

Die Bitcoin Bibel

Das Buch zur digitalen Währung



Dr. Philipp Giese • Maximilian Kops • Sven Wagenknecht
Danny de Boer • Mark Preuss



BTC-ECHO
Deutschsprachige Bitcoin-News

Die Bitcoin Bibel

Das Buch zur digitalen Währung
BTC-ECHO

Copyright © 2016 BTC-ECHO

All rights reserved.

ISBN-10: 1534733191

ISBN-13: 978-1534733190

BTC-ECHO

Die Bitcoin Bibel

Das Buch zur digitalen Währung

Dr. Philipp Giese
Mark Preuss
Maximilian Kops
Sven Wagenknecht
Danny de Boer

IMPRESSUM

Texte: © Copyright by BTC-ECHO

BTC-ECHO

Mark Preuss

Albersallee 34

47533 Kleve

info@btc-echo.de

Alle Rechte vorbehalten.

Tag der Veröffentlichung: 18.06.2016

www.btc-echo.de

INHALT

KAPITEL 1 DAS BITCOIN SYSTEM

WAS IST BITCOIN

POLITISCHE DIMENSION UND REGULIERUNG

DAS BITCOIN-WHITEPAPER

ZUSAMMENFASSUNG DES WHITEPAPERS

WER HAT BITCOIN ERFUNDEN?

SATOSHI NAKAMOTO

WAR ER JAPANER?

WEIß IRGENDJEMAND WER SATOSHI NAKAMOTO WAR?

WAS WISSEN WIR ÜBER IHN?

WIE REICH IST ER?

WAS MACHT ER JETZT?

STEUERN UND RECHT

BITCOIN UND RECHT

RECHTLICHE UND STEUERLICHE PROBLEME

ERST RECHTLICHE PLANUNG, DANN START DES UNTERNEHMENS

BITCOIN UND STEUER

BITCOIN UND STEUER FÜR PRIVATANLEGER

BITCOIN UND STEUER FÜR UNTERNEHMEN

FRÜHZEITIGE BERATUNG SINNVOLL

KAPITEL 2 WELCHEN WERT HABEN BITCOINS?

ANGEBOT

NACHFRAGE

WERTENTWICKLUNG

KAPITEL 3 BITCOIN ALS WERTANLAGE

ZEIT IST GELD

KAPITEL 4 BLOCKCHAIN

WAS IST DIE BLOCKCHAIN

WIE FUNKTIONIERT DIE BLOCKCHAIN

WIE FUNKTIONIERT EINE BITCOIN-TRANSAKTION UND WIE SICHER SIND DIESE?

ALTERNATIVE BLOCKCHAIN-ANWENDUNGEN

AKTUELLE HERAUSFORDERUNGEN VON BITCOIN

KAPITEL 5 BITCOIN-MINING

WAS IST BITCOIN MINING?

BERECHNUNGEN

DIFFICULTY

WIE KANN ICH BITCOIN MINEN?

DIE 51% ATTACKE

WAS IST EINE 51% ATTACKE?

WIE FUNKTIONIERT EINE 51% ATTACKE ?

MÖGLICHKEITEN DER 51%-ATTACKE

KAPITEL 6 BITCOIN-WALLETS

MULTI-SIG WALLETS - BRIEFTASCHEN FÜR TEAMS

COLD-STORAGE - DAS OFFLINE-TRESORSYSTEM VON BITCOIN

WIE ERSTELLE ICH EIN WALLET?

ONLINE-WALLET

MOBILE-WALLET

PAPER-WALLET

BRAIN-WALLET

HARDWARE-WALLET

BITCOIN CORE

WIE SICHER IST MEIN WALLET?

KAPITEL 7 BITCOIN KAUFEN UND VERKAUFEN

MÖGLICHKEITEN BITCOIN ZU KAUFEN

BITCOIN-BÖRSEN

BITCOIN-BROKER

FACE TO FACE

KAPITEL 8 MIT BITCOIN BEZAHLEN

WER AKZEPTIERT BITCOINS?

TOOLS ZUM BEZAHLEN MIT BITCOINS

ANDROID

iOS

WINDOWS-PHONE

ÜBERSICHT: WALLET-APPS FÜR UNTERWEGS

KAPITEL 9 BITCOIN AKZEPTANZ

GRÜNDE FÜR DIE INTEGRATION VON BITCOIN

ERWEITERUNG DER ZIELGRUPPE

GERINGE TRANSAKTIONSGEBÜHR

ZAHLUNGSSICHERHEIT

INTERNATIONALITÄT

SCHNELLIGKEIT

COINMAP

BTC-ECHO VERZEICHNIS

RISIKEN

DER KUNDE ZAHLT DIE GEBÜHREN

KEIN FIXER UMTAUSCHWERT FÜR BITCOIN

SICHERE AUFBEWAHRUNG VON BITCOINS

BESTANDSDIVERSIFIKATION

BITCOINS IN DER STEUERERKLÄRUNG

KAPITEL 10 DAS DEEP- UND DARKNET

DEEP-WEB

LEGALE INHALTE

DARKNET

WIE KOMME ICH REIN?

1. INSTALLATION TOR-BROWSER

2. KONFIGURATION TOR-BROWSER

SURFEN IM DARKNET

UND JETZT?

KAPITEL 11 PANIC FAQ

SIND BITCOINS SICHER?

WO KANN MAN SICH BEI BITCOIN ANMELDEN?

SIND BITCOINS VERBOTEN?

WIE VIEL IST EIN BITCOIN WERT?

UND WAS MACHST DU, WENN DU GEHACKT WIRST?

DIE WICHTIGSTEN VORTEILE VON BITCOIN

DIE NACHTEILE VON BITCOIN

ERKLÄRE MIR BITCOIN IN EINEM SATZ

VORWORT

Hast Du schon mal versucht Geld in die USA zu überweisen? Wenn ja, dann hast du bestimmt ein längeres Formular für Auslandsüberweisungen bei deiner Bank ausfüllen müssen. Neben den Gebühren und den Wechselkursschwankungen kann es gut und gerne bis zu zwei Wochen dauern bis das Geld auf dem entsprechenden Konto gelandet ist. Vor 50 Jahren war das sicherlich eine sehr zeitgemäße und schnelle Art Geld zu überweisen. Nun hat sich aber durch das Internet und die Digitalisierung einiges geändert, sodass sich die Frage stellt, ob die heutigen Bankdienstleistungen noch zeitgemäß sind. Zwar bietet heute jede Bank Online-Banking an und an den Finanzmärkten können

ausgeklügelte Finanzderivate gehandelt werden, doch hat sich das Bankwesen als solches kaum verändert. Entsprechend groß ist der Innovationsstau, insbesondere was den Zahlungsverkehr anbelangt. Gleichzeitig sinkt das Vertrauen der Bevölkerung gegenüber den Banken und scheint sich auch mehrere Jahre nach Ausbruch der Finanzkrise von 2008 nicht mehr zu erholen. Als Konsequenz versuchen viele Startups im Finanzwesen, sogenannte Fin-Techs, die Bankenbranche mit neuen, innovativen Lösungen zu revolutionieren. Vorreiter sind hier die USA, wo immer weniger Überweisungen von Bankkonto zu Bankkonto erfolgen. Auch das Bezahlen mit Bargeld wird dort immer stärker aus dem Alltag verbannt. Aber nicht nur in den USA, sondern auch in vielen Ländern Europas, vor allem in den Niederlanden und den

skandinavischen Ländern, ist das bargeldlose Bezahlen bereits viel populärer als in Deutschland.

Der Prozess der Digitalisierung lässt sich weder von Staaten noch von Banken aufhalten. Es ist daher nur eine Frage der Zeit bis der durch die Digitalisierung hervorgerufene Strukturwandel den Zahlungsverkehr und andere Finanzdienstleistungen flächendeckend verändern wird. Im Zentrum dieser Evolution steht die digitale Währung Bitcoin. Bitcoin ist die bekannteste aller digitalen Währungen und verfügt über die am besten ausgebaute Infrastruktur - es gibt keine andere digitale Währung mit mehr Akzeptanzstellen als Bitcoin. Wie jede andere technische Innovation wird auch Bitcoin kontrovers von sämtlichen Akteuren diskutiert. So haben viele nationale Regierungen, Zentralbanken und die Europäische

Union verschiedenste Positionspapiere zum Thema Bitcoin veröffentlicht. Oftmals geht es um den Vorwurf, dass Bitcoin aufgrund seiner Anonymität kriminelle Geschäfte begünstigt. Inwiefern das wirklich zutrifft werden wir in diesem Buch noch kritisch hinterfragen. Daneben geht es vor allem um die Technologie, die hinter der Währung Bitcoin steht: die sogenannte Blockchain-Technologie, auf die wir später auch noch ausführlich eingehen werden.

Neben der Politik haben natürlich vor allem Unternehmen und insbesondere Banken ein großes Interesse, die Vorteile von Bitcoin und der dahinter stehenden Technologie Blockchain für sich zu nutzen. So haben sich bereits mehrere Banken zusammengetan, um digitale Währungen zu erforschen. Zusätzlich werden die

Entwicklungen von den Universitäten vorangetrieben. An der Stanford Universität kann man beispielsweise den Studiengang "Bitcoin Engineering" belegen.

Es bleibt festzuhalten: Auch wenn das Potenzial von Bitcoin noch längst nicht ausgeschöpft ist, ist die digitale Währung bereits im Mainstream angekommen. Umso wichtiger ist es sich möglichst rechtzeitig über Bitcoin zu informieren, um die Chancen und Risiken einschätzen und nutzen zu können. Deshalb geben wir Dir mit der Bitcoin-Bibel eine Anleitung an die Hand, mit der Du lernst alle wichtigen Vorgänge und Funktionen rund um Bitcoin zu beherrschen.

Die Informationen in diesem Buch wurden mit größter Sorgfalt

erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden. Die Autoren übernehmen keine juristische Verantwortung oder irgendeine Haftung für eventuell verbliebene Fehler und deren Folgen.

KAPITEL 1 DAS BITCOIN SYSTEM

WAS IST BITCOIN

Bevor wir uns mit der technischen Dimension von Bitcoin auseinandersetzen, macht es Sinn erst einmal den Begriff Bitcoin zu erläutern. Bitcoin setzt sich aus dem Wort "Bit" - der kleinsten Maßeinheit für eine Datenmenge - und dem Wort "Coin", was im Englischen Münze bedeutet, zusammen. Entsprechend handelt es sich um digitale Münzen, die ein eigenes Währungssystem, wie Euro und US-Dollar, darstellen.

Im nächsten Schritt stellt sich die Frage, welche Eigenschaften

Bitcoin zu einer Währung machen und ihm einen Handelswert verleihen. Genau wie die von Staaten bzw. Notenbanken emittierten Währungen erfüllt auch Bitcoin alle Funktionen, die Geld per Definition erfüllen muss:

- 1) **Tauschfunktion** (z.B. Bitcoin gegen Schuhe und Schuhe gegen Bitcoin)
- 2) **Wertaufbewahrungsfunktion** (Das Versprechen, dass Bitcoin einen speicherbaren Gegenwert darstellt und sich zu einer anderen Zeit an einem anderen Ort einlösen lässt)
- 3) **Rechenfunktion** (Bitcoin ist ein Wertmaßstab und kann in Preisen ausgedrückt werden, z.B. ein paar Schuhe = 0,554 Bitcoin)

Das Erfüllen dieser Voraussetzungen erklärt allerdings noch nicht,

warum Bitcoin einen realen Tauschwert besitzt und wir sehr viele Euros oder Dollars bezahlen müssen, um im Gegenzug einen Bitcoin zu erhalten. Die Antwort ist die gleiche wie bei allen anderen staatlichen Währungen auch: Einzig und allein das Vertrauen in die Währung und die Erwartung auch zukünftig Waren oder Dienstleistungen mit der Währung erwerben zu können, lassen den Bitcoin als eine werthaltige Währung erscheinen. Angebot und Nachfrage bestimmen den Bitcoin-Marktwert.

Ganz anders gestaltet sich die Struktur und Herausgabe von Bitcoin gegenüber den klassischen Währungen. Während Euro und Co. der zentralen Kontrolle einer Notenbank unterliegen, wird die Währung Bitcoin von keiner zentralen Institution gesteuert. Auch Staaten bzw. Regierungen haben praktisch keine Möglichkeit, Einfluss auf

Bitcoin zu nehmen. Das entscheidende Merkmal von Bitcoin und der dahinterliegenden Technologie Blockchain ist die dezentrale Struktur des Systems. Durch die Blockchain, die als digitales und dezentrales Transaktionsbuch fungiert, werden alle jemals getätigten Transaktionen aus dem Bitcoin-Netzwerk aufgezeichnet. Es bedarf also keiner zentralen Server, wie bei klassischen Geldüberweisungen, um Bitcoin-Transaktionen zu ermöglichen. Der Grund dafür liegt in den sogenannten Peer-to-Peer-Anwendungen was bedeutet, dass alle Rechner gleichberechtigt ein Rechnernetzwerk darstellen. Demnach kann also auch jeder einfache Home-PC zum Teil des Bitcoin-Netzwerkes werden. Einen kompletten Zugang zu dem Netzwerk erhält man durch die Open-Source-Software Bitcoin-Core, die von den Teilnehmern genutzt

wird, um die dezentrale Datenbank zu verwalten - im weiteren Verlauf des Buches wird geschildert, warum selbst das nicht unbedingt immer notwendig ist. Staaten, Notenbanken, Geschäftsbanken oder sonstige Unternehmen sind dafür nicht nötig.

Ein weiterer, wichtiger Punkt und Unterschied zu den klassischen Währungen ist die Anonymität bzw. Pseudoanonymität von Bitcoin. Anstatt die Namen der Personen sind nur die jeweiligen Adressen, aus Zahlen und Buchstaben, einsehbar. Um Transaktionen im Bitcoin-Netzwerk durchzuführen bedarf es, im Gegensatz zum Bankenzahlungsverkehr, keiner Identitätsprüfung bzw. -offenlegung. Jederder über einen Internetzugang verfügt, kann sich eine Bitcoin-Adresse und ein Wallet (= digitale Brieftasche) zulegen, ohne dabei seine Identität preisgeben zu müssen.

Auch wenn sich das Ganze sehr unsicher und riskant anhört, sind Bitcoin-Transaktionen extrem sicher. Dafür sorgen kryptographische Techniken, die gewährleisten, dass nur der Eigentümer der Bitcoins Überweisungen vornehmen kann und die Geldeinheiten nicht mehrmals ausgegeben werden können. Aus diesem Grund wird die digitale Währung Bitcoin auch als Kryptowährung bezeichnet.

POLITISCHE DIMENSION UND REGULIERUNG

Das Potenzial struktureller Veränderungen durch Bitcoin und die Blockchain-Technologie ist aus politischer, gesellschaftlicher und ökonomischer Sicht enorm. Entsprechend kontrovers wird die Entwicklung digitaler Währungen von verschiedenen Akteuren diskutiert. Da wären zum einen die Staaten und Notenbanken, die die Geld- und Währungspolitik steuern und damit Kontrolle ausüben können. Ein dezentrales Zahlungssystem wie Bitcoin entzieht sich dieser Einflussphäre, da der Staat oder die Notenbank keine Möglichkeit hat, eine zentrale Steuerung und Überwachung des Zahlungsverkehrs vorzunehmen. Dies gilt auch für die Aufsichtsbehörden, die unter anderem für die Regulierung des

Finanzsystems zuständig sind. Insbesondere die Rolle nationaler Behörden wird ad absurdum geführt, da es keinerlei geographische Beschränkungen oder Organisation für den Bitcoin-Zahlungsraum gibt – Bitcoin funktioniert überall gleich und ist global. Zwar ist auch unser gegenwärtiges Finanzsystem global, doch es besteht die Möglichkeit, in den Zahlungsverkehr einzugreifen und Standards, wie beispielsweise mit dem SWIFT-Zahlungsverkehrssystem, zu setzen. Auch Unterschiede zwischen dem europäischen Zahlungsraum (SEPA-Überweisungen) und nicht-europäischen Zahlungsraum existieren bei Bitcoin nicht.

Gerade autoritären Staaten, die ihre Bevölkerung durch Überwachung zu kontrollieren versuchen, ist Bitcoin ein Dorn im Auge. So hat beispielsweise Russland die Bitcoin-Nutzung

untersagt und unter Strafe gestellt. Neben dem Machtverlust des Staates spielt hier auch die Stützung der eigenen Währung eine Rolle. Droht Inflation oder eine Abwertung der nationalen Währung, besteht die Gefahr, dass die Menschen ihr Geld in Bitcoin anlegen und damit die Abwertung der heimischen Währung noch weiter verstärken. Ein anderes Risiko sehen manche Staaten in der Anonymität. So besteht bei Bitcoin nicht die Möglichkeit, die Personen im Hintergrund zu identifizieren oder Konten einzufrieren. Für die Terrorismus- oder Kriminalitätsbekämpfung mag das negativ sein, für politisch Verfolgte ist es hingegen positiv.

Auch positiv ist es für diejenigen, die Angst vor einer Bargeldabschaffung haben. Vor allem in Deutschland setzen viele Menschen die Bargeldzahlung mit persönlicher Freiheit gleich.

Sollte es zukünftig zu einer Einschränkung der Bargeldnutzung kommen, haben die Menschen die Möglichkeit mit Bitcoin ein Stück ihrer Privatsphäre zurückzugewinnen.

Die Funktionsweise der Blockchain-Technologie entzieht sich der staatlichen und behördlichen Logik. Staaten, Notenbanken und Aufsichtsbehörden sind überfordert, da sie nicht wissen, wie sie ein System regulieren sollen das nicht zentral zu erfassen oder zu steuern ist. Konkrete Konzepte zur Regulierung gibt es bis dato daher noch nicht. Zwar sind bereits mehrere Positionspapiere von Regierungen und internationalen Institutionen zum Thema Digitale Währungen veröffentlicht worden, doch blieben diese ohne konkrete Handlungsanweisungen bezüglich der Regulierung.

Folglich sind Bitcoin und Co. nach wie vor (gilt zumindest für Deutschland) von der Kapitalertragssteuer befreit, da die Banken oder Broker-Plattformen keine Möglichkeit haben, Veräußerungsgewinne direkt an den Staat abzuführen. Gewinne aus Bitcoin-Veräußerungsgeschäften werden daher als Spekulationsgeschäfte nach dem Einkommensteuergesetz (§ 23 Abs. 1 Nr. 2) eingestuft. Demnach sind Veräußerungsgewinne nach einer Haltefrist von einem Jahr komplett steuerfrei. Fällt innerhalb der einjährigen Haltefrist ein Veräußerungsgewinn an, greift eine Freigrenze von 600 Euro p.a. - allerdings gilt diese nur für Privatpersonen.

Eine effektive Regulierung und steuerliche Behandlung wäre aber nur denkbar, wenn die Anonymität hinter der Bitcoin-Adresse

aufgelöst werden könnte. Wie eine solche Offenlegung der Identität, technisch wie juristisch, umzusetzen wäre, ist zurzeit noch vollkommen unklar. Die Institutionalisierung juristischer Rahmenbedingungen stößt bei den digitalen Währungen an ihre Grenzen. Es bleibt daher spannend zu sehen mit welchen Lösungen Staaten und Institutionen versuchen werden , digitale Währungen zu regulieren.

Dabei ist anzumerken, dass nicht alle Staaten Bitcoin und Blockchain skeptisch gegenüberstehen. Vor allem im angelsächsischen Raum werden die Vorteile und Chancen der neuen Technologie hervorgehoben. Das Interesse liegt dabei weniger bei den digitalen Währungen, sondern vielmehr bei der dahinterliegenden Technologie, der Blockchain. Schließlich gibt es

neben dem Zahlungsverkehr und der Wertaufbewahrung auch noch andere Möglichkeiten, die Blockchain zu nutzen. In der Blockchain steckt beispielsweise das Potenzial, viele Verwaltungsvorgänge im Sinne eines digitalen, sicheren und transparenten Registers zu optimieren. Auf diese und weitere Nutzungsmöglichkeiten der Blockchain wird aber noch ausführlich in Kapitel 4 (Die Blockchain) eingegangen.

Ähnlich sieht es bei den Banken aus. Auch hier herrscht eine Mischung aus Skepsis und Optimismus. Viele Großbanken und Finanzunternehmen haben sich daher zu einem Konsortium zusammengeschlossen, um gemeinsam das Potenzial der Blockchain und der digitalen Währungen zu erforschen.

DAS BITCOIN-WHITEPAPER

Das Bitcoin-Whitepaper wurde am 31. Oktober 2008 von Satoshi Nakamoto, dem Pseudonym für den Erfinder von Bitcoin, erstmals durch das kryptografische Mailingsystem metzdowd.com veröffentlicht.

In dem Whitepaper stellt Nakamoto erstmals Bitcoin offiziell der Öffentlichkeit vor und beschreibt, was Bitcoin ist, wie die digitale Währung funktioniert und offenbart das Geheimnis, das die digitale Währung vor dem „Double-Spending“ bewahrt. Unter Double-Spending versteht man die doppelte Ausgabe von Bitcoin, die einem jeden Nutzer erlauben würde eine Bitcoin Transaktion zu kopieren, was das Aus für eine jede Währung bedeutet.

ZUSAMMENFASSUNG DES WHITEPAPERS

Eine digitale Währung, die alleinig auf einer Peer-to-Peer-Version beruht, könnte von einer Instanz zur anderen geschickt werden, ohne eine Interaktion von Dritten wie z.B. Finanzinstitutionen.

Digitale Signaturen sind ein Teil der Lösung, aber der größte Vorteil liegt darin, dass keine dritte, vertrauenswürdige Instanz interagieren muss, um dem Problem des Double-Spendings vorzubeugen. Das System beruht alleinig auf einem direkten Peer-to-Peer-System. Das Netzwerk vergibt jeder Transaktion einen einmaligen Zeitstempel und damit einen Platz in einer niemals endenden Blockchain, die auf Hash-basierten Proof-of-Work

basiert. Dieser Eintrag in die Blockchain kann nicht mehr ohne einen erneuten Leistungsnachweis geändert werden. Die längste Kette dient nicht nur als Beweis für die Abfolge der Ereignisse, sondern auch als Beweis dafür, dass sie aus dem größten Pool mit der größten Rechenkapazität entstammt.

Solange der größte Anteil der Rechenkapazität von individuellen Nodes (engl.: Knotenpunkte) zur Verfügung gestellt wird, stellen sie die längste Kette und sichern das Netzwerk vor Angriffen von Hackern ab (Stichwort: 51%-Attacke, Kapitel 5). Das Netzwerk selbst benötigt nur eine minimale Struktur. Nodes (Bitcoin Core Client) können das Netzwerk nach Belieben verlassen und ihm wieder beitreten. Bei einem Wiedereintritt wird automatisch die längste Kette erneut heruntergeladen und die Node erhält den

aktuellsten Leistungsnachweis (Proof-of-Work) und damit einen neuen Platz im Netzwerk.

WER HAT BITCOIN ERFUNDEN?

Wer oder was Bitcoin und die Technologie dahinter erfunden hat, ist bis heute unklar. Keiner weiß, ob es sich bei dem Erfinder von Bitcoin um eine Person, mehrere Personen, eine Institution oder gar einen Staat handelt. Eines ist jedoch klar: Der Erfinder von Bitcoin nannte sich in dem Bitcoin-Whitepaper selbst Satoshi Nakamoto. Seit Auftauchen des Whitepapers gab es bereits viele Vermutungen, wer Satoshi Nakamoto sein könnte.

SATOSHI NAKAMOTO

Auch wenn wir nicht wissen wer sie oder wer er ist, so wissen wir, was er erschaffen hat: Er ist der Erfinder des Bitcoin-Protokolls, welches er in einem Whitepaper im November 2008 über eine

verschlüsselte E-Mail-Adresse veröffentlicht hat.

Im Jahr 2009 veröffentlichte er den ersten Bitcoin-Client und kommunizierte fortan bis Ende 2010 mit der Bitcoin-Community. Danach verschwand er spurlos von der Bildfläche.

Anfangs arbeitete er mit einem Open-Source Team zusammen an dem Projekt und legte immer sehr viel Wert darauf, keine persönlichen Daten bekannt zu geben. Zuletzt hörte man im Frühjahr 2011 von ihm als er sagte:

„Ich werde mich fortan anderen Dingen widmen.“

WAR ER JAPANER?

Man sollte ein Buch nicht anhand seines Titels beurteilen, oder etwa

doch?

„Satoshi“ bedeutet „klar denkend“; „Naka“ könnte „innen oder Beziehung“ bedeuten; „Moto“ bedeutet „Herkunft oder Gründung“.

All diese Dinge passen auf die Person, die eine Bewegung ins Leben gerufen und einen ausgeklügelten Algorithmus erschaffen hat. Das Problem ist nur, dass jedes einzelne Wort mehrere Bedeutungen haben kann.

Wir können also nicht sicher sagen, ob Satoshi Nakamoto ein Japaner ist. Es lässt lediglich vermuten, dass Satoshi ein „Er“ ist.

Der Einfachheit halber werden wir Satoshi Nakamoto als „Ihn“ bezeichnen, auch wenn er eine Sie, ein etwas oder mehrere Personen gewesen sein kann.

WEISS IRGENDJEMAND WER SATOSHI NAKAMOTO WAR?

Nein, aber die Kriminaltechniken die Menschen heutzutage nutzen, werfen oftmals mehr Fragen als Antworten auf. Der New Yorker Joshua Davis glaubt Satoshi Nakamoto sei ein Kryptographie-Student des Dublin Trinity College namens **Michael Clear**.

Zu seiner Schlussfolgerung kam er durch eine Analyse aller Nakamoto-Schreiben, die mehr als 80.000 Wörter beinhalteten. Hier suchte er nach sprachlichen Hinweisen. Er verdächtigte aber auch den finnischen Wirtschafts-Soziologen und ehemaligen Spieleentwickler **Vili Lehdonvirta**.

Beide haben gesagt sie seien nicht die Erfinder von Bitcoin. In

einem Web Summit 2013 teilte Michael Clear sogar öffentlich mit, er sei nicht Satoshi Nakamoto.

