Krankheitsmustern. Durch das Falten erhalten Proteine ihre dreidimensionale Struktur[49].

3.7 Anonymität

Ein lange vernachlässigter Aspekt digitaler Währungen ist die Anonymität. Zwar kann durch die eingangs beschriebenen, häufigen Wechsel der Bitcoin-Adresse bei jeder Transaktion eine gewisse Anonymität erreicht werden. Jedoch ist ein Verlauf weiterhin erkennbar und mit etwas Mühe lassen sich Zusammenhänge zwischen einem Teilnehmer und seinen Transaktionen herstellen. Vor Darkcoin existierte keine tatsächlich anonyme Währung, bei der der Absender einer Transaktion nicht identifizierbar ist.

Darkcoin führte mit seinem DarkSend genannten Verfahren eine Möglichkeit für die wirklich anonyme Übertragung von Coins zwischen den Teilnehmern ein. Das brachte der Währung neben einem guten Ruf in Hackerkreisen und unter Drogenhändlern zwischenzeitlich den dritten Platz bei der Marktkapitalisierung ein. Mittlerweile wurde das ursprünglich etwas komplizierte Verfahren durch eine Weiterentwicklung abgelöst.

Die Anonymisierung funktioniert vollkommen automatisch. In Abb. 3.12 hält ein Sender A 26 Darkcoins vor, die zuvor in bestimmte, runde Beträge gruppiert wurden. Bei Erhalt der 26 Darkcoins hat der Client von Sender A (rot in der Grafik) diese automatisch in das Anonymisierungsverfahren gegeben. Hierbei arbeiten in Reihe geschaltete sogenannte Masternodes und mischen die hereingegebene Anzahl Coins. Mindestens 2 Masternodes müssen für DarkSend benutzt werden, damit Masternodes nicht den Absender und den

