# Towards a More Anonymous Bitcoin

Thea Heim
Betreuer: Heiko Niedermayer
Seminar Future Internet SS2016
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: heimt@in.tum.de

## KURZFASSUNG

Ein Bitcoin Konto funktioniert zwar ohne Angabe persönlicher Daten wie Name, Adresse oder Telefonnummer kann trotzdem aber nicht als anonym bezeichnet werden. Alleine die Blockchain, die alle Transaktionen vom Tag eins bis heute speichert, und von jeder beliebigen Person eingesehen werden kann, bietet eine Menge Möglichkeiten für einen erfolgreichen Deanonymisierungs-Angriff. Darüber hinaus kann über das Peer-to-peer Netzwerk, welches keiner zentralen Kontrolle unterliegt, mit vergleichsweise geringem Aufwand auf die Identitäten der Nutzer geschlossen werden. Eine Lösung für mehr Anonymität im Bitcoin System ist der CoinJoin Mechanismus. Hier schließen sich für eine Transaktion mehrere Teilnehmer des Netzwerkes zusammen und erschweren somit die Möglichkeit durch die Analyse der in der Blockchain festgehaltenen Transaktionen (Clustering) auf Identitäten zu schließen erheblich. JoinMarket ist eine Implementierung für diesen Mechanismus, die zudem noch eine Lösung für das Grundproblem der CoinJoin Idee - nämlich, dass sich die Gruppe der Teilnehmer, die für eine gemeinsame Transaktion in Frage kommt, auch erst einmal finden muss - liefert. Dennoch kann auch dieses System in der derzeitigen Implementierung noch nicht vollkommen die Anonymität seiner Nutzer schützen, weil es immer noch Angriffsmöglichkeiten wie beispielsweise die Sybil-Attacke bietet.

## Schlüsselworte

Bitcoin, Blockchain, CoinJoin, JoinMarket

## 1. EINLEITUNG

In der heutigen Zeit der Digitalisierung verliert Bargeld als Zahlungsmethode zunehmend an Bedeutung. Elektronische Bezahlmethoden wie z.B. PayPal, Geldkarte, Kreditkarte oder Online-Banking werden immer häufiger eingesetzt und nehmen bereits einen großen Anteil im Handel ein [12].

Neben den genannten Online-Bezahlsystemen erfreuen sich auch digitale bzw. virtuelle Währungen immer größerer Beliebtheit. Der Unterschied zu den herkömmlichen elektronischen Währungen besteht darin, dass nicht die Ursprungswährung (z.B. Euro) erhalten bleibt, sondern in eine künstliche Währung (z.B. Bitcoin) gewechselt wird [17]. Die bekannteste, weltweit verfügbare digitale Währung ist Bitcoin. Sie hat sich seit seiner Einführung (2009) durch den bis heute unbekannten Erfinder Satoshi Nakamoto zunehmend verbreitet [19]. Im Jahr 2013 ist die Währung Bitcoin auch durch die Bundesregierung Deutschland als „privates Geld“ anerkannt worden [15]. Sorge und Krohn-Grimberge [20] beziffern die Anzahl an Bitcoin-Nutzern im Jahr 2013 auf 3,4 Millionen und die Anzahl an Bitcoin-Konten auf ca. 12 Millionen (ein Nutzer kann beliebig viele Konten eröffnen).

Während die Währung in Teilen der USA bereits im Arbeitsalltag angekommen ist (Angestellte im Bundestaat Kentucky können sich bereits ihr Gehalt in Bitcoin ausbezahlen lassen [4]), ist die Anzahl von Internet-Plattformen, auf denen mit Bitcoin bezahlt werden kann, noch stark eingeschränkt. Die Währung wird vor allem auf kleineren Internet-Marktplätzen genutzt und teilweise durch größere Organisationen wie z.B. Wikileaks oder Wordpress akzeptiert. Die Verwendung bei gewöhnlichen Zahlvorgängen wie beispielsweise in Supermärkten ist momentan noch nicht absehbar [12].

Der Anreiz mit digitalen Währungen wie Bitcoin zu bezahlen besteht nach Peyrl ([17]) für den Nutzer v.a. darin, dass für die Verwendung nichts weiter als ein Rechner mit Internetzugang benötigt wird, auf dem die entsprechende Bitcoin-Software installiert ist. Die Zahlungsvorgänge werden abhängig von der Größe der Transaktion innerhalb kürzester Zeit abgeschlossen und es fallen keine bzw. sehr niedrige Transaktionsgebühren an. Zudem genießt der Nutzer eine gewisse Unabhängigkeit, da virtuelle Geldsysteme keiner staatlichen Kontrolle unterliegen. Die Tatsache, dass Bitcoin ohne Angabe personenbezogener Daten verwendet werden kann, macht Bitcoin besonders interessant für Personen, die bei ihren Transaktionen eine gewisse Anonymität wahren möchten.

Diese Eigenschaft der Unabhängigkeit bzw. Anonymität wird nach einer kurzen allgemeinen Einführung in das Bitcoin Konzept (Teil 2) in dieser Arbeit näher betrachtet. Dabei wird die in der Literatur häufig diskutierte Frage aufgeworfen, wie anonym Bitcoin wirklich ist (Teil drei). Hier wird v.a. die Funktion der Blockchain, die alle getätigten Transaktionen speichert, kritisch betrachtet. Zudem werden die Schwächen des dezentralen Peer-to-Peer Netzwerkes, auf dem Bitcoin basiert, dargestellt und ein Überblick über erfolgreiche Hackerangriffe in der Vergangenheit gegeben. Im vierten Teil dieses Artikels wird die Bitcoin-Platform JoinMarket vorgestellt, die ein Ansatz für Transaktionen mit mehr Anonymität ist. Abschließend wird ein kurzes Fazit über das Bitcoin-System in Bezug auf dessen Anonymität gezogen.