Adam Penenberg von FastCompany bestritt die Vermutung und sagte, Satoshi Nakamoto sei ein Zusammenschluss von drei Personen: **Neal King**, **Vladimir Oksman**, und **Charles Bry**. Dies fand er heraus, indem er verschiedene Sätze aus dem veröffentlichten Whitepaper bei Google eingab um zu sehen, ob diese Wortphrasen bereits zuvor irgendwo aufzufinden waren.

Es stellte sich später heraus, dass einer der drei namentlich in einer Patentanmeldung zur Aktualisierung und Verteilung von kryptischen Schlüsseln genannt war. Die *Bitcoin.org* Domain, die Satoshi Nakamoto zur Veröffentlichung des Whitepapers genutzt

hatte, wurde nur 3 Tage nach der Patentanmeldung registriert und gesichert.

Registriert wurde die Domain in Finnland und einer der Patent-Antragsteller reiste 6 Monate zuvor in das Land. Alle drei „Verdächtigten“ bestreiten bis heute Satoshi Nakamoto zu sein.

Auf jeden Fall wurde die Bitcoin.org-Domain am 18. August 2008 durch einen anonymen japanischen Service-Anbieter und einem japanischen ISP registriert. Danach soll die Domain lediglich nach Finnland übertragen worden sein. Dies entkräftet die Finnland-Theorie ein wenig.

Wiederum andere Zungen behaupten, der Erfinder von Bitcoin könnte auch **Martii Malmi** sein. Martii lebt in Finnland und ist seit

der Geburtsstunde von Bitcoin an der Entwicklung beteiligt.

Auch **Jed McCaleb** zählt zum Kreis der Auserwählten. Er ist ein Liebhaber der japanischen Kultur und wohnt in Japan. Er ist Gründer der umstrittenen Bitcoin-Börse Mt Gox und Mitgründer der dezentralisierten Zahlungssysteme Ripple und Stellar.

Der wohl jüngste „Verdächtige“ ist der australische Geschäftsmann **Craig Wright**. Erstmals machte ein Gerücht im Dezember 2015 die Runde, dass Wright der wahre Satoshi Nakamoto sei. Kurz darauf tauchte jedoch eine E-Mail mit dem Absender *satoshi@vistomail.com* auf, welche weitestgehend Satoshi zugeschrieben wird.

In der Nachricht stand geschrieben: „Ich bin nicht Craig Wright.

Wir sind alle Satoshi.“ Damals basierten die Vermutungen auf unabhängige Aussagen des Wired und Gizmodo Magazins. Beide Journalisten der Magazine beriefen sich dabei auf E-Mails, kryptische Blogbeiträge und Memos von Wright und seinen Geschäftspartnern sowie seinen Anwälten.

Im Mai 2016 aber trat Wright von selbst vor die Öffentlichkeit und sagte der BBC, GQ und gegenüber dem Economist, dass er der Erfinder von Bitcoin sei. Beweisen wollte der Geschäftsmann seine Identität als Satoshi Nakamoto durch den Schlüssel des neunten Bitcoin-Blocks. Von diesem Block hat Satoshi Nakamoto einst Bitcoin an den Entwickler Hal Finnen überwiesen. Dieser bestätigte die Transaktion einen Tag vor seinem Tod. Der gelieferte Schlüssel entpuppte sich später jedoch als eine viel jüngere Transaktion. Kurz

darauf versprach Wright einen neuen Beweis zu liefern – er wollte einige der ersten Bitcoins in einem sehr, sehr alten Wallet kontrollieren und damit seine Behauptungen beweisen. Aber auch dieser Beweis blieb aus. Craig Wrights letzten Worte dazu waren:

“Ich dachte wirklich, dass ich das tun könnte. Ich dachte, ich könnte die Jahre der Anonymität und des Versteckens hinter mir lassen. Aber wie sich die Dinge diese Woche entwickelten, als ich meinen Beweis vorbereitete und zeigen wollte, dass ich die ältesten privaten Schlüssel kontrolliere, brach ich mental zusammen. Ich habe nicht den Mut dazu. Ich kann das nicht tun.”

Es gibt eine Vielzahl von weiteren potentiellen Satoshi Nakamotos,

darunter **Donal O'Mahony**, **Michael Peirce**, **Professor Shinichi Mochizuki** und **Dorian S Nakamoto**. Alle bestreiten die Erfinder einer genialen Erfindung zu sein. In der Bitcoin-Community herrscht also weiterhin Ungewissheit über die Identität von Satoshi Nakamoto.

WAS WISSEN WIR ÜBER IHN?

Eines wissen wir: Basierend auf Interviews mit Weggefährten von Satoshi Nakamoto in den frühen Geburtsstunden von Bitcoin soll er das System penibel genau durchdacht haben. Seine Kodierungen trugen laut Jeff Garzik nicht die Handschrift eines konventionellen Software-Ingenieurs.

WIE REICH IST ER?

Einer Analyse des Bitcoiners Sergio Lerner zufolge, soll Satoshi Nakamoto viele der ersten Blocks im Bitcoin Netzwerk geschürft haben: Rund 1 Millionen Bitcoins.

WAS MACHT ER JETZT?

Das weiß niemand. Aber aus seiner letzten E-Mail vom 23. April 2011 geht hervor:

„Ich werde mich jetzt anderen Dingen widmen. Es ist alles in guten Händen bei Gavin & Co.“

STEUERN UND RECHT

BITCOIN UND RECHT

Einhergehend mit der steigenden Präsenz des Bitcoin in den Medien wird klar, dass jeder, der mit Bitcoins zu tun hat, gewisse Risiken eingeht. Gerade die Verbreitung von Bitcoins als Spekulations- und Zahlungsmittel, ob privat oder im Unternehmen, im In- oder Ausland, kann ungeahnte Hürden mit sich bringen. Sei man nun privater, passiver Nutzer oder aktiver Finanzdienstleister im „Bitcoin-Geschäft“, das Bitcoin-Recht ist für sie von besonderer Bedeutung. Die rechtlichen und steuerlichen Risiken sind wichtig, teilweise jedoch nicht hinreichend aufgreifbar – denn zwar bestehen für einige erste Fragen rund um die Themen Bitcoin, Recht und

Steuern (Bitcoin-Besteuerung) bereits Antworten, andere Bitcoin-Rechtsfragen sind aber noch immer völlig ungeklärt.

Der Bitcoin-Markt unterliegt einer enormen Dynamik. Von daher ist es wenig verwunderlich, dass Politik, Gesellschaft und Staat der tatsächlichen Entwicklung hinterherlaufen. Der digitalen Welt wird erst langsam und stückweise der nötige rechtliche Rahmen gegeben. Diese Schritte sind von hoher Wichtigkeit: Denn nur wenn für alle Beteiligten im Umgang mit Bitcoin & Co. ausreichend Rechtssicherheit besteht, werden sich digitale Währungen langfristig durchsetzen können. Erst dann können Bitcoins durch schnelle und unkomplizierte Bezahlung von Waren und Dienstleistungen den Alltag vollends erleichtern. Dies war schließlich die ursprüngliche Idee hinter der Erfindung der digitalen

Währung.

RECHTLICHE UND STEUERLICHE PROBLEME

Spätestens seit der Schließung der in Deutschland betriebenen Plattform „Bitcoin24“ ist bekannt, dass der Umgang mit Bitcoins Risiken aufweist. Unter dem Vorwurf der Geldwäsche musste der Händler und Verwahrer von Bitcoins seinen Geschäftsbetrieb einstellen. Es wurden Haftbefehle ausgestellt, Server beschlagnahmt und zusätzlich versuchten viele Geschädigte vergebens, an ihr Geld zu kommen oder ihre Bitcoins einzulösen.

Es liegt damit auf der Hand, dass tatsächlich Risiken beim Umtauschen von Bitcoins und ihrem Einsatz gegenwärtig sind. Die zahlreichen rechtlichen und [steuerlichen Fragen](#), die mit Bitcoins

einhergehen, sind damit aber noch nicht gelöst: Sind Bitcoins überhaupt eine Sache im Sinne des BGB? Was genau sind Bitcoins im steuerlichen Sinn? Welche vertraglichen Beziehungen und Ansprüche bestehen unter den Beteiligten? Es geht etwas schief – wie ist es mit der Haftung? Welche Rechte hat ein Bitcoin-Besitzer und welche Pflichten ein Händler oder ein [Betreiber einer Bitcoin-Plattform](#)?

Die staatliche Schließung eines Bitcoin-Handelsunternehmens hat aber, neben diesen steuerlichen und zivilrechtlichen Fragen, noch etwas anderes aufgezeigt: Anbietern, Plattformbetreibern und Händlern von Bitcoins muss mittlerweile klar sein: Bitcoin ist kein rechtsfreier Raum ist. Die staatliche Aufsicht, vor allem die Bankenaufsicht, mag dies bekräftigen. In vielen Fällen bedürfen

Bitcoin-Unternehmen tatsächlich einer [Erlaubnis der BaFin](#) (Bundesanstalt für Finanzdienstleistungsaufsicht). Und auch Vorschriften zur Vermeidung von Geldwäsche, sowie Pflichten zur Identifizierung der Nutzer spielen beim gewerblichen Umgang mit Bitcoin eine Rolle.

Dadurch sind zahlreiche regulatorische Anforderungen von Anbietern und Vermittlern von Bitcoins zu erfüllen. Unter anderem zählen dazu das Haftungskapital und der Nachweis der Sachkund. Die Risiken zur Lagerung und des Eintaushes muss nicht zuletzt auch noch von Bitcoin-Händlern und –Akzeptierenden einkalkuliert werden.

ERST RECHTLICHE PLANUNG, DANN START DES

UNTERNEHMENS

Wer geschäftlich mit Bitcoins zu tun hat oder haben will, dem ist vor allem eines zu raten: Man sollte sich über die Entwicklungen im Bitcoin-Recht auf einem aktuellen Stand befinden und sicherstellen, dass man über ein ausreichendes Know-How verfügt. Erst dann sollte ein regelmäßiges Geschäft mit Bitcoins aufgenommen werden.

Wir empfehlen hier die Kanzlei WINHELLER, welche sich u.a. auf rechtliche und steuerliche Fragen in Sachen Bitcoin & Blockchain spezialisiert hat.

WINHELLER ist bietet nicht nur im klassischen [Bank- und Kapitalmarktrecht](#) kompetente Ansprechpartner. WINHELLER

beobachtet den Markt der digitalen Währungen schon lange und sehr genau. Sie beraten und vertreten zahlreiche Unternehmen auf diesem Gebiet (vgl. z.B. unter anderem das "[Haftungsdach](#)" des Betreibers Bitcoin Deutschland AG). Sowohl vorausschauend als auch im Streitfall beraten WINHELLERs Bitcoin Rechtsanwälte und Steuerberater in Bezug auf Vertragsgestaltungen zwischen den Anbietern von Bitcoins bei sämtlichen steuerrechtlichen Fragestellungen. Die Anwälte der Kanzlei erstellen AGB für Bitcoin-Unternehmen und vertreten euch gegenüber den Aufsichtsbehörden in allen aufsichtsrechtlichen Fragen. Da die WINHELLER Bitcoin Anwälte in regelmäßigem Kontakt zu den Aufsichtsorganen stehen, in besonderem Maße auch zur BaFin, ist die Kanzlei stets auf dem aktuellen Stand der Bitcoin-

Regulierungspraxis.

Entsprechende Kontaktdaten zu den WINHELLER Anwälten findet ihr am Ende des Kapitels.

BITCOIN UND STEUER

„Bitcoin ist weder Geld noch E-Geld“

Anders als der Euro sind Bitcoin und andere kryptographische Währungen kein gesetzliches Zahlungsmittel. Es besteht daher keine gesetzliche Verpflichtung zur Annahme von Bitcoins. Ob ein Verkäufer von Waren oder Dienstleistungen Bitcoins akzeptieren will, ist vielmehr eine rein privatrechtliche Frage, die der Verkäufer für sich allein beantworten kann und muss. Bitcoin kann auch nicht als „E-Geld“ klassifiziert werden, da es beim Minen von Bitcoins,

im Gegensatz zur Emission bei Unternehmen, an einem Emittenten fehlt. Zuletzt wurde dies von der BaFin am 19.12.2013 eindeutig [klargestellt](#).

Zumindest im Ertragssteuerrecht hat die steuerliche Behandlung von Bitcoin zur Folge, dass diese als gewöhnliche immaterielle Wirtschaftsgüter zu behandeln sind. Weiterhin sind die konkreten steuerlichen Folgen von Bitcoin-Geschäften davon abhängig, ob die Geschäfte im privaten Bereich oder in der betrieblichen Sphäre abgewickelt werden.

BITCOIN UND STEUER FÜR PRIVATANLEGER

Für den Privatanleger von Bitcoins ist im Wesentlichen die Frage relevant, wie deren Veräußerung besteuert wird. Ein simples

Beispiel einer Veräußerung ist der Verkauf von Bitcoins gegen Euro über eine Handelsplattform. Beahlt ein Bitcoin-Inhaber jedoch für den Erwerb von Waren oder Dienstleistungen mit Bitcoin, stellt dies aber auch einen Veräußerungstatbestand von Bitcoins als Zahlungsmittel dar.

Im Sinne des § 23 Abs. 1 Nr. 2 des Einkommensteuergesetzes (EStG), liegen in beiden Fällen private Veräußerungsgeschäfte vor, welche auch unter der Bezeichnung „Spekulationsgeschäfte“ bekannt sind. Die Einstufung als Spekulationsobjekt führt steuerlich dazu, dass Veräußerungsgewinne nach einer Haltefrist von mindestens einem Jahr komplett steuerfrei sind. Wird ein Veräußerungsgeschäft innerhalb der einjährigen Haltefrist abgewickelt, greift zumindest noch eine Freigrenze von 600 Euro

per annum. Die Freigrenze bezieht sich also nur auf Bitcoin-Geschäfte des Steuerpflichtigen, sondern gilt für alle privaten Veräußerungsgeschäfte im betreffenden Jahr.

Der Veräußerungsgewinn, der zu besteuern ist, ergibt sich aus der Differenz zwischen dem erzielten Veräußerungspreis und den Anschaffungskosten bzw. Werbungskosten der eingesetzten Bitcoins (z.B. Kaufpreis der früher erworbenen Bitcoins oder Kosten für das Schürfen der Bitcoins).

Entsprechend können Verluste gegengerechnet werden und auch sowohl zurück- als auch in künftige Jahre vorgetragen werden. So können sie mit Gewinnen aus privaten Veräußerungsgeschäften verrechnet werden. Da die eingesetzten Bitcoins zu sehr

unterschiedlichen Zeitpunkten zu unterschiedlichen Kursen / Anschaffungskosten erworben wurden, ergibt sich häufig das Problem die Anschaffungskosten genau zu ermitteln. Die sog. First-in-first-out-Methode (Fifo) mag in diesen Fällen dazu geeignet sein, die Anschaffungskosten zuverlässig zu ermitteln (vgl. zu Fremdwährungsgeschäften LfSt Bayern v. 12.3.2013, S 2256.1.1-6/4 St32). Mit anderen Worten: Man nimmt an, dass die Bitcoins, die zuerst angeschafft / geschürft wurden, auch diejenigen sind, die im Rahmen des privaten Veräußerungsgeschäfts als erstes eingesetzt wurden.

Um ihrem [Finanzamt](#) im Zweifel geeignete Nachweise über die getätigten Transaktionen vorlegen zu können, sollten Anleger ihre Bitcoin-Geschäfte allerdings sorgfältig dokumentieren, denn die

Fifo-Methode ist mit Einführung der Abgeltungssteuer nicht mehr ausdrücklich gesetzlich geregelt. Der gewöhnliche individuelle Einkommensteuersatz wird hier als Steuersatz zugrunde gelegt. Die Abgeltungssteuer hat insoweit also keine Bedeutung.

BITCOIN UND STEUER FÜR UNTERNEHMEN

Im Gegensatz zu Privatanlegern können gewerblich tätige Unternehmen keine privaten Veräußerungsgeschäfte tätigen. Geschäfte mit Bitcoins, die sich im Betriebsvermögen befinden, führen stattdessen in aller Regel zu Einkünften aus Gewerbebetrieb gemäß § 15 EStG. Es gibt also keine Mindesthaltedauer, nach deren Ablauf Steuerfreiheit eintritt. Zusätzlich zur Gewerbesteuer unterliegen die erzielten Gewinne des Unternehmens, je nach

Rechtsform, dann der Einkommensteuer (Personengesellschaften) oder der Körperschaftsteuer (GmbHs, AGs etc.).

Neben den ertragsteuerlichen Auswirkungen von Bitcoin-Geschäften, ist für Unternehmer vor allem aber auch deren umsatzsteuerliche Behandlung besonderem Interesse. Die Finanzbehörden behandeln den späteren Verkauf von Bitcoins über eine Handelsplattform jedoch regelmäßig als gewöhnliche umsatzsteuerbare Lieferung. Eine ärgerliche Praktik für Unternehmen, die Bitcoin als Zahlungsmittel akzeptieren. Ob dieser Umgang korrekt ist, bleibt aber fraglich: Nach einem Urteil des EuGH ist nämlich der reine An- und Verkauf von Wertpapieren in einem Unternehmen schon gar keine unternehmerische Tätigkeit und damit nicht steuerbar. Geschäfte mit Bitcoins könnte man

hiermit vergleichen.

Das Bundesfinanzministerium hat sich auch zu Steuerbefreiungstatbeständen im Zusammenhang mit Bitcoin-Geschäften bereits geäußert: Da es sich bei Bitcoin nicht um ein gesetzliches Zahlungsmittel handelt, ist der Handel von Bitcoin und die Vermittlung von Bitcoin-Umsätzen danach nicht etwa gemäß § 4 Nr. 8 Buchst. b UStG von der Umsatzsteuer befreit. Jedenfalls nach Meinung des Bundesfinanzministeriums mag sich jedoch im Einzelfall eine Steuerbefreiung aus § 4 Nr. 8 Buchst. c UStG ergeben. Letztere Vorschrift befreit Umsätze „im Geschäft mit Forderungen“ sowie die Vermittlung dieser Umsätze.

Nach einer Äußerung des Bundesfinanzministeriums, sollen

Transaktionen anders als der Verkauf von Bitcoins, von der Umsatzsteuer nicht berührt werden. Sie dienen lediglich der bloßen Entgeltentrichtung und können als Zahlungsmittel (also z.B. für den Erwerb von Dienstleistungen oder Waren) nicht gemäß § 1 Abs. 1 UStG steuerbar sein. Diese Aussage überrascht auf den ersten Blick, wenn man davon ausgeht, dass Bitcoins gewöhnliche Wirtschaftsgüter und gerade kein Geld sind. Beim „Bezahlvorgang“ werden Bitcoins gegen andere Waren und Dienstleistungen eingetauscht und löst damit üblicherweise Umsatzsteuer auf beiden Seiten aus. In vielen Fällen folgt das Umsatzsteuerrecht allerdings nicht streng dem Ertragsteuerrecht. Es dürfte daher korrekt sein, Bitcoins zumindest als „Entgelt“ im umsatzsteuerlichen Sinne zu behandeln. Denn in der Tat verfolgt der Unternehmer, der Bitcoins

als Zahlungsmittel einsetzt, keine über die reine Entgeltentrichtung hinausgehenden wirtschaftlichen Interessen. In einem solchen Fall fällt keine Umsatzsteuer an, wie der BFH schon 1969 entschieden hatte.

Wenn die ersten finanzgerichtlichen Urteile vorliegen, mag erst wirkliche Klarheit vorliegen. Die umsatzsteuerliche Behandlung von Bitcoin-Geschäften ist bis dahin bislang nur zum Teil zufriedenstellend geklärt.

FRÜHZEITIGE BERATUNG SINNVOLL

Gerade weil der falsche Umgang mit diesem Thema schnell den Vorwurf der leichtfertigen Steuerverkürzung oder der gar vorsätzlichen Steuerhinterziehung im Raum stehen lässt, raten wir

insbesondere Unternehmen, die durch die Annahme von Bitcoins als Zahlungsmittel eine Vorreiterrolle einnehmen, sich rechtzeitig fachkundig informieren zu lassen. Denn spätestens nach den jetzt veröffentlichten Stellungnahmen des BMF kann und muss jeder Unternehmer wissen, dass eine Umsatzbesteuerung von Bitcoin in Betracht kommt. Es kann jedoch andererseits auch nicht die Patentlösung sein, aus „vorausseilendem Gehorsam“ vorsorglich Umsatzsteuer auf alle Bitcoin-Aktivitäten auszuweisen und abzuführen. Die richtige Strategie hängt vielmehr von vielen Faktoren wie Art, Größe und dem Geschäftszweig des Unternehmens ab.

Die Kanzlei WINHELLER gibt euch gerne die nötige Hilfestellung, wenn ihr Fragen zu diesem Thema habt. Als Full-Service-Kanzlei

bietet WINHELLER dabei nicht nur die rechtliche Vertretung, sondern auch das gesamte Spektrum der Steuerberatung an. Besonders die laufende Finanzbuchhaltung kann bei Bitcoin-Unternehmen anspruchsvoll und aufwändig sein.



WINHELLR, der richtige Ansprechpartner für rechtliche und steuerliche Bitcoin Angelegenheiten

Webseite: www.winheller.com/

Bitcoin und Steuern:

Rechtsanwältin Anka Hakert

E-Mail: info@winheller.com

Telefon: (069 / 76 75 77 80)

Bitcoin, BaFin und FinTech

Rechtsanwalt Lutz Auffenberg

E-Mail: info@winheller.com

Telefon: (069 / 76 75 77 80)

Finanzdienstleister und Banken

Rechtsanwalt Eike Weerda

E-Mail: info@winheller.com

Telefon: (069 / 76 75 77 80)

KAPITEL 2

WELCHEN WERT

HABEN BITCOINS?

Um diese Frage beantworten zu können, müssen wir zunächst einmal den Begriff „Wert“ definieren.

Wie erhält eine Ware, ein Rohstoff/Edelmetalle oder eine Währung einen Wert? Oder anders gesagt, wie erhalten diese drei Wirtschaftsgüter die Wichtigkeit für die Befriedigung der subjektiven Bedürfnisse?

Waren oder Produkte erhalten durch die für die Herstellung aufgebrauchten Ressourcen und durch das Marktgleichgewicht

(Angebot und Nachfrage) einen Wert.

Genauso sieht es bei den **Edelmetallen oder Rohstoffen** aus. Auch hier bestimmen, wie beim Gold, Angebot und Nachfrage den Wert. Gold gefällt nicht nur wegen seines Glanzes. Gold ist vor allem leicht zu bearbeiten und, noch wichtiger, es trotzt den meisten chemischen Einflüssen. Dieser „bleibende Wert“ des Goldes ist bis heute das wichtigste Verkaufsargument – nicht nur, wenn es um Geldanlage geht, sondern auch im Geschäft mit Schmuck und Münzen, den klassischen Goldprodukten. Außerdem ist Gold über alle Grenzen hinweg beweglich.

Fiat-Währungen wie **Euro, Dollar oder Yuan** haben im Gegensatz zum Gold keinen physischen Wert. Der Wert der Währung wird

durch die Sicherheiten der Regierungen gegeben und setzt sich aus dem Verhältnis von umlaufender Geldmenge zum aktuellen Warenangebot zusammen. Den Wert eines Euro, ausgedrückt in der Stückzahl Bananen einer bestimmten Qualitätsklasse, ermittelt man durch Versuchskäufe bei Gemüsehändlern und Berechnung des Durchschnittspreises. Den Wert eines Euro in Dollar oder Pfund erfährt man bei der Wechselstube. Wenn dort die Kunden immer mehr Euro in Dollar wechseln wollen, merkt der Geldwechsler, dass er seinen Wechselkurs dem veränderten Verhältnis von Angebot und Nachfrage anpassen muss, genauso wie der Gemüsehändler auch.

Der physische Wert eines **Bitcoin** liegt bei genau 0,00 EUR, 0,00 USD oder 0,00 Yuan. Wie aber kam Bitcoin zu den

rekordverdächtigen Preisen von über 1.240 US-Dollar und überstieg damit sogar den Goldpreis?

Zunächst einmal ist und war in den enormen Kursausbrüchen ein großer Spekulationsanteil enthalten. Viele Menschen haben von Bitcoin gehört, haben das enorme Wachstum gesehen und investierten. Zu den Bestzeiten im Jahr 2013 erreichte Bitcoin ein Marktvolumen von mehr als 11 Mrd. US-Dollar. Viele Menschen werden in die digitale Währung investiert haben, ohne überhaupt zu wissen was für eine durchdachte Technologie dahinter steckt. Bitcoin ist nämlich auf **21 Mio. Coins** limitiert und die Schwierigkeit zum berechnen (auch schürfen oder minen genannt) steigt mit zunehmend verfügbaren Rechenkapazitäten.

ANGEBOT

Das Errechnen von Bitcoins wird immer schwieriger und verlangt zunehmend mehr Rechenleistung. Wenn man vor einigen Jahren noch mit dem heimischen Computer mehrere Bitcoins pro Tag errechnen konnte, würde der gleiche Prozess heutzutage mehrere Jahre, wenn nicht Jahrzehnte dauern.



Abbildung1: Verlauf der Bitcoin-Mining Schwierigkeit (Quelle: Blockchain.info)

Halten wir also einmal fest: Bitcoin ist auf 21 Mio. Coins limitiert und die Schwierigkeit steigt mit Zunahme der Rechenkapazität, die erforderlich ist um neue Coins zu schürfen.

Als Resultat daraus steigt der Wert pro Bitcoin aufgrund der limitierten Verfügbarkeit und der steigenden Nachfrage mit wachsender Bekanntheit. Hinzu kommt, dass im Code von Bitcoin ein sogenanntes Block-Halving codiert ist. D.h: alle 210.000 Blocks oder ca. alle 4 Jahre erhalten die Miner nur noch die Hälfte an Bitcoins als Entlohnung für ihre Mining-Arbeit. Bis 2012 erhielten die Miner 50 BTC pro Block, nach dem 28. November 2012 waren das nur noch 25. Ab Juli 2016, also weitere 210.000 Blocks später sind das nur 12,5 BTC pro Block. Die Schwierigkeit wird also

immer größer und der Reward, ausgedrückt in Stückzahl, immer niedriger. Damit die Miner weiterhin die gleiche Anzahl Bitcoins generieren können, müssen sie zwangsläufig in neue Hardware und steigenden Stromkosten investieren. Wenn die Nachfrage also bleibt, muss der Wert zwangsläufig weiter steigen.

