Fachhochschule Wedel
Seminararbeit

Fachrichtung Wirtschaftsinformatik (Bachelor)

Seminar IT-Sicherheit

Thema:

Bitcoin
eine anonyme und digitale Währung

Wintersemester 2012/2013

Eingereicht von: *Tobias Krebber*

Matr.Nr.: winf9255

Email: winf9255@fh-wedel.de

Seminarleiter: *Prof. Dr. Gerd Beuster*

0 Inhalt

0 Inhalt ..... **II**

1 Einleitung **1**

2 Das Konzept **2**

3 Technisches Design **3**

3.1 Der Client **3**

3.2 Coins und Transaktionen **4**

3.2.1 Aufbau 4

3.2.2 Ablauf 5

3.2.3 Signieren von Transaktionen 6

3.3 Proof of Work **8**

3.3.3 Bitcoin Mining 8

3.3.3.1 Timestamp 9

3.3.3.2 Der Block 9

3.3.3.3 Die Aufgabe 10

3.3.3.4 Bestätigung von Transaktionen 11

3.3.3.5 Transaktionsgebühr 12

2.3.3.6 Motivation 12

3.3.3.7 Zeitgleiches lösen 13

4 Sicherheit **14**

4.1 Angriff auf die Block-Chain **14**

4.2 Angriff auf den Client **14**

4.3 Angriff auf die wallet.dat **15**

4.4 Angriff auf SHA256 ..... **15**

4.5 Ist Bitcoin also sicher? **15**

5 Anonymität 16

6 Rechtliche und wirtschaftliche Aspekte 17

6.1 Rechtliche Sicht 17

6.2 Wirtschaftliche Sicht 18

7 Fazit 19

8 Quellenverzeichnis i

9 Abbildungsverzeichnis ii

1 Einleitung

Eine Welt ohne elektronischen Zahlungsverkehr wäre heutzutage kaum noch vorstellbar. Jeder nutzt und vertraut in Überweisungen per Online-Banking, Kreditkarten und Lastschriftverfahren – Bargeld verliert dabei immer mehr an Bedeutung. Neben den gängigen Zahlungsmethoden entwickeln sich immer mehr neue Dienste für die schnelle, online-basierte Bezahlung. PayPal, ClickAndBuy und die Paysafecard sind nur einige von vielen Beispielen dafür. Aber in Zeiten von ständigen Finanzkrisen und Staatsbankrotte offenbart sich eine ganz entscheidende Schwäche dieser Konzepte: Sie alle basieren auf bereits existierenden Währungen und stellen als Service lediglich einen alternativen Zahlungsverkehr bereit. Deshalb ist es nicht verwunderlich, dass es auch Konzepte von Zahlungssystemen gibt, die sich nicht direkt mit etablierten Währungen befassen und eigene Wege finden, um Werte zu „generieren". Solche Systeme wären unberührt von staatlichen Einflüssen und Währungskrisen. Gerade bei einem so sensiblen Thema wie Geld ist es besonders interessant, ob es eine technische Implementierung schafft, genug Sicherheit und damit auch Vertrauen zu schaffen, um ein valider Ersatz für bestehende Währungen zu sein. Dafür muss das System Eigenschaften wie Fälschungssicherheit, Vertrauenswürdigkeit und Seltenheit bieten, die wir von unseren bestehenden Währungen gewohnt sind.

Ein beachtenswerter Vorschlag dazu wurde im Jahre 2008 von Satoshi Nakamoto gemacht. In seinem Whitepaper „Bitcoin: A peer to peer electronic cash system"[Q7] stellt er ein Konzept vor, um eine neue, digitale Währung zu realisieren. Ich werde in meiner Ausarbeitung dieses Konzept näher vorstellen und einen Überblick über die Implementierung, Sicherheitsaspekte und Anonymität des Bitcoin-Universums geben, welches seit 2009 existiert und genutzt wird. Außerdem soll geklärt werden, in welchem rechtlichen Kontext Bitcoin steht und welche wirtschaftliche Bedeutung das System hat.

2 Das Konzept

Hinter Bitcoin steht die Idee, ein anonymes Zahlungssystem mit eigener Währung zu entwickeln, welches komplett ohne eine dritte Instanz auskommt. Mit einer dritten Instanz ist hierbei beispielsweise eine Bank gemeint, die eine Zahlung abwickelt. Diese dritte Instanz hat bei unseren gewöhnlichen Zahlungssystemen jedoch eine entscheidende Funktion: Sie garantiert die Vertrauenswürdigkeit der einzelnen Zahlungspartner, in dem sie einerseits Zahlungen rückgängig machen kann oder, wie bei Kreditkarten, die Zahlungsfähigkeit eines Zahlungspartners gewährleistet. Bei Bitcoin soll diese Vertrauenswürdigkeit nicht durch eine Institution, sondern durch kryptografische Verfahren sichergestellt werden[Q7, S. 1]. Transaktionen werden von den Nutzern digital signiert, um die Echtheit der Zahlungen zu gewährleisten. Außerdem werden alle Transaktionen ans Netzwerk öffentlich gemacht, damit diese von anderen Nutzern geprüft und bestätigt werden können. Allerdings bleiben die Nutzer Anonym, es existiert lediglich eine öffentliche Adresse, der Public Key, mit dem ein Nutzer identifiziert wird[Q3, S. 11]. Abgeschlossene Transaktionen werden dann durch den Einsatz von Rechenleistung abgespeichert und vor nachträglicher Änderung geschützt. Außerdem sind Transaktionen unumkehrbar, was zur Folge hat, dass der Empfänger einer Zahlung diese auch sofort für sich verbuchen kann, ohne eine Stornierung fürchten zu müssen[Q7, S. 1]. Alle diese Faktoren sollen es möglich machen, eine sichere und Vertrauenswürdige Zahlungsumgebung zu schaffen, in der die Benutzer dank der Sicherheit der kryptografischen Verfahren problemlos und ohne Bedenken agieren können.

3 Technisches Design

Es sind viele Komponenten nötig, um eine elektronische Währung inklusive Unterstützung des Zahlungsverkehrs zu realisieren. Die Teilnehmer des Netzwerkes müssen die Möglichkeit haben, zu interagieren, es muss definiert werden, wie sich ein „Coin" zusammensetzt und die nötige Sicherheit muss gewährleistet werden. Außerdem muss der Wert der Währung durch künstliche Knappheit generiert werden. Im Folgenden sollen die unterschiedlichen Komponenten und Systeme vorgestellt werden, die im heutigen Bitcoin System zum Einsatz kommen.