## 2. EINFÜHRUNG IN BITCOIN

In diesem Kapitel wird eine Einführung in die Funktionsweise von Bitcoin gegeben. Dazu wird im ersten Teil zunächst erläu-


doi: 10.2313/NET-2017-05-1_01

tert, wie das System der kryptographischen Hashfunktionen in der Bitcoin Software eingesetzt wird. Im zweiten Teil wird darauf eingegangen, welche Möglichkeiten ein Nutzer hat Bitcoins zu erwerben und welches Angebot gegenwärtig für den Handel mit Bitcoins besteht.

## 2.1 Funktionsweise

Wie in der Einleitung bereits beschrieben, ist die einzige Voraussetzung für die Verwendung von Bitcoin ein Rechner mit Verbindung zum Internet, auf dem die Bitcoin-Software installiert ist. Jeder, der mit seinem Rechner die Bitcoin-Software nutzt, ist automatisch Teil des Bitcoin-Netzwerkes. Das Netzwerk realisiert Überweisungen zwischen den Konten der Nutzer, wobei jeder Nutzer ein oder mehrere Konten besitzen kann. Jedes Konto wird über eine Bitcoin-Adresse identifiziert und jeder Bitcoin-Adresse ist ein bestimmtes Bitcoin-Guthaben zugeordnet [20].

Das Bitcoin-Netzwerk ist ein Peer-to-Peer-Netzwerk (siehe Abbildung 1), was bedeutet, dass es - anders als im herkömmlichen Zahlungsverkehr über Banken - keine zentrale Instanz oder Server gibt, worüber die Kommunikation unter den Teilnehmern abgewickelt wird. Demnach sind alle Teilnehmer gleichberechtigt miteinander verbunden und bezüglich neuer Informationen zu jedem Zeitpunkt auf dem gleichen Wissensstand [18].

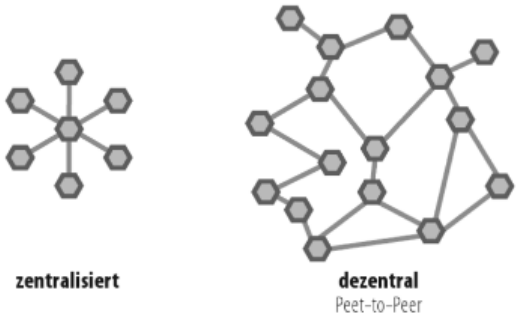


**Abbildung 1: Vergleich Peer-to-Peer Netzwerk (dezentral) mit zentralem Netzwerk [18]**

Gerade aufgrund des Fehlens einer vertrauenswürdigen Instanz muss man sich die Frage stellen, wie die Integrität der Bitcoins erreicht werden kann. Dazu verwendet das System sogenannte (kryptographische) Hashfunktionen, d.h. jede Bitcoin-Adresse setzt sich aus einem öffentlichen Schlüssel (jedem Nutzer bekannt) und einem mathematisch korrespondierenden privaten Schlüssel (nur dem Besitzer bekannt) zusammen. Kann ein Nutzer nachweisen, dass er den zu einer öffentlichen Adresse zugehörigen privaten Schlüssel kennt, darf er über den entsprechenden Bitcoin verfügen [18].

Um Betrug zu verhindern (z.B. mehrfaches Überweisen eines Beitrages von einem Konto) werden in Bitcoin alle durchgeführten Transaktionen in der sogenannten „Blockchain“ veröffentlicht. Jede neue Transaktion gilt zunächst als unbestätigt und wird erst nach Überprüfung durch einen Bitcion Teilnehmer, dem sogenannten „Miner“, in die Blockchain eingetragen. Als Miner kann jeder Teilnehmer des Netzwerkes fungieren. Sein Ziel ist es einen sogenannten „One-Way-Hash“zu lösen. Dies schafft ein Nutzer nur mit extrem großer Rechenleistung, wobei sein Ergebnis sehr leicht rückwärts gerechnet und somit überprüft werden kann [20]. Nach Becker et al. [2] sichert also die ständige Erbringung hoher Rechenleistung die Vertrauenswürdigkeit der Bitcoins.

## 2.2 Erwerb & Handel

Eine Möglichkeit zum Erwerb von Bitcoins ist das im vorherigen Abschnitt beschriebene freiwillige Bitcoin-Mining. Für einen erfolgreich erbrachten Arbeitsbeweis werden einem Miner die mit den Transaktionen verbundenen Transaktionsgebühren und eine Belohnung für die Erbringung der Rechenleistung gutgeschrieben [19]. Nach Vogel [21] nehmen die Miner (also Teilnehmer, die durch Mining Bitcoins erwerben) nur einen geringen Teil des Bitcoin-Netzwerkes ein, da hierfür ein hohes technisches Verständnis sowie ein stetig steigender Rechenaufwand benötigt wird. Eine weitere Variante des Bitcoin-Mining ist das Cloud-Mining. Hierbei erwerben die Miner ihre Bitcoins „durch das Anmieten von Rechenleistung [21]“.