NACHFRAGE

Soviel zum knappen Angebot. Wie entsteht aber die Nachfrage nach einer Währung, die nur aus digitalen Schlüsseln besteht?

Hier kommen die einzigartigen Vorteile von Bitcoin als digitale Währung ins Spiel. Denn neben der spekulativen Beliebtheit von Bitcoin, sind die Vorteile von Bitcoin als Währung der Schlüssel für die bestehende und allmählich wachsende Nachfrage.

Nicht nur die Verbraucher erfreuen sich an der digitalen Währung – auch Großbanken, internationale Konzerne und Institutionen sind auf die digitale Währung gekommen und schätzen ihre Vorteile:

Kosten

Eine Bitcoin Transaktion kostet derzeit 31 Satoshi, also weniger als 0,01 US-Dollar. Eine Bank kann schon mal leicht 15 Euro für einen internationalen Geld-Transfer verlangen.

Schnelligkeit

Bitcoin kann überall hin versendet werden und es dauert nur wenige Minuten bis das Netzwerk die Zahlung bestätigt. Anders als beispielsweise Gold kann Bitcoin problemlos über das Internet

transferiert werden.

Verfügbarkeit

Konventionelle Banken machen es einem oft schwer ein Konto oder ein Geschäftskonto zu eröffnen, was oftmals mit vielen bürokratischen Hürden verbunden ist. Im Kontrast dazu kann jeder ein Bitcoin-Konto (Wallet) eröffnen.

Sicherheit

Bitcoin selbst ist extrem sicher und eignet sich daher nicht nur als Währung, sondern auch als Anlagegut. Der Grund für die in der Vergangenheit durch diverse Hackerangriffe gestohlenen Bitcoin beruht nicht auf der Sicherheit von Bitcoin, sondern auf den nicht

ausreichend geschützten Bitcoin-Börsen.

Anonymität

Nutzer können mehrere Bitcoin-Konten (Wallets) besitzen und diesen sind keinen Namen, Adressen oder anderen persönlichen Informationen zugeordnet.

Transparenz

Das Netzwerk speichert jede, wirklich jede einzelne Transaktion in einem riesigen Register, der Blockchain. Die Blockchain weiß alles. Wenn jemand eine öffentliche Bitcoin-Adresse besitzt, kann jeder einsehen, wie viele Bitcoin sich auf diesem Konto befinden. Sie wissen lediglich nicht wem diese Adresse gehört. Viele Nutzer

benutzen dennoch wechselnde Adressen und transferieren nur Teile von Bitcoin an eine Adresse, wodurch der Grad der Anonymität erhöht wird.

WERTENTWICKLUNG

Bitcoin erfreut sich seit der Veröffentlichung einer konstanten Preissteigerung – sollte man meinen.

In Wirklichkeit hatte ein Bitcoin mit Veröffentlichung der Technologie einen Wert von 0,00 US-Dollar.

2009

Mit Gründung der ersten Bitcoin-Börse (New Liberty Standard) am **5. Oktober 2009** erhält Bitcoin erstmals einen Wert. Der Wert wurde anhand der Stromkosten berechnet, die benötigt wurden um 1 Bitcoin zu generieren – 0,00076 USD oder $1 \text{ USD} = 1.309,03 \text{ BTC}$. Damals lag die Schwierigkeit zum Berechnen (Minen) von Bitcoin

bei 1,00.

2010

Anfangskurs: 0,00076 USD

Endkurs: 0,30 USD

Jahreshoch: 0,30 USD

19. Juli: Bitcoin bekommt erstmals einen wirklich messbaren Gegenwert – 1 BTC = 0,07 US-Dollar.

31. Dezember: Am Ende des Jahres lag der Wert für ein Bitcoin bereits bei 0,30 US-Dollar. Bitcoin erreichte erstmals ein Marktvolumen von > 1 Mio. US-Dollar.

2011

Anfangskurs: 0,30 USD

Endkurs: 4,72 USD

Jahreshoch: 31,91 USD

09. Februar: Bitcoin erreicht auf der Bitcoin-Börse MtGox erstmals einen Wert von 1 USD pro Bitcoin.

02. Juni: Bitcoin erreicht auf der Bitcoin-Börse Mt Gox einen Wert von 10 USD pro Bitcoin.

08. Juni: Bitcoin erreichte der Kurs am 08. Juni einen rekordverdächtigen Höchstwert von 31,91 US-Dollar (MtGox).

12. Juni: Die erste Bitcoin-Blase (The Great Bubble of 2011) platzt und der Kurs fällt auf 10 USD.

2012

Anfangskurs: 5,27 USD

Endkurs: 13,45 USD

Jahreshoch: 13,51 USD

16. August: Bitcoin-Kurs erreicht Jahreshöchstwert von 13.51 USD.

28. November: Block-Halving Day I – Es findet das erste Bitcoin-Halving statt und der Reward pro Block halbiert sich von 50 auf 25 BTC. Der Kurs zeigt sich mit 12,35 USD unbeeindruckt von dem Event.

2013

Anfangskurs: 13,30 USD

Endkurs: 757 USD

Jahreshoch: 1.242 USD

22. Februar: Bitcoin erreicht erstmals wieder seit 2011 einen Wert von 30 USD.

28. Februar: Bitcoin erreicht neues 601 Day All-Time-High (ATH) und knackt erstmals die 31,91 USD aus dem Jahre 2011.

11. März: Zwei unterschiedliche Bitcoin-Versionen verursachen ein Pausieren aller Transaktionen und der Kurs fällt um 23% auf 37 USD. Er erholt sich jedoch wieder schnell.

21. März: Der Preis pro Bitcoin steigt um 70% rasant auf 74,90 US-

Dollar an.

28. März: Das Bitcoin Marktvolumen erreicht 1 Mrd. US-Dollar.

April: Bitcoin erreicht erstmals einen Wert von 100 US-Dollar.

10. April: Neues All-Time-High bei 266 US-Dollar. Nur ein Jahr zuvor lag der Preis pro Bitcoin bei 13 US-Dollar.

16. April: Der erste große Bitcoin-Crash – der Kurs fällt zurück auf 68,36 US-Dollar.

Oktober: Der Bitcoin-Online Schwarzmarkt Silk-Road wird hochgenommen und der Preis pro Bitcoin fällt von 139 US-Dollar auf 109 US-Dollar. Kurz darauf erholt sich der Kurs mit 128 US-Dollar.

06. November: Bitcoin erreicht mit 269 US-Dollar neues All-Time-High. Kurz zuvor verkündete der chinesische Online-Händler Baidu, zukünftig Bitcoin als Zahlungsmittel zu akzeptieren.

17. November: Bitcoin erreicht um 11:50 GMT rekordverdächtige 503,10 US-Dollar (Mt Gox).

19. November: Bitcoin knackt die 1.000 US-Dollar Marke.

29. November: Bitcoin erreicht bisherige Höchstmarke von 1.242,00 US-Dollar.

18. Dezember: Chinesische Zentralbank zieht es in Erwägung Bitcoin zu verbieten – Kurssturz auf 522 US-Dollar.

2014

Anfangskurs: 770 USD

Endkurs: 320 USD

Jahreshoch: 651,39 USD

10. April: ICBC Bank (China) kündigt mündlich der Bitcoin-Börse Huobi – Kurssturz auf 361 US-Dollar.

12. Juni: Expedia akzeptiert Bitcoin-Zahlungen – Bitcoin erholt sich bei 627 US-Dollar.

Juni-Dezember: Bitcoin verliert an Fahrt und fällt konstant.

2015

Anfangskurs: 314 USD

Endkurs: 430,05 USD

Jahreshoch: 465,50 USD

Januar – Juli: Konstanter Kursverlauf in einer Range zwischen 220 – 260 US-Dollar.

4. November: Kursausbruch! Bitcoin knackt nach einem Jahr mit 408,74 US-Dollar erneut die 400er Marke.

2016

Anfangskurs: 434,46 USD

Endkurs: -

Jahreshoch: -

KAPITEL 3 BITCOIN ALS WERTANLAGE

In den Populärnachrichten tauchen immer wieder Namen auf, die einigen Bitcoin-Enthusiasten schon geläufig sind. Der Streit um das Aufkommen des Social Media Netzwerks Facebook wütete in den Vereinigten Staaten stärker als in Europa, Hollywood-Filme wollten uns einen spannenden Einblick in den Kampf um Rechte, Ideen und das große Geld geben.

Wie in den vorherigen Kapiteln bereits angesprochen besitzt der Bitcoin einen intrinsischen Wert, der sich hauptsächlich an dem Vertrauen der Nutzer und Investoren bemisst. Die tadellosen und zukunftsweisenden Eigenschaften des Bitcoin, lassen traditionelle

Währungen im Schatten der neuen Finanztechnologie stehen. Es wundert also nicht, dass der Bitcoin von vielen als Wertanlage gesehen wird. So auch von großen Unternehmen wie Tyler und Cameron Winklevoss.

Die beiden Sportler und ehemaligen Harvard-Studenten sind als Ruderer 2008 bei den Olympischen Spielen in Peking angetreten. Abseits ihrer sportlichen Leistungen entwickelten sie ein soziales Netzwerk namens „ConnectU“. Dieses Netzwerk wurde zusammen mit der Harvard Universität entwickelt und diente angeblich als Vorlage für Mark Zuckerbergs Facebook. In einem Rechtsstreit klagten die Winklevoss-Brüder auf Schadensersatz für ihre gestohlene Idee. Sie gingen siegreich aus diesem Streit hervor und bekamen 65 Mio. US-Dollar. Die jungen Brüder bauten ihre Pläne

weiter aus und sind als Internet-Unternehmer weithin bekannt. Ihre Bitcoin-Börse *Gemini* erlangte im Oktober 2015 sogar die Genehmigung des New York Department of Financial Services. Ihre favorisierte Anlage sind digitale Währungen. So investierten sie angeblich so viel Geld in Bitcoin, dass sie laut eigenen Aussagen 1% des Bitcoin Marktkapitals besäßen. Auch ein großes Investment in Ether, der Währung von Ethereum, sollen die beiden getätigt haben.

Marc Andreessen und Ben Horowitz sind ebenfalls zwei Namen die man mit Facebook in Verbindung bringt. Die beiden Unternehmer verkauften in der Vergangenheit ihr eigenes Unternehmen an den Software Riesen Hewlett Packard und investierten in Facebook und eBay. Heute sitzen sie im Gremium des Sozialen Netzwerks und der

Handelsplattform. Es wundert nicht, dass auch sie in Bitcoin investierten.

Diese Namen sind nur ein kleiner Teil von Investoren, die ihr Kapital in digitalen Währungen sichern und mehren wollen. Welche Faktoren mögen bei dieser Entscheidung eine Rolle gespielt haben?

Unlängst gab der Gouverneur des amerikanischen Staats Delaware bekannt, dass er die rechtliche Regulierung zum Handel von Aktien auf Basis einer Bitcoin-Blockchain unterstützen wolle. Staaten haben sich bisher relativ schwer mit dem Aufstieg und der Verbreitung digitaler Währungen getan, in manchen Ländern verhalf es gerade dem Bitcoin zum Erfolg.

Zwar gäbe es laut einigen Nachrichtenblättern keine handfeste

Erklärung für die übertriebene Akzeptanz des Bitcoins in China, jedoch fand BTC-ECHO in der Vergangenheit Hinweise für das große Interesse.

Immer wieder scheinen chinesische Anleger das Ökosystem des Bitcoin so stark zu beeinflussen, dass markante Sprünge zu erkennen sind. In den meisten Fällen sind es Aufwärtstrends. In China gibt es einen wackeligen, teils betrügerischen Immobilienmarkt. Investoren fliehen in eine „finanzielle Grauzone“. Da der Geldfluss durch die Regierung eingeschränkt ist und Investoren in und aus China dadurch behindert werden, kam die Idee des Bitcoin gerade recht. Das chinesische Pendant zu WhatsApp namens „WeChat“ fügte sogar eine Funktion in sein Chatprogramm ein, mit der man zum chinesischen Neujahr digitale

„Geschenkumschläge“ mit Bitcoins an Freunde versenden konnte.

Ist der durchschnittliche Nutzer von Bitcoin noch relativ vorsichtig mit seinen Investments in die digitale Währung, so scheinen erfahrene Unternehmer mit großen Summen Bitcoin wie eine Goldalternative zu nutzen. Ein wichtiger, bisher von den Medien kaum erwähnter weiterer Aspekt des Bitcoin ist die *Zeit*.

Von Kritikern wird der Bitcoin häufig deswegen als zukunftslos abgestempelt. Haben wir in den vorherigen Kapiteln zwar den Vergleich mit Gold, Geld und Vertrauen gezogen, so scheint bei traditionellen Denkern immer ein Bezug zu materiellen Werten bestehen zu müssen. Die jetzige Phase wird auch als informationelle Revolution bezeichnet. Abstrakte, nicht greifbare Werte, steigen in

ihrem Ansehen mehr als bisher in der Geschichte des modernen Menschen. Die Gier nach Gold geht weit in die Vergangenheit zurück, doch kein Finanzkonstrukt hat bisher die Zeit selbst in sein System verankert.

ZEIT IST GELD

Wie bereits erwähnt ist die Mathematik hinter Bitcoin eine unschlagbar sichere Angelegenheit. Doch wie kommt die Zeit ins Spiel? Einfach gesagt: anhand der selbstregulierenden Natur der Bitcoin-Difficulty.

Der US Ökonom Milton Friedman wurde für seine Werke im 20. Jahrhundert mit dem Alfred-Nobel-Gedächtnispreis für Wirtschaftswissenschaften ausgezeichnet. Er verfasste Bücher zu

verschiedensten Themen, unter anderem auch zu seiner Annahme der Entstehung von Inflation und Deflation.

Inflation mag der geläufigere der beiden Begriffe sein. Kurz und knapp erklärt, beschreibt die den „Wertverfall“ eines Zahlungsmittels, wenn die vorhandene Geldmenge die Menge produzierter Güter und Dienstleistungen immer weiter überschreitet. Wir gehen in den Supermarkt und erinnern uns, dass wir für unser Geld mal „mehr bekommen haben“. Deflation ist der Inflation gegenüber gesetzt, um ihr entgegenzuwirken senkte die Europäische Zentralbank den Leitzins.

Wir erkennen die chaotische Kraft zwischen Inflation und Deflation wenn sie nicht richtig reguliert wird. Um die Geldmenge an

makroökonomische und finanzielle Faktoren zu binden, schlug der Ökonom Friedman die „Friedman k-Prozent Regel“ vor. Obwohl der kommerzielle Durchbruch von Computern und Netzwerken noch in ferner Zukunft lag, hatte Friedman zu der damaligen Zeit schon die Idee, dass eine solche Regulierung am besten maschinell, mit einem Computer, durchzuführen sei.

An diesem Punkt schließt sich der Kreis. Die Difficulty des Netzwerks passt sich den Gegebenheiten an, sodass ungefähr alle 10 Minuten ein neuer Block geschürft wird. Im Umkehrschluss macht es den Bitcoin berechenbarer als eine Zentralbank, die je nach Belieben eine neue Ausschüttung von Geldmitteln vornehmen kann. Manipulationen könnte man ausschließen. Wir erkennen also Friedmans Vorstellung zur Regulierung von Inflation. Die 10

Minuten Block-Zeit bleiben bestehen, ob das Netzwerk nun stark anwächst oder schwächelt. Auf 21 Millionen Coins im Gesamten macht es den Bitcoin (bzw. die meisten digitalen Währungen) zu einem Geldsystem mit der Zeit als Rückgrat.

Heute einen Kredit für das Haus aufnehmen bevor sich die Zeiten ändern? Lieber jetzt das Geld ausgeben, da man nicht weiß was es in ein paar Jahren noch für einen Wert hat? Jeder kann es an sich selbst beobachten wie unnötig kompliziert traditionelle Währungen sein können. Die Ausschüttung von Coins ist transparent, die Blockhalbierungs-Rate einsehbar.

KAPITEL 4

BLOCKCHAIN

WAS IST DIE BLOCKCHAIN

Die Blockchain könnte sich zur größten Erfindung des bisherigen 21. Jahrhunderts entwickeln, da sie das Zeug hat hochmoderne Technologien abzulösen. Die meisten werden zum ersten Mal von der Blockchain in Verbindung mit Bitcoin etwas gehört haben. Bitcoin hat die Blockchain sozusagen erst bekannt gemacht, da die Digitalwährung auf der Blockchain-Technologie basiert.

Die Blockchain kann wie folgt definiert werden:

“Mit der Blockchain hat man Zugang zu einer vollkommen neuartigen Netzwerk-Infrastruktur. Das wichtigste Merkmal dieser Infrastruktur ist die Dezentralität, die bedingt, dass die Steuerung und Verwaltung nicht durch eine zentrale Institution erfolgt. Entsprechend wird die Blockchain vom gesamten Netzwerk organisiert. Das Netzwerk wiederum setzt sich aus den Teilnehmern zusammen, die sich durch Download der Software an das Netzwerk angeschlossen haben. Server, die von Unternehmen oder Institutionen an einem bestimmten Ort betrieben und zentral kontrolliert werden, sind damit nicht mehr nötig. Jeder einzelne Rechner, egal wo auf der Welt, stellt die Infrastruktur für das Netzwerk bereit. Durch dieses Funktionsprinzip wird die Notwendigkeit einer vermittelnden, dritten Instanz unnötig. Banken,

Notare, zentrale Serverbetreiber und viele andere könnten dadurch, zumindest theoretisch, überflüssig gemacht werden.”

Neben der technischen Effizienz und potentiellen Kostenersparnis, ist es daher vor allem die Unabhängigkeit von Akteuren und zentralen Instanzen wie Staaten, Notenbanken oder großen IT-Unternehmen, die den Reiz der Blockchain ausmacht. Dazu gehört auch die Vermeidung von Intransparenz. Dadurch, dass jede jemals getätigte Transaktion in der Blockchain aufgezeichnet wird und von jedem eingesehen werden kann, handelt es sich um ein sehr transparentes System. Aus diesen Gründen ist die Nutzung der Blockchain nicht nur aus technischer und ökonomischer Sicht relevant, sondern auch aus gesellschaftlicher und politischer.

Wie die Blockchain funktioniert und technisch aufgebaut ist, erfahrt
Ihr im nächsten Kapitel.

WIE FUNKTIONIERT DIE BLOCKCHAIN

Um zu verstehen, wie die Blockchain funktioniert, lässt es sich nicht vermeiden etwas ins technische Detail zu gehen. Dazu macht es Sinn sich den Begriff Blockchain näher anzuschauen. Ähnlich wie der Begriff Bitcoin ist auch dieser aus zwei Wörtern zusammengesetzt. Zum einen aus dem Begriff „Block“, der eine Art Datenprotokoll darstellt, und zum anderen aus dem englischen Begriff „Chain“, was im deutschen *Kette* bedeutet. Es handelt sich damit um Datenblöcke, die wie eine Kette miteinander verbunden sind.

Soweit so gut, nun zum nächsten Schritt. Des Weiteren wissen wir, dass in so einem Block alle Transaktionen des jeweiligen

Netzwerks, in unserem Fall des Bitcoin-Netzwerks, aufgezeichnet werden. Diese Blocks sind durch elektronische Ketten miteinander verbunden und durch eine spezielle Kryptographie (Verschlüsselungstechnik) abgesichert. Dabei beinhaltet jeder Block einen Hash des vorherigen Blocks. Der Hash ist eine algorithmische Funktion in Form einer Zeichenfolge, die als Datenbasis dazu dient eine digitale Signatur zu erstellen. Anwendung findet hier der SHA-256-Hashing-Algorithmus, der nach dem Trial- and Errorprinzip arbeitet. Theoretisch spielt hier auch Glück eine Rolle, da derjenige einen Block generiert, der zuerst eine 256-bit lange Nummer durch Zufall richtig berechnet hat. Dieser Nummer, auch Target genannt, muss die Hash-Funktion insofern entsprechen, dass sie gleich oder kleiner dem Target ist.

Durch diese Signatur wird sichergestellt, dass die Reihe vom letzten bis zum ersten Block (der sog. Genesis-Block) nachvollziehbar bleibt. Um zudem auch die richtige Reihenfolge zu gewährleisten, ist in jedem neuen Block der Hash-Wert des Vorgänger-Blocks enthalten, sodass eine nahtlose Kette entsteht. Hierbei ist festzuhalten, dass jeder Block nach der Berechnung nicht mehr veränderbar ist. Jede Buchung bzw. Transaktion wird notiert. Vorstellen können wir uns das ganze wie eine Excel-Datei, bei der nur neue Einträge erstellt, aber keine alten gelöscht werden können. Jeder Block muss also durch komplexe, algorithmische Berechnungen neu erstellt werden. Allerdings nimmt der Schwierigkeitsgrad der Rechenaufgaben mit steigender Block-Anzahl zu. Dies hat zur Folge, dass das Errechnen eines Blocks

immer länger dauert. Sobald die Netzwerkteilnehmer eine solche Rechenaufgabe gelöst haben, wird der Block an die Kette angehängt.

Der Grundgedanke dahinter nennt sich Proof-of-Work. Dieser Mechanismus soll sicherstellen, dass jeder Teilnehmer, der von der Blockchain profitiert, auch genügend Arbeitsleistung in die Block-Berechnungen investiert.

Die Netzwerkteilnehmer, die sich an der Bewältigung der Rechenaufgaben beteiligen, sprich die Arbeit leisten, werden Miner genannt. Diese Miner verfügen über Hardware, mit der sich die komplexen Rechenaufgaben bewältigen lassen. Im übertragenen Sinne können wir uns diese Miner wie Bergbau-Arbeiter vorstellen,

die versuchen Rohstoffe bzw. Edelmetalle zu schürfen. Nur anstatt einem Presslufthammer verwenden sie Hochleistungsrechner und anstatt Gold werden Coins, in unserem Fall Bitcoins, gemined (geschürft). Bitcoins sind also die Belohnung für das Berechnen von Blocks und erklären, warum Personen oder inzwischen ganze Unternehmen, trotz der Hardware- und Energiekosten, Mining betreiben.

Um Missverständnissen an dieser Stelle im Vorfeld entgegen zu wirken: Auch wenn Bitcoin-Mining notwendig ist, braucht nicht jeder einzelne User ein Miner sein, um das Bitcoin-Netzwerk für Transaktionen zu nutzen.

Neben den Minern sind es sogenannte Nodes, die dafür sorgen, dass

das Bitcoin-Netzwerk am Laufen gehalten wird und Transaktionen schnell und sicher verarbeitet werden können. Die Hauptaufgabe der Nodes besteht in dem Beobachten und Bestätigen von Bitcoin-Transaktionen, um vor allem dem Problem des Double-Spendings entgegen zu wirken. Umso mehr Nodes es gibt, also Personen, die ihre Rechnerleistung dem Netzwerk zur Verfügung stellen und damit als eine Art dezentraler Serverbetreiber fungieren, umso schneller und sicherer kann das Bitcoin-Netzwerk betrieben werden. Insbesondere sogenannte Full-Nodes sind für das Netzwerk unentbehrlich. Diese unterscheiden sich von den einfachen Nodes dadurch, dass sie alle Transaktionen streng mit dem klar definierten Bitcoin-Regelwerk abgleichen und somit einen Sicherheitsstandard garantieren, der nicht mit einfachen Nodes erreicht werden kann.

Der Grund hierfür liegt darin, dass einfache Nodes nur dem Netzwerk folgen und theoretisch auch von den Bitcoin-Kernregeln, z.B. bezüglich Datenformat oder Blockgröße, abweichen können.

Im Gegensatz zum Bitcoin-Mining gibt es für die Nodes aber keine finanzielle Gegenleistung. Dies führt zu dem Problem, dass es einen chronischen Mangel an Nodes und insbesondere Full-Nodes gibt. Es ist daher wahrscheinlich, dass Bitcoin-Unternehmen Kapazitäten schaffen werden, um als Full-Nodes das Bitcoin-Netzwerk, im eigenen Interesse, am Laufen zu halten.

WIE FUNKTIONIERT EINE BITCOIN-TRANSAKTION UND WIE SICHER SIND DIESE?

Nachdem wir geklärt haben wie die Blockchain technisch funktioniert, können wir nun in die Praxis gehen und schauen wie eine Bitcoin-Transaktion abläuft.

Vorerst macht es aber Sinn sich den Weg einer klassischen Banküberweisung anzuschauen. Angenommen Du möchtest von deinem Bankkonto in Deutschland Geld in die USA überweisen, wie würde eine solche Transaktion ablaufen?

1. Du weist das Geld bei deiner Hausbank an.
2. Die Hausbank überweist das Geld an eine deutsche

Korrespondenzbank.

3. Die deutsche Korrespondenzbank überweist das Geld an eine internationale Clearingstelle.

4. Die internationale Clearingstelle überweist das Geld an eine amerikanische Korrespondenzbank.

5. Die amerikanische Korrespondenzbank überweist das Geld an die Hausbank des Empfängers.

Dieser Vorgang dauert mehrere Tage und kostet hohe Gebühren. Wie würde es denn aussehen, wenn wir Geld von Deutschland in die USA, über die Bitcoin-Blockchain, versenden möchten?

Du überweist von deiner digitalen Geldbörse Bitcoins an die

Bitcoin-Empfängeradresse. Nachdem die Transaktion von den Bitcoin-Netzwerk verarbeitet worden ist, kann der Empfänger über die Bitcoins verfügen.

Im Gegensatz zur klassischen Banküberweisung muss das Geld keine Umwege über andere Banken oder Vermittlungsstellen nehmen, sondern kann direkt von Person A zu Person B überwiesen werden. Dies geht schneller und ist kostengünstiger als eine Banküberweisung.

Nachdem wir den Weg einer Bitcoin-Überweisung kennengelernt haben, können wir nun schauen, wie im Bitcoin-Netzwerk eine Überweisung verarbeitet wird. Dadurch können wir verstehen, warum Bitcoin-Transaktionen sowohl schnell als auch sicher sind.

