F A C H H O C H S C H U L E W E D E L

Seminar IT-Sicherheit

Bitcoin

Wintersemester 2015/2016

Eingereicht von:	Hendrik Helmken (Mat.-Nr. winf1083) E-Mail: winf1083@fh-wedel.de
Erarbeitet im:	7. Semester
Abgegeben am:	06.01.2016
Betreuer (FH Wedel):	Prof. Dr. Gerd Beuster Fachhochschule Wedel Feldstraße 143 22880 Wedel Tel. 04103 8048 – 38 Email: gb@fh-wedel.de

Inhaltsverzeichnis

Literaturverzeichnis

[1] S. Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Zugriff am Dezember 2015].

[2] „Spiegel Online," [Online]. Available: http://www.spiegel.de/netzwelt/web/bitcoin-erfinder-angeblich-enttarnt-ist-es-craig-wright-a-1066828.html. [Zugriff am Dezmber 2015].

[3] „Bitcoin Developer Documentation," [Online]. Available: https://bitcoin.org/en/developer-documentation. [Zugriff am Dezember 2015].

[4] „Anzahl der Transaktionen pro Tag," [Online]. Available: https://blockchain.info/de/charts/n-transactions. [Zugriff am Dezember 2015].

[5] D. Assenmacher, „Bitcoin und E-Commerce," [Online]. Available: https://www.wi.uni-muenster.de/sites/default/files/public/department/itsecurity/mbc13/mbc13-assenmacher-paper.pdf. [Zugriff am Dezember 2015].

[6] „Gambler's Ruin Problem," [Online]. Available: http://www.columbia.edu/~ks20/FE-Notes/4700-07-Notes-GR.pdf. [Zugriff am Dezember 2015].

[7] „Common Vulnerabilities and Exposures," [Online]. Available: https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures#CVE-2010-5139. [Zugriff am Dezember 2015].

[8] „Mt Gox und die verschwundenen Bitcoins," [Online]. Available: http://www.heise.de/newsticker/meldung/Mt-Gox-und-die-verschwundenen-Bitcoins-2131432.html. [Zugriff am Dezember 2015].

[9] „Mt Gox meldet auch in den USA Insolvenz an," [Online]. Available: http://www.heise.de/newsticker/meldung/Mt-Gox-meldet-auch-in-den-USA-Insolvenz-an-2140079.html. [Zugriff am Dezember 2015].

[10] „Bitcoin Release 0.9.1," [Online]. Available: https://bitcoin.org/en/release/v0.9.1. [Zugriff am Dezember 2015].

[11] „Bitcointalk Forum,“ [Online]. Available: https://bitcointalk.org/index.php?topic=83794.0#post_allinvain_theft. [Zugriff am Dezember 2015].

[12] „World's First Bitcoin ATM Opens In Vancouver, Canada,“ [Online]. Available: http://mashable.com/2013/10/30/bitcoin-atm-2/#a620qhgoF5q7. [Zugriff am Dezember 2015].

[13] „Bitcoin FAQ,“ [Online]. Available: https://en.bitcoin.org/en/faq. [Zugriff am Dezember 2015].

[14] „Non-specialized hardware comparison,“ [Online]. Available: https://en.bitcoin.it/wiki/Non-specialized_hardware_comparison. [Zugriff am Dezember 2015].

[15] „Bitmain ANTMINER S7 Batch 8,“ [Online]. Available: https://www.bitmaintech.com/productDetail.htm?pid=00020151117034129818 0m44675v0613. [Zugriff am Dezember 2015].

Abbildungsverzeichnis

Einleitung

Bitcoin ist das erste dezentralisierte Peer-to-Peer Zahlungsnetzwerk. Dieses Netzwerk wird nur von den Nutzern betrieben und ist ohne zentrale Autorität oder Vermittler. Bitcoin ermöglicht vollständig digitales Geld und ist aus Nutzerperspektive mehr oder weniger Bargeld für das Internet.

Das erste Konzept einer *Krypto-Währung* wurde erstmals auf der Cypherpunk Mailingliste von Wei Dai beschrieben. [1] Zentraler Gegenstand dieses Konzeptes ist eine neue Art von Geld, welche Kryptographie anstelle einer zentralen Autorität verwendet, um die Herstellung und Transaktion zu kontrollieren. Unter dem Pseudonym Satoshi Nakamoto wurde die erste Bitcoin-Spezifikation 2009 verfasst. [1]

Laut mehreren Medienberichten soll es sich bei dem Pseudonym um zwei Personen handeln, den Australier Craig Wright sowie den mittlerweile verstorbenen US-Amerikaner Dave Kleiman. [2]

Die Bitcoin Software ist Open Source, aus diesem Grund gibt es keinen „Besitzer“ des Bitcoin Netzwerkes. Die Entwicklung findet durch mehrere Entwickler der Bitcoin Community statt, als Versionierungstool wird github verwendet. Der Begriff Bitcoin steht einerseits für die digitale und virtuelle Währung, andererseits ist es auch ein Protokoll, mit welchem diese Währung realisiert wird.

Technik

Bitcoin Protokoll

Das Bitcoin-Protokoll basiert auf der Arbeit Satoshi Nakamotos. In dieser wird eine Form elektronischen Bargeldes beschrieben, welche als Bitcoin bezeichnet wird. Dabei soll diese Form elektronischen Bargeldes ausschließlich in einem gleichberechtigten Peer-to-Peer Netzwerk verwaltet werden. Die dezentrale Organisationsstruktur des Bitcoin-Systems ist der große Unterschied zu traditionellen Geldsystemen, da das Bitcoin-System ohne eine zentrale Kontrollinstanz auskommt. Der Austausch von Geldeinheiten findet direkt statt, ohne eine zentrale Kontrollinstanz wie im Bankensystem.