3.1 Der Client

Jeder, der Bitcoins zum Bezahlen einsetzen und Teil des Bitcoin Netzwerkes werden möchte, kann dies ganz einfach tun. Dazu muss nur die entsprechende Software runtergeladen werden (z.B. auf www.bitcoin.org). Die Software stellt einen Client zur Verfügung, über den mit dem Netzwerk interagiert werden kann.

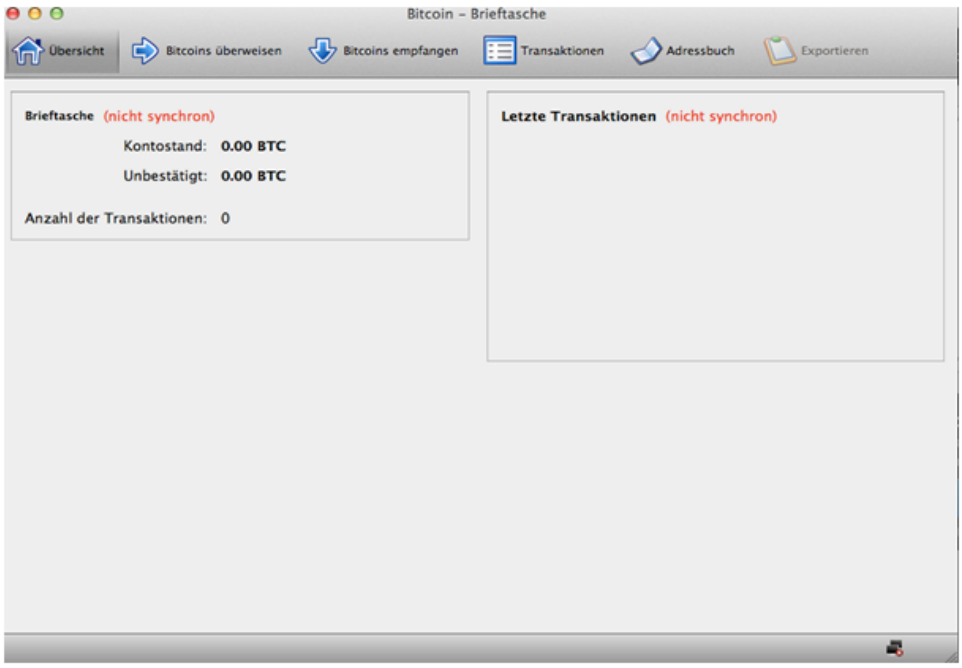

Abbildung 1: Bitcoin Client

Der installierte Client legt gleichzeitig die Daten an, die für die Abwicklung einer Transaktion von Nöten sind. Diese sind in der Datei „wallet.dat” gebündelt, die hierbei, wie der Name schon verrät, wie eine Art Brieftasche fungiert. In der Datei befinden sich die Bitcoin Adresse, unter der der jeweilige Teilnehmer adressierbar ist, der Private Key, mit dem Transaktionen signiert werden (Siehe 3.2.3) und eine Liste mit allen Transaktionen, die bisher im Bitcoin-Netzwerk abgewickelt wurden[Q3, S. 11]. Die Bitcoin Adresse, auch Public-Key genannt, fungiert hierbei ähnlich wie eine Kontonummer.

3.2 Coins und Transaktionen

Bitcoin werden zwar in der Einheit BTC ausgewiesen, eine einzelne „Coin”, im Sinne einer isolierten Einheit, wie wir sie vom Bargeld kennen, existiert aber nicht. Vielmehr dienen einzelne Transaktionen dazu, darzustellen, wer gerade wie viele Bitcoins besitzt[Q3, S. 12]. Alle Transaktionen, die im Netzwerk stattfinden, werden öffentlich gemacht[Q7, S. 2]. So ist für jeden nachweisbar, ob er über die entsprechende Menge an Bitcoins, die er gerade überweisen möchte, auch wirklich verfügt. Dies wird anhand der Bitcoin Adresse des jeweiligen Clients ausgewiesen, einen Namen oder eine postale Adresse gibt es nicht. Die Besitzverhältnisse sind also dezentral im Netzwerk gespeichert.

3.2.1 Aufbau

Eine Transaktion hat immer ein oder mehrere Inputs und einen oder mehrere Outputs. Der Input wird gespeist von den Outputs ein oder mehrerer vorhergegangener Transaktionen. Die Inputs einer Transaktion können auch in mehrere Outputs aufgeteilt werden. So ist es z.B. möglich Beträge zu überweisen, die nicht exakt dem Output einer vorherigen Transaktion entsprechen. Das geschieht, in dem man beispielsweise einen Output von 20 BTC so aufteilt, dass 10 BTC an einen anderen Teilnehmer überwiesen werden und 10 BTC an den Ersteller selber. So gibt man sich gewissermaßen selbst Wechselgeld[Q3, S.12ff]. Dazu ein kurzes Beispiel:

3.2.2 Ablauf

In dem nun folgenden Beispiel soll deutlich werden, wie eine Transaktion ablaufen kann.

Es gibt 2 Transaktionen, die an Alice adressiert sind:

Transaktion 1	Output: 2 BTC
Transaktion 2	Output: 3 BTC

Abbildung 2: Transaktionen, die an Alice adressiert sind

Alice ist also momentan stolze Besitzerin von 5 BTC. Nun hat Alice sich auf einer seriös anmutenden Homepage von Bob Stricksocken bestellt und möchte diese via Bitcoin bezahlen. Die Socken kosten 2,50 BTC. Die neue Transaktion (Transaktion 3), die Alice nun an Bob sendet, sieht also vereinfacht folgendermaßen aus:

