UNIVERSITÄT KOBLENZ · LANDAU
Fachbereich 4: Informatik

Institute for Management
Institut für Management

Transaktionsüberwachung in dezentralen digitalen Transaktionssystemen mit öffentlicher Transaktionshistorie

Bachelorarbeit

zur Erlangung des Grades eines Bachelor of Science (B.Sc.)
im Studiengang Informationsmanagement

vorgelegt von

Markus Münzel

Erstgutachter:	Prof. Dr. Klaus Diller Institut für Management
Zweitgutachter:	jProf. Dr. Thomas Kilian Institut für Management

Koblenz, im Dezember 2013

Erklärung

Hiermit bestätige ich, dass die vorliegende Arbeit von mir selbständig verfasst wurde und ich keine anderen als die angegebenen Hilfsmittel – insbesondere keine im Quellenverzeichnis nicht benannten Internet–Quellen – benutzt habe und die Arbeit von mir vorher nicht in einem anderen Prüfungsverfahren eingereicht wurde. Die eingereichte schriftliche Fassung entspricht der auf dem elektronischen Speichermedium (CD-ROM).

	Ja	Nein
Mit der Einstellung dieser Arbeit in die Bibliothek bin ich einverstanden.	☐	☐
Der Veröffentlichung dieser Arbeit im Internet stimme ich zu.	☐	☐

.....

(Ort, Datum) (Unterschrift)

Inhaltsverzeichnis

Abbildungsverzeichnis

Abstrakt

deutsch

Dezentrale digitale Transaktionssysteme mit öffentlicher Transaktionshistorie haben ihrer Architektur nach keine Transaktionsüberwachung, um unerwünschte Transaktionen zu unterbinden und deren Sender und Empfänger zu identifizieren. Mit Einführung einer öffentlichen Liste von Adressen, welche zu solchen unerwünschten Transaktionen gehören, ist es möglich, diese Adressen durch allgemeinen Ausschluss zu isolieren und dadurch die unerwünschten Transaktionen zu unterbinden sowie Besitzer unerwünschter Adressen zu deanonymisieren. Die Verwaltung von öffentlichen Listen kann dabei dezentral von mehreren Instanzen mit Hilfe eines Vertrauensnetzwerks durchgeführt werden, sodass der dezentrale Charakter der Systeme erhalten bleibt.

english

The architecture of decentralized digital transaction systems with public transaction history provides no transaction monitoring to prevent unwanted transactions and to identify the transmitter and receiver of those transactions. With the introduction of a public list of unwanted addresses, it is possible to isolate these unwanted addresses by general exclusion and thereby to prevent unwanted transactions, as well as to identify the owners of unwanted addresses. The public list management can be performed by decentralized multiple instances using a trust network, so that the decentralized nature of the systems is maintained.

1 Einleitung

Gängige Währungen wie der Euro, der Dollar oder das britische Pfund zeichnen sich unter anderem dadurch aus, dass die ihnen zugrunde liegenden Währungssysteme zentraler Lenkung und damit einer zentralen Kontrolle unterliegen.
Die Länder der gerade exemplarisch genannten Währungen haben staatliche Notenbanken eingerichtet, die diese zentrale Kontrolle übernehmen und beispielsweise die Geldmenge steuern[1]. Die Währungssysteme sind ihrer grundlegenden Architektur nach nicht digital. Transaktionen in den Währungen werden allgemein nicht öffentlich von Person zu Person oder über Banken abgewickelt.

Konträr zu diesen Systemen sind jedoch auch Währungssysteme vorstellbar, in denen alle Transaktionen öffentlich sind, welche einer völlig digitalen Architektur unterliegen und dezentral organisiert sind. In dezentralen Systemen, ohne zentralen Emittenten der Währung, wäre keine zentrale Einflussnahme wie die Steuerung der Geldmenge möglich. Eine völlig digitale Natur eines Währungssystems kann Vorteile gegenüber gängigen Systemen haben wie etwa mögliche geringere Transaktionskosten und problemlose internationale Transaktionen.

Transaktionen in einem solchen Währungssystem werden digital zwischen den einzelnen Parteien ohne dritte Partei abgewickelt. Nur die Transaktion als solche ist öffentlich in der Transaktionshistorie sichtbar, die involvierten Parteien sind aber nicht in der Historie vermerkt.
Im Gegensatz dazu sind in gängigen Währungssystemen den Banken die bei einer Transaktion beteiligten Parteien bekannt, die Transaktion an sich ist aber nicht öffentlich. Banken

[1] Vgl. Bundesrepublik Deutschland 2013: Bundesbankgesetz - BBankG, als Beispiel für die Steuerung der Geldmenge in Deutschland siehe §14 Abschnitt vier.

sind nach den in ihren Ländern geltenden Gesetzen[2] dazu verpflichtet, Transaktionen, die z.B. in Verdacht stehen, der Geldwäsche zugeordnet werden zu können, zu identifizieren.

In einem dezentralen digitalen Währungssystem stellt sich daher die Frage, inwieweit es Betrug, Geldwäsche und andere kriminelle Aktivitäten begünstigen würde, da ein zentrales Einschreiten zur Verhinderung dessen aufgrund fehlender zentraler Instanz mit Kenntnis der bei einer Transaktion involvierten Parteien nicht möglich ist.

Die vorliegende Arbeit wird ein mögliches Konzept erläutern, wie eine Transaktionsüberwachung in einem solchen dezentralen System mit öffentlicher Transaktionshistorie arbeiten könnte, um Aufgaben wie Geldwäschebekämpfung etc. zu gewährleisten ohne dabei den dezentralen Charakter des Systems durch Einführung einer zentralen Instanz auszuhebeln.
Darüber hinaus werden neben dem Konzept mögliche Auswirkungen einer Überwachung auf Eigenschaften des System als solches und seine ehrlichen Nutzer untersucht.

Bereits seit den 1980er Jahren wurden verschiedene Konzepte digitaler Geld- und Währungssysteme erdacht[3]. Keines dieser Systeme setzte die Eigenschaften der Dezentralität praxistauglich um. Erst im Jahr 2009 wurde ein digitales dezentrales Währungssystem mit öffentlicher Transaktionshistorie unter dem Namen Bitcoin öffentlich, welchem seit 2011 größeres öffentliches Interesse zuteil wird.
Als Vertreter der zu Anfang beschriebenen dezentralen digitalen Währungssysteme[4] wird das Bitcoin System in dieser Arbeit zuerst eingehend erläutert, um das Konzept der Transaktionsüberwachung dann an diesem erklären zu können und mögliche Implikationen der Überwachung am Beispiel des realen Bitcoin Systems zu veranschaulichen.

[2] Vgl. Bundesrepublik Deutschland 2008: Geldwäschegesetz - GwG, als Beispiel für die Verpflichtung Deutscher Bank siehe §2.

[3] Auf welche unter anderem in Abschnitt 3.4 eingegangen wird.

[4] Das Bitcoin System wird häufig als digitales Krypto-Währungssystem betitelt. Ob es als Währungssystem zu betiteln ist, liegt außerhalb der Betrachtung dieser Arbeit. Die Bezeichnung als Währungssystem spielt für die weitere Betrachtung in dieser Arbeit keine Rolle. Das Bitcoin System wird daher folgend als Transaktionssystem bezeichnet.

2 Gliederung der Arbeit

In Teil I der vorliegenden Arbeit wird als Grundlage für das Verständnis das Bitcoin System eingehend beschrieben. Welche Eigenschaften und Vorteile dem System zugeordnet werden können, wird dargelegt, um aufzuzeigen, weshalb ein Befassen mit Transaktionssystemen dieser Art überhaupt interessant ist. Neben der Historie an digitalen Geld- und Transaktionssystemen, die vor dem Bitcoin System erdacht wurden und auf denen es teils aufbaut, wird die Funktionsweise des Systems in Hinblick auf das in Kapitel 6 eingeführte Transaktionsüberwachungskonzept beschrieben. Daneben steht im Fokus, wie das System genutzt wird, welche Dienste in Verbindung mit ihm bisher entstanden sind und wie seine momentane Nutzung ausgestaltet ist. Ökonomische Aspekte des Bitcoin Systems, wie die Frage, weshalb der Bitcoin Währung überhaupt ein Wert angerechnet werden kann oder wie das System einzuordnen ist, werden der Vollständigkeit halber angerissen, stehen aber nicht im Fokus.
Teil II schließlich befasst sich mit den Herausforderungen und Problemen, denen das Bitcoin System aktuell ausgesetzt ist. Kursschwankungen, Systemverwundbarkeit und ökologische Bedenken sind drei beispielhafte Herausforderungen, die erläutert werden. Der zentrale Aspekt der Arbeit wird schließlich in Teil II aufgegriffen. Transaktionen, gehörig zu allgemein unerwünschtem, im Regelfall illegalen Vorgehen, können über das Bitcoin System abgewickelt werden. Daran anknüpfend wird das Konzept der Transaktionsüberwachung, welches diesem Problem entgegenwirken soll, beschrieben und die Implikationen der Überwachung auf das System und seine Nutzer diskutiert.

Teil I

Grundverständnis des Bitcoin Systems

3 Das Bitcoin System

Bevor in Abschnitt 3.6 die genaue Funktionsweise des Bitcoin Systems erläutert wird, ist folgende Beschreibung als vereinfachte Funktionsbeschreibung des Systems aus Nutzerperspektive zum besseren Verständnis vorgelagert.
Bitcoin[1] Nutzer[2] kann jeder werden[3], der Zugriff auf einen Computer[4] mit Internetzugang hat. Der Nutzer bezieht eines der verfügbaren Bitcoin Programme aus dem Internet und installiert es auf seinem Rechner, um dann mit diesem Programm die Geldeinheiten des Systems, welche als Bitcoins bezeichnet werden, zu erhalten oder zu versenden. Mit diesem Programm kann er sich sein Bitcoin Konto, welches allgemein als Wallet bezeichnet wird, anlegen und verwalten.
Das Konto selbst enthält jedoch nicht die Bitcoins des Nutzers. Diese werden im Bitcoin System selbst in der sogenannten Block Chain[5] gespeichert. Das Bitcoin Programm des Nutzers kommuniziert daher über das Internet mit allen anderen aktiven Bitcoin Programmen, um von diesen, wenn es dem System beitritt, die aktuelle Block Chain zu beziehen[6]. Mit seinem Programm kann der Nutzer sich dann beliebig viele Bitcoin Adressen anlegen, mit denen er Bitcoins empfangen und wieder an Bitcoin Adressen versenden kann. Zum Senden und Empfangen von Bitcoins muss er immer mit dem Bitcoin Netzwerk verbunden sein.

Die Block Chain speichert jede im Bitcoin System durchgeführte Transaktion zwischen

[1] Im Folgenden wird mit „Bitcoin“ immer das Bitcoin System bezeichnet, mit „Bitcoins“ werden die Einheiten an transferierbarem Guthaben innerhalb des Bitcoin Systems betitelt.
[2] Aus Gründen der besseren Lesbarkeit wird im gesamten Text auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.
[3] Nutzer im Sinne von Teilnehmer im Bitcoin Netzwerk. Es ist mittlerweile auch möglich Bitcoins ohne Computer auf andere Weise zu besitzen, wie in Abschnitt 4.3 erläutert wird.
[4] Auch per Smartphone siehe Kapitel 4.
[5] Genaueres dazu folgt in Unterabschnitt 3.6.2.
[6] Vgl. Nakamoto 2008: Bitcoin Proposal.

den Bitcoin Adressen. Sie wird als „Chain“, englisch für „Kette“, bezeichnet, da sie durch kryptografische Funktionen nicht nur die Transaktionen, sondern auch deren zeitliche Abfolge abbildet und somit eine gedachte Kette aller jemals im Bitcoin System durchgeführten Transaktionen bildet.
Sendet ein Nutzer Bitcoins an eine Adresse, so wird diese Transaktion mit Senderadresse und Empfängeradresse sowie dem transferierten Bitcoin Betrag in der öffentlichen Block Chain gespeichert. Zu diesem Zweck sendet der Nutzer seine Transaktion mittels des Bitcoin Netzwerks an alle anderen Nutzer. Seine Transaktion wird dann in die Block Chain aufgenommen und ist gültig. Dies bedeutet, dass aus der Block Chain immer öffentlich ersichtlich ist, zu welcher Adresse aktuell wie viele Bitcoins gehören.

Um Bitcoins zu besitzen, muss der Bitcoin Nutzer also nachweisen, Eigentümer einer dieser Adressen zu sein. Dies tut er mit seiner Wallet. Bei der Erstellung einer Adresse legt das Bitcoin Programm in ihr eine einzigartige Zeichenfolge[7] an.
Diese Zeichenfolge dient fortan dazu, dass derjenige, in dessen Besitz die Zeichenfolge ist, gegenüber dem Bitcoin System beweisen kann, dass er über die Adresse und daher auch über die Bitcoins, welche der Adresse über die Block Chain zugerechnet werden, verfügen darf.
Geht die Zeichenfolge verloren oder wird sie anderen als dem rechtmäßigen Besitzer bekannt, können die Bitcoins, zugehörig zu der Adresse der Zeichenfolge, nicht mehr bzw. auch von dem nicht rechtmäßigen Besitzer transferiert werden.
Die Wallet ist dabei eine Datei, die das Bitcoin Programm auf dem Rechner des Nutzer anlegt. Sie enthält alle erstellten Adressen des Nutzers sowie die für den Eigentumsnachweis der Adressen nötigen Zeichenfolgen und ist dementsprechend wie ein Zugangsschlüssel für die Bitcoins des Nutzers zu betrachten und auch dementsprechend zu schützen[8].

Will der Nutzer eine Transaktion durchführen, ist der Prozess vereinfacht im Folgenden erörtert. Der Nutzer benötigt die Bitcoin Adresse des Empfängers. Er erstellt mit seinem Bitcoin Programm einen Transaktionsauftrag, in dem er festlegt, wie viele Bitcoins der Empfängeradresse gutgeschrieben werden sollen.

[7] Dieser Zeichenfolge ist ein Private-Key zu dem auch ein Public-Key, die Bitcoin Adresse, gehört. Weitere Erklärungen folgen in Unterabschnitt 3.6.2.
[8] Siehe Abschnitt 4.1.1.

In diesen Transaktionsauftrag fließen in einem kryptografischen Signierverfahren die Zeichenfolgen aus seiner Wallet ein, um zu beweisen, dass der Nutzer über die Bitcoins der Absenderadressen verfügen kann.
Den Transaktionsauftrag sendet sein Bitcoin Programm dann in das Bitcoin Netzwerk an alle anderen Nutzer. Wieder in einem kryptographischen Verfahren[9] wird seine Transaktion in die Block Chain aufgenommen.
Dieser Prozess des Aufnehmens in die Block Chain nimmt Zeit in Anspruch. Erst wenn seine Transaktion in die Block Chain aufgenommen worden ist, ist sie gültig.
Dabei kann der Nutzer Bitcoins beispielsweise aus Tauschbörsen beziehen oder beim sogenannten „Mining“ Bitcoins erzeugen. Das Mining ist der Prozess, bei welchem Transaktionen an die Block Chain angefügt werden. Beteiligt sich ein Nutzer erfolgreich durch Bereitstellen von Rechenleistung an diesem Anfügeprozess, wird er mit Bitcoins belohnt, die seiner Adresse gutgeschrieben werden. Dieser Mining Prozess wird systembedingt vorgegeben, bei Erreichen von 21 Millionen erzeugten Bitcoins eingestellt[10]. Die maximale Menge an Bitcoins ist folglich beschränkt.

3.1 Eigenschaften

Um zu verstehen, warum Bitcoins als digitales Geld- oder Transaktionssystem Anklang finden, ist es nötig sich die Vorteile, die dem System angerechnet werden, sowie die Eigenschaften von Bitcoin bzw. den Bitcoins vor Augen zu führen. Die Eigenschaften hängen eng mit den im nächsten Abschnitt 3.2 behandelten Bitcoin zugeordneten Vorteilen zusammen und entsprechen sich demnach teilweise.

3.1.1 Dezentralität

Eine der für diese Arbeit wichtigsten Eigenschaften von Bitcoin ist dessen Dezentralität. Im System gibt es aus Systemarchitekturperspektive keine Instanz[11], die zentral Steuerungs- oder Kontrolleinfluss auf das System hat. Dazu zählt vor allem, dass die Emission von Bitcoins nicht zentral erfolgt, sondern jeder Nutzer Emittent von Bitcoins durch Bereitstellen

[9] welches in Unterabschnitt 3.6.2 näher erklärt wird
[10] Die Festlegung auf die Höhe der maximalen Menge wird in Unterabschnitt 3.6.3 erläutert.
[11] Die Entwickler des Bitcoin Clients haben alleine als Instanz Einfluss auf den Bitcoin Client und daher alleine Einfluss auf die Eigenschaften des Systems. Die Betrachtung dieses Punktes folgt in Kapitel 5.

von Rechenleistung werden kann. Die Dezentralität beruht bei Bitcoin auf der Umsetzung des Systems als Peer-to-Peer Netzwerk[12].
Aus der Dezentralität leiten sich zwei weitere Eigenschaften ab. Bitcoin Transaktionen sind erstens irreversibel, denn eine einmal an die Block Chain angefügte Transaktion kann nicht mehr rückgängig gemacht werden. Wobei schon Ansätze existieren, diese Eigenschaft durch Zusatzdienste auszuhebeln[13].
Bitcoins haben zweitens keinen vom System aus festgelegten fixen Wert bzw. Tauschwert gegenüber gängigen Währungen[14].

3.1.2 Digitalität

Die Bitcoin Architektur erzwingt eine völlig digitale[15] Umsetzung des Systems. Die nötige Nutzerkommunikation und die Rechenleistung zum Anfügen von Transaktionen an die Block Chain oder zur Durchführung anderer nötiger kryptografischer Berechnungen kann nur mittels Rechner praxistauglich umgesetzt werden.
Daher existieren die Zeichenfolgen, die zur Verfügung über die den Adressen zugeordneten Bitcoins berechtigen, in letzter Konsequenz bei Nutzung[16] nur als Bits auf einem beliebig gearteten Speichermedium. Auch die Block Chain, welche im System gespeichert wird, ist letztlich nur eine Menge von Bits. Transaktionsaufträge werden ebenfalls digital erstellt und über das Internet digital im System abgewickelt.
Aufgrund der Digitalität und der damit verbundenen Nutzung des Internets zum Betrieb der Kommunikation innerhalb des Bitcoin Systems ist das System als online System betitelbar, welches daher global nutzbar und nicht wie gängige Währungen auf bestimmte geografische Räume beschränkt ist.

[12] „A distributed network architecture may be called a Peer-to-Peer (P-to-P, P2P,...) network, if the participants share a part of their own hardware resources (processing power, storage capacity, network link capacity, printers,...). These shared resources are necessary to provide the Service and content offered by the network (e.g. file sharing or shared workspaces for collaboration). They are accessible by other peers directly, without passing intermediary entities.“ (W. Kellerer 1998 zitiert duch Schollmeier: Classification of Peer-to-Peer Networking)
[13] Siehe Unterabschnitt 4.2.3.
[14] Der Tauschwert wird über Angebot und Nachfrage in Tauschbörsen bestimmt.
[15] Auf dem System beruhende Ausgestaltungen sind nicht zwingend rein digital. Siehe dazu Kapitel 4.
[16] Zur dauerhaften Speicherung einer Adresse ist es auch möglich die Adressen z.B. auf Papier zu drucken. Bei einer Überweisung über das System muss diese jedoch wieder digitalisiert werden.

3.1.3 Virtualität

Eng zusammenhängend mit der Digitalität von Bitcoins ist auch deren virtuelle Beschaffenheit. Bitcoins können wie gängige Währungen als Zahlungsmittel fungieren[17]. Sie existieren aufgrund ihrer Digitalität nur beschränkt physisch auf Speichermedien. Dennoch können sie ihrer Wirkung nach die Funktion von Geld haben. Eine genauere ökonomische Betrachtung der Frage, was Bitcoins sind - etwa Geld, Tauschmittel etc. - wird in dieser Arbeit jedoch nicht weiter vertieft.

3.1.4 Open-Source

Zusammenhängend mit der digitalen und virtuellen Beschaffenheit lässt sich Bitcoin auch die Eigenschaften des offen gelegten Quelltextes attestieren[18]. Das gesamte Bitcoin Protokoll wurde im Sourcecode[19] des originären Bitcoin Programms abgebildet und ist frei zugänglich und damit auch das System als Ganzes Open-Source[20].
Jeder hat ausgehend davon die Möglichkeit das Bitcoin Programm weiter zu entwickeln[21] oder basierend auf dem Bitcoin Quelltext eigene Abwandlungen[22] des Bitcoin Systems zu erstellen.
Momentan wird das originäre Bitcoin Programm von der Bitcoin Foundation als Open-Source-Projekt weiterentwickelt[23].

3.1.5 Anonymität

Der Nutzer muss sich, um Teil des Bitcoin Systems zu werden, systembedingt niemandem gegenüber identifizieren. Die Zuordnung der Adressen zu Nutzern kann aus dem System allein nicht durchgeführt werden. Gleichwohl zwischen Transaktionspartnern die Identität im Regelfall beidseitig oder einseitig bekannt ist.

[17] Siehe Abschnitt 4.4 für Akzeptanzstellen von Bitcoins als Zahlungsmittel.
[18] Vgl. Bitcoin Developers 2013: Bitcoin Source Code URL: `https://github.com/bitcoin/bitcoin`.
[19] „[...]der für Menschen lesbare, in einer Programmiersprache geschriebene Text eines Computerprogramms [...]“ (Wikipedia: Quelltext)
[20] Vgl. Bitcoin Project 2013: Bitcoin.org FAQ URL: `http://bitcoin.org/en/faq`.
[21] Siehe Abschnitt 4.1.1.
[22] Unter anderem mit Litecoin Project: Litecoin und Miers: Zerocoin wurde dieser Weg schon beschritten.
[23] Vgl. Bitcoin Foundation 2013: Bitcoin Foundation: About URL: `https://bitcoinfoundation.org/about/`.