Grundsätzlich können wir uns die Bitcoin-Blockchain wie eine digitale Datei mit Namen und Kontoständen vorstellen.

Tom	8,4
Lisa	2,9
Mario	5,5
Stefanie	0,6

Abbildung 2: Blockchain Tabelle

Angenommen Tom möchte von Stefanie ein Fahrrad kaufen. Dazu überweist er den Betrag von 1,5 BTC (BTC = Währungskürzel für Bitcoin) an Stefanie.

Tom	6,9 (-1,5)
Lisa	2,9
Mario	5,5
Stefanie	2,1 (+1,5)

Abbildung 3: Blockchain Tabelle

Entsprechend sinkt Toms Kontostand um - 1,5 BTC und Stefanies Kontostand steigt um + 1,5 BTC.

Doch wieso kann Tom dem Bitcoin-Netzwerk vertrauen, ohne Angst haben zu müssen, dass seine Zahlung nicht bei Stefanie ankommt? Um diese Frage zu beantworten, müssen wir uns die Verwaltung des Bitcoin-Transaktionsbuches anschauen.

Da es keine zentrale Institution gibt, die die Verwaltung der Kontodaten sicherstellt, besitzt jeder *Betreiber einer Full Node* eine Kopie des gesamten Transaktionsbuches. Das bedeutet, dass jeder sämtliche Kontostände des gesamten Bitcoin-Netzwerks einsehen kann. Um die Anonymität und Privatsphäre zu gewährleisten werden daher keine Namen in dem Transaktionsprotokoll

aufgeführt.

Das Transaktionsbuch sieht daher nicht wie oben dargestellt aus. Statt der Namen enthält es die Bitcoin-Adresse des jeweiligen Teilnehmers.

1PsR49Sdf2V...	6,9 (-1,5)
3Stg11WgFF2...	2,9
3zeP96W2qr...	5,5
1W8w7xtr33h...	2,1 (+1,5)

Abbildung 4: Blockchain Tabelle

Bei der Bitcoin-Adresse handelt es sich um eine Kette von 27 - 34 alphanumerischen Zeichen, die mit einer 1 oder 3 beginnen. Die Adressen können von jedem Teilnehmer kostenlos und beliebig oft generiert werden, ähnlich wie eine E-Mail-Adresse.

Nun stellt sich die Frage, wie die Transaktionsbücher synchron gehalten werden können, obwohl jeder sein eigenes verwaltet.

Bleiben wir bei unserem obigen Beispiel. Wenn Tom Bitcoins an Stefanie senden möchte, teilt er dies dem gesamten Netzwerk, in Form einer Nachricht mit. Die Nachricht würde wie folgt aussehen:



Abbildung 5: Transaktion

Jeder Bitcoin-Teilnehmer, der sein Transaktionsbuch aktualisiert, kann die Überweisung von Tom und Stefanie einsehen.

Leider wissen wir damit immer noch nicht warum Bitcoin-Transaktionen vor Missbrauch und Betrug geschützt sind. Hier kommen die schon erwähnten Miner ins Spiel. Diese Power User

sorgen neben dem Generieren neuer Bitcoin dafür, dass das System am Laufen gehalten bzw. das Transaktionsbuch verwaltet wird.

Um eine Bitcoin-Transaktion durchzuführen, bedarf es einer Art Unterschrift, die sicherstellt, dass die Nachricht von einem echten Bitcoin-Besitzer kommt. Anstatt einer handschriftlichen Unterschrift handelt es sich hierbei um eine Unterschrift, die mithilfe mathematischer Algorithmen erstellt wird.

Dazu wird jede Bitcoin-Adresse mit einem zugehörigen Private Key generiert. Die Private-Keys wiederum sind in der Wallet, der digitalen Brieftasche, gespeichert. Diese werden benötigt, um gemeinsam mit der Transaktionsnachricht eine digitale Signatur zu erstellen. Ohne den Private-Key kann keine Transaktion ausgeführt

oder auf die Bitcoins zurückgegriffen werden. Daher ist es sehr wichtig sich diesen gut zu notieren. Für eine Transaktion werden die Private-Keys zusammen mit der Transaktionsnachricht einer kryptografischen Funktion zugeführt. Eine weitere Funktion überprüft dann genau diese verschlüsselte Funktion. Dadurch kann die digitale Signatur bestätigt werden, sodass sichergestellt wird, dass Besitzer und Transaktion echt sind und zusammengehören. Die digitalen Signaturen haben dabei den Vorteil, dass sie im Gegensatz zur handschriftlichen Unterschrift nicht kopiert oder wiederverwendet werden können. Jede Signatur ist einmalig.

Ein weiterer wichtiger Aspekt ist die Reihenfolge der Transaktionen. Zwar können wir durch die digitalen Signaturen überprüfen von wem die Transaktion veranlasst worden ist, nicht

aber, wann bzw. zu welchem Zeitpunkt dies geschah. Das ist ein Problem, da durch das globale Netzwerk Zeitverzögerungen eintreten können, die bei unzureichender Kontodeckung zu ungedeckten Zahlungen führen können. Ein Problem, das wir beispielsweise von ungedeckten Schecks kennen. Um ein Double-Spending zu verhindern, kommen alle neu erzeugten Transaktionen in eine Warteschleife. Von dort aus werden sie in eine Transaktionskette eingeordnet und ihre Reihenfolge wird festgelegt.

Anschließend findet eine Lotterie statt, in der festgelegt wird, welche Transaktion als nächstes dran kommt. Dazu suchen sich die Teilnehmer eine Transaktion aus der Warteschleife aus und versuchen ein mathematisches Problem zu lösen. Umso mehr Rechenleistung ein Teilnehmer für die Berechnung bereitstellt,

umso höher ist die Wahrscheinlichkeit die Aufgabe schnell zu lösen. Ziel dieser Rechenaufgabe ist es, dass die Transaktion mit dem Ende der Transaktionskette verknüpft wird. Die Person bzw. deren Hardware, die als erstes die Aufgabe löst, darf die Transaktion mit dem Ende der Kette verknüpfen.

Als Belohnung erhält die Person Bitcoins. Diesen Vorgang nennt man, wie wir bereits schon früher kennengelernt haben, Mining .

Es wurden zwei zentrale Aspekte der Bitcoin zugrunde liegenden Technologie genannt: die Private Keys und das Mining. Da diese derart zentral sind, werden wir in den Kapiteln über Bitcoin Wallets und Bitcoin Mining noch einmal vertiefend darauf eingehen.

Wie wir sehen hat die Bitcoin-Blockchain erhebliche Vorteile

gegenüber der gegenwärtigen Bankeninfrastruktur. Insbesondere was Effizienz, Sicherheit und Transparenz anbelangt erweist sich die Blockchain-Technologie als eine sehr gute Alternative zu herkömmlichen Transaktionen. So bedarf es keiner Firewalls oder anderer IT- Sicherheitsmaßnahmen, für die Banken hohe Summen ausgeben müssen, um sich vor Hackerangriffen zu schützen. Dadurch dass weltweit viele Kopien der Blockchain , Online wie Offline existieren hat der Hacker keine Möglichkeit Daten im Blockchain-Netzwerk zu verändern.

ALTERNATIVE BLOCKCHAIN-ANWENDUNGEN

Wie wir bereits wissen geht die Blockchain-Technologie weit über die Möglichkeiten eines Zahlungsverkehrssystems hinaus. Bitcoin und andere digitale Währungen sind nur die Spitze des Eisbergs. Das Konzept einer automatisierten und dezentralen Internetinfrastruktur lässt sich theoretisch auf sämtliche steuerbare Systeme und Organisationsprozesse übertragen.

Auch politische Systeme, wie das Funktionieren eines Staatsapparates, sind davon nicht ausgenommen. Um dies zu realisieren, arbeiten inzwischen viele Unternehmen, Organisationen und Institutionen zusammen. Vor allem das Blockchain-Projekt namens Ethereum ist dabei in den Fokus vieler Akteure geraten. Mit

dieser neuen Blockchain soll es möglich sein, nicht nur Geldtransaktionen, wie bisher mit Bitcoin möglich, vorzunehmen, sondern auch wirtschaftliche, und in fernerer Zukunft auch gesellschaftliche und politische Interaktionen, zu programmieren.

Mithilfe der Blockchain-Technologie könnte zukünftig ganz demokratisch ein Staatsentwurf bzw. ein politisches System programmiert werden. Eine Verfassung, die die gesamte Organisation eines Staates umfasst, soll durch diese dezentrale Datenbank festgelegt und programmiert werden können. Beispielsweise wäre ein Finanzamt oder Notar nicht mehr nötig, da alle Eigentumsverhältnisse und Steuerangelegenheiten in der Blockchain-Datenbank aufgezeichnet werden und von jedem transparent eingesehen werden können.

Bis es soweit ist, sollen vor allem intelligente Verträge, sogenannte Smart Contracts, in entsprechenden Blockchains abgelegt werden. Diese intelligenten Verträge ermöglichen es, ohne eine dritte Kontrollinstanz (wie z.B. Bank oder Notar) Verträge miteinander abzuschließen. Mehrere Staaten versuchen bereits die Registerfunktion der Blockchain-Technologie für ihre Behörden zu nutzen. Diese soll vor allem für Grundbucheintragungen bzw. als Grundstücks-Verzeichnis genutzt werden. Ein ebenfalls hohes Potenzial wird im Energiesektor gesehen. So hat beispielsweise das amerikanische Startup LO3 eine Plattform auf Blockchain-Basis entwickelt, mit der es möglich ist Strom zu handeln. Das Peer-to-Peer Konzept der Blockchain ermöglicht es selbst erzeugten Strom, z.B. durch Solarpanels, an andere Personen weiterzuverkaufen,

ohne den Weg über einen Energieversorger gehen zu müssen.

Neben Unternehmen und dem öffentlichen Sektor haben die Banken ein hohes Interesse an der Blockchain-Technologie. Auch hier geht es weniger um die Nutzung einer digitalen Währung als um die Optimierung von Prozessen und die Steigerung der Wirtschaftlichkeit. Als ein Beispiel ist der Handel mit Wertpapieren und dessen Verbuchung zu nennen. Eine Verwaltung über die Blockchain kann die Effizienz steigern und die Kosten senken. Gleichzeitig können die Kosten für IT-Sicherheit, um sich vor Hacker-Angriffen zu schützen, gesenkt werden. Weiteres Potenzial versprechen sich Banken auch im Kreditgeschäft, da die Blockchain dazu genutzt werden kann Ausfallrisiken besser zu evaluieren. Um dieses Potenzial zu realisieren, haben sich bereits über 40

Großbanken zu einem Banken-Konsortium zusammengeschlossen. Unter der Führung eines Blockchain-Startups namens R3CEV arbeiten die Konkurrenten zusammen an neuen Blockchain-Lösungen. Eine weitere Motivation für die Kooperation der Großbanken ist die Befürchtung, dass sie in den nächsten Jahren Marktanteile an Fin-Techs, die ebenfalls mit der Blockchain arbeiten, verlieren könnten.

AKTUELLE HERAUSFORDERUNGEN VON BITCOIN

Jede neue technologische Entwicklung muss gegen Widerstände ankämpfen und Hürden nehmen. Bitcoin ist da leider keine Ausnahme und so steht die digitale Währung aktuell vor mehreren Herausforderungen.

Eine dieser Herausforderungen ist die sogenannte Skalierungs-Debatte. Das Bitcoin-Netzwerk ist mit dem hohen Aufkommen an Transaktionen überfordert, sodass es immer länger dauert bis eine Transaktion vom Netzwerk bestätigt und in Blöcke gepackt wird. Um dennoch schnell eine Transaktion durchzuführen, besteht die Möglichkeit höhere Gebühren zu zahlen und somit den Vorgang zu beschleunigen. Um dieser Entwicklung entgegen zu wirken, werden

Lösungen diskutiert, wie die Kapazität der Transaktions-Blöcke hochgeschraubt werden kann. Die Community unterteilt sich dabei in zwei Lager. Zum einen gibt es die Bitcoin Core Entwickler, die das Projekt nach der Bitcoin-Geburtsstunde von dem pseudonymen Entwickler Satoshi Nakamoto übernommen haben und seither weiterentwickeln. Zum anderen gibt es das Bitcoin Classic Team. Diese Konkurrenz ist möglich, da es sich um ein Open-Source Projekt handelt, an dessen Code auch andere Entwickler arbeiten können. Genau das macht gerade das Bitcoin Classic Team. Sie wollen die Blockgröße von 1 MB auf 2 MB vergrößern und damit den Transaktionsdurchfluss pro Block verdoppeln. Im Gegenzug schlägt das Team von Bitcoin Core vor, die Kapazität dadurch zu vergrößern, indem sie den Speicherplatz, den eine Signatur im

Block benötigt, reduzieren (Segregated Witness).

Dieser Diskurs ist richtungsweisend für die Zukunft von Bitcoin. Neben dem Aspekt, dass das Bitcoin- Netzwerk schneller werden muss, geht es auch darum wie das Bitcoin-Netzwerk genutzt werden soll. Auf der einen Seite gibt es die Verfechter von Bitcoin Classic, die durch die Vergrößerung der Blocksize (von 1 MB auf 2 MB) mehr Transaktionen zu niedrigeren Kosten abwickeln möchten. Auf der anderen Seite stehen die Verfechter von Bitcoin Core, die größere Transaktionen zu einem allerdings höheren Preis abwickeln möchten. Es bleibt spannend zu beobachten, welche Community sich in der nächsten Zeit durchsetzen wird.

Korrespondierend zur Skalierung-Debatte schließt sich das Problem

der "Mining-Zentralisierung" an. Vereinfacht gesagt geht es darum, dass China inzwischen enorme Mining-Kapazitäten aufgebaut hat, die eine dezentrale und gleichmäßige Verteilung der Mining-Erträge verhindern. In den letzten Monaten und Jahren sind die Anforderungen an die Rechenleistung zum Minen von Blöcken so stark gestiegen, dass nur noch kommerzialisierte Rechenzentren von extremer Größe wirtschaftlich arbeiten können. Die Zeiten, in denen es möglich war alleine mit dem Home-PC Bitcoin-Erträge zu erwirtschaften, sind lange vorbei. Dadurch entstehen Asymmetrien, hin zu einigen großen Playern, die über ausreichend Hardware und entsprechend Kapital verfügen. Folglich wird der Grundgedanke eines dezentralen Netzwerks mit vielen verschiedenen Minern durch eine Zentralisierung auf einige wenige unterwandert. Dies hat zur

Folge, dass viele Miner im Wettbewerb um die Blocks leer ausgehen. Die technische Erklärung dafür ist in der hohen Geschwindigkeit von chinesischen Mining-Rechenzentren zu finden, die die Blocks anderen Minern vor der Nase "wegminen". Es kann also sein, dass jemand anfängt einen Block zu minen, der gar nicht mehr gültig ist, da es bereits einen neuen Block gibt – Aufwand und Kosten vergebens.

Zu diesem Zentralisierungsproblem kommt noch ein weiteres, was gemeinhin unter dem Begriff "Great Firewall of China" subsumiert wird: Im Rahmen des Projekts "goldener Schild" hat die Regierung Chinas viele Mühen auf sich genommen, weite Teile des Internets vor seinen Bürgern zu verbergen. Neben den damit zusammenhängenden ethischen Kritikpunkten führt das zu einer

schlechteren Internet-Performance in China. Da ein Großteil der Mining-Kapazitäten in China lokalisiert ist, hat diese Great Firewall of China ihrerseits einen negativen Einfluss auf die Gesamtperformance des Netzwerks.

Vor diesem Hintergrund argumentieren die Bitcoin Core Anhänger, dass es falsch sei die Blockgröße von 1 MB auf 2 MB, wie es das Team von Bitcoin Classic vorschlägt, anzuheben, da dann nicht-chinesische Miner das Nachsehen hätten und die Asymmetrien im Bitcoin-Netzwerk weiter zunehmen. Auch für die chinesischen Miner wäre entsprechend der Argumentation des Bitcoin Core Teams diese Erhöhung der Blockgröße dank der Probleme, die die Great Firewall of China mit sich bringt, problematisch.

KAPITEL 5 BITCOIN- MINING

Get rich with Bitcoin! "Get money using Bitcoin!" "The new era of Gold-Mining!" "Get rich with Bitcoin-Mining!"

Wenn man nach Bitcoin-Mining sucht, findet man viel darüber, ob man damit Geld verdienen kann oder nicht. Doch was genau ist Bitcoin-Mining? Das warum und wie wollen wir nach den schon erklärenden Worten in den vorangehenden Seiten in diesem Kapitel vertiefen .

WAS IST BITCOIN MINING?

Letztlich ist Bitcoin-Mining ein Begriff, der einen Nebenaspekt des damit beschriebenen Prozess benennt. Hauptaufgabe des Minings ist es, Transaktionen zusammenzufassen, zu validieren und als Blöcke zur Blockchain hinzuzufügen.

Diese Aufgabe ist essentiell für Bitcoin, sorgt das doch dafür, dass die Transaktionen überhaupt bestätigt werden können. Da diese Aufgabe derart obligatorisch ist, werden Miner für ihre Mühen entlohnt - sie erhalten Bitcoins. Diese Bitcoins werden in diesem Prozess erzeugt und kommen sozusagen aus dem Nichts. Genau deshalb redet man vom Bitcoin-Mining: so wie die Goldschürfer im Wilden Westen aus dem Boden Gold schürften, bekommen die

Miner dafür Geld. Damit ist auch klar, warum so viele Artikel im Internet sich auf diesen Geldaspekt fokussieren und entweder behaupten, man könne durch Mining unheimlich viel Geld machen oder konstatieren, dass Mining sich nicht mehr lohne.

Bevor wir zum Thema Geld verdienen kommen, möchte ich die essentielle Rolle des Mining-Prozesses genauer darstellen. Jedem Bitcoin-Nutzer muss klar sein, dass es Miner braucht - egal wie profitabel es ist.

BERECHNUNGEN

Was geschieht nun beim Mining? Um das zu verstehen, fangen wir mal deutlich früher an, nämlich bei der Transaktion selbst und rufen uns in Erinnerung, was im Kapitel über die Blockchain gesagt wurde. Sagen wir also, man will sich mittels Bitcoin was kaufen. Also senden wir 1 BTC an den Empfänger. Was konkret passiert, ist dass wir dem Bitcoin-Netzwerk signalisieren, dass von Adresse X 1 BTC an Adresse Y gesendet wird. So weit, so gut, möchte man meinen.

Das Problem ist, dass wir von digitalen Währungen reden. Letztlich wurde nur ein Eintrag erzeugt, nichts Physisches wurde weiter gegeben. Was versichert dem Verkäufer nun, dass ich kein böser

Mensch bin, der versucht, via Double Spending (dh. über doppelte Ausgabe eines Bitcoin) ihn zu betrügen? Eine Lösung wäre, diese Transaktion in einem Timestamp-Server abzulegen, auf dem jede Transaktion mit einem Zeitstempel versehen zentral gespeichert ist. Dieser Server überprüft auch, ob hier Transaktionen vorliegen, die eventuell unmöglich sind.

Nun wäre Bitcoin aber nicht dezentral, wenn das ein einzelner Server wäre. Was Bitcoin stattdessen macht, ist in einem Prozess zusammen gefasst, der Proof-of-Work heißt. Dabei werden alle in jüngster Zeit zusammen gekommenen Transaktionen zusammengefasst und über einen Verschlüsselungsmechanismus in eine Zeichenkette einer bestimmten Länge konvertiert. Diese Zeichenkette, Merkle-Root genannt, fungiert als eine

Seriennummer, die die später im Block enthaltenen Transaktionen beschreibt. Sobald diese Merkle-Root offiziell ist - wann, werden wir gleich klären - sind die entsprechenden Transaktionen unumkehrbar in der Blockchain gespeichert.

Ok, wir haben jetzt also abgespeichert, welche Transaktionen in jüngster Zeit geschehen, aber noch ist das alles einfach separat gespeichert. Wie wird das nun Teil des offiziellen Systems?

Dazu müssen die Transaktionen in einem Block zusammen gefasst werden, der, sofern er akzeptiert wird, der Blockchain angefügt wird. Diese Blockchain schließlich verbindet alle Blöcke vom ersten erzeugten bis zum aktuellen.

Ein Block enthält noch etwas mehr als die Merkle-Root, unter

anderem auch eine Zeichenkette (Hash genannt), die den vorherigen Block beschreibt. Des Weiteren wird ein Zeitstempel eingefügt, der selbst eine Kontrolle darstellt, ob der Block soweit Sinn macht. Zusammen mit ein paar anderen Nummern (bspw. der Versionsnummer des verwendeten Bitcoin Protokolls und einer Zählervariable, zu der wir noch kommen) kann diese ganze Information wiederum in einen Hash überführt werden, die dann den aktuellen Block beschreibt.

Bisher mag uns Menschen da der Kopf rauchen, für einen Computer wären das aber nur ein paar Funktionen. So weit, so simpel. Simpel sollte dieser Mechanismus aber gerade nicht sein, da das dem Missbrauch Tür und Tor öffnen würde. Deshalb wird der Mechanismus künstlich erschwert, was im nächsten Abschnitt

beschrieben ist.

DIFFICULTY

Die im vorherigen Abschnitt angesprochene künstliche Erschwerung wird erzielt, indem man bestimmte Charakteristiken von den zu erzeugenden Hashs verlangt. So sagt man dann, dass der erzeugte Hash kleiner als ein bestimmter festgelegter Wert sein soll (was dann das im Blockchain-Kapitel erwähnte Target ist). Wie oben beschrieben ist, fließt in die Erzeugung des Hashs die die aktuellen Transaktionen beschreibende Merkle-Root, die Hash vom vorherigen Block, der Zeitstempel und "ein paar andere Nummern" wie im vorherigen Abschnitt etwas schwammig angedeutet. Eine dieser Nummern ist letztlich einfach ein Zähler, der so lange variiert wird, bis der erzeugte Hash kleiner als das Target ist. Dieser Zähler

wird Nonce genannt. Je nachdem, was das Target ist, kann das mehr oder weniger Lösungen obiger Berechnungen ausschließen. Deshalb hat man eine Größe eingeführt, die misst, wie schwierig es ist, einen Block zu erzeugen, dessen Hash unterhalb des Targets liegt - die Difficulty. Diese liegt zur Zeit bei 1:175 Milliarden. Man sieht also, dass es äußerst unwahrscheinlich ist, diese Blocks beim ersten Mal zu erzeugen oder anders herum gesagt wird man höchstwahrscheinlich viele Berechnungen mit unterschiedlichen Nonces benötigen. Repetitive Berechnungen? Klingt nach einem Job für Computer - und so gibt es für diesen Prozess quasi exklusiv gefertigte Rechner.

Wenn man sich die Entwicklung der Difficulty ansieht, sieht man, dass diese - bis auf ein paar Ausnahmen - immer weiter angestiegen

ist. Seit den Ursprungstagen von Bitcoin ist das Mining viel schwieriger geworden! Grund dafür ist, dass in regelmäßigen Abständen (alle 2016 Blöcke, was ungefähr zwei Wochen entspricht) die Difficulty der Performance des Blockchain-Netzwerkes angepasst wird. Man möchte gewährleisten, dass alle zehn Minuten ein Block erzeugt wird. Damit das nicht zu schwer oder zu leicht wird (Computer werden immer leistungsfähiger) wird die Difficulty so gesetzt, dass dieses Ziel weiterhin erreicht wird.

"Ja, aber was ist mit dem Geld?"

Nun wissen wir, warum Mining für das Bitcoin Netzwerk notwendig ist, wir wissen, was für Rechnungen durchgeführt werden und dass diese immer schwieriger werden. Und wie Bud Spencer fragen wir

nun die Frage nach "den Kohlen". Warum soll man angeblich reich dadurch werden? Die Mühe, die sich die Leute machen, diese Berechnungen anzustellen, kostet etwas. Computer müssen mit Strom versorgt werden, man benötigt einen Zugang zum Internet und das alles will auch gewartet werden. Damit das alles nicht einfach auf der Basis von Luft und Liebe funktioniert, wird der Miner, der als erstes einen Block mit dem aktuellen Target findet, sprich, der vom Netzwerk akzeptiert wird, in Bitcoin entlohnt - dem Mining-Reward.

Es wird noch interessanter: diese Bitcoin werden größtenteils aus dem nichts generiert. So wie der Glücksritter am Klondyke nach Gold schürft, suchen die Miner nach Blöcken, die dem aktuellen Target entsprechen.

Die Analogie zum Goldschürfen geht noch weiter: es ist im Bitcoin-Protokoll festgelegt, wie viele Bitcoin es jemals geben wird. Keine europäische Zentralbank kann einfach Bitcoin generieren. Wie das funktioniert? Nach festgelegten Intervallen wird die Entlohnung halbiert. Zur Zeit sind wir bei 25 BTC, ab Juli 2016 werden es nur noch 12.5 BTC sein. Das ist eine Menge Geld - nach aktuellem Kurs 10.000 € bzw 5.000 € - und alle zehn Minuten wird dieser Betrag ausgeschüttet! Dementsprechend groß ist auch die Konkurrenz.

Neben dem Mining-Reward wird den Minern ein Anteil der Transaktionsgebühren gezahlt. Man wird, je nach genutztem Wallet, die Höhe der Transaktionsgebühr festlegen können. Man schafft letztlich mit der Gebühr einen Anreiz bei den Minern, die

Transaktion in den Block aufzunehmen. Dementsprechend kann man als Faustregel sagen, dass die Bestätigung der Transaktion, das Einfügen der eigenen Transaktion in die Blockchain, umso länger dauert, je weniger man als Gebühr zahlt. Da dieses Einfügen der eigenen Transaktion in die Blockchain für den Zahlungsempfänger ein Garant dafür ist, dass er nicht betrogen wird (und, je nach Brisanz des Geschäftes Leute durchaus mehrere solcher Bestätigungen abwarten), verzögert eine geringe Gebühr den Vertragsabschluss.

