:get know howww
UBIT Steiermark

BlockchainHub Graz

Das Internet der Werte – Blockchain Technologie & Kryptowährungen als Basis einer neuen Wirtschaft

Kapitel 1: Was ist Bitcoin und wie funktioniert es?





Von DI Thomas Zeinzinger

BlockchainHub Graz (https://blockchainhub.net/graz/)

Meetup jeden letzten Montag im Monat
http://www.meetup.com/de-DE/BlockchainHub-Graz/

Inhaltsverzeichnis

Schlagwort Dezentralisierung 1
Bitcoin in der Praxis 3
1. Schritt: Sie benötigen ein Wallet 3
2. Schritt: Sie benötigen Bitcoins 4
a) Bargeld gegen Bitcoin 4
b) Bitcoinbon kaufen und einlösen - bitcoinbon.at 5
c) Bitcoins kaufen über Banktransfer - https://coinfinity.co/bitcoin-onlinekauf/ 5
3. Schritt: Mit Bitcoin zahlen 6
a) Bitcoins senden 6
b) Bitcoins empfangen 8
Bitcoin als Wertspeicher im Anlageportfolio 9
Paperwallets statt Handywallets 9
1. Erstellung eines Paperwallets im Internet 9
2. Ausdruck auf einem Paperwallet Drucker 10
3. Wertschrift (Paperwallet) 10
Kursentwicklung von Bitcoin 10
Volatilität 11
Bitcoin: A Peer-to-Peer Electronic Cash System – Wie alles anfing 12
Exkurs – Krise seit 2007/2008 12
Die Technik hinter Bitcoin 15
Spezialitäten im Bitcoin Zahlungsverkehr 20
Keine Umkehrbarkeit der Zahlung 20
Automatische Treuhänder 20
Bitcoin ist nicht anonym 20

Sofort-Transaktion und bestätigte Überweisung 21
Steuer und Regulierung 21
Bitcoin – Geldmenge 22
Kreditwesen mit Bitcoin 22
Totgesagte leben länger – Gesammelte Bitcoin Nachrufe 23
Die FMA Warnung – Zum Nachdenken 24
Der Abschluss: Häufig gestellte Fragen und ein Glossar der falschen Begriffe 27
Was ist Bitcoin? 27
Was ist ein Wallet? 27
Was ist die Blockchain? 27
Wie entstehen Bitcoins? 27
Was sind die Miner? 27
Wer definiert den Preis von Bitcoin? 27
Wem gehört Bitcoin? 28
Kann ich eine Bitcoin Transaktion rückgängig machen? 28
Ist eine Bitcoin Transaktion anonym? 28
Worum die uns geläufigen Begrifflichkeiten in Bitcoin nicht gut funktionieren? 28

Schlagwort Dezentralisierung

Ein Großteil des Geldes, das wir heute verwenden, seien es Euro oder Dollar oder eine andere Währung, ist digital, ein realer Gegenwert in Form von hinterlegtem Gold steht der Geldmenge schon lange nicht mehr gegenüber, selbst dem Bargeld nicht mehr. Die USA hatte sich bereits 1933 von dem Goldstandard gelöst, weil sie die Geldmenge erhöhen wollten, um die herrschende Deflation zu bekämpfen. Der Begriff für ein Tauschmittel ohne inneren Wert ist auch FIAT Geld, vom lateinischen Wort für „es werde“, im Gegensatz zu Warengeld, das einen Wert besitzt wie beispielsweise Gold, Reis, Getreide, Silber, Tabak… Interessant ist es auch, dass unser Geld im Euroraum eigentlich zu 82 % als Giralgeld besteht, aus durch die Banken geschaffenem Geld, das eigentlich nur ein Versprechen der Bank an die Kunden ist, dieses Geld bei Bedarf auszuzahlen oder auf ein anderes Konto zu verschieben. Nur 18 Prozent des Euros liegen in Form von Bargeld oder Reserven der Zentralbank real vor.

Auch ohne kryptografischer Verfahren zum Verschlüsseln von kritischen Daten könnte der digitale Zahlungsverkehr nicht funktionieren. Überweisungen, Kreditkartenzahlungen – all die enthaltenen Daten müssen während der Bearbeitung mehrfach verschlüsselt werden.

Hier unterscheidet sich unser aktuelles Geldsystem wenig von der Kryptowährung Bitcoin. Denn auch dort handelt es sich um „digitales“ Geld, das keinen inneren Wert besitzt (auch wenn durchaus argumentiert wird, dass die investierte Rechenleistung und somit der Stromverbrauch einen inneren Wert generieren würde und es sich daher nicht um FIAT Geld handelt) und kryptografische Prinzipien werden ebenfalls verwendet.

Der große Unterschied liegt jedoch darin, dass es mit Bitcoin erstmals gelungen ist, ein Geldsystem innerhalb eines dezentralen Netzwerks zu erschaffen, an dem jeder, der möchte, teilnehmen kann. Zum ersten Mal wurde ein Rechenalgorithmus entwickelt, der es ermöglichte, ohne eine zentrale Stelle darüber Einigkeit zu erlangen, ob eine Transaktion Gültigkeit hat oder nicht. Damit wurde erstmals das so genannte „Double Spending“ Problem gelöst, also die Fragestellung, wie verhindert werden kann, dass ein und dasselbe Geld zweimal ausgegeben wird.

Unser aktuelles Geldsystem funktioniert nur über viele miteinander verwobene zentrale Stellen, Banken, Regulierungsbehörden, Settlement- und Clearingstellen, Staaten und Zentralbanken… Geldpolitik wird als wichtiges wirtschaftspolitische Maßnahme gesehen, zentral werden Zinssätze, Geldmenge etc. gesteuert.

Das System ist so komplex, dass es nur die wenigsten verstehen, je tiefer man sich einliest, umso rätselhafter wird es, wie ein solches Finanzsystem überhaupt funktionieren kann – und auch die Folgen der Geldpolitik sind nicht abschätzbar, da viele nichtplanbare Faktoren einen Einfluss auf das Ergebnis haben.

Bitcoin funktioniert auf Basis von wenigen Regeln – und es ist transparent, sowohl der Source Code und die Weiterentwicklung ist offen und jedem zugänglich, wie auch die einzelnen Transaktionen sind für jeden einsehbar. Ein jeder kann sich am Netzwerk der sogenannten Miner beteiligen. Und die Geldmenge ist langfristig gesehen begrenzt. Und Bitcoin basiert niemals auf Schulden, ein jeder existierende Bitcoin wurde in einem Rechenprozess geschaffen, das aktuell bestehende Kreditsystem würde unter Bitcoin so nicht funktionieren.

Wer sich also ernsthaft mit Bitcoin auseinandersetzt, lernt auch unser normales Geldsystem besser kennen.