Untersuchungen bezüglich der Anonymität haben jedoch gezeigt, dass diese unter Zuhilfenahme von weiteren, außerhalb des Systems gewonnenen Daten grundsätzlich angreifbar ist.[24]
Nichtsdestoweniger wirft die grundlegende Anonymität ein Problem auf. Das sogenannte Double-Spending Problem tritt unter anderem bei anonymen online Geldsystemen auf[25]. Nutzer könnten versucht sein, ein und dieselben, unter ihrem Zugriff stehenden, Bitcoins mehrfach an verschiedene Transaktionspartner zu überweisen.
Bitcoin löst dieses Problem durch eine öffentliche Transaktionshistorie, der schon anfangs genannten Block Chain und einem Proof-of-Work[26] Mechanismus. Diese öffentliche Transaktionshistorie stellt eine weitere Eigenschaft Bitcoins dar.

Das Bitcoin System kann, zusammenfassend in seiner grundlegenden Installation ohne die in Kapitel 4 erläuterten, darauf aufbauenden Ausgestaltungen mit einzuschließen, folgendermaßen beschrieben werden.
Bitcoin ist ein virtuelles, völlig digital arbeitendes, unter Open-Source-Prinzip implementiertes und gewartetes, in allen finanz- und geldpolitischen Einfluss- bzw. Steuerungsaspekten dezentrales globales online Transaktionssystem, in welchem aufgrund der Dezentralität alle Transaktionen öffentlich abgewickelt werden, Transaktionen irreversibel sind, kein fixer Tauschwert gegenüber anderen Währungen existiert sowie zur Nutzung des Systems keine Nutzeridentität dem System selbst gegenüber offen gelegt werden muss.

3.2 Vorteile

Weshalb Bitcoin als digitales Geld- oder Transaktionssystem eine gewisse Verbreitung und Annahme findet, kann unter anderem mit den Vorteilen des Systems begründet werden. Die Vorteile resultieren dabei aus den vorangehend beschriebenen Eigenschaften. Die anfängliche Beschreibung der Vorteile des Systems soll nicht über dessen auch vorhandenen Schwierigkeiten hinwegtäuschen, auf die in Form von Herausforderungen in Kapitel 5 eingegangen wird.

[24] was in Abschnitt 3.3 genauer beleuchtet wird
[25] Vgl. Godbole/Kahate 2003: Web Technologies.
[26] Proof-of-Work: englisch für Arbeitsnachweis.

3.2.1 Transaktionseigenschaften

Aus den Eigenschaften der Bitcoin Transaktionen resultieren eine Reihe von Vorteilen, die sich gegenüber bisher gängigen online Bezahlsystemen ergeben.
Im Gegensatz zu gängigen online Bezahlsystemen, bei denen jede durchgeführte Transaktion mit Transaktionsgebühren behaftet ist[27], hat Bitcoin den Vorteil, geringere Transaktionskosten zu verursachen. Der Client des Bitcoin Nutzers berechnet bei der Erstellung eines Transaktionsauftrages eine Transaktionsgebühr, welche von verschiedenen Faktoren abhängig ist[28]. Diese Gebühr streichen die Nutzer ein, welche die Transaktion bestätigen.
Bitcoins lassen sich bis zu einem Bruchteil von 10^{-8} aufteilen. Diese kleinste Stückelung wird Satoshi genannt[29].
Darüber hinaus fallen auch, wie bei anderen digitalen Geld- oder Währungssystemen, Transaktionskosten für die Handhabung von physischem Geld weg.
Die online Beschaffenheit des Bitcoin Systems ermöglicht grenzüberschreitende internationale Transaktionen. Es macht keinen Unterschied, ob die Transaktion an einen Nutzer innerhalb des eigenen Staates oder einem anderen Kontinent getätigt wird.
Die Möglichkeit Transaktionen über Skripte, die nach bestimmten Regeln, wie Zeit- oder Bedingungstriggern, Transaktionen anstoßen[30] abzuwickeln, kann als weiterer Vorteil, der sich aus der völlig digitalen Beschaffenheit des Systems ergibt, genannt werden.

3.2.2 Dezentralität

Durch die Dezentralität ist Bitcoin nicht alleine von einer Instanz beeinflussbar, was beispielsweise die Steuerung der Geldmenge anbelangt. Dies wird Bitcoin oft als Vorteil zugesprochen[31].
Die Geldmenge ist im System auf 21 Millionen Bitcoins festgelegt. Durch das Bestätigen von Transaktionen werden im Schnitt alle 10 Minuten eine gewisse Anzahl an Bitcoins

[27] Vgl. PayPal 2013: PayPal: Gebühren URL: `https://www.paypal.com/de/webapps/mpp/gebuehren`, als Beispiel für ein mit Gebühren behaftetes online Bezahlsystem.
[28] Vgl. Bitcoinfees 2013: Bitcoin Transaktionsgebühren URL: `http://bitcoinfees.com/`.
[29] Vgl. Bitcoin Wiki 2013: Bitcoin - Transaction URL: `https://en.bitcoin.it/wiki/Talk:Transactions`.
[30] Vgl. Barber/Boyen/et al. 2012: How to Make Bitcoin a Better Currency.
[31] Es existiert eine Vielzahl von Quellen, welche die Dezentralität Bitcoins als größten Vorteil ansehen.

erzeugt. Diese Anzahl nimmt im Zeitverlauf ab. Alle 210.000 Blöcke[32] wird die Blockbelohnung halbiert, was aktuell im Schnitt alle vier Jahre geschieht[33]. Das erste Mal wurde die Blockbelohnung am 28.11.2012 von 50 Bitcoins auf 25 halbiert[34]. Dieser Prozess ist vom Entwurf her dem Goldschürfen nachempfunden[35], bei dem die Menge an gefundenem Gold in einer Mine im Regelfall im Zeitverlauf immer weiter abnimmt bis kein Gold mehr in der Mine gefunden wird. Aufgrund dieser Assoziation mit dem Goldschürfen erlangte das Erzeugen neuer Bitcoins, das Mining, seine Bezeichnung.
Es können durch die feste Deckelung der Menge im übertragenden Sinne keine neuen Bitcoin Vorkommen erschlossen werden oder durch geldpolitische Maßnahmen die Tauschkurse beeinflusst werden. Der Bitcoin Wert soll so geschützt werden.[36]
Die Durchführung einer Bitcoin Transaktion kann ebenfalls nicht von einer Instanz beeinflusst werden. Ist einem Bitcoin Nutzer eine Bitcoin Adresse bekannt, so kann er einen Transaktionsauftrag erstellen, der dieser Adresse Bitcoins gutschreibt, denn das Bitcoin System wird den Auftrag immer durchführen[37]. Aktuell nimmt die Organisation WikiLeaks unter anderem Spenden über Bitcoin an, da andere WikiLeaks Spendenkanäle teils von deren Anbietern wie PayPal gesperrt wurden[38].
Ausgehend von der dezentralen Organisation und online Implementierung des Bitcoin Systems ist es global über das Internet für jeden[39] nutzbar.

3.2.3 Anonymität

Im nächsten Abschnitt 3.3 wird gezeigt, dass ein Bitcoin Nutzer unter gewissen Umständen innerhalb des Bitcoin Systems identifiziert werden kann und ihm Adressen mit dazu gehörigen Transaktionen zugeordnet werden können.
Dennoch bietet Bitcoin eine gewisse grundsätzliche Anonymität bei seiner Nutzung. Dies

[32] Siehe Unterabschnitt 3.6.3.
[33] Vgl. Bitcoin Clock 2013: Bitcoin Clock URL: http://bitcoinclock.com/.
[34] Vgl. Blockchain Explorer 2012: Block 210000 URL: https://blockexplorer.com/block/000000000000048b95347e83192f69cf0366076336c639f9b7228e9ba171342e.
[35] Vgl. Friedman 2011: Bits and bob.
[36] Vgl. Nakamoto 2008: Bitcoin Proposal.
[37] Sofern die Transaktion mit einer Gebühr behaftet ist, wird sich immer ein Bitcoin Nutzer finden, welcher die Transaktion bestätigt.
[38] Vgl. Spiegel 2013: Paypal stoppt Geldfluss an WikiLeaks URL: http://www.spiegel.de/netzwelt/netzpolitik/wachsender-druck-paypal-stoppt-geldfluss-an-wikileaks-a-732856.html.
[39] Für jeden nutzbar, der Zugang zu einem PC mit Internetanschluss hat.

kann insofern als Vorteil betrachtet werden, als dass ähnlich, wie bei analogen Bezahlvorgängen zwischen zwei Parteien mit z.B. Eurobanknoten die Parteien zur Durchführung der Transaktion nicht die Identität der anderen Partei gegenüber preisgeben müssen.
Bei Spenden wird der Vorteil deutlich. Will ein Nutzer eine Spende an eine Instanz tätigen und nicht öffentlich mit dieser Spende in Verbindung stehen, so kann er dies unter Verwendung von Bitcoin tun, sofern der Spendenempfänger eine öffentliche Bitcoin Adresse bereitstellt.

Zusammenfassend erfordert das Bitcoin System geringe bis keine Transaktionskosten und eignet sich für grenzüberschreitende globale Transaktionen. Darüber hinaus ist es keiner zentralen Instanz unterworfen, welche Einfluss auf das System nehmen kann, und bietet eine gewisse Anonymität.

3.3 Anonymität

Wie bereits angedeutet ist die Anonymität, die Bitcoin seinen Nutzern bietet, aufgrund der öffentlichen Transaktionshistorie keineswegs perfekt. Die ursprüngliche Intention bei der Entwicklung des Bitcoin Protokolls bzw. vielmehr die Idee hinter der Entwicklung von Bitcoin an sich war nicht ein vollkommen anonymes Transaktionssystem zu schaffen[40].

Bei der abschließenden Beschreibung in Abschnitt 3.1 wurde Bitcoin daher auch nicht als anonymes Transaktionssystem betitelt, auch wenn es in abgestuftem Maße Anonymität bietet.
Häufig wird Bitcoin jedoch als anonyme digitale Währung betitelt[41], ohne darauf hinzuweisen, dass es sich bei dieser Anonymität vielmehr um eine Art Pseudoanonymität handelt. Daher soll nun der Untersuchungsstand zur Identifizierung von Bitcoin Nutzern dargelegt werden.

[40] Vgl. Nakamoto 2008: Bitcoin Proposal.
[41] Vgl. WikiLeaks 2013: WikiLeaks Spenden Tweet URL: `https://twitter.com/wikileaks/status/80774521350668288?_escaped_fragment_=/wikileaks/status/80774521350668288#!/wikileaks/status/80774521350668288`, als Beispiel für die Bezeichnung als anonyme Währung.

3.3.1 Analyse der Block Chain

Bitcoin Nutzer können sich eine beliebige Anzahl an Bitcoin Adressen erstellen und somit für jede Transaktion eine andere, neue Adresse verwenden. Dass diese Maßnahme nicht ausreicht, um zu gewährleisten nicht über Auswertung der Transaktionshistorie und weiterer Daten Nutzer zu identifizieren bzw. Nutzer zu gruppieren, zeigten Reid und Harrigan[42] bereits 2011.
Sie werteten die Block Chain aus und erstellten dabei zwei Graphen. Der erste Graph bildet alle Transaktionen zwischen den Bitcoin Adressen ab.
Den zweiten Graphen leiteten sie aus dem ersten ab. Er stellt Transaktionen zwischen Nutzern dar. Da ein Nutzer sich beliebig viele Adressen erzeugen kann, mussten Reid und Harrigan einem Nutzer seine Adressen zuweisen. Da eine Bitcoin Transaktion an eine Adresse aus mehreren anderen Adressen gespeist werden kann, ist es folglich so, dass alle Adressen, die durch genau eine Transaktion belastet werden, ein und demselben Nutzer gehören müssen, da nur er alle diese Adressen belasten kann.[43]
Aus diesen beiden Graphen leiteten Reid und Harrigan Informationen über die Nutzer ab. Mittels globaler und lokaler, aus den Graphen abgeleiteten Netzwerkeigenschaften, konnten sie Ausreißer identifizieren oder den Kontext, in dem sich ein Nutzer bewegt, anhand seiner Interaktionen mit anderen Nutzern feststellen[44]. Es gelang ihnen, zeitliche Analysen sowie Flussanalysen durchzuführen und somit Bitcoin Bewegungen zwischen Gruppen von Nutzern auszumachen[45].
Weiter zeigten sie auf, dass es unter Zuhilfenahme der Graphen möglich ist, mit Daten z.B von Bitcoin Faucet[46] oder freiwillig veröffentlichten Adressen auf Twitter oder Blogs ein Mapping von Bitcoin Adressen auf deren Nutzer, in Form von deren IP Adressen, durchzuführen.
Dabei weisen sie darauf hin, „[...]dass große zentralisierte Bitcoin Dienstleister dasselbe

[42] Reid/Harrigan 2011: Analysis of Bitcoin System Anonymity.
[43] Besitzt ein Nutzer z.B. eine Adresse A mit 2 Bitcoins und eine Adresse B mit 3 Bitcoins und will an Adresse C 5 Bitcoins überweisen, so erstellt der Bitcoin Client eine Transaktion, bei der C 5 Bitcoins gutgeschrieben werden, jeweils 2 aus A und 3 aus B. Betrachtet man diese Transaktion, so sieht man, dass A und B in einer Transaktion an C überwiesen haben und somit ein und demselben Nutzer gehören müssen.
[44] Vgl. Reid/Harrigan 2011: Analysis of Bitcoin System Anonymity, Seite 15.
[45] Vgl. ebd.
[46] Bitcoin Faucet 2013: Bitcoin Faucet URL: `http://freebitcoins.appspot.com/`, Die Seite Bitcoin Faucet verschenkte kleinste Bitcoin Beträge.

mit ihren Daten tun können.“[47] Große Dienstleister können dabei Bitcoin Tauschbörsen sein. Sie sind in der Lage Adressen in der Block Chain ihren eigenen Kunden zuzuordnen, wenn diese Adressen von dem Kunden mit der beim Dienstleister registierten Adresse als Input für eine Transaktion gewählt wurde.
Reid und Harrigan kommen letztlich zu dem Schluss[48], dass es mit ihrer Repräsentation der Block Chain als Netzwerkgraph möglich ist, nur durch passive Analyse viele Adressen in Verbindung zu setzen und mit externen Informationen wie IP Adressen zu verknüpfen. Einer wie auch immer gearteten aktiven Analyse wird von ihnen ein noch viel größeres Potenzial zur Informationssammlung über Nutzer zugerechnet.
Außerdem weisen sie auf Kaminsky[49] hin, welcher anmerkt, dass wenn sich ein Nutzer gleichzeitig Verbindungen zu allen Bitcoin Nutzern aufbaut und auf Transaktionensaufräge lauscht, er über längere Zeit davon ausgehen kann, dass ein Nutzer, der eine Transaktion über die Verbindung als erster weiter gibt, wohl auch deren Quelle ist.

3.3.2 Analyse der Anonymität bei Bitcoin Nutzung nur in universitärem Umfeld

Eine weitere Untersuchung, die aufzeigt wie eingeschränkt die Anonymität des Bitcoin Systems in der realen Anwendung ist, stellten Elli/Ghassan/ et al. an[50]. Sie untersuchten, wie es um die Anonymität von Bitcoin bestellt ist, wenn Bitcoins als Währung für die täglichen Transaktionen aller Personen im universitären Bereich angenommen wird.
Dazu analysierten sie nicht nur das originäre Bitcoin System, sondern konzipierten einen Simulator, welcher Transaktionen, wie sie in einem universitären Umfeld vorkommen[51], generiert.
Sie konnten damit zeigen, dass 40% der simulierten Nutzer im universitären Umfeld identifiziert werden konnten, selbst wenn sie zum Schutz der Identität für jede Transaktion eine neue Adresse generierten.[52]

[47] Reid/Harrigan 2011: Analysis of Bitcoin System Anonymity, Seite 17, aus dem Englischen „We also note that large centralized Bitcoin service providers can do the same with their user information.“
[48] Vgl. ebd.
[49] Kaminsky 2011: TCP/IP Presentation.
[50] Vgl. Androulaki/Karam/et al. 2012: User Privacy in Bitcoin.
[51] z.B. Bezahlen des Mensaessens, Aufladen des Druckkontos
[52] Vgl. Androulaki/Karam/et al. 2012: User Privacy in Bitcoin, Seite 14.

Die drei geschilderten Untersuchungen und Ansätze zeigen auf, dass es mit Clustring und anderen Netzwerkanalysetechniken sowie genügend externen Informationen, über die beispielsweise Bitcoin Tauschbörsen verfügen, zwar nicht möglich ist jeder Bitcoin Adresse einen Nutzer zuzuweisen, es aber möglich ist Nutzergruppen und Bitcoinströme zwischen Gruppen zu identifizieren.

3.4 Historie

Ein anonymes digitales Geldsystem[53] wurde bereits 1990 von Chaum, Fiat und Naor entwickelt, aufbauend auf der ersten Idee Chaums aus dem Jahre 1982[54]. Im Gegensatz zu Bitcoin braucht es jedoch eine zentrale Partei, um zu funktionieren[55].
Im Jahr 1998 wurde von Wei Dei ein verteilt arbeitendes, digitales Geldsystem[56] beschrieben. Ein System, aufbauend auf Wei Deis Beschreibung, braucht ein synchrones und nicht kompromittierbares Kommunikationssystem. Diese Anforderungen verhinderten eine praktische Umsetzung.
Nick Szabo beschreibt mit BitGold[57] ein dezentrales digitales System zum Abbilden von Besitz, welches wie Bitcoin auf einem Proof-of-Work Ansatz beruht. Dem BitGold System mangelt es unter anderem an der fehlenden Möglichkeit Besitz zu übertragen, um in der Praxis Anklang zu finden[58].

Erstmalig veröffentlicht[59] wurde die Idee für das Bitcoin System im Jahr 2008 in einem von Satoshi Nakamoto auf der Cypherpunks Mailinglist veröffentlichten Papier[60]. Die Cypherpunks Mailinglist ist eine Mailliste auf der Diskussionen rund um Kryptographie und deren Auswirkungen auf die Gesellschaft geführt werden[61]. Die Liste wird nicht vom

[53] Vgl. Chaum/Fiat/Naor 1990: Untraceable Electronic Cash.
[54] Vgl. Chaum 1982: Blind Signatures for blind payment.
[55] Siehe Double-Spending Problem in Unterabschnitt 3.6.1.
[56] Vgl. Dai 1998: B-Money Proposal URL: `http://www.weidai.com/bmoney.txt`.
[57] Vgl. Szabo 2008: Bit gold URL: `http://unenumerated.blogspot.de/2005/12/bit-gold.html`, Die BitGold Idee hat Szabo bereits früher geäußert, eine Quelle dafür ist jedoch nicht verfügbar.
[58] Vgl. Peck 2012: Bitcoin: The Cryptoanarchists' Answer to Cash URL: `http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/0`.
[59] Vgl. Nakamoto 2008: Bitcoin P2P e-cash paper URL: `http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html`.
[60] Vgl. Nakamoto 2008: Bitcoin Proposal.
[61] Vgl. Cypherpunks 2013: Cypherpunks Mailing List URL: `http://www.cypherpunks.to/list/`.

Betreiber moderiert und ist öffentlich abonnierbar.
Nutzer der Liste haben dabei seit 2001 die Möglichkeit, durch Nutzung von Re-Mailern, anonym Beiträge zu veröffentlichen[62]. Auch Satoshi Nakamoto ist nur ein Pseudonym. Die Identität des Bitcoin Systementwicklers ist unbekannt und bereits mehrfach Anlass für Spekulationen gewesen[63], vor allem auch deswegen, da sich Nakamoto im April 2011 aus der Entwicklung des Bitcoin Clients komplett zurückzog[64].
Im Januar 2009 veröffentlichte[65] Nakamoto auf Sourceforg[66] den ersten Bitcoin Client, was somit als Geburtsstunde des Bitcoin Netzwerks betrachtet werden kann.
Zwei Tage vor dieser Veröffentlichung wurde der erste Block der Block Chain angelegt[67], welcher allgemein als Genesis Block bezeichnet wird[68]. Im 170. Block findet sich die erste Bitcoin Transaktion, welche von Nakamoto an Hal Finney angewiesen worden sein soll[69].

3.5 Verbreitung und Bekanntheit

Die Verbreitung bzw. Bekanntheitssteigerung von Bitcoin verlief bisher nicht linear. Betrachtet man den Google Trend, dargestellt in Abbildung 3.1 als Indikator für das öffentliche Interesse an Bitcoin bzw. die öffentliche Wahrnehmung, so wurde Bitcoin erst ab 2011 öffentliches Interesse zuteil. Im Februar 2011 zeigt der Google Trend für Bitcoin erstmals einen Wert von Null verschieden[70]. Im Juni 2011 findet sich eine erste Spitze. Danach bleibt der Wert annähernd konstant bei etwa 5 Punkten, bevor er dann Anfang des Jahres

[62] Vgl. Cypherpunks 2013: Cypherpunks Mailing List Remailers URL: http://www.cypherpunks.to/remailers/.
[63] Vgl. Wallace 2011: The Rise and Fall of Bitcoin URL: http://www.wired.com/magazine/2011/11/mf_bitcoin/all/2013.
[64] Vgl. Davis 2011: The Crypto-Currency.
[65] Vgl. Nakamoto 2009: Bitcoin v0.1 released URL: http://www.mail-archive.com/cryptography@metzdowd.com/msg10152.html.
[66] Sourceforg ist eine Plattform, welche "[...]die führende Quelle für Open-Source Entwicklung und Verteilung"(Dice Holdings Inc.: Sourceforg About) sein möchte.
[67] Vgl. Blockchain Explorer 2009: Block 0 URL: https://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.
[68] Siehe z.B. Bitcoin Stackexchange: Block 0.
[69] Vgl. theymos 2013: Block 0 URL: http://bitcointalk.org/index.php?topic=91806.msg1012234#msg1012234.
[70] Der Wert ist auf 100 als Maximum skaliert.