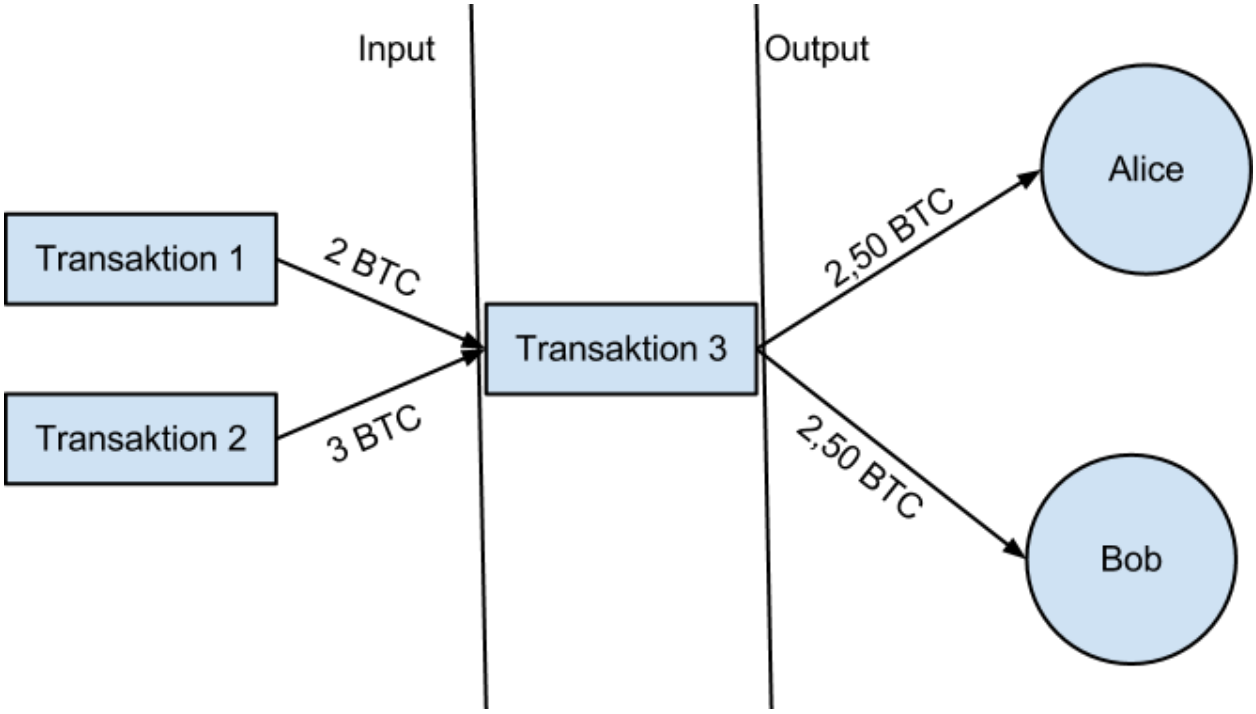

Abbildung 3: Schematischer Aufbau einer Transaktion

Am Ende ist Bob also um 2,50 BTC reicher und Alice bleiben noch 2,50 BTC übrig. Transaktion 1 und Transaktion 2 sind vollständig aufgebraucht und werden in Zukunft nicht mehr als Inputs akzeptiert werden.

Es gilt:

$$\sum_{i=1}^{\#Inputs} Wert(Input_i) \geq \sum_{j=1}^{\#Outputs} Wert(Output_j)$$

Übersteigt der Input den Output, wird die Differenz als Transaktionsgebühr eingesetzt (Siehe 3.3.3.5). Wie man sieht, wird somit eine Transaktion, die zum Bezahlen benutzt wird, stets vollständig aufgebraucht[Q2].

3.2.3 Signieren von Transaktionen

Doch wie kann Bob nun sicher sein, dass Alice die Transaktionen 1 und 2 auch wirklich besitzt, bzw. dass sie auf wirklich über die BTC verfügt, die sie ihm überweist?

Hier kommen der Private- und der Public-Key aus der „wallet.dat" zum Einsatz. Jeder User, der eine Transaktion erstellt, erstellt zunächst einen Hash-Wert mittels SHA256, für den er als Input den Public-Key des Empfängers so wie die Hash Werte der vorangegangenen Transaktionen verwendet. Dann signiert er diesen mit seinem Private-Key via ECDSA Verschlüsselung[Q3, S. 18]. Ist der Signierende der rechtmäßige Empfänger der vorhergegangenen Transaktionen, so lässt sich dies mittels seines Public-Key, der, wie der Name schon sagt, öffentlich ist, ganz leicht verifizieren. Eine Transaktion, die durch den Public-Key des agierenden Users nicht verifizierbar ist, würde von keinem Teilnehmer des Netzwerkes akzeptiert werden.

Um den Ablauf inklusive Signierung besser zu verstehen, betrachten wir noch einmal das Beispiel aus 3.2.2:

Es seinen $N = \{A, B\}$ die Nutzer Alice und Bob. Alice verfügt über die Transaktionen $T_A = \{t_1, t_2\}$ wobei gilt:

$$OUTPUT(t_1) = 2 \ \wedge OUTPUT(t_2) = 3.$$

Diesmal möchte Alice Bob nur 2 BTC überweisen. Dafür kann sie t_1 verwenden, da diese ja genau einen Output von 2 BTC hat. Zuerst wird also der Hash Wert für die neue Transaktion berechnet:

$$H_{neu} = SHA256(H_{alt}, k_b P)$$

Wobei $k_b P$ der Public-Key von Bob ist. Jetzt signiert Alice diesen Wert mit ihrem Private-Key und erstellt so die Signatur:

$$S = \ ECDSA_{sign}(k_a X, H_{neu})$$

Wobei $k_a X$ der Private-Key von Alice ist. Bob kann nun ganz einfach verifizieren, ob Alice befugt ist, die Transaktion durchzuführen. Dazu muss gelten:

$$ECDSA_{check}(k_a P, S) = \mathrm{T}$$

Diese Notation ist jedoch stark vereinfacht und soll nur den groben Ablauf darstellen. Bitcoin verwendet zur Verifikation ein selbst entwickeltes Skript[Q3, S. 42]

Schematisch lässt sich dieses Vorgehen folgendermaßen darstellen (unabhängig von dem eben genannten Beispiel):