Neben dem Mining existieren noch sogenannte Faucets und Give-Away-Applikationen (z.B. `http://moonbit.co.in/`). Diese verteilen Gratis-Bitcoins für Leistungen wie z.B. das Anklicken von Werbeanzeigen. Zudem können geringe Mengen an Bitcoins über Bitcoin-Onlinespiele (z.B. `https://freebitco.in`) erworben werden [21].

Am häufigsten werden Bitcoins aber über Tauschplattformen (z.B. `coinbase.com`) erworben. Hier erhalten die Nutzer Bitcoins im Tausch gegen eine konventionelle Währung wie Euro oder Dollar [21].

Die Bitcoins der Teilnehmer werden mit Hilfe der Bitcoin-Software in sogenannten „Wallets“ gespeichert. Wallets sind digitale Brieftaschen, die die Schlüsselpaare eines oder mehrerer Nutzer aufbewahren und wesentliche Funktionen wie die Durchführung von Überweisungen, das Erzeugen neuer Schlüsselpaare sowie die Verwaltung von Adressen gewährleisten [19].

Gegenwärtig steigt die Anzahl von Anbietern, die Bitcoin als Währung anerkennen. Der Großteil des Angebots ist sehr technisch orientiert, wobei „Internet- und mobile Dienstleistungen wie VPN, (Web-)Hosting und Programmierung [10]“ überwiegen. Laut Bitcoin Wiki [6] reicht das Angebot außerdem von materiellen Gütern verschiedenster Art (Musik, Bücher, Kleidung, Lebensmittel, etc.) über den Reise- bzw. Tourismusbereich (Reiseportale, Hotels, Flüge, etc.) bis hin zu ersten Restaurants, die eine Bezahlung in Bitcoin akzeptieren.

# 3. WIE ANONYM IST BITCOIN?

Für eine Transaktion mit den gängigen Bezahlmethoden (Kreditkarte, Online-Banking, etc.) ist es erforderlich seine Kontodaten entweder direkt an die involvierte Person oder an einen unabhängigen Zwischenakteur (z.B. Paypal) weiterzugeben. Im Gegensatz dazu ermöglicht Bitcoin die Durchführung von Transaktionen ohne die Angabe von persönlichen Daten [21]. Aus diesem Grund wird dem Bitcoin-System gelegentlich Anonymität unterstellt.

Im Zuge einer Internet Infrastruktur, in der es möglich ist IP


doi: 10.2313/NET-2017-05-1_01

Adressen nachzuverfolgen, und der bereits angesprochenen Blockchain, die alle jemals durchgeführten Transaktionen speichert, muss man sich die Frage stellen, inwieweit man beim Bitcoin-System überhaupt von Anonymität sprechen kann. Dies soll nachfolgend diskutiert werden.

## 3.1 Blockchain

Vogel [21] bezeichnet die Blockchain als „Buchhaltungsdatenbank [...], die alle Bitcoin-Transaktionen seit 2009 speichert." Es handelt sich dabei um eine Kette aus Blöcken, in der jeder Block verschlüsselte Daten zu den durchgeführten Transaktionen enthält (siehe Abbildung 2). Ein neuer Block wird erst an den vorherigen Block angehängt wenn er den Verifizierungsvorgang durch die Miner bestanden hat (siehe 2.1). Tatsächlich wird ca. alle 10 Minuten ein neuer Block gebildet, wobei die Blockgröße derzeit auf 1 MB limitiert ist [5].

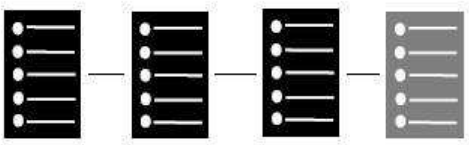

**Abbildung 2: Blockchain [20]**

Die Blockchain kann also von jedem Nutzer eingesehen werden und enthält Informationen über jede Transaktion, die eine Adresse jemals an eine andere Adresse getätigt hat. Die Anonymität ist dadurch aber auf den ersten Blick nicht gefährdet, weil eine Adresse nur aus einem zufälligen Zahlenwert besteht und jeder Teilnehmer beliebig viele Adressen besitzen kann [9].

Trotzdem birgt dieses System in Bezug auf die Anonymität auch Gefahren für die Nutzer. Ein Risiko besteht nach Hobson [9] darin, dass ein Nutzer seine Bitcoin-Adresse zusammen mit seiner Identität entweder versehentlich oder sogar absichtlich veröffentlicht (z.B. um eine Spende zu erhalten). Jede Transaktion, die von oder an diesen Nutzer getätigt wird, wäre dann für alle Teilnehmer einsehbar. Spendet dieser Nutzer beispielsweise an eine umstrittene Gruppe oder Person, deren Bitcoin Adresse ebenfalls irgendwann veröffentlicht wurde, kann jeder Teilnehmer eine Verbindung zwischen den beiden Bitcoin-Adressen bzw. Identitäten herstellen. Zudem ist es relativ wahrscheinlich, dass ein Nutzer Bitcoins an einen anderen, ihm persönlich bekannten Nutzer, transferiert. Kennt man also die Identität der einen Bitcoin-Adresse besteht für die andere Bitcoin-Adresse automatisch erhöhte Gefahr ebenfalls erkannt zu werden.

