

# Sicherheit und Datenschutz bei Bitcoin

Danny Leonhardt

Technische Universität Dresden  
Fakultät Informatik  
Professur Datenschutz und Datensicherheit  
[s8186045@mailbox.tu-dresden.de](mailto:s8186045@mailbox.tu-dresden.de)

**Zusammenfassung** Bitcoin hat den Anspruch, ein dezentrales, sicheres elektronisches Zahlungssystem ohne die Notwendigkeit von vertrauenswürdigen Dritten zu sein. Diese Arbeit untersucht, inwiefern Bitcoin den Anforderungen an ein sicheres Zahlungssystem gerecht wird. Die im Protokoll festgelegten Mechanismen bieten einen starken Schutz für Transaktionen im System selbst. Wird ein Nutzer aber angegriffen, bevor diese Mechanismen wirken können, erweist sich das Fehlen einer übergeordneten Instanz als Problem. Dass Transaktionen nicht rückgängig gemacht werden und Bitcoins endgültig verloren gehen können, kann für den Nutzer einen großen finanziellen Schaden bedeuten. Die oft behauptete Anonymität des Systems hält nicht stand, sobald externe Informationen mit dem Bitcoin-Netzwerk verknüpft werden.

## 1 Einleitung

Zeitgleich mit dem Wachstum des kommerziellen Handels im Internet wuchs auch der Wunsch nach einem einsatzfähigen digitalen Zahlungsmittel. Bitcoin ist der Versuch, elektronisches Geld ohne Bindung an eine analoge Währung bereitzustellen. Bitcoin ist die heute aktuellste Implementierung einer elektronischen Währung. Der Öffentlichkeit vorgestellt wurde es im Jahr 2008 durch Satoshi Nakamoto, veröffentlicht wurde eine erste Version im Januar 2009.[1] Die technischen Grundlagen, auf denen es aufbaut, bestehen für sich allerdings schon deutlich länger. Ein direkter Vorgänger von Bitcoin ist das von Wei Dai bereits 10 Jahre eher vorgestellte Konzept des b-money, welches bereits die Möglichkeit des Erzeugens von Geldes durch einen Proof-Of-Work vorstellte, aber nie über den Status einer Idee hinaus kam.[2] Ein noch früherer Vorgänger ist das von David Chaum entwickelte und von der Firma DigiCash vertriebene eCash.[3] Obwohl eCash technisch ausgereift war, bereits die Möglichkeit anonymen Geldzahlens und -empfangens bot und auch einige Verbreitung fand, ging es in Folge des Bankrotts der Firma DigiCash unter. Einen großen Bekanntheitsgrad erlangte Bitcoin im Sommer des Jahres 2011, als es im Zusammenhang mit Drogengeschäften und dem Anstieg des Tauschkurses auf bis zu 30 Dollar pro Bitcoin auch außerhalb des Internets zum Thema in den Medien wurde. Ob Bitcoin sich neben konkurrierenden, bereits etablierten Systemen wie Paypal behaupten kann, wird neben rechtlichen Fragen vor allem auch von den implementierten

Sicherheitsmechanismen abhängen, die im Folgenden genauer betrachtet werden sollen.

## 2 Eigenschaften von Bitcoin

Es soll hier nur ein kurzer Überblick über das Bitcoin-System gegeben werden. Für die Sicherheit wichtige Eigenschaften werden unter Abschnitt 4 näher vorgestellt. Die wichtigste Eigenschaft von Bitcoin ist seine Dezentralität. Alle Daten wie Transaktionen und Geldschöpfungen werden in einem Peer-To-Peer-Netzwerk verteilt, anstatt durch eine zentrale Stelle verwaltet zu werden. Transaktionen zwischen den Teilnehmern des Netzes erfolgen über digitale Pseudonyme. Die Transaktionen werden signiert und in einer für alle Teilnehmer öffentlichen Historie gespeichert. Sowohl die Bitcoins als auch die Pseudonyme der Teilnehmer sind öffentliche Schlüssel eines Schlüsselpaars. Um mit Bitcoins handeln zu können, muss der Nutzer eine Open-Source Software herunterladen und installieren. Diese Software erzeugt eine elektronische Geldbörse, welche den Speicherplatz für die Bitcoins und Adressen des Nutzers darstellt.

### 2.1 Blöcke

Alle in Bitcoin stattfindenden Transaktionen werden in Blöcken zusammengefasst und im Netzwerk der Teilnehmer verteilt. Ein einzelner Block enthält mindestens einen Verweis auf den vorhergehenden Block, einen Teil oder alle Transaktionen, die seit Erzeugung des letzten Blocks stattgefunden haben sowie einen Proof-Of-Work. Die Blöcke bilden so eine Kette, die alle bislang getätigten Transaktionen enthält und so eine Transaktionsgeschichte nicht nur jeder einzelnen Geldeinheit sondern des gesamten Systems darstellt.

### 2.2 Mining

Mining bezeichnet das Erzeugen neuer Blöcke. Mit einer speziellen Software versuchen die Teilnehmer Lösungen für eine mathematische Aufgabe zu finden. Die Schwierigkeit dieser Aufgabe ist bekannt und wird so gewählt, dass das Netzwerk die Lösung innerhalb einer bestimmten Zeitspanne findet und so die Zahl neuer Blocks konstant bleibt. Der Teilnehmer, der die richtige Lösung findet, veröffentlicht diese als Proof-Of-Work in einem neuen Block und erhält dafür neu erzeugte Bitcoins. Da neues Geld losgelöst von einer analogen Währung durch das Computernetzwerk geschöpft wird, ist im Gegensatz zu Paypal und eCash auch keine Anbindung an eine bestehende Währung nötig. Die Menge der Bitcoins ist mathematisch auf 21 Millionen begrenzt.