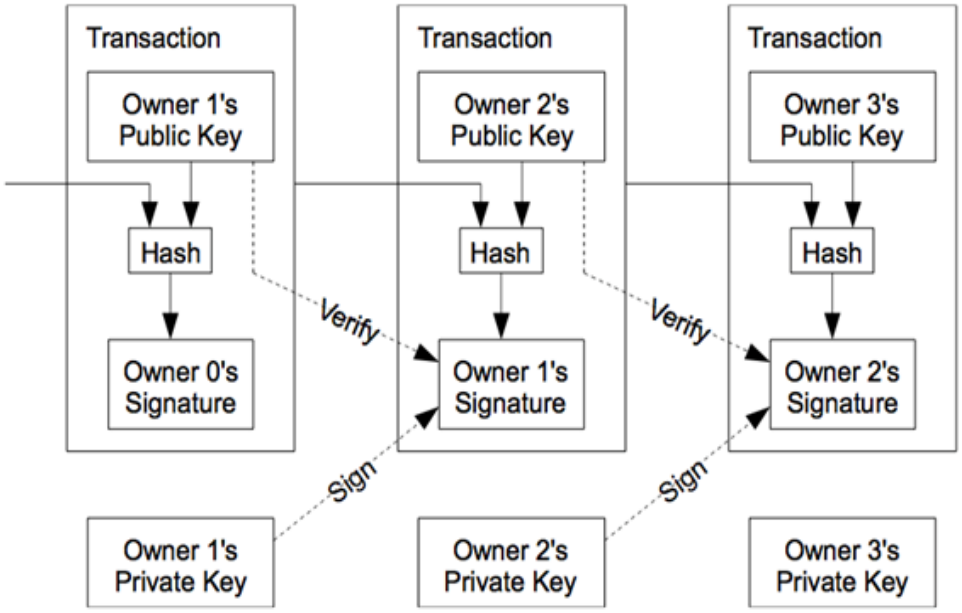

Abbildung 4: Verifizierung von Transaktionen

3.3 Proof of Work

Auch wenn die Signaturen verhindern, dass illegale Transaktionen vorgenommen werden können, so kann der Empfänger jedoch bisher nicht sicher sein, dass die entsprechenden Bitcoins nicht zeitgleich auch an jemand Anderen überwiesen werden. Um diese Problematik der Mehrfachüberweisungen („Double Spending")[Q7, S. 2] in den Griff zu bekommen, gibt es im Bitcoin Netzwerk das so genannte „Proof of Work System"[Q7, S. 3]. Es löst nicht nur das Problem des Double Spending, sondern stellt gleichzeitig eine Möglichkeit dar, um neue Bitcoins zu generieren.

3.3.3 Bitcoin Mining

Jeder User hat die Möglichkeit, mit Hilfe der passenden Software neue Bitcoins zu „erstellen", das so genannte Bitcoin Mining[Q3, S. 11]. Was so vielversprechend klingt bedeutet eigentlich nur, dass mit Hilfe der Rechenkapazität des ausführenden Rechners versucht wird, eine bestimmte Aufgabe zu lösen. Im Folgenden werden die essentiellen Punkte und der Ablauf des Minings verdeutlicht.

3.3.3.1 Timestamp

Um das Double Spending zu verhindern, wurde für Transaktionen allgemein festgelegt, dass die zuerst bestätigte Transaktion die gültige ist. Alle späteren Transaktionen, die den selben Output als Input nutzen, werden ignoriert und als ungültig betrachtet. Deshalb ist es nötig, die Transaktionen mit einem Timestamp zu versehen, der diese Invariante sicherstellt[Q7, S. 2].

3.3.3.2 Der Block

Teilnehmer, die versuchen, die aktuelle Aufgabe zu lösen, erstellen dabei einen Block, der wie folgt aufgebaut ist:

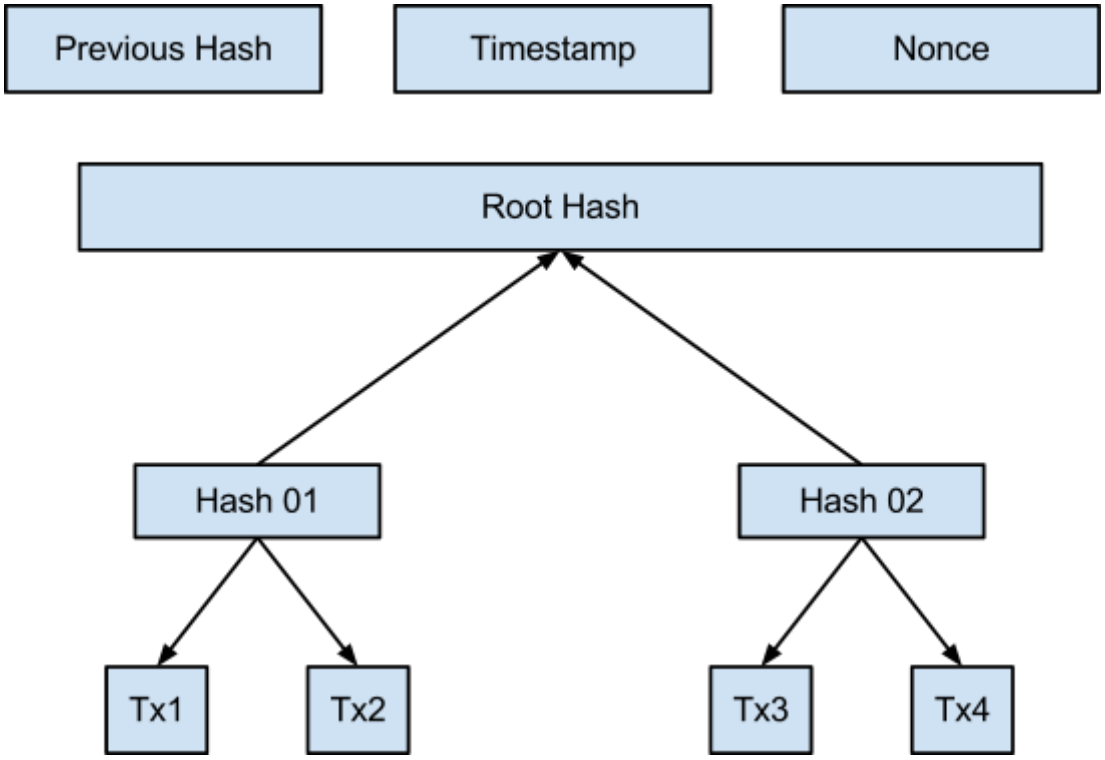

Abbildung 5: Vereinfachter Aufbau eines Blocks

Der Block enthält in seinem Header den geforderten Timestamp. Zusätzlich ist eine Referenz auf den vorherigen Block vorhanden (Previous Hash), so dass aus den Böcken eine Kette, die so genannte Block-Chain entsteht. In der Block-Chain sind alle Transaktionen enthalten, die jemals im Netzwerk getätigt wurden[Q3, S. 11].

Um eine Transaktionen mit einem Timestamp in Verbindung zu bringen, sind alle Transaktionen, die bis zum Zeitpunkt der Blockerstellung vom Blockersteller als gültig akzeptiert wurden und alle, die schon im vorherigen Block enthalten waren, in einem HashTree abgespeichert. Das Feld Nonce ist relevant für das Lösen der Aufgabe.