2013 im April auf 90 Punkte steigt[71] und dann im November auf das aktuelle Maximum von 100 Punkten zu steigen.
Die erste reale Bitcoin Transaktion wird allgemein für das Jahr 2010 angenommen, als eine

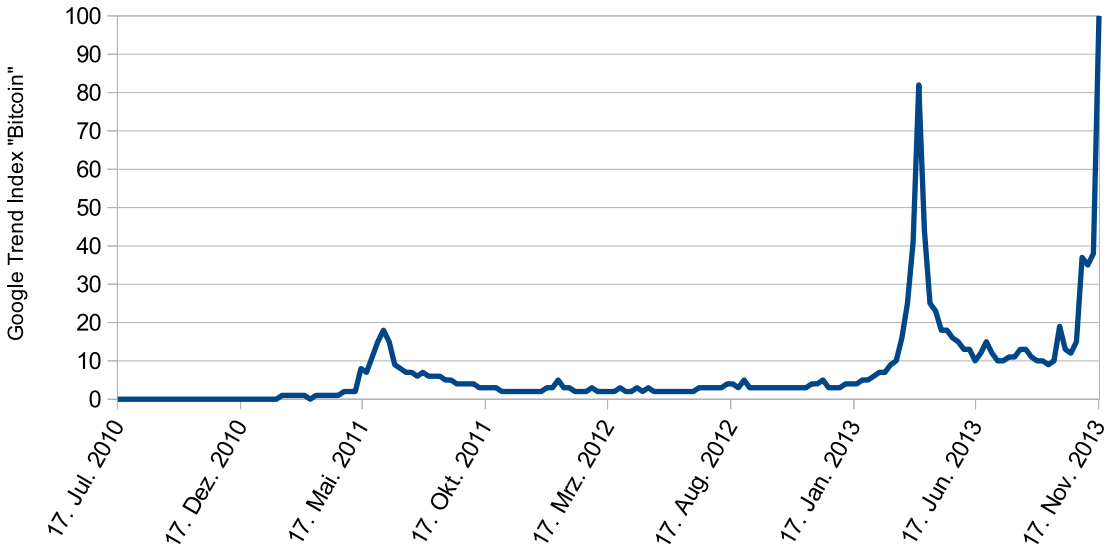

Abbildung 3.1: Google Trend für den Suchbegriff "Bitcoin", Daten von Google Inc.: Google Trend: Bitcoin

Pizza für 10000 Bitcoins erstanden worden sein soll[72]. Erste Spenden über Bitcoin nahm z.B. WikiLeaks bereits 2011 an[73]. Die Marktkapitalisierung[74] erreichte Ende März 2012 erstmals ein Volumen von einer Milliarde US-Dollar[75].

[71] Anfang des Jahres 2013 erlebte der Bitcoin Tauschkurs gegen gängige Währungen einen Hochstand, bevor der Tauschwert wieder sank.
[72] Vgl. Merchant 2013: This Pizza Cost 750.000 Dollar URL: `http://motherboard.vice.com/blog/this-pizza-is-worth-750000`.
[73] Vgl. WikiLeaks 2013: WikiLeaks Spenden Tweet URL: `https://twitter.com/wikileaks/status/80774521350668288?_escaped_fragment_=/wikileaks/status/80774521350668288#!/wikileaks/status/80774521350668288`.
[74] Die Bitcoin Marktkapitalisierung ist die Menge an bereits vorhandenen Bitcoins multipliziert mit deren Tauschwert in der entsprechenden Währung.
[75] Vgl. Qkos Services Ltd. 2013: Marktkapitalisierung URL: `http://blockchain.info/de/charts/market-cap`.

3.6 Funktionsweise

Zu Anfang dieses Kapitel 3 wurde das Bitcoin System vereinfacht vornehmlich aus Nutzerperspektive erläutert, um einen ersten Einblick in die Funktionsweise und Möglichkeiten des Systems, vor allem dessen Eigenschaften, darbieten zu können.

Dieser Abschnitt wird nun die genaue Funktionsweise[76] des Systems beleuchten. Man kann das Bitcoin System in drei verschiedene Elemente einteilen, um seine Funktionsweise anhand des Zusammenwirkens dieser Elemente zu erklären. Das erste Element sind die Nutzer, welche Transaktionen tätigen und die Bitcoins besitzen. Das zweite Element ist die Block Chain, welche die Bitcoin Transaktionshistorie abbildet und somit auch abbildet, welche Adressen wie viele Bitcoins enthalten.
Bisher noch wenig Beachtung gefunden hat das dritte Element, die Miner. Sie sind dafür zuständig, Bitcoin Transaktionen an die Block Chain anzufügen und werden dafür mit Bitcoins belohnt.
Die Block Chain verbindet als Bindeglied die Elemente der normalen Nutzer mit den Minern. Nachfolgend wird nun die genaue Funktionsweise der einzelnen Elemente erörtert.

3.6.1 Nutzer

Eine Bitcoin Adresse und die dazugehörige Zeichenfolge zum Nachweis des Besitzes der Bitcoin Adresse bilden ein Schlüsselpaar im Sinne der asymmetrischen Verschlüsselung. Die Bitcoin Adresse ist dabei der öffentliche Schlüssel (Public-Key), die Zeichenfolge zum Besitznachweis der private Schlüssel (Private-Key)[77].
Bei der asymmetrischen Verschlüsselung kann ein solches Schlüsselpaar beliebig durch eine mathematische Funktion erzeugt werden. Diese Generierung des Schlüsselpaares geschieht durch den Bitcoin Client[78] des Nutzers beim Erzeugen einer neuen Bitcoin Adresse.

[76] Gewisse Vereinfachungen in Bezug auf die kryptographischen Verfahren werden jedoch immer noch vorgenommen.
[77] Fortan werden Bitcoin Adresse und Zeichenfolge im Text nur noch mit Private-Key und Public-Key betitelt.
[78] Der Bitcoin Client ist das Bitcoin Programm, welches ein Nutzer zur Teilnahme am Bitcoin System benötigt. Es wird fortan im Text immer mit Bitcoin Client betitelt.

Wie der Name verdeutlicht, bleibt der private Schlüssel nur dem Nutzer des Schlüsselpaares bekannt. Bei Bitcoin behält der Bitcoin Nutzer seinen privaten Schlüssel geschützt in seiner Wallet, der öffentliche Schlüssel wird je nach Kontext anderen Nutzern zugänglich gemacht. Der erzeugte öffentliche Schlüssel wird dem Transaktionspartner als Bitcoin Adresse bekannt gegeben und gelangt bei einer Transaktion dann in die Block Chain.

Digitale Signatur

Das Schlüsselpaar der asymmetrischen Verschlüsselung hat dabei eine Eigenschaft, welche für das Bitcoin System genutzt wird. Mittels einer Signaturfunktion, welche den privaten Schlüssel und ein beliebiges digitales Artefakt als Argumente benötigt, ist es möglich, dieses digitale Artefakt mit dem privaten Schlüssel digital zu signieren und mit dem öffentlichen Schlüssel diese Signatur zu verifizieren.
Möchte Alice[79] ein Dokument A signieren, um z.B. nachzuweisen, dass sie es genau so erstellt hat, so tut sie dies mit ihrem privaten Schlüssel. Sendet sie das Dokument mit der Signatur nun an Bob, so kann er mit dem ihm bekannten öffentlichen Schlüssel von Alice prüfen, ob die Signatur des Dokumentes wirklich von Alice erstellt wurde und so sichergehen, dass das Dokument auch wirklich von Alice erstellt wurde.
Dabei ist es Bob nicht möglich, Rückschlüsse auf den privaten Schlüssel von Alice zu ziehen.
Übertragen auf den Bitcoin Kontext bedeutet dies, dass ein Bitcoin Nutzer mit seinem privaten Schlüssel nachweisen kann, dass er den zu diesem privaten Schlüssel gehörigen öffentlichen Schlüssel, die Bitcoin Adresse, erstellt hat und daher über die der Adresse zugeschriebenen Bitcoins verfügen kann.

Transaktion

Im Bitcoin System wird „[...]eine elektronische Münze als eine Kette von digitalen Signaturen“[80] definiert.

[79] Alice und Bob sind gängige Platzhalternamen für Nutzer in Beispielen der Kryptographie.
[80] Vgl. Nakamoto 2008: Bitcoin Proposal, aus dem Englischen „[...]an electronic coin as a chain of digital signatures.“

Eine Bitcoin Münze ist somit keine Münze im eigentlichen Sinne. Daher wird in der vorliegenden Arbeit auch von Bitcoin Guthaben gesprochen. Ein solches Guthaben zu besitzen bedeutet, den Private-Key zu einer Bitcoin Adresse[81], der ein Bitcoin Guthaben in der Transaktionshistorie gutgeschrieben ist, zu besitzen. Da der Besitz von Bitcoins somit über das Verfügen über einen Private-Key definiert ist, gibt es zwei grundsätzliche Arten eine Transaktion durchzuführen.
Erstens kann durch die Transaktion des Private-Keys an den Transaktionspartner diesem Zugang zu den Bitcoins des Private-Keys gewährt werden. Diese Transaktion wird daher auch „Transfer of keys“[82] oder „out of band transaction“[83] genannt.
Zweitens kann eine Transaktion über das Bitcoin System durchgeführt werden. Diese Art der Transaktion wird beispielsweise „transfer of balance“[84] genannt und wird nun genauer erläutert.

Wie eine Bitcoin Münze oder Guthaben den Besitzer wechselt, wird in Abbildung 3.2 dargestellt. Die abgebildeten Transaktionen werden nacheinander jeweils vom aktuellen Besitzer des Guthabens erstellt, um das Guthaben einer anderen Adresse und damit einem anderen Besitzer gutzuschreiben. Betrachtet man etwa Transaktion Zwei, so wird in dieser Transaktion dem Besitzer von Private-Key Zwei ein Bitcoin Guthaben transferiert. Will dieser nun das erhaltene Guthaben an Adresse Drei von Nutzer Drei überweisen, so erstellt er die Transaktion Drei. Dazu wird mit Hilfe einer kryptographischen Hashfunktion[85] ein Hashwert der empfangenden Adresse Drei und der Transaktion Zwei, welche Nutzer Zwei das Guthaben transferierte, gebildet. Diesen Hash signiert Nutzer Zwei mit seinem Private-Key und bestätigt somit, dass sein Guthaben an Nutzer Drei übergeht.
Ein Empfänger einer solchen Transaktion kann nun überprüfen, ob die Transaktion valide ist. Mit dem Public-Key (die belastete Adresse) kann er die Signatur der Transaktion verifizieren und so sichergehen, dass der Sender auch über diesen bei der Transaktion

[81] Die Bitcoin Adresse ist der Public-Key.
[82] Šurda 2012: Economics of Bitcoin.
[83] Christin/Brito 2012: Nicolas Christin on anonymous online market Silk Road URL: `https://cdn-surprisinglyfree.s3.amazonaws.com/SFC-125-120822.mp3`.
[84] Šurda 2012: Economics of Bitcoin.
[85] „Die Vorschrift, die einem Bitvektor einen Hashwert zuordnet, wird kryptographische Hashfunktion genannt[...]“(Küsters/Wilke: Moderne Kryptographie), der Hashwert ist dabei eine Prüfsumme von immer gleicher Länge. Es ist dabei nicht möglich, aus dem Hashwert die ihm zugrunde liegenden Daten zu konstruieren. Außerdem ist es sehr unwahrscheinlich, zwei unterschiedliche Datensätze zu finden, die den gleichen Hashwert haben. Eine kryptographische Hashfunktion ist z.B. SHA-256, welche auch bei Bitcoin genutzt wird.

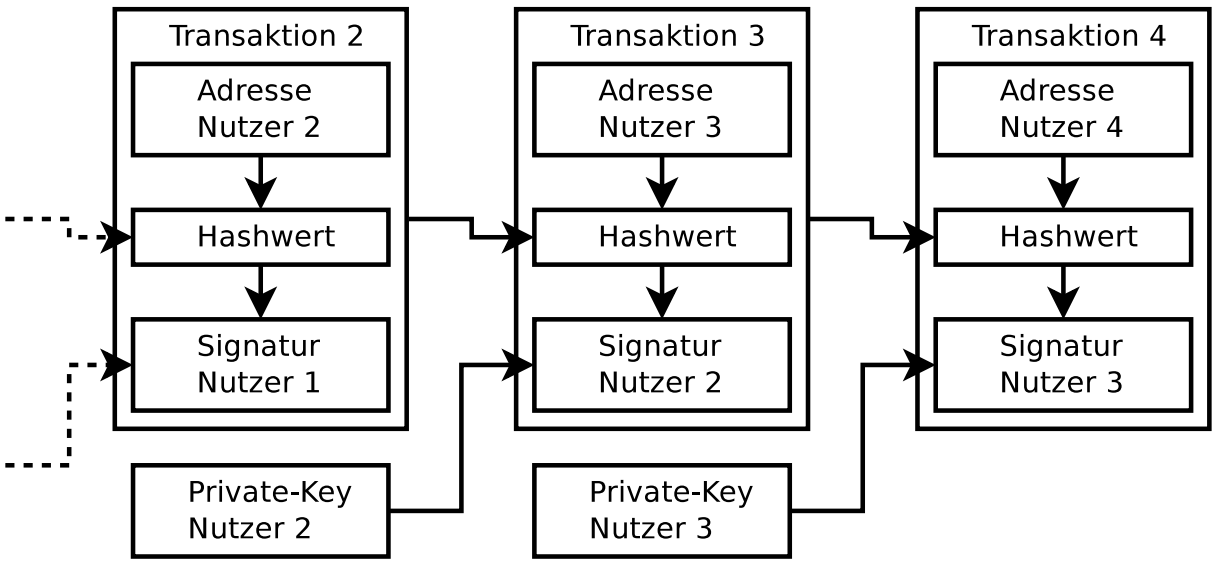

Abbildung 3.2: Bitcoin Guthaben, das durch Transaktionen den Besitzer wechselt, Abbildung in Anlehnung an Nakamoto: Bitcoin Proposal

belasteten Public-Key verfügen durfte, da er zum Erstellen der validen Signatur den Private-Key besitzen musste.

Teilen von „Münzen“ Da nicht immer ein komplettes einer Adresse zugeordnetes Guthaben transferiert werden soll oder das einer Adresse zugeordnete Guthaben nicht ausreichend für eine Transaktion ist, können Transaktionen auch mehrere sie speisende Adressen und empfangende Adressen haben[86]. Möchte ein Nutzer etwa 10 Einheiten überweisen, verfügt aber nur über jeweils zwei Adressen mit 5 Einheiten, so wird der Bitcoin Client bei einer Überweisung von 10 Einheiten die beiden Adressen mit je 5 Einheiten als Eingangs-Adressen nutzen. Dieser Aspekt spielt in Kapitel 6 eine wichtige Rolle, da aus einer Transaktion, welche mehrere Eingangs-Adressen hat, zweifelsfrei erkennbar ist, dass die Eingangs-Adressen einem Besitzer zugeordnet werden können.
Umgekehrt verhält es sich, wenn nur 5 Einheiten überwiesen werden sollen, aber nur eine Adresse mit 10 Einheiten verfügbar ist. Dann erstellt der Bitcoin Client eine Transaktion, in der 5 Einheiten der Zieladresse überwiesen werden und die restlichen 5 Einheiten wieder der sendenden Adresse gutgeschrieben werden.

[86] Vgl. Nakamoto 2008: Bitcoin Proposal.

Double-Spending Problematisch ist, dass der Empfänger einer Transaktion nicht überprüfen kann, ob der Sender die Public-Keys schon vorher belastet hat. Dieses Problem bei anonymen digitalen Geldsystemen ist unter dem Namen Double-Spending bekannt[87]. Exemplarisch wurde dieses Problem in der Vergangenheit beispielsweise bei Chaum/Fiat/Naor: Untraceable Electronic Cash dadurch gelöst, dass jede erstellte digitale Münze beim Ausgeben an ihren Emittenten zurückgegeben wurde. Dadurch ist sichergestellt, dass eine Münze nur einmal ausgegeben wird. Würde versucht werden, dieselbe Münze nochmal auszugeben, so würde der Emittent dies bemerken.

Öffentliche Transaktionshistorie Da Bitcoin ein dezentrales System ist, gibt es einen solchen zentralen Emittenten nicht. Dem mehrfachen Belasten eines Public-Keys wird bei Bitcoin dadurch begegnet, dass alle Transaktionen öffentlich[88] gemacht werden. So kann ein Empfänger die Transaktion als valide betrachten, wenn die Transaktion in die öffentliche Historie aufgenommen worden ist.
Eine öffentliche Transaktionshistorie alleine hat dabei jedoch noch eine Schwäche. Die Allgemeinheit an Nutzern muss sich einigen, welche Historie gültig ist. Beispielhaft bedeutet dies, dass wenn zwei Transaktionen gleichzeitig auftreten und einen Public-Key belasten, sichergestellt sein muss, dass in die Historie nur die erste der beiden Transaktionen aufgenommen und dass von allen Nutzern dieselbe Transaktion als erste betrachtet wird.
Dieser Vorgang des Abstimmens über die gültige Transaktionshistorie wird im dezentralen Bitcoin Peer-to-Peer Netzwerk über einen Proof-of-Work Mechanismus erreicht[89], welcher beim Anhängen von neuen Transaktionen an die Block Chain zur Anwendnung kommt und nun im nachfolgenden Unterabschnitt 3.6.2 behandelt wird.

3.6.2 Block Chain

Die Block Chain[90] stellt eine zeitliche Abfolge aller jemals im Bitcoin System durchgeführten Transaktionen dar. Die zeitliche Abfolge der Transaktionen wird durch eine Kette von Hashwerten dargestellt. Neue Transaktionen werden vom Bitcoin System, bevor sie an die Block Chain angefügt werden, zu einem Block zusammengefasst[91]. Dieser Block

[87] Vgl. Godbole/Kahate 2003: Web Technologies.
[88] Wie es auch bei Dai: B-Money Proposal der Fall ist.
[89] Vgl. Nakamoto 2008: Bitcoin Proposal.
[90] Beispielhaft in Abbildung 3.3 dargestellt.
[91] Vgl. ebd.

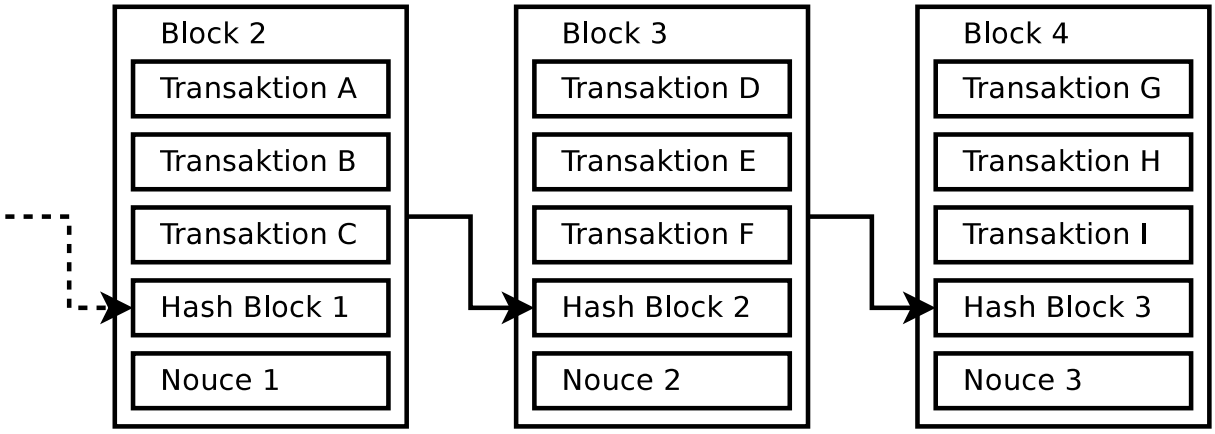

Abbildung 3.3: Vereinfachte Darstellung der Block Chain

enthält neben den neu angefallenen Transaktionen auch einen Hashwert des letzten vorher an die Block Chain angefügten Blocks. Da in jeden neuen Block durch das Einbeziehen des Hashwerts des vorhergehenden Blocks dieser vorhergehende Block miteinbezogen wird, entsteht somit zwangsläufig eine zeitliche Abfolge an Transaktionsblöcken. Darüber hinaus enthält jeder Block auch eine Nouce, deren Zweck im nächsten Abschnitt erörtert wird.
Das Erstellen eines neuen Blocks erfolgt durch die als Miner bezeichneten Teilnehmer des Bitcoin Netzwerkes. Diese Miner sind keine Nutzer im Sinne von Unterabschnitt 3.6.1, sondern nur damit beschäftigt, neue Transaktionen in valide Blöcke zu fassen und dadurch an die Block Chain anzuhängen.

Proof-of-Work

Die bisher noch nicht erklärte Nouce eines Blocks spielt bei der Erstellung neuer Blöcke eine entscheidende Rolle. Bei der Erstellung des Blocks muss die Nouce eine genaue Anforderung erfüllen. Dabei ist es schwer, eine Nouce zu finden, die für einen neuen Block die geforderte Anforderung erfüllt. Schwer meint hierbei, dass es nicht möglich ist, die Nouce zu berechnen, sondern durch Testen zufälliger Noucen die richtige gefunden werden muss.
Damit ein Block valide ist, muss sein Hashwert eine vom System festgelegte Anzahl an führenden Nullen aufweisen[92]. Um einen Block mit der geforderten Anzahl an führenden

[92] Vgl. Nakamoto 2008: Bitcoin Proposal.

Nullen zu erzeugen, muss der Block verändert werden können, um auch seinen Hashwert verändern zu können.
Ein Miner, der einen neuen Block erstellen möchte, tut dies, indem er zufällig neue Noucen für den Block generiert und von diesem Block dann samt der Nouce den Hashwert bildet. Hat er eine Nouce für den Block gefunden, die zu einem Hashwert mit genug führenden Nullen führt, so hat er damit einen validen Block erzeugt.
Dieses Finden der Anforderung genügenden Nouce wird als Proof-of-Work bezeichnet. Der Miner beweist (to proof: beweisen) mit dem Bekanntmachen der Nouce, dass er Arbeit (work: Arbeit) in Form von Rechenaufwand für das Testen vieler Noucen aufgewandt hat.
Der bei Bitcoin genutzte Proof-of-Work Mechanismus wird durch die Hashcash Funktion abgebildet. „Die Hashcash CPU Kostenfunktion errechnet einen Beweis, welcher als Ausführungsnachweis genutzt werden kann.“(Back: Hashcash). Ursprünglich wurde die Hashcash Funktion für die E-Mail Spam Bekämpfung erdacht[93].
Der Proof-of-Work Mechanismus erfüllt im Bitcoin System zwei Funktionen[94]. Er ermöglicht zum einen das gerade erläuterte Erstellen einer zeitlichen Abfolge von Transaktionen, zum anderen löst der Proof-of-Work aber auch „[...]das Problem der Festlegung auf eine Vertretung bei Mehrheitsentscheidungen “[95]. Denn hat ein Miner einen neuen Block erzeugt, so sendet er diesen wieder mittels Broadcast in das Netzwerk. Alle anderen Miner empfangen den Block und arbeiten fortan an der Erstellung eines Blocks aufbauend an dem neu erhaltenen Block. Dabei prüfen sie vorher, durch Überprüfen der führenden Nullen des Block Hashwerts, ob der neu empfange Block valide ist.