[48] Halford, Rob (2014), Gridcoin.us

[49] Anonym (Unbekannt), Wikipedia

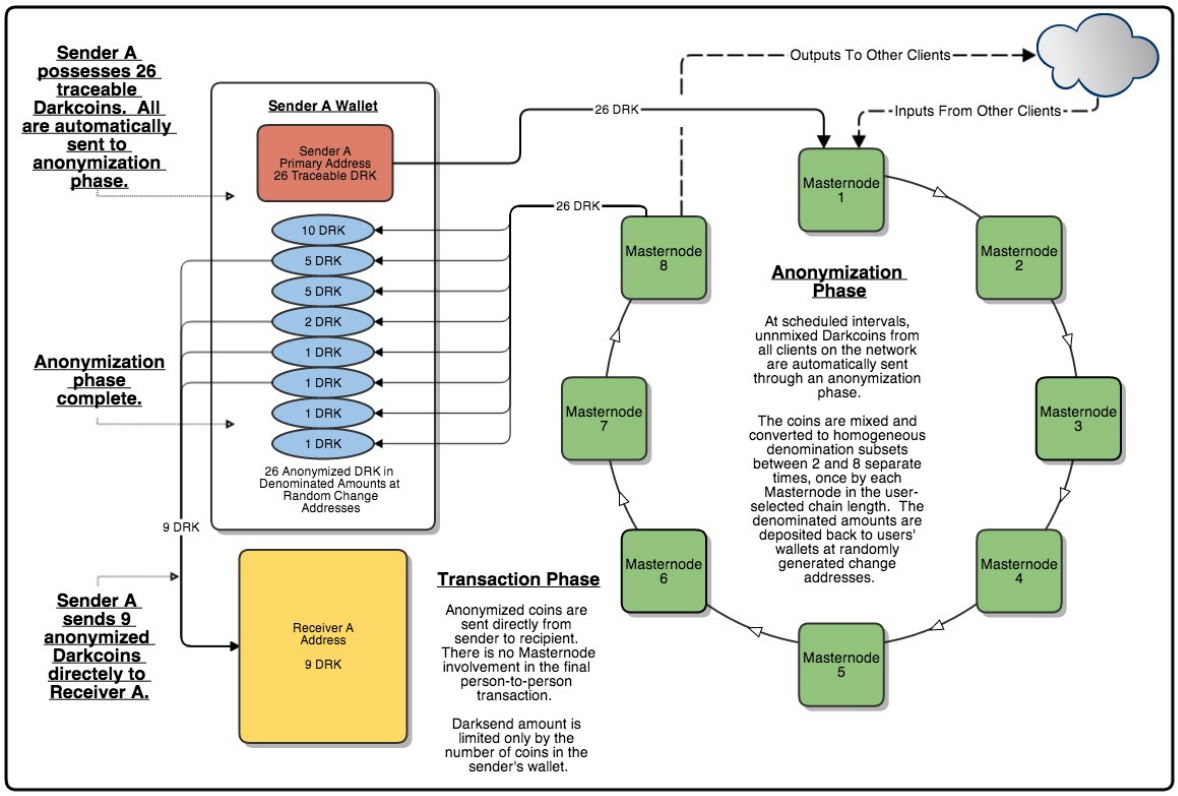

Abbildung 3.12: DarkSend+ Schema für die automatische Anonymisierung von Inputs (darkcointalk.org)

Empfänger einer zu anonymisierenden Coin-Anzahl kennen. Maximal können 8 Masternodes dieses vermischen vornehmen. Der letzte Masternode schickt die gestückelten Coinbeträge an zufällig erzeugte Wechselgeld-Adressen. Dabei kann er nicht wissen wie viele Coins und von wem ursprünglich diese Coins kamen. Der Sender A gibt an den Empfänger A (gelb in der Grafik) von seinen 26 Coins 9 ab. Dazu übergibt er dem Empfänger passend gestückelte Inputs aus dem vorherigen Anonymisierungsprozess[50]. Das Mixen könnte auch ungerade Werte verarbeiten, jedoch soll durch homogene Größen die Zuordnungswahrscheinlichkeit gesenkt werden. Für die Anonymisierung erhalten Masternodes einen Teil der Transaktionsgebühren.

[50]Duffield, Evan and Hagan, Kyle (2014), darkcoin.io

4 Auswertung

Anhand der technischen Untersuchung und des Vergleichs verschiedener Aspekte dezentraler, elektronischer Währungen, können einige Schlüsse gezogen werden.

Währungen, die ausschließlich digital existieren, sind neu, interessant und keineswegs mehr nur eine verrückte Idee. Ohne Banken, Regulierungen, Steuern oder andere externe Einflüsse sollte diese Art der Währung besser und unabhängiger werden als "etablierte" Währungen. In den vergangenen 3 Jahren hat sich allerdings gezeigt, dass ohne jeglichen Einfluss auf dezentrale Währungen viele unglückliche Ereignisse wie Hackerattacken oder Diebstähle passieren. Auch illegale Geschäfte z.B. mit Drogen können kaum unterbunden werden.

Da Coin-Währungen allerdings global funktionieren und durch einzelne Regierungen kaum zu unterbinden sind, sollte es im Interesse von Regierungen sein, gemeinsam mit anderen Regierungen über die Existenz von Coin-Währungen zu diskutieren. Auch aus der Perspektive der Nutzer sollte es von Vorteil sein, wenn Regierungen dezentrale Währungen unter bestimmten Bedingungen anerkennen. Jederzeit können erhebliche Kursschwankungen durch Haltungswechsel einzelner Regierungen gegenüber den digitalen Währungen auftreten. Zudem würde ein Mindestmaß an Regulierung zu einer Rechtssicherheit beitragen, die vor allem die Akzeptanz unter Händlern erhöhen könnte und damit die Währung aufwertet.