3.3.3.3 Die Aufgabe

Die angesprochene Aufgabe besteht in diesem Kontext daraus, mittels zweifacher SHA256-Berechnung[Q4] den Block-header so zu hashen, dass der resultierende Wert unterhalb eines bestimmten Grenzwertes, dem Target[Q3, S. 13] liegt. Da dies beim Hashen durch eine Einwegfunktion geschieht, kann die Aufgabe nur durch ausprobieren gelöst werden und ist dementsprechend rechenaufwändig. Für das Hashing werden hierbei folgende Werte als Input verwendet:

Feld	**Bedeutung**	**Wird verändert wenn...**	**Größe(Bytes)**
Version (v)	Versionsnummer des Blockes	...eine neue Version vom Client spezifiziert wird	4
Previous Hash (p)	Hash-Wert des vorangehenden Blockes	...ein neuer Block berechnet wurde	32
Root Hash (r)	Wurzel des Transaktionsbaumes	...eine neue Transaktion akzeptiert wird	32
Timestamp (d)	Zeit- und Datumsstempel	...die Zeit voranschreitet	4
Target (t)	Zielwert der Berechnung	...das Target vom System angepasst wurde	4
Nonce (n)	Numerisches Feld, das beliebig geändert werden kann	...ein Wert berechnet wurde, der oberhalb des Targets liegt	4

Abbildung 6: Input für die SHA256 Berechnung

Es muss also gelten:

$$SHA256\big(SHA256(v,p,r,d,t,n)\big) < t$$

Das aktuelle Target wird automatisch vom System so angepasst, dass im Schnitt alle 10 Minuten ein neuer Block „gelöst" wird.[Q3, S. 13] In dem Block ist die Nonce das einzige Feld, welches keine tiefere Bedeutung besitzt, jedoch genutzt werden kann, um den resultierenden Hash-Wert zu verändern. Da die Nonce allerdings nur eine Größe von 32 Bit hat und deshalb nach kurzer Zeit vollständig abgetastet ist, müssen auch noch andere Daten des Block Headers verändert werden, um den Block zu lösen. Hierzu bietet sich natürlich zum einen der Timestamp an, da er sich während der Berechnung logischerweise mit fortschreitender Zeit von selbst verändert. Außerdem können andere Transaktionen bestätigt und in den Block eingebaut werden, wodurch der Root Hash verändert wird[Q4]. Sobald ein Teilnehmer einen neuen Block gefunden hat, wird dieser im gesamten Netzwerk verbreitet[Q7, S. 3], damit er von den anderen Nutzern validiert und als neuer Previous Hash verwendet werden kann.

3.3.3.4 Bestätigung von Transaktionen

Wenn eine Transaktion erstellt wird, wird diese sofort allen Teilnehmern des Netzes mitgeteilt[Q7, S. 2]. Ein Teilnehmer, der gerade einen Block bearbeitet, kann diese Transaktion nun mittels des in 3.2.3 erläuterten Verfahrens verifizieren. Ist die Transaktion gültig, so baut er sie in den Transaktionsbaum seines Blockes ein, was ihm zusätzlich ein weiteres Spektrum an Lösungswerten für das SHA-256 Hashing eröffnet. Gleichzeitig trägt der Ersteller des Blockes dazu bei, dass Transaktionen im Netzwerk abgewickelt werden. Denn eine Transaktion wird dann von einem Empfänger akzeptiert werden, wenn diese in möglichst vielen Blöcken bestätigt wurde. Deshalb können Überweisungen mit höheren Beträgen eventuell länger dauern, da das Bedürfnis nach möglichst vielen Bestätigungen bei solchen Beträgen natürlich größer ist[Q10, S. 4].

3.3.3.5 Transaktionsgebühr

Beim Anlegen einer neuen Transaktion wird gleichzeitig festgelegt, mit welcher Transaktionsgebühr die Transaktion belegt werden soll. Diese Gebühr ist dabei nicht zwingend erforderlich, sie beschleunigt jedoch die Bestätigung der Transaktion. Denn je höher die Transaktionsgebühr ist, desto eher wird ein anderer Nutzer diese verifizieren und in seinen Block einbauen. Da alle ~10 Minuten ein neuer Block berechnet wird, ist es natürlich erstrebenswert, seine Transaktion sofort in den nächsten Block zu bringen, damit diese in den darauf folgenden Blöcken automatisch einbezogen wird[1].

2.3.3.6 Motivation

Aber wo liegt die Motivation, Zeit und vor allem die nötige Energie(→Strom) in eine solche Berechnung zu stecken? Die Hauptmotivation liegt darin, wie bereits angesprochen, neue BTC zu erhalten. Denn wer einen Block löst, der darf an den Beginn des Transaktionsbaumes eine neue Transaktion auf sich selber setzen, in der die entsprechende Belohnung überwiesen wird. Momentan liegt diese bei 25 BTC[Q3, S. 35] (momentan ca. 2000€) , was eine nicht zu vernachlässigende Summe ist. Allerdings wird dieser Betrag alle 4 Jahre automatisch halbiert, so dass die Menge an möglichen Bitcoins auf lange Sicht bei 21 Millionen BTC stagnieren wird[Q3, S. 10]. Zusätzlich zu dieser Summe, erhält der Lösende auch noch die Transaktionsgebühren der bestätigten Transaktionen. Da die Menge an Bitcoins, die man für das Lösen eines Blockes erhält langfristig bei Null ankommen wird, sollen die Transaktionsgebühren als Langzeitmotivation dienen[Q7, S. 4]. Ob sich irgendwann die Kosten des Minings (Strom und Hardware) überhaupt noch rechnen, ist eine andere Frage und wird wohl zukünftig zum Problem für

[1] Wurde ein Block als gültig befunden, werden alle Transaktionen aus diesem Block in den nächsten übernommen[Q4]. Ein Block, der ungültige Transaktionen enthält, würde vom Netzwerk ebenfalls als ungültig befunden werden.

Bitcoin werden. Eine Lösung dafür sind so genannte „Mining Pools“, bei denen mehrere Teilnehmer gemeinsam Rechenkapazität investieren und die erwirtschaftetet BTC am Ende untereinander aufteilen. Auf diese Art und Weise haben auch Nutzer mit verhältnismäßig schwachen Rechnern die Möglichkeit, BTC zu erstellen, auch wenn der Gewinn natürlich wesentlich kleiner ausfällt[Q3, S. 31].

3.3.3.7 Zeitgleiches lösen

Doch was passiert nun, wenn ein Block gelöst wurde, jedoch andere Teilnehmer noch dabei sind, ebenfalls diese Aufgabe zu lösen und es eventuell auch schaffen? In solchen Fällen, in denen es mehrere Referenzen auf einen vorherigen Block gibt, wird immer die längste Block-Chain als gültig befunden. Die Teilnehmer, die einen Block also zu spät lösen, bekommen leider keine Belohnung in Form von BTC, da ihre Transaktion auf Grund der fehlenden Aktualität nicht akzeptiert werden würde. Die Problematik wird darüber hinaus dadurch entschärft, dass ein gelöster Block sofort ans ganze Netzwerk verbreitet wird. Befinden die anderen Teilnehmer diesen für gültig, werden sie sofort anfangen, mit dem Hash Wert des neuen Blocks weiterzurechnen, um die Block-Chain fortzuführen und sich nicht länger mit dem alten Block befassen[Q3, S. 14].