Letztlich ist das einer der Punkte, der zeigt, dass Bitcoin Leute für mündig hält und ihnen die Freiheit schenkt, das Maß für ihre Sicherheit und für die Effizienz des Zahlungsverkehrs selbst zu wählen. Einem guten Freund würde ich wahrscheinlich sofort

glauben, dass er mich nicht betrügt, da könnte ich mir die Transaktionsbestätigung ganz schenken - man würde sofort sehen, dass eine Transaktion stattfand und fertig. Aber wenn irgendein windiger Mogul einem einen riesigen Betrag Geld für das Eigenheim zahlt? Da möchte man mehr Sicherheit haben!

Man muss hier betonen, dass die Transaktionsgebühren bei Beträgen liegen, die umgerechnet 2 Cent entsprechen. Das ist deutlich billiger als die durchschnittliche Kreditkarten-Transaktion.

WIE KANN ICH BITCOIN MINEN?

Wir wissen jetzt warum man minen muss und was es dafür für Geld gibt. Ich gehe mal davon aus, dass der durchschnittliche Leser gerne mehr Geld haben will. Wäre es da nicht sinnvoll, seinen Computer über Nacht anzulassen und fröhlich drauflos zu minen? Computer an und man macht mit etwas Glück 25 BTC.

So einfach ist das nicht. Wenn wir auf dem durchschnittlichen Laptop Bitcoin minen würden, wären wir so langsam mit den Berechnungen, dass uns größtenteils Konkurrenten im Mining-Netzwerk die Bitcoins wegschnappen würden. Wir würden viel Geld für den Strom ausgeben und nichts dafür bekommen.

Letztlich können wir uns vorstellen, dass es auf den Trade-Off ankommt, wie viel man an Geld reinstecken will und wie viel man zurückbekommt. Es ist ein Investment, wo wir uns gut überlegen sollten, wo wir Geld anlegen.

Generell gibt es drei Ansätze, die wir verfolgen können:

Wir können uns denken "Everybody for himself" und Solo-Mining betreiben. Wir würden, falls wir einen Block finden, der vom Netzwerk akzeptiert wird, den vollen Reward und die Transaktionsgebühren erhalten.

Beim Pool-Mining könnten wir mit unserem Equipment eine größere Gruppe von Minern unterstützen. Die Wahrscheinlichkeit, Geld zu machen, wäre größer, wir würden aber weniger bekommen.

Wir können uns auch in größere Mining-Farms einkaufen. Man zahlt Geld und wird dafür an den Rewards beteiligt - mint aber nicht selber.

Grob kann man berechnen, wie sehr sich welches Equipment lohnt: dazu nimmt man das aktuelle Target, teilt es durch $1e77$ (grob, an sich durch 2^{256}). Damit haben wir die Wahrscheinlichkeit, überhaupt einen Block zu finden. Diesen Wert invertieren wir und multiplizieren ihn mit der Hashrate - was uns die ungefähre Zeit bis zum Finden eines Blocks liefern würde. Ein Antminer hat ungefähr 5TH/s und ist einer der besten Miner, die man für Geld kaufen kann. Selbst mit dem wird es aktuell über tausend Tage dauern, um einen Bitcoin zu bekommen.

Warum ist das so? Wie schon dargestellt, nicht nur du und ich haben erkannt, dass Mining ein lukratives Geschäft ist. Unter anderem in China gibt es riesige Anlagen - so genannte Mining-Farmen, deren Wahrscheinlichkeit, den vom Netzwerk dann akzeptierten Block zu finden, deutlich größer ist - sie haben deutlich größere Hashrates.

Genau deshalb gibt es Pool-Mining. Da ein einzelner Miner zuhause kaum rentabel minen kann, kann man sich mit seiner Hashrate einem Pool anschließen. Man würde dann anteilig bezahlt werden, muss oft eine gewisse Gebühr entrichten - aber dafür schürft man mit einer deutlich höheren Hashrate. Generell existieren unterschiedliche Geschäftsmodelle, die mehr oder weniger zentralisiert sind. Außerdem ist darauf zu achten, dass man sich

einen Pool sucht, der das aktuelle Bitcoin-Protokoll unterstützt. Schließlich existieren noch unterschiedliche Rewardmodelle, man sollte also eines wählen, was einem optimal passt. Die wichtigsten seien kurz vorgestellt:

PPS (Pay per Share): Quasi die Mutter aller Rewardmodelle. Miner bekommen für jeden gelösten Block einen Anteil entsprechend der dem Pool gestifteten Hashrate - egal, ob dieser nun der erste im gesamten Netzwerk ist oder nicht. Für den einzelnen Miner ist das ein stabiles Einkommen - für den Betreiber des Mining-Pools ein ziemliches Risiko, weshalb dieses Modell nicht mehr so oft angewandt wird.

PPLNS (Pay per least n shares): Wenn ein Block gefunden und

vom Netz anerkannt wird, erhalten alle Miner entsprechend ihrer Hashrate, die sie die letzten N Blocks hatten, Anteile. Damit sind ältere Hasen Neulingen gegenüber etwas im Vorteil.

DGM (Double geometry method): Hier zahlt der Operator nur, wenn das Finden eines Blocks länger dauert - bei kurzen Runden behält er das Geld als Kompensation für etwaige Durststrecken.

Schließlich kann man noch bequem sein und minen lassen. Du kannst Dich in einen Cloud-Mining-Service einkaufen und danach regelmäßig Geld aufs Konto bekommen. Das klingt nicht nur windig, das ist es des Öfteren auch. Es gab eine Reihe von Scams und teilweise hat man den Eindruck, dass es den Betreibern weniger um die Absicherung einer dezentralen, digitalen Währung, sondern

um eine Möglichkeit, Fiat-Geld anzuhäufen geht. Dennoch ist zu sagen, dass es vielen Cloud-Mining-Services wirklich um Bitcoin geht und sie bspw. etwas gegen die Zentralisierung der Hashrate auf gigantische Mining-Pools tun wollen - und für jemanden, der das Bitcoin-Ökosystem am Leben erhalten will, aber zum Mining (egal ob Solo oder Pool-Mining) nicht die Möglichkeiten hat, sind Cloud-Mining-Services eine gute Option.

DIE 51% ATTACKE

WAS IST EINE 51% ATTACKE?

Bitcoin ist, wie jedes System, nicht perfekt. Hier erfahrt ihr was eine 51% Attacke ist, was sie kann und wie man sie verhindern kann.

“Be your own Bank!” – einer der bekanntesten Slogans der Bitcoin-Community. Als Freund dezentraler Organisation, der irgendwo zwischen Belloc und Hughes pendelt, hat mich der Slogan immer angesprochen. Zu oft hat man jedoch den Eindruck, dass man aus solchen Slogans gerne Floskeln Marke “Alles für alle und das umsonst” macht. Wenn wir wirklich das Bankensystem dezentralisieren wollen, müssen wir auch die Verantwortung, die in ihren Händen liegt, dezentralisieren. Und das bedeutet, dass wir

nicht nur Nutzer sein können, sondern aufgeklärte, kritische Nutzer sein müssen, die ein Auge auf der [Blockchain](#) haben. Wir müssen die Gefahren kennen, und wissen, was Signale für einen Angriff auf die Blockchain sind. Betrachten wir deshalb die 51% Attacke.

WIE FUNKTIONIERT EINE 51% ATTACKE ?

Die Bitcoin-Infrastruktur besteht, grob gesagt, aus den Nutzern (bzw. genauer gesagt ihren Wallets), unterschiedlichen User-Interfaces, den Minern und den Nodes. Die Nodes sind dabei dafür verantwortlich, das Bitcoin-Netzwerk aufrecht zu erhalten und verwalten den Transaktionsverkehr. Nodes garantieren, dass alle Transaktionen den Regeln entsprechen. Die Aufgabe der Miner ist schließlich, Transaktionen zu Blöcken zusammen zu fassen und

diese an die Blockchain anzuhängen.

Die berühmte 51% Attacke ist nun folgendes Szenario: sagen wir mal, ein Angreifer würde es schaffen, über 50% der Miner zu stellen. Wenn wir auf blockchain.info schauen, können wir schnell sehen, dass drei der großen [Mining](#)-Pools (AntPool, F2Pool und Btcc Pool) mehr als 50% der Hashrate aufbringen. Die Sorge ist also nicht nur rein hypothetisch, sondern durchaus real. In anderen Altcoins ist sowas anscheinend schon mal passiert.

Sagen wir also, die drei genannten Mining-Pools tun sich aus was für Gründen zusammen. Was könnten sie dann tun?

Um das zu klären gehen wir mal zu den Roots, sprich zu Satoshi Nakamotos Paper zurück. Im Abschnitt 11 betrachtet er das

Problem, wenn ein Angreifer falsche Blöcke in das System speisen will. Letztlich kann man errechnen, wie wahrscheinlich es ist, dass ein Angreifer “seine” Blockchain durchbekommt.

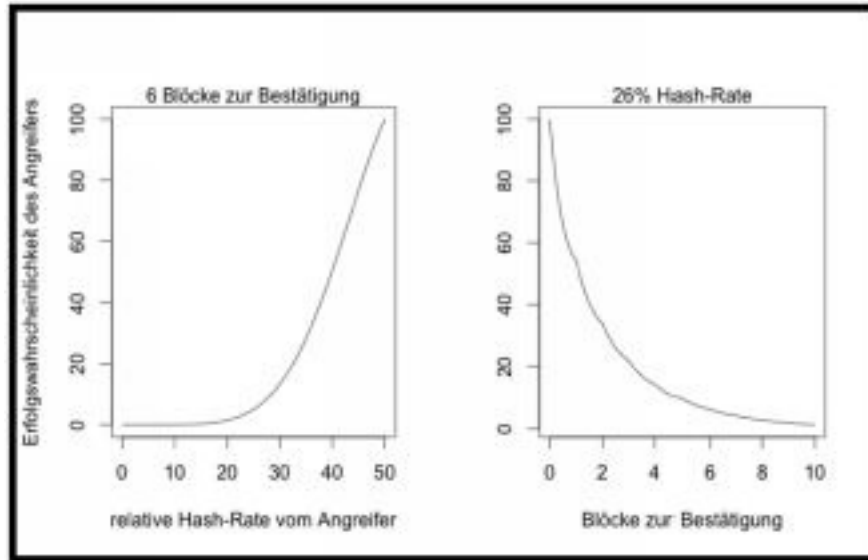


Abbildung 6: Erfolgswahrscheinlichkeit 51%-Attacke

In obigen Abbildungen ist diese Erfolgswahrscheinlichkeit

dargestellt, links in Abhängigkeit der relativen Hash-Rate des Angreifers (bei einer Annahme von 6 Bestätigungen einer Transaktion) und rechts in Abhängigkeit der Anzahl an *Bestätigungen* (bei Annahme einer relativen Hash-Rate von 26% auf Seiten des Angreifers).

Wir erkennen schnell, dass wenn die Hashrate des Angreifers größer oder gleich die des Gegners ist, die Wahrscheinlichkeit, Dinge zu ändern, gleich eins ist. Das bedeutet, dass jemand mit mehr als 50% der Hashrate auf seiner Seite unglaublich viel Macht hätte; obige Formel würde immer zu seinen Gunsten entschieden. Man sollte außerdem im Hinterkopf haben: Auch wenn die Attacke 51% Attacke heißt und suggeriert, dass man mehr als fünfzig Prozent der Hashrate für die Attacke benötigt, kann man anhand der Formel von

Nakamoto erkennen, dass bei einer geringeren Kontrolle die Wahrscheinlichkeit für den Erfolg eines Angriffes einfach kleiner ist. Sprich: Man sollte sich nicht einfach an den 51% hochziehen, schon mit deutlich weniger kann man eine Menge Mist bauen.

MÖGLICHKEITEN DER 51%-ATTACKE

Was könnte nun so ein Angreifer tun?

Solange er die Kontrolle hat, könnte er Double-Spend-Transactions durchführen. Genauer gesagt könnte er Transaktionen umkehren und woanders hin transferieren. Das würde natürlich das Bitcoin-Ökosystem vollkommen durcheinander werfen.

Er könnte beliebig viele Transaktionen verhindern oder genauer gesagt, ihnen keine Bestätigungen zusichern. Der Angreifer könnte

bspw. gezielt bestimmte Zahlungen sperren und damit einzelne Firmen ausschalten. Er könnte beliebig viele Miner davon abhalten, irgendwelche gültigen Blocks zu minen und die Rewards dafür selbst einheimsen. Das ist eine Menge. Dementsprechend sollte man die Gefahr durchaus ernst nehmen.

WAS KANN MAN DAGEGEN TUN?

Das Schöne an der Blockchain ist, dass alles transparent ist. Wir können die Blockchain beobachten. Direkt auf [Blockchain.info](https://blockchain.info) kann man erkennen, welche Mining-Pools welche Blocks gefunden haben. Das ist natürlich kein “Gegenmittel”, kann jedoch helfen zu erkennen, ob es Mining-Pools gibt, die signifikant häufig einen Block der Blockchain beisteuern.

Leider ist es ansonsten im Fall von Bitcoin schwer, als Einzelner was dagegen zu tun. Man kann nicht einfach dafür sorgen, dass die “guten” Miner insgesamt mehr Hashing-Power bekommen. Es wurde ansonsten vorgeschlagen, feindliche Miner durch gezielte DDoS-Attacken lahmzulegen, was aber auch nicht trivial ist.

Eine Sache jedoch, die auch ein Otto-Normal-Verbraucher in solch einem Krisenfall tun kann, ist, dass er *die Bestätigungszahl einer Transaktion* zur Abwehr von doppelten Transaktionen erhöht. Sollte ein Angreifer wirklich 50% oder mehr der Hashrate innehaben, würde das nichts daran ändern, dass seine Blockchain-Version sich immer durchsetzen würde, aber es bringt Zeit. Für Bitcoin wird es wahnsinnig teuer sein, die 51% der Hashrate aufrecht zu erhalten. Man kann also damit den Angreifer ausbluten.

Schließlich kann man beruhigend hinnehmen, dass Gavin Andersen zwar das klassische Bonmot “That would be bad” hinsichtlich einer 51%-Attacke brachte, aber auch sagte, dass es recht einfach wäre, von einem Developer-Standpunkt her sich dagegen zu verteidigen. Eine Idee wäre, dass der Angreifer letztlich nicht nur eine Menge an Hashrate, sondern auch eine Menge an Bitcoins aus der Zeit vor dem Angriff haben müsste . Insgesamt würde man dadurch nicht nur die 51%-Attacke ziemlich teuer machen, sondern auch dafür sorgen, dass der Angreifer schnell ausblutet.

Zusammenfassend lässt sich sagen, dass eine 51%-Attacke auf Bitcoin eine ernste Sache ist, die jedoch detektiert werden kann und wo wir Nutzer zumindest handeln können. Wichtig ist, wie schon in der Einleitung angesprochen, dass wir Bitcoin-Nutzer den Slogen

“Be your own Bank” ernst nehmen und das Netzwerk im Auge behalten.

KAPITEL 6 BITCOIN- WALLETS

Zum Geld gehört natürlich immer auch die Frage, wie man es aufbewahrt. Sei es im Sparschwein, im Portemonnaie, im Tresor oder auf der Bank - um Geld zu besitzen, muss es irgendwo verwahrt werden. Das gilt auch für eine virtuelle Währung.

Geld, was früher eine bestimmte Menge eines wertvollen Metalls war, ist immer mehr zu einer virtuellen Größe geworden. Wir brauchen da nicht sofort zu Kryptowährungen zu gehen; jeder, der mit MasterCard, EC oder Paypal zahlt, sieht die Geldscheine, die den Besitzer wechseln, nicht mehr. Geld in der heutigen Zeit ist also

(Verzeihung, wenn ich hier etwas trocken werde) eine abzählbare Menge, bei der man sich auf einen bestimmten Tauschwert geeinigt hat (bzw. immer wieder neu einigt). Was es außerdem braucht, ist ein System, das festhält, wem gerade welche Menge Geld gehört. So kann dann also Handel entstehen: Ein bestimmter Betrag an Geld kann den Besitzer wechseln und für ein Produkt, einen Service oder was auch immer getauscht werden.

Bei Bitcoin ist das alles nicht so unterschiedlich. Auch Bitcoin braucht ein System, in dem gespeichert wird, wer wie viele Bitcoins hat und wohin er diese überweist bzw. von wo er Bitcoins empfängt. Es wurde schon erklärt, dass das alles der Blockchain zu entnehmen ist, die durch die Arbeit der Miner aufgebaut und von den Nodes gespeichert wird. Wir wissen also, wie der Bitcoin-Fluss

abgebildet wird. Was jetzt noch fehlt, ist ein Zugang, den ein Bitcoin-Besitzer zu seinen Bitcoins hat - es fehlt eine Geldbörse, oder ein Wallet, wenn man Englisch spricht.

Das Wallet ist also die digitale Form einer Geldbörse. Es muss mehrere Dinge können:

1. Es muss einen bestimmten Betrag an Bitcoin enthalten.
2. Dieser Betrag darf nur dem Nutzer zur Ausgabe zur Verfügung stehen.
3. Es muss möglich sein, dass Geld dort abgelegt werden kann.

Wie macht das Bitcoin? Nun, in der Blockchain wird in den Blöcken gespeichert, von welcher Adresse wann wie viele Bitcoin

zu welcher Adresse transferiert wurden. Man kann also zu einem beliebigen Zeitpunkt (bspw. gerade jetzt) anhand dieser Daten sehen, wie viele Bitcoin mit welcher Adresse verknüpft sind.

Diese Adresse ist nun letztlich das Wallet, weshalb wir sie jetzt mal genauer betrachten:

Wenn wir auf die Blockchain bspw. auf blockchain.info schauen, können wir dort tatsächlich uns einzelne Transaktionen ansehen, siehe

<https://blockchain.info/tx/e17a3ff613bd62d59ad1f58f2962f8389871>:

In der Transaktion

e17a3ff613bd62d59ad1f58f2962f8389871fe61f8dad4dabf5e36d03ff

wurde also ein kleiner Betrag - 0.0118133 BTC - von der Adresse

13hh1d87wxFiRnMYRZFHBEwCtFvG3xXsgdan

die Adresse

1C1TU74L6pZRmKNZ8omJuwpiDygcumSW6Q überwiesen.

Der Zahlende hatte eine kleine Transaktionsgebühr - 0.0001 BTC - zu zahlen, der Rest ging an den Empfänger. Wir haben also mithilfe dieser Adressen zwei der obigen drei Forderungen erschlagen können:

Die Adressen sind mit einem bestimmten Betrag assoziiert, siehe:

<https://blockchain.info/address/1C1TU74L6pZRmKNZ8omJuwpiDygcumSW6Q>

und die Transaktion selbst beweist Punkt Nr. 3.

Wir merken außerdem, dass die Adressen - die ihrerseits Public-Key

genannt werden (Fußnote: was letztlich falsch ist, es sind aus dem Public-Key generierte Adressen, was jedoch oft synonym benutzt wird) - dieselbe Länge haben - beide sind 34 Zeichen lang. Sie lesen sich wie Gibberish, was aber einen Grund hat, denn sie leiten sich direkt von dem Inner Sanctum, dem freien Zugriff auf das Bitcoin Wallet ab. Dieser Zugriff wird “Private-Key” genannt, da dies der Schlüssel ist, der deine Bitcoin vor den gierigen Fingern etwaiger Langfinger rettet.

Der Private-Key selbst ist deutlich länger als der Public-Key und kann bspw. folgende Form aufweisen:

18E14A7B6A307F426A94F8114701E7C8E774E7F9A47E2C2035I

Das sind 64 Zeichen! Man kann sich vorstellen, dass ein Brute-

Force-Knacken eines solchen Private-Keys unglaublich komplex ist. Auf der anderen Seite muss man sich jedoch auch diesen Private-Key merken, denn ohne ihn kommt man nicht an das Wallet.

Ohne hier zu viele Details zu klären kann der Public-Key aus dem Private-Key generiert werden. Wenn man also den Private-Key besitzt, besitzt man automatisch den Public-Key. Das ist jedoch unumkehrbar: Niemand kann mithilfe des Public-Key den Private-Key generieren.

Mit dieser Unumkehrbarkeit steht und fällt Bitcoin. Wenn dies nämlich möglich wäre, wäre das Geld in einem Wallet nicht sicher. Da das so ist, bedeutet das jedoch auch, dass jeder Wallet-Besitzer seinen Private-Key unbedingt aufheben muss - ist er verloren ist das

Geld weg. Man kann sich dann an niemanden wenden und einen Antrag auf Password-Recovery stellen - auch das ist eine Dimension dessen, auf einen Middle-Man zu verzichten.

Natürlich könnte man jetzt zu einer Kurzschlussreaktion neigen und das Geld auf einem der Exchange-Anbieter liegen lassen (davon an anderer Stelle mehr) - doch damit würde man die Verantwortung für sein Geld nur in die Hände eines unbekannten Dritten geben; das kennen wir von Banken, hat dort nicht immer gut geklappt und mit Mt Gox gibt es in der Bitcoin-Szene ein düsteres Beispiel, wo das enden kann. Deshalb hier die Empfehlung: erstell dir ein Wallet! Wie das funktioniert und wie du ein passendes wählst erfährst Du hier.

MULTI-SIG WALLETS - BRIEFTASCHEN FÜR TEAMS

Ihr werdet, wenn ihr euch Wallets aussucht, oft über den Begriff "Multi-Sig-Wallet stolpern. Was ist das?

Nehmen wir mal an, wir hätten einen gemeinsamen Fundus - innerhalb unserer Familie, unserer Firma oder unseres Clubs. Es wäre dann schön, wenn man in einem gemeinsamen Konto bestimmte Dinge regeln könnte: Kann jemand allein auf das Konto zugreifen? Wer hat zuletzt auf das Konto zugegriffen?

Im Rahmen dessen, was wir von einem Wallet hörten, ist das nicht ganz einfach; wissen alle Parts nur einen Teil des Private-Keys? Das könnte zwar unsere erste Forderung realisieren, aber zum einen nicht die zweite, zum zweiten scheidet sie aus, wenn man ein

System aufbauen möchte, in dem zum Zugang nicht ein Konsens von 100%, sondern sagen wir mal von 75% nötig wäre.

All das ist mit Multi-Sig-Wallets möglich, wobei Multi-Sig für Multi-Signature steht. Ein Multi-Signature-Wallet ist durch mehrere Private-Keys gesichert. Technisch gesehen kann man sie derart implementieren, dass es für eine Transaktion n Bestätigungen von m Accounts braucht. Das eröffnet interessante Möglichkeiten:

1/2 (dh. $n=1$, $m=2$) Wallets wären ein Konto, dass man gemeinsam mit seinem Partner/seiner Partnerin nutzt. Jeder hätte von sich aus Zugriff, man könnte aber nachvollziehen, wer wann was ausgegeben hat.

2/2 Ein Wallet hätte man auf dem PC, ein anderes auf seinem

Smartphone. Damit hätte man eine Two-Way-Verification geschaffen. Hacker müssten jetzt sowohl den Private-Key vom Wallet auf dem PC als auch den vom Wallet auf dem Smartphone haben, um Kontrolle über das Geld zu besitzen.

7/10 übertreiben wir doch mal und nehmen ein Board bestehend aus zehn Mitgliedern an, dass über die Geschicke einer großen Firma entscheiden soll. Man akzeptiert Beschlüsse bzgl. Investitionen etc., wenn über $\frac{2}{3}$ des Boards zustimmen.

Das wahnsinnig interessante an Multi-Sig-Wallets ist, dass das auf der Blockchain selbst möglich ist. Es wird also entsprechend dem Ideal von Bitcoin keine Third-Party benötigt, die den Zugriff auf ein Konto kontrolliert und verwaltet.

COLD-STORAGE - DAS OFFLINE-TRESORSYSTEM VON BITCOIN

Wer sich beim Lesen an reguläre Online-Konten erinnert fühlt, liegt absolut nicht falsch: viele Bitcoin-Wallets funktionieren von außen betrachtet ähnlich und werden auch so verwendet (siehe Online-Wallet, Mobile-Wallet, Bitcoin-Core-Wallet; Konzepte, die weiter unten besprochen werden).

Diese Wallets sind größtenteils online, so dass man schnell Zahlungen tätigen kann. Nun kennen wir in der klassischen Welt des Geldes noch eine andere Art von Geldablage: Geld, was primär ruhen soll. Denken wir dabei nicht an ein Sparkonto, sondern ein Sparschwein oder einen Tresor. Wir wollen das Geld sicher

ablegen. Dafür sind sogenannte Cold-Storages prädestiniert.

In einem Cold-Storage liegt die Information, die einem den Zugriff auf das Geld ermöglicht, in irgendeiner Form offline. Das kann bedeuten, dass man sich den Private-Key ausgedruckt hat (siehe Paper-Wallets), dass man sich eine Passphrase, die man in den Private-Key umwandeln kann, merkt (Brain-Wallets) oder dass man den Private-Key in der einen oder anderen Form offline gespeichert hat, bspw. auf einem USB-Stick oder einem nicht mit dem Internet verbundenen PC.

Eine besonders ausgeklügelte Gruppe von Cold-Storages sind Hardware-Wallets, bei denen man technisch gesehen etwas komplexer vorgeht als beim oben beschriebenen USB-Stick und so

die Usability und die Sicherheit erhöht. Im späteren Verlauf werden unterschiedliche Typen von Cold-Storages beschrieben. Hier kann man schon eine gemeinsame positive Sache festhalten: es ist zwar auf der einen Seite schwierig, an das Geld zu kommen, aber das Deponieren von Geld im Cold-Storage ist eine ganz normale Transaktion mit dem zum Cold-Storage gehörenden Public-Key als Zieladresse. Hintergrund dafür ist, dass ein Cold-Storage, wie jede Wallet, keine Bitcoin enthält.

Auch wenn man es gerne anders liest, soll man sich merken: Bitcoin, die von der Blockchain getrennt werden würden (wie das auch immer gehen soll), würden keine Bitcoin mehr sein. Was ein Cold-Storage offline speichert sind lediglich die Zugangsinformationen zum Wallet.

WIE ERSTELLE ICH EIN WALLET?

Wie komme ich nun zu einem Wallet? Wie im weiteren Verlauf des Kapitels dargestellt, existieren hier verschiedene Möglichkeiten. Das Essentielle ist aber immer dasselbe: generiere einen einmaligen Private-Key. Was das aber konkret heißt ist, abhängig vom jeweiligen Wallet-Typ. Diese wollen wir hier kurz darstellen.