Simultane Blockerstellung

Werden zwei Blöcke folgend auf den gleichen vorherigen Block nahezu gleichzeitig erzeugt und in das Netzwerk gesendet, so kann es aufgrund des Peer-to-Peer Netzwerks dazu kommen, dass manche Miner den einen Block als ersten erhalten, andere Miner den andern Block als erstes. Die Miner arbeiten dabei immer an dem Block weiter, den sie zuerst erhalten haben, speichern aber den alternativen zweiten Block ab. Es entstehen also temporär zwei Gruppen von Minern, die unterschiedliche Historien fortführen.
Dieser Zustand wird beim Finden des nächsten Blocks aufgelöst. Erhält ein Miner einen

[93] Vgl. Back 2002: Hashcash.
[94] Vgl. Nakamoto 2008: Bitcoin Proposal.
[95] aus dem Englischen „[...]solves the problem of determining representation in majority decision making.“ (Vgl. ebd.)

weiteren Block, so verwirft er den vorherigen Block, der nicht von dem jetzt erhaltenen Block fortgesetzt wurde. So ist sichergestellt, dass sich immer nur eine Historie fortsetzt, nämlich die Block Chain, in die am meisten Rechenaufwand zum Testen von Noucen investiert wurde.

Änderung eines Blocks

Daraus folgt auch, dass wenn jemand versucht einen Block aus der Block Chain zu ändern, er den Proof-of-Work für jeden nachfolgenden Block erneut berechnen müsste, da sich die eine Änderung durch die Hashkette in allen weiteren Blocks fortsetzt. Denn nur wenn alle folgenden Blocks valide bleiben, kann die veränderte Block Chain als längste Block Chain von allen anderen Clients akzeptiert werden. Der dazu nötige Rechenaufwand ist dementsprechend hoch, was eine große Hürde gegenüber missbräuchlicher Änderung der Transaktionshistorie darstellt. Ein mögliches sich ergebendes Angriffsszenario durch Allokation von Rechenleistung wird in Kapitel 5 thematisiert.

Variable Schwierigkeit

Da dem Netzwerk nach Belieben Nutzer und auch Miner beitreten können[96], ergibt sich aus der schwankenden Rechenleistung des gesamten Systems ein Problem. Die Dauer zur Erzeugung eines neuen Blocks ist nicht konstant. Treten immer mehr Miner dem Netzwerk bei, so ist im gesamten System immer mehr Rechenleistung zum Testen einer neuen Nouce vorhanden. Die Nouce kann infolgedessen durchschnittlich schneller gefunden werden. Die Schwierigkeit der Noucen Findung wird daher im Bitcoin System je nach Rechenleistung variiert[97]. Steigt die gesamte Rechenleistung und damit die Anzahl der erzeugten Blöcke pro Stunde, so wird die Schwierigkeit beispielsweise erhöht. Dies geschieht dadurch, dass mehr führende Nullen bei dem Hashwert der neuen Blöcke gefordert werden, um einen validen Block zu erzeugen. Eine neue valide Nouce zu finden wird mit zunehmender Anzahl an führenden Nullen schwieriger[98]. Nach 2016 erzeugten Blocks wird die Schwierigkeit der Blockerstellung justiert. Dieses Justieren geschieht

[96] Vgl. Nakamoto 2008: Bitcoin Proposal.
[97] Vgl. ebd.
[98] Vgl. Back 2002: Hashcash.

zum gegenwärtigen Zeitpunkt im Schnitt alle 14 Tage[99]. Dabei wird die Schwierigkeit auf Basis der letzten 2016 Blocks so gewählt, dass alle 10 Minuten ein Block erzeugt wird.

Das Bestätigen einer Transaktion, was gleichbedeutend mit dem Erstellen eines neuen Blocks ist, läuft zusammenfassend folgendermaßen ab. Die Nutzer senden ihre Transaktionsaufträge in das Netzwerk, welche von den Minern gesammelt und zu einem Block zusammengefasst werden. Die Miner suchen nun eine Nouce für den Block, um einen validen Block zu erzeugen. Hat ein Miner eine valide Nouce gefunden, sendet er den Block ins Netzwerk und alle anderen Miner arbeiten an diesem Block weiter, sofern er valide ist und die in ihm enthaltenen Transaktionen nicht schon durchgeführt wurden.

3.6.3 Miner

Die Miner stellen die für das Anhängen an die Block Chain nötige Rechenleistung bereit. Dabei gibt es eine Reihe von Aspekten, die nun beschrieben werden. Es wird hinterfragt, welche Anreize die Miner zum Bereitstellen der Rechenleistung haben oder wie das Mining in der Praxis ausgestaltet ist.

Mining Client

Die für das Mining verwendeten Clients unterscheiden sich von den normalen Bitcoin Nutzer Clients. In den ersten Versionen des Bitcoin Clients war es auch mit diesem möglich, am Mining teilzunehmen. Mit zunehmender Größe des Bitcoin Systems und damit wachsenden Anforderungen an den Client als Mining Client, beispielsweise um auch verteiltes Mining auf mehreren Grafikkarten oder Mining im Team zu betreiben, wurden spezielle Mining Clients[100] entwickelt, die nur noch Mining Funktionalität bereitstellen und nicht mehr zum Erstellen von Transaktionsaufträgen fähig sind.

[99] Vgl. Bitcoin Clock 2013: Bitcoin Clock URL: `http://bitcoinclock.com/`.
[100] Wie etwa Kolivas: cgminer oder Luke-Jr: bfgminer.

Anreiz

Das Bereitstellen von Rechenleistung kann nicht kostenfrei geschehen. Der Miner hat Kosten für die Anschaffung der Hardware, auf welcher er das Testen der Noucen durchführt, sowie laufende Kosten in Form von Stromkosten oder auch Kühlkosten für seine Systeme. Das Bitcoin System bietet den Minern daher einen Anreiz, dafür Rechenleistung bereitzustellen[101].
Dem erfolgreichen Miner werden für jeden neuen Block durch eine spezielle Transaktion[102] in diesem Block neue Bitcoins an eine seiner Adressen gutgeschrieben. Die Anzahl an neuen Bitcoins wird dabei schrittweise reduziert. Alle 210.000 Blöcke wird die Blockbelohnung halbiert, angefangen bei 50 Bitcoins.
Die maximale Menge an Bitcoins ergibt sich aus dieser Halbierung alle 210.000 Blöcke, wie aus der Summenformel der sich ergebenden geometrischen Reihe in Gleichung 3.1 zu entnehmen ist. Die Entwicklung der Menge ist in Abbildung 3.4 dargestellt.

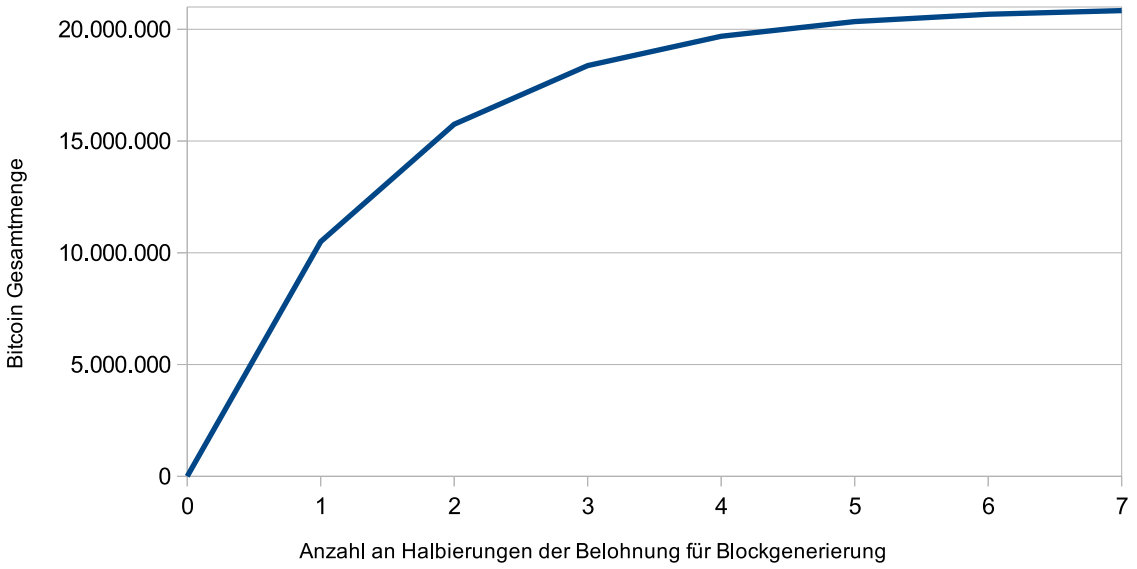

Abbildung 3.4: Entwicklung der Gesamtmenge an Bitcoins.

$$\sum_{i=0}^{\infty} 210.000 * \frac{50}{2^i} = \sum_{i=0}^{\infty} 10.500.000 * (\frac{1}{2})^i = 21.000.000 \tag{3.1}$$

[101] Vgl. Nakamoto 2008: Bitcoin Proposal.
[102] Vgl. ebd.

Gleichung 3.2 gibt die Menge an neu erzeugten Bitcoins in Abhängigkeit von der Anzahl an bisherigen Halbierungsschritten an. Man erkennt, dass schon nach siebenfacher Halbierung der Bitcoin Ausschüttungsmenge je Block nur noch Bruchteile von neuen Bitcoins generiert werden.

$$n_i = \frac{50}{2^i} \tag{3.2}$$

Die Partialsumme in Gleichung 3.3 zeigt, dass nach sieben Halbierungsschritten die erzeugte Bitcoin Menge bereits 20.917.698,75 beträgt. Mit der Annäherung an die maximalen 21 Millionen Bitcoins wird der Mining Anreiz aus der Blockberechnung somit immer kleiner bis verschwindend gering.

$$\sum_{i=0}^{n} 10.500.000 * (\frac{1}{2})^i = 21.000.000 * (1 - (\frac{1}{2})^{n+1}) \tag{3.3}$$

Es existiert aber noch ein weiterer Anreiz für die Miner, auch nach dem Erreichen der maximalen Bitcoin Menge Transaktionen zu bestätigen. Die Nutzer können bei einer Transaktion eine Transaktionsgebühr angeben. Diese Gebühr darf sich der erfolgreiche Miner gutschreiben. Die Gebühr ist allerdings nicht zwingend im Bitcoin Protokoll vorgeschrieben. Da ein Miner jedoch frei entscheiden kann, welche Transaktionen er in einen Block aufnimmt, kann eine Transaktion mit einer Gebühr den Anreiz bei ihm auslösen, die Transaktion priorisiert vor anderen Transaktionen mit weniger Transaktionsgebühr durchzuführen. Überlegungen zu möglichen Problemen bei Erreichen der Bitcoin Obergrenze für den Anreiz der Miner werden in Kapitel 5 behandelt.

Mining Hardware

Das Mining von Bitcoins erfolgte zu Beginn des Bitcoin Systems auf handelsüblichen CPUs. Mit zunehmender Größe des Netzwerks und damit verbundener Steigerung der gesamten dem System angehörenden Rechenleistung und somit auch der Schwierigkeit, einen validen Block zu erzeugen, wurde das Mining auf CPUs unrentabel.
Für die wiederholte Berechnung der Block Hashwerte mit unterschiedlichen Noucen stellten sich Grafikkarten als besser geeignet heraus. Seit 2011 werden auch sogenannte FPGA[103] Boards eingesetzt und machen zunehmend Grafikkarten zur Berechnung der

[103]FPGA: Field Programmable Gate Array (deutsch: Feld programmierbare Gatter-Anordnung).

Hashwerte unrentabel. Seit 2013[104] werden auch ASIC[105] zum Mining eingesetzt und verdrängen zunehmend andere Techniken[106].

Pooled Mining

Da das alleinige Finden eines validen Blocks bei wachsender Schwierigkeit der Blockerstellung für einen, nur über geringe Rechenleistung, in Relation zur Schwierigkeit, verfügenden, Miner sehr unwahrscheinlich ist, sind sogenannte Mining Pools entstanden[107].
In diesen Mining Pools schließen sich mehrerer Miner zusammen und suchen gemeinsam nach einem neuen validen Block. Sie teilen dazu die zu Überprüfenden möglichen Noucen auf die Mitglieder des Mining Pools auf. Findet ein Miner eine valide Nouce, so wird der entstehende Gewinn unter allen Minern, die sich an der Erstellung beteiligt haben, aufgeteilt.
Dabei gibt es unterschiedliche Ansätze den anfallenden Gewinn aufzuteilen. Durch Pool Hopping[108] kann es bei manchen Ansätzen zur Gewinnverteilung dazu kommen, dass Miner, die verschiedene Mining Pools beobachten und zu bestimmten Zeitpunkten zwischen diesen wechseln, einen höheren Gewinn zugesprochen bekommen, als Miner, die dieselbe Rechenleistung aufbringen und nur bei einem Mining Pool beteiligt waren[109].

3.7 Zusammenfassung

Kapitel 3 hat das Bitcoin System an sich erklärt. Das dezentrale digitale Transaktionssystem weist Vorteile wie geringe bis keine Transaktionskosten und Unabhängigkeit von zentralen Instanzen auf. Es ist Open-Source basiert und bietet eine gewisse Anonymität. Das Bitcoin

[104] Vgl. Zerlan 2013: ASIC Update URL: `https://forums.butterflylabs.com/announcements/692-bfl-asic-status-3.html`.
[105] ASIC:Application-Specific Integrated Circuit (deutsch: anwendungsspezifische integrierte Schaltung).
[106] Vgl. Taylor 2013: Bitcoin and The Age of Bespoke Silicon.
[107] z.B. Eclipsemc: Eclipse Mining Consortium oder BTCMine: BTC Mine
[108] „A hoppable pool is one where the attractiveness of mining, in terms of expected earnings, variance and maturity time, varies according to the pool's current state. Pool-hopping is then the exploitation of this circumstance by mining only when the attractiveness is high and leaving when the attractiveness is low."(Rosenfeld: Bitcoin Pooled Mining Reward Systems)
[109] Vgl. Rosenfeld 2011: Bitcoin Pooled Mining Reward Systems.

System folgt auf eine Reihe von publizierten möglichen digitalen Geldsystemen, welche jedoch Unterschiede zu Bitcoin aufweisen und nie weitere Verbreitung bzw. überhaupt praktische Umsetzung fanden.
Ein Nutzer sendet seine Transaktion ins Bitcoin Peer-to-Peer Netzwerk, wo sie durch eine Proof-of-Work Funktion in eine öffentliche Transaktionshistorie aufgenommen und damit gültig wird. Der zur Verhinderung des Double-Spending Problems eingesetzte Proof-of-Work wird von den Minern vollbracht, welche dafür mit Bitcoins belohnt werden.

4 Ausgestaltung und Nutzung

Nachdem in Kapitel 3 das Bitcoin System beschrieben wurde, wird das folgende Kapitel auf die Ausgestaltung des Systems in der Praxis eingehen. Vielfältige Dienste und Akzeptanzstellen von Tauschbörsen bis zur ersten Bitcoin Bank sind in den ersten vier Jahren nach seiner Inbetriebnahme entstanden und werden nun vorgestellt.

4.1 Wallet Dienste

In den vorangehenden Kapiteln wurde immer von der Nutzung des Bitcoin Systems durch einen Nutzer ausgegangen, welcher über seinen Bitcoin Client an seinem Computer handelt.
Neben dieser Nutzung, mit im Folgenden als Software Wallet bezeichneten Bitcoin Clients, gibt es jedoch noch weitere Möglichkeiten, mobil oder webbasiert das Bitcoin System zu nutzen.

4.1.1 Software Wallets

Software Wallets ermöglichen es den Nutzern, Transaktionen zu tätigen und Bitcoin Eingänge auf ihren Adressen zu verfizieren. Dabei haben die Nutzer die alleinige Kontrolle über ihre Private-Keys.

Desktop Wallets

Der ursprünglich von Satoshi Nakamoto veröffentlichte Software Bitcoin Client wird als Bitcoin-Qt Client weiterentwickelt und steht heute nicht nur wie ursprünglich für Windows, sondern auch für Linux und Mac OS zur Verfügung. „Die erstmalige Initialisierung

von Bitcoin-Qt kann einen kompletten Tag dauern“[1], da die komplette ständig durch neue Transaktionen wachsende Block Chain aus dem Bitcoin Netzwerk heruntergeladen werden muss. Zum Zeitpunkt dieser Arbeit betrug die Größe ca. 10,2 GB[2].
Dieses Laden der gesamten Block Chain stellt einen Nachteil des ursprünglichen Clients dar, welcher von anderen Clients gelöst wird. Multibit[3] ist ein Bitcoin Client, welcher nur einen Teil der Block Chain aus dem Netzwerk lädt. Nur mit den Blockheadern ist es diesen Clients möglich, Transaktionen zu verifizieren[4], ohne die ganze Block Chain zu beziehen. Andere Bitcoin Clients wie Armory[5] wollen dem Nutzer erweiterte Funktionalitäten im Umgang mit der Wallet wie Backup- und Verschlüsselungsfunktionen bieten.

Mobile Wallets

Wie für Desktop Computer gibt es auch für Smartphones Wallet Clients in Form von Apps[6]. Diese Clients laden wie der Desktop Client Multibit nur Teile der Block Chain herunter, können aber dennoch Transaktionen und deren Verifikation durchführen. Die Private-Keys bleiben dabei auch vollständig auf dem Smartphone des Nutzers.

Sicherung der Wallets

Bei Nutzung der Software Wallets, ob für Desktop Computer oder mobile Geräte, hat der Bitcoin Nutzer dabei das Risiko zu tragen, seine Wallet mit den über den Zugang zu seinen Bitcoins entscheidenden Private-Keys ausreichend zu sichern.
Geht seine Wallet durch Datenverlust oder Diebstahl[7] verloren, sind seine Bitcoins unwiderruflich für ihn verloren.
Es existieren mehrere mögliche Ansätze den Umgang mit dem Bitcoin System abzusichern[8].

[1] Vgl. Bitcoin Project 2013: Bitcoin.org Download URL: `http://bitcoin.org/de/download`.
[2] Vgl. Qkos Services Ltd. 2013: Blockchain Größe URL: `http://blockchain.info/charts/blocks-size`.
[3] Vgl. MultiBit 2013: MultiBit Bitcoin Client URL: `https://multibit.org/`.
[4] Nakamoto 2008: Bitcoin Proposal.
[5] Vgl. Armory 2013: Armory Bitcoin Client URL: `http://bitcoinarmory.com/`.
[6] z.B. die Android App "Bitcoin Wallet"von Andreas Schildbach
[7] Siehe Kapitel 5 für Verlust durch Maleware etc.
[8] Vgl. Bitcoin Project 2013: Securing your wallet URL: `http://bitcoin.org/en/secure-your-wallet`.

Verschlüsselung Die Wallet-Datei kann durch Verschlüsselung mit frei zugänglichen Verschlüsselungswerkzeugen[9] abgesichert werden. Das der Verschlüsselung zugrunde liegende Passwort muss, um einen wirksamen Schutz zu garantieren, stark[10] gewählt werden.

Aufteilen des Private-Keys Ergänzend zur Verschlüsselung kann der Private-Key in mehrere Teile zerlegt werden[11]. Nur mit allen Teilen des Schlüssels ist es dann möglich, den ganzen Schlüssel wiederherzustellen und Transaktionen zu erstellen.
Darüber hinaus werden Implementationen angedacht, welche es ermöglichen, Transaktionen von einer Adresse nur durch Involvieren mehrerer Private-Keys zu erlauben[12]. Dieses Multi Signatur Verfahren kann dann auch einen Schutz vor Diebstahl darstellen, da ein Dieb alle Private-Keys von verschiedenen Personen stehlen muss. Es erhöht aber auch die Gefahr des Verlustes. Verliert nur einer der Nutzer seinen Private-Key durch Datenverlust, sind die Bitcoins nicht mehr zugänglich.

Sicherungskopie der Wallet Die Wallet kann auf mehreren Medien gesichert werden, um das Risiko des Datenverlusts auf einem dieser Medien zu reduzieren[13].

Sichere Systeme Ein nicht von Malware oder anderen Schädlingen befallenes System schützt vor Ausspähung der Private-Keys. Selbst wenn diese durch eine der oben erörterten Maßnahmen geschützt sind, so können die Private-Keys bei Nutzung auf einem kompromittierten System ausgespäht werden.
Ein sauberes System zur Nutzung des Bitcoin Clients kann beispielhaft durch das Verwenden einer Linux Virtuellen Maschine unter Windows umgesetzt werden[14].

Wallet für tägliche Nutzung Eine weitere, oft vorgeschlagene Absicherung[15] ist eine Wallet für tägliche Transaktionen und eine Wallet zum Aufbewahren des restlichen haupt-

[9] z.B. Truecrypt
[10] Siehe z.B. Google Inc.: Starkes Passwort.
[11] Vgl. Buterin 2013: Bitcoin private key splitter URL: `https://github.com/vbuterin/btckeysplit`.
[12] Vgl. Reiner 2013: Multi-Sig Transaction Distribution URL: `https://en.bitcoin.it/wiki/BIP_0010`.
[13] Vgl. ebd.
[14] Vgl. Collier 2013: Virtual Machine for Bitcoin Users URL: `https://bitcointalk.org/index.php?topic=9937.0`.
[15] Vgl. ebd.

sächlichen Teils der eigenen Bitcoins zu erstellen.
Die Wallet für die tägliche Nutzung bleibt dabei auf dem Computer des Nutzers mit weniger Maßnahmen zu deren Sicherung, damit die Nutzbarkeit im täglichen Umgang erhalten bleibt. Die andere Wallet wird dann mit den beschriebenen Maßnahmen seperat davon gesichert und befindet sich nicht auf einem aktiv genutzten Computer und wird nur im Bedarfsfall auf einen solchen kopiert.