Herrera-Joancomarti [8] beschreibt in seinem Artikel „Research and Challenges on Bitcoin Anonymity" die Methode des Clustering, mit deren Hilfe man bei Analyse der Blockchain von anonymen Bitcoin-Adressen auf Identitäten schließen kann. Der Grundgedanke dahinter ist, dass eine Transaktion aus mehreren sogenannten „Input"-Adressen besteht. Input-Adressen sind Outputs vorheriger Transaktionen und müssen immer als Ganzes verschickt werden (d.h. es können keine Teilbeträge von einem Konto genommen werden und der gesendete Gesamtbetrag muss größer oder gleich dem Output-Betrag sein). Werden nun beispielsweise 1 BTC von der einen und 5 BTC von der anderen Adresse an eine weitere Adresse transferiert, kann man davon ausgehen, dass beide Adressen denselben Besitzer haben. Verwendet dieser Nutzer nun für eine andere Transaktion nochmals eine der beiden Adresse plus eine weitere Adresse, so kann man diesem Nutzer schon drei Adressen zuordnen. Auf diese Weise können Cluster über Adressen im Bitcoin-Netzwerk gebildet und einem Nutzer zugeordnet werden. Bezieht man dann noch Informationen mit ein, die man - wie im vorheringen Abschnitt beschrieben - extern gesammelt hat (z.B. veröffentlichte Bitcoin-Adressen auf Twitter) so kann sogar auf die Identität, die sich hinter diesen Clustern verbirgt, geschlossen werden.

Für Vogel [21] ist ein weiteres Risiko „die Stelle, an der ein Bitcoin-Verwender seine BTC in konventionelle Währungen umtauscht". Der Teilnehmer muss an diesem Punkt seine „persönlichen Daten wie Name und Kontonummer - sofern er nicht gegen Bargeld tauscht - an eine Handelsplattform weitergeben." Sobald er das tut ist ein Zusammenhang zwischen Bitcoin-Adresse und Identität hergestellt.

## 3.2 P2P-Netzwerk

Wie in 2.1 beschrieben ist die zugrundeliegende Technik für Transaktionen im Bitcoin-System ein Peer-to-Peer-Netzwerk. Zum einen ermöglicht dieses dezentrale Netzwerk einen Zahlungsverkehr fernab von staatlicher Kontrolle, zum anderen birgt es Risiken für die Nutzer bzgl. Anonymität. Im Jahr 2014 veröffentlichten drei Forscher der Universität Luxemburg [3] in ihrem Paper „Deanonymisation of clients in Bitcoin P2P network" eine Vorgehensweise wie man die IP-Adressen der Nutzer im Bitcoin-Netzwerk aufdecken kann. Die Forscher benötigten dazu die folgenden vier Schritte.

1. Mit Hilfe der Methode „GETADDR" wird nach allen bekannten peers im Netzwerk gesucht. Diese Liste muss ständig aktualisiert werden.
2. Im zweiten Schritt wird eine Liste von denjenigen Bitcoin Clients, deren Identität man aufdecken möchte, erstellt. Dazu verwendet der Angreifer entweder IP-Adressen-Bereiche von bekannten Internet Providern oder sammelt bereits im Bitcoin Netwzerk publizierte Adressen.
3. Anschließend wird damit begonnen die Clients, die sich mit dem Netzwerk verbinden, zu ihren Entry Nodes zuzuordnen. Dazu verwendet der Angreifer die in 4 beschriebene Methode. Laut den Forschern reichen schon drei Entry Nodes, um einen Nutzer eindeutig zu identifizieren. Bereits bei zwei Entry Nodes wird schon ein großer Prozentsatz an Nutzern identifiziert.
4. Der vierte Schritt läuft parallel zu den Schritten 1 bis 3. Hier versucht der Angreifer die Transaktionen, die im Netzwerk erscheinen, den Entry Nodes und anschließend den Nutzern zuzuordnen. Um das zu schaffen, wartet der Angreifer bei allen eingerichteten Verbindungen auf „INVENTORY" Nachrichten und sammelt für alle Transaktionen T die ersten q Adressen von Bitcoin Servern, die die INVENTORY Nachricht weitergeleitet haben. Nachfolgend vergleicht er die gesammelten Adressen mit der in 1 erstellten Liste und findet


doi: 10.2313/NET-2017-05-1_01

mögliche Paare aus Entry Nodes und Clients. Bei ihrem Versuch erreichten die Forscher eine Quote von 11%, mit der sie IP-Adressen erfolgreich den Nutzern zuordnen konnten.

Zusammenfassend bleibt festzuhalten, dass die Forscher mit vergleichsweise geringem Aufwand (ca. 1500 Dollar pro Monat) eine Lösung für die Deanonymisierung von IP-Adressen gefunden haben. Auch wenn die Erfolgsquote mit 11% noch relativ gering ausfällt, kann bei Bitcoin nicht von vollständiger Anonymität gesprochen werden. Gerade für Kriminelle könnte diese Studie ein Anreiz sein, um die Identität von Nutzern herauszufinden.