## 3 Anforderungen an elektronisches Geld

Jedes Zahlungssystem muss bestimmten Anforderungen genügen, um seine gewünschte Funktion zu erfüllen, also Geld sicher von einer Stelle zu einer anderen transferieren zu können. Bezogen auf Bitcoin sind dies nach [4]:

- Ein Nutzer kann erhaltene Bitcoins transferieren
- Bitcoins gehen einem Nutzer nur dann verloren, wenn dieser den Willen dazu hat
- Von einem zahlungswilligen Nutzer an einen eindeutig bestimmten anderen Nutzer gesendete Bitcoins können auch nur von diesem empfangen und genutzt werden
- Ein vollzogener Transfer muss dritten gegenüber nachweisbar sein
- Auch bei Zusammenarbeit mehrerer Nutzer dürfen diese nicht in der Lage sein, ihre Bitcoins unrechtmäßig zu vermehren.

Kann Bitcoin diese Anforderungen erfüllen, gilt es bezüglich Verfügbarkeit und Integrität als sicher. Des Weiteren gilt es, die Mehrfachausgabe von Geld (Double-Spending-Problem) zu verhindern und Fälschungssicherheit zu gewährleisten. Bitcoin wird oft als „anonymes Zahlungssystem“ bezeichnet. Will es dem gerecht werden, muss die Identität des Geldsenders gegenüber dem Empfänger geschützt werden, ebenso wie gegenüber dritten. Die Entwickler selbst betrachten Anonymität nicht als Hauptziel von Bitcoin. Da dies aber nicht unbedingt der öffentlichen Wahrnehmung entspricht, muss den Nutzern bewusst gemacht werden, wieviel Vertraulichkeit sie tatsächlich erwarten können.

## 4 Sicherheitsmechanismen von Bitcoin

### 4.1 Öffentliche Schlüssel und Bitcoin-Adressen

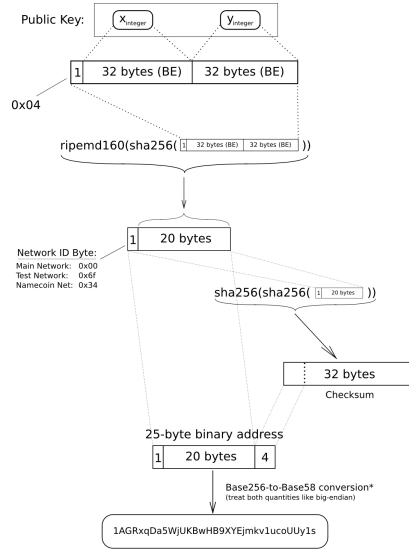
Bitcoin-Adressen sind das zentrale Element des Protokolls. Alle Transaktionen erfolgen zwischen Adressen. Auch die Erzeugung neuer Bitcoins ist eine Transaktion an ein neue erzeugte Adresse. Grundlage jeder Bitcoin-Adresse ist der öffentliche Teil eines ECDSA-Schlüsselpaars. Dieser Schlüssel wird wie in Bild 1 dargestellt mit SHA256 und RIPEMD-160 mehrfach gehasht und letztendlich auf 160Bit verkürzt. Dies dient weniger der Sicherheit als mehr der Lesbarkeit und Handhabbarkeit der Adressen. Die Bitcoin-Adresse und der zugehörige private Schlüssel werden in der Geldbörse wallet.dat gespeichert. Sowohl ECDSA als auch SHA256 gelten als sicher und werden in verschiedenen Standards empfohlen, etwa auch vom National Institute of Standards and Technology, dass Sicherheitsstandards für amerikanische Behörden verwaltet. [5][6] Die Wahl der für den ECDSA-Algorithmus verwendeten Kurve secp256k1 ist außergewöhnlich und erfolgte laut Nakamoto „zufällig“. Die Kurve scheint eine bessere Performance zu haben als die öfter verwendeten zufälligen Kurven, was teilweise als Hinweis auf Sicherheitsprobleme gedeutet wird.[7] Ein Beweis dafür steht aber noch aus.

Jeder Nutzer kann sich beliebig viele neue Adressen und damit Schlüsselpaare erzeugen. Dies geschieht lokal und völlig unabhängig vom Netzwerk.

### 4.2 Transaktionen

Will nun Nutzer eine bestimmte Anzahl Bitcoins an Nutzer B senden, benötigt er zuerst eine Bitcoin-Adresse  $addr_B$  von Nutzer B sowie eine eigene Adresse

### Elliptic-Curve Public Key to BTC Address conversion



\*In a standard base conversion, the 0x00 byte on the left would be irrelevant (like writing '052' instead of just '52'), but in the BTC network the left-most zero chars are carried through the conversion. So for every 0x00 byte on the left end of the binary address, we will attach one '1' character to the Base58 address. This is why main-network addresses all start with '1'  
 etotheipi@gmail.com / 1Gffm7LkXcNFPrty6yF4jBoe5rVka4sn1

