Bitcoin

Seminararbeit
ETIT
RUB

Lena Sophie Brüder
Matrikel 108010244444
Lena.Brueder@rub.de

Bochum, 20. Februar 2012

Inhaltsverzeichnis

1 Was ist Bitcoin?

Bitcoin ist ein elektronisches Geldsystem, das zum Verhindern von double-spending[1] auf einem peer-to-peer-Netzwerk aufbaut. Dabei helfen die Teilnehmer des Netzwerkes, es am Leben zu halten, und es ist keine zentrale Instanz dafür nötig. Es wurde ursprünglich von Satoshi Nakamoto in 2009 vorgestellt (siehe [9]).

In dieser Seminararbeit soll sowohl die Funktionsweise von Bitcoin herausgearbeitet, als auch eine Auswahl an Schwachstellen untersucht werden.

2 (Elektronisches) Geld

2.1 Was ist Geld?

Issing ([8, S.1]) definiert Geld folgendermaßen:

> In der Nationalökonomie wird der Geldbegriff heute allgemein von den **Geldfunktionen** her bestimmt: Alles, was Geldfunktionen ausübt, **ist** Geld.

Als Geldfunktionen betrachtet er hier die Funktionen als:

- Tausch- und Zahlungsmittel
- Wertaufbewahrungsmittel
- Recheneinheit

Tausch- und Zahlungsmittel werden dadurch unterschieden, dass Zahlungsmittel auch zur Tilgung von Schulden verwendet werden können. Als Recheneinheit wird Geld verwendet, um den direkten Vergleich von Waren zu umgehen. Beim direkten Vergleich von n Waren müssen $n(n-1)$ Umrechnungsfaktoren berücksichtigt werden, um alle Waren vergleichen zu können. Über den Umweg des wertquantifizierenden Geldes sind dafür nur n Werte nötig.

Die wichtigste Eigenschaft von Geld ist, dass es nicht beliebig verfügbar ist. Wäre es beliebig verfügbar, hätte es keinen Wert mehr. Daher wurde, bevor es Banknoten und Münzen gab, auf knapp vorhandene Güter als universelles

[1] mehrfaches Ausgeben desselben Geldes

Tauschmittel zurückgegriffen, wie etwa Gold. Die ersten Münzen wurden geprägt, um den Austausch von Gold zu vereinfachen: Durch eine geprägte Münze wurde vom Ausgebenden garantiert, dass diese eine definierte Menge an Gold beinhaltet.

Als die ersten Banknoten aufkamen, waren diese oftmals durch Goldreserven gedeckt – jeder konnte bei einer Bank einen Geldschein in die entsprechende Menge Gold tauschen lassen, und hatte ein Anrecht darauf.

Bei den meisten zur heutigen Zeit verfügbaren Währungen existiert keine Bindung mehr an Gold: Solche Währungen werden Fiat-Währungen genannt. Ihr Wert ist hauptsächlich dadurch geprägt, dass viele Menschen an den Wert einer Währung und deren längerfristiger Stabilität glauben. Vorteil für die ausgebende Stelle ist die prinzipielle Möglichkeit, Geld in beliebiger Menge herstellen zu können, wenn es benötigt wird. Für die Stabilität einer Währung und den Glauben der Nutzer an diese ist es jedoch essentiell, dass sich die Geldmenge nicht von einem auf den anderen Moment drastisch verändert. Das Nachdrucken von Geld ist also nicht in beliebiger Menge möglich, ohne die Inflation zu beschleunigen. Auch bei Gold ist es wichtig, dass sich die Menge nicht in kurzer Zeit stark ändert, jedoch haben historische Beobachtungen gezeigt, dass das Auffinden einer sehr großen Menge Gold ungleich schwerer ist als das Bedrucken bunter Papierscheine.

2.2 Wichtige Eigenschaften

Geld ist nur begrenzt verfügbar, kann nicht oder nur schwer kopiert werden. Dies ist essentiell für den Wert des Geldes. Dies trifft auf alle Geldarten zu:

- Gold ist ein seltenes Edelmetall, und muss gefunden/geschürft werden. Besonders große Vorkommen sind selten.
- Goldmünzen wurden geprägt um eine bestimmte Goldmenge zu garantieren und sind daher als Gold zu zählen
- Geldmünzen werden in einer beschränkten Menge von einer ausgebenden Institution hergestellt und in Umlauf gebracht. Meist ist dies ein Staat, es kann sich aber auch um private Institutionen handeln (z.B. Liberty Dollar, ...)
- Banknoten sind wie Geldmünzen zu betrachten, jedoch günstiger herzustellen

Anders als bei Gegenständen in der realen Welt sind Bits in Speichern von Geräten erst einmal kopierbar. Möchte man elektronische Geldmünzen als Dateien auf einem Computer ablegen, wird es ohne spezielle Maßnahmen einfach, elektronisches Geld zu vervielfachen – es wäre wertlos, vor allem weil man es mehrfach ausgeben könnte (→ double-spending).

2.3 Historische Entwicklung von elektronischem Geld

Hier werden verbreitete oder wichtige elektronische Geldsysteme vorgestellt. Sie unterscheiden sich teils in der Funktionsweise sehr stark. Herausgestellt sei, dass sie ausnahmslos auf eine zentrale Instanz angewiesen sind, die – mehr oder weniger stark – für das Funktionieren des jeweiligen Systems nötig ist.

Online-Überweisungen ermöglichen es, am Computer eine Banküberweisung auszuführen. Sie sind allerdings eher eine Schnittstelle des schon vorhandenen Überweisungssystems an den Endbenutzer, die von den Banken jeweils selbst bereitgestellt werden. Es können damit Geldbeträge von einem auf ein anderes Konto übertragen werden. Ein solcher Betrag wird auf einem Konto abgezogen, und auf dem anderen gutgeschrieben. Benutzer haben jedoch keinen direkten Zugriff auf das Kontensystem, sondern geben jeweils Aufträge an ihre Bank, die diese ausführt.

PayPal ist prinzipiell ähnlich gestaltet wie eine Online-Banküberweisung innerhalb einer Bank. Der große Vorteil von PayPal ist die sofortige Gutschrift eines Betrags beim anderen Zahlungsbeteiligten. Dies ist allerdings auch bei Banküberweisungen innerhalb einer Bank oft anzutreffen.

Die Verbindung zu PayPal wird über SSL abgesichert. Eine weitere Verschlüsselung zwischen Benutzer und den PayPal-Servern findet nicht statt. PayPal liegt also kein besonderes kryptografisches System zugrunde, auf dessen Grundlage die Benutzer eigenverantwortlich handeln könnten – sie sind jeweils darauf angewiesen darauf zu vertrauen, dass PayPal die Überweisung wie bestimmt weiterleitet, und der Empfänger sich sein Geld auch auszahlen lassen kann. Dies ist leider keine Selbstverständlichkeit: PayPal behält sich vor, das Konto in einigen Fällen zu sperren und das Restguthaben einzubehalten. Dazu zählt beispielsweise, die „Geschäfte in einer Weise zu führen, [...] die zu Beschwerden

[...] führen könnte“[2] . Diese und ähnliche Regelungen wurden in der Vergangenheit dazu benutzt, Konten zu sperren. Dazu zählt u.a. das PayPal-Spendenkonto von Wikileaks[3].

ecash ist ein Verfahren, das anonymen Geldverkehr vergleichsweise zu Bargeld ermöglicht. Es beruht auf der Vertauschbarkeit der Reihenfolge von RSA-Signatur und RSA-Verschlüsselung. Es werden digitale Münzen mit einem bestimmten Wert erzeugt, die nicht mehr teilbar sind. Eine solche Münze wird von einer Partei in Zusammenarbeit mit einer zentralen Instanz (die *Zentralbank*) erzeugt und kann später ohne Zusammenarbeit mit der Zentralbank ausgegeben werden. Zur Überprüfung der Gültigkeit einer Münze ist kein Kontakt mit der Bank nötig, double-spending kann jedoch nur in Zusammenarbeit mit der Bank erkannt werden. Wird ein Fall von double-spending erkannt kann die Zentralbank in Zusammenarbeit mit den beiden betrogenen Parteien die Identität des Betrügers mit sehr hoher Wahrscheinlichkeit feststellen. Für nur eine Partei mit Zentralbank ist dies nicht möglich.