4.1.2 Web Wallets

Ein Bitcoin Nutzer kann die Verwaltung seiner Wallet auch einem Internetdienst übertragen und nicht mehr nur über seine eigenen Software Wallet abwickeln.
Diese Web Wallets bieten dem Nutzer den Vorteil, dass alle Dienste des Anbieters über ein Webinterface zugänglich sind, somit unabhängig von Ort und Gerät Zugriff auf diese Wallet Dienste, wie Transaktionsdurchführung, möglich ist. Erste Anbieter von Web Wallets speicherten dabei den Private-Key des Nutzers ab. Nach einer Reihe von Diebstählen von Bitcoins bei solchen Diensten sind auch Web Wallet-Anbieter auf den Markt getreten, welche nur über verschlüsselte Private-Keys verfügen und der Nutzer immer noch über seine Private-Keys alleine verfügt[16].

4.2 Finanzdienste

Bitcoins werden dezentral emittiert. Schon zu Beginn des Bitcoin Systems existierten daher bereits Wechselkurse[17]. Die Etablierung von Tauschbörsen war infolgedessen ein logischer Schritt. Neben Tauschbörsen entwickeln sich weitere Dienste rund um das Bitcoin System, welche Finanzdienste, wie das bequeme Verwalten der Wallet[18] oder andere gängigen Banken ähnelnde Dienstleistungen, versprechen.

[16] Vgl. Bitcoin Wiki 2013: Browser-based wallet URL: `https://en.bitcoin.it/wiki/EWallet`.
[17] Siehe nächsten Abschnitt.
[18] Siehe Unterabschnitt 4.1.1.

4.2.1 Tauschbörsen

Um an Bitcoins zu gelangen, hat ein Nutzer drei Möglichkeiten. Er nimmt am Mining-Prozess teil und generiert neue Bitcoins, er bietet Waren oder Dienste gegen Zahlung von Bitcoins an, oder er tauscht gängige Währungen auf einer Tauschbörse gegen Bitcoins.
In den Anfangszeit dominierte das Mining als Bitcoin Quelle, da für einen Nutzer mit herkömmlichen CPUs noch wirtschaftlich die Möglichkeit bestand, Bitcoins zu erzeugen. Der erste bekannte Bitcoin/Dollar Wechselkurs[19] stammt aus dem Jahr 2009 und wurde aufgrund der Elektrizitätspreise in den USA und der Anzahl an erzeugten Bitcoins pro 30 Tage berechnet. Mittlerweile gibt es eine Vielzahl von Tauschbörsen wie Mr.Gotex, Bitcoin Central oder bitcoin.de.
BTC China ist zum aktuellen Zeitpunkt mit etwa einer Million getauschten Bitcoins in 30 Tagen die weltweit größte Tauschbörse für Bitcoins[20].
Bitcoin Central ist die erste Tauschbörse, welche eine Partnerschaft mit einer Bank eingehen konnte[21].

Ablauf eines Tausches

Exemplarisch für einen Ablauf eines Tausches von Bitcoins gegen eine gängige Währung an einer der Bitcoin Tauschbörsen werden nun die nötigen Schritte zur Durchführung eines Tausches bei der Tauschbörse bitcoin.de[22] beschrieben. Die dazu nötigen Schritte sind grundsätzlich bei allen anderen genannten Tauschbörsen ähnlich, nur deren Umsetzung von Börse zu Börse ist jeweils anders ausgestaltet.

Registrierung Zur Nutzung der Tauschbörse muss sich ein Bitcoin Nutzer zuerst bei dieser registrieren. Dazu sind die Angaben über sein Geschlecht, Vornamen, Nachname, vollständige Adresse, Geburtsdatum, Geburtsort sowie eine seiner E-Mail Adressen und ein Passwort nötig. Im Anschluss muss er über einen an seine E-Mail Adresse zugesendeten Link diese E-Mail Adresse bestätigen.

[19] Vgl. New Liberty Standard 2009: 2009 Exchange Rate URL: `http://newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate`.
[20] Vgl. Bitcoincharts 2013: Browser-based wallet URL: `http://bitcoincharts.com/markets/`.
[21] Vgl. Paymium 2013: Bitcoin Central Webseite URL: `https://bitcoin-central.net/`.
[22] Vgl. Flaskämper 2013: Bitcoin-Marktplatz: bitcoin.de URL: `https://www.bitcoin.de/de`.

Verifizierung Anschließend wird der Nutzer aufgefordert seine Mobiltelefonnummer anzugeben. Er erhält an diese einen Code geschickt, welchen er im Portal zur Verifizierung der Nummer angeben muss. Auch sein Bankkonto muss der Nutzer vor dem ersten Tausch verifizieren. Dazu nutzt bitcoin.de den Dienstleister sofortüberweisung.de. Gegenüber diesem Dienstleister gibt der Nutzer seine Bankdaten samt PIN für seinen online Banking Zugang bei seiner Bank an. Der Dienstleister führt dann eine Überweisung über wenige Eurocent über den online Banking Zugang des Nutzers an Bitcoin.de durch, um den Zugang des Nutzers zu dem Bankkonto zu verifizieren. Dazu wird der Nutzer je nach Bankinstitut beispielsweise auch dazu aufgefordert, die für die Überweisung nötige TAN anzugeben.

Tauschangebot Nach der Registrierung und Verifizierung kann der Nutzer tauschen. Will er Bitcoins gegen eine gängige Währung erhalten, so sucht er aus einer Liste von aktuell verfügbaren Tauschofferten ein ihm passendes Angebot aus. Eine Tauschofferte besteht immer aus der Anzahl der offerierten Bitcoins und Angaben über den Tauschpartner, bestehend aus dessen Identifikationsstatus[23] und Heimatland. Den Tauschkurs für die Tauschofferte legt dabei der einstellende Nutzer fest, orientiert sich aber an den bei der Tauschbörse angegeben Kursen.

Tausch Hat sich der Nutzer für ein Tauschangebot entschieden und eines ausgewählt, so werden ihm die Bankdaten des Tauschpartners mitgeteilt und er überweist den fälligen Tauschbetrag auf dieses Konto. Der Tauschpartner muss im Gegenzug die zu tauschenden Bitcoins auf eine Adresse überweisen, die bitcoin.de verwaltet. Bestätigt er dann, dass er das Geld auf seinem Konto erhalten hat, werden die Bitcoins von bitcoin.de dem Tauschpartner gutgeschrieben. Er kann sich nun diese Bitcoins im bitcoin.de Portal auf eine beliebige Bitcoin Adresse überweisen lassen oder sie bei bitcoin.de belassen.

[23] Ein Nutzer kann seine Identität über das Post Identverfahren gegenüber bitcoin.de verifizieren. Dadurch wird bei seinen Tauschofferten allen möglichen Tauschpartnern gegenüber ausgewiesen, dass der Nutzer gegenüber bitcoin.de authentifiziert ist.

4.2.2 Geldautomat

Der Tausch von gängigen Fiatwährungen in Bitcoins kann ebenfalls durch einen Bitcoin Geldautomat erfolgen[24]. Der Nutzer erstellt einen QR-Code seiner Adresse und lässt den Automaten diesen einscannen. Er zahlt den zu tauschenden Betrag in dem Automaten ein, und die entsprechende Anzahl an Bitcoins wird an seine Adresse transferiert.

4.2.3 Bitcoin Bank

Flexcoin nennt sich selbst die weltweit erste Bitcoin Bank, wobei diese Aussage von Flexcoin selbst auf ihrer Internetseite relativiert wird „Wir sind keine richtige Bank, die US Dollar oder andere nationale Währungen akzeptiert[...]“[25].
Flexcoins angebotene Dienstleistungen[26], die vornehmlich versuchen Schwierigkeiten zu lösen, die die Dezentralität von Bitcoin mit sich bringt, ähneln jedoch teils denen wirklicher Banken.
Flexcoin bietet seinen Kunden Zugriff auf die Verwaltung ihrer bei Flexcoin hinterlegten Bitcoin Guthaben von mehreren Geräten, wie PCs oder Smartphones. Überweisungen zwischen Flexcoin Konten werden direkt bestätigt, sind transaktionskostenfrei und bedürfen keiner Bestätigungswartezeit wie im originären Bitcoin System. Die Bitcoin Adressen können bei Flexcoinüberweisungen mit vorher festgelegten natürlichsprachlichen Pseudonymen adressiert werden. In Zukunft will Flexcoin des Weiteren Bitcoin Zahlungen reversibel machen, sodass irrtümliche Überweisungen zwischen Flexcoin Konten rückgängig gemacht werden können.
Was Flexcoin von anderen Web Wallet Anbietern aus Unterabschnitt 4.1.2 unterscheidet, ist, dass Flexcoin einen so genannten monatlich gewährten Discount auf hinterlegtes Guthaben gewährt[27]. Dieser Discount kann als eine Art Verzinsung des Bitcoin Guthabens betrachtet werden[28].

[24] Vgl. Kannenberg 2013: Erster Bitcoin-Geldautomat URL: `http://www.heise.de/newsticker/meldung/Erster-Bitcoin-Geldautomat-in-den-USA-ausgeliefert-1954415.html`.
[25] Vgl. Flexicon Bank 2013: Flexcoin the bitcoin bank URL: `http://www.flexcoin.com/`, aus dem Englischen „We are not a true bank that accepts USD or any national currency, only bitcoins“.
[26] Vgl. Flexicon Bank 2013: Flexcoin the bitcoin bank URL: `http://www.flexcoin.com/103.html`.
[27] Vgl. ebd.
[28] Vgl. Bitcoin Stackexchange 2011: Bitcoin bank with deposit URL: `http://bitcoin.stackexchange.com/questions/1426/is-there-a-bitcoin-bank-which-gives-interest-on-my-deposit`.

4.3 Physische Bitcoins

Bitcoins völlige digitale Umsetzung lässt sich, bei ausreichendem Vertrauen in die dazu eingesetzte Technik und Hersteller, teilweise aushebeln und Bitcoins auch in physischer Form abbilden.

4.3.1 Münzen

Casascius Coins[29] sind eine physische Umsetzung der Bitcoins. Auf der Seite des Herstellers können Bitcoin Münzen mit einem Bitcoin Wert von 1 oder 0,5 oder 0,1 Bitcoin erworben werden. Die Münzen bestehen dabei aus Silber. Unter einem auf die Münze aufgebrachten Hologramm befindet sich ein Private-Key, der zu einer Bitcoin Adresse mit dem jeweiligen Wert der Münze gehört.
Der Public-Key ist außen auf der Münze abgebildet. Das Hologramm soll dabei verhindern, dass niemand unbemerkt den Private-Key der Münze auslesen und die Bitcoins transferieren kann. Das Hologramm wird beim Ablösen beschädigt, sodass für jeden sichtbar ist, dass die Münze entwertet wurde.
Solange das Hologramm intakt ist, kann die Münze zum physischen Austausch von Bitcoins genutzt werden. Beim Besitzwechsel der Münze wird der Private-Key weitergegeben und der neue Besitzer kann über die Bitcoins, die dem Public-Key der Münze zugeschrieben sind, verfügen, indem er den Private-Key unter dem Hologramm ausliest oder die Münze wiederum weitergibt. Da der Public-Key auf der Münze aufgedruckt ist, kann über Internet-Seiten wie z.B. von Blockexplorer überprüft werden, ob die Münze noch ihren Wert hat.
Die Nutzung der Münze setzt jedoch voraus, dass das Hologramm sicher vor unbemerktem Auslösen schützt und dass der Hersteller der Münze die Private-Keys nicht gespeichert und in Zukunft die Münze nicht entwertet.

4.3.2 Geldscheine

Analog zu den Casascius Coins setzt Bitbills dasselbe Prinzip des verdeckten Private-Keys für die Umsetzung von Bitcoins als eine Art Geldschein[30] ein. Der Private-Key wird vom

[29] Vgl. Caldwell 2013: Physical Bitcoins by Casascius URL: `https://www.casascius.com/`.
[30] Vgl. Bitbills Inc. 2013: Bitbills FAQ URL: `http://bitbills.com/faq`.

Hersteller der Bitbills mit einen QR-Code dargestellt und zwischen zwei Schichten einer Plastikkarte vom Format einer üblichen Kreditkarte eingefügt. Der Public-Key befindet sich wieder auf der Außenseite der Karte. Vertrauen in den Hersteller, die Private-Keys nicht gespeichert zu haben, sowie in die Sicherheit des Ausleseschutzes des Private-Keys in Form des QR-Codes innerhalb der Karte, werden für die Nutzung der Bitbills vorausgesetzt.
Es existieren darüber hinaus viele weitere Anbieter von physischen Bitcoins. Bitcoin Paper Wallet[31] ermöglicht beispielsweise das eigenhändige Herstellen von physischen Bitcoins.

Grundlegend handelt es sich bei den gerade beschriebenen physischen Bitcoins um Ausprägungen des in Abschnitt 3.6.1 beschriebenen Transfer of Keys Prinzips. Der Private-Key wird übermittelt, ohne dass der Sender ihn nach dem Transfer noch kennt.

4.4 Waren und Dienstleistungen

Neben den sich mit dem Beziehen und Verwalten von Bitcoins befassenden Diensten akzeptieren auch Anbieter von Waren und Dienstleistungen Bitcoins als Zahlungsmittel. Bitcoin Akzeptanzstellen lassen sich über verschiedene Listen[32] ausfindig machen.
Nicht nur im Internet können Bitcoins als Zahlungsmittel verwendet werden, in Berlin Kreuzberg und Neu Köln haben sich mehrere Geschäfte und Gaststätten dazu entschieden Bitcoins zu akzeptieren[33].

4.4.1 Drogenhandel

Neben einer Vielzahl an legalen Dienstleistungs- und Warenangeboten gegen Bitcoins hat jedoch besonders eine Akzeptanzstelle von Bitcoins Aufmerksamkeit erregt. Im Juni 2011

[31] Vgl. Becker 2013: Bitcoin paper wallet URL: `https://bitcoinpaperwallet.com/`.
[32] Siehe etwa BitcoinIT: Handel oder Spend Bitcoins: Places to Spend Bitcoins.
[33] Vgl. Eckert 2013: Wie Berlin zur weltweiten Bitcoin-Hauptstadt wurde URL: `http://www.welt.de/finanzen/geldanlage/article119820142/Wie-Berlin-zur-weltweiten-Bitcoin-Hauptstadt-wurde.html`.

berichtete Adrian Chen[34] über den online Drogenmarktplatz Silk Road.
Auf Silk Road konnten verschiedenste Drogen gegen Bitcoins erworben werden, welche dann per Post zugestellt wurden. Die Seite zu dem Silk Road Marktplatz ließ sich dabei nur über das Anonymisierungs-Netzwerk TOR aufrufen. Käufer der illegalen Substanzen waren so nicht identifizierbar. Mit Hilfe eines Bewertungssystems wurden Verkäufer des Marktplatzes bewertet. Diesen Verkäufern gegenüber gaben die Käufer ihre Postanschrift preis.
Von Januar 2011 bis September 2013[35] wurde der Marktplatz betrieben, bis es amerikanischen Behörden gelang den Betreiber über ein Posting in einem Forum zu ermitteln[36].

4.4.2 Glücksspiel

Auch Glücksspiel kann mit Bitcoins betrieben werden. Ein Vertreter für Bitcoin Glücksspiel ist Satoshi Dice[37]. Satoshi Dice wirbt mit der Aussagen enorme Mengen an Bitcoin Gewinnen seien möglich. Zur Teilnahme an dem Dienst ist keine Registrierung nötig.

4.5 Mixer

Ein weiterer auf dem Bitcoin System aufbauender Dienst ist ein sogenannte Mixer.
Mixer-Dienste versprechen ihren Nutzern gegen eine Gebühr Transaktionen an angegebene Empfängeradressen zu verschleiern, sodass aus der Block Chain nicht mehr ablesbar ist, dass der Nutzer an den Empfänger eine Transaktion durchgeführt hat.
Zu diesem Zweck muss der Nutzer Guthaben an den Mixer-Dienst senden, welcher dann die Transaktion über Umwege an den Empfänger leitet.

[34] Vgl. Chen 2011: The Underground Website Where You Can Buy Any Drug Imaginable URL: http://kotaku.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.
[35] Vgl. Maas 2013: Anklageschrift Silk Road.
[36] Vgl. Eikenberg 2013: Silk Road: ausgeschaltet URL: http://www.heise.de/security/meldung/Silk-Road-FBI-schaltet-Drogen-Handelsplattform-im-Tor-Netz-aus-1972026.html.
[37] Vgl. Chen 2011: The Underground Website Where You Can Buy Any Drug Imaginable URL: http://kotaku.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.

Der Nutzer solcher Dienste muss dabei dem Mixer-Dienst vertrauen, das ihm anvertraute Guthaben dem Empfänger auch zu transferieren. Darüber hinaus legen die Mixer-Dienste wie BitLaundry oder Bitcoinfog nicht offen wie genau die Verschleierung der Transaktion vorgenommen wird, sodass sich der Nutzer nicht direkt eine Meinung über die Wirksamkeit des Dienstes bilden kann, beispielhaft in Abbildung 3.3 dargestellt.

4.6 Zusammenfassung

Kapitel 4 hat die Ausgestaltungen des Bitcoin Systems und seine praktische Nutzung geschildert.
Neben den originären Software Wallets für Computer kann der Bitcoin Nutzer auch auf seinem mobilen Endgerät oder im Web seine Wallet verwalten und Transaktionen tätigen. Es existieren Bitcoin Finanzdienste im weiteren Sinne wie Tauschbörsen, die es ermöglichen, Bitcoins in gängige Währungen und vice versa zu tauschen oder auch erste Bitcoin-Geldautomaten, die ebenfalls den Tausch von gängigen Währungen gegen Bitcoins ermöglichen. Erste Ansätze klassische Bankdienstleistungen für Bitcoin zu realisieren wurden ebenfalls thematsiert.
Bitcoins können auch unter gewissen Rahmenbedingungen in physischer Form genutzt werden. Etwa als Münze, in die durch ein Hologramm der Private-Key geschützt eingebracht ist oder als eine Art Geldschein, bei dem der Private-Key in einer Plastikkarte im Format einer EC-Karte geschützt eingebracht ist.
Eine Vielzahl von Akzeptanzstellen von Bitcoins sind seit der Veröffentlichung des Systems im Internet entstanden, sodass verschiedenste Waren und Dienstleistungen mit Bitcoins bezahlt werden können. In Berlin Kreuzberg und Neu Köln akzeptieren einige Geschäfte und Lokale bereits Bitcoins.
Auf dem Marktplatz Silk Road konnten bis September 2013 Drogen und andere illegale Substanzen erworben werden, und auch Glücksspiel ist mit Bitcoins bei Anbietern wie Satoshi Dice möglich.

Der Vollständigkeit halber sei an dieser Stelle erwähnt, dass bei der Auseinandersetzung mit Bitcoin auch rechtliche Fragestellungen eine Rolle spielen, als auch ökonomische

Überlegungen, ob Bitcoin Geld und/oder Währung ist, interessieren. Diese Aspekte spielen für das Verständnis und die Motivation hinter der im letzten Kapitel vorgestellten Transaktionsüberwachung jedoch keine Rolle und werden somit hier auch nicht näher erläutert.

Teil II

Probleme des Systems

5 Herausforderungen

Den Vorteilen des Bitcoin Systems stehen Probleme und Herausforderungen gegenüber, welche nun erläutert werden und einen kritischen Blick auf das System werfen.

5.1 Systemverwundbarkeit

Bitcoin beruht auf einem System, welches über ein Peer-to-Peer Netzwerk realisiert worden ist. Normale Bitcoin Clients und Mining Clients schließen sich über das Netzwerk zusammen.
Dabei ist das Bitcoin Protokoll nicht fehlerfrei. Mit dem Update des Clients auf Version 0.8.0 kam es zu einer sogenannten Chain Fork[1], das heißt einer zwischenzeitlichen dauerhaften Koexistenz von zwei unterschiedlichen Block Chains. Es wurden dadurch zwischenzeitlich zwei Block Chains weiter fortgesetzt, sodass Bitcoins doppelt, jeweils einmal in jeder Block Chain, hätten ausgegeben werden können. Das Problem wurde durch den Aufruf der Bitcoin Client Entwickler an die Miner, die neue Version des Clients nicht zu benutzten und erst auf ein Update zu warten, gelöst. Dieser Chain Fork zeigt auch einen weiteren prinzipiellen Schwachpunkt des Systems auf.
Bitcoin ist ein dezentral arbeitendes System. Die Weiterentwicklung des ursprünglichen Bitcoin Clients wird jedoch von einer zentralen Instanz, der Bitcoin Foundation, übernommen[2]. Auch wenn der Quelltext dieses Hauptclients offen liegt und somit von jedem prinzipiell geprüft werden kann, so kann der zentrale Entwicklerkreis, wie an dem Chain Fork Zwischenfall gesehen, Einfluss auf die Nutzung des Systems haben. Somit kann argumentiert werden, dass das Bitcoin System nicht völlig dezentral ist,

[1] Vgl. Bitcoin Org 2013: Chain Fork Information URL: `http://bitcoin.org/chainfork.html`.
[2] Vgl. Bitcoin Foundation 2013: Bitcoin Foundation: About URL: `https://bitcoinfoundation.org/about/`.

sondern durch diese zentrale Weiterentwicklung eine Art zentrale Einflussinstanz besteht, auch wenn deren Einflussnahme durch den offenen Quelltext allgemein kontrolliert wird.