Es müssen für digitales Geld Anforderungen erfüllt werden, die auch für reguläres Bargeld gelten. Da es sich bei Bitcoin als Geldeinheit im Prinzip um eine lange, mit bestimmten mathematischen Berechnungen erzeugte Zeichenkette handelt, ist es sehr einfach, eine solche digitale Währungseinheit zu kopieren. Dies führt zum sogenannten Problem *Double-Spending* [3], bei dem von einer Person eine Geldeinheit unrechtmäßig mehrfach verwendet wird. Dieses Problem tritt bei Bargeld nicht auf. Im traditionellen Zahlungssystem existieren aus diesem Grund Drittparteien, welche die Verifikation von Transaktionen durchführen. Dieses Verfahren widerspricht jedoch der Grundidee des Bitcoin-Protokolls, welches auf kryptographischer Kontrolle basiert. [1] Im Bitcoin-Protokoll wird das Double-Spending Problem mit der sogenannten *Blockchain* gelöst. Dieses öffentliche Register beinhaltet alle jemals getätigten Transaktionen und kann von jeder Person eingesehen werden. In Transaktionen werden alle Bewegungen von Geldeinheiten (auch Teilen dieser Geldeinheit) erfasst und später in der Blockchain verpackt.

Netzwerk

Die Kommunikation im Bitcoin-Netzwerk findet mittels TCP statt. Der Standardport ist 8333, jedoch ist es möglich, einen beliebigen anderen Port zu benutzen. IPv6 wird seit der Bitcoin-Core Version 0.7 unterstützt. In diesem Netzwerk werden per Broadcast Transactions und Blöcke propagiert.

Bis zur Version 0.6 des Bitcoin-Core Clients wurde die initiale Verbindung zum Netzwerk über einen IRC-Channel im *irc.lfnet.org* hergestellt. Dabei hat der Bitcoin-Client einen Channel auf diesem IRC-Server betreten, wobei der Benutzername jeweils die codierte IP-Adresse enthält. Durch das decodieren der anderen Benutzernamen des Channels erhält man somit eine Liste einiger aktuell mit dem Bitcoin-Netzwerk verbundenen Teilnehmern. In

neueren Versionen der Client-Software wird eine Liste von einigen Hostnamen benutzt, der Client löst diese Hostnamen in IP-Adressen auf und versucht eine Verbindung mit diesen aufzubauen. Alle 30 Minuten sendet die Client-Software eine Nachricht an verbundene Teilnehmer, um die Verbindung aufrecht zu erhalten. Wenn von einem Teilnehmer seit 90 Minuten keine Nachrichten empfangen wurden, wird diese Verbindung geschlossen.

Bitcoinadresse

Die Bitcoinadresse ist eine Kette von 27 – 34 alphanumerischen Zeichen, die mit einer 1 oder 3 beginnen und ein Ziel für eine Bitcoin Zahlung eindeutig identifizieren. Nutzer können Adressen beliebig und kostenlos erzeugen. Erhalten kann man eine Adresse über den lokal installierten Bitcoin-Client, einen Wechseldienst oder einen online Wallet[1] Dienst.

Eine Zahlung mit Bitcoins wird an eine der Adressen des Zahlungsempfängers gesendet. Zur erhöhten Anonymität bietet es sich an, für jede Transaktion eine neue Adresse zu verwenden. Eine Person kann mehrere Adressen seinem Wallet zuordnen.

Abbildung 1 zeigt graphisch die verschiedenen Schritte, die nötig sind, um eine gültige Bitcoin-Adresse zu erzeugen. Im Folgenden werden diese Schritte genauer betrachtet.

1. Es wird der öffentliche Schlüssel benötigt. Dieser wird mittels des Elliptic Curve Digital Signature Algorithm, kurz ECDSA, generiert. Dabei werden jeweils die 32-Byte Blöcke der X- bzw. der Y-Koordinaten des öffentlichen Schlüssels verwendet. Zusätzlich wird am Anfang 1 Byte (0x04) angefügt.
2. Auf diesem 65-Byte langen Schlüssel wird die Hashfunktion SHA-256 angewendet.
3. Auf diesem 32-Byte langen Hash wird die Hashfunktion RIPEMD-160 ausgeführt, welcher als Ergebnis einen 20-Byte langen Hash liefert.
4. Als nächsten Schritt wird ein Netzwerk-ID-Byte dem Hash vorangestellt. Für das Hauptnetzwerk wird 0x00 verwendet. Somit ist diese Zeichenfolge nun 21 Byte lang.
5. Die Prüfsumme wird durch das zweimalige Ausführen von SHA-256 hintereinander auf die Zeichenfolge aus Schritt 4 berechnet. Jedoch werden für die Prüfsumme der Bitcoin-Adresse nur die ersten 4 Byte von dem Hash benutzt.
6. Die Ergebnisse von Schritt 4 und 5 werden nun zusammengefügt, wobei die Prüfsumme aus Schritt 5 der Zeichenkette aus Schritt 4 angehängt wird. Dies ist die 25-Byte binäre Bitcoinadresse.

[1] siehe Kapitel Wallet, Seite 15

7. Abschließend wird das Ergebnis aus Schritt 6 mit Base58 codiert, woraus sich eine für das menschliche Auge leserlichere Adresse ergibt. Dieses Adressenformat ist das am häufigsten benutzte.

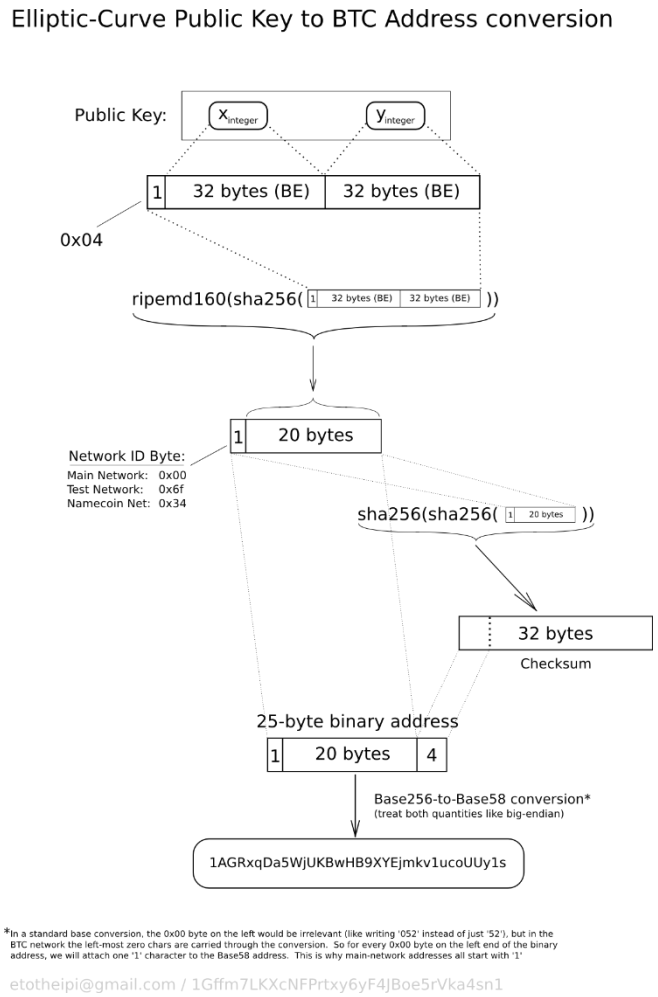

Abbildung 1: Erzeugen von Bitcoinadresse (Quelle: https://en.bitcoin.it/wiki/File:PubKeyToAddr.png)

