Bitcoin

Michael Lamberty, Norbert Pohlmann

März 2015

1 Was ist Bitcoin?

Um zu verstehen, was Bitcoin ist, müssen wir einen Blick in die Natur des Geldes werfen: Eine zu selten gestellte Frage, mit der hier begonnen werden soll ist: Was ist dieses „Geld“ überhaupt?

Ohne die Entwicklung von Geld über Tauschwaren hin zu modernem Hochgeschwindigkeitshandel aufzuzeichnen, richtet sich der erste Gedanke, der beim Wort „Geld“ fällt, auf das Greifbare: Münzen und Scheine. Fragt man nach dem Wert einer solchen Münze, dann ist die naheliegende Antwort zwar ihr Nennwert, doch steht dieser im Kontrast zum Materialwert, der selbst bei einem 2€-Stück nur wenige Cent beträgt.

Doch wie kommt diese Diskrepanz zu Stande?

Das Vertrauen in den Wert von Geld ist eine gewachsene Größe und lässt sich weder durch kurzfristige Einbrüche, wie die Hyperinflation der Reichsmark, noch durch langfristige Entwertungen erschüttern – Bargeld wird überall akzeptiert. „Cash is King“ und „nur Bares ist Wahres“.

Doch das meiste Geld liegt längst nicht mehr „auf der Hand“, es liegt auf dem Bankkonto, symbolisiert durch Zahlen auf dem Kontoauszug. Das Vertrauen in das Bargeld erstreckt sich auch über diese Zahlen, denn unsere Erfahrung zeigt uns, dass ein Geldautomat die Zahlenkolonnen auf dem Bildschirm auch wieder in Bargeld zurück verwandelt. Auf den ersten Blick handelt es sich um zwei Darstellungsformen ein- und derselben Sache, allerdings steckt der Teufel im Detail:

Ein kurzer Gedanke sei an die Speicherung des elektronischen Geldes verwendet: Nur kindliche Naivität würde glauben machen, dass die Bank für jeden Kunden ein getrenntes Konto führen würde oder dass das Geld in der Bank physikalisch existent sei – in Wirklichkeit befindet sich nur ein Bruchteil des Geldes im Umlauf. Das, was wir als Geld bezeichnen, existiert lediglich in den IT-Systemen der Bank. Die Bank führt Buch, wer wie viel Geld einzahlt oder abbucht; der Kontostand jedes Einzelnen ist die Summe aller Transaktionen, in die sein Konto involviert war.

Anders als Bargeld kann Geld in seiner elektronischen Form nicht einfach transferiert werden: Der Versuch bei einer Bank vorstel-

lig zu werden, um sein Konto auf dem PC zu Hause zu verwalten, würde mit einem Lächeln quittiert, das Vertrauen der Bank in den Kunden ist sehr gering.

Banken als Mittelsmänner

Wenn wir nun also „elektronisches Geld“ an eine andere Person senden wollen, benötigen wir dazu die Bank. Und auch der Empfänger der Überweisung kann das Geld nicht ohne seine Bank in Empfang nehmen. Hinter den Kulissen vergrößert sich der Abstand zur naiven Vorstellung einer Geldübergabe: Die Bank des Senders senkt den Betrag auf dessen Konto, während die Empfängerbank den Betrag erhöht. Erst am Ende des Tages werden die eigentlichen Abrechnungen vollzogen und die Banken begleichen ihre gesammelten gegenseitigen Forderungen. Das Geld im Bankkonto hat keine unabhängige Existenz: Während Bargeld auch für sich existieren kann, braucht das elektronische Guthaben immer eine Bank, die dessen Existenz und Betrag konstatiert. Kurz: Ohne Bank kein Geld!

Anarchie ohne Bank?

Warum beruht unser Geldsystem auf Banken? Dies sei an einem einfachen Beispiel erklärt: Nehmen wir an, ein Nutzer hat 20€ auf seinem Konto und kann dieses – aus Gründen der Einfachheit – auch nicht überziehen. Nun kauft er für diese 20€ ein Buch bei Amazon. Kurz darauf möchte er dieselben 20€ an einen Freund überweisen, dem er noch Geld schuldet. Diese Art von Angriff wird als „double spending“, also doppeltes Ausgeben bezeichnet. In unserem Fall hat nur die Bank den ausreichenden Überblick, beide Transaktionen zu sehen und aufgrund des ungedeckten Kontos die letztere als ungültig zu deklarieren – weder Amazon noch die empfangene Bank wissen von der jeweils anderen Überweisung. Durch die zeitliche Abfolge der Überweisungen kann die Bank feststellen, welche Überweisung die erste war und die zweite entsprechend blockieren.
Zurück zur lokalen Speicherung: Wie wäre eine solche Speicherung zu realisieren? Der triviale Ansatz wäre die Speicherung der Währungseinheiten als Dateien, aber digitale Güter lassen sich beliebig kopieren. Bargeld umgeht diese Probleme, indem zumindest Banknoten mit einer Seriennummer ausgestattet sind, so dass Duplikate erkannt werden können. Doch an dieser Stelle ist wieder Vertrauen in die Bundesdruckerei nötig, denn würde diese einfach wahlfrei Banknoten drucken, wäre deren Wert ebenfalls gefährdet.