In Deutschland wird Bitcoin als "privates Geld" anerkannt. Kursgewinne sind nach einem Jahr sogar steuerfrei[51]. Der US-Bundesstaat New York hingegen hat bereits einen "BitLicense" genannten Entwurf vorgelegt, in dem Vorschriften zu Geldwäsche, Verbraucherschutz und Cybersicherheit festgehalten sind[52]. Diese Vorschriften sollen zwar nur für Finanzdienstleister gelten, sind aber ein erster Schritt in Richtung Regulierung dezentraler Währungen. In anderen Ländern wie z.B. China ist Finanzdienstleistern der Handel mit Bitcoins gänzlich untersagt[53].

Es gibt unter den dezentralen Währungen einige technische Besonderheiten. So ist die Anonymität in der Umsetzung von DarkCoin (3.7) offenbar ein reizvoller Aspekt für viele

[51] Fennen, Nicolas (2013), Netzpolitik
[52] Kannenberg, Axel (2014), Heise
[53] Knoke, Felix (2014), Spiegel Online

Teilnehmer, fördert jedoch auch einen illegalen Wirtschaftszweig. Für andere Teilnehmer ist die Verarbeitungsdauer von Transaktionen von hoher Bedeutung (3.4), wobei erläutert wurde wie sich die Wahl der Blockbildungszeit als eine Sicherheitslücke herausstellen kann. Werden neue Währungen vorgestellt, sind sie am Tag ihrer Einführung bereits durch verschiedenste Techniken (2.6) vernetzt. Viele technische Aspekte dezentraler Währungen sind durchaus ausgereift.

Einer der meistdiskutierten Aspekte ist die Erzeugung von Coins und der damit verbundenen Methode des Arbeitsbeweises. In Medien wird oft auf populistische Art und Weise besonders die Möglichkeit des "Geld verdienens" in den Vordergrund gestellt. Dabei ist ohne Investition in leistungsstarke Hardware die Chance auf einen tatsächlichen Verdienst bei PoW-basierten Währungen gering. Dennoch ist das Angebot der Hersteller groß. Es gibt immer stärkere ASIC Miner mit immer höheren Hashraten je Sekunde, die verkauft oder vermietet werden. Unternehmen wie "Coinbau" wollen ASIC Miner mit garantierten Hashraten vermieten, wobei das Risiko eines erfolgreichen Geschäfts letztlich beim Kunden liegt.

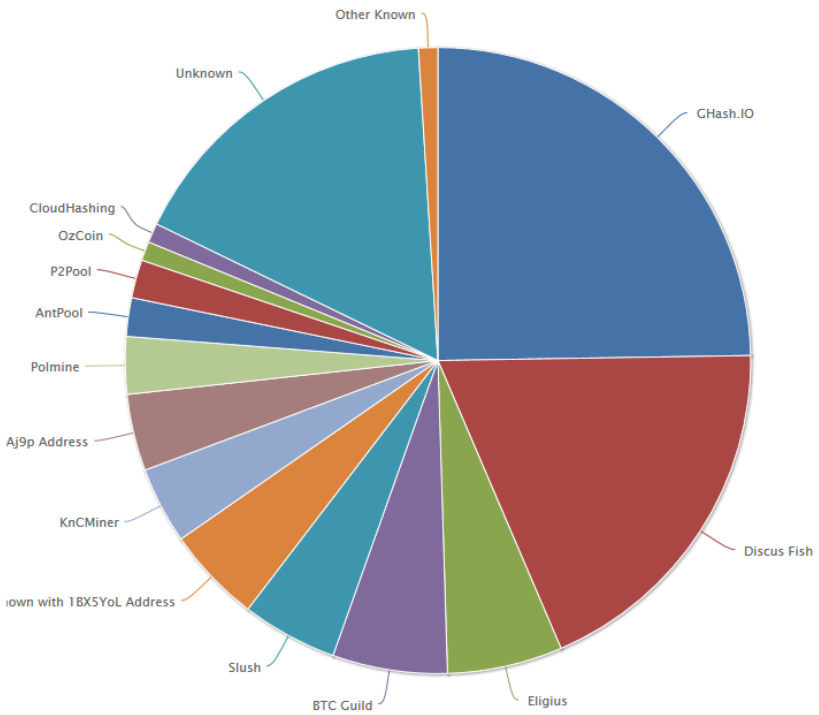

Abbildung 4.1: Verteilung der Hashrate im Bitcoin-Netzwerk (blockchain.info)