Transaktionen

Bitcoins existieren nur innerhalb von Transaktionen. Eine Transaktion beinhaltet Einträge zu ein oder mehreren Eingaben sowie ein oder mehreren Ausgaben, vergleichbar mit einem Eintrag in einer Buchhaltung.

Für die Durchführung einer Transaktion ist es nicht notwendig, dass der Empfänger zu dem Zeitpunkt online ist. Es ist zudem auch nicht erforderlich, direkt mit dem Empfänger verbunden zu sein. Eine Transaktion wird dem Bitcoin-Netzwerk mitgeteilt, indem die Transaktion beliebigen, mit dem Sender verbundenen Teilnehmern des Peer-to-Peer

Netzwerkes gesendet wird. Diese verbreiten die Transaktion dann wiederum an alle mit ihnen verbundenen Teilnehmern. Eine Transaktion gilt als gültig, wenn diese in die Blockchain aufgenommen wurde. Da Transaktionen nicht verschlüsselt sind, können alle jemals getätigten Transaktionen ausgelesen werden.

Eine Transaktion besteht im Wesentlichen aus zwei Feldern, Input und Output. Das Feld Input beinhaltet alle Quelltransaktionen, diese werden mittels eines Hash-Wertes sowie eines Index-Wertes angegeben. Der Index-Wert ist dabei der spezifische Output in der referenzierten Input-Transaktion. Das Feld Output beinhaltet zum einen den Wert der Transaktion, angegeben in Satoshi[2], zum anderen die Bitcoin-Adressen der Empfänger. Da jeder Output einer Transaktion nur genau einmal referenziert werden kann, wird nicht verwendetes Guthaben an einen selber gesendet (zu vergleichen mit Wechselgeld bei Bargeld). Die Differenz zwischen Input und Output wird als Transaktionsgebühr benutzt. Diese wird dem Miner gutgeschrieben, der die Transaktion als erstes erfolgreich in einen Block schreibt. Damit eine Transaktion bevorzugt von einem Miner verarbeitet wird, kann man diese Gebühr erhöhen.

In folgendem Beispiel will Alice einen Betrag an Bob überweisen. Vereinfacht dargestellt läuft eine Transaktion folgendermaßen ab:

- Alice signiert eine Nachricht, die aus allen benötigten Informationen besteht, mit ihrem privaten Schlüssel.
- Über den öffentlichen Schlüssel von Alice kann in Kombination mit ihrer an die Nachricht angehängten Signatur festgestellt werden, ob Alice berechtigt ist, diese Transaktion durchzuführen. Die Transaktion wird nach ca. 10 Minuten durch das hinzufügen der Transaktion zu der Blockchain durch einen Miner bestätigt und autorisiert. Mit jedem weiteren Miner, der diesen Block inklusive der Transaktion von Alice und Bob bestätigt, steigt die Sicherheit, dass die Transaktion korrekt abgewickelt wurde, exponentiell.

[2] 1 BTC = 100.000.000 Satoshi

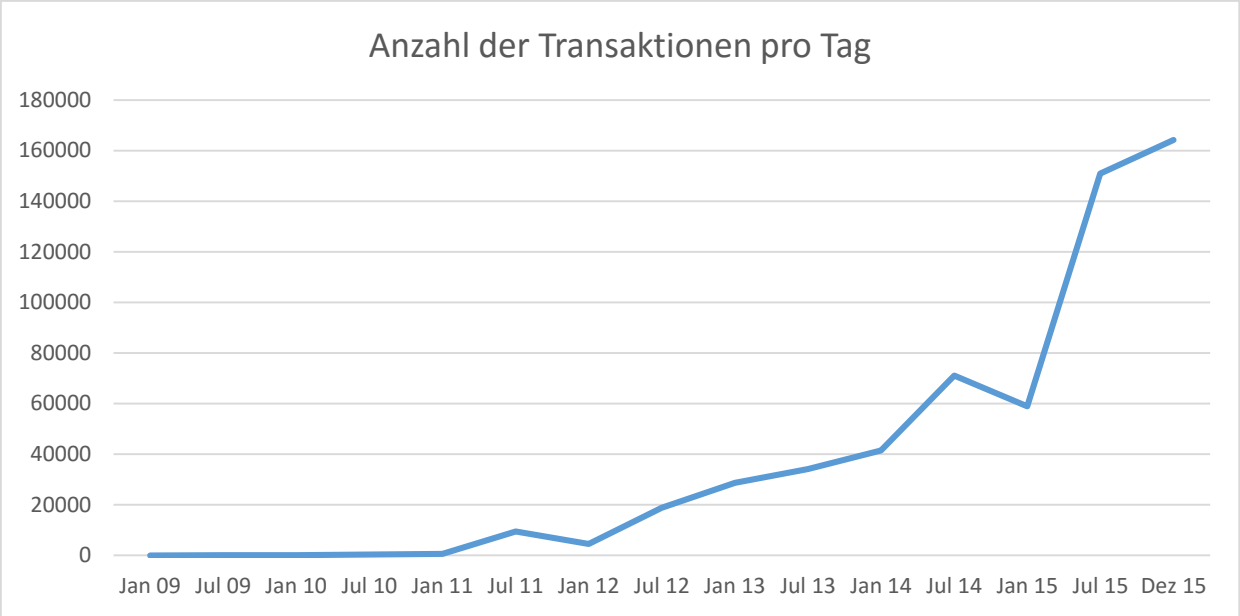

Abbildung 2 Transaktionen/Tag (Datenquelle: blockchain.info)

Abbildung 2 zeigt die Transaktionen pro Tag in dem Zeitraum von Januar 2009 bis Januar 2016. Bis Mitte 2012 lag die Anzahl der Transaktionen pro Tag auf einem maximalen Wert von ca. 12.000. In dem Zeitraum danach ist die Anzahl der Transaktionen stark gestiegen bis auf einen Wert von ca. 185.000 für Januar 2016. Dies zeigt die steigende Popularität des Bitcoin-Systems.