ONLINE-WALLET

Für die meisten ist das der erste Schritt in die Wallet-Welt. Auf verschiedenen Seiten kann man sich eines einrichten, Links zu diesen Wallet-Anbietern finden sich in dem Premium-Bereich zu diesem Buch. Der Prozess ist recht einfach - auch wenn es natürlich Unterschiede im Komplexitätsgrad gibt. Letztlich sind Online-

Wallets Web-Services, die sich oft um den Private-Key Deines Wallets kümmern. Sie sind von jedem internetfähigen Gerät oft ohne zusätzliche Apps zugänglich.

Neben dem einfachen Erstellen eines Wallets, dass sich bei Online-Wallets nicht sonderlich von einer Registrierung bei einem Online-Service unterscheidet, ist eine gemeinsame positive Sache, dass deine Privatsphäre auf der Blockchain geschützt ist - man wird dort Deine Transaktionen von verschiedensten Adressen aus sehen können. Das Ganze nennt sich dann Rotating-Address.

Leider ist sowas auch unseren werten Damen und Herren Regierenden der EU aufgefallen, weshalb diese bei Online-Wallets auf eine Know Your Customer Policy (KYC) drängen. Für deine

miesen Geldwäsche-Aktionen, dein Verticken von Drogen, sprich, etwaige illegale Pläne, sind damit Online-Wallets trotz der Rotating-Address nutzlos. Aber in einem pseudonymen System wie Bitcoin kann nicht nur das LKA oder Hacker, sondern prinzipiell jeder auf die Verbindung Bitcoin-Adresse - Person kommen. Und vielleicht will man einfach nicht, dass theoretisch die ganze Welt weiß, dass man dieses oder jenes gekauft hat.

Eine wirklich negative Sache bei vielen Online-Wallets ist, dass sie oft volle Kontrolle über dein Geld haben. Anders als bei einer Bank gibt es darüber hinaus auch keine Versicherung im Fall des Verlustes von Bitcoin. Selbst jene Online-Wallets, die für etwaige Transaktionen auf jeden Fall eine Bestätigung vom Nutzer benötigen, sind zentralisierte Dienstleister, sprich, man braucht auf

jeden Fall eine stark zentralisierte Third-Party.

In der Hinsicht kann man Web-Wallets als sehr gute Transfer-Stationen sehen; gerade Coinbase ist bezüglich der Möglichkeit, Bitcoin für eine Handvoll Dollar (oder Euro) zu kaufen, hier zu erwähnen. Es ist jedoch äußerst empfehlenswert, langfristig auf eine andere Lösung umzusteigen.

MOBILE-WALLET

In der heutigen Zeit ist alles mobil. Wir können Zahlungen über eine Paypal-App initiieren oder Transaktionen mittels der App der Bank Deines Vertrauens in die Wege leiten. Natürlich geht das auch “in Bitcoin” und so gibt es eine Menge an mobilen Wallets. Anders als im Fall der Online-Wallets ist hier (größtenteils) der Besitzer im

Besitz des Private-Key. Es gibt sogar Wallets, die NFC unterstützen, sodass ein Ablegen des Mobilephones an eine bestimmte Stelle eine Bitcoin - Transaktion initiieren kann.

Mobile-Wallets speichern oft einen Teil der Blockchain auf dem Device und synchronisieren diesen mit Nodes des Vertrauens, ein Verfahren, dass als Simplified-Payment-Verification bekannt ist. Natürlich muss einem hier klar sein, dass man auch z.T. auf eine Third-Party angewiesen ist, aber deutlich weniger als bei Exchanges oder Online-Wallets. Schick ist - wie bei Online-Wallets - dass Mobile-Wallets oft mit Rotating-Adresses arbeiten und so ein Mindestmaß an Privatsphäre garantieren. Oft nutzen Wallets die Device-eigenen Sicherheitsmaßnahmen, so sind Wallets auf dem iPhone mit iCloud verbunden, so dass man im Fall des Verlustes /

Diebstahls eines Smartphones trotzdem beruhigt schlafen kann.

Schließlich hat jedes Mobile-Wallet, das Zugriff zur Kamera hat, die Möglichkeit, via QR-Code einen Public-Key einzulesen. Einfach einscannen und bezahlen - die Welt kann so einfach sein!

Insgesamt sind Mobile-Wallets eine feine Sache, mit der man "On The Go" sein Geld verwalten und einsehen kann. Wir können hier das **Jaxx** oder **Bread** Wallet empfehlen.

PAPER-WALLET

Oft geht es nicht um das schnelle Zahlen von Geld. Man will seine mühsam verdienten Bitcoin irgendwo sicher verwahren - mit

möglichst wenig Aufwand, versteht sich.

Die Möglichkeit soll sicher, leicht und billig sein - womit wir beim Paper-Wallet wären . Ein Paper-Wallet ist eigentlich nur ein Zettel, auf dem Public- und Private-Key stehen. Man kann solche Wallets schnell selber erstellen, nach Senden von Geld auf dieses Wallet ist das Geld in dem Paper-Wallet “gespeichert” - natürlich nicht auf dem Papier, sondern in der Blockchain, aber nur jene, die die Information auf dem Blatt Papier haben, können an die Bitcoins ran. Anständige Services speichern diesen Private-Key natürlich nirgendwo.

Wie oben schon gesagt ist das Transferieren von BTC auf ein Paper-Wallet recht simpel: einfach an die entsprechende Adresse

Geld schicken! Das Geld vom Paper-Wallet zu bekommen ist etwas komplexer - soll es ja aber auch sein, schließlich ist ein Paper-Wallet kein Giro-Konto. Man importiert dazu den Private-Key, um damit ein neues Wallet, bspw. ein Online-Wallet, zu schaffen. Nun wird der gesamte auf dem Paper-Wallet gespeicherte Betrag dorthin transferiert. Zwar soll man das auch partiell können, jedoch führte in der Vergangenheit das oft zum Verlust der restlichen Coins.

Merken wir uns: ein Paper-Wallet ist KEIN Ersatz für ein Online-Wallet oder ein Mobile-Wallet! Es ist eher vergleichbar mit einer Geldanlage in Papierform.

Eine wichtige Sache bei Paper-Wallets ist, dass dieses (ausgedruckte) Blatt Papier das einzige ist, was einen Besitzer der

mit dem Wallet assoziierten BTC von jemand anderem unterscheidet: Wer es bei Dir zuhause findet (und entweder entwendet oder fotografiert) kann an dein Geld kommen. Deshalb sollte man diese Paper-Wallets wirklich sicher lagern.

BRAIN-WALLET

Die vorher vorgestellte Problematik hinsichtlich des Diebstahls der Bitcoin in einem Paper-Wallet hat zu einer weiteren Entwicklung geführt - dem Brain-Wallet. Dieses Wallet wird hier der Vollständigkeit halber und als Warnung vorgestellt.

Der Gedanke war durchaus gut: man steht bei Paper-Wallets vor dem Dilemma, dass der Schlüssel zum Geld auf einem theoretisch für jeden Menschen einsehbaren Blatt Papier steht. Es gibt weder

eine Zwei-Wege-Authentifizierung noch ein zentrale Autorität, die einem im Fall des Diebstahls das Geld zurückerstatten kann. Wenn man nun dafür sorgen könnte, dass dieses Blatt Papier gar nicht erst existiert?

Wie sich herausstellt kann man das tun: man kann letztlich fast eine beliebige Zeichenkette in einen Private-Key umwandeln. So kann man dann statt diesem nicht ganz einfach zu merkendem Kauderwelsch einen entsprechenden Passphrase auswendig lernen.

Diesen Satz kann man nun mit einer Seed als zusätzlichem Randomizer (wie z.B. BrainWallet.io) in einen Private-Key und einen Public-Key umwandeln. Andere Methoden lassen dich nicht den Passphrase erfinden (allein schon, weil das extrem unsicher ist),

sondern generieren selbst eine Liste an Wörtern. Diese sich zu merken ist natürlich nicht ganz leicht, aber deutlich leichter, als einen ewig langen Private-Key auswendig zu lernen!

So, von der Idee her ist damit ein Wallet generiert, dass keinen anderen Counterpart als das Gedächtnis des Besitzers hat. Klingt schick, oder?

Leider ist das menschliche Gehirn keine gute Entropiequelle. Schon allein der Fokus auf verständlichen Text - ja, auch mit dem einen oder anderen Sonderzeichen - begrenzt die Anzahl der möglichen Brain-Wallets in einer Weise, dass White Hat Hacker Ryan Castellucci auf der Defcon23 die Knackbarkeit von Brain-Wallets zeigen konnte. Zusammenfassung: Nette Idee, aber Finger davon

lassen, wenn es um Beträge geht, die man nicht verlieren will.

HARDWARE-WALLET

Ich habe im Zusammenhang mit Cold-Storages schon über Hardware-Wallets gesprochen, die eigentliche Diskussion wollte ich aber erst führen, wenn andere Wallet-Typen schon bekannt sind.

Wir wissen schon mal, dass ein Hardware Wallet den Private-Key offline speichert. Das macht ein Paper-Wallet auch, warum sollte ich also deutlich mehr Geld ausgeben?

Nun, bei einem Paper-Wallet haben wir das Problem, dass der Zettel, den wir ausgedruckt irgendwo zu liegen haben, von jedem Menschen nutzbar ist. Einmal geklaut ist das Geld weg. Außerdem ist das Geld weg, wenn jemand den Zettel wegwarf - ohne wenn

und aber ist es dann unzugänglich. Schließlich mag man vielleicht ein Komplettsystem haben, bei dem man nicht das Paper-Wallet in ein Online-Wallet importieren muss. Auf diese Probleme haben Hardware-Wallets Antworten. Sie können bspw. so konzipiert sein, dass man nur in Zusammenarbeit mit einem Programm an das Geld kommt und dieses Programm eine Zwei-Wege-Authentifizierung benötigt. Dann würde ein Dieb nicht mehr einfach das Hardware-Wallet, sondern auch das Smartphone bzw. andere zur Bestätigung benutzte Medien benötigen.

Die Private-Keys sind bei einem Hardware-Wallet meistens verschlüsselt in einem abgesicherten Bereich, der nicht einfach von nicht lizenzierten Methoden her zugänglich ist. Man braucht sich also, obwohl man ihn besitzt, nicht um den Private-Key zu

kümmern. Schließlich ist der Zugang zum Hardware-Wallet selbst auch oft durch eine Pin gesichert. Ein Dieb benötigt also das Hardware-Wallet, Deine Pin und ggf. Dein Smartphone.

Nun kann einem auch ein Hardware-Wallet gestohlen werden, es kann auch verloren gehen etc. Hier glänzen Wallets durch einen Recovery-Mechanismus, der an Brain-Wallets erinnert: im Zuge der Wallet-Erstellung wird ein Security-Passphrase generiert, den man nutzen kann, um das Wallet auf einem anderen Device derselben Firma wiederherzustellen.

Hardware-Wallets gibt es in verschiedenen Ausführungen: sie können an USB-Sticks erinnernde Smartcards sein, sie können wie Kreditkarten aussehen oder wie Stand-Alone Boxen. Als

bekannteste Anbieter wären hier **Ledger** oder **TREZOR** zu nennen.

BITCOIN CORE

Am Ende des Kapitels reden wir über die ursprüngliche und aufwändigste Alternative für ein Wallet: man kann natürlich auch einen kompletten Bitcoin-Client, eine Node betreiben.

Das ist keine Möglichkeit, die ich jemandem, der mal in Bitcoin reinschnuppern will, empfehlen würde - zur Node gehört der Download der gesamten Blockchain. Und hier reden wir von einer Datenmenge, die 100 GB übersteigt. Dafür ist man wirklich unabhängig: man ist Teil der Blockchain und selbst wenn die anderen Nodes vom Netz genommen sind, wird Dank Deines Bitcoin Core Clients Bitcoin weiter existieren.

Man ist dann von niemandem abhängig - kein Wallet-Anbieter, ja, nicht einmal andere Nodes können Dir schaden. In der Hinsicht ist das das sicherste und stabilste aller Wallets.

Das Bitcoin Core-Wallet ist eher für die Hardliner. Leute, die mal in Bitcoin reinschnuppern wollen wären damit hoffnungslos überfordert. Falls man aber Gefallen an Bitcoin findet sollte man überlegen, einen Bitcoin Core-Client aufzusetzen: man hat dann nicht nur das sicherste aller Wallets, nein, man unterstützt das Bitcoin-Netzwerk, indem man es dezentraler macht. Außerdem kann man erst dann beim alten Spruch "Be your own Bank" mit vollster Zustimmung "Jepp" sagen - alle anderen Methoden vertrauen halt immer noch einem Middle-Man, auch wenn dieser dezentral ist.

WIE SICHER IST MEIN WALLET?

Wie schon weiter oben gesagt ist der Private-Key mit seinen 64 Zeichen sehr, sehr lang. 256 bit, um genau zu sein. Das bedeutet, dass es 2^{256} verschiedene Kombinationen gibt, was ungefähr einer eins mit 77 Nullen entspricht. Um abzuschätzen, wie wahrscheinlich es ist, ein Wallet mittels einem Trial-and-Error-Verfahren zu knacken, wagen wir ein Gedankenexperiment. Sagen wir mal, wir würden alle jemals generierten Bitcoin (21 Millionen BTC, wie im Kapitel Bitcoin-Mining beschrieben wurde) derart verteilen, dass jedes einzelne Satoshi in eine eigene Wallet kommt. Das würde dann bedeuten, dass insgesamt 2.1 Billionen Wallets mit jeweils einem Satoshi gefüllt wären, die Bitcoin wären also maximal verteilt. Selbst dann würden immer noch 10^{52} leere Wallets

vorhanden sein, die Wahrscheinlichkeit, einen Private-Key (mit einem Satoshi!) zu finden wäre also ca. $1/10^{52}$.

Der aktuell schnellste Computer - Tianhe-2 - kann $3 \cdot 10^{16}$ Operationen pro Sekunde abarbeiten. Das bedeutet, dass pro Jahr ca. 10^{24} Operationen durchgeführt werden können. Dieser Computer würde immer noch durchschnittlich $1 \cdot 10^{28}$ Jahre (10 Oktillionen Jahre) benötigen - um schließlich an einen Satoshi zu kommen.

Um einen Vergleich zu haben: das Universum ist circa 20 Milliarden Jahre alt, d.h. $2 \cdot 10^{10}$ Jahre. Das Gesamtalter des Universums passt $5 \cdot 10^{17}$ mal in diese Zeit!

Das wäre ein Brute-Force-Ansatz, aber wie steht es um den Mechanismus? Da dieser deterministisch ist müsste man ihn auch

umkehren können, oder? Sprich: da man aus einem Private-Key einen Public-Key generieren kann, müsste man aus einem Public-Key auch einen Private-Key generieren können.

Ohne hier zu sehr ins Detail zu gehen gehört der Verschlüsselungsmechanismus hinter Bitcoin (SHA-256) zu einer Gruppe an Verschlüsselungsfunktionen, die darauf angelegt sind, umkehrbar (bzw. möglichst schwer umkehrbar) zu sein. Wir können uns das - sehr plump ausgedrückt - so ähnlich vorstellen wie das Zerschlagen einer Teetasse, die vom Tisch fällt. Die Funktion ist eindeutig (intakte Tasse + Tischrand \rightarrow Scherben), aber die komplette Umkehrfunktion ist unbekannt (Scherben + ??? \rightarrow intakte Tasse), die Scherben zusammenkleben gibt uns zwar wieder die Tasse aber keine komplett intakte Tasse, wir sehen weiterhin die

Stellen, wo sie kaputt ging.

Natürlich ist die Sorge, dass SHA-256 irgendwann geknackt wird, bei einigen Leuten vorhanden. Wir sollten aber im Hinterkopf haben, dass erstens, wie dargestellt, die Verschlüsselungsmechanismen darauf angelegt sind, unumkehrbar zu sein, zweitens kann man im Hinterkopf haben, dass SHA256 und andere SHA-Verschlüsselungen viele Anwendungsbereiche haben (Überprüfung, dass herunter geladene Dateien nicht corrupted sind, PGP...) - es sind Methoden, die sich bisher bewährt haben. Diese Methoden werden nicht nur von Bitcoin-Enthusiasten ständig überprüft - falls ein Verdacht aufkommen sollte, dass SHA-256 unsicher ist, wird das sehr schnell bekannt - und wie andere digitale Währungen zeigen kann man auch auf anderen Verschlüsselungen

eine Währung aufbauen - Bitcoin würde dann halt überarbeitet werden. Nachdem wir über die systemimmanenten Risiken sprachen, darf nicht verschwiegen werden, was in den anderen Unterkapiteln angerissen wurde: ein Wallet ist nur so sicher wie seine Implementierung und sein Anwender. Egal wie sicher Bitcoin ist - es ist eine schlechte Idee, massig Geld auf einem windigen Exchange liegen zu lassen oder ein Paper Wallet mit allem Geld offen mit sich zu führen. Die Eigenverantwortung über das eigene Geld, die man mit Bitcoin sich erkaufte, bedeutet, dass man sich über die Pros und Kontras hinsichtlich eines Wallets informiert und überlegt, was man selbst zur Sicherheit seines Geldes tun kann. Dieses Buch zu lesen ist ein erster Schritt. Wir planen zu aktuellen Wallets im VIP-Bereich Reviews und Informationen zu

verschiedenen Wallets zu posten und euch so zu informieren. Außerdem werden auf BTC-Echo neue Wallets vorgestellt.

KAPITEL 7 BITCOIN

KAUFEN UND

VERKAUFEN

Der Kauf bzw. Verkauf von Bitcoins war in der Vergangenheit und in den ersten Jahren der Bitcoin-Ära ein echtes Abenteuer. Die meisten Nutzer schürften bei der damals noch niedrigen Schwierigkeit ohnehin ihre Bitcoins meist selbst. Nur mit steigenden und den zum Mining benötigten Rechenkapazitäten, die der heimische Computer nicht mehr leisten konnte, wurde das Private-Mining oftmals unrentabel und die Nutzer begannen allmählich nach Möglichkeiten zu suchen, Bitcoins zu kaufen.

Zu Zeiten des ersten Bitcoin-Booms schossen die Handelsplattformen wie Pilze aus dem Boden. Die ersten Kurssprünge lösten eine regelrechte Goldgräberstimmung aus und jeder wollte die schnelle Mark verdienen – die selbsternannten „Börsen“, genauso wie die Käufer und Verkäufer. Es muss nicht erwähnt werden, dass es in einer solchen Wild-Wild-West Umgebung viele schwarze Schafe unter den Handelsplattformen gab. Die Plattformen, die es hingegen ernst meinten, konnten oftmals keinen angemessenen Sicherheitsstandard bieten und somit war auch das Schlachtfest der Hacker eröffnet. Viele Börsen wurden Opfer solcher Attacken - auch heute noch. Deshalb sollte man, wie im Kapitel über Bitcoin Wallets dargestellt, sich gut überlegen wo man die digitale Währung kauft und noch viel wichtiger: sicher

aufbewahrt.

Auch die nachvollziehbare Unwissenheit der Banken über die neuen digitalen Währungen führte zu zahlreichen Problemen. Viele Börsen taten sich enorm schwer ein Bankkonto für ihr neues Geschäftsfeld zu finden. Entweder wurden die Konten nur wenige Tage später geschlossen oder aber gesperrt und das Guthaben der Nutzer eingefroren – hier laufen bis heute Verfahren zahlreicher „Opfer“. Oftmals wurden die Überweisungen von den Banken aber auch ohne jeglichen Grund einfach abgelehnt – einige von euch werden sich vielleicht erinnern.

Es war eine wirklich abenteuerliche Zeit, die vielen Leuten vermutlich einen Haufen Geld eingebracht hat und anderen

wiederum eine Menge Geld gekostet haben wird. Auch hier wieder ein Appell an alle Nutzer: Investiere nur so viel Geld wie du auch verkraften kannst zu verlieren.

Der Markt hat viele Handelsplattformen kommen und gehen sehen. Aber die wilde Zeit hatte auch etwas Gutes, was wir bis heute beobachten: Es wurde sehr schnell die Spreu vom Weizen getrennt.

Sicherlich, auch heute kommt es immer wieder zu Hackerangriffen, aber die meisten Börsen sind vorbereitet und bewahren nur noch einen Bruchteil der Guthaben in sogenannten „Hot-Wallets“ (Online-Wallets) auf. Der Löwenanteil der Bitcoin wird schon fast standardmäßig sicher in „Cold-Wallets“, also Offline-Wallets ohne jegliche Verbindung zum Internet verwahrt. Somit sind die Schäden

im Falle eines „erfolgreichen“ Hackerangriffs meist überschaubar und von den Börsen versichert.

Seriöse Plattformen setzen alles daran das Guthaben und die Transaktionen der Nutzer mit höchsten Sicherheitsstandards abzusichern.

MÖGLICHKEITEN BITCOIN ZU KAUFEN

Wer heute Bitcoin oder eine andere digitale Währung käuflich erwerben will, hat dazu mehrere Möglichkeiten. Im nachfolgenden Abschnitt stellen wir verschiedene Wege vor, die wir als sicher, schnell und effizient erachten. Für welche Möglichkeit ihr euch letztendlich entscheidet liegt an euren Vorzügen in Sachen Schnelligkeit, Sicherheit und dem Maß an Anonymität.

BITCOIN-BÖRSEN

Bitcoin-Börsen sind der Klassiker für den Kauf bzw. Verkauf von Bitcoin. Das Prinzip ist ganz einfach und wie an einer Börse so üblich: Verkäufer bieten ihre Bitcoins für einen bestimmten Preis zum Verkauf an und Käufer geben das jeweilige Angebot ab. Findet

sich hier eine Übereinstimmung, kommt der Handel (Trade) zustande und die Bitcoins wechseln ihren Besitzer.

Bei den Bitcoin-Börsen wird meist das Guthaben in Euro oder Bitcoin (BTC) auf die Börse eingezahlt. Das Guthaben befindet sich also in der Verantwortlichkeit der Online-Börse und sollte daher gut vor Hackerangriffen abgesichert sein. Aber auch hier gibt es Unterschiede:

Manche Börsen verwalten beide Guthaben (BTC und EUR) online, andere wiederum verwahren nur die Bitcoin-Bestände und überlassen den Geldaustausch den beiden Parteien (Käufer und Verkäufer).

Bei der ersten Variante bezahlt der Käufer den Verkäufer direkt mit

seinem zuvor eingezahlten Online-Guthaben. Der Verkäufer erhält den Kaufpreis in Euro also auf seinem Online-Konto gutgeschrieben. Der Käufer erhält im Gegenzug Bitcoin auf seinem Online-Wallet.

Bei der zweiten Variante agiert die Börse lediglich als Treuhänder und als Online-Wallet. Hier treffen sich Käufer und Verkäufer, machen den Deal und die Börse blockiert die gekauften Bitcoins auf Seite des Verkäufers so lange, bis die Gegenseite das Geld über das private Konto direkt an der Verkäufer überwiesen hat. Nach erfolgreicher Überweisung markiert der Verkäufer die Zahlung als „erhalten“ und dem Käufer werden der entsprechende Betrag in BTC auf seinem Online-Wallet gutgeschrieben. Das bekannteste Beispiel ist hier wohl die deutsche Bitcoin-Börse Bitcoin.de.

Die meisten professionellen Trader handeln ausschließlich an Bitcoin-Börsen. Professionelle Trader tätigen an einem Tag nicht selten mehrere hundert Transaktionen. Oftmals voll automatisch und mit Hilfe von Trading-Bots. Zudem bieten einige Börsen eine Stop-Loss Funktion, also einen automatischen Verkauf, bzw. Kauf sobald der Kurs einen bestimmten Wert erreicht. Das ist nur möglich wenn beide Guthaben, Euro und BTC, auf der Börse eingezahlt sind.

Bitcoin-Börsen bieten also einige Vorteile in Sachen Verfügbarkeit und professionellem Trading. Nachteil ist jedoch, dass die Verantwortlichkeit über das Guthaben bei der Börse liegt und diese entsprechend abgesichert sein muss.

BITCOIN-BROKER

Neben den Bitcoin-Börsen etablieren sich zunehmend mehr Bitcoin-Broker am Markt. Bitcoin-Broker bieten anders als bei den Bitcoin-Börsen keine eigenen Wallets oder Online-Konten an und sind somit zu keiner Zeit im Besitz der Nutzer-Guthaben. Der Nutzer kauft nach erfolgreicher Registrierung beim Broker, ähnlich wie in einem Online-Shop, direkt Bitcoin. Je nach gewählter Zahlungsmethode erhält der Nutzer die Bitcoin binnen weniger Minuten in einem von ihm zuvor eigens eingerichteten Bitcoin-Wallet gutgeschrieben.

Bitcoin-Broker agieren als Mittelsmann, d.h. der Nutzer überweist dem Broker den gewünschten Kaufbetrag in EUR und der Broker schickt dem Nutzer im Gegenzug Bitcoin. Die Bitcoin selbst kauft

der Broker in Echtzeit bei großen Onlinebörsen und berechnet dem Nutzer eine geringe Gebühr für diese Dienstleistung. Der Vorteil hier ist die schnelle Verfügbarkeit, je nach Zahlungsmethode (Giropay, Sofort-Überweisung, SEPA oder Kreditkarte) und die direkte Transaktion auf ein eigenes Bitcoin-Wallet.

Einer der bekanntesten deutschsprachigen Bitcoin-Broker ist AnycoinDirect. AnycoinDirect bietet eine Vielzahl an Zahlungsmöglichkeiten und neben Bitcoin auch, Ether, Litecoin, Dogecoin Dash & Co zum Kauf bzw. Verkauf an.

BITCOINS KAUFEN MIT SOFORTÜBERWEISUNG AUF ANYCOINDIRECT

Eine Möglichkeit Bitcoin sehr schnell und unkompliziert zu kaufen bzw. zu verkaufen bietet die Bitcoin Börse [Anycoin Direct](#).

Hier kann der Nutzer nach einer kurzen Anmeldung gleich mit dem Kauf bzw. Verkauf der digitalen Währungen Bitcoin, Litecoin Ether & Co beginnen. Das Besondere an Anycoin Direct ist der Kauf von digitalen Währungen per Sofortüberweisung. Die Plattform verspricht eine Zustellung der Bitcoin direkt nach Zahlungseingang, also innerhalb von nur wenigen Minuten.