## 3.3 Erfolgreiche Hackerangriffe

Wenngleich der Verzicht von Kontrolle beim dezentralen Bitcoin System eine Neuerung bedeutet und für viele Nutzer reizvoll ist, ermöglicht diese Tatsache auch ein unkontrollierbares Ausmaß an kriminellen Aktivitäten. In der Vergangenheit gab es trotz großer Sicherheitsvorkehrungen immer wieder erfolgreiche Hackerangriffe auf Bitcoin Wallets. Erst im August diesen Jahres sollen Hacker Bitcoins im Wert von 65 Millionen Dollar von der Plattform Bitfinex gestohlen haben [16]. Der bislang größte Hackerangriff betraf die japanische Bitcoin-Börse Mt.Gox, einst die größte Bitcoin-Börse der Welt. Bei diesem Angriff wurde fast eine halbe Milliarde Dollar gestohlen, was schließlich dazu führte, dass die Börse Konkurs anmelden musste [13]. Solche Hacker verschaffen sich Zugriff auf Bitcoin Wallets privater Nutzer und überschreiben die Guthaben an eine andere Adresse. Ist dies passiert, besteht für den Nutzer keine Möglichkeit mehr sich die Bitcoins wiederzubeschaffen. Besonders betroffen sind von diesen Angriffen tatsächlich die privaten Nutzer, weil sie meist keine besonderen Maßnahmen ergreifen, um ihre Anonymität zu bewahren. Personen, die Bitcoins für ihre kriminellen Machenschaften verwenden sind in dieser Hinsicht meist wesentlich versierter und treffen entsprechende Vorkehrungen, um ihre Identität zu schützen [7].

## 3.4 CoinJoin für mehr Anonymität

Eine Lösung für mehr Anonymität in Bitcoin Transaktionen bietet der sogenannte „CoinJoin Mechanismus“. Die Grundidee dahinter ist, dass sich mehrere voneinander unabhängige Sender und Empfänger von Bitcoins zusammenschließen und - anstelle von mehreren einzelnen Transaktionen - eine einzige Transaktion gemeinsam tätigen (siehe Abbildung 3)[14]. Dabei gibt es keine Begrenzung in der Anzahl der Nutzer, die sich für eine Transaktion zusammenschließen [1].

Der Vorteil darin ist, dass die Inputs und zugehörigen privaten Schlüssel einer Transaktion nicht nur einer einzelnen Person oder mehreren zusammengehörigen Nutzern bekannt sind und somit die in 3.1 beschriebene Deanonymisierungs-Methode des Clustering erheblich erschwert wird [11]. Dabei gilt, je höher die Anzahl der Teilnehmer an einer CoinJoin-Transaktion, desto schwieriger wird es für den Angreifer irgendetwas aus der Blockchain herauszulesen. Limitiert wird die CoinJoin Methode vor allem dadurch, dass für die Teilnahme an einer Transaktion andere Nutzer gefunden werden müssen, die zur selben Zeit eine Zahlung tätigen wollen. Dies ist nicht immer einfach und führt dazu, dass CoinJoin nur selten genutzt wird [1].

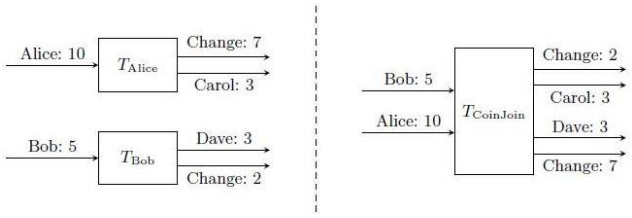


**Abbildung 3: CoinJoin-Mechanismus: Zwei oder mehrere einzelne Transaktionen (links) werden in einer Transaktion kombiniert (rechts)[14]**

Im nachfolgenden Kapitel wird die Plattform JoinMarket beschrieben, die eine Lösung für das grundsätzliche Problem von CoinJoin Transaktionen bietet.

# 4. JOINMARKET

JoinMarket ist eine Plattform für den Handel mit Bitcoins, welche auf dem Konzept des CoinJoin Mechanismus aufbaut und mit dem Ziel entwickelt wurde den Nutzern bei ihren Transaktionen mehr Anonymität zu bieten. Laut einer Analyse von Möser und Böhme [14], betrug der Umsatz dieser Plattform in einem betrachteten Zeitraum von acht Monaten bis zu acht Millionen USD.

In diesem Kapitel werden sowohl die Funktionsweise der Plattform näher erläutert, als auch die Ergebnisse einer Studie, in der die Plattform über einen 8-monatigen Zeitraum analysiert wurde, zusammengefasst.

## 4.1 Funktionsweise JoinMarket

Die Plattform JoinMarket ermöglicht ihren Nutzern die Umsetzung von CoinJoin Transaktionen. Im Gegensatz zur „normalen“ CoinJoin Transaktion wurde hier aber ein Konzept entwickelt, das dem Nutzer jederzeit entsprechende Transaktionspartner für eine gemeinsame CoinJoin Transaktion zur Verfügung stellt. Dazu werden die Nutzer in sogenannte „Makers“ und „Takers“ eingeteilt [14].

**Makers** stellen ihre Bitcoins beliebigen Takers zur Durchführung von CoinJoin Transaktionen zur Verfügung. Zum einen erhöhen sie dadurch die Anonymität ihrer eigenen Transaktion (haben aber keine Eile ihre Transaktion durchzuführen) und zum anderen erhalten sie eine kleine Gebühr für die Bereitstellung ihrer Bitcoins.

**Takers** haben keine Zeit auf einen Transaktionspartner zu warten und verwenden deshalb die Bitcoins der Makers für ihre CoinJoin Zahlung. Im Gegenzug bezahlen sie die sogenannte „maker fee“ an die Makers [22].