**Abbildung 1.** Umwandlung eines öffentlichen Schlüssels in eine Adresse

mit Bitcoins,  $addr_A$ , die er durch eine vorhergehende Transaktion bekommen hat, etwa durch Mining. Eine Transaktion besteht aus Inputs und Outputs. Ein Output gibt an, wieviele Bitcoins an welche Adresse geschickt werden sollen. Ein Input besteht aus einem Verweis auf den Output einer vorherigen Transaktion. Die Transaktion  $t_1$  besteht also aus einem Verweis auf mindestens eine vorherige Transaktion  $t_{prev}$ , einem Index auf deren gewählten Output  $out_i$ , der Adresse  $adr_{receiver}$  an die die Bitcoins gesendet werden soll, sowie die Anzahl der zu sendenden Bitcoins  $amount$ . Jeder Input wird mit dem privaten Schlüssel  $pk_{t_{prev}}$  signiert, der zur entsprechenden Adresse der vorherigen Transaktion gehört:

$$\begin{aligned}
 input_1 &= (t_{prev}, out_i) \\
 output_1 &= (adr_{receiver}, amount) \\
 transaction &= hash((sign(input_1, pk_{t_{prev}})), (output_1))
 \end{aligned}$$

Die Transaktion wird nun dem Netzwerk bekanntgegeben. Jeder Nutzer in Besitz des öffentlichen Schlüssels von A und B kann überprüfen, dass B der tatsächlich gewollte Empfänger der Bitcoins ist, da seine Adresse in der Transaktion angegeben wurde. Außerdem kann überprüft werden, dass A tatsächlich die Bitcoins gesendet hat, denn nur er ist im Besitz des privaten Schlüssels, der zur Adresse in der vorherigen Transaktion gehört. Durch die angegebene vorherige

Transaktion kann wiederum zurückverfolgt werden, woher A das Recht an diesen Bitcoins hatte.[1] Die Transaktion gilt allerdings erst als endgültig bestätigt, wenn wenigstens sechs Blöcke die Richtigkeit bestätigen, um eine Mehrfachausgabe von Geld zu verhindern.[9]

Eine Transaktion kann mehrere Adressen besitzen, aus denen das Geld abgehoben wird. Ebenso kann sie mehrere Adressen als Empfänger besitzen. Letzteres geschieht auch immer dann, wenn nicht das komplette Geld einer Adresse aufgebraucht wird. Das Restgeld wird an eine neue Adresse des Senders überwiesen.

### 4.3 Verhindern von Double-Spending mit einem Proof-Of-Work

Wie kann B sich nun sicher sein, dass A das Geld ausschließlich ihm gesendet und nicht mehrfach ausgegeben hat? Da es im Bitcoin-Netzwerk keine zentrale Autorität gibt, welche die doppelte Ausgabe von Geld kontrollieren könnte, muss auch diese Kontrolle durch die Teilnehmer des Netzwerks erfolgen. Die von Bitcoin umgesetzte Mechanik basiert auf einem Vorschlag von Adam Back.[8]

Zunächst wird festgelegt, dass bei der Mehrfachausgabe von Geld nur die jeweils erste Transaktion Gültigkeit hat. Transaktionen müssen also Timestamps bekommen. Dies geschieht in Blöcken von Transaktionen. Um zu gewährleisten, dass keine manipulierten Blöcke erzeugt werden, ist das Erstellen jedes Blocks mit einem Proof-Of-Work verbunden: Der SHA256-Hash eines Blocks muss kleiner als ein bestimmter Grenzwert sein. Dazu muss im Block ein passender Wert für einen 32 Bit großen Nonce gefunden werden. Der Block wird anschließend veröffentlicht, inklusive des Nonce, des Hashs und des Timestamps und einem Verweis auf den vorhergehenden Block. Ein Block wird allgemein akzeptiert, wenn eine Überprüfung die Korrektheit der Transaktionen und des Nonce ergibt.

Eine Änderung eines Blocks würde eine komplette Neubearbeitung des Proof-Of-Work erfordern, da auch kleinste Änderungen des Inputs in SHA256 zu großen Änderungen im Hash führen. Wollte ein Angreifer einen manipulierten Block in die Blockkette einführen, müsste er nicht nur den Block selbst, sondern auch alle darauf folgenden Blöcke und damit deren Proof-Of-Work bearbeiten. Er bräuchte aber mehr als die Hälfte der Rechenkapazität des gesamten Netzes um die längste Kette an Blocks zu erzeugen, denn nur diese wird als korrekt identifiziert. Hätte ein Angreifer tatsächlich so viel Rechenkapazität, könnte er eigene Transaktionen rückgängig machen und das Geld erneut ausgeben sowie die Bestätigungen für andere Transaktionen verhindern oder zumindest verzögern. Bei so viel Rechenkapazität wäre es aber lukrativer, durch die Einnahme von Transaktionsgebühren Geld zu verdienen, womit solch ein Angriff an Sinn verliert.

### 4.4 Fälschungssicherheit

Neue Bitcoins entstehen durch das Finden neuer Blöcke und dem damit verbundenen Proof-Of-Work. Diese Bitcoins sind selbst auch nur spezielle Transaktionen, die keine Vorgängertransaktion haben. So lange die Mehrheit der Teilnehmer ehrlich ist, werden in der Blockkette nur gültige Transaktionen akzeptiert

und für jede Adresse, die Bitcoins besitzt, kann nachgeprüft werden, wo diese Bitcoins ursprünglich herkommen. Eine Fälschung ist in diesem Sinne nicht möglich.