Vertrauen als Währung

Wir haben nun festgestellt, dass wir tagtäglich mit einer digitalen Währung konfrontiert werden und haben die Herausforderungen aufgezeigt, die eine solche Währung mit sich bringt. Doch bisher beruhen alle unsere Vorschläge auf einer zentralen Bank, die die Währung verwaltet und Transaktionen überwacht. Es stellt sich also zum Abschluss die Frage: Können wir eine digitale Währung realisieren, welche ohne Bank auskommt?

Bitcoin

Die Antwort auf diese Frage ist – wenig überraschend – ja. Bitcoin ist eine

dezentrale Währung, die die Vorteile eines Bankkontos (Geld weltweit transferieren) mit denen von Bargeld (Währungsaustausch ohne Mittelsmann) kombiniert. Doch wie können die in den vorherigen Abschnitten beschriebenen Probleme gelöst werden? Bitcoin funktioniert ähnlich wie die eingangs beschriebene Bank, die Zahlungs- Ein- und Ausgänge für jeden Kunden notiert und verwaltet. Im Fall von Bitcoin reduziert sich die Bank auf ihre Buchführung: Alle vergangenen Bitcoin-Transaktionen sind in einer dezentralen Datenbank, der **Blockchain** gespeichert. Ein Teilnehmer am Bitcoin-Netzwerk identifiziert sich über seine **Adresse**, die – ähnlich einer Kontonummer – eindeutig ist und benötigt wird, um Überweisungen auszustellen oder zu erhalten. Die Adressen errechnen sich aus individuellen asymmetrischen Schlüsselpaaren, die in der **Wallet** gespeichert werden.

Hier ein vereinfachtes Beispiel: Nutzer A möchte 3 Bitcoin an Nutzer B überweisen. Dazu erstellt er eine **Transaktion**, in welcher er die Menge der zu übertragenden Bitcoin sowie den Empfänger (also die Adresse von B) spezifiziert. Diese Transaktion signiert er mit dem Private Key seiner Bitcoin-Adresse und verbreitet sie im Bitcoin-Netzwerk.

Andere Nutzer im Bitcoin-Netzwerk prüfen nun die Transaktion auf Gültigkeit (Besitzt A die angegebenen Bitcoin? Stimmt die Signatur?) und leiten diese weiter, falls sie korrekt ist. Dieser Vorgang wiederholt sich, bis das ganze Netzwerk von der Transaktion erfahren hat. Anders als bei einer Banküberweisung ist dieser Vorgang pseudonym: Es ist nicht zwingend notwendig, die Identität von A oder B preis zu geben, aber die Überweisung und damit Verknüpfung zwischen den beiden Adressen ist öffentlich bekannt.

Erreicht die Transaktion einen **Miner**, so speichert er diese, um sie später in der **Blockchain** zu persistieren. In der Bank-Analogie sind Miner die Angestellten der Bank: Sie kümmern sich darum, dass die Transaktion dem Empfänger zugänglich wird.

Die Miner versuchen nun – entweder einzeln oder in Gruppen, sogenannten Pools – aus den gesammelten Transaktionen einen neuen **Block** zu schaffen. Dieser beinhaltet alle Transaktionen, die ein Miner erhalten hat und die noch nicht in der Blockchain zu finden sind. Um zu verhindern, dass inflationär Blöcke erzeugt und Transaktionen durchgeführt werden, muss für jeden Block ein Proof-of-Work, also eine rechenaufwändige Aufgabe (Challenge), erbracht werden. Weiterhin beinhaltet jeder Block eine Referenz auf seinen Vorgänger, so dass das Veröffentlichen eines neuen Blocks dazu führt, dass alle anderen Miner ihre bisherige Arbeit abbrechen und an einem neuen Block arbeiten müssen. Sobald ein Block gemint wurde, wird er ebenfalls im Netzwerk verbreitet, so dass jeder Client den Block an seine lokale Kopie der Blockchain anhängen kann.

Sobald sich eine Transaktion in der Blockchain befindet, kann der Empfänger mittels seines Public Key beweisen, dass er seine eigene Adresse berechnen kann. Auf diese Weise kann er seine Transaktion beanspru-

chen und die referenzierten Bitcoin ausgeben.