3 Wie funktioniert Bitcoin?

Wie im klassischen Bankensystem hat jeder Benutzer von Bitcoin (mindestens) ein Konto. Mit diesem Konto sind alle zugehörigen Überweisungen (→Transaktionen) verknüpft. Jedes Konto besitzt ein private-/public-key-Paar, mit dem Transaktionen unterschrieben, und von anderen verifiziert werden können. Eine digitale Münze wird dann definiert als Kette von Signaturen; sie wird durch eine Transaktion an einen neuen Besitzer weitergegeben, und von diesem eventuell aufgeteilt.

3.1 Transaktionen

Eine Transaktion besteht aus ein oder mehr **Input**s, und zwei oder mehr **Output**s. Die Inputs verweisen auf Outputs vergangener Transaktionen, die dem

[2] PayPal-Nutzungsbedingungen vom 7. September 2011, Punkt 9.1.l, „Verbotene Aktivitäten“, `https://cms.paypal.com/de/cgi-bin/?cmd=_render-content&content_ID=ua/UserAgreement_full&locale.x=de_DE`

[3] `http://www.heise.de/newsticker/meldung/PayPal-sperrt-Spendenkonto-von-Wikileaks-1147516.html`

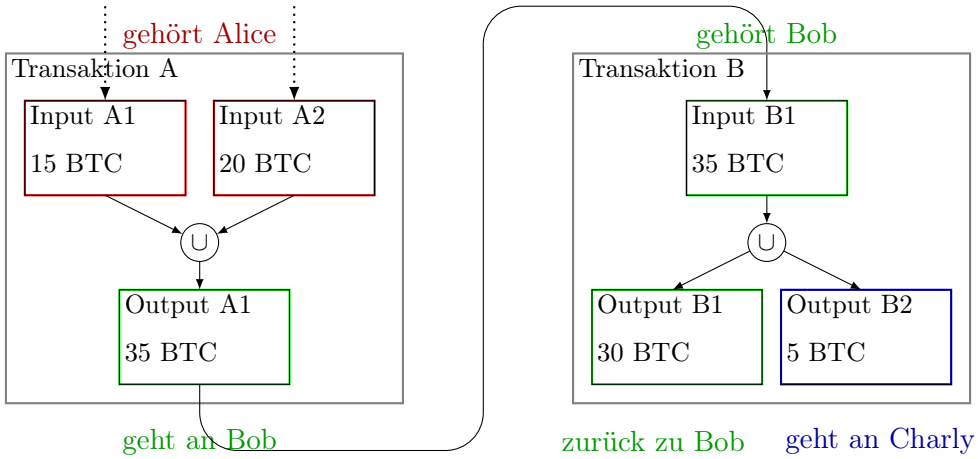

Abb. 1: Eine Beispieltransaktion – Fokus Input/Output

Aussteller der aktuellen Transaktion geschickt wurden. Sie werden zusammengerechnet und bilden die Geldmenge, die maximal auf die Outputs verteilt werden kann. Mindestens ein Output versendet diese Bitcoins an einen neuen Besitzer, ein anderer sendet das „Rückgeld“ an den Aussteller zurück. Es ist möglich, mit einer Transaktion Bitcoins an mehrere Empfänger zu versenden. Dies wird in Abbildung 1 dargestellt.

Besteht eine Differenz zwischen der Summe der Inputs und der Summe der Outputs, so wird sie als **Transaktionsgebühr** verstanden und geht an denjenigen, der die Transaktion bestätigt (s.u.).

Um sicherzustellen, dass eine Transaktion nur vom Eigentümer einer Münze erzeugt werden kann, werden digitale Signaturen verwendet. Der Eigentümer unterschreibt den Hash einer Transaktion mit seinem privaten Schlüssel. Andere können nun anhand des öffentlichen Schlüssels feststellen, ob eine Transaktion von der richtigen Person unterschrieben wurde, oder nicht (siehe Abbildung 2). Dadurch wird sichergestellt, dass nur die Person Transaktionen für ein Konto ausstellen kann, die Kenntnis von dem privaten Schlüssel des Kontos hat. Da die Inputs einer Transaktion nur von Outputs gespeist werden können, die den Aussteller dieser Transaktion erreicht haben wird sichergestellt, dass eine Person nur Geld ausgeben kann, welches ihr auch gehört.

Allerdings ist noch nicht feststellbar, ob eine Person Geld nicht mehrfach ausgegeben hat (→ **double-spending**). Normalerweise wird dafür eine zen-

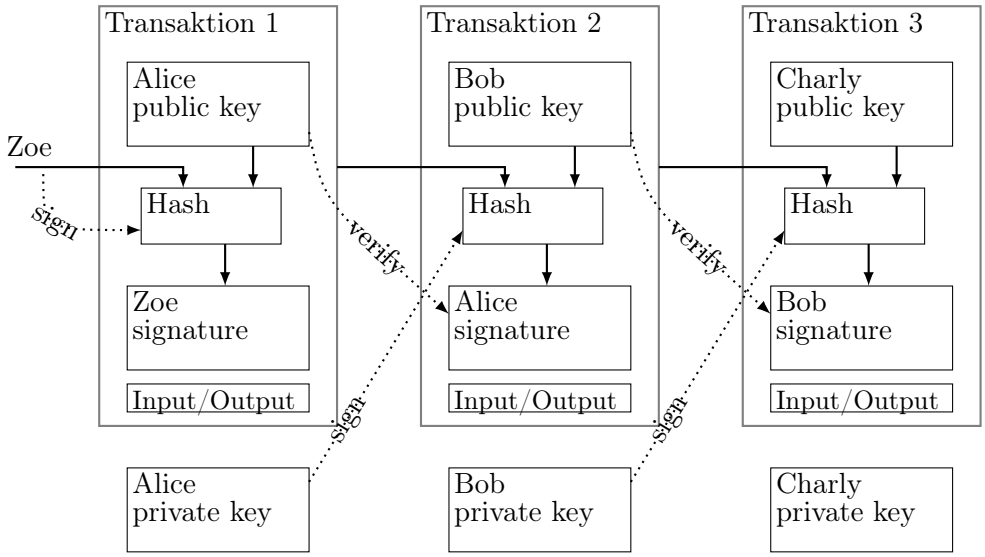

Abb. 2: Eine Beispieltransaktion – Fokus Signaturen

trale Instanz (Bank) verwendet, die alle Transaktionen überwacht und dann festlegt, wann eine Transaktion als gültig angesehen wird. Allerdings stellt eine zentrale Instanz auch immer ein Risiko dar: Fällt sie aus oder verweigert ihre Zusammenarbeit mit einem Teilnehmer, kann dieser keine Transaktionen mehr ausführen. Daher verzichtet Bitcoin auf diese Zentrale und verteilt diese Aufgabe auf die Teilnehmer des Systems[4].