#### 4.5 Bruch von SHA256 oder ECDSA

Was für Auswirkungen hätte nun ein zukünftiger Bruch von SHA256 oder ECDSA? Ein Bruch von SHA256 hätte zunächst keine Auswirkungen auf die Schlüssel und Bitcoin-Adressen, da die dort verwendeten Hashs nicht zur Sicherheit beitragen. Es würde aber dazu führen, dass der Proof-Of-Work zunächst nutzlos wird. Nutzt nur ein Angreifer die Sicherheitslücke, könnte er in die Blockkette eingreifen, da er den anderen Teilnehmern gegenüber einen großen Rechenvorteil hat. Wird die Lücke aber weitläufiger bekannt, würde sich automatisch die Schwierigkeit des Proof-Of-Works erhöhen. Dies könnte eventuell schon ausgleichend wirken, oder aber eine neuer Proof-Of-Work müsste implementiert werden. Würde ECDSA gebrochen, könnte ein Angreifer etwa aus bekannten öffentlichen Schlüsseln die zugehörigen privaten Schlüssel erzeugen und so das damit verknüpfte Geld selbst nutzen. Ein solches Sicherheitsloch würde nicht nur zu einem technischen Zusammenbruch von Bitcoin führen, sondern das Geld auch komplett entwerten. Vermutlich würde ECDSA erst für bestimmte Kurven gebrochen. Ob hier die Wahl einer eher speziellen Kurve ein Nachteil wird, muss sich in Zukunft zeigen.<sup>[10]</sup>

#### 4.6 Potentieller Angriff: Adresswechsel

Eine Möglichkeit, eine Transaktion doch zu manipulieren, entsteht durch einen Angriff direkt beim Sender. Das Bitcoin-Protokoll spielt dabei selbst keine Rolle. Ein Angreifer kann dem Sender zum Beispiel unbemerkt eine manipulierte Version des Bitcoin-Clients unterschieben, etwa direkt beim Download oder später durch eine eingeschleufte Schadsoftware. Dieser manipulierte Client unterscheidet sich in nichts vom originalen Client, außer, dass die eingegebene Empfängeradresse durch eine vom Angreifer gewählte Adresse ersetzt wird. Erst dann wird die Transaktion erstellt und signiert, die Sicherheitsmechanismen werden umgangen und es entsteht eine legitime, vom Sender aber natürlich nicht gewünschte Transaktion. Sobald die Transaktion veröffentlicht wurde, kann der Sender (und auch jeder andere) aber natürlich kontrollieren, an wen das Geld wirklich gesendet wurde. Er weiß jetzt, dass eine Manipulation stattgefunden hat und kann seinen Klienten überprüfen. Er weiß auch, welche Adresse das Geld bekommen hat. Um die Transaktion rückgängig zu machen, müsste der Block, der die Transaktion beinhaltet, gelöscht werden, inklusive aller darin enthaltenen weiteren Transaktionen, was wiederum Auswirkungen auf andere Geschäfte hat (z.B. könnte bei einer Transaktion gegen eine Ware diese schon geliefert worden sein). Auch alle nachfolgenden Blöcke und deren Transaktionen wären davon betroffen. Alle betroffenen Blöcke müssten neu erstellt werden, was auch wieder für jeden Block einen Proof-Of-Work bedeutet. Es ist also nicht möglich, die Transaktion rückgängig zu machen.

Durch Mechanismen wie Programm-Code-Prüfsummen könnten den Angriff zwar schwieriger machen, aber nie ganz ausschließen.

#### 4.7 Sicherheit der Geldbörse

Die Bitcoin-Geldbörse enthält alle Adressen und die zugehörigen Schlüssel des Nutzers. Im originalen Client werden die Adressen in einer Berkeley DB-Datenbank gespeichert, die sich in der Datei `wallet.dat` befindet. Diese Datenbank ist transaktional und sehr performant, empfangene Transaktionen speichert sie unmittelbar bei deren Eingang.<sup>[12]</sup> Ein Verlust von Geld durch einen Systemabsturz wird so unwahrscheinlicher gemacht. Die in der Datei enthaltenen Schlüssel können seit Version 0.4 verschlüsselt werden. Dies ist allerdings optional und auch nur ein Feature des Original-Clients. Bei dieser Art der Verschlüsselung werden auch nur die privaten Schlüssel gesichert, alle anderen Informationen bleiben unverschlüsselt.

Beim Verlust einer herkömmlichen Geldbörse stehen die Chancen gut, dass eine andere Person sie findet, es sei denn, die Geldbörse ging in einer schwer zugänglichen Gegend verloren. Der Finder kann sie nun entweder zurückgeben oder aber das Geld selbst nutzen, was auf die gleichen Folgen wie ein Diebstahl hinausläuft. Im Fall von Bargeld bemerkt der Besitzer zwar den Diebstahl, die Verwendung des gestohlenen Geldes aber kann er nicht verfolgen. Verliert man auch seine EC- oder Kreditkarte, kann man diese sperren lassen. Geschieht dies nicht rechtzeitig, können eventuell schon getätigte Transaktionen ganz oder teilweise durch die autorisierende Stelle (die Bank) rückgängig gemacht werden. Wird nicht die Karte selbst sondern die bei Onlinegeschäften benötigten Daten gestohlen (Kreditkartennummer, Gültigkeitsdauer, Sicherheitsnummer etc.), kann dies wiederum vom Nutzer unbemerkt geschehen, die Folgen können aber immer noch ganz oder teilweise rückgängig gemacht werden.

Bei Verlust einer Bitcoin-Geldbörse sind die Folgen andere. Geht die Datei tatsächlich ganz verloren, etwa durch eine zerstörte Festplatte, geht auch das damit verbundene Geld endgültig verloren. Dies gilt nicht nur für den Nutzer, sondern für das gesamte System. Die maximal mögliche Menge an Bitcoins reduziert sich also. In der Transaktionsgeschichte lässt sich zwar ablesen, an welche Adresse die verloren gegangenen Bitcoins zuletzt gesendet wurden, mangels privatem Schlüssel kann aber niemand mehr den Besitz nachweisen.