Doch am besten ist es, es einmal selbst auszuprobieren. Dazu braucht es gar nicht so viel – ich möchte Sie – sollten Sie bislang noch nie Bitcoin besessen haben – gerne dazu einladen, den Selbstversuch zu wagen und ein paar Euros in Bitcoin zu investieren, um mit der Technologie etwas herumspielen zu können. Viel Spaß dabei! Alle anderen können das nächste Kapitel grundsätzlich überfliegen.

Bitcoin in der Praxis

Hier nun die Einladung an Sie, Bitcoin auszuprobieren. Bitcoin ist kein theoretisches System, es funktioniert bereits seit 2009 in der Praxis. Also sollten Sie noch kein aktiver Bitcoin-User sein, lassen Sie sich bitte auf diesen Versuch ein und folgen Sie der Anleitung, wie Sie ein Bitcoin-Wallet installieren, Bitcoins besorgen und damit bezahlen oder spenden. Es reicht völlig, wenige Euros zu investieren.

Diejenigen die Bitcoins als Anlageform sehen, bekommen dann noch zusätzliche Informationen, die über das erste Grundverständnis des täglichen Gebrauchs hinausgehen.

1. Schritt: Sie benötigen ein Wallet

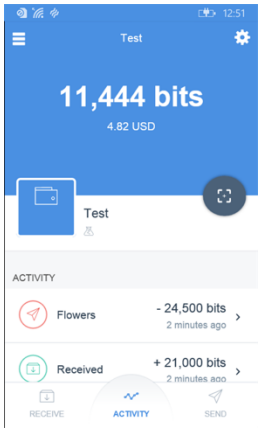
Das Wallet hat die Funktion einer Geldbörse auf Ihrem Handy (=Smartphone) und erlaubt die einfache Überweisung von Bitcoins direkt an den Empfänger. Dabei kann es sich um die Bezahlung in einem Kaffee oder Geschäft handeln oder die Guthabenaufstockung bei Microsoft oder noch vieles mehr.

Wir empfehlen für den Start die Verwendung der kostenlosen Handy-App Copay:

Android: https://play.google.com/store/apps/details?id=com.bitpay.copay

iOS: https://itunes.apple.com/at/app/copay-bitcoin-wallet/id951330296?mt=8

Windows Phone: https://www.microsoft.com/de-at/store/p/copay-bitcoin-wallet/9wzdncrcwvrq



Wenn man die App installiert hat, wird man angeleitet, sich eine „Wiederherstellungsphrase“ zu erstellen. Das ist notwendig, um das Wallet für den Fall, dass das Handy kaputt wird oder gestohlen wird, einfach auf einem neuen Gerät wiederhergestellt werden kann.

WICHTIG: Schreiben Sie sich diese „Wiederherstellungsphrase“ auf und heben Sie sie am besten bei Ihren Dokumenten gut auf. Machen Sie keine Screenshots der Wiederherstellungsphrase bzw. speichern Sie dieses keinesfalls in der Cloud.

Weiters ist es in unserem Kulturraum empfehlenswert, in den Einstellungen von „bits“ auf „BTC“ und „USD“ auf „EUR“ umzustellen (BTC ist das Akronym für Bitcoin).

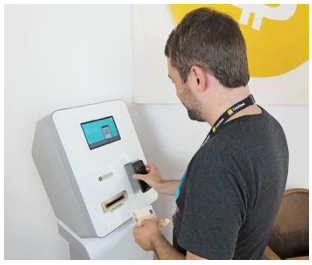
Die weiteren Einstellungen können Sie jederzeit einfach in Ruhe studieren, aber für die ersten Experimente sollte es jetzt schon reichen.

2. Schritt: Sie benötigen Bitcoins

Die aktuell einfachste Möglichkeit an Bitcoins zu kommen, ist der Kauf und deshalb beschränken wir uns hier vorerst auch mal auf die Beschreibung dieses Weges.

Bitcoins können Sie, analog zu Fremdwährungen, bei Bitcoin-Händlern kaufen. Wir werden den Prozess anhand von drei Möglichkeiten beschreiben, die von der Firma Coinfinity (www.coinfinity.at) hier in Graz bereitgestellt werden. Sie können aber auch gerne bei Kraken (www.kraken.com) , Bitpanda (www.bitpanda.com) oder VirWoX (www.virwox.com) Ihre Bitcoins kaufen. Eine Auflistung von weiteren Bitcoin-Händlern und dazugehörige Bewertungen finden Sie hier: https://www.bestbitcoinexchange.io/. Weitere Möglichkeiten an Bitcoins zu kommen werden noch von Bitcoin Austria e.V. aufgelistet: https://bitcoin-austria.at/de/bitcoininfo/wie-bekomme-ich-bitcoins

a) Bargeld gegen Bitcoin



Für alle, die in Graz wohnen, ist es vielleicht am einfachsten mit etwas Bargeld ihre ersten Bitcoins zu kaufen. Dafür gibt es eigene Bankomaten (ATMs), bei denen man Bargeld „reingibt“ und Bitcoins im Wallet landen. Der Bitcoin Automat steht bei Coinfinity in der Mariahilferstraße 23, 8020 Graz.

Weitere Standorte von Bitcoin Automaten finden Sie unter: https://coinatmradar.com/country/14/bitcoin-atm-austria/

b) Bitcoinbon kaufen und einlösen - bitcoinbon.at



Durch den Bitcoinbon wird die Möglichkeit geboten, Bitcoins per Coupon in mehr als 3.000 Verkaufslokalen (hauptsächlich Trafiken) überall in Österreich zu erwerben. Ob es diesen Bon auch in Ihrer nächstgelegenen Trafik gibt, können Sie hier herausfinden: https://www.bitcoinbon.at/outlets/

Damit die Bitcoins auf Ihrem Wallet landen, müssen Sie diesen Bon auf der Webseite einlösen.

c) Bitcoins kaufen über Banktransfer - https://coinfinity.co/bitcoin-onlinekauf/

Sobald Sie verifiziert sind, können Sie Bitcoins kaufen (Zahlung per SOFORT Überweisung oder SEPA-Überweisung) und Bitcoins verkaufen (Auszahlung per SEPA-Überweisung). Der Bestellvorgang dauert nur wenige Sekunden, Sie erhalten die Bitcoins bei Bezahlung mittels SOFORT prompt. Sie benötigen dafür die Bitcoin-Wallet-Adresse, auf die Sie die Bitcoins hin überwiesen haben möchten.

Auch wenn es im Vergleich zum typischen Fremdwährungskauf (Euro → Pesos, Euro → Kuna) verhältnismäßig einfach ist an Bitcoins zu kommen, so liegt doch noch immer die größte Hürde in der Beschaffung der Bitcoins. Also herzlichen Glückwunsch, wenn Sie diese Hürde überwunden haben. Wenn jetzt also 10, 25 oder 50 Euro in Ihrem Wallet sind, wird durch Rumprobieren alles einfacher verständlich, wie dieses Geldsystem funktioniert und wofür es überhaupt gut ist. Dieses Grundverständnis wird auch benötigt, wenn wir in späteren Kapiteln weiterführende Möglichkeiten, weit über das „einfache“ Geldsystem hinaus, besprechen.