Denn es ist ungewiss, wie sich der Kurs dezentraler Währungen entwickelt und wie hoch demnach der Gewinn eines bestimmten Arbeitseinsatzes sein kann. Für den Arbeitsbeweis haben sich verschiedene Verfahren als geeignet herausgestellt. Neben der Erzeugung möglichst vieler Hashes ohne einen Nutzen, gibt es auch sinnvolle Einsatzgebiete für die Rechenkraft der

Teilnehmer eines Coin-Netzwerkes wie die Berechnung von Primzahlen oder die Unterstützung vielfältiger BOINC Projekte. Des weiteren gibt es PoS und PoB Verfahren, die weitaus weniger Rechenleistung als PoW Verfahren beanspruchen und dennoch den Erhalt von Coin-Netzwerken gewährleisten können.

Während der Fokus vieler Teilnehmer auf der Gelderzeugung liegt, wird die Wichtigkeit der Dezentralität des neuen Geldkonzeptes oft vernachlässigt. Abb. 4.1 illustriert die Verteilung der Rechenkraft (ausgedrückt in Hashrate) nach Akteuren im Bitcoin Netzwerk (siehe auch 3.2.1). Dabei fällt auf, dass "GHash.IO" und "Discus Fish" einen erheblichen Anteil an der Hashrate des Netzwerks halten und damit zusammen einen großen Einfluss auf das Netzwerk haben. Es darf nicht vergessen werden, dass die Marktkapitalisierung im Fall von Bitcoin bei fast 7 Mrd. USD liegt und im Zweifelsfall nur zwei Akteure über die Stabilität des gesamten Netzwerks entscheiden.

Es sollte daher im Interesse aller Teilnehmer liegen, einen dezentralen Weg der Hashraten-Verteilung anzustreben. Wenn man das Verfahren PoW betrachtet, sind "P2Pools" eine gute Alternative im Vergleich zu konventionellen, zentralen Mining Pools. Doch für die Teilnahme in "P2Pools" einen eigenen Full Node zu betreiben könnte für einige Teilnehmer eine hohe Anforderung sein, da der Speicherbedarf der Blockchain derzeit bei Dogecoin 5,82GB und bei Bitcoin sogar 26,08GB beträgt. Durch die in Netzwerken getätigten Transaktionen wächst die Blockchain täglich weiter an. Es gibt Ansätze zur Reduzierung der Blockchain, die allerdings derzeit bisher nur in einigen Währungen umgesetzt wurden.

Dezentralität kann nur erreicht werden, wenn ein einzelner Teilnehmer keinen großen Anteil der Blöcke des Netzwerks berechnen kann. Als alternative Verfahren haben sich PoS und PoB herausgestellt. Die Hashrate eines einzelnen tritt in den Hintergrund und stattdessen wird als Arbeitsbeweis im Fall von PoS der Besitz von Coins mit mehr Coins belohnt. PoS hat allerdings den Schwachpunkt, dass viel Besitz und wenig Umlaufgeschwindigkeit belohnt wird, wodurch die Währung nicht als Zahlungsmittel genutzt wird. Im Fall von PoB muss ein Teil der Coins vernichtet werden um die Chance auf neue Coins zu erhalten.