Ein Nutzer, der möglichst schnell eine Transaktion durchführen möchte, nimmt also die Rolle eines Takers ein und wählt einen oder mehrere Maker aus, um mit ihm oder ihnen eine gemeinsame Transaktion durchzuführen. Erlaubt sind auf JoinMarket 2 bis maximal 20 Transaktionspartner in einer Transaktion. Die maker fee, die er als Gegenleistung bezahlen muss, ist dabei ein Prozentwert, der sich an der Höhe der Zahlung orientiert. Um eine Transaktion endgültig zu tätigen,


doi: 10.2313/NET-2017-05-1_01

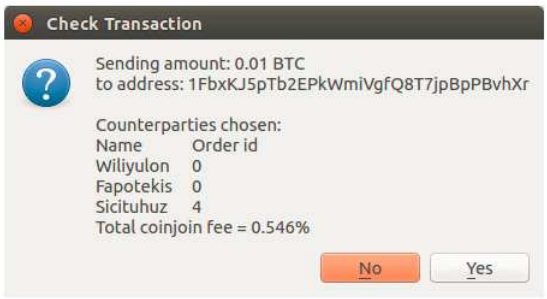


**Abbildung 4: Beispiel: Eine Transaktion mit 3 Transaktionspartnern kostet 0,534% maker fee [22]**

muss jeder Nutzer der entsprechenden maker fee zustimmen (siehe Abbildung 4). Andernfalls kann die Transaktion nicht durchgeführt werden [22].

In der derzeitigen Implementierung von JoinMarket kommunizieren Takers und Makers über einen zentralisierten Internet Relay Chat (IRC) Kanal. Ein Maker tritt dem Kanal bei und eröffnet sein Angebot für eine Bitcoin Transaktion. Die Angebote werden bei JoinMarket nicht auf einem zentralen Server gespeichert, sondern in einem öffentlichen Auftragsbuch, das jeder Teilnehmer lokal verwalten kann. Wenn ein Maker ein neues Angebot erstellt, ein bereits vorhandenes Angebot verändert, oder die Plattform verlässt wird die lokale Datenbank aktualisiert. Ein Maker muss seine Verbindung zum IRC Server halten, um an CoinJoin Transaktionen teilnehmen zu können [14].

JoinMarket ordnet Makers und Takers nicht automatisch zueinander. Ein Taker, der eine Transaktion durchführen möchte, hat bei der Auswahl seiner Transaktionspartner folgende drei Möglichkeiten [14]:

1. Zufällige Auswahl von einer Liste, die Angebot und zugehörige Gebühr entsprechend gewichtet
2. Auswahl nach Gebühr (niedrigste Gebühr zuerst)
3. Manuelle Auswahl

## 4.2 Analyse JoinMarket

Möser und Böhme [14] analysierten die Plattform JoinMarket über einen acht-monatigen Zeitraum von Anfang Juni 2015 bis Ende Januar 2016. Die Ergebnisse sind in ihrer Publikation „Join Me on a Market for More Anonymity“ beschrieben und werden nachfolgend kurz zusammengefasst.

Abbildung 5 zeigt die Marktveränderungen von JoinMarket im betrachteten Zeitraum. Die Gesamtzahl der verfügbaren Bitcoins entwickelte sich von anfangs wenigen hundert bis zu einem Maximum von über 2000 BTC Ende November 2015. Obwohl die Anzahl zum Ende des Betrachtungszeitraumes wieder bis auf 1500 BTC sank, wurden die Transaktionsangebote innerhalb der acht Monate nahezu konstant mehr. Da aber die Anzahl der Makers über den gesamten Zeitraum nahezu gleich blieb, schlossen die Forscher darauf, dass die Makers mehr und mehr dazu übergingen nicht mehr nur eine sondern gleich mehrere Installationen des Programms zu verwenden. Ein Fakt, der die nachfolgende Graphik verfälschen könnte, ist, dass die Plattform nicht gewährleisten kann, dass jedes Transaktionsangebot wahrheitsgemäß ist. Makers könnten beispielsweise mehr Bitcoins anbieten als sie eigentlich haben, oder besonders niedrige Gebühren verlangen und die Transaktion dann im letzten Schritt noch abbrechen.

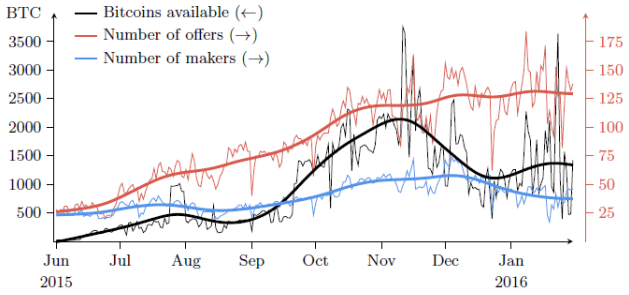


**Abbildung 5: Marktveränderungen der Plattform JoinMarket im Zeitraum von 8 Monaten [14]**

Die Anzahl der abgeschlossenen JoinMarket Transaktionen während der betrachteten acht Monate belief sich laut der Studie auf ca. 10.000, d.h. ungefähr 41 Transaktionen pro Tag. Die höchste Transaktionsrate wurde dabei im Oktober und November gemessen mit ca. 150 Transaktionen pro Tag.

Die wohl größte Gefährdung für die Nutzer besteht darin, dass die Plattform besonders anfällig für Sybil-Angriffe ist. Um einen Taker zu deanonymisieren müsste der Angreifer lediglich eine große Anzahl an Makers verkörpern und sich mit diesen in einer CoinJoin-Transaktion als unabhängige, einander unbekannte Individuen ausgeben. Ziel wäre es dann der einzige Partner des Takers in der entsprechenden Transaktion zu sein und - weil der Angreifer genau weiß welche Inputs und Outputs zu ihm selbst gehören - sofort aufzudecken wohin der Taker sein Geld überweisen möchte. Damit wäre der CoinJoin Mechanismus ausgehebelt und eine Transaktion genauso transparent wie im „normalen“ Bitcoin System.