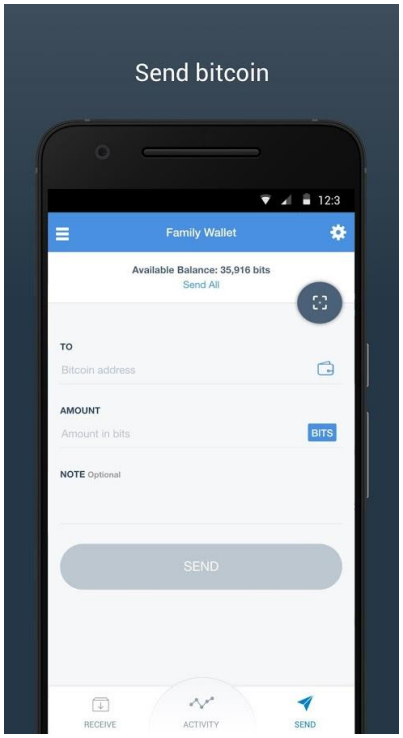
HINWEIS: Wenn Sie bis hierher gelesen haben und noch keine Bitcoins in Ihrem Wallet haben, würde ich Sie bitten, die beiden vorigen Schritte durchzuführen, bevor Sie weiterlesen.

---

3. Schritt: Mit Bitcoin zahlen

Wenn Sie nun Ihr Copay Wallet auf Ihrem Handy aufmachen, dann sollten Sie die verfügbare Menge an Bitcoins (BTC) sehen und klein darunter den aktuell umgerechneten Wert in Euro (EUR). Der Kurs von Bitcoin ergibt sich durch Angebot und Nachfrage und deshalb ändert er sich auch laufend, je nachdem wieviel gerade auf der im Wallet eingestellten Referenzbörse für Bitcoin gezahlt wird. Wenn Sie sich durch die laufenden Preisinformationen auf Ihrem Handy gestört fühlen, dann stellen Sie diese einfach in den Einstellungen der App ab.

a) Bitcoins senden



Da die Bitcoin-Adressen noch deutlich länger sind als IBAN Nummern ist es üblich diese als QR-Code abzuscannen, das ist schnell und fehlerfrei machbar.

Für die erste Überweisung benötigen Sie also eine Empfängeradresse. Probieren Sie daher als ersten Schritt aus, einem Freund oder Bekannten einen kleinen Betrag zu überweisen, oder aber Sie spenden bspw. 1 € für einen guten Zweck. Dafür aktivieren Sie den QR-Code-Scanner und lesen die jeweiligen Adresse des Empfängers ein.

Wenn Sie sich für das Spenden entschieden haben, finden Sie hier drei Organisationen, die Spenden in Bitcoins empfangen. Vielleicht ist ja hier schon das passende für Sie dabei.

Netzpolitik.org	XKCD.com	bitcoinfoundation.org
Kritische Sichtweisen zu Datenschutz, Überwachung, usw.	Nerdige Kunstwebseite mit Comics und Grafiken	Weiterentwicklung des Bitcoin Protokolls
1FMHxhVJo6RREtfaLDVMA1VvoKV1jc12a	14Tr4HaKkKuC1Lmpr2YMAuYVZRWqAdRTcr	3JDs4hAZeKE7vER2YvmH4yTMDEfoA1trnC

Weitere Organisationen, die sich über eine Spende freuen würden, finden Sie hier: https://en.bitcoin.it/wiki/Donation-accepting_organizations_and_projects

Wenn Sie sich entschieden haben, wem Sie einen Betrag in Bitcoin schicken möchten, dann brauchen Sie sich nur noch für den Betrag zu entscheiden. Sollte bei ihnen „Betrag in BTC“ auf der App stehen, dann tippen Sie einfach auf das BTC-Zeichen und Ihre App schaltet auf „Betrag in Euro“ um. 1 Euro (oder beliebigen Betrag) eingeben und auf Senden drücken.

Wenn es sich um das Bitcoin Konto Ihres Freundes handelt und der zufälligerweise neben Ihnen steht, dann sehen Sie normalerweise eine unmittelbare Bestätigung auf seinem Handy, dass eine Zahlung verarbeitet wird.

Im Bitcoin Netzwerk dauert die Verarbeitung durchschnittlich 10 Minuten und die übertragenen Bitcoins befinden sich in diesem Zeitraum entweder in Ihrem Besitz oder im Besitz des Empfängers. Dazwischen gibt es niemanden, der Ihre übertragenen Bitcoins aufbewahrt und dann an den Empfänger weiterreicht.

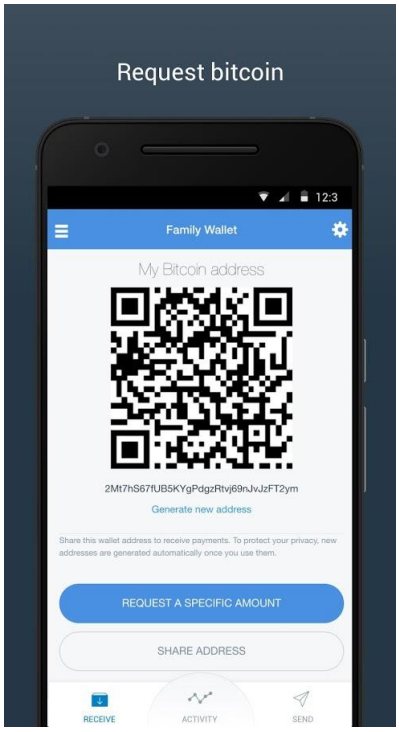
Das Bitcoin-Netzwerk ist damit ein echtes Peer-to-Peer Netzwerk, d.h. Ihre gesendeten Bitcoins gehen direkt in den Besitz des Empfängers über und es gibt keine Mittelsmänner – z.B. Banken, Paypal oder Kreditkartenunternehmen, die diese Transaktion möglich machen.

Wenn man so nennen will, ist deshalb Bitcoin die „Demokratisierung des Geldes“. Jeder darf mitmachen und jeder kann an jeden direkt überweisen. Wenn man bedenkt, dass aktuell nur eine Milliarde der Menschen weltweit Zugang zu einem Konto haben, mit dem Sie

international agieren können, von den restlichen 6,5 Milliarden Menschen jedoch 2 Milliarden Zugang zum Internet haben, bekommt man eine Ahnung, was eine Peer-to-Peer-Überweisungsmöglichkeit von Geld für diese Menschen bedeuten könnte.