3.2 Timestamp-Server

Ohne eine zentrale Instanz ist der einzige Weg um festzustellen, ob eine Transaktion bereits durchgeführt wurde, alle Transaktionen zu kennen. Da potentiell jeder mithelfen kann, das System am Laufen zu halten, müssen also alle Transaktionen aller Teilnehmer jedem Teilnehmer bekannt sein.

Sollte es mehrere Transaktionen geben, die den Output einer anderen Transaktion verwenden, wird die früheste davon als gültig betrachtet. Um sicherstellen zu können, welche Transaktion als erstes getätigt wurde, müssen sich

[4]Tatsächlich wird die Aufgabe nur an die Teilnehmer übertragen, die sich dafür zur Verfügung stellen. Diese werden dafür belohnt.

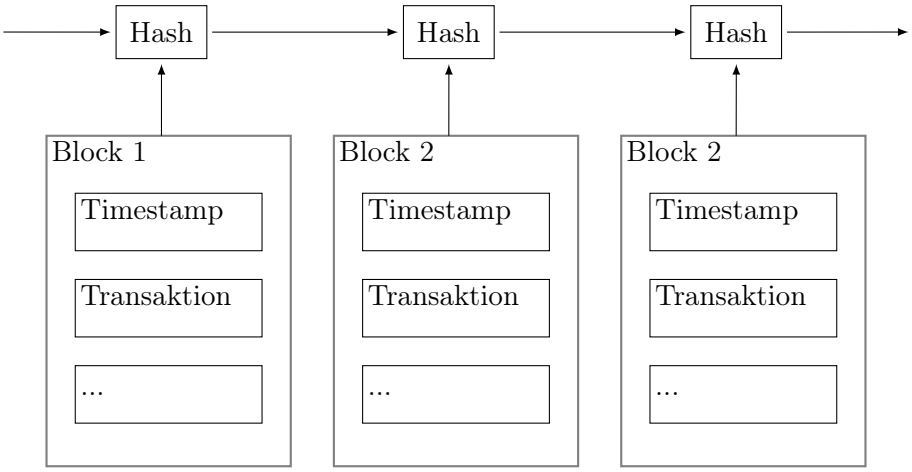

Abb. 3: Timestamp-Kette

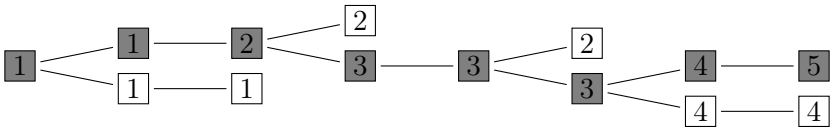

Abb. 4: Die längste Kette (grau) ist gültig. Die Zahl deutet die Schwierigkeit, unter der der Block berechnet wurde, an. Je höher die Zahl, desto höher die Schwierigkeit.

alle Teilnehmer auf eine gemeinsame Transaktionshistorie einigen. Diese wird im Wesentlichen durch die Verkettung mehrerer **Block**s erreicht, die jeweils Datum und Uhrzeit, eine Nonce, sowie Referenzen auf die enthaltenen Transaktionen und den Hash des vorhergehenden Blocks enthalten.

Etwa alle 10 Minuten wird ein solcher Block vom Netzwerk erzeugt. Er wird gemeinsam mit seinem Hash veröffentlicht – dieser Hash muss bestimmte Eigenschaften haben (s.u.), damit der Block als gültig angesehen wird. Ist eine Transaktion in einem Block enthalten beweist dies, dass sie zu dem Erstellungszeitpunkt des Blocks bereits existiert haben muss – sonst wäre sie im Block nicht enthalten.

Die Blöcke werden im Laufe der Zeit verkettet, wobei jeweils die längste[5]

[5]Bei der Bestimmung, welche Kette als längste anzusehen ist zählt sowohl die Anzahl der

Kette (siehe Abb. 4) als gültige Transaktionshistorie angesehen wird. Aufgrund der vorherbestimmten Eigenschaften des Hashs eines Blocks ist dieser nicht leicht zu berechnen. Eine Transaktion, die in einem solchen Block enthalten ist, gilt als **bestätigt**.

3.3 Proof-of-work

Damit ein Block als gültig angesehen wird, muss sein Hash kleiner sein als ein bestimmter **Zielwert**. Da die Inhalte eines Blocks bis auf die Nonce vorherbestimmt sind, wird diese so lange inkrementiert, bis ein gültiger Hash erzeugt wird. Der Zielwert wird je nach im Netzwerk vorhandener Rechenkapazität alle 2016 Blöcke so bestimmt, dass im Mittel alle 10 Minuten vom gesamten Netz ein neuer Block erzeugt werden kann. Dabei ist es durchaus möglich, dass das Erzeugen eines speziellen Blocks einmal deutlich früher oder auch deutlich später gelingt – im statistischen Mittel werden jedoch circa 10 Minuten erreicht, oder etwa 14 Tage für 2016 Blöcke.

Hat ein Teilnehmer einen gültigen Hash gefunden, kann der Inhalt des Blocks nicht mehr verändert werden, ohne die geleistete Arbeit zunichte zu machen. Es ist also schwierig, einen neuen Block zu erzeugen, und ebenso schwierig, einen erzeugten Block zu verändern. Mit der Veröffentlichung eines neuen Blocks wird demnach bewiesen, dass eine gewisse Menge an Rechenleistung aufgebracht wurde, ihn zu erzeugen. Für die anderen Teilnehmer ist es allerdings leicht, die Richtigkeit des Hashes zu erkennen: Es muss lediglich der Hash über den entsprechenden Block erzeugt und mit dem behaupteten Wert verglichen werden.

Werden nun Blöcke verkettet, so wird es für einen Angreifer zunehmend schwieriger, eine weiter in der Vergangenheit liegende Transaktion rückgängig zu machen oder zu verändern: Er müsste dafür schneller rechnen als der Rest des Netzwerkes, da er sowohl den betreffenden Block, als auch die angehängte Kette von weiteren Blöcken neu berechnen müsste. Daher spricht man auch von Transaktionen mit x **Bestätigungen**, wenn sie in einem Block enthalten ist, nach dem schon $x - 1$ weitere Blöcke erzeugt wurden.

Da die Schwierigkeit der Berechnung des Hashes eines Blockes mit zuneh-

Blöcke, als auch die in ihnen aufgewendete Rechenleistung. 5 Blöcke, die mit wenig Rechenleistung erzeugt wurden sind evtl. weniger wert als 3 Blöcke, die mit viel Rechenleistung erzeugt wurden.

mender Rechenleistung des Netzwerkes steigt, steigt auch der Wert einer Bestätigung mit wachsender Rechenleistung des Netzwerkes.

Damit gilt bei Bitcoin: Je mehr Rechenleistung ein Teilnehmer hat, desto größeres Stimmgewicht hat er und bestimmt damit die gültige Transaktionshistorie.