Die potenzielle Sicherheit unter den verglichenen Währungen ist hoch. Wallets können verschlüsselt werden und durch Script-Befehle können Transaktionen erst unter Verwendung von zwei privaten Schlüsseln freigegeben werden (2.2). Obgleich diese Möglichkeiten existieren, ist es bereits häufiger vorgekommen, dass große Mengen Coins gestohlen wurden. Der Grund könnte die zentrale Aufbewahrung von Coins in unverschlüsselten Wallets (Hot Wallets) auf dem eigenen Rechner oder bei Finanzdienstleistern sein.

Das in 3.5.2 untersuchte Problem der Umlaufgeschwindigkeit dezentraler Währungen bleibt als problematische Entwicklung bestehen. Angenommen wurde, dass die Umlaufgeschwindigkeit einer Währung stellvertretend für die Akzeptanz selbiger als reguläres Zahlungsmittel steht. Dadurch kann aus dem in Abb. 3.9 gezeigten Verlauf der Umlaufgeschwindigkeit gefolgert

werden, dass Bitcoin wie auch seine Alternativen kaum als Zahlungsmittel genutzt werden. Die Umlaufgeschwindigkeit einer Währung sollte mit der Wertsteigerung linear ansteigen. Da trotz Kursanstieg die Umlaufgeschwindigkeit nicht gestiegen ist, kann eine Nutzung von Bitcoin und anderen Coin-Währungen als Spekulationsobjekte geschlussfolgert werden.

Diese ungleiche Entwicklung von Wert und Umlaufgeschwindigkeit könnte sich als ein charakteristisches Problem aller Währungen herausstellen. Die technischen Feinheiten scheinen unterdessen eine eher untergeordnete Rolle zu spielen. Gary North beschreibt Bitcoin gar als ein modernes Ponzi Schema. Das Wachstum einer Währung kann demnach nur erhalten werden, wenn mehr Menschen in sie investieren und sich einen höheren Gewinn erhoffen, als sie jeweils investiert haben[54]. Ähnliche Überlegungen äußert auch Patrik Korda. Er behauptet "der ständig steigende Preis hätte nichts mit dem tatsächlichen Wert der Währung gemeinsam" und dass der Kurs bald fallen würde[55].

Die Aussagen von North und Korda sind fast ein Jahr alt. Seit Februar 2014 verhält sich der Kurs von Bitcoins für seine Verhältnisse stabil zwischen €400 und €600[56]. Die Kurse alternativer, dezentraler Währungen gleichen sich an den Kurs des Bitcoins an. Der Erfolg dezentraler, elektronischer Währungen hängt wie der Erfolg von klassischen, zentralen Währungen von der Akzeptanz seiner Nutzer ab. Tausende Händler akzeptieren mittlerweile Coin-Währungen als Zahlungsmittel. Das Selbstverständnis in der Benutzung als Zahlungsmittel ist derzeit jedoch nicht zu beobachten.

Coins können als einheitliche, internationale Werteinheit den globalen Handel im Internet und auch in Ladengeschäften vereinfachen. Geldwechsel und hohe Transaktionsgebühren könnten durch eine globale Verwendung von Coin-Währungen abgeschafft werden. Es bleibt daher zu hoffen, dass Halter von Bitcoins, Litecoins, Dogecoins und anderen Coins erkennen, wie wichtig die Benutzung von Coins als Zahlungsmittel statt als Wertanlage für den langfristigen Erhalt dieser Währungen ist.

[54] North, Gary (2013), Gary North's Specific Answers
[55] Sobiraj, Lars (2013), Gulli News
[56] Anonym (2014), Finanzen.net

Literaturverzeichnis

[Ano09] ANONYM: *Bitcoin v0.1 released*. Mailing List, 2009. http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html; abgerufen am 02.08.2014 - Datei: Bitcoins_Release.pdf.

[Ano10] ANONYM: *Pizza for bitcoins?* Forum, 2010. https://bitcointalk.org/index.php?topic=137.0; abgerufen am 28.07.2014 - Datei: Bitcoins_Pizza.pdf.