Wie hoch die Wahrscheinlichkeit für eine erfolgreiche Sybil-Attacke aus Sicht des Angreifers ist, hängt stark von der Anzahl der Teilnehmer an einer CoinJoin-Transaktion ab. Je größer die Personenzahl bei einer Transaktion, desto geringerer ist die Erfolgsquote. Vor allem weil die voreingestellte Anzahl an Makers, die ein Taker für eine Transaktion benötigt auf JoinMarket bei 2 steht, schließen sich die meisten Takers nur mit zwei Makers für eine Transaktion zusammen. Auch nachfolgende Statistik (siehe Abbildung 6) belegt, dass sich nur sehr wenige Takers für mehr als zwei Makers entscheiden, wodurch ein möglicher Versuch einer Deanyonymisierung für einen Angreifer noch erleichtert wird.

Zusammenfassend bleibt zu sagen, dass JoinMarket zwar eine Lösung für das grundsätzliche Problem von CoinJoin Transaktionen - nämlich das Finden eines Transaktionspartners - liefert, die Implementierung aber im jetzigen Zeitpunkt noch nicht optimal ist. Zum einen schützt die Plattform die Nutzer nicht ausreichend vor Angriffen (v.a. Sybil) und zum anderen baut die Architektur auf einem zentralisierten IRC Server auf, was eigentlich diametral entgegengesetzt dem dezentralen Gedanken von Bitcoin ist.


doi: 10.2313/NET-2017-05-1_01

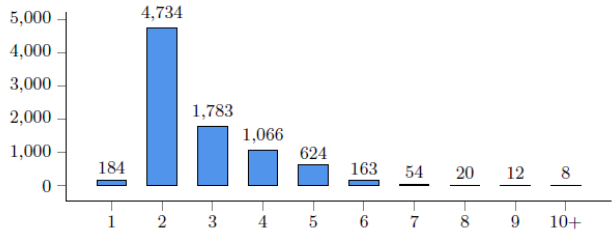


**Abbildung 6: Anzahl der Makers, die von den Takers ausgewählt werden (Default = 2) [14]**

Der Vollständigkeit halber muss an dieser Stelle noch erwähnt werden, dass JoinMarket nicht die einzige Implementierung des CoinJoin Mechanisums ist. Nach Young [22] gibt es folgende fünf weitere Implementierungen: „Mycelium CoinJoin wallet“, „CoinShuffle“, „Dark Wallet“, „Darksend of Dash“, „Shared Coins“.

# 5. ZUSAMMENFASSUNG

Diese Arbeit beschäftigte sich mit der virtuellen Währung Bitcoin und insbesondere der Frage, inwieweit der Nutzer bei der Bezahlung mit Bitcoins anonym bleibt. Um diese Frage zu beantworten war es zunächst wichtig das Konzept des Bitcoin Systems zu erläutern. Die Basis bildet ein dezentrales Peer-to-Peer System, das keiner staatlichen Kontrolle unterliegt. Ein Bitcoin Konto kann ohne Angabe persönlicher Daten eröffnet werden und wird über eine kryptographische Hashfunktion adressiert. Der öffentliche Schlüssel eines solchen Kontos ist allen Teilnehmer bekannt, der private Schlüssel nur dem Administrator. Alle Transaktionen von der Einführung des Bitcoin Systems bis heute werden in der Blockchain gespeichert und können von jeder beliebigen Person eingesehen werden. Werden die öffentlichen Schlüssel mit Informationen von externen Quellen (Facebook-Einträge, Blog-Einträge, IP-Adressen) verknüpft können Angreifer relativ schnell auf die Identität hinter den Konten schließen. In der Vergangenheit gab es bereits mehrere solcher erfolgreichen Hackerangriffe, bei denen Bitcoins im Wert von mehreren Millionen Dollar gestohlen wurden. Die Leidtragenden dieser Angriffe waren meist private Bitcoin Nutzer, die sich nicht mit zusätzlichen Maßnahmen vor solchen Attacken geschützt haben.

Doch welche Möglichkeiten gibt es die Anonymität des Nutzers besser zu bewahren? Dazu wurde in dieser Arbeit die JoinMarket Plattform näher erläutert. Diese basiert auf dem CoinJoin Mechanismus, bei dem - anders als im normalen Bitcoin System - eine Transaktion nicht mehr nur von einer Person zu einer Person abgewickelt wird, sondern sich mehrere Personen für eine Transaktion zusammenschließen. Dieser Mechanismus macht es deutlich schwieriger für einen Angreifer, die Identität einer Person nachzuvollziehen. Dennoch hat auch die CoinJoin Methode eine Schwäche und zwar das „Finden“ der Teilnehmer untereinander, um dann gemeinsam eine Überweisung zu tätigen. Dafür hat die JoinMarket Plattform das Prinzips der Takers und Makers eingeführt, bei dem die Makers Angebote für Bitcoin Transaktionen öffentlich machen und von den Takers gegen Bezahlung ausgewählt werden können, um eine dringende CoinJoin Transaktion zu tätigen. Eine in dieser Arbeit beschriebene Analyse zeigt deutlich, dass die Plattform JoinMarket im letzten Jahr an Attraktivität gewonnen hat, aber auch hier nicht von vollständiger Anonymität gesprochen werden kann. Besonders anfällig scheint die Plattform für Sybil-Angriffe zu sein und in der derzeitigen Implementierung gibt es noch keine Schutzmechanismen gegen diese Attacke. Das Fazit dieser Ausarbeitung ist, dass Bitcoin zwar anonymer als andere elektronische Zahlungsmittel, aber noch weit entfernt von vollständiger Anonymität ist.