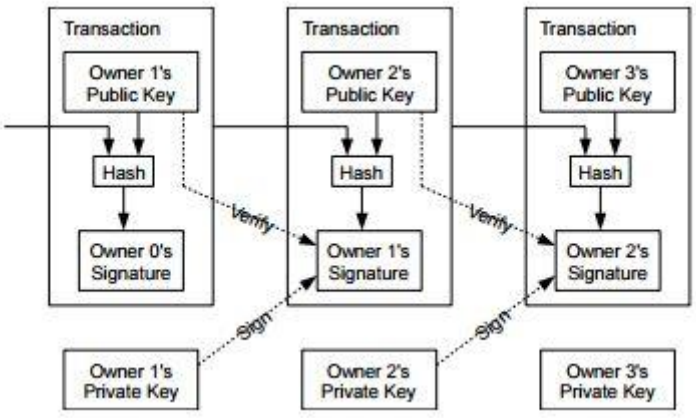

Abbildung 3: Transaktionen (Quelle: [1], Abbildung 1)

Abbildung 3 erläutert, wie die Transaktion jeweils als Input für die nächste dient und wie die Zugehörigkeit mittels Verifikation von digitalen Signaturen überprüft werden kann.

Mining

Das Bitcoin-Protokoll ist auf Recheneinheiten angewiesen, welche in weiterer Folge nur noch als Miner bezeichnet werden. Die Miner erzeugen neue gültige Hash-Werte aus gebündelten Transaktionen, welche anschließend an die Blockchain eingefügt werden. Gebündelte Transaktionen werden Transaktionsblöcke genannt, welche in weiterer Folge nur noch als Block bezeichnet werden.

Damit ein Block in die Blockchain aufgenommen wird, müssen bestimmte Regeln eingehalten werden. Der neue Hashwert eines Blockes muss mit einer bestimmten Mindestanzahl an Nullen beginnen. Diese Anzahl wird vom Bitcoin-Netzwerk automatisch festgelegt und als Difficulty bezeichnet. Derzeit wird alle 2016 Blöcke überprüft, ob die durchschnittliche Bearbeitungszeit eines Blockes bei 10 Minuten liegt. Dies bedeutet, dass alle zwei Wochen die Difficulty, wie die Anzahl der Nullen im Bitcoin-Netzwerk bezeichnet wird, angepasst wird. Umso mehr Miner am Mining-Prozess teilnehmen, umso höher wird die Difficulty.

Jeder Block enthält als erste Transaktion die Auszahlung der Belohnung für den Erzeuger des Blockes. Durch dieses Verfahren stellt das Mining einen finanziellen Anreiz für Miner dar.

Der Mining-Prozess läuft vereinfacht notiert folgendermaßen ab (Pseudocode):

```
Zeichenkette input initialisieren;
input = input + 'Version des Blocks';
input = input + '256-Bit Hash des vorherigen Blockheaders';
input = input + '256-Bit Hash der Liste aller neu hinzugekommenen
Transaktionen';
input = input + 'aktueller UNIX-Timestamp';
input = input + 'Target (entspricht der aktuellen Difficulty)';
input = input + '32-Bit Nonce (0x00)';

while 'Anzahl der Nullen am Beginn von output' < 'Difficulty' do
Zeichenkette output = input + 'Nonce + 1';
sha256(sha256(output));
end
```

Zunächst wird eine Zeichenkette bestehend aus der Version des Blocks, dem Hash des vorherigen Blockheaders und der Liste aller neuen Transaktionen, dem aktuellen Timestamp, der Difficulty sowie der Nonce konkateniert. Von dieser Zeichenkette wird mit der Hashfunktion SHA-256 der Hash errechnet, wenn der erhaltene Hashwert die geforderte Anzahl an Nullen am Anfang besitzt, ist ein neuer Block gefunden. Dieser wird dann in die Blockchain aufgenommen. Wenn jedoch die erforderliche Anzahl an Nullen nicht erreicht

wurde, wird die Nonce erhöht und die Hashfunktion abermals ausgeführt. Dieser Prozess wird so oft wiederholt, bis ein gültiger neuer Block gefunden wurde oder ein anderer Miner bereits einen gültigen Hash für diesen Block gefunden hat.

Blockchain

Wie bereits gezeigt, werden alle Transaktionen in Blöcken in zeitlich abgestimmten Abständen zusammengefasst. In diesen Blöcken liegen die Transaktionen in chronologischer Reihenfolge vor. In der Blockchain werden alle Blöcke zusammengefasst.

Im Bitcoin-Netzwerk gibt es mangels einer zentralen Kontrollstelle eine Regel, mit welcher eine Blockchain als einzig gültige definiert wird. Da jeder Block den Hash des vorherigen Blockes enthält, entsteht eine Kette aus Blöcken vom ersten Block bis zum aktuellen Block. Da mehrere Miner am Mining-Prozess beteiligt sind und diese auch parallel neue Blöcke erstellen, kann es zu der Situation kommen, dass es zwei verschiedene Wege in der Blockchain gibt. Jedoch wird die Blockchain, an der die meisten Miner beteiligt sind, zwangsläufig schneller länger. Daraus ergibt sich, dass in diese Blockchain die größere Rechenleistung geflossen ist. Dies bedeutet, dass diese Blockchain vom Bitcoin-Netzwerk als gültig erachtet wird und die andere, kürzere Blockchain nicht fortgeführt wird. Die kürzere Blockchain wird als Fork bezeichnet. In der Praxis treten Forks dann auf, wenn zwei neue Blöcke innerhalb von nur wenigen Sekunden kreiert werden. Der Block, welcher zuerst von einem anderen fortgesetzt wird, wird automatisch zur neuen gültigen Blockchain, da diese Kette von Blöcken länger ist. Alle Transaktionen der kürzeren Blockkette werden dem Pool aller offenen Transaktionen hinzugefügt.