3.4 Leistungsanreiz

Die Rechenleistung, die nötig ist um die Blockkette zu erweitern, kostet Geld. Es ist daher nicht selbstverständlich, dass die Teilnehmer Rechenleistung investieren, um das System lauffähig zu halten. Um die Teilnehmer dennoch dazu zu motivieren, wird ein Leistungsanreiz geschaffen:

Derjenige, der einen neuen Block erzeugt, mit einer gewissen Menge an Bitcoins belohnt – aktuell sind dies 50 BTC. Die Belohnung halbiert sich alle 210.000 Blöcke, sodass letztendlich etwa 21 Millionen Bitcoins existieren. Der Anreiz, beim Erweitern der Blockkette zu helfen, wird dann durch Transaktionsgebühren (siehe Seite 7) hergestellt. Jedem Blockerzeuger steht es frei, nur solche Transaktionen zu bestätigen, die eine Transaktionsgebühr bezahlen. In der Theorie wird es zu dem Zeitpunkt, an dem kaum noch Belohnungen für das Errechnen eines Blocks gezahlt werden, ohne Bezahlung von Transaktionsgebühren kaum noch bis nicht mehr möglich sein, Transaktionen bestätigen zu lassen.

Aktuell reicht die Belohnung nicht mehr aus, um die Stromkosten eines Rechners zu decken, der nur für Mining eingesetzt wird[6]. Zwischenzeitlich war es allerdings möglich, nicht nur den Strom, sondern zugleich auch noch die Hardware über Mining von Bitcoins zu finanzieren.

3.5 Exkurs: Merkle-Bäume

Merkle-Bäume (auch: *Hash-Bäume*) sind Bäume, die in ihren Knoten Hashwerte aller Kinder speichern. In den Blättern werden Hashwerte von Daten gespeichert, die mit den Hashwerten auf Integrität o.Ä. geprüft werden sollen. Oft werden Binärbäume verwendet, es spricht jedoch nichts dagegen, auch mehr Kinder zuzulassen (siehe Abbildung 5).

[6] `http://www.3dcenter.org/artikel/kann-bitcoin-mining-grafikkarte-gewinnbringend-sein`, wird auch in [11] angesprochen

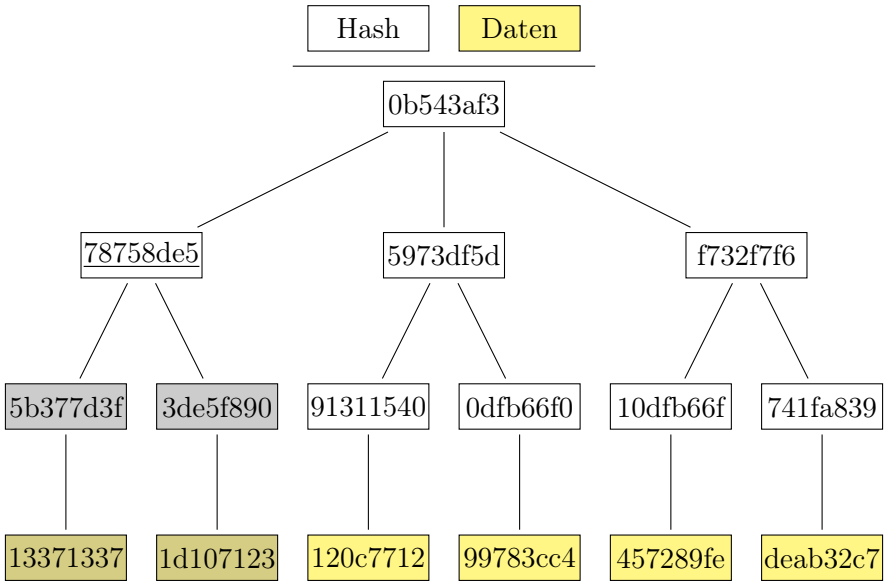

Abb. 5: Ein beispielhafter Merkle-Tree

Sie werden unter anderem verwendet, wenn man die Integrität von vielen kleinen Teilen von Daten überprüfen möchte, die zu einem gemeinsamen großen Teil zusammengesetzt werden können. Dies ist beispielsweise in P2P-Netzen der Fall, wenn immer nur Teile einer großen Datei heruntergeladen werden müssen. Ist ein Teil des Hashbaums bereits verifiziert worden (in der Abbildung etwas dunkler hinterlegt), kann er bis zu einem gemeinsamen Elternteil (unterstrichen) gelöscht werden – dieser Teil reicht dann zur Überprüfung der Gesamtintegrität aus. Je nach Anwendungsfall dürfen die Daten dann gelöscht werden, oder auch nicht.

Merkle-Bäume werden bei Bitcoin eingesetzt, um bei einigen Netzknoten Speicher sparen zu können.

3.6 Speicherplatz sparen mit Merkle-Bäumen

In einem Block sind Referenzen auf die enthaltenen Transaktionen gespeichert. Diese bestehen hauptsächlich aus ihren Hashwerten, die jeweils als Merkle-Baum angeordnet sind. In dem Block wird dann die Wurzel des Merkle-Baums vermerkt. Bei Veröffentlichung enthält ein solcher Block alle Transaktionen mit

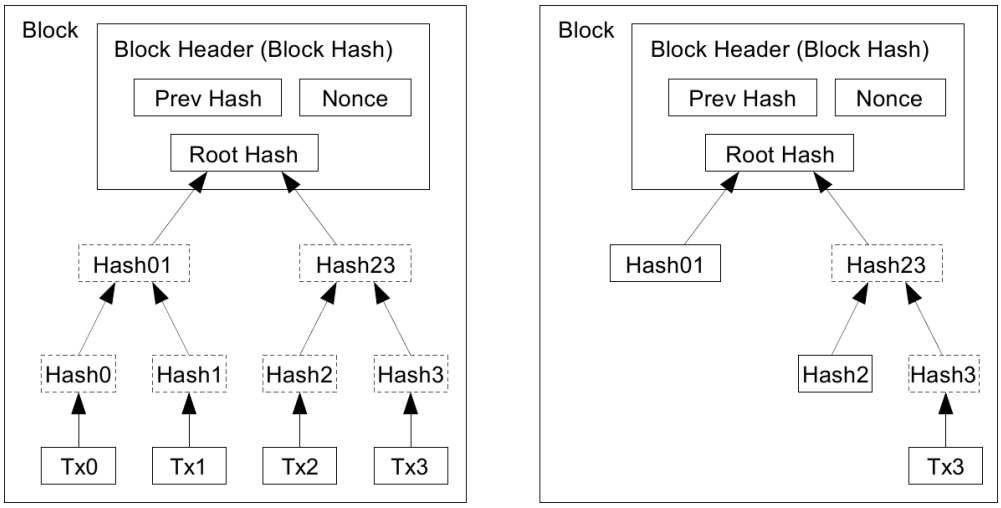

Abb. 6: Speicher sparen mit Merkle-Bäumen, Quelle: Abbildung in [9], S.7.

den entsprechenden Daten. Sind die Outputs der Transaktionen jedoch zu späterer Zeit wieder verwendet worden und in genügend Blocks bestätigt worden, so reicht es aus, statt der gesamten Transaktion mit Daten lediglich ihre Hashwerte zu speichern. Die Richtigkeit der Hashwerte wird schon durch die Bestätigungen gewährleistet: Zum Zeitpunkt der Erzeugung dieser müssen die Daten vorgelegen haben, und sie müssen richtig gewesen sein.