Und immer mehr Geschäfte online und vor Ort akzeptieren Bitcoins als Zahlungsmittel: Mehr Infos hier: http://usebitcoins.info/index.php oder https://coinmap.org/welcome/ Es sind aber noch nicht alle lokalen Geschäfte in der Karte vermerkt – daher am besten immer Ausschau nach dem Bitcoin-Zeichen halten.

b) Bitcoins empfangen



Wieder zurück zu Ihrem Handy Wallet von Copay.

Wenn Sie auf den Button Empfangen drücken, dann wird der QR-Code für Ihre Wallet-Adresse dargestellt. Wenn der Sender diese einscannt und den Betrag auswählt, der gesendet werden soll, dann landet dieser umgehend auf Ihrem Konto.

Sie können auch über den unten angebotenen Button einen definierten Betrag in den QR-Code einbauen. Dann muss der Sender nur noch scannen und auf senden drücken.

Eine wesentliche Eigenschaft des Bitcoin Systems ist, dass Sie nur senden können, was Sie auch wirklich haben. Es gibt keinen Überziehungsrahmen, da es keinen Kredit in diesem System gibt. Es gibt ja auch keine Bank, die Ihnen jetzt mal einfach einen Kreditrahmen in diesem System zur Verfügung stellt und dafür Zinsen verlangt.

Auch können Sie nicht zweimal denselben Betrag an verschiedene Personen überweisen. Es wird immer überprüft, ob Sie den Betrag haben und nur dann wird er auch an nur einen möglichen Empfänger gesendet. Mit der Erfindung von Bitcoin im Jahr 2008 wurde damit erstmals, wie bereits erwähnt, das sogenannte „Double Spending Problem“ für Geldüberweisungen im Internet ohne Mittelsmänner (Banken, Treuhänder, ...) gelöst.

Bitcoin als Wertspeicher im Anlageportfolio

All jene, die unserem von Staaten, Zentralbanken und riesigen Investmentbanken kontrollierten Geldsystem nicht besonders trauen (und deren Zahl ist nach der Krise 2008 sicherlich gewachsen), überlegen wegen Alternativen für die Anlage ihrer Ersparnisse. In der Regel greift man auf Immobilien, Gold oder Aktien zurück, um das Geld in realen Werten zu „speichern“. Zunehmend wird dafür aber auch Bitcoin interessant, da die bisherigen Kursverläufe sehr positiv sind und es eine natürlich eingebaute Limitierung von maximal 21 Millionen Bitcoins gibt.

Sollten Sie auch überlegen, ob Bitcoin eine geeignete Anlageform für Sie ist, hier einige Informationen:

Paperwallets statt Handywallets

Wer also nicht täglich mit Bitcoin zahlen möchte oder eine größere Menge in Bitcoin „speichern“ möchte, ohne sich Gedanken über eventuelle Handydiebstähle oder eventuelles Ausspähen durch Schadsoftware am Handy machen zu wollen, kann ein sogenanntes „Paperwallet“ verwenden. Dabei wird besonders darauf geachtet, dass die Generierung sicher ist und der private Schlüssel, mit dem man Zugriff auf das Konto erhält, nur vom Besitzer gesehen wird.

Dafür gibt es drei Möglichkeiten:

1. Erstellung eines Paperwallets im Internet - https://www.bitaddress.org



Das erstellte Paperwallet einfach ausdrucken und die Bitcoin Adresse (Bild – linke Seite) für die Übermittlung von Bitcoins verwenden.

Der Private Key gibt jeden, der ihn weiß den vollen Zugriff auf das hinterlegte Vermögen. Deshalb ist es wichtig, dass dieser Schlüssel niemanden gezeigt wird und nicht auf dem Computer in welcher Form auch immer gespeichert wird.

2. Ausdruck auf einem Paperwallet Drucker



Dabei handelt es sich um speziell für die Erstellung eines Bitcoin Kontos und dazugehörigem Privaten Schlüssel gebaute Drucker.

Ein derartiges Gerät finden Sie ebenfalls bei der Firma Coinfinity in der Mariahilferstraße 23, 8020 Graz. Sollten Sie ohnehin schon vor Ort sein, dann können Sie dieses generierte Paperwallet gleich mit Bargeld am Bitcoin Automaten aufladen.

3. Wertschrift (Paperwallet)



Auch wenn es sich um eine weitere Form des Paperwallets handelt, so verdient dieses Produkt der Firma Coinfinity eine Erwähnung, denn gerade für konservative Kunden könnten es vertrauenswürdiger sein.

Denn der private Schlüssel wird unter notarieller Aufsicht erstellt und ist zu keinem Zeitpunkt von irgendjemanden einzusehen – weder visuell noch elektronisch gibt es eine Möglichkeit des Ausspähens. Damit hat man die Gewissheit, dass niemand, außer dem Eigentümer der Wertschrift auf die darauf gespeicherten Bitcoins Zugriff habt.

Vorausgesetzt natürlich, man achtet gut auf sein Paperwallet, dass es nicht in falsche Hände gerät.

Kursentwicklung von Bitcoin

Als Bitcoin Ende 2008 vorgestellt wurde, war sicher niemand in der Lage zu sagen, wie sich der Kurs im Verhältnis zu anderen Währungen entwickeln würde. Es war vielmehr eine technische Lösung für ein bis dahin nicht gelöstes Problem.

Am Anfang war es vielleicht auch nur eine „Spielerei“ unter Technikern. Wir wollen hier auch nicht weiter darüber spekulieren was die Beweggründe waren, weil rückblickend kann man wohl sagen, dass es eine unglaublich geniale Erfindung war, ohne dass es dafür einen Patentinhaber gibt. Die erste Transaktion in die Realwirtschaft (zugegebenermaßen über den Umweg von USA nach England und der Mithilfe einer Kreditkarte) war der Kauf zweier Pizzas

für 10.000 Bitcoin am 21. Mai 2010[1] – dies entsprach zum damaligen Zeitpunkt ungefähr 30 $. Heute wäre diese Pizza wohl über 7 Millionen € wert, es hat sich beim Kurs also einiges getan.



http://coinmarketcap.com/currencies/bitcoin/#charts

Wie man an dem Chart gut erkennen kann, hat es Ende 2013 einen riesigen Ansturm auf Bitcoin gegeben und kurzfristig wurden Preise über 1.000 USD pro Bitcoin erreicht. Bis zum Anfang 2015 ging der Trend dann nach unten und seit Ende 2015 geht der Wechselkurs gegenüber den USD beständig nach oben. Aktuell (24.11.2016) bewegt sich der Kurs im Bereich von 740 USD / 700 EUR und hat sich seit Anfang Februar 2016 quasi verdoppelt.