Um eine Bitcoin-Geldbörse zu stehlen, genügt es bei einer unverschlüsselten Datei bereits, wenn ein Angreifer eine Kopie der Datei erstellen kann. Die Bitcoins können jetzt sowohl vom rechtmäßigen Besitzer als auch vom Angreifer verwendet werden. Diese Dopplung wird erst aufgelöst, nachdem einer der beiden die Bitcoins in einer Transaktion genutzt hat. Hat der Angreifer die Bitcoins genutzt, würde eine Nutzung durch den rechtmäßigen Besitzer als Mehrfachausgabe verworfen werden. Der rechtmäßige Besitzer sieht nun zwar, an welche Adresse sein Geld gesendet wurde, kann die Transaktion aber nicht mehr rückgängig machen. Merkt der Besitzer rechtzeitig, dass seine Geldbörse kompromittiert wurde, kann er dem Angreifer zuvorkommen und alle Bitcoins in eine neue Geldbörse überweisen. Der Angreifer hätte dann zwar alle Schlüssel

und Adressen der gestohlenen Geldbörse, aber kein Geld, dass er damit ausgeben kann. Da das Kopieren der Geldbörse unbemerkt geschehen kann, hat der Angreifer allerdings einen großen Vorteil. Das Bitcoin-Konzept ohne zentrale Autorität stellt hier ein Sicherheitsrisiko für den Nutzer dar.

Zum Schutz der Geldbörse sollte diese also komplett verschlüsselt sein, etwa durch einen Truecrypt-Container, und es sollte ein sicheres Backup erstellt werden. Dies schützt aber natürlich trotzdem nicht vor einem Angreifer, der den Rechner des Besitzers bereits vollständig unter Kontrolle hat. Durch eine Verschlüsselung steigt wiederum das Verlustrisiko: Kann man die Datei nicht mehr entschlüsseln, ist das Geld verloren.

Es ist auch möglich, die Geldbörse bei einem Onlineanbieter zu führen. Damit legt man aber die volle Verfügungsgewalt in die Hand des Anbieters, was ein hohes Maß an Vertrauen erfordert. Außerdem sind solche Sammlungen von Geldbörsen natürlich auch attraktiv für Angreifer.

Ein behaupteter Angriff durch Kopieren der Geldbörse eines Bitcoin-Nutzers fand im Juni 2011 statt und hatte zu diesem Zeitpunkt einen erbeuteten Wert von etwa einer halben Million US-Dollar zur Folge. [11]

## 5 Datenschutz und Anonymität

In der öffentlichen und medialen Berichterstattung wird das Bitcoin-System oft als anonym bezeichnet und diesbezüglich mit Bargeld verglichen.[13][14] Ein erster Blick bestätigt diese Vermutung. Um Dienste wie Paypal oder Moneybookers nutzen zu können, muss man die Daten für ein bereits bestehendes Bankkonto oder einer Kreditkarte hinterlegen. Damit liegen bereits direkt beim Anbieter verifizierte Daten wie der eigene Name, die Kontonummer und ähnliches vor. Durch Kommunikation mit der Bank des Teilnehmers lassen sich noch deutlich mehr Daten erfahren. Um mit Bitcoins handeln zu können, wird hingegen nur eine Software benötigt. Es ist keine Registrierung notwendig, nicht einmal eine E-Mail-Adresse. Alle Transaktionen finden nur zwischen den in Abschnitt 4.1 dargestellten Adressen statt.

Benutzt man für alle Transaktionen nur eine einzige Bitcoinadresse, erreicht man bereits die Anonymität eines Geschäftsbeziehungsseudonyms. Bitcoin motiviert aber die Erstellung einer neuen Adresse für jede Transaktion. Den Nutzer kostet dies eine sehr kleine Menge Speicherplatz, auf das Netzwerk hat die Erstellung einer Adresse überhaupt keine Auswirkungen. Im Original-Client wird automatisch nach jeder Transaktion eine neue Adresse vorgeschlagen. Durch diese Nutzung der Adressen erreicht man die Anonymität eines Transaktionsseudonyms. In herkömmlichen Systemen hat man mit der Kontonummer meist ein nichtöffentliches Personenpseudonym. Die Zuordnung zu einer Identität ist nur wenigen Stellen bekannt, so lange kein Name zur Nummer angegeben wird.[4] Die von Bitcoin erreichte Anonymität ist zunächst also deutlich stärker als die anderer Geldsysteme, mit Ausnahme von Bargeld.

## 5.1 Rückverfolgbarkeit

Durch die Veröffentlichung jeder Transaktion an alle Teilnehmer und die Struktur der Transaktionsgeschichte ermöglicht Bitcoin allerdings die totale Rückverfolgbarkeit von Geld. Dies ist in anderen Zahlungssystemen nur schwer oder gar nicht möglich und ist eine Besonderheit der Bitcoins. Sobald durch das Erzeugen eines Blocks ein Nutzer A Bitcoins gutgeschrieben bekommt, wird dies in einer Generierungs-Transaktion öffentlich festgehalten. Nutzt A nun dieses Geld, um einem Nutzer B etwas zu überweisen, prüft Nutzer B, dass die Bitcoins wirklich A gehörten. Diese Kette wird immer weiter gereicht, so dass irgendwann ein Nutzer K, und alle anderen Teilnehmer des Bitcoin-Netzwerks das von K erhaltene Geld über alle Stationen hinweg bis zurück zu ihrer Generierung für A zurückverfolgen können. Betrachtet man das Netzwerk nur für sich, hat das keine Auswirkungen auf die Anonymität. Die Nutzung von Bitcoins wäre aber sinnlos, wenn man mit ihnen nichts kauft. Doch sobald die Bitcoins gegen Waren und Dienstleistungen oder andere Währungen ausgetauscht werden, beginnt die Anonymität zu sinken.