3.7 Nichtrückabwickelbarkeit von Transaktionen

Transaktionen sind, wenn sie bekanntgegeben wurden, nicht mehr rückabwickelbar. Dies folgt vor allem daraus, dass Clients alle Transaktionen sofort verwerfen, die einen vorher verwendeten Output noch einmal verwenden. Eine Transaktion kann erst als sicher angesehen werden, wenn sie vom Netz genügend oft bestätigt wurde; wurde sie oft bestätigt, ist die Transaktion mindestens der Hälfte der Netzknoten bekannt und wurde dort akzeptiert. Dies verhindert automatisch das Annehmen einer Transaktion mit ebendiesem alten Output bei mindestens der Hälfte der Netzknoten, sodass diese Transaktion nie Gültigkeit über der alten erreichen kann.

Ein Mechanismus, der diesen Standardprozess aufweichen würde, ist nicht

implementiert, nicht geplant und vor allem im Bitcoinsystem nicht gewünscht. Es wird nicht als Schwäche, sondern als Stärke des Systems angesehen, dass Transaktionen nicht rückabwickelbar sind.

4 Potentielle Schwachstellen von Bitcoin

4.1 klassische Angriffsvektoren

Wie bei jedem Verfahren, das kryptographische Algorithmen verwendet, ist auch Bitcoin abhängig davon, dass die **verwendeten Algorithmen** nicht **gebrochen** werden. Dies betrifft vor allem das Hashverfahren SHA-256 und das Signaturverfahren ECDSA. Allerdings ist es möglich, das Signatur- und Hashverfahren zu ändern, sollten wesentliche Schwachpunkte bei ihnen gefunden werden.

Weiterhin erlauben, wie bei jeder Software, **Programmfehler** die Übernahme eines laufenden Clients. Darüber könnte entweder der Computer, auf dem der Client läuft, oder aber der Client selbst kompromittiert werden. Es könnte dadurch möglich werden, die Bitcoins des kompromittierten Clients *sofort* auf ein anderes Konto zu übertragen, oder die privaten Schlüssel zu stehlen und dies zu einem beliebigen *späteren* Zeitpunkt zu tun. Die Sicherheit der privaten Schlüssel ist – wie bei jedem anderen System, bei dem eine PKI verwendet wird – essentiell für die Sicherheit von Bitcoin.

Bis Version 0.4 des offiziellen Bitcoin-Clients war die Datei `wallet.dat`, die digitale Brieftasche, nicht verschlüsselbar. Sie enthält u.A. den privaten Schlüssel der benutzten Bitcoin-Adresse[7]. Dadurch war es möglich, mit einer gestohlenen `wallet.dat` die Bitcoins eines Teilnehmers für eigene Zwecke zu benutzen. Dies wurde von Schadsoftware ausgenutzt (z.B. `Infostealer.Coinbit`[8] nach Symantec-Benennung). In aktuellen Clients kann die `wallet.dat` verschlüsselt werden, wodurch eine gestohlene Datei ohne den zugehörigen Schlüssel weitgehend wertlos ist.

Es wäre prinzipiell auch möglich, dass eine **Hintertür im Quellcode eines Clients** eingebaut wird, wie dies beispielsweise mit der IPSec-Implementierung von OpenBSD Ende 2010 vermutet wurde (siehe [2]). Ein solches Problem lässt

[7] Die Bitcoin-Adresse ist gleichzusetzen mit der Verbindung Kontonummer/Bankleitzahl im klassischen deutschen Bankensystem.

[8] `http://www.symantec.com/security_response/writeup.jsp?docid=2011-061615-3651-99`

sich allerdings durch eine große Anzahl von verschiedenen Clientimplementierungen besser verteilen, sodass nicht alle Teilnehmer kompromittiert wären. Diese Lösung bezieht sich ebenso auf das Problem der Programmierfehler eines speziellen Clients – wobei zu beachten bleibt, dass viele Clientimplementierungen wohl eher für *andere* Fehler in jedem Client sprechen, denn für *weniger* Fehler. Natürlich ist es einfacher, einen Client zu pflegen als viele.

Desweiteren können natürlich **bisher unbekannte Schwachstellen im System selbst** liegen, an die niemand zuvor dachte. Sollten sie existieren, könnte das System von einem auf den anderen Tag wertlos werden.

4.2 Nicht authentifizierte IP-Transaktionen

Transaktionen können direkt an IP-Adressen versendet werden, ohne dass die versendende Partei die Bitcoinadresse der Zielperson kennen muss. Dies ist eine Funktion des offiziellen Bitcoin-Clients, die erst durch einen Aufrufparameter aktiviert werden muss, und die aufgrund ihrer Schwachstellen in der Diskussion steht, aus dem Code entfernt zu werden[9].

Dabei wird von Alice eine Verbindung zu der angegebenen IP-Adresse von Bob aufgebaut. Läuft dort ein Bitcoin-Client, der IP-Transaktionen annimmt, sendet Alice optional eine Nachricht (textuell) zu Bob. Dieser generiert daraufhin eine komplett neue Bitcoin-Adresse und schickt diese zurück an Alice. Sie sendet nun auf dem normalen Weg die Bitcoins an diese Adresse.

Problematisch ist, dass bei der Verbindung zwischen Alice und Bob keine Authetifizierung stattfindet. Dadurch ist es möglich, eine Man-in-the-middle-Attacke zu benutzen, um Alice eine fremde Bitcoinadresse unterzuschieben, wenn sie versucht mit Bob zu kommunizieren. Dazu fängt Oskar die Nachricht von Alice an Bob ab, und gibt sich als Bob aus. Dies gelingt ihm, da es für Alice keinen Mechanismus gibt, um festzustellen ob sich wirklich Bob meldet, oder jemand der sich als Bob ausgibt. Nun schickt Oskar ihr die neu erzeugte Bitcoinadresse.

Sie würde dann ihre Bitcoins an eine falsche Adresse schicken. Wenn sie den Fehler bemerkt (z.B. weil Bob sich beschwert), wäre es zu spät, da Bitcoin-Transaktionen nicht rückabwickelbar sind.

[9] `https://bitcointalk.org/index.php?topic=9334.0`

4.3 Die „Finney"-Attacke

Hal Finney stellte seine Attacke in [6] vor. Angenommen, ein Angreifer erzeugt ab und an einen Block selbst, in dem er eine Transaktion bestätigt, die von einer Adresse A zu einer Adresse B geht. Beide Adressen gehören dem Angreifer. Nachdem er diesen Block erzeugt hat, veröffentlicht er ihn noch nicht – stattdessen verschickt er die gleichen Bitcoins[10], die er an Adresse B verschickt hat, an einen Verkäufer mit Adresse C. Dieser wartet ein paar Sekunden, um einen möglichen double-spending-Versuch zu erkennen, und verschickt darauf ohne weitere Bestätigung in einem Block seine Waren an den Angreifer. In diesem Moment oder kurz darauf veröffentlicht dieser den bereits berechneten Block, und die darin gespeicherte Transaktion von A nach B. Diese würde die Transaktion von A nach C verdrängen, weil sie schon bestätigt ist. Der Verkäufer hat seine Waren versendet, und der Angreifer hat nichts bezahlt.