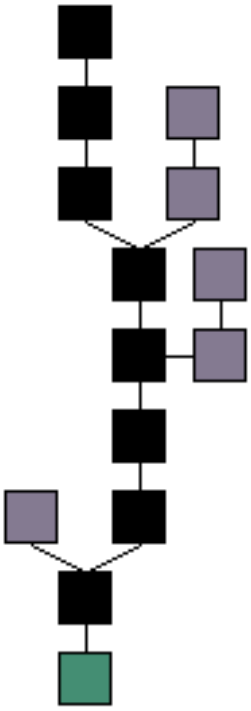

Abbildung 4: Blockchain mit Forks (Bitcoin Wiki: https://en.bitcoin.it/wiki/File:Blockchain.png)

Abbildung 4 zeigt eine Blockchain, wobei der grüne Block der Ursprungsblock ist. Die gültige Blockchain besteht aus den schwarzen Blöcken, lila Blöcke kennzeichnen Forks, welche verworfen wurden.

Die Größe der Blockchain betrug im Januar 2012 500MB, seitdem ist die Größe auf 50GB im Dezember 2015 angewachsen. Dieser rasante Anstieg der Größe der Blockchain lässt sich mit der erhöhten Anzahl von Transaktionen erklären. In Abbildung 5 ist dieses Wachstum graphisch dargestellt.

Es muss jedoch nicht jeder Knoten im Bitcoin-Netzwerk die komplette Blockchain lokal vorliegen haben. Für Anwendungen, die nur für eine Wallet konzipiert sind, reicht es aus, wenn diese nur die Block-Header im Speicher halten. Dadurch entfällt auch der initiale Download der Blockchain, was eine große Zeitersparnis darstellt.

Ende Dezember 2015 gab es etwa 156.000 Transaktionen am Tag, dies entspricht ca. 1,8 Transaktionen/Sekunde. [4]

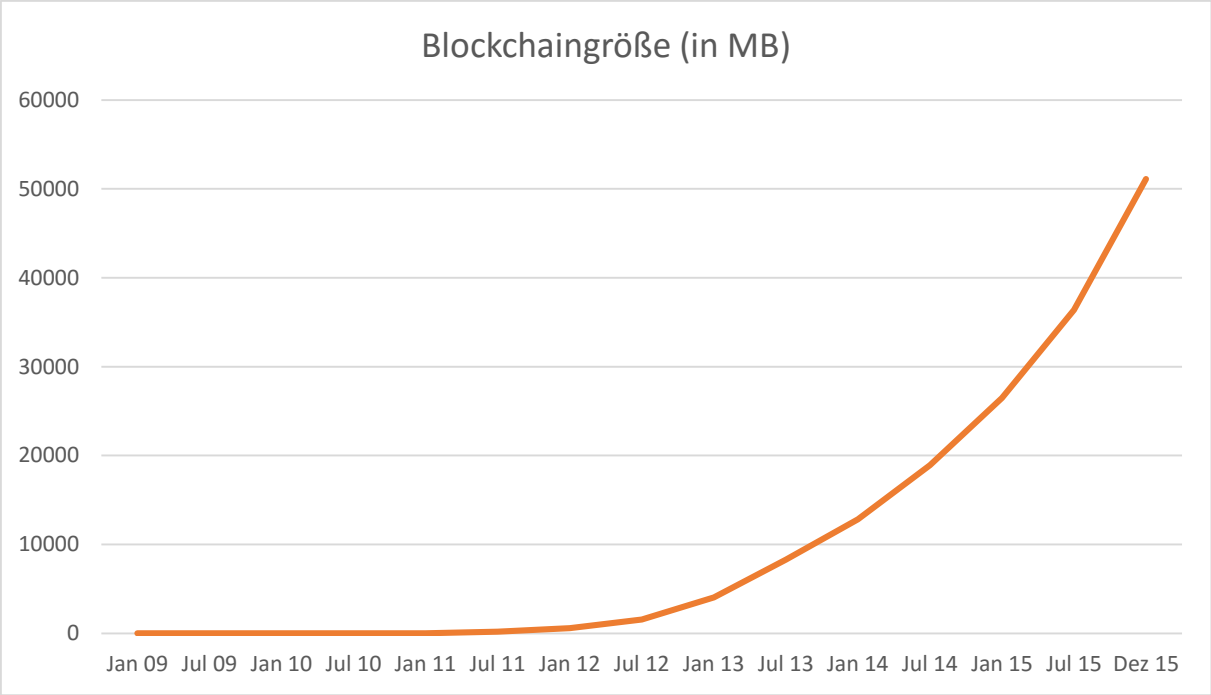

Abbildung 5 Blockchaingröße (Datenquelle: blockchain.info)

Obergrenze

Das Problem der initialen Verteilung der Währung wird durch das System gelöst, wie Bitcoins erzeugt werden: Nur durch das Finden eines Blockes werden Bitcoins erzeugt und dem Finder als Belohnung gutgeschrieben. Am Anfang wurden 50 Bitcoins für das Finden eines Blockes ausgegeben, diese Summe wird nach jeweils 210.000 Blöcken halbiert. Daraus ergibt sich eine maximale, jemals im Umlauf befindliche Anzahl an Bitcoins, welche mit folgender Formel berechnet werden kann [5]:

$$\sum_{k=0}^{\infty}\left(210.000 * 50 * \frac{1^k}{2}\right) = \frac{10.500.000}{1-\frac{1}{2}} = 21.000.000$$

Wie in Abbildung 6 zu sehen, ist die Anzahl von 21 Millionen Bitcoins noch nicht erreicht. Mit Stand Dezember 2015 sind etwa 15 Millionen Bitcoins im Umlauf.