Bei den Tests von BTC-Echo hat die gesamte Kaufabwicklung weniger als 10 Minuten gedauert!




REGISTRIERUNG

Eine Registrierung ist sinnvoll und schützt die Verbraucher genauso wie den Händler! Deshalb hat sich Anycoin Direct für eine Quick-Registrierung entschieden. Jede seriöse Börse sollte einen solchen

Prozess anbieten.

Mit einem Klick auf „Registrieren“ gelangt der Nutzer direkt zu der Eingabemaske für die initiale Registrierung. Hier werden zunächst die E-Mail-Adresse, der Vorname, Name und die Adressdaten erfasst:

Registrieren

Haben Sie bereits einen Account? [Anmelden](#) Ihr Account

☐ Geschäftskonto

Abbildung 7: Registrierung Anycoin Direct

Kurz darauf erhält der Nutzer eine E-Mail mit einem einmaligen Token (Schlüssel). Diesen gibt ihr bitte im nachfolgenden Feld ein. Mit einem Klick auf „Aktivieren“ gelangt ihr dann auch schon zum aktivierten Benutzerkonto auf Anycoin Direct:



Konto aktivieren

Können Sie unsere E-Mail nicht finden? Aktivierungsmail erneut
senden

Eine E-Mail wurde versendet an info@btc-echo.de

Token

Aktivieren

MAXIMALBETRÄGE

Zur eigenen Sicherheit und zur Sicherheit der Kunden hat Anycoin Direct ein ausgeklügeltes Verfahren zur Verifizierung und zur Erhöhung der Maximalbeträge entwickelt.

Mit der alleinigen initialen Registrierung kann der Nutzer Bitcoins, Litecoins, Ether Coins usw. für maximal 100 Euro pro Tag, bzw. 250 Euro pro Woche kaufen (Level 1):

Kryptowährung kaufen

Level	Anzahl Transaktionen pro Tag	Maximaler Betrag (Euro) pro Tag	Maximaler Betrag (Euro) pro Woche
Level 1	2	100	250
Level 2	2	400	1000
Level 3	3	1.000	1.900
Level 4	5	1.500	5.000
Level 5.1	5	3.000	25.000

Kryptowährung kaufen (SEPA)

Level	Anzahl Transaktionen pro Tag	Maximaler Betrag (Euro) pro Tag	Maximaler Betrag (Euro) pro Woche
Level 5.1	1	5.000	15.000
Level 5.2	2	15.000	30.000

Kryptowährung verkaufen

Level	Anzahl Transaktionen pro Tag	Maximaler Betrag (Euro) pro Tag	Maximaler Betrag (Euro) pro Woche
Level 1	2	500	1.000
Level 2	2	1.000	3.000
Level 3	3	2.500	5.000
Level 4	5	10.000	25.000
Level 5.1	5	15.000	50.000

Reichen diese Limits nicht aus, dann nehmen Sie bitte Kontakt mit uns auf.

Abbildung 9: Maximalbeträge Anycoin Direct

Mit der Zahlungsmethode Sofortüberweisung könnt ihr bereits im ersten Level Bitcoins kaufen. Level 2 (400 Euro pro Tag) erreicht

ihr automatisch 7 Tage nach der ersten erfolgreichen Transaktion. Um z.B. mit SEPA-Überweisung auf Anycoin Direct bezahlen zu können, müsst ihr euch zunächst für das Level 5.1 freischalten lassen. Das geht recht fix, indem ihr ein Selfie mit eurem Personalausweis macht und Anycoin Direct per Chatfunktion zukommen lasst. Generell empfiehlt sich diese Art der Verifizierung um den maximalen Kauf- bzw. Verkaufsbetrag zu erhöhen:

Level	Bedingungen
Level 1	In den ersten 7 Tagen nach ihrer ersten Transaktion beginnen Sie mit Level 1.
Level 2	7 Tage nach der ersten Transaktion erhält Ihr Account automatisch ein Upgrade auf Level 2.
Level 3	Nach 7 Tagen auf Level 3 können Sie eine Kopie Ihres Personalausweises einsenden. Nach dessen Genehmigung wird Ihr Account auf Level 3 erhöht.
Level 4	Um auf Level 4 zu gelangen, können Sie uns eine Meldebescerigung (Proof of Residence) zuschicken. Nach dessen Genehmigung wird Ihr Account auf Level 4 erhöht.
Level 5.1	Um auf Level 5.1 zu gelangen, können Sie uns ein ID-Selfie über die Webcam in der Chatfunktion auf unserer Website zukommen lassen. Nach dessen Genehmigung wird Ihr Account auf Level 5.1 erhöht.
Level 5.2	Nach Ihrem ersten erfolgreichen SEPA-Auftrag erhält Ihr Account automatisch Level 5.2.

Abbildung 10: Level Anycoin Direct

Mit dem Level 5.1 könnt ihr nicht nur die SEPA Funktion nutzen – ab sofort könnt ihr auch digitale Währungen im Wert von 15.000 Euro pro Tag kaufen bzw. verkaufen. Nach der ersten erfolgreichen Transaktion gelangt ihr automatisch in das Level 5.2

KAUFABWICKLUNG MIT SOFORTÜBERWEISUNG

Nach der erfolgreicher Anmeldung auf Anycoin Direct kann der Kauf von Bitcoin per Sofortüberweisung auch schon beginnen.

Dazu gebt ihr in die Kaufeingabemaske lediglich die gewünschte Anzahl Coins oder den Betrag für den ihr Bitcoin kaufen wollt ein. Die Umrechnung erfolgt automatisch. Danach wählt ihr als Zahlungsmethode „Sofort“ aus und gebt eine gültige Bitcoin-Adresse ein. Dazu benötigt ihr vorab ein Bitcoin-Wallet.

Keine Angst bei der Eingabe der Bitcoin-Adresseingabe – solltet ihr eine ungültige Adresse eingeben wird euch das System direkt darüber informieren:

Nachdem ihr alle Felder zur Kaufabwicklung erfolgreich gefüllt habt und einen Haken zur Akzeptanz der Nutzerbedingungen gesetzt habt, könnt ihr den Kauf mit einem Klick auf „Kaufen“ abschließen. Hierzu gelangt ihr direkt zur sicheren Eingabemaske zur Ausführung einer Sofortüberweisung.

FACE TO FACE

Wer es klassisch und noch anonym mag, kann Bitcoin auch Face to Face "auf der Straße“ kaufen – fast so einfach wie einen Lolly am Kiosk nebenan.

Auf Localbitcoins vereinbaren die Käufer und Verkäufer zuvor online einen Preis und treffen sich dann um den Deal abzuschließen. Hier bezahlt der Käufer direkt vor Ort in Bar und lässt sich die

Bitcoin auf seinem mobilen Wallet vom Verkäufer überweisen – das war`s. Der zuvor festgelegte Kurs dient jedoch lediglich als Indikation. Der finale Preis wird beim eigentlichen Treffen aktuell festgelegt.

Bitte beachtet hier nur, dass der Verkäufer bereits im Vorfeld weiß wie viel Geld ihr mit euch tragen werdet. Ein Treffen nachts um 12 Uhr unter der nächsten Brücke ist hier vielleicht nicht unbedingt empfehlenswert.

KAPITEL 8 MIT BITCOIN BEZAHLEN

Was nützt die ganze Theorie eines ausgeklügelten Systems, wenn man es nicht praktisch nutzen kann? In diesem Kapitel geht es genau deswegen sehr praktisch zur Sache. Wir schauen uns an, wie man nach der Einrichtung eines Wallets mit Bitcoins zahlen kann, welche Tools sich dazu eignen und wo es überhaupt möglich ist, den Einkauf oder die Dienstleistung mit einer Bitcoin-Transaktion zu begleichen.

WER AKZEPTIERT BITCOINS?

Dieses Buch richtet sich vornehmlich an Leser aus Deutschland, der Niederlande, Österreich und der Schweiz, aber selbstverständlich auch an alle weiteren deutschsprachigen Leser. In den deutschsprachigen Regionen sind Bitcoins im stationären Handel bisher nicht weit verbreitet. Das gilt vor allem für Deutschland, hängt aber dennoch stark von der Stadt ab. In Berlin beispielsweise tummeln sich einige Restaurants und Geschäfte, in denen man mit Bitcoins bezahlen kann. In kleineren oder ländlicher gelegenen Städten ist Bitcoin für Ladenbesitzer leider meist ein Fremdwort.

In den Niederlanden spielen Amsterdam und Arnheim mit einer ausgeprägten Bitcoin-Kultur in der ersten Liga der modernen

Geschäfte. Hier finden sich ganze Einkaufsstraßen, in denen man als Kunde fast überall mit Bitcoins bezahlen kann.

Vielleicht haben sie sich bereits beim Lesen der Kapitelüberschrift gewundert, wie wir eine aktuelle und vollständige Liste an Bitcoin Akzeptanzstellen in dieses Buch mit einbauen möchten. Wir werden an dieser Stelle selbstverständlich keine Liste anführen. Stattdessen bieten wir einen entsprechenden Verweis auf die Website:

<http://www.btc-echo.de/bitcoin-akzeptanzstellen/>

Dort findet ihr eine Liste der Bitcoin akzeptierenden Unternehmen. Die Liste stets aktuell gehalten, sodass es nicht sinnvoll wäre, in diesem Buch eine Liste anzuführen, die bei der Drucklegung bereits veraltet wäre.

TOOLS ZUM BEZAHLEN MIT BITCOINS

Welches Tool, bzw. ob man überhaupt eines zur Bezahlung mit Bitcoins nutzt, hängt von der Frage ab, ob man offline oder online einkaufen möchte. Prinzipiell benötigt man als Kunde nämlich meist nur eine Wallet, von der man Bitcoins an den Empfänger senden kann. Wer eine Wallet eingerichtet hat und vom Computer online einen Kauf über Bitcoins abschließt, benötigt dafür meist kein zusätzliches Tool.

Um in stationären Geschäften bezahlen zu können, muss man seine Bitcoins allerdings stets dabeihaben. Schließlich lässt dich der Kellner oder Verkäufer erst gehen, wenn die Bitcoins auf seinem Gerät angekommen sind. Du ahnst es: Eine mobile Wallet muss her,

damit wir die Bitcoins unterwegs mitnehmen können. Nachfolgend wird für jedes der gängigen mobilen Betriebssysteme eine Wallet vorgestellt. Selbstverständlich gibt es in den jeweiligen Downloadstores weitere Alternativen, die den Rahmen dieses Buchs jedoch sprengen würden.

ANDROID

Für Android-Smartphone gibt es die App „Bitcoin-Wallet“ von *Bitcoin Wallet Developers*. Die Wallet ist kostenlos im Playstore erhältlich.

Besonders erfreulich an dieser Wallet-App ist das schlichte Design. Man fühlt sich hier wohl, wenn man unterwegs schnell einmal einen Blick auf die (digitalen) Finanzen werfen möchte. So einfach wie

den Kontostand eines Bankkontos wird der Betrag in Bitcoins angezeigt. Er wird allerdings auch gleich in die Fiat-Währung des Herkunftslands umgerechnet. Als Nutzer sieht man also auch, wie viel „*Geld*“ man in Form von Bitcoin zur Verfügung hat. Praktisch, um gleichzeitig auch größere Kursschwankungen im Auge zu behalten.

Die App kann mehrere Bitcoin-Adressen verwalten und beliebig viele neue Adressen erstellen. Die verwalteten Adressen lassen sich in einer Übersicht anzeigen. Um diese auch sicher aufzubewahren, gibt es die Möglichkeit von Backups. Ein Backup anzufertigen sei an dieser Stelle selbstverständlich empfohlen. Gerade bei Smartphones, die je nach Modell schnell einmal Speicherprobleme verursachen können, sollte man seine Walletdaten exportieren, um

im Notfall auch von anderen Geräten darauf zugreifen zu können.

Bitcoin



mBTC **428.79**

≈ EUR 171.78



● 2. April 21:15
37kz gcp9 fNBu **- 5.00**

Netzwerk-Gebühr - 0.10

≈ EUR - 1.89

● 2. Feb. **+ 89.00**

● 3. Jan. **+ 60.00**

● 2.12.2015 **+ 27.00**

◀ ANFORDERN

SENDEN ▶



Nutzung auf eigene Gefahr. Lies die Sicherheitshinweise.



Abbildung 12: Android Wallet

Fazit: Eine kostenlose App, die vollumfänglich alles mitbringt, was man von einer Wallet App erwartet. Mit ein paar netten Features wie QR-Codes werden zusätzliche Funktionen geliefert, die gerade auf Smartphones sinnvoll sind.

IOS

Beliebt unter Nutzern von iOS Geräten ist die Coinbase-App. Sie bietet ähnliche Features wie die oben vorgestellte Wallet-App für Android-Geräte und sieht sogar noch ein Stück moderner aus.

In der App wird der aktuelle Kontostand und der Gegenwert in Fiat-Währungen wie dem US-Dollar angezeigt. Man kann sich also

einen etwas genaueren Überblick über die Finanzen verschaffen und Währungsschwankungen gleich in die Bewertung mit einbeziehen, wenn man den realen Gegenwert vor Augen hat.



Abbildung 13: Coinbase IOS Wallet

CoinBase möchte gleichzeitig mehr als nur den Status Quo als Wallet-App erreichen. Es scheint, als wolle das Unternehmen eine weiter gefasste Finanzlösung für unterwegs schaffen: Die App ermöglicht es nämlich auch, sein Sparverhalten zu organisieren und z.B. den nächsten Urlaub (finanziell) zu planen.

Die Coinbase-App kann kostenlos aus dem Appstore geladen werden.

WINDOWS-PHONE

Das Angebot an Wallet-Apps für die Windows-Phones sieht bisher noch etwas düster aus. Praktisch alternativlos ist die App im Store kostenlos erhältlich (**Fehler! Linkverweis ungültig.**). Das Layout orientiert sich dabei sehr stark an die eben gesehene Gestaltung der

CoinBase-App. Auch hier wird der aktuelle Guthabenstand (sowohl in BTC, als auch in Euro) auf blauem Hintergrund dargestellt. Ebenso baute man hier das Feature der QR-Codes mit in die App ein. Das hat den entscheidenden Vorteil, dass man nicht erst Bitcoin-Adressen über eine E-Mail austauschen muss, wenn man sich trifft und die Rechnung gleich bezahlen möchte. Stattdessen kann der Sender durch den QR-Code einfach den Public-Key, also die Bitcoin-Adresse seines Gegenübers, mit einem QR-Scanner einscannen.

Die App wird von BitPay entwickelt und vertrieben. BitPay ist ein Zahlungsabwickler, der zum Beispiel auch im Kapitel „Bitcoin akzeptieren“ für Unternehmen vorgestellt wurde. Die App basiert ebenfalls auf der API von BitPay.

ÜBERSICHT: WALLET-APPS FÜR UNTERWEGS

Eine sehr gute Übersicht über die erhältlichen Wallet-Apps und Programme liefert die bitcoin.org Website. Unter <https://bitcoin.org/de/waehlen-sie-ihre-Wallet> sind die wichtigsten Clients aufgelistet und können nach Betriebssystem geordnet angezeigt werden. Sie sind außerdem in die Kategorien „Unterwegs“, „Desktop“, „Hardware“, „Web“ unterteilt. Bei entsprechender Auswahl schlägt ihnen das Tool gleich ein paar passende Wallet Programme vor.

KAPITEL 9 BITCOIN

AKZEPTANZ

GRÜNDE FÜR DIE INTEGRATION VON BITCOIN

Zunächst einmal stellt sich die Frage, ob die Integration einer weiteren Bezahlmethode in den Onlineshop oder den stationären Handel überhaupt sinnvoll ist. Die Aufnahme einer weiteren Zahlungsmöglichkeit bedeutet für Unternehmen zu Beginn einen zusätzlichen Aufwand und scheint, das Problem der ohnehin schon undurchsichtigen Zahlungsflüsse nicht wirklich zu lösen. Allerdings nehmen Zahlungsabwickler, die sich auf die Abwicklung von Bitcoin Zahlungen spezialisiert haben,

Unternehmen den größten Teil der Arbeit ab und können diese Prozesse automatisieren.

Andererseits bieten digitale Währungen im Speziellen einige Vorteile gegenüber klassischen Bezahlvarianten, die Unternehmen zum beidseitigen Vorteil nutzen können.

ERWEITERUNG DER ZIELGRUPPE

Unter den Nutzern von Bitcoin sind besonders viele Menschen unterwegs, die sich für das System als solches interessieren und es nach Möglichkeit selbst unterstützen. Die Unterstützung leisten die Bitcoiner durch den Einsatz der Währung an möglichst allen Orten, an denen er möglich ist.

Ein Unternehmen, das Bitcoin als Zahlungsmethode integriert hat,

sammelt dabei gleich Pluspunkte bei einer wachsenden Gruppe von Bitcoin-Enthusiasten. Die Menge an Akzeptanzstellen ist im deutschsprachigen Raum bisher sehr gering, sodass man mit Bitcoins einen hohen Marketingeffekt erzielen kann.

Bisher hat nur ein Bruchteil der Onlineshops Bitcoin integriert, sodass man mit diesem Schritt nach wie vor eine Pole-Position im Wettbewerb erzielen kann.

Im ersten Teil des Buchs wurde die Sicht der Bitcoin-Nutzer verdeutlicht. Genau auf diese erwähnten Vorteile, die einem Nutzer gegenüber einer herkömmlichen Kreditkartenzahlung oder Überweisung entstehen, kommen wir an diesem Punkt zu sprechen: Gibt es zwei sehr ähnliche Produkte in unterschiedlichen Shops, die

sich ebenfalls sehr ähnlich sind, allerdings nur einer der beiden Anbieter Bitcoin-Zahlungen entgegennimmt, dann kann dies mit hoher Wahrscheinlichkeit das ausschlaggebende Kriterium für einen Bitcoin-Nutzer sein, sich für das Geschäft mit Bitcoin-Zahlungsmöglichkeit zu entscheiden.

GERINGE TRANSAKTIONSgebÜHR

Bitcoin-Transaktionen verlangen für die Abwicklung von Natur aus nur sehr geringe Gebühren. Setzt man für die Verarbeitung der Bitcoin-Zahlungen einen Drittanbieter-Service ein, entstehen zwar zusätzliche Gebühren, die allerdings im Vergleich zu den Kosten einer Kreditkartenzahlung nach wie vor vorteilhaft sind.

Das Unternehmen wird nur sehr gering durch Transaktionsgebühren

belastet. Ein Problem ist hingegen, dass bei Bitcoin-Transaktionen immer der Sender die Gebühren bezahlt. Deswegen zwingt man den Kunden leider dazu, die Transaktion auf seine Kosten durchzuführen. Da wir in diesem Fall von Centbeträgen sprechen, geht es weniger um einen großen Verlust, den der Kunde erleidet, sondern eher um die Tatsache, dass er überhaupt etwas dazuzahlen muss. Als Geschäftsbetreiber kann man sich sicher denken, dass auch dies schon ein (wenn auch nur kleines) negatives Gefühl hervorrufen könnte.

Um diesen negativen Effekt zu umgehen, kann man auf Käufe mit Bitcoin-Zahlung einen Skonto gewähren. Diesen gewährt man schließlich auch bei schnellen Bezahlungen, die bei Bitcoins nun einmal fester Bestandteil sind, insofern der Kunde die Transaktion

sofort durchführt (s. u. Schnelligkeit).

ZAHLUNGSSICHERHEIT

Anders als bei Zahlungen wie bspw. dem Lastschriftverfahren können Bitcoin Zahlungen nicht storniert werden. Sind sie erst einmal vom System erfasst und entsprechend von den Minern verarbeitet worden, ist die Transaktion unwiderruflich in der Blockchain verankert und kann nur rückgängig gemacht werden, indem der Empfänger den Betrag manuell zurückschickt.

Als Empfänger einer Zahlung untersteht man folglich nicht dem Stornorisiko, weil die Bitcoin Transaktion rein technisch abläuft und nicht etwa eine Dritte Instanz wie eine Bank einen Einfluss darauf hat und die Transaktion ggf. auf Kundenwunsch stornieren

kann.

Findet die Bitcoin-Transaktion ohne einen Vermittler statt, ist der Empfänger nach der Transaktion im Besitz der Bitcoins. Anders ist die Situation allerdings, wenn ein Zahlungsabwickler (s.u.) zum Einsatz kommt, der die Bitcoin-Zahlungen als dritte Partei abwickelt. In diesem Fall liegt das Vertrauen des Unternehmens letztlich wieder bei diesem Zahlungsabwickler, auf dessen Auszahlung der Umsätze man angewiesen ist.

INTERNATIONALITÄT

Je nachdem, welche Art von Unternehmen den Bitcoin als Zahlungsmethode integriert, ist die Differenzierung nach Kundenherkunft relevant. Im Falle eines Onlineshops für digitale

Produkte kann es fatale Folgen haben, wenn beispielsweise nur Banküberweisungen akzeptiert werden. Kunden aus anderen Ländern als dem Firmensitz würden damit sehr benachteiligt, wenn nicht sogar ausgegrenzt, werden. Entweder, weil es ein so hoher Aufwand ist, eine internationale Überweisung vom Land des Käufers zum Verkäuferland durchzuführen oder schlicht wegen der hohen Gebühren, die auf den Kunden selbst zukommen. Leider sind die universellen Zahlungsmöglichkeiten, die man weltweit einsetzen kann, sehr beschränkt und hauptsächlich auf Kreditkarten fokussiert.

Bitcoins hingegen sind ein einheitliches System, dass auf der ganzen Welt demselben Schema folgt und überall auf dieselbe Weise verwendet wird. Jeder, der Bitcoins besitzt, kann mit Bitcoins

bezahlen. Allerdings kann nicht jeder, der eine Menge US-Dollar besitzt, in einem europäischen Shop (ohne horrende Gebühren) in Euro bezahlen. Wer digitale Produkte vertreibt und Bitcoin als zusätzliche Zahlungsmöglichkeit aufnimmt, kann somit möglicherweise ganz neue Zielgruppen ansprechen.

SCHNELLIGKEIT

Die Ausführung einer Bitcoin-Transaktion dauert nur wenige Minuten. Aufgrund der erwähnten Zahlungssicherheit kann sich ein Unternehmen also nach Durchführung der Transaktion sicher sein, dass der gezahlte Betrag sich wirklich im Besitz des Empfängers befindet. Die Transaktion kann insgesamt schneller durchgeführt werden als beispielsweise über den Weg einer Überweisung und ist

nicht dem Risiko ausgesetzt, dass sie innerhalb der nächsten sechs Wochen rückgängig gemacht werden kann (wie eine Lastschriftzahlung).

Diese Schnelligkeit der Zahlung kommt wiederum der Abwicklung des Bestellvorgangs zu Gute. Der Kunde erhält das gewünschte Produkt deutlich schneller, insbesondere dann, wenn es sich um einen Kauf über unterschiedliche Staaten handelt. In diesem Punkt ist ein Shop mit Bitcoin-Akzeptanz also vielen alternativen Zahlungsmethoden wie Lastschrift, Überweisung und Rechnung überlegen.

FAZIT:

Bitcoins werden von vielen Nutzern als Lifestyle gelebt, der ihnen

neue Möglichkeiten bietet. Die Nutzer sind stark daran interessiert, diese Bewegung der digitalen Währungen zu unterstützen und bewerten die Akzeptanz von Bitcoins deswegen teilweise als ausschlaggebend.

Daher gibt es durchaus Kunden, die sich auf Grundlage der Zahlungsmöglichkeit für einen Shop entscheiden. Auch der Effekt des Ausprobierens ist nicht zu unterschätzen. Viele Bitcoin-Nutzer möchten einfach einmal herausfinden, wie es ist, im echten Leben mit der digitalen Währung zu bezahlen. Je nach Preiskategorie des angebotenen Produkts ist es kein seltenes Szenario, dass ein Kunde ein Produkt kauft, das er nicht unbedingt benötigt, aber gerne mit Bitcoins bezahlt.

Tipp: Mit Bitcoin-Zahlungen werben

Wie oben beschrieben, kann die Unterstützung von Bitcoin-Zahlungen maßgeblich für die Kaufentscheidung sein. Deshalb sollte man die Kunden explizit auf die Bezahlungsmöglichkeit hinweisen und das Marketingpotenzial ausschöpfen, das Bitcoins mit sich bringen.

Stationärer Handel

Klein, aber wirkungsvoll: Den eigenen Betrieb sollte man sichtbar mit Hinweisen ausstatten, dass hier Bitcoins entgegengenommen werden. Im Internet kann man sich Sticker & Aufkleber mit Aufschriften wie „*Bitcoin Accepted here*“ oder dem klassischen Bitcoin Logo bestellen.

Die Sticker sehen zunächst unscheinbar aus, können aber extrem wirkungsvoll sein. Jeder Bitcoin-Nutzer freut sich über solche Sticker. Ein potenzieller Kunde (Bitcoin-Nutzer), der zufällig an einem Café vorbeikommt und dem in derselben Straße etliche weitere Gastronomien zur Verfügung stehen, wird jene mit Bitcoin-Akzeptanz deutlich wichtiger wahrnehmen. Ein spontaner Blick auf das Bitcoin-Logo an der Fensterscheibe wird schnell zum ausschlaggebenden Kaufkriterium.

Tatsächlich sind einige Gastronomien nur dadurch bekannt geworden, dass sie Bitcoins akzeptierten. Sie gehörten zu den ersten Unternehmen. Touristen, die bereits davon gehört hatten, und zufällig in der Stadt waren, besuchten also gerne die besagten Restaurants, um die damals extrem seltene Möglichkeit zu nutzen,

seine Bitcoins im realen Leben einzusetzen. In Berlin konnten sich gewisse Gaststätten dadurch ein riesiges Image aufbauen und wurden bundesweit bekannt. Ich erinnere mich nach wie vor an den Namen des Restaurants, dass ich vor Jahren (!) einmal gehört, allerdings nie besucht habe. Dieser Wiedererkennungswert (der sich tatsächlich bestätigt hat) ist wirklich nur auf die Akzeptanz von Bitcoin zurückzuführen, weil die besagte Gaststätte damals eine der ersten Akzeptanzstellen war und so über etliche Blogartikel, Bücher und Medienberichte bekannt wurde.