5.2 Kursschwankungen

Der Bitcoin Tauschkurs hat seit der Einführung des Bitcoin Systems schon mehrere Hochphasen mit anschließendem Kursverfall erlebt. Bis zum aktuellen Zeitpunkt ist der Tauschkurs gegenüber gängigen Währungen jedoch tendenziell sehr stark gestiegen. Von anfänglichen Centbeträgen liegt der Dollartauschkurs, wie Abbildung 5.1 zu entnehmen ist, aktuell bei über 500 Dollar.

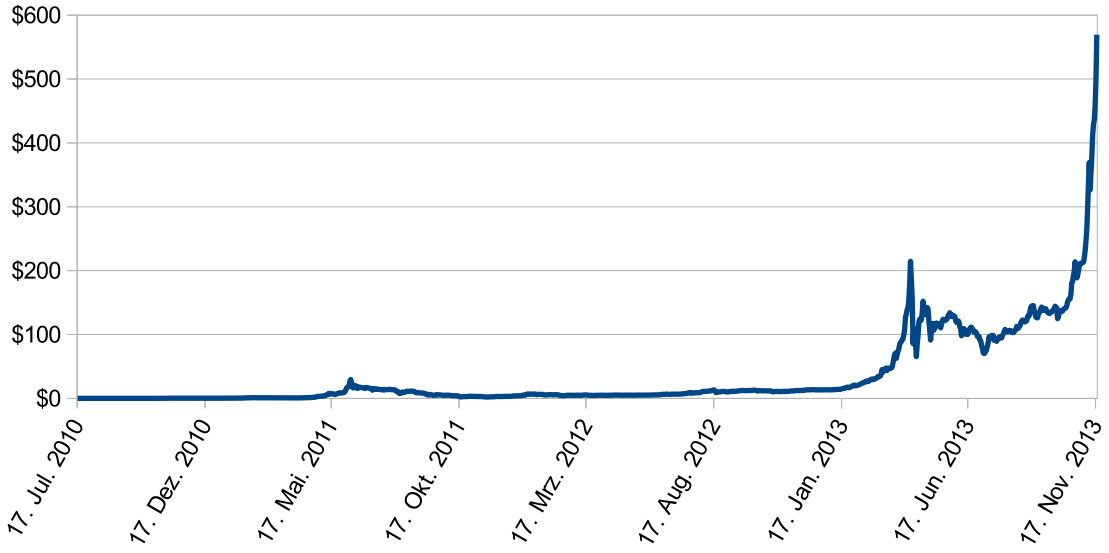

Abbildung 5.1: Dollartauschkurs gegenüber Bitcoin an der Tauschbörse MtGox, Daten von Bitcoin Charts: MtGox exchange rate Dollar/Bitcoin

Das Horten von und Spekulieren mit Bitcoin Guthaben kann aufgrund der starken Kursentwicklung als weiteres Problem des Bitcoin Systems angesehen werden. Die Kursentwicklung lässt vermuten, dass viele Bitcoin Guthaben nur aufgrund von Aussicht auf Spekulationsgewinne gehalten werden und nicht, um damit Zahlungen vorzunehmen. Damit verbunden ist ein weiteres mögliches Problem für den Tauschkurs, welches durch

die Konzentration großer, in Relation zur Bitcoin Obergrenze, Bitcoin Guthaben entsteht. Untersuchungen der Block Chain[3] lassen vermuten, dass eine Instanz, welche von Beginn des Bitcoin Systems an am Mining beteiligt war, im frühen Zeitraum des Systems ein Bitcoin Guthaben von etwa einer Million Bitcoins angehäuft hat. Dieses Guthaben ist bis zum aktuellen Zeitpunkt nicht transferiert worden. Diese eine Million Bitcoins machen etwa 5% des gesamten jemals verfügbaren Bitcoin Guthabens aus und zum aktuellen Zeitpunkt sogar etwa 8%[4]. Wird dieses gesamte Guthaben zu einem Zeitpunkt auf den Tauschmarkt gebracht, hätte dies große Auswirkungen auf die Kursentwicklung.
Durch DDoS[5] Angriffe auf große Bitcoin Tauschbörsen wie BTCChina[6] oder MtGox[7] wird versucht, Einfluss auf die Kursentwicklung zu nehmen. Die Angriffe auf die Börsen haben das Ziel die Erreichbarkeit der Börsen für deren Nutzer zeitweise zu verhindern. Es lässt sich vermuten, dass die Absicht der Angreifer hinter diesen Angriffen ist, die Nutzer der Tauschbörsen zu verunsichern, sodass diese vermehrt ihre Bitcoin Guthaben verkaufen. Infolgedessen würde sich der Bitcoinkurs verändern und diese vorhersehbare Veränderung dann von den Angreifern ausgenutzt werden.

Der Bitcoin Tauschkurs unterliegt demnach dem Risiko von starken Kursschwankungen.

5.3 Komplexität

Ein Nutzer, der die Risiken der Nutzung des Systems für sich persönlich bewerten möchte, hat einen hohen Aufwand das dafür relevante Wissen zu erlangen. Das System ist in seiner Gesamtheit sehr komplex und daher für einen unerfahrenen Nutzer schwer durchschaubar. Eine Nutzung nach persönlicher Risikoabwägung ist daher nur nach eingehender Befassung mit dem System möglich.

[3] Vgl. Lerner 2013: The Well Deserved Fortune of Satoshi Nakamoto URL: `https://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/`.
[4] Aktuell sind bereits etwa 12 Millionen Bitcoins erzeugt worden.
[5] DDoS: Distributed denial of service attack
[6] Vgl. Leyden 2011: DDoS Bitcoin exchange BTCChina URL: `http://www.theregister.co.uk/2013/10/17/bitcoin_exchange_ddos_flood/`.
[7] Vgl. Sharwood 2011: DDoS Bitcoin exchange MtGox URL: `http://www.theregister.co.uk/2013/04/22/mtgox_ddos/`.

Problematisch ist in diesem Zusammenhang schon etwa die in Abschnitt 4.1.1 thematisierte Sicherung der Wallet. Nur mit ausreichend Wissen ist es möglich, die Wallet ausreichend vor Verlust zu schützen. Einer weiten Verbreitung von Bitcoin in seiner originären Ausgestaltung steht seine Komplexität in der Nutzung gegenüber.

5.4 Ökologische Bedenken

Der für das Funktionieren des Bitcoin Systems essenzielle Proof-of-Work verlangt Rechenleistung. Die Rechenleistung des Bitcoin Systems, gemessen in Hashes pro Sekunde, hat sich dabei seit März 2013 bis zum aktuellen Zeitpunkt November 2013 mehr als verhundertfacht[8]. Das Aufbringen dieser Leistung geht einher mit wachsendem Energieverbrauch und Umweltbelastung. Eine Kalkulation[9] geht davon aus, dass ein sicheres, auf einem Proof-of-Work basierendes Transaktionssystem, sofern es die gleiche Anzahl an Transaktionen wie das bestehende weltweite elektronische Bankentransaktionssystem abwickeln soll, einen ökologischen Fingerabdruck in der Größenordnung des weltweiten Flugverkehrs verursachen würde. Diese Umweltbelastung kann als weiterer Nachteil des Systems angesehen werden.

5.5 Rechtlicher Status

Bitcoin als online System ist nicht an Staatsgrenzen gebunden. Es ist keinem staatlichen Gebiet alleine zuzuordnen und wird weltweit genutzt. Bitcoin als Zahlungsmittel steht dabei in vielen Ländern unter staatlicher Beobachtung, da Bitcoin prinzipiell etwa als Konkurrenz zu staatlich deklarierten Währungen aufgefasst werden kann. Jedoch hat Thailand als bisher einziger Staat Bitcoin verboten[10]. Der rechtliche Status von Bitcoin bleibt dabei in weiteren Staaten bisher nicht grundsätzlich geregelt. Daraus ergibt sich eine Rechtsunsicherheit hinsichtlich der grundsätzlichen Nutzung von Bitcoin. Druch Rechtsunsicherheit

[8] Vgl. Bitcoin Co Ltd. 2013: Trading suspended due to Bank of Thailand advisement URL: `https://bitcoin.co.th/trading-suspended-due-to-bank-of-thailand-advisement/`.

[9] Vgl. Breuker/Heide/et al. 2012: Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency.

[10] Vgl. Bitcoin Co Ltd. 2013: Trading suspended due to Bank of Thailand advisement URL: `https://bitcoin.co.th/trading-suspended-due-to-bank-of-thailand-advisement/`.

können für Bitcoin Nutzer Transaktionskosten in Form von Informationssuchkosten entstehen. Auch kann nicht ausgeschlossen werden, dass von weiteren Staaten versucht wird, Bitcoin zu verbieten oder zu regulieren.

5.6 Kriminalität

Ein weiterer Grund für ein Verbot oder Regulation von Bitcoin könnte die Vereinfachung bzw. Ermöglichung von kriminellen Geschäften durch das Bitcoin System sein. Unterabschnitt 4.4.1 beschrieb den Drogenmarktplatz Silk Road, welcher nur durch die Nutzung von Bitcoins in seiner Art existieren konnte.
Die australische Regierung geht etwa davon aus, dass

> „The anonymous nature of digital currencies may appeal to criminal groups and individuals who seek to use digital currencies as an instrument of crime to pay for illegal goods and services and obscure the source of illicit funds or evade tax.“(Australian Government: Austrac typologies and case studies report 2012)

In den USA forderte[11] ein Abgeordneter des US-Senats bereits 2011 Bezug nehmend auf Silk Road, Bitcoin in den USA zu verbieten.

5.7 Zusammenfassung

Das Bitcoin System bietet nicht nur Vorteile. Es ist das erste System seiner Art, welches Verbreitung findet. Dementsprechend findet sich in der Nutzung des Systems Potenzial für Verbesserungen.
Erstens weist das System an sich Schwächen auf, aber auch seine Auswirkungen ökologischer Natur und die Bewertung von rechtlicher Seite aus werfen problematische Fragen auf. Der Tauschkurs gegen gängige Währungen unterliegt dem Risiko, starken Schwankungen ausgesetzt zu sein, was die Verwendung von Bitcoins als Zahlungsmittel erschwert. Die Nutzung des Systems für unerwünschte Aktivitäten ist ein weiterer problematischer Aspekt. Um eine unerwünschte Nutzung von dezentralen online

[11] Vgl. Wolf 2011: Senators seek crackdown on "Bitcoin"currency URL: http://www.reuters.com/article/2011/06/08/us-financial-bitcoins-idUSTRE7573T320110608.

Transaktionssystemen mit öffentlicher Transaktionshistorie wie Bitcoin einzuschränken, wird nun im nachfolgenden Kapitel 6 ein Transaktionsüberwachungskonzept vorgestellt.

6 Transaktionsüberwachung

Dezentrale online Transaktionssysteme, wie sie in Kapitel 1 beschrieben wurden, haben ihrer Architektur nach keine für Transaktionen nötige dritte Instanzen, welche zu illegalen Aktivitäten gehörenden Transaktionen identifizieren und zwecks Strafverfolgung melden könnten.
In gängigen Währungssystemen sind Banken als dritte Partei bei vielen Transaktionen beteiligt. Sie sind beispielsweise in Deutschland nach dem „Geldwäschegesetz“[1] dazu verpflichtet, die Aufgabe der Transaktionsüberwachung nach den gesetzlichen Vorgaben zu übernehmen, um so z.B. Geldwäsche zu verhindern.

Ohne dritte Instanz konnte mit Hilfe des Bitcoin Systems, als Vertreter der dezentralen online Transaktionssysteme, z.B. der bereits beschriebene[2] online Drogenshop Silk Road entstehen oder viele Diebstähle von Bitcoin Guthaben unaufgeklärt bleiben[3].
Der Marktplatz Silk Road konnte zwar von amerikanischen Behörden abgeschaltet und der Betreiber ermittelt werden[4]. Laut Heise Security gelang die Ermittlung des Betreibers jedoch nicht durch Überwachung und Auswertung von Transaktionen der Silk Road Bitcoin Adressen, sondern über ein Posting des Silk Road Betreibers in einem Forum für Rauschmittel zum Zeitpunkt der Online Schaltung des Marktplatzes.
Diese beiden Beispiele, Silk Road und die Diebstähle, zeigen, dass auch in dezentralen online Transaktionssystemen, wie im Bitcoin System, eine Überwachung von Transaktionen wünschenswert sein kann.

Diese Ausarbeitung befasst sich jedoch nicht mit der Frage, ob und inwieweit eine Trans-

[1] Vgl. Bundesrepublik Deutschland 2008: Geldwäschegesetz - GwG.
[2] Siehe Unterabschnitt 4.4.1.
[3] Siehe Kapitel 5.
[4] Vgl. Eikenberg 2013: Silk Road: ausgeschaltet URL: `http://www.heise.de/security/meldung/Silk-Road-FBI-schaltet-Drogen-Handelsplattform-im-Tor-Netz-aus-1972026.html`.

aktionsüberwachung auch in dezentralen Systemen wünschenswert bzw. erstrebenswert ist, und auch nicht damit, wie eine solche Überwachung gerechtfertigt sein könnte[5].
Im Fokus steht, wie eine Transaktionsüberwachung zwecks Vermeidung und Aufklärung unerwünschter Vorgänge konzeptionell in dezentralen online Transaktionssystemen mit öffentlicher Historie arbeiten kann, und darüber hinaus, welche Auswirkungen eine Überwachung nach diesem Konzept auf die Eigenschaften des Systems und seine ehrlichen Nutzer hätte.

6.1 Isolation von Adressen

Der erste Teil des Konzeptes zur Transaktionsüberwachung in dezentralen online Transaktionssystemen zielt auf die Vermeidung von Transaktionen unerwünschter Vorgänge ab und beruht auf der Überwachung der öffentlichen Transaktionshistorie eines solchen Systems.
Der zweite Teil des Konzeptes wird in Abschnitt 6.3 beschrieben und befasst sich mit der Identifizierung von Besitzern der Adressen unerwünschter Vorgänge. Dazu werden Adressen isoliert, welche durch geeignete Maßnahmen unerwünschtem Vorgehen zugeordnet werden können, sodass die diesen Adressen zugeschriebenen Guthaben nicht weiter verwendet werden können. Isoliert meint dabei, dass keine andere Adresse bereit ist, Guthaben von der als unerwünscht eingestuften Adresse zu empfangen, ohne hinzunehmen, dadurch selbst als unerwünschte Adresse eingestuft zu werden.
Alle weiteren Erörterungen des Konzepts werden nun anhand des Bitcoin Systems vorgestellt, da es das erste in der Praxis eingeführte Transaktionssystem der untersuchten Art ist. Das Isolationskonzept zielt letztlich also darauf ab, alle Bitcoin Guthaben, die unerwünschtem Vorgehen zugeordnet werden, einzufrieren. Dieses Einfrieren geschieht durch das öffentliche Bekanntmachen aller Adressen mit unerwünschtem Guthaben.

[5] Daher wird im folgenden Text auch von unerwünschtem Vorgehen gesprochen. Was unerwünschte Vorgänge sind, bleibt offen.

6.1.1 Rote Adressen

Man stelle sich beispielhaft einen vereinfachten Ausschnitt der Transaktionshistorie wie in Abbildung 6.1 in Form eines Art Sequenzdiagramms vor. Die Knoten A, B, X usw. repräsentieren Bitcoin Adressen. Die gerichteten Kanten zwischen zwei Knotenlinien bilden eine Transaktionen zwischen den beiden Knoten ab. Die Richtung der Kante gibt dabei die Flussrichtung des transferierten Guthabens an.

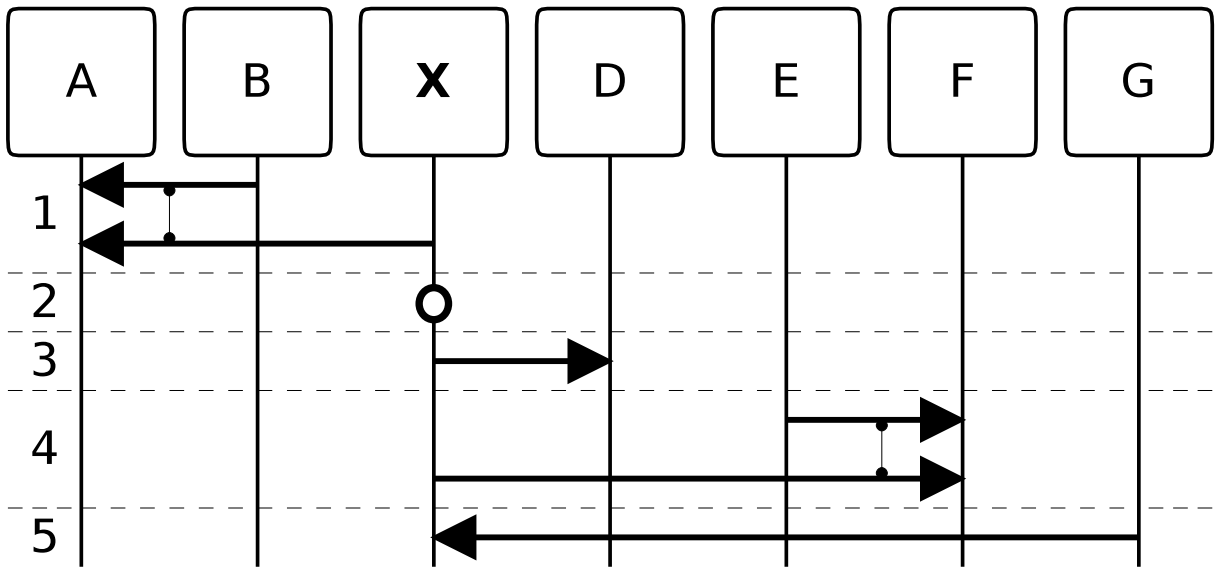

Abbildung 6.1: Transaktionsdiagramm der öffentlichen Transaktionshistorie als Beispiel für die Einstufung roter Adressen.

Sind mehrere Adressen Eingang für genau eine Transaktion[6] so sind die zusammengehörenden Transaktionskanten, wie etwa in Stufe Eins oder Vier, untereinander durch eine Verbindungskante kenntlich gemacht.
Knoten X sei nun eine Adresse, welche in unerwünschte Vorgehen verwickelt ist[7] und deren Guthaben isoliert werden soll. Isolierte Adressen werden ab jetzt als rote Adressen bezeichnet. Die Einstufung von Knoten X als rote Adresse geschehe in Stufe Drei.

[6] Siehe Transaktionen mit mehreren Eingängen Abschnitt 3.6.1.
[7] Wie eine Adresse als unerwünscht eingestuft werden könnte, soll später betrachtet werden. Der unerwünschte Status von X wird daher vorerst als gegeben angesehen.

6.1.2 Öffentliche Liste

Um die Isolation der Adresse und deren Guthaben zu erreichen, müssen alle ehrlichen Nutzer von der identifizierten roten Adresse wissen. Zu diesem Zweck wird nun eine weitere Komponente in Form einer Liste eingeführt, welche allen Bitcoin Nutzern, wie die Transaktionshistorie, öffentlich zugänglich sein soll. Diese Liste enthält alle Adressen mit rotem Status und wird ständig aktualisiert.
Jeder ehrliche Nutzer wird nun keine Transaktionen von roten Adressen der Liste entgegennehmen und seinen Transaktionspartner vorher nach dessen Adresse fragen.[8].
Somit sind rote Adressen isoliert. Es ist nicht mehr möglich, etwa über Tauschbörsen andere Nutzer zu finden, die bereit sind, für gängige Währungen Transaktionen von der roten Adresse zu empfangen oder sonst wie das Guthaben in andere Werte umzusetzen. Denn akzeptiert ein ehrlicher Nutzer eine Transaktion von einer roten Adresse, so wird auch seine Adresse als rot eingestuft.
Diese Fortschreibung des roten Status ist durch die öffentliche Transaktionshistorie in Form der Block Chain möglich. Durch die ständige Auswertung aller neuen, an die Block Chain angefügten Blöcke kann jede Adresse identifiziert werden, welche Transaktionen von einer roten Adresse angenommen hat. Auch kann durch die Auswertung der bereits in der Block Chain gespeicherten Transaktionen Rückschlüsse auf weitere rote Adressen gezogen werden.

Knoten X wird in Stufe Zwei durch geeignete Maßnahmen als rote Adresse identifiziert, in Abbildung 6.1 verdeutlicht durch den Kreis auf der Knotenlinie. Transaktionen Eins, die vor Stufe Zwei liegt, geschieht somit bevor Knoten X in die rote Liste aufgenommen wurde, alle Transaktionen nach Stufe Zwei wurden durchgeführt, als Knoten X bereits auf der Liste stand.

Fortschreibung der Liste

Das Grundprinzip der Transaktionsüberwachung ist somit die Fortschreibung des roten Status auf alle Adressen, welche mit einer roten Adresse in Verbindung stehen.

[8] Im Bitcoin System kann von jeder Adresse auf jede beliebige andere Adresse Guthaben transferiert werden, ohne dass der empfangende Besitzer der Adresse den Eingang unterbinden könnte. Dieses Problem wird später diskutiert

Fall Eins Der einfachste Fortschreibungsfall wurde bereits erläutert und ist durch die Transaktion zwischen Knoten X und D in Stufe Drei dargestellt. Empfängt eine Adresse Guthaben von einer roten Adresse, so wird die empfangende Adresse auch rot. Folglich ist Adresse D nach Ausführung von Stufe Drei eine rote Adresse. Denn akzeptiert ein Empfänger Transaktionen von einer roten Adresse, so ist davon auszugehen, dass der Empfänger mit dem Sender kooperiert oder der Sender auch Besitzer der Empfängeradresse ist.

Fall Zwei Ein weiterer Fortscheibungsfall ergibt sich in Stufe Vier, wenn eine Transaktion mehrere Eingänge hat und einer dieser Eingänge eine rote Adresse ist. Adresse E ist noch nicht rot, wird aber mit X zusammen Eingang einer Transaktion an Adresse F. Da alle Eingänge einer Transaktion genau einem Besitzer gehören müssen, werden alle Eingangsadressen dieser Transaktion an Adresse F auch als rot eingestuft. Nach Stufe Vier ist auch Adresse E rot sowie nach Fall Eins Adresse F.