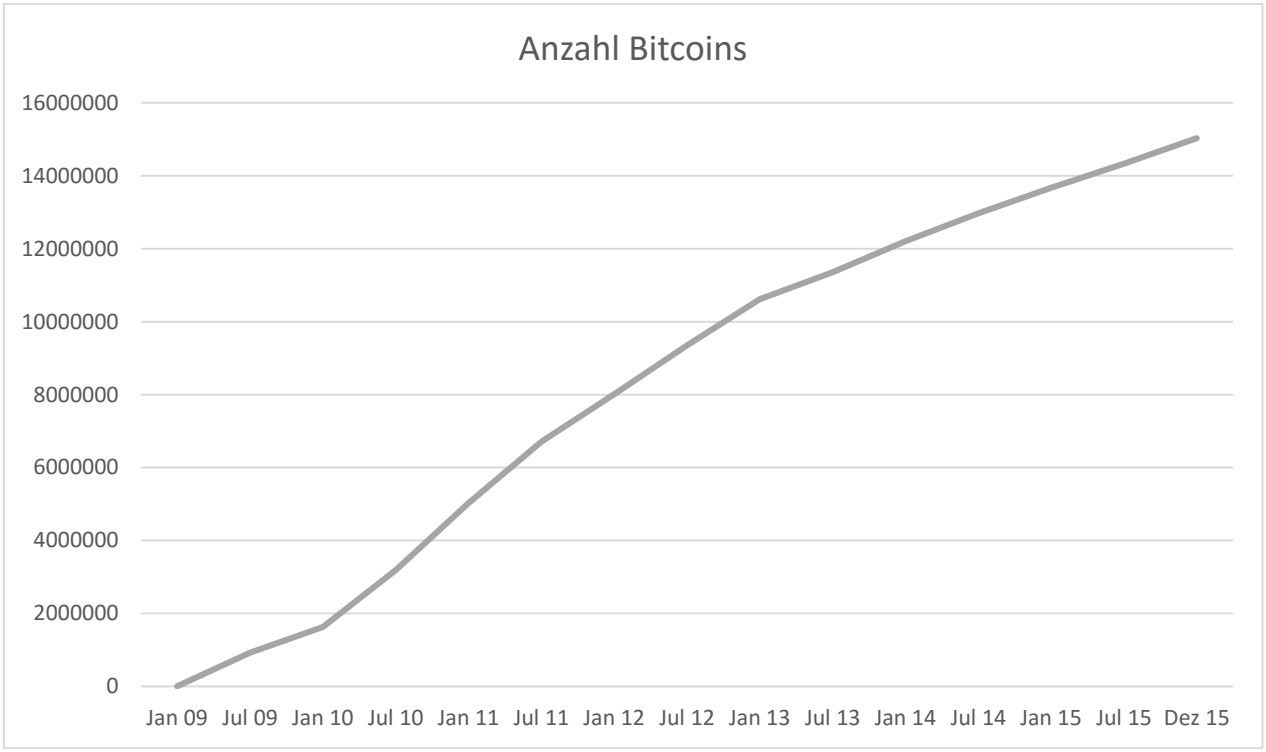

Abbildung 6 Anzahl Bitcoins (Datenquelle: blockchain.info)

Sicherheit

Anonymität

Die Anonymität des Bitcoin-Protokolls war zu Beginn nicht von zentraler Bedeutung. Wie bereits in vorigen Kapiteln gezeigt, werden alle jemals getätigten Transaktionen in der öffentlichen Blockchain hinterlegt. In den Transaktionen stehen jeweils die Daten zu Empfangsadresse, Sendungsadresse und dem Betrag. Die Sendungs- bzw. Empfangsadresse liegt als Bitcoin-Adresse vor.

Ein direkter Rückschluss auf die Person hinter einer Bitcoin-Adresse ist nicht direkt möglich. Es gibt jedoch zumindest zwei Möglichkeiten, um die Anonymität einer Bitcoin-Adresse aufzuheben:

1. Das Bitcoin-Netzwerk ist ein Peer-to-Peer Netzwerk. In diesem ist es wie in jedem Peer-to-Peer Netzwerk möglich, die IP-Adressen anderer Teilnehmer festzustellen. Über die IP-Adresse ist die Identität einer Person mittels des juristischen Weges über den Internet Service Provider sowie eines richterlichen Beschlusses feststellbar.
2. Anhand der (un)beabsichtigten Veröffentlichung der Bitcoin-Adresse eines Nutzers.

Um zu verhindern, dass durch die Zuordnung einer Bitcoin-Adresse zu der Identität der Person alle Transaktionen ausgelesen werden können, ist es zu empfehlen, für jede Transaktion eine neue Bitcoin-Adresse zu verwenden.

51% Angriff

Bei dem 51% Angriff handelt es sich um eine Möglichkeit, eine alternative Blockchain im Netzwerk als gültig werden zu lassen. Dies hat zum Beispiel zum Ziel, einen getätigten Einkauf durch *Double Spending* in der alternativen Blockchain rückgängig zu machen. Es ist jedoch nicht möglich, willkürlich Transaktionen zu verändern, sondern nur die eigenen. Somit ist der Handlungsspielraum des Angreifers stark eingeschränkt. Um diese Form des Angriffes jedoch erfolgreich durchzuführen, benötigt der Angreifer mehr als 50% der Rechenleistung des gesamten Bitcoin-Netzwerkes. Dieser Angriff wird als 51% Angriff bezeichnet.

Wenn der Angreifer 10% des Netzwerkes kontrolliert, ist die Wahrscheinlichkeit eines erfolgreichen Angriffes bei 0,1%, wenn der Angreifer hingegen mehr als 50% der Hashrate des Netzwerkes kontrolliert, liegt die Wahrscheinlichkeit bei 100%. [3]

Nakamoto beschreibt die Wahrscheinlichkeit eines erfolgreichen Angriffs in Analogie zum *Gambler's Ruin Problem.* [6] Dieser Vergleich ist charakterisiert durch ein Ausgangs-Defizit und eine unbeschränkte Anzahl an Versuchen, um den Break-Even-Point zu erreichen. Beim 50%-Angriff ist das Ausgangs-Defizit die Differenz an Blöcken zwischen Angreifer- und ehrlicher Blockchain. Ist nun die Wahrscheinlichkeit des früheren Findens eines neuen Blockes durch die ehrlichen Rechner größer als jene der Angreifer, so sinkt die Wahrscheinlichkeit jemals wieder aufzuholen exponentiell mit der Größe der Distanz zwischen Angreifer- und ehrlicher Blockchain.