[Ano13a] ANONYM: *Article: Moore's law*. Webseite, 2013. http://www.britannica.com/EBchecked/topic/705881/Moores-law; abgerufen am 10.08.2014 - Datei: mooreslaw.pdf.

[Ano13b] ANONYM: *Dollarkurs auf Mt.Gox zwischen 01.10-31.12.2013*. Website, 2013. http://bitcoincharts.com/charts/mtgoxUSD#rg730zigDailyzczsg2013-10-01zeg2013-12-31ztgMzm1g10zm2g25zl; abgerufen am 20.07.2014 - Datei: Bitcoincharts_BTCKursHoch.pdf.

[Ano14a] ANONYM: *List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses*. Forum, 2014. https://bitcointalk.org/index.php?topic=83794.msg923921#msg923921; abgerufen am 20.07.2014 - Datei: bitcointalk_org_topic_83794.pdf.

[Ano14b] ANONYM: *Litecoin Development Team's official position on Litecoin's proof of work*. Forum, 2014. https://litecointalk.org/index.php?topic=18166.0; abgerufen am 05.08.2014 - Datei: litecoin_nohardfork.pdf.

[Ano14c] ANONYM: *Mining hardware comparison*. Wiki, 2014. https://en.bitcoin.it/wiki/Mining_hardware_comparison; abgerufen am 05.08.2014 - Datei: mining_hardware.pdf.

[Ano14d] ANONYM: *The Monarch*. Webseite, 2014. http://www.butterflylabs.com/monarch/; abgerufen am 05.08.2014 - Datei: butterfly_monarch.pdf.

[Ano14e] ANONYM: *The Monarch*. Webseite, 2014. http://bitcoinprbuzz.com/zeusminer-announces-the-first-scrypt-asic-miners-to-ship-worldwide/; abgerufen am 05.08.2014 - Datei: first_scrypt_asic.pdf.

[Ano14f] ANONYM: *Source Code: chainparams.cpp*. Codeverwaltung, 2014. https://github.com/bitcoin/bitcoin/blob/master/src/chainparams.cpp#L96; abgerufen am 04.08.2014 - Datei: BitcoinDNS.pdf.

[Ano14g] ANONYM: *Wallet encryption*. Wiki, 2014. https://en.bitcoin.it/wiki/Wallet_encryption; abgerufen am 12.08.2014 - Datei: wallet_encryption.pdf.

[Ano14h] ANONYM: *Why Proof-of-Burn*. Webseite, 2014. https://www.counterparty.co/why-proof-of-burn/; abgerufen am 10.08.2014 - Datei: counterparty_pob.pdf.

[BacX] BACK, ADAM: *Hashcash FAQ*. Website, X. http://www.hashcash.org/faq/; abgerufen am 13.07.2014 - Datei: Hashcash_FAQ.pdf.

[Cap12] CAP, CLEMENS H.: *HMD Praxis der Wirtschaftsinformatik*. Gabler Verlag, Deutschland, Ausgabe 49 Auflage, 2012.

[Che11] CHEN, ADRIAN: *The Underground Website Where You Can Buy Any Drug Imaginable*. Webseite, 2011. http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160; abgerufen am 20.07.2014 - Datei: Gawker_Any_Drug_Imaginable.pdf.

[Con11] CONWAY, EDMUND: *50 Schlüsselideen Wirtschaftswissenschaft*. Spektrum Akademischer Verlag, Deutschland, 2011.

[Dö13] DÖRNER, STEPHAN: *2013 – das Jahr des Bitcoin*. Forum, 2013. http://www.wsj.de/article/SB10001424052702304367204579266381130266234.html; abgerufen am 20.07.2014 - Datei: WSJ_JahrdesBitcoins2013.pdf.

[DaiX] DAI, WEI: *B-Money: a scheme for a group of untraceable digital pseudonyms*. Website, X. http://www.weidai.com/bmoney.txt; abgerufen am 13.07.2014 - Datei: bmoney.txt.