## 5.2 Deanonymisierung

Im Folgenden soll grob ein Szenario skizziert werden, in dem Bitcoinadressen eines Online-Shop-Kunden ihre Anonymität verlieren. Ein Nutzer Bob besitzt mehrere Bitcoin-Adressen, darunter die beiden Adressen *12yfLbr* und *16u9P3E* mit je vier Bitcoins. Er kauft beim Online-Händler Shop42 ein Buch und bezahlt dafür sechs Bitcoins an die Händler-Adresse *1KvBAbv*. Um die Ware zu sich nachhause geliefert bekommen zu können, muss er seinen echten Namen und seine Adresse beim Händler hinterlegen. Die Transaktion, mit der die Ware in Bitcoins bezahlt wird, wird dem Netzwerk bekanntgegeben. Jeder Nutzer hat jetzt folgende Informationen zur Verfügung:

- Die Input-Adressen *12yfLbr* und *16u9P3E* gehören ein und demselben Nutzer X
- Nutzer X hatte vor der Transaktion auf beiden Adressen je vier Bitcoins
- Output-Adresse *1KvBAbv* erhält sechs Bitcoins, Adresse *19eLATL* erhält zwei Bitcoins (das übrig gebliebene Wechselgeld)

Jedem Teilnehmer ist also bekannt, dass die zwei Bitcoin-Adressen einem Nutzer gehören, dem wahrscheinlich auch noch eine der Output-Adressen gehört. Dies ist noch kein Bruch der Anonymität. Der Händler aber kann den Input-Adressen den Namen und die Lieferadressen aus seiner Kundendatenbank zuordnen. Außerdem weiß er, welche der Output-Adressen ihm selbst gehört, und welche Adresse für das Wechselgeld bestimmt ist. Die ihm vorliegenden Informationen sind also schon viel präziser:

- Die Adressen *12yfLbr* und *16u9P3E* gehören Käufer Bob, wohnhaft in Dresden, Rathausstraße 24
- Käufer Bob besitzt insgesamt acht Bitcoins

- Käufer Bob kauft das Buch „Datenschutz für Dummies“ für sechs Bitcoins
- Käufer Bob besitzt nach dem Kauf noch zwei Bitcoins auf Adresse *19eLAtL*

Wenige Tage später enthält eine Transaktion zwei Bitcoins von Bobs Adresse *19eLAtL* und weitere sechs Bitcoins von einer anderen Adresse *12cbQLT*. Die Output-Adresse *1Q2TWHE* erhält fünf Bitcoins und Adresse *1JhXuRH* erhält drei Bitcoins. Für jeden Nutzer außer Bob und dem Händler sehen die Informationen wieder so aus, wie in der ersten Transaktion beschrieben. Der Händler kann aber sein Wissen auf diese Transaktion anwenden und weiß zusätzlich nun auch:

- Bob besitzt zusätzlich die Adresse *12cbQLT* mit sechs Bitcoins
- Bob besitzt entweder die Adresse *1Q2TWHE* mit fünf Bitcoins oder die Adresse *1JhXuRH* mit drei Bitcoins

Später erhält der Händler eine Bestellung, die von Adresse *1JhXuRH* bezahlt wird. Durch Verknüpfung mit seiner Kundendatenbank erhält er nicht nur Informationen zu Alice, der die Adresse gehört, sondern auch weitere Informationen zu Bob, denn er weiß jetzt, welche der beiden Output-Adressen zu ihm gehört:

- Bob besitzt die Adresse *1Q2TWHE* mit fünf Bitcoins

Bekommt Bob von einem weiteren Nutzer auf eine seiner bekannten Adressen eine Einzahlung, etwa drei Bitcoins auf *1Q2TWHE*, wird auch dies dem Händler bekannt. Er weiß insgesamt also:

- Die Adressen *12yfLbr* und *16u9P3E* gehören Käufer Bob, wohnhaft in Dresden, Rathausstraße 24
- Käufer Bob wohnt in Dresden, Rathausstraße 24
- Käufer Bob besitzt insgesamt acht Bitcoins
- Käufer Bob kauft das Buch „Datenschutz für Dummies“ für sechs Bitcoins
- Käufer Bob besitzt nach dem Kauf noch zwei Bitcoins auf Adresse *19eLAtL*
- Bob besitzt die Adresse *1Q2TWHE* mit acht Bitcoins
- Bob hatte einen finanziellen Kontakt mit Alice

Diese Liste lässt sich solange erweitern, wie die bekannten Adressen für eingehende oder ausgehende Transaktionen verwendet werden. Zusätzlich hat der Händler analoge Informationen zu den Adressen von Alice und allen weiteren seiner Kunden, die mit Bitcoins bezahlen. In diesem Szenario findet der Kontakt zwischen zwei der Kunden direkt statt, je nach Kundenanzahl des Händlers sind solche Direktverbindungen wahrscheinlicher oder unwahrscheinlicher. Aber auch indirekte Verbindungen können weiterverfolgt werden, da ja alle Transaktionen offen liegen. Die Beziehungen der einzelnen Adressen lassen sich umso leichter verknüpfen, desto öfter eine Adresse wiederverwendet wird. Eine ähnliche Verknüpfbarkeit wie dargestellt gibt es natürlich auch, wenn Bitcoins im Tausch gegen eine andere Währung gekauft werden.