4.4 Cancer Nodes

Bei Cancer Nodes handelt es sich um "krankhafte" Netzknoten, die sich nicht normal verhalten, sondern das Netz in irgendeiner Art stören. Dabei sind verschiedene Angriffe denkbar, die möglicherweise für einen ehrlichen Knoten unentdeckbar blieben.

Dazu verbindet sich ein Angreifer mit sehr vielen (> 100.000) Clients, die je eine eigene IP-Adresse benötigen, zum Netzwerk – idealerweise zum Bootstrap-IRC-Kanal des Netzes, der dazu verwendet wird, die ersten Verbindungen von Clients untereinander zu ermöglichen. Diese Clients könnten beispielsweise Rechner aus einem Botnetz sein, die unter der Kontrolle des Angreifers stehen. Dann ist die Wahrscheinlichkeit, dass sich ein ehrlicher Client nur zu krankhaften Knoten verbindet, sehr hoch. Nun hat der Angreifer verschiedene Möglichkeiten.

Der Angreifer kann verhindern, dass Blöcke und Transaktionen, die nicht unter seiner Kontrolle stehen, an den ehrlichen Knoten weitergeleitet werden. Den ehrlichen Knoten würden nur noch vom Angreifer gebilligte Transaktionen in nur vom Angreifer erzeugten Blöcken erreichen. Dadurch befindet sich der ehrliche Knoten in einem **neuen Netzwerk**. Der Angreifer ist jetzt in der Lage, in diesem Netzwerk mit weniger Rechenkapazität die längste Blockkette zu erzeugen. Dabei kann er seine Bitcoins sowohl in dem neu erzeugten, als auch in dem originalen Netzwerk ausgeben ($\rightarrow$ double-spending). Dieser Fall könnte

[10] Outputs einer vorhergehenden Transaktion

bemerkt werden, wenn die aktuelle Schwierigkeit beim Minen oder die Transaktionsrate in kurzer Zeit stark abfällt. Für eine hohe Schwierigkeit ist eine große Menge Rechenkapazität nötig, die der Angreifer nicht notwendigerweise hat. Für eine hohe Transaktionsrate könnte der Angreifer Transaktionen erzeugen, die ständig Bitcoins zwischen Adressen bewegen, die unter seiner Kontrolle stehen.

Statt nur eigene Transaktionen an ehrliche Knoten weiterzuleiten, kann der Angreifer auch schlicht keine Transaktionen und Knoten mehr weiterleiten und effektiv **Knoten vom Netzwerk trennen**. Er würde seine eigenen Ziele erreichen, wenn er das Bitcoinsystem zwar nicht zu seiner eigenen Bereicherung benutzen, aber deren Nutzung durch andere unterbinden möchte.

Wenn sich der ehrliche Knoten auf Transaktionen ohne Bestätigungen verlässt, beispielsweise weil er nicht so lang auf die Bestätigung warten möchte oder kann[11], kann der Angreifer nur **einige Transaktionen herausfiltern**, um double-spending-Angriffe möglich zu machen. Dazu erzeugt der Angreifer zunächst eine Zahlung an eine andere, potentiell unter seiner Kontrolle stehende Adresse, gibt sie dem Rest des Netzwerks bekannt und leitet sie nicht an den ehrlichen Knoten weiter. Kurz darauf erzeugt er eine weitere Transaktion mit dem selben Input, wie die vorhergehende, und leitet sie nur an den ehrlichen Knoten weiter. Die zuerst bekanntgegebene Transaktion wird sich gegen die zuletzt bekanntgegebene, und nur dem einen Knoten bekannte Transaktion durchsetzen. Auch wenn diese Attacke der Finney-Attake ähnlich sieht, sind sie zu unterscheiden: Bei der Finney-Attacke steht ein erzeugter Block unter der Kontrolle das Angreifers, hier ist dies nicht der Fall.

4.5 Timejacking

Timejacking versucht, einen Knoten zeitweise vom Netzwerk zu isolieren und in dieser Zeit Überweisungen an ihn zu tätigen, die bei späterer Wiederverbindung zum Netzwerk durch die inzwischen längere Blockkette des Netzes aufgehoben werden. Dabei werden Implementierungsdetails der Verarbeitung der Zeitstempel ausgenutzt, die bisher noch nicht angesprochen wurden. Die Attacke ist, im Gegensatz zu den Cancer Nodes, auch möglich wenn alle Knoten noch Kontakt zu ehrlichen Knoten haben.

[11] Beispiel: Bitcoin als Bargeldersatz, die Kneipe Room77 in Berlin akzeptiert Bitcoin zum Bezahlen der Burger, `http://www.imghaven.com/images/16166/room77.jpg`, Abruf: 15.12.2011

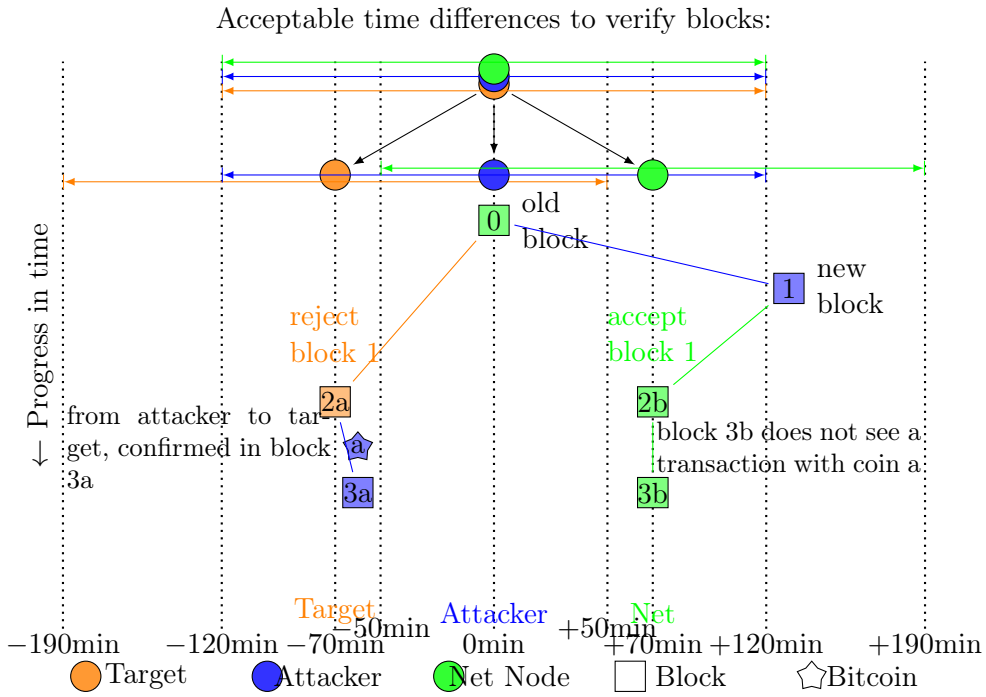

Abb. 7: Timejacking. Die Farbe von Blöcken und Bitcoins legt fest, wer die zugehörige Aktion zum Erzeugen/versenden durchgeführt hat. Kreise geben mit ihrer Farbe an, wer sich in welcher „Zeitzone“ befindet.