Fall Drei Der letzte Fall tritt ein, wenn in einer Transaktion einer roten Adresse Guthaben transferiert wird. Alle Adressen, die roten Adressen Guthaben transferieren, werden ebenfalls rot eingestuft. Dieser Fall ist in Stufe Fünf abgebildet.

Rückwirkung der Liste

Nicht nur bei Transaktionen, welche nach der Aufnahme einer Adresse in die Liste durchgeführt werden, kann es, wie gerade geschildert, zur Fortschreibung des roten Status auf andere Adressen kommen. Wird eine Adresse neu als rot eingestuft, so hat dies auch Auswirkungen auf zeitlich vor der Einstufung liegende Transaktionen, in welche die neue rote Adresse involviert war.
Hat vor der Einordnung der roten Adresse eine Transaktion mit mehreren Eingängen stattgefunden, bei der die neu eingestufte rote Adresse beteiligt war, so ist analog zu Fall Zwei bei der Fortschreibung allen anderen damals beteiligten Eingangsadressen der rote Status zuzuordnen. Dargestellt ist dieser Fall in Stufe Eins. Knoten B wird zusammen mit Knoten X Eingang für eine Transaktion an Knoten A. Knoten B gehört daher auch dem Besitzer von Knoten X. Knoten A wird hingegen nicht als rot eingestuft. Der Besitzer von

Knoten A konnte noch nicht wissen, dass er eine Transaktion von einer roten Adresse empfängt, da diese noch nicht auf der öffentlichen Liste stand.

Durch die Fortschreibung und Rückwirkung der Liste wird erreicht, dass alle Adressen, die eindeutig auch unter Kontrolle des Besitzers der identifizierten roten Adresse stehen, oder von denen auszugehen ist, dass sie mit dem Sender kooperieren, ebenfalls isoliert werden.
Tabelle 7.1 zeigt die öffentliche Liste des in Abbildung 6.1 gegebenen Transaktionsbeispiels. Dabei wird die Entwicklung der Liste im Zeitverlauf nach Stufen dargestellt.

Stufe	rote Adressen
1	
2	X, B
3	X, B, D
4	X, B, D, E, F
5	X, B, D, E, F, J

Tabelle 6.1: Adressen mit rotem Status in den verschiedenen Stufen.

6.1.3 Adressen mit limitiertem Eingang

Eine zentrale Bedingung für das Funktionieren des vorgestellte Konzeptes ist, dass Nutzer bestimmen können, von welchen Adressen aus sie Transaktionen annehmen. Ist es einem Nutzer nicht möglich, eine Transaktion von einer roten Adresse an eine seiner eigenen Adressen zu unterbinden, ist das ganze Isolationskonzept hinfällig.
Besitzer von roten Adressen könnten beliebige andere, nicht rote Adressen durch eine Überweisung kompromittieren, dadurch bedingt, dass alle Empfänger von Transaktionen, ausgehend von roten Adressen, auch rot eingestuft werden.
Ein möglicher Ansatz zur Lösung dieses Problems innerhalb des Bitcoin System wäre es, Adressen einzuführen, bei welchen der Besitzer festlegen kann, von welchen Adressen aus seiner Adresse Guthaben gutgeschrieben werden kann. Eine Idee zur Implementation einer solchen Funktion wird nun vorgestellt.

Erstellt ein Bitcoin Nutzer eine neue Adresse, so ist diese vorerst nur ihm bekannt. Gibt er

seine Adresse einem Transaktionspartner preis und überweist dieser ihm Guthaben, so ist spätestens dann die neue Adresse in einem Block in der Block Chain öffentlich gemacht. Jeder Nutzer kann dann ab diesem Zeitpunkt der Adresse Guthaben gutschreiben.
Will ein Nutzer Transaktionen nur von bestimmten Adressen aus zulassen, so könnte er dies durch eine öffentliche Nachricht kundtun. Alle Bitcoin Miner wüssten dann, dass sie nur Transaktionen bestätigen sollen, die von den vom Besitzer erlaubten Adressen stammen.

Adressen-Schloss

Wie in Abbildung 6.2 dargestellt, könnte der Nutzer, bevor er seine Adresse einem Transaktionspartner preisgibt, eine Nachricht über das Netzwerk an alle Minern senden, in der er mitteilt, von welchen Adressen seine neu erstellte Adresse Guthaben empfangen darf. Solch eine Nachricht, welche nun als Adressen-Schloss bezeichnet wird, signiert der Nutzer mit seinem Private-Key. So wird sichergestellt, dass nur Besitzer von Adressen auch Schlösser für diese anlegen können.
Die Miner können dann anhand der Signatur des Adressen-Schlosses überprüfen, ob der wirkliche Besitzer der Adresse das Schloss erstellt hat.

Validierung Ein Miner, welcher eine Transaktion in einen Block aufnehmen möchte, würde neben den bereits bestehenden Validierungen[9] einer Transaktion weiter prüfen, ob für die vorliegende Transaktion ein Adressen-Schloss hinterlegt ist.
Ist ein Schloss hinterlegt, prüft er, ob die Adresse in der Transaktion im Schloss eingetragen ist. Falls nein, wird die Transaktion verworfen. Für alle Transaktionen ohne vorhandenes Transaktions-Schloss werden wie gehabt alle Senderadressen akzeptiert.

Speicherung Damit eine Transaktion vom Bitcoin System in dem beschriebenen Validierungsprozess bewertet werden kann, ist es nötig, alle Adressen-Schlösser im System dauerhaft zu hinterlegen.
Die Adressen-Schlösser könnten zwecks Speicherung in die Block Chain aufgenommen werden. So wäre gewährleistet, dass der Besitzer des Schlosses sich vergewissern kann,

[9] Der Miner validiert u.a. zuerst, ob kein Double-Spending mit der neuen Transaktion durchgeführt wird.

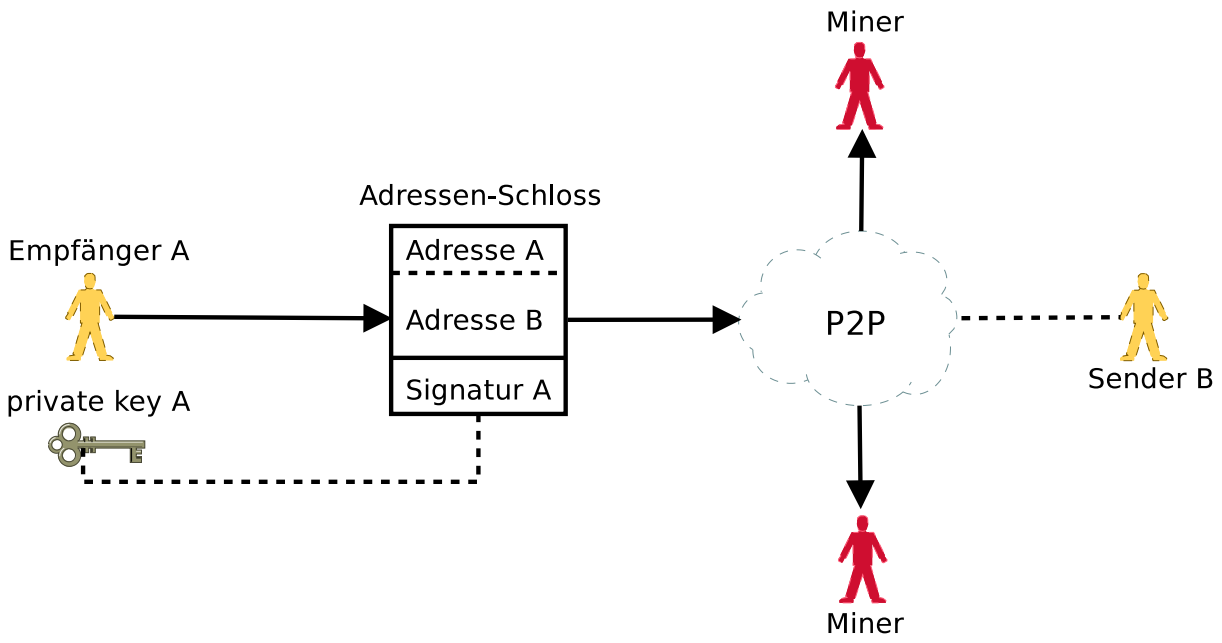

Abbildung 6.2: Empfänger A, der ein Adressen-Schloss für seine neue Adresse erzeugt, um eine Transaktion von Sender B zu empfangen.

dass seine Adresse gesichert ist, und zum anderen könnten so alle Miner auf die Schlösser zugreifen.
Zur Erstellung eines Schlosses wäre bei Speicherung jenes Schlosses in der Block Chain dann eine Gebühr nötig, ähnlich der freiwilligen Gebühr bei Transaktionen. Der das Schloss in die Block Chain aufnehmende Miner dürfte die Gebühr einbehalten. Ohne diese Gebühr würde der Anreiz für die Miner fehlen, die Schlösser mit in die Block Chain aufzunehmen.

Speichergröße Es ist davon auszugehen, dass für den Großteil der Adressen ein Adressen-Schloss angelegt werden würde, da mit bestehendem Adressen-Schloss keine Kompromittierung der eigenen Adresse vorgenommen werden kann.
Diese zusätzlichen Daten würden die Größe der Block Chain wesentlich steigern. Vor allem auch deshalb, weil bei Aktualisierung eines Adressen-Schlosses das vorhergehende Schloss aufgrund der Hashketten Eigenschaft[10]nicht aus der Block Chain entfernt werden kann.

[10]Siehe Unterabschnitt 3.6.2.

6.1.4 Transaktionsblockade

Um zu verhindern, dass ehrliche Adressen durch Überweisungen von roten Adressen kompromittiert werden, wäre neben den in Unterabschnitt 6.1.3 vorgestellten limitierten Transaktionseingängen durch Adressen-Schlösser auch eine Transaktionsblockade zielführend.
Lehnen alle Miner Transaktionen von roten Adressen ab, so ist die Isolation der Adressen ebenfalls gewährleistet. Die Transaktionsblockade setzt an einer anderen Stelle im System an als das Adressen-Schloss. Während beim Adressen-Schloss der Nutzer Transaktionen mit roten Adressen verhindert, verhindert bei der Transaktionsblockade der Miner ohne Zutun des Nutzers Transaktionen von roten Adressen.
Warum das Konzept des Adressen-Schlosses der Transaktionsblockade vorzuziehen ist, wird in Unterabschnitt 6.4.3 diskutiert.

6.2 Initiale Identifizierung roter Adressen

Bisher wurde noch nicht betrachtet, wie eine Adresse als rote Adresse identifiziert werden kann. Einige Ansätze werden daher folgend erörtert. Wie und weshalb eine Adresse letztlich als rot identifiziert wird, ist für das Isolationskonzept dennoch weniger entscheidend, weshalb im Anschluss in Abschnitt 6.4 diskutiert wird, wie die entscheidende Verwaltung der Liste organisiert werden könnte.

6.2.1 Testkäufe

Im Falle von Silk Road führte das FBI mehrere Testkäufe[11] durch. Bei solchen Testkäufen werden Überweisungen an eine Bitcoin Adresse von Silk Road durchgeführt. Diese Testkäufe können daher dazu dienen, rote Adressen zu identifizieren.
Betreiber illegaler Seiten wären gezwungen, für jeden ihrer Kunden eine eigene Adresse zu generieren, damit immer nur ein Guthaben isoliert wird, falls der Kunde ein Testkäufer war. Den Betreibern wäre es somit nicht mehr möglich, große Guthaben

[11] Vgl. Eikenberg 2013: Silk Road: ausgeschaltet URL: `http://www.heise.de/security/meldung/Silk-Road-FBI-schaltet-Drogen-Handelsplattform-im-Tor-Netz-aus-1972026.html`.

zu aggregieren und die Guthaben in großer Menge z.B. in gängige Währungen zu tauschen.

6.2.2 Diebstähle

Auch bei Diebstählen können rote Adressen entstehen. Ein Bestohlener würde nachweisen, dass ihm Bitcoins entwendet und an eine Adresse überwiesen wurden, die nicht unter seinem Einfluss steht. Diese Adresse würde dann als rot eingestuft.

6.3 Deanonymisieren von roten Adressen

Das Deanonymisieren der Besitzer roter Adressen ist neben der Isolation der roten Guthaben der zweite Teil des Transaktionsüberwachungskonzeptes und wird nun vorgestellt. Neben dem Isolieren von zu unerwünschtem Vorgehen gehörenden Guthaben innerhalb des Bitcoin Systems mittels der öffentlichen Liste der roten Adressen, kann mit der öffentlichen Liste auch versucht werden, Besitzer roter Adressen zu identifizieren.

6.3.1 Gelbe Adressen

Hat ein Besitzer einer roten Adresse, bevor seine Adresse als rot eingestuft wurde, Transaktionen mit ehrlichen Nutzern durchgeführt, so können diese Nutzer ihn prinzipiell deanonymisieren.
Allen Besitzern von Adressen, die vor der Einstufung der roten Adresse mit dieser interagiert haben, kann zweifelsfrei keine Kooperation mit dem Besitzer der roten Adresse nachgesagt werden. Diese Nutzer wussten nichts von dem potenziellen roten Status ihres Transaktionspartners.
Dennoch könnten alle diese Adressen Besitzer durch ihre Interaktion mit der roten Adresse prinzipiell Wissen über deren Besitzer haben, weshalb sie dazu beitragen könnten, ihn zu deanonymisieren. Adressen von Besitzern, die vor der Einstufung mit roten Adressen interagiert haben, werden als gelb eingestuft und folgend gelbe Adressen genannt.
Hat eine rote Adresse z.B. über eine Tauschbörse vor der Einstufung Bitcoins mit ehrlichen

Nutzern getauscht, so sind diesen ehrlichen Nutzern die Bankdaten des Besitzers der roten Adresse bekannt.

Letztliches Ziel der Einführung gelber Adressen ist es folglich, Adressen zu identifizieren, die rote Adressen deanonymisieren könnten.

Gelber Status

Analog zur Fortschreibung und Rückwirkung des roten Status gibt es zwei Fälle bei der Einstufung einer Adresse als gelbe Adresse. Die Fälle unterscheiden sich dahin gehend von den Fällen der roten Adressen, als dass der Besitzer, der in die Transaktionen mit der baldigen roten Adresse involvierten Adresse, nicht wissen konnte, dass er mit einer potenziell unerwünschten Adresse interagiert. Die rote Adresse war zum Zeitpunkt der betrachteten Transaktionen noch nicht in der öffentlichen Liste vermerkt.
Immer wenn eine Adresse neu als rot eingestuft wird, werden alle vorherigen Transaktionen, in die die neue rote Adresse involviert war, dahingehend untersucht, ob die anderen an den Transaktionen beteiligten Adressen als gelb eingestuft werden. Die Fälle zur Einstufung als gelbe Adresse werden in Abbildung 6.3 dargestellt und nun beschrieben. In dem Transaktionsdiagramm wird in Stufe Fünf Knoten X als rot identifiziert.

Fall eins Knoten C hat in Stufe Zwei vor der Einstufung in Stufe Fünf Guthaben von Knoten X empfangen. Der Besitzer der empfangenden Adresse könnte wissen, wer der Besitzer von Adresse X ist. Daher wird Adresse C als gelb eingestuft. Alle Adressen, die Guthaben von einer rote Adresse transferiert bekommen haben, bevor diese rot eingstuft wurde, werden gelb eingestuft.

Fall Zwei Hat eine Adresse einer roten Adresse vor der Einstufung Guthaben gutgeschrieben, so wird sie als gelb eingestuft. Der Besitzer der gelben Adresse könnte wissen, wem er Guthaben transferiert hat. Dargestellt ist dieser Fall in Stufe Eins. Knoten A transferiert Guthaben an Knoten X, bevor dieser rot wird.

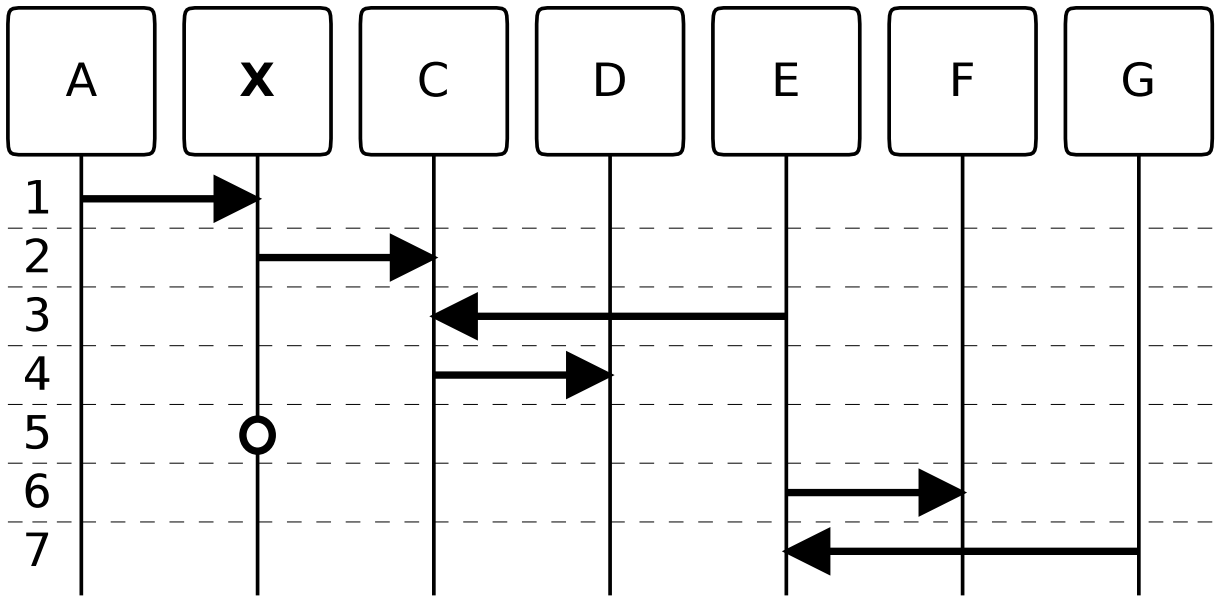

Abbildung 6.3: Transaktionsdiagramm der öffentlichen Transaktionshistorie als Beispiel für die Einstufung gelber Adressen.

6.3.2 Besitzer gelber Adressen

Adressen mit gelbem Status werden wie die roten Adressen in der öffentlichen Liste hinterlegt, sodass alle Bitcoin Nutzer über die Einstufung informiert sind. Tabelle 7.2 zeigt dabei, welche Adressen in der jeweiligen Stufe aus Abbildung 6.3 als gelb eingestuft sind.

Stufe	gelbe Adressen
1	-
2	-
3	-
4	-
5	A, C, D, E
6	A, C, D, E, F
7	A, C, D, E, F, G

Tabelle 6.2: Adressen mit gelben Status in den verschiedenen Stufen.

Der gelbe Status soll im Gegensatz zum roten Status jedoch auf die Nutzung einer Adresse keinen Einfluss haben. Der gelbe Status wird zwar in der öffentlichen Liste vermerkt, dient

aber nicht dazu, dass die gelbe Adresse als Transaktions Adresse isoliert werden soll[12], sondern der Status soll dazu dienen, die Besitzer der gelben Adressen darauf hinzuweisen, dass sie potenziell die Möglichkeit haben könnten, einen Besitzer einer roten Adresse zu deanonymisieren.
Jeder Besitzer einer gelben Adresse kann aufgrund der öffentliche Liste erkennen, ob er mit einer roten Adresse interagiert hat, und nach seinen eigenen Kriterien entscheiden, ob er die Identität der roten Adresse preisgeben möchte, sofern er die Identität hinter dieser Adresse wirklich kennt.

6.3.3 Abstufungen des gelben Status

Die Stufen ab Stufe Drei in Abbildung 6.3 sind noch nicht erläutert worden. Diese Stufen gehören zu Transaktionen, bei denen man eine Fortschreibung des gelben Status analog zur Fortschreibung des roten Status vornehmen könnte.
Betrachtet man Knoten D, so hat dieser Knoten Guthaben von Knoten C transferiert bekommen. Der Besitzer von Knoten D kann wissen, wer Besitzer von C ist, und der Besitzer von Knoten C kann wiederum wissen, wer Besitzer von Knoten X ist, welcher rot eingestuft ist. Entscheidet sich nun der Besitzer von Knoten D, die Identität des Besitzers von Knoten C preiszugeben, so könnte ein Druck auf Besitzer C entstehen, seinerseits die Identität des Besitzers von Knoten X preiszugeben.
Ähnlich verhält es sich auch mit der Transaktion in Stufe Drei. Knoten E überweist Guthaben an Knoten C und kann somit prinzipiell wissen, wer Besitzer von Knoten C ist, ihn deanonymisieren, sodass ein Druck auf Besitzer C entsteht, Besitzer X ebenfalls zu deanonymisieren.
Die in Stufe Sechs und Sieben dargestellten Transaktionen setzen diese Fortschreibungsüberlegung des gelben Status für Transaktionen nach der Einstufung von Knoten X als rote Adresse fort.
Im Gegensatz zur unbegrenzt tiefen Fortschreibung des roten Status ist jedoch zu überlegen, bis zu welcher Tiefe eine Fortschreibung des gelben Status noch zielführend ist. Knoten F etwa könnte nur Knoten E deanonymisieren, Knoten E dann erst Knoten C und dieser erst den eigentlich betroffenen roten Knoten X. In diesem Beispiel liegt die Tiefe der gelben Fortschreibung bei zwei. Über zwei Knoten wird erst der Knoten deanonymisiert,

[12] Denn der gelben Adresse kann wie erläutert nicht zweifelsfrei eine Kooperation mit einer roten Adresse nachgewiesen werden.

der den roten Knoten deanonyisieren könnte.
Je größer die Abstufung[13] des gelben Status ist, desto unwahrscheinlicher ist es, dass ein Deanonymisierung dieser gelben Adresse auch zu einer Deanonymisieren der roten Adresse führt, denn alle Knoten bis zur roten Adresse müssen dazu ebenfalls ihren Transaktionspartner deanonymisieren.
Der gelbe Status ist daher nur bis zu einer sinnvollen Abstufung fortzuschreiben.