Volatilität

Nachdem sich der Preis von Bitcoin (und allen anderen Kryptowährungen) durch Angebot und Nachfrage bestimmt, gibt es auch massive Preisschwankungen. Der Kurs kann innerhalb sehr kurzer Zeit deutlich nach oben als auch nach unten gehen und auch ein Totalverlust ist nicht auszuschließen. Deshalb wird auch zu Recht auf allen seriösen Portalen darauf verwiesen und es ist nicht anzuraten, Bitcoin als Speicher für einen großen Teil der oder gar die gesamten Ersparnisse zu verwenden. Und seien Sie vorsichtig mit Investmentangeboten, die zu gut um wahr zu sein klingen, egal ob es dabei um Bitcoin-Mining oder Investments in andere (angebliche) Kryptowährungen handelt. Gier ist meist ein schlechter Berater. Bei einigen der Angebote liegt der Verdacht nahe, dass es sich um ein Pyramidenspiel oder schlichtweg Betrug handelt.

[1] http://www.vice.com/de/read/diese-pizza-kostet-2-millionen-euro-bitcoins-geld-krise

Bitcoin: A Peer-to-Peer Electronic Cash System – Wie alles anfing

Exkurs – Krise seit 2007/2008

2007 und 2008 häuften sich die Negativschlagzeilen in den Wirtschaftsteilen der großen Zeitungen. Die Industriestaaten schlitterten in eine Rezession. Begonnen hatte es im Prinzip mit einer Immobilienpreisblase in den USA. Der Anreiz für die Banken war groß, auch Subprimekredite zu vergeben, also Hypothekenkredite an Schuldner mit geringer Bonität. Die steigende Hauspreise schienen als Sicherheit auszureichen, Kredite wurden darauf basierend ständig refinanziert, die Kreditsummen stiegen. Diese Kredite jedoch in den eigenen Büchern zu behalten, hätte für die Banken nach den bankaufsichtlichen Eigenkapitalregeln bedeutet, einen gewissen Anteil des Eigenkapitals dafür hinterlegen zu müssen. Daher wurden diese Kredite gebündelt und mithilfe der Ratingagenturen durch Strukturierung in erstklassige Wertanlagen transformiert – die dann innerhalb der USA und auch im Ausland gehandelt wurden.

Die Immobilienpreise blieben nicht auf dem Niveau, denn durch ein Steigen des Leitzinses und einer leichten Abschwächung der Wirtschaft konnten immer mehr der Subprime-Kreditinhaber ihre Raten nicht mehr bezahlen und sahen sich gezwungen, ihre Häuser zu verkaufen. Das steigende Angebot führte zu einem Wertverlust der Häuser, dies wiederum bedeutete für die Banken und Investoren, dass sie nun zunehmend ungesicherte Kreditforderungen hatten, die aus den Subprimekrediten geschnürten Wertpapiertranchen verloren ihren Wert. Die Folge waren Verluste und Insolvenzen bei Finanzinstituten. Einen traurigen Höhepunkt erreichte diese Kettenreaktion mit dem Zusammenbruch der amerikanischen Großbank Lehman Brothers, die nicht mit öffentlichem Geld gerettet wurde. Andere Banken, auch in Europa wurden durch Bankenhilfsprogramme der Staaten wieder stabilisiert, in Österreich wurde zum Beispiel am 29.10.2008 ein Hilfsprogramm in der Höhe von 100 Milliarden Euro beschlossen, zusätzlich übernahm der Staat auch Garantien für Kredite zwischen Banken und befristet für Spareinlagen in unbegrenzter Höhe. Die Maßnahmen stießen teilweise auch auf scharfe Kritik, denn die Steuergelder wurden hier zu einem nicht geringen Teil in den Erhalt der Vermögen von ohnehin Wohlhabenden investiert. So wurde in Österreich die Constantia Privatbank gerettet, wo die Mindesteinlage zur Kontoeröffnung bei 500.000 € lag.

Und die Krise berührte auch die Bevölkerung. Millionen weltweit haben Ihre Häuser verloren, Millionen von Menschen auch ihren Job, in China allein waren es damals 20.000.000. In der Euro-Zone ging die Industrieproduktion von Frühjahr 2008 bis Frühjahr 2009 um 20 % zurück, das ist vergleichbar mit dem ersten Jahr der Weltwirtschaftskrise 1930. Die Anzahl der hungernden Menschen stiegen bis 2009 um 100 Millionen an.
Und was die Menschen damals noch verloren, war ein Stück ihres Vertrauens in Banken und das Finanzwesen.

Für alle, die mehr zu diesem Thema wissen wollen, hier zwei Empfehlungen:



Josef Stiglitz – Nobelpreisträger und hochangesehener Wirtschaftswissenschafter hat 2010 das Buch: *Im freien Fall. Vom Versagen der Märkte zur Neuordnung der Weltwirtschaft.* Siedler, München 2010, ISBN 978-3-88680-942-4 geschrieben.
Darin erklärt er, wie es zur 2008er Krise kommen konnte – und erklärt, wie wir solche Katastrophen in Zukunft verhindern können.



The Big Short – ist ein Film mit unglaublich guter Besetzung und sehr anschaulicher Darstellung der amerikanischen Immobilienblase, die letztendlich beim Platzen im Jahr 2008, Lehman Brothers zusammenbrechen ließ und die ganze Weltwirtschaft getroffen hat. Gier, Macht und Betrug in einem Netzwerk, das sich selbst am Leben hält und wo getanzt wird, bis die Musik aufhört zu spielen.

2007 begann irgendwo auf der Welt ein bislang Unbekannter an einer kryptografisch verschlüsselten Währung zu arbeiten, den so genannten Bitcoins. Unter dem Pseudonym Satoshi Nakamoto hat er Ende 2008 in einer Mailingliste ein Whitepaper veröffentlicht, in dem er Bitcoin vorstellt, ein elektronisches Geldsystem, dass einem erlaubt, Geld von einem zum anderen zu senden, ohne dass dafür ein Finanzinstitut genutzt werden muss. Und das weltweit und mit keinen oder geringen Gebühren. Am 3. Januar 2009 wurde der initiale Block der Bitcoin-Blockchain – der sogenannte Genesisblock generiert, Satoshi Nakamoto war einer der Entwickler der initialen Anwendung. Ende 2010 zog er sich aus dem Projekt zurück, ohne in der ganzen Zeit viel über sich preiszugeben. Die Entwicklung wird nun von vielen als Open Source Projekt weitergeführt[2].

Bis heute ist die Identität von Satoshi Nakamoto unbekannt, seine selbst geminten Bitcoins unberührt. Dies gab natürlich Anlass zu vielen Spekulationen. Offen war, ob es sich wirklich um eine Einzelperson handelte oder um eine Gruppe von Menschen. Auch warum er sich komplett aus der Weiterentwicklung von Bitcoin zurückgezogen hat und auch seine E-Mails nicht mehr beantwortete, war fraglich. Und auch, wenn er angab Japaner zu sein, sprach er Englisch, als wäre es seine Muttersprache. Und er nutzte eine GMX-E-Mail-Adresse.