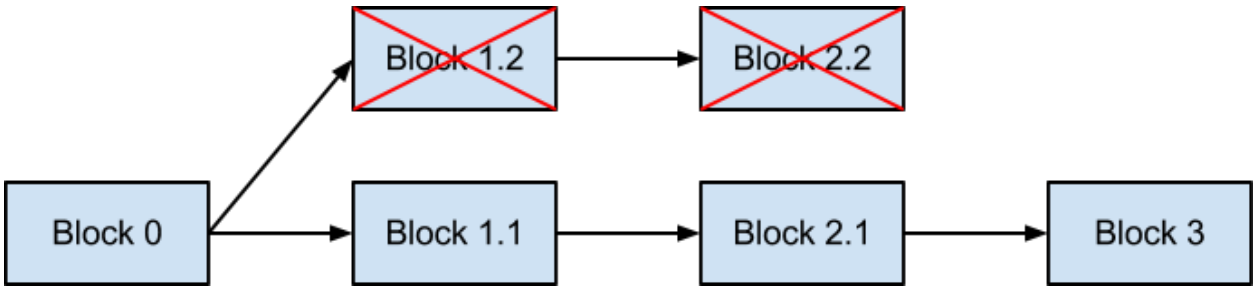

Abbildung 7: Beispielhafter Aufbau einer Block-Chain

Abbildung 6 zeigt ein Beispiel, wie ein solches „doppeltes Lösen“ aussehen kann. In diesem Fall würde die Transaktionen aus Block 1.2 und 2.2 nicht akzeptiert werden (außer natürlich sie tauchen in den gültigen Blöcken auf). Auch die Ersteller dieser beiden Blöcke würden leer ausgehen[Q3, S. 14].

4 Sicherheit

Nach der Betrachtung der Implementierung stellt sich nun natürlich die Frage, wie sicher das System ist und was potentielle Angriffsflächen und Schwachstellen sind. Gerade Bezahlsysteme sind, die vor allem auf das Vertrauen der Nutzer angewiesen sind, sind immer nur so populär, wie sie auch sicher sind. Im Folgenden sollen mögliche Angriffsvektoren dargestellt werden.

4.1 Angriff auf die Block-Chain

Bei der Suche nach möglichen Angriffsflächen fällt der Blick natürlich schnell auf die Transaktionen und die Block Chain. So wäre es zum Beispiel denkbar, einen manipulierten Block in die Kette einzuschleusen und sich somit unrechtmäßig Bitcoins zuzuweisen oder sich als Ersteller des Blockes auszugeben. Dieser Gedanke ist möglich, allerdings ist es dafür für den Angreifer nötig, eine deutlich höhere Rechenkapazität als das restliche Bitcoin-Netzwerk aufzubringen. Denn wird auch nur ein Block manipuliert, so müssen alle folgenden Blöcke neu berechnet werden, da diese ja eine Referenz auf den vorhergegangenen Block enthalten. Solange die größte Rechenkapazität von ehrlichen Nutzern bereitgestellt wird, hat ein Angreifer also keine Chance, eine Neuberechnung der Blöcke durchzuführen. Schließlich rechnet das Netzwerk kontinuierlich weiter und müsste vom Angreifer auch noch überholt werden, da ja nur die längste Block-Chain als gültig akzeptiert wird[Q7, S. 6].

4.2 Angriff auf den Client

Der Bitcoin-Client dient, ähnlich wie eine Eingabemaske beim Online-Banking, vorrangig dazu, über das vorhandene Bitcoin-Vermögen zu verfügen. Gelingt es nun einem Angreifer, diesen Client zu manipulieren und den Nutzer somit unwissentlich Transaktionen durchführen zu lassen, so werden diese natürlich als gültig akzeptiert und der Nutzer hat keine Möglichkeit, dies zu widerrufen.

4.3 Angriff auf die wallet.dat

Die wallet.dat eines Users enthält alle Informationen, die nötig sind, um eine Transaktion mit seinen Bitcoins durchzuführen. In vorherigen Bitocin-Clients wurde diese Datei unverschlüsselt auf dem Rechner des Users abgelegt und war somit nur so sicher, wie es das Netzwerk des Users war. So gab es Fälle, in denen die wallet.dat einfach von einem Angreifer kopiert werden konnte. Dieser war dann in der Lage, über alle Bitcoins des Users frei zu verfügen. Seit einiger Zeit legt der Client diese Datei jedoch verschlüsselt ab, was es für einen Angreifer zwar schwerer, aber nicht unmöglich macht, fremde Transaktionen zu stehlen. Darüber hinaus gibt es auch Dienste wie MyBitcoin.com, die als eine Art Cloud jederzeit den Zugriff auf die eigene wallet.dat ermöglichen. Allerdings gab es auch bei Anbietern dieser Art diverse Sicherheitsprobleme, so kamen dem Cloud-Wallet Dienst MyBitcoin vor einiger Zeit über 25.000 Bitcoin abhanden[Q10, S. 2].

4.4 Angriff auf SHA256

Da das gesamte Proof-of-Work System und teilweise auch die Signatur von Transaktionen auf SHA256 Hashing beruht, stellt diese wohl die größte potentielle Angriffsfläche dar. Wäre es möglich, den Algorithmus zu umgehen, und sofort valide Blöcke zu generieren, so wäre das gesamte Proof-of-Work System außer Kraft gesetzt und es könnten Blöcke ohne Zeitaufwand generiert werden. Da damit die Kernfunktion von Bitcoin nichtig gemacht werden würde, würde dies wohl ein Ende für das System bedeuten, da BTC komplett an Wert verlieren würden. Dieser Fall ist allerdings sehr unwahrscheinlich, da es bisher keine bekannten Schwächen bei SHA256 gibt.

4.5 Ist Bitcoin also sicher?

Zusammenfassend lässt sich sagen, dass die Angriffsvektoren bei Bitcoin ähnlich denen des Online-Bankings sind. Die größten Sicherheitsrisiken liegen nämlich hauptsächlich auf Seite des Benutzers und sind abhängig davon, wie sicher das System ist, von dem aus mit dem Bitcoin Netzwerk interagiert wird. Das Bitcoin-System als solches

ist dagegen durch seine Sicherheitsmechanismen bestens gerüstet und bietet nur wenige bis gar keine Sicherheitslücken, solange der Großteil der Nutzer ehrliche Absichten hegt. Es ist dabei aber auch nicht zu vergessen, dass aktuell sichere Verfahren wie SHA256 auch ihr Verfallsdatum haben und, wenn auch noch nicht in naher Zukunft, durch neue Verfahren ersetzt werden müssen, wenn Bitcoin Bestand haben soll[Q3, S. 36].