Das Bitcoin-Netzwerk versucht, für das **Netzwerk** eine **gemeinsame Zeit auszuhandeln**, damit klar ist welche Blöcke aktuell, und welche eventuell ungültig sind. Diese Zeit basiert auf dem Median der Zeiten aller Peers eines Knotens – unterscheidet sich der so bestimmte Wert allerdings um mehr als 70 Minuten von der Systemzeit des Rechners, wird die Systemzeit verwendet. Möchte ein Angreifer die Netzwerkzeit eines bestimmten Knotens verändern, müsste er sich zu diesem Knoten mit ein paar Clients verbinden (mehr als die Hälfte der Verbindungen genügen), und eine veränderte Zeit übermitteln. So wird es möglich, eine Zeitdifferenz von bis zu 70 Minuten zu erzeugen. Versucht man gleichzeitig, den Rest des Netzes zeitlich in die andere Richtung zu beeinflussen, entstehen bis zu 140 Minuten Zeitdifferenz zwischen den Zielknoten und dem Rest des Netzwerks, ohne dass ein Knoten auf die wirkliche Zeit zurückfallen würde.

Diese **Zeit wird** ebenfalls **verwendet**, **um Blocks zu verifizieren**. Dabei werden solche als ungültig betrachtet, deren Zeitstempel sich um mehr als 2 Stunden von der aktuellen Netzwerkzeit unterscheidet. Ebenfalls werden solche Blöcke verworfen, deren Zeitstempel früher datiert ist als der Median der letzten 11 Blöcke vorher.

Im weiteren Verlauf wird davon ausgegangen, der Angreifer habe erfolgreich die Zeit der meisten Netzknoten um fast 70 Minuten in die Zukunft verschoben, und die Zeit des angegriffenen Knotens um fast 70 Minuten in die Vergangenheit. Es wird empfohlen, den weiteren Verlauf gleichzeitig mit Abbildung 7 und dem folgenden Text nachzuvollziehen.

Erzeugt ein Angreifer nun einen Block, dessen Zeitstempel mehr als 120 Minuten vor der aktuellen echten Zeit datiert ist, würde der Zielknoten den Block nicht akzeptieren, da er für ihn mehr als 3 Stunden in der Zukunft liegt. Die anderen Knoten des Netzwerkes würden den Block allerdings akzeptieren, und beginnen, neue Blöcke an ihn anzuhängen. Neu erstellte Blöcke tragen einen Zeitstempel fast 70 Minuten in der Zukunft, gesehen von der echten Zeit – und 140 Minuten in der Zukunft, gesehen von der Zeit des Zielknotens. Alle diese Blöcke erscheinen für ihn ungültig, da sie mehr als 2 Stunden in der Zukunft liegen. Er ist effektiv **vom Netzwerk getrennt worden**.

Nun sendet der Angreifer eine Transaktion an den Zielknoten und erzeugt einen Block, der die Transaktion bestätigt und im Zeitfenster des Zielknotens liegt. Block und Transaktion werden nur an den Zielknoten geschickt. Der Zielknoten akzeptiert die Bestätigung und wird die Bezahlung in einen Gegenwert umsetzen (Versendung von Waren, Braten eines Burgers, ...).

Wird jetzt die Uhrzeit des Zielknotens zurückgesetzt (z.B. durch einen Reconnect zum Netzwerk), wird er die inzwischen gewachsene, längere, richtige Blockkette entdecken und **die alte Kette verwerfen**. Er kann eine neue Zahlung mit den gleichen Bitcoins erhalten, und würde sie trotzdem akzeptieren. Der Rest des Netzwerks hat den Angriff möglicherweise nicht bemerkt, denn bis auf die verschobene Zeit gab es keine auffälligen Aktivitäten.

4.6 Risiken bzgl. Analyse von Verkehrsdaten

Bitcoin ist ein pseudonymes Geldsystem. Durch Analyse des Datenverkehrs von Netzknoten kann ein Angreifer feststellen, zu welchem Netzanschluss welche Bitcoinadresse gehört – obwohl dies von den Clients nicht bekanntgegeben wird. Dabei beobachtet der Angreifer jede Transaktion, die von dem Client empfangen und gesendet wird. Sendet der Client eine Transaktion in das Netzwerk, die er noch nicht von einem anderen Knoten empfangen hat, so stammt sie ursprünglich von diesem Netzanschluss. Sie kann aufgrund der digitalen Signatur auch nicht von einem betrügerischen Knoten gesendet werden[12], sodass der Angreifer sicher sein kann, den richtigen Netzknoten gefunden zu haben. Dieses Problem ließe sich durch Verschlüsselung des Datenverkehrs zwischen Netzknoten verhindern. Möglicherweise wäre noch immer feststellbar, wann ein Netzknoten eine eigene Transaktion versendet – es wäre aber nicht mehr offenbar, welche Adresse ihm gehört.

Durch die öffentliche Transaktionshistore und die Verkettung von Transaktionen ist es darüber hinaus möglich, Geldflüsse zu analysieren. Dadurch ist es beispielsweise einfacher als im traditionellen System, Geldwäsche zu entdecken, da die Daten hier vollkommen öffentlich sind. Es gibt keinen Grund, warum Systeme, die im normalen Bankensystem von Strafverfolgungsbehörden eingesetzt werden, nicht auch im Bitcoinsystem gut arbeiten können sollten.

4.7 Risiken bzgl Pseudonymität/Anonymität

Bitcoinadressen sind pseudonym: Zuerst einmal kann niemand sagen, wem eine bestimmte Adresse gehört. Trotzdem kann man feststellen, von welcher Adresse jede Transaktion gestartet wurde. Zusätzlich ist die Transaktionshistorie öffentlich. Wird nun eine Adresse in der Kette der Transaktionen öffentlich bekannt,

[12] Identitätsdiebstahl wird an dieser Stelle ausgeschlossen.

z.B. weil Bob seine Adresse zum Empfangen von Spenden benutzt und gemeinsam mit seiner EMail-Adresse veröffentlicht, kann von dort eventuell verfolgt werden, wer welche Transaktion erhalten hat. Im Spendenfall ist es wahrscheinlich, dass Bob das empfangene Geld mit Alice und Charly teilt, die auch am Projekt mitarbeiten. Obwohl sie ihre Adressen nicht veröffentlicht haben kann geschlossen werden, welche dies sind, wenn Bob die empfangenen Spenden direkt weiterleitet. Denkbar sind beliebig komplexe Erweiterungen.

4.8 Risiken bzgl. Wasserzeichen und illegalen Daten

In Transaktionen können an einigen Stellen beliebige Daten untergebracht werden. Da alle Clients Kopien von mindestens den nicht verwerteten Transaktionen haben müssen wird es für einen Angreifer möglich, bestimmte Daten auf vielen Rechnern zu platzieren. Dies kann in Verbindung mit Cancer Nodes dazu verwendet werden, bestimmte Rechner zu markieren, selbst wenn ihre Speicher verschlüsselt sind (Wasserzeichenangriff). Ebenfalls ist es möglich, Daten abzulegen die in bestimmten Kontexten als illegal angesehen werden. Bitcoin könnte damit zu einem Legalitätsproblem werden, sogar wenn Bitcoin selbst nicht illegal ist.

5 Der Wert von Bitcoins

Der Wert von Bitcoin bestimmt sich genauso, wie sich der Wert anderer Devisen bestimmt.