Das Nachrichtenmagazin Newsweek meinte 2014 einmal den Bitcoin-Erfinder im Kalifornier Dorian Satoshi Nakamoto gefunden zu haben. Dieser dementierte jedoch sofort und setzte auch rechtliche Schritte gegen das Magazin.

Und erst vor wenigen Monaten im Mai 2016 wurde die Diskussion wieder angestoßen, als der Australier Craig Steven Wright von sich behauptete, der wahre Satoshi Nakamoto zu sein. Doch anfängliche angebliche Beweise stellten sich als Fälschung heraus, der richtige Beweis fehlt bis heute.[3]

[2] https://bitcoin.org/de/entwicklung

[3] https://bitcoinblog.de/2016/05/04/craig-satoshi-wright-erntet-heftige-betrugsvorwuerfe-und-kuendigt-an-fruehe-bitcoins-zu-bewegen/

Die Technik hinter Bitcoin

Lassen Sie uns doch einmal etwas tiefer in das Whitepaper eintauchen. Sie müssen hier nicht alles im Detail verstehen, um Bitcoin benutzen zu können. Die wenigsten Internetnutzer verstehen, wie das Internet funktioniert. Doch muss Ihnen als Bitcoin-Nutzer bewusst sein, dass es sich hier um ein dezentrales System handelt, bei dem Sie die volle Verantwortung für das investierte Geld tragen. Lassen Sie sich daher im Zweifel zur genauen Handhabung beraten.

Hier der Abstract des Whitepapers:

> **Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

> *Eine reine Peer-to-Peer (Gleichgesinnter-zu-Gleichgesinnter) Version eines elektronischen Geldes würde es erlauben online Zahlungen direkt von einer Partei zur Anderen zu schicken, ohne durch ein Finanzinstitut gehen zu müssen.*

Unser gesamtes Finanzwesen ist auf zentralen Institutionen aufgebaut, die Geld ausgeben, die Geldmenge regulieren, die Zinsen festlegen, usw. Hier wird aber ein Zahlungssystem bei dem es für die Überweisung keinen Mittelsmann (=Bank) braucht beschrieben.

> *Digitale Signaturen stellen ein Teil der Lösung dar, aber die wichtigsten Vorteile gehen verloren, wenn eine vertrauenswürdige dritte Partei noch erforderlich ist, um Doppel-Ausgaben (Double-Spending) zu verhindern.*

Die gravierende Problematik im digitalen Geldverkehr ist die Sicherstellung, dass jemand nicht eine Überweisung an mehrere Empfänger senden kann – z.B. jemand hat 100€ und überweist diese 2x an verschiedene Personen. Im Finanzsystem verwendet man sogenannte Clearing- und Settlement Systeme, um das möglichst zu verhindern.

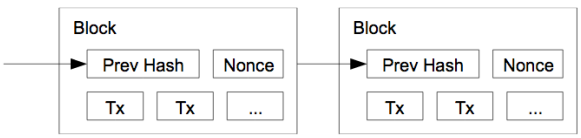
> *Wir schlagen eine Lösung des Doppel-Ausgaben Problems mit Hilfe eines Peer-to-Peer-Netzwerk vor. Das Netzwerk versieht Transaktionen mit einem Zeitstempel indem sie in einem Hashwert einer fortlaufenden hash-basierenden proof-of-work Kette landen, sodass ein Datensatz gebildet wird, der nicht ohne Wiederholung der zuvor geleisteten Arbeit (proof-of-work) geändert werden kann.*

Um das verstehen zu können, muss man wissen was ein Hashwert ist und das ist leichter als man denkt – jeder kann sich Hashwerte ausrechnen, indem man eine Nachricht bei http://hashgenerator.de/ eingibt. Im Prinzip geht es darum, mit einem mathematischen Algorithmus, eine Zeichenkette beliebiger Länger in einen eindeutigen Zeichensatz mit konstanter Länge zu verwandeln. Gleiche Datensätze ergeben immer den gleichen Hashwert, minimalste Änderungen führen zu komplett anderen Hashwerten. Andererseits kann man von einem Hashwert nicht auf den Datensatz zurückrechnen. Bitcoin verwendet den SHA-256 Algorithmus.

Beispiel (Achtung der Unterschied ist nur der Punkt am Ende):

Ich liebe Bitcoin → SHA256 Hashwert:
983df8e8ba4517b281fb3be5a38ed92e780853e7ed2d26dfe50d14c95c55692b

Ich liebe Bitcoin. → SHA256 Hashwert:
53c5f29c9322db96046e64956f0fbe741b54b45e70041678f05f26cdd2ce9a8a



Das, was hier als Kette bezeichnet wird, ist die sogenannte „Blockchain“ und diese wird deshalb so genannt, weil die einzelnen Transaktionen („Tx“) in sogenannten Blöcken zusammengefasst werden. Der Hashwert eines Blocks muss zur Absicherung des Netzwerks vor Angreifern – wir wollen ja Betrug durch Doppel-Ausgaben vermeiden – eine vorgegebene Struktur vorweisen. Diese Struktur wird dadurch erreicht, dass die „Nonce“ so lange automatisiert verändert wird, bis der Hashwert der Blocks die Anforderungen erfüllt. Wenn die Nonce bekannt ist, kann man dann leicht nachprüfen, ob proof-of-work (Nachweis von Arbeit) erfüllt ist und den Block als valide oder nicht valide identifizieren.

Valide Blöcke verlängern die Blockchain und es kann ein älterer Block nicht mehr verändert werden (z.B. Löschung einer Transaktion), ohne die gesamte Kette neu berechnen zu müssen.