Mit basalen Accessoires (Aufkleber, Schilder und Fußmatten), die zunächst primitiv scheinen, kann man sich als Unternehmen also eine beachtliche Marke aufbauen.

KOSTENLOSES ONLINEMARKETING À LA BITCOIN

Ein Unternehmen, das Bitcoins akzeptiert, hebt sich allein durch die Zahlungsmethode vom Wettbewerb ab. Im Internet gibt es Verzeichnisse, die genau solche Unternehmen listen und Karten erstellen, auf denen alle Akzeptanzstellen zu sehen sind. An dieser Stelle werden zwei Möglichkeiten des Onlinemarketings erklärt:

COINMAP

Die Coinmap ist ein Geotool, in dem alle Geschäfte erfasst werden, in denen man mit Bitcoins bezahlen kann. Besucher können sich Bitcoin-Akzeptanzstellen in ihrer Umgebung anzeigen lassen und diese nach Kategorien ordnen.

Die Website mit der Coinmap ist unter coinmap.org erreichbar.

Zudem gibt es die Möglichkeit, den Shop kostenpflichtig zu promoten. Das Unternehmen wird dann in den Suchergebnissen weiter vorne angezeigt und hervorgehoben. Allerdings lohnt sich die Promotion wahrscheinlich erst dann, wenn es im näheren Umfeld eine große Konkurrenz an Bitcoin-Shops gibt. Weitere Informationen zur Coinmap Promotion findet man unter <http://coinmap.org/promote>

BTC-ECHO VERZEICHNIS

Im BTC-ECHO Verzeichnis werden Bitcoin-Shops ebenfalls kostenlos gelistet. Unter btc-echo.de/bitcoin-akzeptanzstellen findet man die aktuelle Liste der Unternehmen mit Bitcoin Akzeptanz. Das

Verzeichnis wird redaktionell moderiert, daher ist zur Eintragung des eigenen Unternehmens eine E-Mail an info@btc-echo.de notwendig.

FAZIT

Die Integration der Zahlungsmethode bringt also gleichzeitig einen weitestgehend kostenlosen Marketingeffekt mit sich. Mit Onlineportalen wie *Coinmap* oder dem BTC-Echo Verzeichnis kann man als Unternehmen nach außen kommunizieren, dass entsprechende Zahlungen willkommen sind. (Potenzielle) Kunden, die Bitcoins mögen, werden auch Ihr Geschäft mögen!

RISIKEN

Selbstverständlich bergen digitale Währungen auch Risiken für Geschäftsbetriebe. Deshalb möchten wir an dieser Stelle explizit auf Fallstricke eingehen, die Bitcoin-Shops betreffen.

DER KUNDE ZAHLT DIE GEBÜHREN

Wie bereits angedeutet ist bei Bitcoin-Transaktionen immer der Sender für die Entrichtung der Transaktionsgebühr verantwortlich. Das ist erst einmal unglücklich, wenn der Kunde in einem Shop einkauft und (evtl. neben den Versandkosten) noch weitere unerwartete Zusatzkosten zahlen muss. Zwar liegen die Transaktionskosten in einer Größenordnung, bei der es sich für den Kunden nicht lohnen würde, einen anderen Shop für die Bestellung

aufzusuchen. Die Gebühren befinden sich i.d.R. im Bereich von wenigen Cents. Dennoch sind Zusatzkosten erfahrungsgemäß immer eine kleine Enttäuschung für den Kunden, unabhängig von der Höhe. Auch wenn es sich nur um wenige Cent Zusatzkosten handelt.

Ein entsprechend formulierter Hinweis wie im folgenden Beispiel wäre also ein akzeptabler Kompromiss zwischen Händler und Kunden:

Auf Bestellungen, die vollständig mit Bitcoins bezahlt werden, wird ein Skonto i.H.v. einem Prozent gewährt. Transaktionsgebühren, die bei der Durchführung einer Bitcoin-Transaktion vom Sender bestimmt werden können, müssen vom Kunden getragen werden.

Selbstverständlich sollte der Hinweis vorher in Absprache mit einem Anwalt rechtlich abgesichert sein. Obiges Beispiel ist nur eine Demonstration einer Lösung des Gebührenproblems.

KEIN FIXER UMTAUSCHWERT FÜR BITCOIN

Wenn man Bitcoins auf direktem Wege akzeptieren möchten und sie in dieser Form gelagert werden, unterliegen sie dem Risiko der Kursschwankungen. Das andere Szenario ist der direkte Tausch von Bitcoins in die entsprechende Landeswährung wie bspw. dem Euro. Der Unterschied zwischen der nativen Bitcoin-Akzeptanz und dem automatischen Tausch in die Fiat-Währung wird im folgenden Kapitel erklärt.

Sollte man sich allerdings für den Weg der Bitcoin-Aufbewahrung

entscheiden, unterliegen die Bestände den Kursschwankungen. Da Bitcoins eine sehr volatile Währung sind, ist dieses Risiko nicht zu unterschätzen, auch wenn sich die Volatilität in der Vergangenheit meist positiv auf die Wertbestände ausgewirkt hat. Kursveränderungen um zweistellige Prozentanteile über Nacht sind keine Dinge der Unmöglichkeit. Wer die Bitcoins direkt akzeptiert und als solche aufbewahrt, sollte sich gegen zu große Kursschwankungen absichern, zum Beispiel durch feste Limits, bei denen der Bestand automatisch in die Fiat-Währung getauscht wird, um die Verluste zu begrenzen.

SICHERE AUFBEWAHRUNG VON BITCOINS

Wenn man die Bitcoin-Umsätze behalten möchte, ohne sie direkt in

Fiat-Währungen zu tauschen, ist man selbst für die Aufbewahrung verantwortlich. Letztendlich hat man die Wahl zwischen Cold-Wallets (Offline-Aufbewahrung), Wallets auf dem eigenen Gerät oder Online-Wallets, also Drittanbieter, die für die Aufbewahrung verantwortlich sind.

Vollständige Sicherheit ist in diesem Zusammenhang praktisch nicht erreichbar, sodass immer ein Verlustrisiko besteht. Durchaus einige Bitcoin-Unternehmen oder -Marktplätze haben es in die Schlagzeilen geschafft, weil ihnen große Mengen an Bitcoins entwendet wurden. Setzt man die Anzahl der bekannten Fälle eines Bitcoin-Raubes allerdings in Verhältnis zu den Nutzerzahlen, sind die Opferzahlen relativ gering.

Um das Risiko zu minimieren, sollte man den Bestand an Bitcoins im Optimalfall streuen.

BESTANDSDIVERSIFIKATION

Man sollte den Bestand weitestgehend auf die Aufbewahrungsmöglichkeiten aufteilen. Den größten Anteil sollte man in den Cold-Wallets halten. Da der Private-Key nur offline gespeichert ist und in einem Safe aufbewahrt werden kann, ist das Risiko geringer als bei Drittanbietern, die die Daten mit unterschiedlich starker Verschlüsselung aufbewahren. Online-Wallets bieten sich trotzdem an, um immer ein wenig Guthaben auf Reserve zu haben, damit man bspw. Retouren oder sonstige Rückbuchungen durchführen kann. Insbesondere dort sollte so weit

wie möglich gestreut werden.

BITCOINS IN DER STEUERERKLÄRUNG

Da Bitcoins eine relativ neue Errungenschaft sind, gibt es bisher wenig rechtskräftige Urteile. So war lange Zeit unklar, wie der An- und Verkauf von Bitcoins versteuert werden muss und ob Bitcoins offiziell als Währung oder Gut gelten. Je nach Auslegung würde Umsatzsteuer auf den Handel anfallen.

Im Oktober 2015 hatte ein Unternehmer in der Schweiz geklagt, der eine Plattform anbot, auf der Bitcoins angekauft wurden und an andere Interessenten verkauft wurden. Gemäß diesem Urteil fiel in dem Fall keine Umsatzsteuer auf die Transaktionen an.

Da es uns rechtlich leider nicht erlaubt ist, an dieser Stelle eine

Rechtsberatung zu geben und diese sich vermutlich in Zukunft schneller verändern wird, sollte man einen Steuerberater zu Rate ziehen, wenn man Bitcoins akzeptieren möchte und diese anschließend selbst verkauft oder gar aufbewahrt. Schließlich ist nicht automatisch klar, mit welchem Wert die vorhandenen Bitcoins beziffert werden sollen. Durch Kursschwankungen ist es möglich, dass ein Bitcoin am Jahresende bei der Erstellung der Jahresbilanz oder des Jahresabschlusses viel weniger wert ist, als zu dem Zeitpunkt, an dem Sie ihn als Gegenleistung erhalten haben. Andersherum kann er genauso an Wert gewonnen haben. In diesem Fall wird das Finanzamt sicher nicht lange auf sich warten lassen.

Einen Weg, diese rechtlichen Bedenken aus dem Weg zu räumen, sind die Zahlungsabwickler, die im folgenden Kapitel vorgestellt

werden.

Einschub: Klage aus der Vergangenheit gegen Ausschluss von der Umsatzsteuerbefreiung bei Bitcoin-Handel in Schweden.

In Schweden hatte es bereits einen gerichtlichen Fall gegeben, indem die Behandlung von Bitcoins als Währung diskutiert wurde. Die Person hatte mit Bitcoins gehandelt und An- und Verkäufe durchgeführt, wobei die Bitcoins jeweils kurz vor dem Ankauf beschafft und kurz nach einem Verkauf wieder in Kronen getauscht wurden (Händlerprinzip). Der Kläger hatte gegen den Bescheid der Steuerrechtskommission geklagt, dass seine Dienstleistungen „nicht unter die in Kapitel 3 § 9 des Mehrwertsteuergesetzes vorgesehene Steuerbefreiung falle.“

KAPITEL 10 DAS DEEP- UND DARKNET

Viele werden den Satz oder Gedanken kennen: „Google ist doch das Internet“. Diesen Trugschluss haben vermutlich bereits viele von euch zu hören bekommen. Je nach Zielgruppe und Brisanz der Themen ist von der Oberfläche bis zum tiefen Abgrund alles im Internet zu finden – abhängig von den drei Stufen „Suchmaschinen“, „Deep-Web“ und „Darknet“. Wir stellen euch die drei Stufen genauer vor und gewähren euch einen kurzen Einblick in das Dark-Web, in dem sich u.a. auch Bitcoin als eine beliebte Zahlungsmethode einen speziellen Ruf machen

konnte.

Wer denkt Google, Bing & Co. wären „Das Internet“ und würden alle Informationen des Internets zur Verfügung stellen, der liegt gehörig falsch.

Suchmaschinen fischen nur den oberen Teil, also den Teil der explizit für Suchmaschinen freigegeben wurde, aus dem Internet ab – das Paralleluniversum des Internets, das Deep- oder gar das Darknet bleibt dem „normalen“ Internetuser hier verborgen.

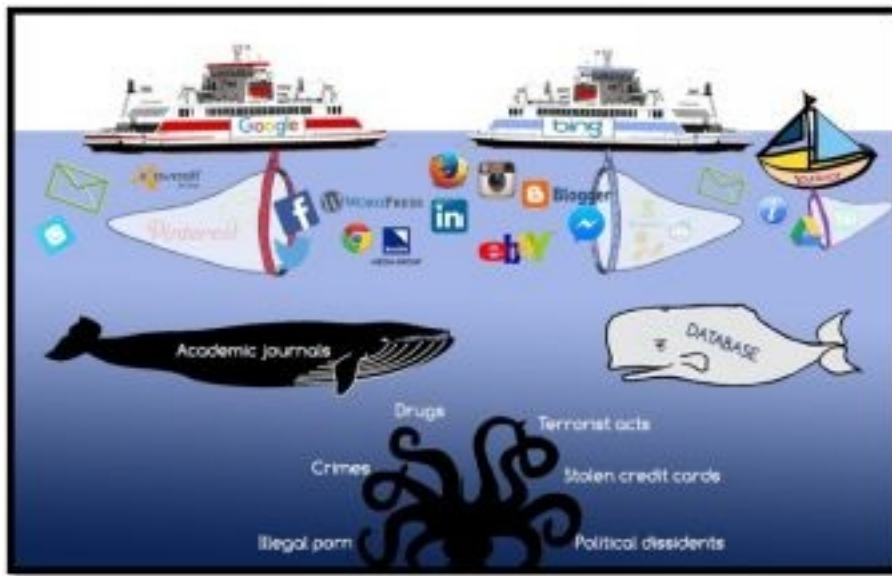


Abbildung 14: Darknet (Quelle: <http://de.awdnews.com>)

Wenn ein Webseiten-Betreiber nicht will, dass eine bestimmte Webseite über den normalen kommerziellen Weg (Google, Bing & Co.) auffindbar ist, kann das bereits mittels einer kleinen Datei, die nahezu jede Webseite besitzt, der robots.txt Datei, verhindern. Ein

Eintrag in diese Datei und die Webseite oder Unterseiten der
Webseite verschwinden aus dem Index der Suchmaschinen.

DEEP-WEB

Experten zufolge soll das Deep-Web tausendmal größer sein als das „oberflächliche“ Daily-Use-Web.

Das Deep-Web ist nicht wie von vielen vermutet ausschließlich ein Netz für Kriminelle. Es ist einerseits lediglich eine Ansammlung von Webseiten, die durch die zuvor genannte robots.txt Datei oder durch die Eingabe von Passwörtern von Suchmaschinen nicht indexiert werden und andererseits eine Datenbank, deren Inhalte von Google, Bing & Co. nicht verstanden werden, denn erst wenn ein User eine spezielle Anfrage an die Datenbank stellt, wird das gewünschte Ergebnis an den User ausgeliefert.

LEGALE INHALTE

Jeder Betreiber einer Webseite bestimmt selbst welche Inhalte er für Suchmaschinen freigeben will und welche eben nicht. Alle Seiten oder Unterseiten, die für die Crawler der Suchmaschinen nicht freigegeben werden oder mit einem Passwort verschlossen werden, gehören bereits zum Deep-Web.

So sind beispielsweise oftmals Bibliotheken, Fachinformationen oder Preisinformationen von der Websuche bewusst ausgeschlossen. Die Crawler der Suchmaschinen müssen hier „draußen bleiben“ und haben keine Chance bestimmte Seiteninhalte in den Index der Suchmaschinen zu laden.

Kostenpflichtige Anbieter wie BrightPlanet hingegen versprechen

ihren Nutzern auch einen Einblick in das Deep-Web – natürlich gegen entsprechende Bezahlung.

DARKNET

Kommen wir zum eigentlichen Thema des Kapitels: Dem Darknet.

Entstanden ist das Darknet zu Zeiten von Napster, eDonkey & Bittorrent. Damals und auch heute noch standen solche Plattformen im Fokus der Strafverfolger und die Betreiber suchten nach Möglichkeiten ihre Geschäfte unbehelligt weiter fortzusetzen. Das Ergebnis war ein Pendant zu den öffentlichen FileSharing-Plattformen: Das Darknet.

Im Darknet finden wir Seiten, die nicht einmal im Deep-Web zu finden sind. Während das Deep-Net bereits an der Grenze zu den illegalen Inhalten kratzt, befinden wir uns im Darknet mitten drin.

Wer also darauf aus ist sich Waffen, Drogen, Netflix-Accounts oder seines gleichen illegal zu beschaffen oder ein wenig Anarchisten-Schnack zu halten, wird im Darknet sicherlich fündig. Gezahlt wird meist in Bitcoin.

Das Surfen im Darknet selbst ist nicht illegal. Sobald ihr jedoch anfangt über irgendwelche Produkte zu verhandeln, was wir tunlichst nicht empfehlen, habt ihr die legale Grenze bereits überschritten. Also auch hier gilt die Devise: "Nur gucken - nicht anfassen."

WIE KOMME ICH REIN?

1. INSTALLATION TOR-BROWSER

Um einen Zutritt in das Darknet zu erhalten, benötigt ihr zunächst eine bestimmte Software, den Tor- Browser. Das komplette Bundle könnt ihr euch für alle Betriebssysteme herunterladen oder aber ihr installiert euch das Tor-AddOn für den Firefox-Browser. Der Tor-Browser anonymisiert eure Verbindung, indem er die Verbindung durch eine unzählige Anzahl von Tor-Servern schleust und die Route dadurch für die Behörden nicht nachvollziehbar macht.

2. KONFIGURATION TOR-BROWSER

Entpacke die Tor-Datei und öffne sie. Darauf öffnet sich ein Dashboard auf dem für den Darknet-Laien der Button „Tor starten“ zu sehen ist. Ein Klick darauf und der Browser lädt eine Liste aller verfügbarer Tor-Server und verbindet sich mit ihnen auf einer

zufälligen Route. Nur so lässt sich die Identität des Nutzers nicht zurückverfolgen. Durch das zufällige Routing rund um den Globus entsteht hier ein kleiner Nachteil, den ihr sicherlich schnell bemerken werdet. Die Geschwindigkeit ist unterirdisch und versetzt uns in das DSL-Vorzeitalter zurück. Aber ihr seid immerhin anonym unterwegs.



Abbildung 15: Screenshot Tor-Browser Darknet

SURFEN IM DARKNET

Das Interface des Tor-Browsers wird euch sicherlich an dem des Firefox- oder Chrome-Browsers erinnern, die Funktionsweise ist

jedoch etwas komplizierter und weniger nutzerfreundlich als manch einer es gewohnt sein mag. Das Darknet befindet sich weit unter dem komfortablen Google-Hoheitsgebiet, aber wenn man sich einmal daran gewöhnt hat, ist auch der Tor-Browser für jeden bedienbar. Vertipper werden hier nicht einfach korrigiert. Ihr solltet also genau wissen wo ihr hin wollt und die korrekte Adresse eingeben. Viele gute Tipps zur Navigation findet ihr in den Hidden Wikis <http://wikitjerrta4qgz4.onion/> oder auf der Tor-Linksseite <http://torlinkbgs6aabns.onion/>.



Abbildung 16: Screenshot Tor-Browser

Wie ihr hier bereits seht, enden die Adressen mit ".onion". Diese Endung ist speziell für Tor-Browser Webseiten und können nicht auf kommerzielle Weise in Firefox & Co. geöffnet werden.

UND JETZT?

Genauso wie im normalen Web ist es natürlich jedem Nutzer selbst überlassen was er im Darknet anstellt, kauft oder veröffentlicht.

Wichtig ist jedoch, dass ihr eine aktuelle Virensoftware installiert habt und nicht gerade mit Admin-Rechten im Untergrund surft. Solltet ihr euch nämlich einen Virus einfangen, könnte das wie mit dem normalen Web böse Folgen für den Rechner mit sich ziehen.

Betreten auf eigene Gefahr!

PANIC FAQ

Wenn du dieses Buch gelesen hast, darfst du dich zu den Auserwählten zählen, die schon heute verstehen, worum sich die digitale Revolution im Bereich der Finanzwelt dreht. Digitale Währungen – der Bitcoin ist eine davon – stoßen mit dem Konzept viele neue Ideen an und hinterfragen lang etablierte Strukturen von Banken und Finanzinstitutionen. Dementsprechend skeptisch ist meist der erste Blick auf den Bitcoin. Nicht allzu selten wird man als „Der mit den Bitcoins“ auf die „Währung für Drogenhändler“ angesprochen und kritischen, aber oft berechtigten, Fragen ausgesetzt. Um dir abschließend einen Kompaktüberblick über die gesamte Welt der Kryptowährungen

und gleichzeitig eine „Panik FAQ“ für unangenehme Fragen mit auf den Weg zu geben, stellen wir uns hier einigen klassischen FAQs an das System des Bitcoin.

SIND BITCOINS SICHER?

Die Frage wird oft zu schwammig gestellt, denn es kommt darauf an, in welcher Sphäre man sie betrachtet. Es gibt Dinge, die das Bitcoin-System vollständig kompromittieren könnten, beispielsweise die Entwicklung eines Quantencomputers, bei dem die verwendete SHA256 Verschlüsselung hinüber wäre. Oder der Angriff, bei dem eine Partei mehr als 50% der Hashpower im gesamten Netzwerk erreicht (51% Attacke) und damit Transaktionen verfälschen könnte. Das wären Risiken, die recht nah

am System der Kryptowährung liegen.

Oft werden aber auch Dinge, die schlichtweg nichts mit dem Bitcoin an sich zu tun haben, als Risiko oder Gefahr dargestellt. Ein gehackter Nutzer wurde nicht gehackt, weil das Bitcoin-System eine Schwachstelle hatte, sondern weil die privaten Schlüssel nicht richtig aufbewahrt wurden. Viele Betroffene neigen allerdings schnell dazu, die Schuld auf die Kryptowährung abzuwälzen, obwohl der eigentliche Einflussfaktor außerhalb des Bitcoin-Systems lag.

Zusammenfassend muss also zwischen Risiken differenziert werden, die im System liegen, und Gefahren, die von der individuellen Nutzung ausgehen. Das gilt nicht nur für Bitcoins,

sondern auch für jedes andere Finanzsystem. Das abgeschlossene Bitcoin-System in sich ist weitestgehend sicher.

WO KANN MAN SICH BEI BITCOIN ANMELDEN?

Weil es keine zentrale Institution gibt, die den Bitcoin betreibt, gibt es auch keine Stelle, an der man sich im klassischen Sinne registrieren kann. Um selbst Bitcoins zu kaufen, zu verkaufen, zu minen oder zu benutzen, benötigt man eine Bitcoin-Wallet, die öffentliche und private Schlüssel verwaltet und damit die Teilnahme am System ermöglicht.

SIND BITCOINS VERBOTEN?

Im deutschsprachigen Raum sind (bis zur Drucklegung dieses Buchs) keine Verbote bekannt. In manchen Ländern wie Russland

versucht man aber tatsächlich, die Benutzung von Bitcoins unter Strafe zu stellen.

WIE VIEL IST EIN BITCOIN WERT?

Weil das System der Bitcoins dezentral ist, gibt es auch keine Institution, die feste An- und Verkaufspreise zum Tausch in eine Fiat-Währung garantiert. Der Wert von Bitcoins ergibt sich letztendlich also nur aus Angebot und Nachfrage.

UND WAS MACHST DU, WENN DU GEHACKT WIRST?

Es kann in praktisch jedem Geldsystem passieren, „gehackt“ zu werden. Der Diebstahl einer Geldbörse lässt sich schließlich auch

nicht darauf zurückführen, dass der Euro eine schlechte Währung ist. Genau so wenig kann man von Einzelfällen, in denen Bitcoins gestohlen wurden, auf die Sicherheit des Systems schließen. In eigentlich allen Fällen lagen die Ursache für den Diebstahl außerhalb des eigentlichen Systems.

DIE WICHTIGSTEN VORTEILE VON BITCOIN

Das dezentrale System basiert nur auf den Nutzern und der gegenseitigen Teilnahme. Es kommt vollständig ohne zentrale Kontrollinstanzen aus, die in das Geschehen eingreifen. Dadurch entsteht ein freier Finanzverkehr, der praktisch nicht regulierbar ist. Das bedeutet gleichzeitig, dass jeder Teilnehmer seine Identität für sich behalten kann und (im abgeschlossenen System!) anonym

bleibt.

Das gesamte System der Bitcoins beruht auf Mathematik. Die maximale Menge an Bitcoins ist mathematisch begrenzt und kann (anders als in bestehenden Geldsystemen) nicht politisch beeinflusst werden. Durch das Schöpfen von neuen Bitcoins im Mining, bei dem die Vergütungen immer geringer werden, entsteht sogar ein deflationärer Charakter.

Die Transaktionen können weltweit, innerhalb von wenigen Minuten und mit minimalen Transaktionsgebühren ausgeführt werden. Damit kann sich der Bitcoin gegenüber dem herkömmlichen (inter-) nationalen Zahlungsverkehr durchsetzen. Egal ob Wochenende, Feiertag oder Ostern, Bitcoin Transaktionen

werden rund um die Uhr durchgeführt. Für sogenannte Remissen (Sendungen von Migranten in ihr Heimatland) kamen sonst nur Anbieter wie Western Union infrage, bei denen die Transaktionsgebühren i.d.R. deutlich höher als bei einer Bitcoin-Transaktion sind.

Bitcoins sind anonym. Transaktionen sind hinter kryptischen Bitcoin Adressen verborgen und nicht etwa mit Klarnamen hinterlegt, wie es beispielsweise bei der Eröffnung eines Bankkontos geschieht. Innerhalb des Systems kann jede einzelne Transaktion über die Blockchain nachverfolgt werden, allerdings keine direkte Zuordnung der Bitcoin-Adressen zu einer Person geleistet werden. Aber Achtung: Auch mit Bitcoins ist man nicht zu 100% anonym unterwegs! Wer Bitcoins beispielsweise über einen

Marktplatz per Überweisung kauft, hinterlässt also theoretisch auch darüber eine Spur zu seiner Identität, weil der Marktplatzbetreiber sowohl Bitcoin Adresse, als auch die wahre Identität kennt. Folglich kann er beide Daten zusammenführen.

DIE NACHTEILE VON BITCOIN

Das gesamte System der Bitcoins beruht auf Mathematik. Eine versehentlich ausgeführte Transaktion kann nicht rückgängig gemacht werden, weil es keine zentrale Instanz gibt, die solch eine Entscheidungsgewalt besitzt. Damit trägt der Nutzer die vollständige Verantwortung für seine Bitcoins.

Bitcoins sind anonym. Die Anonymität ist Vor- und Nachteil des Bitcoin zugleich. Zum Verhängnis wird sie gerade deshalb, weil sie

optimale Bedingungen für kriminelle Aktivitäten mit sich bringt. Das verleitet viele Leute dazu, Bitcoin gleich als eine unseriöse „Drogendealer-Währung“ abzustempeln und ihr nicht sonderlich viel Vertrauen beizumessen.

ERKLÄRE MIR BITCOIN IN EINEM SATZ

Bitcoin ist eine Währung, basierend auf einem dezentralen System, in dem alle auftretenden Transaktionen in der sogenannten Blockchain, einem offenen Transaktionsbuch, gespeichert und von anderen Teilnehmern des Netzwerks geprüft werden.

BTC-ECHO