Diese Deanonimisierbarkeit hat auch Auswirkungen auf die unter Abschnitt 4.6 und 4.7 beschriebenen Angriffe. Dem Angreifer nutzen die Bitcoins nichts,

wenn er sie nicht irgendwann gegen eine andere Wahrung oder eine Ware austauscht. Gelingt es dem Diebstahlsopfer oder einer Strafverfolgungsbehore, innerhalb des weiteren Weges der Bitcoins die Identitat eines Adressinhabers festzustellen, kann die Kette eventuell bis zuruck zum Angreifer aufgelost werden.

Es ist moglich, eine einmal erfolgte Deanonymisierung wieder aufzuheben, indem man die kompromittierten Adressen mit einem anderen Nutzer tauscht. Dies kann zum Beispiel uber einen Mixing-Service geschehen: Viele Nutzer zahlen ihre Bitcoins in einen groen Pool ein, aus dem sie dann wieder Geld abheben. Die Anonymitat eines solchen Mixes steigt mit der Zahl der Nutzer. Problematisch ist, dass der Anbieter des Service letztendlich im Besitz aller Bitcoins der Nutzer ist und dieses auch fur sich selbst nutzen kann. Es ist also ein hohes Ma an Vertrauen erforderlich.

Eine weitere Angriffsmoglichkeit auf die Anonymitat stellt das Abhoren des Netzwerkverkehrs dar. Kann etwa ein Internet Service Provider zuordnen, von welcher IP-Adresse eine Transaktion an das Bitcoin-Netzwerk gesendet wurde, kann er die Absenderadresse und die bei ihm zur entsprechenden IP vorliegenden Daten verknupfen und die Anonymitat auflosen. Einen Schutz dagegen bietet die Nutzung eines Anonymisierungsdienstes wie Tor.

### 5.3 Analyse der Anonymitat durch Reid und Harrigan

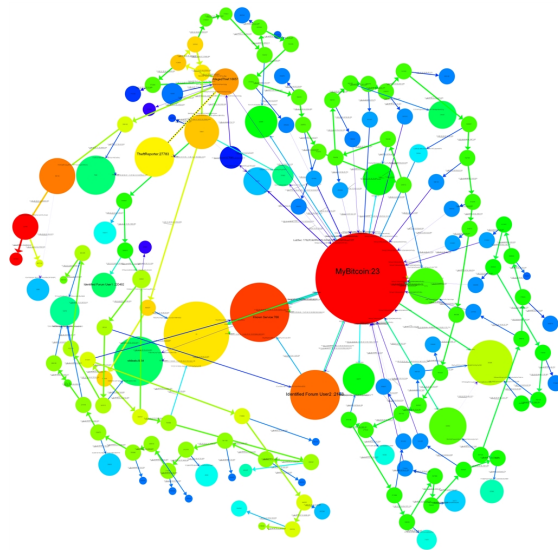
Um Bitcoin-Adressen mit Informationen zu dessen Inhabern verknupfen zu konnen, ist nicht unbedingt der direkte Kontakt zu den Nutzern erforderlich. Eine andere Moglichkeit besteht darin, zum Beispiel Foren nach Bitcoin-Adressen abzusuchen, und zusammen mit den Nutzernamen der Poster und wenn vorhanden auch deren weiteren Kontaktdaten abzuspeichern. Diese Daten konnen dann wiederum fur weitere Suchen verwendet werden.

Die bislang wohl umfangreichste Studie der Auswirkung der offentlichen Transaktionshistorie erfolgte durch Fergal Reid Martin Harrigan.[15] In ihrer Analyse betrachteten sie alle zwischen dem 3. Januar 2009 und dem 12. Juli 2011 erfolgten Transaktionen. Aus den Daten erstellen sie zwei Netzwerk-Graphen. Im Transaktions-Netzwerk reprasentiert ein Knoten eine Transaktion und jede gerichtete Kante zwischen zwei Knoten den Output an der Quelle und den entsprechenden Input am Ziel. Im Nutzer-Netzwerk steht jeder Knoten fur einen Nutzer und jede Kante fur eine Transaktion. Entgegen der Erwartung der Autoren lassen sich aus dem Nutzer-Netzwerk viele zyklische Verbindungen ablesen, anstatt in viele nicht verbundene Einmaladressen aufgeteilt zu sein. Trotz der Empfehlung, Adressen nicht wieder zu verwenden, scheinen viele Nutzer also nicht standig neue Adressen anzulegen, was die Anonymitat der genutzten Adressen vermindert.

Um den Adressen indentifizierende Informationen zuordnen zu konnen, sammelt man zunachst offentlich gemachte Adressen, die bereits mit anderen Daten verbunden sind. Das konnen zum Beispiel die IP-Adressen von Spendern auf einer Bitcoin-Spendenwebseite sein oder von den Nutzern selbst in einem Forum oder auf Twitter unter ihrem Nutzernamen veroffentlichte Adressen. Diese

Daten werden zusammen gespeichert. Mit Hilfe der jetzt schon vorhandenen Informationen können weitere Daten gesammelt werden, zum Beispiel über andere Dienste bei denen der gleiche Nutzernamen verwendet wird. Diese Daten werden nun den Adressen im Transaktions-Netzwerk zugeordnet. In vielen Transaktionen tauchen dann als Input bereits bekannte zusammen mit bislang unbekannt Adressen auf. Diese Adressen müssen aber zwingend dem gleichen Nutzer gehören. Durch die Wiederverwendung der Adressen werden so viele bisher unbekannt Adressen mit Informationen zu ihrem Besitzer verbunden. Da nun bekannt ist, welche Adressen welchem Nutzer gehören, entstehen auch bislang unentdeckte Verbindungen zwischen den Knoten im Nutzer-Netzwerk.