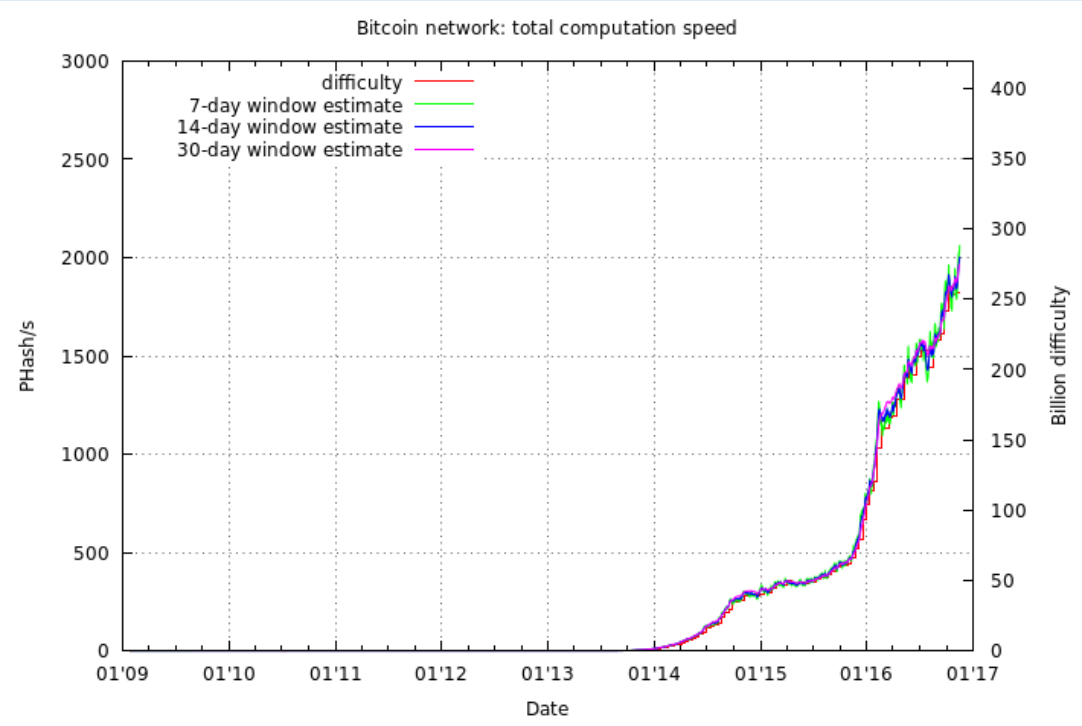
> *Die längste Kette dient nicht nur als Beweis für die Reihenfolge von bestätigten Ereignissen, sondern ist Beweis, dass es aus dem größten Pool an CPU-Leistung kam. Solange ein Großteil der CPU-Leistung durch Knoten kontrolliert wird, die nicht kooperieren um das Netzwerk anzugreifen, werden sie die längste Kette erzeugen und schneller sein als eventuelle Angreifer.*

Wenn die sog. Miner für den nächsten Block die Nonce suchen, kann es passieren, dass zwei unabhängig voneinander kurz nacheinander eine richtige Berechnung vorstellen. Wenn dann der nächste Blockberechnungsprozess auf den jeweils unterschiedlichen Blöcken weitergeführt wird, dann ergibt sich quasi eine „Gabelung“. Im Durchschnitt benötigt die Berechnung eines Blocks im Bitcoin Netzwerk 10 Minuten, aber sobald eine dieser Block-Berechnungen auf einem der Äste etwas länger dauert, dann bekommt der schnellere Ast von den Minern den Vorzug und der andere Ast wird obsolet.

In einem Angriff-Szenario heißt das, dass der Angreifer mehr als 50% der gesamten Rechenleistung benötigt, um schneller als die restlichen Miner neue Blöcke berechnen zu können.

Exkurs:

Das Bitcoin Netzwerk ist optimiert auf die Berechnung von SHA-256 Hashwerten und verwendet dafür Spezialhardware – sog. ASICs. Damit man ein Gefühl für die vorhandene Rechenleistung bekommt: 2014 hat das Bitcoin Netzwerk die Rechenleistung der weltweit 2 Milliarden PC überflügelt, welche auf 20 PetaHash/s geschätzt wurde. Die aktuelle Rechenleistung liegt bei 2000 PetaHash/s und damit beim 100-fachen aller 2 Milliarden PC von 2014[4].



http://bitcoin.sipa.be/

[4] Blockchain Temporality: Smart Contract Time Specifiability with Blocktime / Melanie Swan / http://www.blockchainstudies.org
https://books.google.at/books?id=2guPDAAAQBAJ&pg=PA189&lpg=PA189&dq=peta+hash+supercomputer&source=bl&ots=BCjylLqDXM&sig=0VM8YBOsFLErbCb-tsldYZ7txMM&hl=de&sa=X&ved=0ahUKEwig6Z7hjK7QAhXOERQKHdOgBCcQ6AEIRTAF#v=onepage&q=peta%20hash%20supercomputer&f=false

> *Das Netzwerk selbst erfordert nur eine minimale Struktur. Die Nachrichten werden auf Basis Best Effort („größte Bemühung"– wie auch beim Internet) gesendet und Knoten können nach Belieben das Netzwerk verlassen und wieder hinzukommen. Dabei akzeptieren sie die längste proof-of-work Kette als Beweis für die bestätigten Ereignisse, während sie weg waren.*

Hier wird vor allem die Zuverlässigkeit des Protokolls sichergestellt. Es ist jederzeit möglich, das Netzwerk zu verlassen und wieder dazuzukommen. Einzige Voraussetzung ist, dass man die längste Blockchain als die gültige akzeptiert und darauf aufbauend die nächsten Blöcke berechnet.

Weitere Details lassen sich natürlich im vollständigen Whitepaper nachlesen:

https://bitcoin.org/bitcoin.pdf

Spezialitäten im Bitcoin Zahlungsverkehr

Keine Umkehrbarkeit der Zahlung

Sie kennen das vielleicht von PayPal, Lastschriftverfahren oder Einzugsermächtigungen, wo es verhältnismäßig einfach ist, das Geld vom Empfänger zurückzufordern. Diese Rücküberweisungen sind im Bitcoin System nicht möglich, da es wie wir ja inzwischen wissen, keine Mittelsmänner gibt. Sollte jemand fälschlicherweise Bitcoins erhalten haben, dann muss die Rücküberweisung freiwillig durchgeführt werden. Wenn man aber nur die Bitcoin-Adresse hat, dann wird es schon sehr schwierig mit der Kontaktaufnahme.

Automatische Treuhänder

Große Bitcoin-Transaktionen oder Transaktionen ohne jegliches Vertrauen werden auch teilweise durch Multisignaturen abgesichert. Ein Beispiel dafür kann sein, dass der Sender und Empfänger je einen Schlüssel haben und dann noch ein Schiedsrichter einen weiteren Schlüssel bekommt. Wenn nun der Sender die Bitcoins schickt, dann kann der Empfänger das zwar sehen, aber nicht ohne Zustimmung des Senders darauf zugreifen. Der Empfänger erbringt daraufhin seine Leistung oder schickt ein Produkt und wenn es angekommen ist, dann geben beide die Zahlung frei. Sollte es zu einem Streitfall kommen, dann entscheidet der Schiedsrichter zusammen mit einer der zwei Parteien, wer das Geld bekommen soll.