5 Anonymität

Bitcoin wird als anonyme Währung angepriesen, was vor allem dadurch erreicht wird, dass Name und Adresse des Nutzers keine Rolle spielen. Identifiziert werden Nutzer nur durch ihre Bitcoin-Adresse, wobei ein Nutzer beliebig viele dieser Adressen besitzen kann. Dies hat zur Folge, dass die gesamte Privatsphäre bei Bitcoin grundsätzlich anders aufgebaut ist, als bei herkömmlichen Zahlungsmethoden. Bei traditionellen Zahlungssystemen ist die Zahlung immer direkt mit der Identität verknüpft (Spätestens die Bank oder der Zahlungsdienst kennt die Identität eines Zahlenden). Allerding sind Transaktionen nicht öffentlich, sondern unterliegen der Geheimhaltung und können nur von den Beteiligten und der verwaltenden 3. Instanz eingesehen werden:

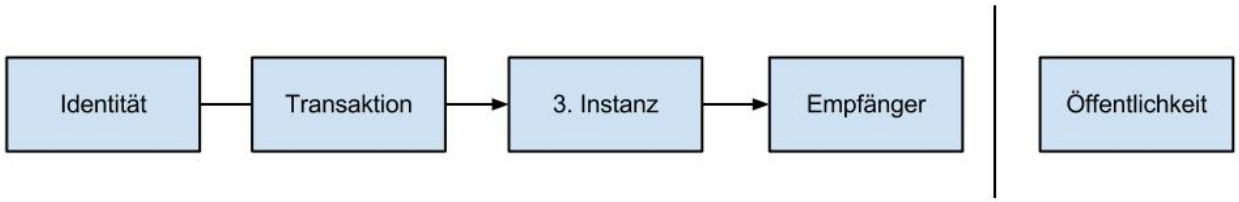

Abbildung 8: Privatsphäre bei traditionellen Zahlungen

Bei Bitcoin hingegen wird die Identität komplett von den Transaktionen gelöst. Stattdessen sind es hier die Transaktionen, die öffentlich gemacht werden, um eine Verifizierung durch das Netzwerk zu ermöglichen[Q7, S.6]:

Abbildung 9: Privatsphäre bei Bitcoin

Allerdings verhindert das System nicht, dass einzelne Transaktionsschritte nachvollzogen werden können. Da die Public Keys der Teilnehmer bekannt sind, lassen sich so Zahlungsströme erkennen und kann ein Key einem Nutzer beispielsweise durch Unachtsamkeit oder Verlust der wallet.dat zugeordnet werden, droht die Anonymität in Teilen zu bröckeln. Mitarbeitern des University College Dublin ist es beispielsweise gelungen, Spenden, die via Bitcoin an das Netzwerk WikiLeaks getätigt wurden, gezielt zuzuordnen[Q9].

6 Rechtliche und wirtschaftliche Aspekte

Die Einführung einer elektronischen Währung ist ohne Frage eine technische Herausforderung. Aber auch die wirtschaftlichen und rechtlichen Aspekte sollten nicht außer Acht gelassen werden. Denn was ist Bitcoin rechtlich gesehen überhaupt? Und wer muss das System kontrollieren bzw. welche rechtlichen Pflichten ergeben sich für die Bitcoin-Nutzer? Und wie bildet sich der Kurs von BTC?

6.1 Rechtliche Sicht

Das erste Problem beginnt damit, einzuordnen, ob Bitcoin eine wirkliche Währung ist oder viel mehr ein Tauschgut oder eine Ware. Nicht gerade hilfreich ist dabei die Tatsache, dass eigentlich keine wirkliche Definition von Geld existiert. Im Palandt findet sich, bezogen auf das BGB jedoch folgende Definition von Geld. Demnach sind Gelder „...gesetzliche Zahlungsmittel, die jeder Gläubiger einer Gelschuld kraft Gesetzes an-

nehmen muss“[Q8, §245 Abs. 3].Dieser Punkt trifft auf Bitcoin nicht zu, da sie bisher vom Gesetz in keiner Weise beachtet werden. Hier offenbart sich auch eigentlich schon der springende Punkt: Von Geld erwartet man, dass es jederzeit per Gesetz akzeptiert werden muss. Und dies ist bei Bitcoin nicht der Fall. Deshalb ist Bitcoin viel mehr als eine Tauschware anzusehen, die als monetärer Wert akzeptiert werden kann, jedoch nicht akzeptiert werden muss[Q5].

Ein weiteres Problem, besonders für den Staat, ist die Anonymität des Systems. Da Transaktionen nicht zugeordnet werden können, können darauf auch keine Steuern erhoben werden. Die Problematik ist hierbei eine ähnliche wie beim Bargeld, da die Zahlungen eben nicht von einer dritten Instanz überwacht werden. Somit laufen alle Bitcoin-Transaktionen am staatlichen Steuersystem vorbei und bieten somit eine perfekte Umgebung für kriminelle Aktivitäten. Da unser bisheriges Rechtssystem anonyme Währungen nicht kennt, bleibt hier eine große Grauzone.

6.2 Wirtschaftliche Sicht

Aus wirtschaftlicher Sicht ist es besonders spannend, wie sich überhaupt der Wert von BTC bildet. Da es keinen konkreten materiellen Gegenwert gibt, ist der Kurs einzig und allein von Angebot und Nachfrage abhängig. Zwar ist der Gedanke hinter Bitcoin, dass die investierte Rechenkapazität den Gegenwert bildet, jedoch ist diese im Ernstfall nicht als konkreter monetärer Wert behandelbar. Je nach weltpolitischer Lage und globalen Ereignissen schwankt der BTC Kurs extrem, so hat er sich z.B. von Januar bis April 2013 mehr als ver-7-facht[Q1].Diese Kurssteigerung ist vor allem der Eurokrise zu verdanken, die immer mehr Menschen dazu bringt, sich nach alternativen Kapitalanlagen umzuschauen. Die Prognosen für den Bitcoin Kurs stehen deshalb gut, auch da es immer mehr Anlaufstellen gibt, die BTC akzeptieren. Hier ist es natürlich wieder unklar, welche steuerlichen Pflichten für solche Geschäfte gelten sollen, z.B. ob jemand beim Umtausch von Bitcoin in beispielsweise Dollar zu irgendwelchen Abgaben verpflichtet ist oder welche Rolle die Mehrwertsteuer bei Verkäufen spielen soll. Da der Kurs extrem schwankt, ist Bitcoin eine sehr unsichere Anlage. Der aktuelle Kurs zeigt zwar, wie pro-