Die Autoren wenden ihre Analysemethode auch auf den unter [11] beschriebenen Diebstahl an und können die komplizierten Verschleierungstransaktionen des Angreifers nachvollziehen und übersichtlich darstellen (siehe Abb. 2).



**Abbildung 2.** Visualisierung des Diebstahls, <http://anonymity-in-bitcoin.blogspot.com/2011/07/bitcoin-is-not-anonymous.html>

In ihrer Arbeit nutzen die Autoren nur eine passive Analyse und merken an, dass mit aktivem Eingreifen in das Netzwerk noch deutlich mehr und detailliertere Informationen gewonnen werden können. Denkbar wäre etwa eine Verbindung der aus der Netzwerkanalyse ermittelten Daten mit solchen Informationen, wie sie unter 5.2 dem Händler zur Verfügung stehen. Das Bitcoin-Netzwerk könnte so Eigenschaften eines sozialen Netzwerkes bekommen, welches man wiederum mit dafür geeigneten Methoden analysieren und verfeinern kann.

## 6 Fazit

Bitcoin ist der aktuellste Versuch, ein zu Bargeld analoges Bezahlsystem im Internet zu etablieren. Es setzt dabei auf eine dezentrale Struktur ohne vertrauenswürdige Drittparteien. Über die Korrektheit einer Transaktion entscheidet, wer am meisten Rechenkapazität investiert hat. Dabei wird davon ausgegangen, dass immer eine Mehrzahl an ehrlichen Teilnehmern im Netz agiert. Die für die Signierung und Validierung der Transaktionen und das Erzeugen neuer Blöcke verwendete Kryptographie ist heute als sicher anzusehen. Ein Angreifer kann aber außerhalb des Systems ansetzen. Gelingt es ihm, private Schlüssel mit deren Bitcoins zu stehlen, ist der Schaden für den Betroffenen nicht wieder rückgängig zu machen. Gleiches gilt für den Verlust der Geldbörse. Ob die Sicherheitsmaßnahmen genügen, liegt also zu einem großen Teil am Verhalten des Nutzers. Durch die Struktur von Bitcoin lassen sich einmal gemachte Transaktionen nicht rückgängig machen. Dieses Risiko muss jedem Nutzer bewusst sein.

Auch die Bitcoin oft nachgesagte Anonymität hängt vor allem davon ab, welche Daten die Nutzer mit ihren Bitcoinadressen verbinden. Für sich gesehen erreicht das System eine sehr hohe Anonymität. Durch die Verknüpfung mit Daten die beim Kauf von Waren und Dienstleistungen anfallen oder die an einer Stelle öffentlich gemacht wurden kann diese Anonymität schrittweise immer weiter reduziert werden. Die Deanonymisierung eines einzelnen Nutzers kann durch die Verkettung der Transaktionen auch zur Deanonymisierung weiterer Nutzer führen. Auch hier gilt also, dass den Nutzern bewusst sein muss, dass sie selbst für ihre Anonymität die Verantwortung tragen.

## Literatur

1. Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System. (2008) <http://www.bitcoin.org/bitcoin.pdf>
2. Wei Dai: b-money (1998) <http://www.weidai.com/bmoney.txt>
3. David Chaum, A. Fiat, M. Naor: Untraceable electronic cash. In Proceedings on Advances in Cryptology. (1990)
4. Birgit Pfizmann, Michael Waidner, Andreas Pfizmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. (1990)
5. National Institute of Standards and Technology (NIST): Digital Signature Standard (DSS). [http://csrc.nist.gov/publications/fips/fips186-3/fips\\_186-3.pdf](http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf)
6. National Institute of Standards and Technology (NIST): Secure Hash Standard. <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>
7. Mike Hearn (Bitcoin-Entwickler): Aus einem Forumseintrag <https://bitcointalk.org/index.php?topic=10697.0> <https://bitcointalk.org/?topic=2699.0>
8. Adam Back: Hashcash - a denial of service counter-measure. (2002) <http://www.hashcash.org/papers/hashcash.pdf>
9. Bitcoin-Wiki: <https://en.bitcoin.it/wiki/Confirmation>

10. Garrett Burgwardt: <http://thebitcoinsun.com/post/2011/06/07/The-Bitcoin-Stress-Test>
11. Forumsbericht über einen behaupteten Bitcoin-Diebstahl: <https://bitcointalk.org/index.php?topic=16457.0>
12. Oracle Berkley DB <http://www.oracle.com/us/products/database/berkeley-db/index.html>
13. Thomas Fischermann (Zeit.de): Anarcho-Geld (30.06.2011) <http://www.zeit.de/2011/27/Internet-Bitcoins>
14. Christian Stöcker (Spiegel.de): Geld aus der Steckdose (31.05.2011) <http://www.spiegel.de/netzwelt/netzpolitik/0,1518,765382,00.html>
15. Fergal Reid, Martin Harrigan: An Analysis of Anonymity in the Bitcoin System (2011) <http://arxiv.org/abs/1107.4524>