6.4 Verwaltung der Liste

Neben den Testkäufen und Diebstählen sind viele weitere Szenarien denkbar, die dazu führen, dass Adressen isoliert werden sollten. Die Verwaltung, sprich das Aufnehmen in und das Entfernen von Adressen aus der Liste für rote Adressen, wurde bisher nicht thematisiert.
Neben dem initialen Aufnehmen von Adressen in die Liste und Auswerten der Rückwirkung der Adressenaufnahme übernimmt die Listenverwaltung auch das Fortschreiben der Liste.
Dazu wertet der Listenbetreiber ständig die Block Chain aus und prüft dabei, ob neue Blöcke Transaktionen enthalten, die zu einer Fortschreibung des roten oder gelben Status aufgrund der Listeneinträge führen.
Die Verwaltung der Liste spielt eine zentrale Rolle, da die Verwaltung die Entscheidungsgewalt darüber besitzt, nach welchen Kriterien Adressen in die Liste aufgenommen werden.

6.4.1 Zentrale Verwaltung

An diesem Punkt wird die zentrale Transaktionsüberwachung im Bitcoin System prinzipiell möglich. Einigen sich alle Nutzer auf eine Instanz, welche die Verwaltung der Liste nach definierten Kriterien übernimmt, so entsteht eine zentrale Überwachungsinstanz.
Jedoch hätte es eine alleinige zentrale Verwaltung wahrscheinlich schwer, sich als bevorzugtes Konzept zur Listenverwaltung durchzusetzen
Denkt man z.B. an die Sperrung der PayPal Konten von WikiLeaks, so könnte auch eine

[13] Die Tiefe der Fortschreibung des gelben Status wird fortan als Abstufung bezeichnet. Je größer die Abstufung ist, desto größer ist die Tiefe der Fortschreibung.

zentrale Instanz Adressen isolieren, die ein Teil der Bitcoin Nutzer nicht isolieren will. Diese Pluralität bei der Definition der Aufnahmekriterien von Adressen führt zu dem wahrscheinlicheren Fall, mehrere Instanzen vorzufinden, die jeweils Listen verwalten.

6.4.2 Mehrere zentrale Verwaltungen

Die verschiedenen Auffassungen darüber, welche Adressen isoliert werden sollen, könnten in mehreren Listen Ausgestaltung finden. Ein Nutzer entscheidet sich dann für die Listen, welche seine Auffassung über die Aufnahmekriterien am besten abbildet. Konkret auf das WikiLeaks Beispiel bezogen würde sich ein WikiLeaks freundlicher Nutzer für eine Liste entscheiden, die WikiLeaks nicht listet und auch keine Fortschreibung und Rückwirkung des roten Status auf Interaktionen mit diesen Adressen vornimmt.
Durch das Vorhandensein mehrerer Listen würde auch ein Druck auf alle Betreiber von Listen entstehen, nur Adressen aufzunehmen, welche nach allgemein akzeptierten Kriterien ausgewählt wurden. Nimmt beispielsweise ein staatlicher Betreiber einer Liste mit Diebstahladressen auch Adressen von politischen Gegnern auf, so könnten Nutzer seine Liste nicht mehr akzeptieren oder schlicht manche der Eintragungen ignorieren.
Die Listen würden somit neben dem Eintrag der roten Adresse immer auch eine Begründung für die Einordnung enthalten, denn ohne eine solche Begründung wird kein Nutzer einen Eintrag akzeptieren.

Vertrauensnetzwerk

Das Auswählen der Listen oder das Ignorieren einzelner Adressen aus Listen ist dabei für einen einzelnen Nutzer alleine eine Aufgabe, die viel Aufwand erfordert. Denkbar ist daher, dass Vertrauensnetzwerke entstehen, die Listen bewerten, überwachen und Informationen bereitstellen, sodass ein Nutzer nach eigenen Kriterien schnell und einfach Listen auswählen kann. Die Überprüfung der Listen sollte dabei im Bitcoin Client des Nutzer geschehen. Ähnliche Vertrauensnetzwerke, die bereits aus anderem Kontext bekannt sind, könnten dafür Vorbild stehen, wie etwa das Web of Trust für Webseiten Reputation.

6.4.3 Nutzerseitige Verwaltung

Der Bitcoin Client des Nutzers speichert und aktualisiert die ausgewählten Listen. Bei jeder Transaktion prüft er die Transaktion auf Konformität mit den hinterlegten Listen.
Der Nutzer muss somit nur einmal bei der Installation des Clients die Listenauswahl des Clients personalisieren. Denkbar ist, dass der Client standardmäßig mit allgemein anerkannten Listen installiert wird, welche z.B. von staatlichen Stellen stammen und kriminelle Adressen isolieren.
Nach der initialen Auswahl der Listen muss der Nutzer nur noch tätig werden, wenn die von ihm ausgewählten Listen nicht mehr seine persönlichen Isolationskriterien vertreten.

Da Nutzer verschiedene Listen auswählen werden, macht das Verfahren der Transaktionsblockade nur bedingt Sinn. Alle Miner müssten sich über die Auswahl der zu isolierenden Adressen einig sein. Gibt es nur einen Miner, der auch isolierte Adressen in seine Blöcke aufnimmt, so könnte nicht verhindert werden, dass rote Guthaben andere Adressen unfreiwillig kompromittieren. Bei dem Konzept des Adressen-Schlosses hat der Nutzer auch bei vielen vorhandenen Listen die volle Kontrolle über eingehende Adressen.

6.5 Auswirkungen

Das Einführen des Isolationskonzeptes hätte Auswirkungen auf die Nutzung des Transaktionssystems.

6.5.1 Transaktionen

Einem Transaktionsempfänger müsste für jede Transaktion die Sende Adresse bekannt sein. Der Empfänger würde eine neue Adresse samt Adressen-Schloss für die Sende Adresse erstellen und erst dann könnte die eigentliche Transaktion durchgeführt werden.
Dieser Prozess stellt einen zusätzlichen Aufwand im Umgang mit dem System dar. Eine einfache Transaktion geht der zeitaufwendige Schritt des Wartens auf die Aufnahme des Adressen-Schloss in die Block Chain zusätzlich voraus.

Auch die Aufwände zum zusätzlichen Austausch der Senderadresse und die Miner Gebühr der Aufnahme des Adressen-Schlosses kommen hinzu.
Bei häufigen Transaktionen zwischen Adressen fallen die zusätzlichen Aufwände zum Anlegen des Schlosses weniger ins Gewicht als bei Transaktionen zwischen Adressen, die nur einmal miteinander interagieren.
Für Transaktionen von geringem Umfang kann, um die gerade erläuterten zusätzlichen Transaktionskosten zu vermeiden, auf das Erstellen eines Adressen-Schlosses verzichtet werden. Ein Besitzer einer Adresse ohne Schloss läuft dann zwar Gefahr, dass durch eine Überweisung an seine Adresse diese kompromittiert wird, dennoch wird er dieses Risiko bei Adressen mit geringen Beträgen wohl hinnehmen und die Transaktionskosten durch das Schloss vermeiden.

6.5.2 Isoliertes Guthaben

Ein weiterer problematischer Punkt ist die durch die Isolation der Adressen eingefrorenen Bitcoins. Da die Menge an Bitcoins begrenzt ist, hat das Einfrieren von Guthaben den Effekt der Reduzierung der Geldmenge.
Die Bitcoins der isolierten Adressen sind von der Zirkulation ausgeschlossen. Da nur der Besitzer des Private-Keys das Guthaben der isolierten Adresse transferieren kann, ist es prizipiell durch die Isolation verloren.
Denkbar wären die Einrichtung von allgemein verwalteten Adressen, welche zur Rückführung isolierter Guthaben dienen. Beschlagnahmte Private-Keys von Besitzern roter Adressen könnten dann dazu verwendet werden, die Guthaben der dazugehörigen roten Adressen auf die Rückführungsadressen zu transferieren. Die Guthaben der Rückführungsadressen würden dann von der sie verwaltenden allgemeinen Instanz z.B. gespendet. Die Rückführungsadressen müssten zu diesem Zweck von der Fortschreibung des roten Status befreit sein, weshalb alle Listen Betreiber mit der Instanz, die die Rückführungsadressen verwaltet, einverstanden sein müssten.
Beschlagnahmte rote Adressen könnten auch durch Entfernen des roten Status wieder in den Umlauf gebracht werden. Rückführungsadressen könnten daher vornehmlich für den Fall eingerichtet werden, dass Besitzer von roten Adressen ihre Guthaben unerkannt freiwillig freigeben möchten, da sie selbst mit dem Guthaben nicht mehr agieren können.

7 Konklusion

Das vorgestellte Transaktionsüberwachungskonzept hat gezeigt, dass es auch in dezentralen online Transaktionssystemen möglich ist, mit Hilfe eines Vertrauensnetzwerks eine Überwachung von Transaktionen zur Vermeidung von z.B. Geldwäsche oder Drogenhandel zu installieren, ohne den dezentralen Charakter des Systems auszuhebeln und eine zentrale Instanz einzuführen.
Die Überwachung kann dezentral über die Isolation von Adressen erfolgen, wobei die Kriterien, die zur Auswahl von zu isolierenden Adressen herangezogen werden, allgemeiner Kontrolle durch das Vertrauensnetzwerk unterliegt.
Der Ansatz ist dabei nicht nur auf das Bitcoin System beschränkt, sondern lässt sich auf alle dezentralen Transaktionssysteme mit öffentlicher Transaktionshistorie übertragen wie sie unter anderem unter dem Begriff Altcoins als Derivate von Bitcoins zur Zeit entstehen. Inwieweit Transaktionsüberwachung in der zukünftigen Entwicklung und Nutzung solcher Systeme eine Rolle spielt, wird die Zukunft zeigen.

Literatur

Androulaki, E.; Karam, G.; et al.: Evaluating User Privacy in Bitcoin. ETH Zurich, NEC Laboratories Europe: Heidelberg, Zürich 2012.

Armory: Armory Bitcoin Client. URL: http://bitcoinarmory.com/. 2013-10-10.

Australian Government: Austrac typologies and case studies report 2012: 2012.

BTCMine: BTC Mine. URL: http://btcmine.com/. 2013-11-14.

Back, A.: Hashcash - A Denial of Service Counter-Measure: 2002.

Barber, S.; Boyen, X.; et al.: Bitter to Better — How to Make Bitcoin a Better Currency. Palo Alto Research Center, University of California, Berkeley: 2012.

Becker, C.: Bitcoin paper wallet. URL: https://bitcoinpaperwallet.com/. 2013-10-31.

Bitbills Inc.: Bitbills FAQ. URL: http://bitbills.com/faq. 2013-10-10.

Bitcoin Charts: Exchange rate Dollar/Bitcoin MtGox from 2010 to 2013. URL: http://bitcoincharts.com/charts/mtgoxUSD#tgSzm1g10zm2g25zv. 2013-11-18.

Bitcoin Clock: Bitcoin Clock. URL: http://bitcoinclock.com/. 2013-10-28.

Bitcoin Co Ltd.: Trading suspended due to Bank of Thailand advisement. URL: https://bitcoin.co.th/trading-suspended-due-to-bank-of-thailand-advisement/. 2013-11-18.

Bitcoin Developers: Bitcoin Source Code on github. URL: https://github.com/bitcoin/bitcoin. 2013-10-02.

Bitcoin Faucet: Bitcoin Faucet. URL: http://freebitcoins.appspot.com/. 2013-10-23.

Bitcoin Foundation: Bitcoin Foundation - Developing a More Open Economy. URL: https://bitcoinfoundation.org/about/. 2013-10-23.

Bitcoin Org: 11/12 March 2013 Chain Fork Information. URL: http://bitcoin.org/chainfork.html. 2013-11-14.

Bitcoin Project: Bitcoin.org Download. URL: http://bitcoin.org/de/download. 2013-10-10.

Bitcoin Project: Bitcoin.org FAQ. URL: http://bitcoin.org/en/faq. 2013-10-02.

Bitcoin Project: Securing your wallet. URL: http://bitcoin.org/en/secure-your-wallet. 2013-10-12.

Bitcoin Stackexchange: Is there a Bitcoin bank, which gives interest on my deposit?. URL: http://bitcoin.stackexchange.com/questions/1426/is-there-a-bitcoin-bank-which-gives-interest-on-my-deposit. 2013-10-08.

Bitcoin Stackexchange: Tagged Questions: Genisis Block. URL: http://bitcoin.stackexchange.com/questions/tagged/genesis-block. 2013-10-03.

Bitcoin Wiki: Bitcoin - Transaction. URL: https://en.bitcoin.it/wiki/Talk:Transactions. 2013-10-23.

Bitcoin Wiki: Browser-based wallet. URL: https://en.bitcoin.it/wiki/EWallet. 2013-11-14.

BitcoinIT: Handel. URL: https://de.bitcoin.it/wiki/Handel. 2013-10-31.

Bitcoincharts: Bitcoin Markets Overview. URL: http://bitcoincharts.com/markets/. 2013-11-14.

Bitcoinfees: Bitcoin Transaction Fees Explained. URL: http://bitcoinfees.com/. 2013-10-23.

Blockchain Explorer: Block 0. URL: https://blockexplorer.com/block/000000000019d6689c085ae165 2013-10-03.

Blockchain Explorer: Block 210000. URL: https://blockexplorer.com/block/000000000000048b95347 2013-10-28.

Breuker, J. B. D.; Heide, T.; et al.: Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency. Westfälische Wilhelms-Universität: 2012.

Bundesrepublik Deutschland: Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten. Bundesministerium der Justiz: 2008.

Bundesrepublik Deutschland: Gesetz über die Deutsche Bundesbank. Bundesministerium der Justiz: 2013.

Buterin, V.: Bitcoin private key splittern. URL: https://github.com/vbuterin/btckeysplit. 2013-10-12.

Caldwell, M.: Physical Bitcoins by Casascius. URL: https://www.casascius.com/. 2013-10-08.

Chaum, D.: Blind Signatures for blind payment. Department of Computer Science, University of California, Santa Barbara: 1982.

Chaum, D.; Fiat, A.; Naor, M.: Untraceable Electronic Cash. Center for Mathematics und Computer Science - Netherland, Tel-Aviv University - Israel, IBM Almaden Research Center - USA: Amsterdam, Tel-Aviv, San Jose 1990.

Chen, A.: The Underground Website Where You Can Buy Any Drug Imaginable. URL: http://kotaku.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160. 2013-10-31.

Christin, N.; Brito, J.: Suprisingly free, Nicolas Christin on anonymous online market Silk Road. URL: https://cdn-surprisinglyfree.s3.amazonaws.com/SFC-125-120822.mp3. 2013-10-08.

Collier, M.: Linux Virtual Machine for Windows Bitcoin Users. URL: https://bitcointalk.org/index.php?topic=9937.0. 2013-10-12.

Cypherpunks: Cypherpunks Mailing List Remailers. URL: http://www.cypherpunks.to/remailers/. 2013-10-03.

Cypherpunks: Cypherpunks Mailing List Webseite. URL: http://www.cypherpunks.to/list/. 2013-10-03.

Dai, W.: A scheme for a group of untraceable digital pseudonyms to pay each other with money and to enforce contracts amongst themselves without outside help. URL: http://www.weidai.com/bmoney.txt. 2013-10-03.

Davis, J.: The Crypto-Currency. The New Yorker: New York 2011.

Dice Holdings Inc.: Sourceforg About. URL: http://sourceforge.net/about. 2013-10-03.

Eckert, D.: Wie Berlin zur weltweiten Bitcoin-Hauptstadt wurde. URL: http://www.welt.de/finanzen/geldanlage/article119820142/Wie-Berlin-zur-weltweiten-Bitcoin-Hauptstadt-wurde.html. 2013-10-31.

Eclipsemc: Eclipse Mining Consortium. URL: https://eclipsemc.com/. 2013-11-14.

Eikenberg, R.: Silk Road: FBI schaltet Drogen-Handelsplattform im Tor-Netz aus. URL: http://www.heise.de/security/meldung/Silk-Road-FBI-schaltet-Drogen-Handelsplattform-im-Tor-Netz-aus-1972026.html. 2013-10-16.

Flaskämper, O.: Bitcoin-Marktplatz - Made in Germany. URL: https://www.bitcoin.de/de. 2013-10-08.

Flexicon Bank: Flexcoin the bitcoin bank. URL: http://www.flexcoin.com/. 2013-10-08.

Flexicon Bank: Flexcoin the bitcoin bank. URL: http://www.flexcoin.com/103.html. 2013-10-08.

Friedman, M.: Bits and bob. The Economist: 2011.

Godbole, A.; Kahate, A.: Web Technologies: TCP/IP to Internet Application Architectures. 1st, Tata McGraw-Hill Education: 2003.

Google Inc.: Google Trend: Bitcoin. URL: http://www.google.co.uk/trends/explore?q=Bitcoin#q=Bitcoin&cmpt=q. 2013-10-03.

Google Inc.: Starkes Passwort erstellen. URL: https://support.google.com/accounts/answer/32040?hl=de. 2013-10-12.

Kaminsky, D.: Black Ops of TCP/IP Presentation. Black Hat Chaos Communication Camp: 2011.

Kannenberg, A.: Erster Bitcoin-Geldautomat in den USA ausgeliefert. URL: http://www.heise.de/newsticker/meldung/Erster-Bitcoin-Geldautomat-in-den-USA-ausgeliefert-1954415.html. 2013-10-12.

Kolivas, C.: cgminer: ASIC / FPGA / GPU miner in c for bitcoin and litecoin. URL: https://github.com/ckolivas. 2013-10-28.

Küsters, R.; Wilke, T.: Moderne Kryptographie. Vieweg Verlag, Friedr, & Sohn Verlagsgesellschaft mbH: Wiesbaden 2011.

Lerner, S.: The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius. URL: https://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/. 2013-11-18.

Leyden, J.: How mystery DDoSers tried to take down Bitcoin exchange with 100Gbps crapflood. URL: http://www.theregister.co.uk/2013/10/17/bitcoin_exchange_ddos_flood/. 2013-11-19.

Litecoin Project: Litecoin Project. URL: https://litecoin.org/. 2013-10-02.

Luke-Jr: bfgminer: Modular ASIC/FPGA miner written in C, featuring overclocking, monitoring, fan speed control and remote interface capabilities. URL: http://freebitcoins.appspot.com/. 2013-10-28.

Maas, F.: Anklageschrift gegen Ross Wiliam Ulbricht. United States of America: 2013.

Merchant, B.: This Pizza Cost 750.000 Dollar. URL: http://motherboard.vice.com/blog/this-pizza-is-worth-750000. 2013-10-03.

Miers, I.: Zerocoin Project. URL: http://zerocoin.org/. 2013-10-02.

MultiBit: MultiBit Bitcoin Client. URL: https://multibit.org/. 2013-10-10.

Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org: 2008.

Nakamoto, S.: Bitcoin P2P e-cash paper. URL: http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html. 2013-10-03.

Nakamoto, S.: Re: Bitcoin v0.1 released. URL: http://www.mail-archive.com/cryptography@metzdowd.com/msg10152.html. 2013-10-03.

New Liberty Standard: 2009 Exchange Rate. URL: http://newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate. 2013-10-10.

PayPal: PayPal: Gebühren. URL: https://www.paypal.com/de/webapps/mpp/gebuehren. 2013-10-23.

Paymium: Bitcoin Central Webseite. URL: https://bitcoin-central.net/. 2013-10-10.

Peck, M.: Bitcoin: The Cryptoanarchists' Answer to Cash - How Bitcoin brought privacy to electronic transactions. URL: http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/0. 2013-10-03.

Qkos Services Ltd.: Blockchain Größe. URL: http://blockchain.info/charts/blocks-size. 2013-10-10.

Qkos Services Ltd.: Marktkapitalisierung Bitcoin. URL: http://blockchain.info/de/charts/market-cap. 2013-10-04.

Reid, F.; Harrigan, M.: An Analysis of Anonymity in the Bitcoin System. Clique Research Cluster, University College Dublin, Ireland: Dublin 2011.

Reiner, A.: Multi-Sig Transaction Distribution. URL: https://en.bitcoin.it/wiki/BIP_0010. 2013-10-12.

Rosenfeld, M.: Analysis of Bitcoin Pooled Mining Reward Systems: 2011.

Schollmeier, R.: A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications. Institute of Communication Networks, Technische Universität München: 80333 München, Germany 2002.

Sharwood, S.: DDOS strikes BitCoin exchange Mt.Gox. URL: http://www.theregister.co.uk/2013/04/22/mtgox_ddos/. 2013-11-19.

Spend Bitcoins: Places to Spend Bitcoins - Places that Accept Bitcoins Directly. URL: https://www.spendbitcoins.com/places/. 2013-10-31.

Spiegel: Wachsender Druck: Paypal stoppt Geldfluss an WikiLeaks. URL: http://www.spiegel.de/netzwelt/netzpolitik/wachsender-druck-paypal-stoppt-geldfluss-an-wikileaks-a-732856.html. 2013-10-23.

Szabo, N.: Bit gold. URL: http://unenumerated.blogspot.de/2005/12/bit-gold.html. 2013-10-03.

Taylor, M.: Bitcoin and The Age of Bespoke Silicon. University of California, San Diego: 2013.

Wallace, B.: The Rise and Fall of Bitcoin. URL: http://www.wired.com/magazine/2011/11/mf_bitcoin/all/2013. 2013-10-03.

WikiLeaks: WikiLeaks Tweet über Bitcoin Spenden. URL: https://twitter.com/wikileaks/status/80774521350668288?_escaped_fragment_=/wikileaks/status/80774521350668288#!/wikileaks/status/80774521350668288. 2013-10-03.

Wikipedia: Quelltext. URL: https://de.wikipedia.org/wiki/Quelltext. 2013-10-02.

Wolf, B.: Senators seek crackdown on "Bitcoin"currency. URL: http://www.reuters.com/article/2011/06/08/us-financial-bitcoins-idUSTRE7573T320110608. 2013-11-18.

Zerlan, J.: 22 June 2013 - ASIC Update. URL: https://forums.butterflylabs.com/announcements/692-bfl-asic-status-3.html. 2013-11-14.

theymos: Earliest Block With A Spend. URL: http://bitcointalk.org/index.php?topic=91806.msg1012234#msg1012234. 2013-10-03.

Šurda, P.: Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold?. WU Vienna University of Economics und Business: Wien 2012.