[DL14] DEMIAN LERNER, SERGIO: *25-second irreversible confirmations for instant payments*. Webseite, 2014. http://bitslog.wordpress.com/2014/02/17/5-sec-block-interval/; abgerufen am 12.08.2014 - Datei: bitslog_blocktimes.pdf.

[Gri14] Grieve, Jack: *Researchers uncover likely author of original Bitcoin paper*. Website, 2014. http://www.aston.ac.uk/about/news/releases/2014/april/researchers-uncover-likely-author-of-original-bitcoin-paper/; abgerufen am 15.07.2014 - Datei: Linguistic_Analysis_Bitcoin_Founder.pdf.

[HBG14] Hering, Ekbert, Klaus Bressler und Jürgen Gutekunst: *Elektronik für Ingenieure und Naturwissenschaftler*. Springer Berlin Heidelberg, Deutschland, 6. Auflage Auflage, 2014.

[Kir14] Kirk, David: *Cryptocurrency: What is a fork?* Webseite, 2014. http://www.tech-recipes.com/rx/48517/cryptocurrency-what-is-a-fork/; abgerufen am 09.08.2014 - Datei: hardfork.pdf.

[Lee13] Lee, Timothy B.: *Bitcoin needs to scale by a factor of 1000 to compete with Visa. Here's how to do it.* Blog, 2013. http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/12/bitcoin-needs-to-scale-by-a-factor-of-1000-to-compete-with-visa-heres-how-to
abgerufen am 27.07.2014 - Datei: Bitcoin_needstoscale.pdf.

[Lop09] Lopp, Jameson: *Bitcoin Nodes: How Many is Enough?* Blog, 2009. https://medium.com/@lopp/bitcoin-nodes-how-many-is-enough-9b8e8f6fd2cf; abgerufen am 27.07.2014 - Datei: Medium_WhatIsEnough.pdf.

[M.14] M., Ernest: *Bitcoin: A Peer-to-Peer Electronic Cash System*. Website, 2014. http://www.lightcode.com/downloads/UNITAS_white_paper.pdf; abgerufen am 25.07.2014 - Datei: UNITAS_white_paper.pdf.

[Man07] Mankiw, N. Gregory: *Money and Inflation - Macroeconomics*. Presentation, 2007.

[Nak09] Nakamoto, Satoshi: *Bitcoin: A Peer-to-Peer Electronic Cash System*. Website, 2009. https://bitcoin.org/bitcoin.pdf; abgerufen am 20.07.2014 - Datei: bitcoin_whitepaper.pdf.

[OO91] Okamoto, Tatsuaki und Kazuo Ohta: *Advances in Cryptology - CRYPTO 91*. SP Gabler Verlag, Deutschland, 1991.

[SKG12] Sorge, Christoph und Artus Krohn-Grimberghe: *Datenschutz und Datensicherheit - DuD*. Springer-Verlag, Deutschland, 2012.

[Sza08] Szabo, Nick: *Bit gold*. Website/Blog, 2008. http://unenumerated.blogspot.com/2005/12/bit-gold.html; abgerufen am 13.07.2014 - Datei: Unenumerated_Bitgold.pdf.

[Vig14] Vigna, Paul: *5 Things About MT. Gox's Crisis*. Webseite, 2014. http://blogs.wsj.com/briefly/2014/02/25/5-things-about-mt-goxs-crisis/; abgerufen am 20.07.2014 - Datei: WSJ_briefly_5-things-about-mt-goxs-crisis.pdf.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorgelegte Arbeit mit dem Titel „**Vergleich dezentraler elektronischer Währungen**“, selbstständig und nur unter Verwendung der angegebenen Hilfsmittel erstellt habe.

Alle aus anderen Werken stammenden wörtlichen oder sinngemäßen Übernahmen wurden als diese von mir kenntlich gemacht.

Rangsdorf, den 25. August 2014

Christian Pfnür