Zwischenfälle im Bitcoin-Netzwerk

Der bisher schwerste Softwarefehler im Bitcoin-System wurde am 15. August 2010 entdeckt. Dabei wurde im Block 74638 eine Transaktion entdeckt, die zu einer Gutschrift von 184 Milliarden Bitcoins führte. Als Fehlerursache wurde ein fehlerhafter Ganzzahlüberlauf bei der Summierung von Outputs identifiziert. [7]

Ende Februar 2014 hat die Bitcoin-Börse Mt. Gox in Japan [8] sowie in den USA Insolvenz angemeldet. Im Zuge dessen wurde bekannt, dass annähernd 850.000 Bitcoins verloren wurden. Dies entspricht einem damaligen Wert von 368,4 Millionen Euro. Von den 850.000 Bitcoins gehörten 750.000 Kunden sowie 100.000 der Börse. [9]

Anfang April 2014 wurde bekannt, dass der Bitcoin Core vom Heartbleed-Bug der OpenSSL-Bibliothek betroffen war. Die Entwickler der Software reagierten jedoch umgehend auf diese Sicherheitslücke und schlossen diese mit dem Release von Version 0.9.1. [10]

Bisher wurden Bitcoins nur durch Diebstahl dem rechtmäßigen Besitzer entwendet. Als Beispiel dient der Diebstahl von 25.000 Bitcoins (damaliger Gegenwert in US-Dollar 50.750), der Dieb bzw. Hacker hat sich Zugang zu dem Computer des Nutzers verschafft und so die Bitcoins entwendet. Diese konnten von dem Angreifer unbemerkt wieder in Umlauf gebracht werden. [11] Dies bedeutet jedoch nicht, dass Bitcoins angreifbar sind. Als Vergleich kann man auch nicht sagen, dass der Euro kompromittiert wurde durch einen Bankraub. Dennoch haben solche Meldungen in der Presse einen negativen Einfluss auf die Bewertung von Bitcoin durch die Öffentlichkeit.

Anwendung

Erwerb von Bitcoins

Wechselbörsen

Es gibt bereits einige Online-Wechselbörsen, die eine beliebige Währung in Bitcoins umtauschen. Hier wird oftmals eine Gebühr für diesen Service fällig. Bei Online-Wechselbörsen ist darauf zu achten, dass es sich um seriöse Angebote. Um sich bei einer solchen Börse anzumelden ist meist eine Identifizierung notwendig. Es müssen Personalausweis und Adresse bekanntgegeben werden.

Bitcoin-ATM

Abbildung 7: Bitcoin ATM (Urheber: Micha L. Rieser, Quelle: https://de.wikipedia.org/wiki/Datei:Bitcoin_Geldautomat.jpg)

Neuerdings gibt es an einigen Standorten bereits Bitcoin-ATM, diese ermöglichen gegen eine kleine Gebühr sehr schnell Bargeld in Bitcoins zu tauschen. [12] Man hält dazu lediglich den QR-Code seiner Bitcoin-Adresse bereit und wirft Geld in den Automaten. Der eingeworfene Betrag wird anschließend als Bitcoins an die Adresse übertragen.

Tauschen mit Bekannten

Dabei handelt es sich vermutlich um die einfachste Variante an Bitcoins zu kommen. Kennt man jemanden, der bereits Bitcoins besitzt, kann man diese direkt mit dieser Person tauschen.

Wallet

Das Wallet (englisch für „Portemonnaie“) bezeichnet eine Client-Software, mit Hilfe derer der Nutzer seine Bitcoins verwaltet sowie Transaktionen durchführt. Jedoch ist das Konzept einer Wallet eher mit dem einer Kreditkarte vergleichbar, da Bitcoins nur in der Blockchain existieren, somit wird mit Hilfe des privaten Schlüssels der Nachweis vollbracht, Eigentümer einer gewissen Menge an Bitcoins zu sein.

Mining

Wie bereits gezeigt, ist das Mining ein Prozess, ohne den das Bitcoin-System nicht funktionieren würde. Für die Miner ist der Anreiz die ausgeschütteten Bitcoins, die beim Finden eines Blockes ausgegeben werden. Die Anzahl der ausgeschütteten Bitcoins pro gefundenem Block setzt sich aus den Transaktionsgebühren der in diesem Block verarbeiteten Transaktionen sowie dem mit dem neuen Block neu erzeugten Bitcoins zusammen. Mining kann man als das Bitcoin-Rechenzentrum betrachten, mit der Abweichung, dass es so entwickelt wurde, dass es komplett dezentralisiert ist. [13]

Um am Prozess des Minings teilzunehmen, wird eine Software benötigt (und mittlerweile spezialisierte Hardware). Wie in Abbildung 5 ersichtlich, ist die Hashrate seit Januar 2014 bis Dezember 2015 von 5.000 TH/s[3] auf 900.000 TH/s gestiegen. In der Anfangszeit konnte noch mit einem normalen Computer aussichtsreich am Mining teilgenommen werden, doch mit der steigenden Verbreitung und Anzahl der Miner stieg auch die Hashrate im Bitcoin-Netzwerk, wodurch spezialisierte Hardware wie GPU und ASIC notwendig geworden ist.