5.1 Wertbestimmung von Währungen allgemein

Der Wert einer Währung bestimmt sich maßgeblich darüber, welchen Preis Marktteilnehmer bereit sind für eine Währung zu bezahlen. Einige Marktteilnehmer machen Angebote für den Einkauf – wieviel sie bereit sind, für eine gewisse Menge einer Währung (z.B. 500€) in einer anderen Währung zu bezahlen (z.B. 670 US-$) – oder für den Verkauf. Andere Teilnehmer nehmen dann diese Angebote an – oder eben nicht. Anhand der zustande gekommenen Verkäufe wird dann der aktuelle Wert ermittelt: Es wird der durchschnittliche Wert der letzten x Zeiteinheiten benutzt. An diesem Wert kann gemessen werden, ob der Wert einer Währung aktuell steigt, sinkt, und wie hoch er über-

haupt ist. Ebenso kann daran festgestellt werden, ob der eigene Handel aktuell zu günstigen, oder ungünstigen Konditionen erfolgt.

Ein Beispiel für eine Einrichtung, die Wechselkurse auf diese Art bestimmt, ist EuroFX (`www.eurofx.de`). Dort wird jeweils der Mittelwert der zustande gekommenen Transfers der letzten 24 Stunden von einigen teilnehmenden Kreditinstituten täglich um 13.00h veröffentlicht.

5.2 Wertbestimmung von Bitcoins

Auch bei Bitcoin wird der Marktwert ähnlich bestimmt. Für Bitcoin existieren Marktplätze, die Ver- und Einkaufsabsichten veröffentlichen, und so Verkäufer und Einkäufer zusammenbringen. Die Mittelwerte der letzten, zustande gekommenen Transfers ergibt auch hier den Marktwert. Eine Übersicht über aktuelle Marktpreise von Bitcoins ist z.B. unter `http://bitcoincharts.com/markets/` abzurufen. Dort sind auch Links zu einigen Märkten zu finden. Der größte Markt zum aktuellen Zeitpunkt ist MtGox[13] mit etwa 5,7 Millionen USD Handelsvolumen in 30 Tagen (Stand Dezember 2011).

Zwischenzeitlich wurde für einen BTC bis zu 30 USD gezahlt[14], zur Zeit liegt der Kurs um 3 USD pro BTC.

6 Politische Seite von Bitcoin

Für die politische Diskussion von Bitcoin sind einige Eigenschaften besonders interessant:

- Transaktionen sind nicht rückabwickelbar
- Konten sind nicht sperrbar
- Das System ist nicht abschaltbar
- Konten sind nicht namentlich an eine Person oder eine Organisation gebunden

Besonders der letzte Punkt wird vielfach diskutiert (siehe [3]). Es wird erwartet, dass ein Geldsystem wie Bitcoin zur Geldwäsche einlädt. Vielfach (z.B. in [7])

[13] `https://mtgox.com/`

[14] `http://bitcoincharts.com/charts/mtgoxUSD#rg360zczsg2011-06-08zeg2011-06-10ztgSzm1g10zm2g25zv`

wird in der Diskussion keine Unterscheidung zwischen Anonymität und Pseudonymität gemacht. Auch wird oft auf die Verwendung von Bitcoin in eindeutig illegalen Zusammenhängen (wie etwa SilkRoad) verwiesen. Es sei durch die Nichtabschaltbarkeit von Bitcoin-Adressen nicht möglich, kriminellen Personen und Organisationen den Zugang zu ihren Geldreserven zu verwehren. Auch, dass Transaktionen nicht rückgängig gemacht oder widerrufen werden können, wird als Nachteil für den Verbraucher aufgefasst.

Dies sind allerdings Designprinzipien von Bitcoin, da gerade Punkte wie die Nichtsperrbarkeit von einzelnen Konten adressiert werden sollte. Schließlich sind es nicht immer nur kriminelle Organisationen, denen der Zugang zu ihren Konten verwehrt wird[15].

Außerdem sind diese Punkte ebenfalls zutreffend auf Bargeld. Auch Bargeld wird in eindeutig illegalen Zusammenhängen verwendet – trotzdem gibt es keine Bestrebungen, aus diesem Gründen auf Bargeld zu verzichten und dieses abzuschaffen, da die Vorteile eindeutig überwiegen.

7 Zusammenfassung

Bitcoin ist ein Vorstoß in eine neue Richtung und offenbar der erste Versuch, ein Geldsystem auf demokratischer Basis und ohne zentrale Instanz zu unterhalten. Für viele Fragen bietet das System Antworten, es wirkt insgesamt gesehen sehr durchdacht. Die meisten Probleme kommen von der (in einigen Fällen notwendigen) Akzeptanz nicht bestätigter Zahlungen. In vielen Fällen lassen diese sich schon dadurch lösen, dass nur Zahlungen mit 5 oder mehr Bestätigungen als getätigt angesehen werden. Für die Fälle, in denen die Akzeptanz nicht bestätigter Zahlungen nötig wird ($\rightarrow$ Burger bezahlen), handelt es sich jedoch meist um so geringe Beträge, dass Aufwand und Nutzen eines Angriffs in keinem – für den Angreifer – positiven Verhältnis stehen.

Bitcoin ist, wenn man der einleitenden Definition von Issing folgt, Geld. Was dem System noch fehlt, ist eine breitere Nutzerbasis und das nötige Vertrauen, das den althergebrachten Währungen entgegengebracht wird. Ob das System dem Hype gerecht wird, der Mitte 2011 ausbrach als das System bekannter wurde, bleibt weiterhin abzuwarten – spannend ist das System jedoch auf jeden Fall.

[15] siehe: `http://wikileaks.org/`

Abbildungsverzeichnis

Literatur

[1] *Weaknesses.* `https://en.bitcoin.it/wiki/Weaknesses`. Version: Dezember 2011

[2] Bachfeld, Daniel: FBI-Backdoor in IPSec-Implementierung von OpenBSD? `http://www.heise.de/security/meldung/FBI-Backdoor-in-IPSec-Implementierung-von-OpenBSD-1153180.html`

[3] Biermann, Kai: *Wer im Netz zahlt, soll sich ausweisen.* `http://www.zeit.de/digital/internet/2011-07/internet-geld-anonymitaet`

[4] Chaum, David ; Fiat, Amos ; Naor, Moni: Untraceable Electronic Cash. In: *Proceedings on Advances in Cryptology* (1990)

[5] culubas: *Timejacking & Bitcoin.* `http://culubas.blogspot.com/2011/05/timejacking-bitcoin_802.html`. Version: Dezember 2011

[6] `https://bitcointalk.org/index.php?topic=3441.msg48384#msg48384`

[7] Fischermann, Thomas: *Anarcho-Geld.* `http://www.zeit.de/2011/27/Internet-Bitcoins`

[8] Issing, Otmar: *Einführung in die Geldtheorie*. 15. Auflage. Vahlen, 2011. – ISBN 978–3–8006–3810–9

[9] Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System. (2009), Mai. `http://www.bitcoin.org/bitcoin.pdf`

[10] Pritlove, Tim ; Bogk, Andreas: *Elektronisches Geld: Von eCash bis Bitcoin*. `http://chaosradio.ccc.de/archive/chaosradio_express_182_elektronisches_geld.mp3`. Version: Juni 2011

[11] Richter, Marcus ; Bogk, Andreas ; Kobschätzki, Niels: *Bitcoins: Von Netzgeld und Geldnetzen*. `http://chaosradio.ccc.de/archive/chaosradio_169.mp3`. Version: Juni 2011