fitabel eine Investition in das elektronische Geld sein kann, allerdings sei auch gesagt, dass der Kurs genau so schnell wieder sinken kann. Als eine der größten Bitcoin-Börsen, Mt.Gox[Q6], am 19.06.2011 durch einen Hacker-Angriff mehr als 500.000 BTC verlor, brach der Kurs extrem ein und stagnierte fast ein Jahr lang[Q1]. Solche Wertverluste führen natürlich auch dazu, dass das Erstellen von Bitcoins unattraktiver wird und ohne die User, die durch das Erstellen zur Abwicklung von Transaktionen beitragen, kann das System nicht funktionieren.

7 Fazit

Das hier vorgestellte Bitcoin-Netzwerk wurde anfänglich nur müde belächelt und als „Hacker-Währung“ abgetan. Doch spätestens nach den Krisen in Griechenland, Irland, Spanien, Zypern und Italien wird immer deutlicher, dass der Bedarf nach alternativen Kapitalanlagen vorhanden ist und sicher geglaubte Währungen in ihrer Stabilität gefährdet werden. Außerdem wächst auch das Vertrauen in digitale Lösungen immer mehr und der Einkauf im Internet ist schon lange genau so selbstverständlich, wie der Gang in den Supermarkt. Der Schritt zum direkten Einkauf mit BTC ist deshalb gar nicht so groß.

Bitcoin zeigt auf eine beeindruckende Art und Weise, wie man das komplette Bankwesen nur durch kryptografische Verfahren und eine Dezentralisierung der Zahlungsüberwachung ersetzen kann. Allerdings sollte es im Interesse des Staates sein, einen rechtlichen Rahmen für dieses System zu entwickeln, um kriminelle Aktivitäten und Steuerhinterziehung zu verhindern. Es ist jedoch damit zu rechnen, dass die Nutzer diesem eher skeptisch gegenüberstehen und staatliche Restriktionen ablehnen werden. Hier muss aber Abhilfe geschaffen werden, denn solange Bitcoin in Assoziation mit illegalen Geschäften steht, wird es wohl nur schwerlich im geschäftlichen Alltag Fuß fassen können. Auch ist es noch problematisch, dass Bitcoin auf Grund seiner Andersartigkeit eine hohe Abschreckung auslöst, da Menschen bei einem so sensiblen Thema wie Geld natürlich immer vorsichtig reagieren und nicht jeder ist bereit, auf Verfahren zu vertrauen,

die er eventuell selbst überhaupt nicht versteht. Allerdings machen die unterschiedlichen Clients für Bitcoin, sei es für PC, Tablet oder das Smartphone, in den letzten Jahren immense Fortschritte, was die Benutzerfreundlichkeit und die Sicherheit angeht und es tauchen immer mehr Online-Börsen auf, die Bitcoin umtauschen oder Waren für Bitcoin anbieten. Sollte das so weitergehen, wird man sicher noch das ein oder andere Mal in den Medien über die „Hacker-Währung“ stolpern. Fakt ist, solange Bitcoin nicht flächendeckend akzeptiert wird, ist es natürlich kein Ersatz für bestehende Währungen. Aber es ist eine Möglichkeit sein Geld auf eine bisher einzigartige Art und Weise anzulegen und eine völlig neue Art des Zahlungsverkehrs zu erleben.

8 Quellenverzeichnis

[Q1]: Aktueller Bitcoin Kurs

https://www.bitcoin.de

[Stand: 01.04.2013]

[Q2]: Bitcoin Wiki: Protocol Specification

https://en.bitcoin.it/wiki/Protocol_specification

[Stand: 01.04.2013]

[Q3]: Drainville,Danielle: An Analysis of the Bitcoin Electronic Cash System, University of Waterloo, 21.12.2012

https://math.uwaterloo.ca/combinatorics-and-optimization/sites/ca.combinatorics-and-optimization/files/uploads/files/Drainville,%20Danielle.pdf

[Stand: 03.04.2013]

[Q4]: Erstellung neuer BTC

http://www.dev-eth0.de/bitcoins-erstellung-neuer-btc/

[Stand: 01.04.2013]

[Q5]: Ferner, Jens: Bitcoins: Währung oder Ware?

http://www.ferner-alsdorf.de/2011/06/bitcoins-wahrung-oder-ware/

[Stand: 01.04.2013]

[Q6]: Minick, Theodore: Bitcoin Weekly – The Mt.Gox Attack

http://bitcoinweekly.com/articles/the-mtgox-attack

[Stand: 01.04.2013]

[Q7]: Nakamoto, Satoshi: Bitcoin: A peer to peer electronic cash system
http://www.vsewiki.cz/images/archive/8/89/20110124151146!Bitcoin.pdf
[Stand: 01.04.2013]

[Q8]: Palandt: Bürgerliches Gesetzbuch, 68. Auflage, 2009. Verlag C.H.Beck

[Q9]: Reid, Fergal; Harrigan, Martin: An Analysis of Anonymity in the Bitcoin System
http://arxiv.org/pdf/1107.4524.pdf
[Stand: 03.04.2013]

[Q10]: Sorge, Christoph; Krohn-Grimberghe, Artus: Bitcoin: Eine erste Einordnung
http://www.ismll.uni-hildesheim.de/pub/pdfs/sorge-krohn-grimberghe-bitcoin.pdf
[Stand: 01.04.2013]

9 Abbildungsverzeichnis

Abbildung 1: Bitcoin Client 3

Abbildung 2: Transaktionen, die an Alice adressiert sind 5

Abbildung 3: Schematischer Aufbau einer Transaktion 5

Abbildung 4: Verifizierung von Transaktionen 8

Entnommen aus [Q7, S. 2]

Abbildung 6: Vereinfachter Aufbau eines Blocks 9

Vgl. [Q7, S. 4]

Abbildung 7: Input für die SHA256 Berechnung 10

Vgl. [Q4]

Abbildung 8: Beispielhafter Aufbau einer Block-Chain 13

Abbildung 9: Privatsphäre bei traditionellen Zahlungen 16

Vgl. [Q7, S.6]

Abbildung 10: Privatsphäre bei Bitcoin 17

Vgl. [Q7, S.6]