[3] TH/s = Tera-Hash/Sekunde, Maßeinheit der Rechenkraft des Bitcoin-Netzwerkes

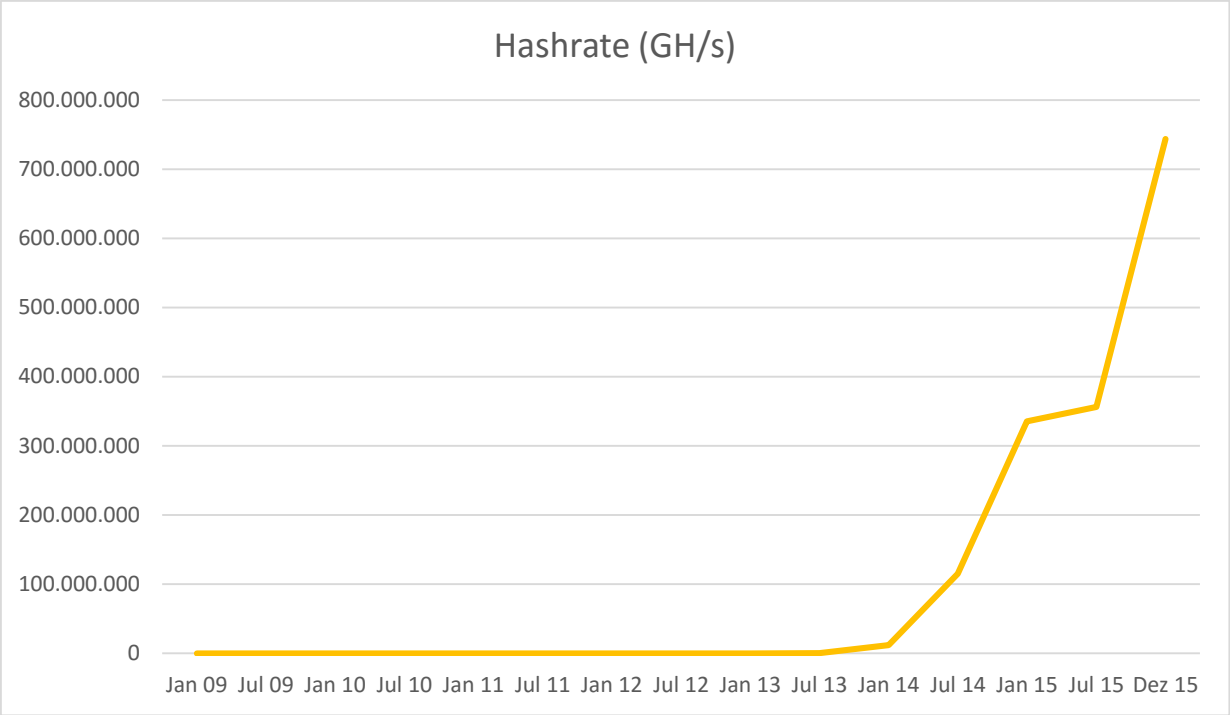

Abbildung 8 Hashrate (Datenquelle: blockchain.info)

Der Vorteil von GPU-Mining ist, dass Grafikkarten wesentlich mehr Rechenoperationen als ein CPU ausführen können. Der Spitzenwert beträgt 2,568 GH/s im Vergleich zum Spitzenwert von 140 MH/s beim CPU-Mining. [14] Das GPU-Mining wurde jedoch bereits durch speziell auf das Mining spezialisierte Hardware ersetzt. Ein aktuelles Gerät der Firma Bitmain hat eine Geschwindigkeit von 4,73 TH/s. [15]

Durch diese Steigerungen der Hashrate ist auch die Steigerung der Difficulty wie in Abbildung 9 ersichtlich zu erklären. Die Difficulty betrug Ende Dezember 2015 etwa 100 Milliarden.

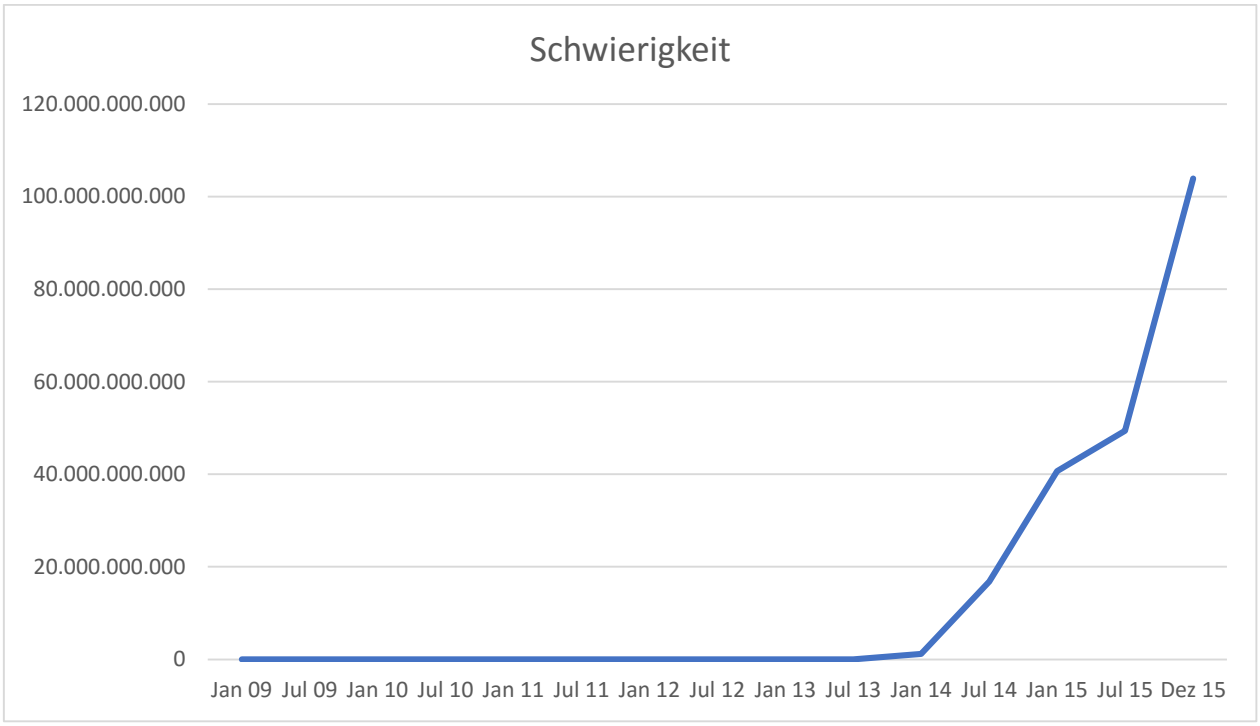

Abbildung 9 Schwierigkeit (Difficulty) (Datenquelle: blockchain.info)

Fazit

Bitcoin verfolgt einen sehr interessanten Ansatz einer Krypto-Währung, welche durchaus als Alternative zu traditionellen Zahlungssystemen betrachtet werden kann. Die steigenden täglichen Transaktionen legen ein Wachstum der Verbreitung nahe. Dadurch steigt die Akzeptanz von Bitcoins generell und vor allem als Zahlungsmittel im Internet. Die Sicherheit und Integrität des Zahlungssystems wird mit Hilfe gängiger und als sicher eingestufter kryptographischer Algorithmen gewährleistet. Zudem sind die bisherigen Zwischenfälle in Verbindung mit Bitcoins nicht auf Schwächen im Bitcoin-Protokoll zurückzuführen.