Der Miner wird für seinen Aufwand aus zwei Quellen belohnt: Primär erhält er eine Mining-Belohnung, aktuell 12,5 Bitcoin, für das Erschaffen eines neuen Blocks, sekundär werden ihm alle Transaktionsgebühren zugeschlagen, die sich im Block befinden.

Verbreitung

Seit dem Minen des ersten Blocks im Januar 2009 breitete sich Bitcoin langsam über den Planeten aus. Heute wird Bitcoin an ca. 10.000 Stellen[1] akzeptiert, dem entgegen stehen über 200.000 aktive Bitcoin-Wallets[2] – dies entspricht etwa der Anzahl der Handynutzer im Jahre 1984. Doch wie kommt es, dass eine disruptive Technologie wie Bitcoin so wenig verbreitet ist, während das Handy kaum aus dem Alltag wegzudenken ist?

Über die Antwort lässt sich nur spekulieren, allerdings lassen sich einige Gründe identifizieren, die für die schwache Verbreitung verantwortlich sein könnten:

- **Schlechte Presse**
  Das Versprechen von Anonymität sowie der Takedown der Internet-Währung *Liberty-Reserve* führten dazu, dass die Early-Adopter von Bitcoin aus dem Bereich der Internet-Kriminalität stammten. Mit dem Takedown des Online-Marktplatz Silkroad wurde erstmals die breite Öffentlichkeit auf das Thema Bitcoin aufmerksam, da dies die einzige dort akzeptierte Währung war. Auf diesem Weg wurde Bitcoin schon sehr früh mit dem Thema Cyberkriminalität verknüpft und genoss einen entsprechend schlechten Ruf in den Medien.

- **Schwankende Wechselkurse**
  Der Wechselkurs von Bitcoin zu bestehenden Währungen unterlag von Anfang an gewissen Schwankungen. Der kometenhafte Aufstieg von praktisch Null auf über 1000 Euro im Jahr 2013 lockte viele neue Nutzer an, doch das Platzen der Blase führte zu einer Verunsicherung, die viele Nutzer bis heute verfolgt. Zwar ergibt sich der Bitcoin-Kurs relativ transparent aus Angebot und Nachfrage an verschiedenen Bitcoin-Börsen, allerdings schwankt diese permanent und schlägt sich so – dank der geringen Handelsmenge – auch auf den Kurs nieder. Diese kleineren Schwankungen werden durch Marktpsychologie verstärkt: Steigt der Kurs dank großer Nachfrage, erwarten Optimisten ein neues Hoch und verstärken den Trend, bis die Ersten abspringen und der Kurs wieder fällt.

- **Schwierige Beschaffung**
  Spätestens seit der Einführung des Euros ist das Wechseln von verschiedenen Währungen aus dem Alltag verschwunden. Erschwerend kommt hinzu, dass Bitcoin nicht an regulären Banken gewechselt wird, sondern entweder an Bitcoin-Börsen oder auf der Straße.

Der Handel über eine Bitcoin-Börse lei-

[1] Spendbitcoin.de, Abrufdatum 2014-11-17
[2] Blockchain.info

det unter einer Einstiegshürde, die primär der Gesetzgebung gegen Geldwäsche geschuldet ist: Ohne umfangreiche Registrierung und Verifikation durch die Börse können Bitcoin weder genoch verkauft werden. Da die Börsen – anders als Banken – keine Filialen haben, an welchen die Registrierung durchgeführt werden kann, muss der Vorgang online durchgeführt werden. Dies kann mehrere Tage in Anspruch nehmen und schreckt durch Aufwand und benötigte Dokumente viele Nutzer ab.

Die Alternative ist der Kauf von Bitcoin auf der Straße. Diese Methode verlangt allerdings auch einiges an Vertrauen, denn der Verkäufer wird meist in bar bezahlt. Vor- und Nachteile dieses Transaktionsweges sind offensichtlich und werden entsprechend nicht weiter diskutiert.

2 Warum Bitcoin?

Nachdem besprochen wurde, warum Bitcoin so wenig verbreitet ist, stellt sich natürlich die Frage, welche Vorteile existieren, die die Existenz einer solchen Technologie rechtfertigen.

Pseudonymität

Zuerst einmal ist Bitcoin pseudonym. Dies bedeutet, dass eine Bitcoin-Transaktion nicht auf ihren Aussteller zurückgeführt werden kann, sondern höchstens auf seine Bitcoin-Adresse. Dies ist besonders wichtig, da die Transaktion später in der Blockchain persistiert wird und damit öffentlich ist. Zur Wahrung der Pseudonymität empfiehlt es sich, für jede Transaktion eine neue Adresse zu generieren, da ansonsten vergangene Transaktionen korreliert werden können. Die Gefahr, dass Bitcoin die Adressen ausgehen besteht nicht, da die Anzahl möglicher Bitcoin-Adressen die Anzahl der Atome in unserem Sonnensystem übersteigt.