# 6. LITERATUR


[1] J. Barcelo. User Privacy in the Public Bitcoin Blockchain. *Journal of Latex Class Files*, 6(1), 2007.

[2] J. Becker, D. Breuker, T. Heide, J. Holler, H. P. Rauer, and R. Böhme. Geld stinkt, Bitcoin auch-Eine Ökobilanz der Bitcoin Block Chain. In *GI-Jahrestagung*, pages 39–50, 2012.

[3] A. Biryukov, D. Khovratovich, and I. Pustogarov. Deanonymisation of clients in Bitcoin P2P network. *ACM Conference on Computer and Communications Security*, 2014.

[4] J. Breithut. Digitales Zahlungsmittel: Bank of America orakelt über große Bitcoin-Zukunft. *Spiegel Online*, Dec. 2013. `http://www.spiegel.de/netzwelt/web/bitcoin-zahlungsmittel-der-zukunft-a-937597.htmll`, zuletzt besucht am 22. August 2016.

[5] B. community. Block size limit controversy. *Bitcoin Wiki*, 2016. `https://en.bitcoin.it/wiki/Block_size_limit_controversy`, zuletzt besucht am 15. November 2016.

[6] B. community. Trade. *Bitcoin Wiki*, 2016. `https://en.bitcoin.it/wiki/Trade`, zuletzt besucht am 28. August 2016.

[7] O. Harman. Bitcoin - Hype oder Währung? Bachelorarbeit, Universität Bern, 2014.

[8] J. Herrera-Joancomartí. *Research and Challenges on Bitcoin Anonymity*, pages 3–16. Springer International Publishing, Cham, 2015.

[9] D. Hobson. What is Bitcoin? *XRDS*, 20(1):40–44, Sept. 2013.

[10] A. Krohn-Grimberghe and C. Sorge. Bitcoin - Anonym Einkaufen im Internet? In *Der gläserne Verbraucher - Wird Datenschutz zum Verbraucherschutz?*, pages 105–114, 2014.

[11] S. Meiklejohn and C. Orlandi. *Privacy-Enhancing Overlays in Bitcoin*, pages 127–141. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[12] S. Merklin, B. Schneider, and M. Schoop. Bitcoin - eine strukturierte Analyse. In *Multikonferenz Wirtschaftsinformatik 2014*, pages 2138–2149, 2014.

[13] T. Mochizuki. So lief die spektakuläre Pleite der Bitcoin Börse ab. *Wall Street Journal*, 2015. `https://www.welt.de/wall-street-journal/article129565422/So-lief-die-spektakulaere-Pleite-der-Bitcoin-Boerse-ab.html`, zuletzt besucht am 27. September 2016.

[14] M. Möser and R. Böhme. Join Me on a Market for Anonymity. *The 15th Annual Workshop on the Economics of Information Security*, 2016. `http://weis2016.econinfosec.org/wp-content/uploads/sites/2/2016/05/WEIS_2016_paper_58.pdf`.

[15] F. Nestler. Deutschland erkennt Bitcoins als privates Geld an. *Frankfurter Allgemeine Zeitung*, Aug. 2013. http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/digitale-waehrung-deutschland-erkennt-bitcoins-als-privates-geld-an-12535059.html, zuletzt besucht am 22. August 2016.

[16] o.A. 65 Millionen Dollar Bitcoins gestohlen. *Handelsblatt*, 2016. http://www.handelsblatt.com/finanzen/anlagestrategie/trends/hackerangriff-65-millionen-dollar-bitcoins-gestohlen/13963284.html, zuletzt besucht am 27. September 2016.

[17] R. Peyrl. Digitale Währungen - Zahlungsmittel der Zukunft? *Zukunftsthema Oberösterreich*, 2015. http://www.ooe-zukunftsakademie.at/Zukunftsthema_digitaleWaehrung_2015.pdfl, zuletzt besucht am 22. August 2016.

[18] J. Platzer. *Bitcoin - kurz & gut*. O'Reilly Verlag, 2014.

[19] C. Sorge and A. Krohn-Grimberghe. Bitcoin: Eine erste Einordnung. *Datenschutz und Datensicherheit - DuD*, 36(7):479–484, 2012.

[20] C. Sorge and A. Krohn-Grimberghe. Bitcoin - das Zahlungsmittel der Zukunft? *Wirtschaftsdienst*, 93(10):720–722, 2013.

[21] M. Vogel. *Relevanz und Risiken von virtuellen Währungen am Beispiel von Bitcoin*. Hochschule Hof, Fachbereich Wirtschaft, 2016.

[22] J. Young. Advances in Anonymity: JoinMarket Releases Version 3 and GUI. *BTCManager.com*, 2016. https://btcmanager.com/news/tech/advances-in-anonymity-joinmarket-releases-version-3-and-gui/, zuletzt besucht am 23. September 2016.



doi: 10.2313/NET-2017-05-1_01