Die Pseudonymität von Bitcoin erlaubt es, Online-Transaktionen durchzuführen, ohne dass amerikanische Unternehmen alle Daten mitschneiden können – sie ist sozusagen ein Garant für die Privatsphäre, die jedem Internet-Nutzer zusteht und durch die Nutzung von PayPal sowie dem Swift-Abkommen untergraben wurde.

Dezentralität

Im Gegensatz zu vorhandenen Lösungen ist Bitcoin dezentral. Es existiert also keine zentrale Struktur oder Entität, die angegriffen werden kann, um Bitcoin abzuschalten.

Dies mag auf den ersten Blick unwahrscheinlich erscheinen, allerdings wurden bereits verschiedene andere rein digitale Währungen von US-Behörden verboten und vom Netz genommen und vorhandene Guthaben damit entwertet. Weiterhin verhindert die dezentrale Struktur, dass der „Verwalter“ von Bitcoin plötzlich Gebühren erhebt, wenn die Kryptowährung erst etabliert ist.

Flexibilität & Kosten

Wirklich punkten kann Bitcoin bei der Flexibilität der Währung: Bisher war es entweder möglich, Geld sofort, aber nur von

Mensch zu Mensch auszugeben (Bargeld, Wertmarken, Bons,...) oder über weite Distanzen (Überweisung, Kreditkarte, Western Union, ...), was mit Wartezeiten verbunden war.

Bitcoin ermöglicht es, praktisch sofort beliebig große Geldbeträge an jeden Punkt auf dem Globus zu überweisen. Die Kosten für eine Transaktion liegen – ungeachtet des Betrags – bei 0,0005 Bitcoin; dies entspricht beim aktuellen Kurs dem Bruchteil eines Cents.

3 Herausforderungen

Wie bereits besprochen ist die größte Herausforderung für Bitcoin das Wachstum. Durch den langsamen Start und negativen Ersteindruck konnte keine Sogwirkung erzielt werden, die anderen, erfolgreichen Technologien zu eigen ist. Die geplatzten Spekulationsblasen führten zu einem weiteren Vertrauensverlust der Währung, wodurch die kritische Masse an Nutzern unerreicht bleibt.

Um Bitcoin zum Durchbruch zu verhelfen, müssen Rahmenbedingungen geschaffen werden, mit denen ein positives Image für Bitcoin erarbeitet und die Vorteile herausgearbeitet werden. Sobald sich die kritische Masse einfindet, kann sich der Bitcoin-Kurs stabilisieren und die Akzeptanz erhöht sich.

4 Bitcoin am if(is)

Um diese Ziele zu erreichen und Bitcoin einen Platz im täglichen Leben zu verschaffen, müssen die richtigen Maßnahmen ergriffen werden. Wir vom Institut für Internet-Sicherheit sind zwar keine Pioniere mehr, wenn es um PR-Arbeit für Bitcoin geht, aber nehmen unsere Rolle umso ernster: Die folgenden Bitcoin-Projekte werden zurzeit vom if(is) betreut:

Bitcoin-App „BitPocket“

Das Institut für Internet-Sicherheit stellt mit BitPocket eine eigene Bitcoin-App bereit, die den Umgang mit Bitcoin erleichtern soll. So kann gewährleistet werden, dass eine umfassende Sicherheitslösung „made in Germany“ entsteht, die den hohen Sicherheitsanforderungen genügt, die der Umgang mit Geld erfordert.

Blockchain-Visualisierung

Die Blockchain ist bereits über 25 GByte groß und besteht aus über 300.000 Blöcken, die wiederum über 50 Millionen Transaktionen beinhalten. Für sich gesehen sind diese Daten nur Überweisungen zwischen zwei Parteien, aber als Ganzes sind sie viel mehr: Die Blöcke spiegeln die Geschichte von Bitcoin wider, viele, kleinere Transaktionen in Zeiten des Booms und die Spuren der Panikverkäufe, als die Blase platzte. Wir hoffen, durch die Analyse der Vergangenheit, Informationen über die Zukunft von Bitcoin ermitteln zu können. Zu diesem Zweck wird die Blockchain geparst und über Big-Data-Algorithmen visualisiert und die Daten nach Abschluss des Projekts zur Verfügung gestellt.

Sichere Bitcoin-Infrastruktur

Das Institut platziert sich weiterhin mit einem eigenen Beitrag zum Bitcoin-Netzwerk in Form eines sicheren Bitcoin-Nodes. Über diesen wird die Kommunikation mit der BitPocket-App abgewickelt, so dass diese keine lokale Kopie der Blockchain vorhalten muss. Insbesondere die sichere Verwendung von Sicherheitsmodulen, soll mehr Vertrauen von Wallets erzielen. Weitere Funktionen der Infrastruktur werden noch entwickelt.