Bitcoin ist nicht anonym

Viele glauben, auch wegen fälschlicher Medienberichterstattung, dass Bitcoin anonyme Überweisungen zulässt. Bitcoin ist vielmehr „Pseudonym“ und jeder (!) kann den Kontostand einzelner Bitcoin-Adressen einsehen. Wenn Sie also Ihren Bitcoin Kontostand verbergen wollen, ist es angeraten bei jeder Transaktion eine neue Bitcoin Adresse zu verwenden. Außerdem sollte klar sein, dass, wenn Sie mit Bitcoin bei einer Firma zahlen, dann sind in deren Datenbank Ihr Kundenkonto mit der verwendeten Bitcoin Adresse gespeichert. Gleiches gilt natürlich auch für gelieferte Güter die mit Bitcoin bezahlt wurden. Insofern sollten Sie nicht vermuten, dass jegliches kriminelle Handeln mit Bitcoin unentdeckt bleiben würde. Auch weil die Börsen sehr wohl mit den Behörden zusammenarbeiten. Näheres zum Schutz Ihrer Privatsphäre finden Sie unter: https://bitcoin.org/de/schuetzen-sie-ihre-privatsphaere

Sofort-Transaktion und bestätigte Überweisung

Die Verteilung einer Transaktion erfolgt innerhalb weniger Sekunden, aber erst in den darauffolgenden 10 Minuten wird die Überweisung bestätigt. Bis zur ersten Bestätigung kann noch geschummelt werden und so richtig abgesichert ist die Überweisung bei Bitcoin erst nach einer Stunde (oder 6 Bestätigungen). Das spielt in der Regel bei kleinen Beträgen und Vertrauensbeziehungen keine große Rolle, aber es sollte bei größeren Überweisungsbeträgen beachtet werden.

Steuer und Regulierung

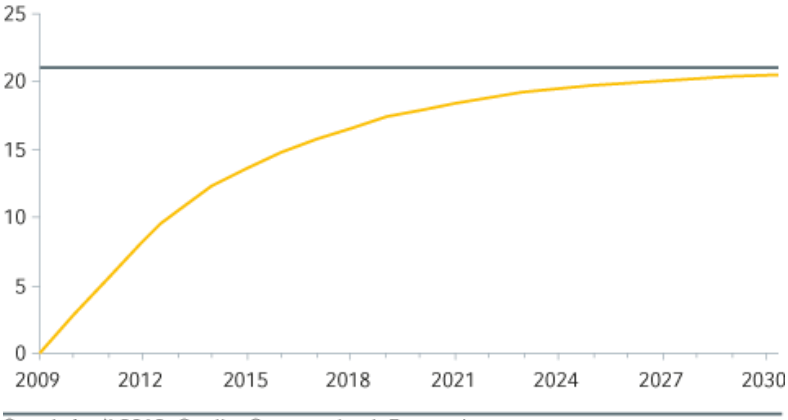
Am 22. Oktober 2015 hat der Europäische Gerichtshof (EuGH) mit einem Entscheid festgestellt, dass beim Umtausch von staatlichen Währungen in die digitale Währung Bitcoin keine Umsatzsteuer anfällt. Damit wird Bitcoin nicht als „Gut“ gesehen, sondern vielmehr mit gesetzlichen Zahlungsmitteln gleichgestellt.

Das heißt natürlich nicht, wie manchmal fälschlicherweise angenommen, dass man durch Bitcoin die gesetzlichen Steuern vermeiden kann. Bitcoin ist vielmehr wie eine Fremdwährung in der Buchhaltung zu verstehen und muss entsprechend regelmäßig in der Buchhaltung bewertet werden. Wer also Bitcoin als Zahlungsmittel verwendet, unterliegt den gleichen steuerlichen Vorschriften, wie wenn man Euro verwendet.

Bitcoin ist nicht reguliert und darauf weist auch die Finanzmarktaufsicht (FMA) auf ihrer Webseite hin. Bitcoin ist ein global aktives Netzwerk von Programmierern, Anwendern und Mining-Computern und schon alleine deshalb entzieht es sich der nationalen Regulierung. Dessen sollte man sich bewusst sein, wenn man mit Bitcoin hantiert. Es gibt also keine staatliche Instanz, die einen vor Schaden schützt!

Es ist aber auch fraglich, ob es bei einer globalen Währung für die wirtschaftliche Entwicklung in Österreich nicht das Beste ist, starke, ehrliche und Steuer zahlende Unternehmen zuzulassen und nicht anderen Ländern einen Standortvorteil zu geben, weil wir uns überreguliert haben!

Bitcoin – Geldmenge



Stand: April 2013; Quelle: Commerzbank Research

Die „Geldschöpfung“ von Bitcoin ist durch die verwendete Software fix definiert und deshalb wird es maximal 21 Millionen Bitcoin geben, wobei zurzeit ca. 16 Millionen Bitcoin erzeugt wurden. Im Bitcoin-Netzwerk entstehen aktuell alle 10 Minuten 12,5 Bitcoin und diese erzeugte Geldmenge bekommen die sogenannten Miner, die die Transaktionen bestätigen. Der gezeigte Kurvenverlauf bei der Bitcoinmenge kommt dadurch zu Stande, dass ca. alle 4 Jahre die alle 10 Minuten erzeugte Bitcoinmenge halbiert wird („Halving“).

Ein wichtiger Hinweis ist hier, dass schon seit mehreren Jahren das „Mining“ mit dem eigenen Rechner deutlich höhere Stromkosten verursacht, als man damit verdienen kann. Die Bitcoin Miningfarmen verwenden Spezialhardware (sog. ASICs – das ist quasi in Hardware abgebildete Software) und benötigt für einen wirtschaftlichen Betrieb Stromkosten im Bereich von 2-3 Euro-Cent. Sollte Ihnen jemand „Bitcoin-Mining“ verkaufen wollen, dann seien Sie auf der Hut, da auch hier Dinge versprochen werden, die wahrscheinlich nicht gehalten werden können (siehe Artikel von Bitcoin Austria über Bitclub Network).

Kreditwesen mit Bitcoin

Nachdem wie oben beschrieben die Bitcoins von den Minern alle 10 Minuten erzeugt werden und es keine andere „Geldschöpfungsquelle“ gibt, kann man es nicht mit dem Kreditsystem des heutigen Geschäftsbankenwesen vergleichen. Die in unserem Finanzsystem übliche Geldschöpfung durch Geschäftsbanken ist im Bitcoin-System nicht möglich, da ja nicht einfach mehr Bitcoins erzeugt werden können. Wer im Bitcoin-System Geld verleihen will, der muss es auch haben und damit entspricht es vielmehr dem Vollgeld, also real vorhandenem, von Zentralbanken ausgegebenem Geld. Nur im Fall von Bitcoin kommt das Geld nicht von der Zentralbank, sondern vom Mining-Netzwerk.

Totgesagte leben länger – Gesammelte Bitcoin Nachrufe

Unter https://99bitcoins.com/bitcoinobituaries/ findet der interessierte Leser eine unkommentierte Sammlung an Artikeln, warum Bitcoins Tage gezählt sind.

Bereit 2010 gab es den ersten kritischen Artikel. Die Wertentwicklung oder die Gefahr, Bitcoins durch Hacker zu verlieren – solchen Themen findet man in den Artikeln thematisiert. Heutzutage stehen vor allem die Schwierigkeit der Bitcoin-Developer-Community, eine gemeinsame Zukunftsstrategie zu finden, und die vielen anderen auf der hinter Bitcoin liegenden Blockchaintechnologie aufbauenden Entwicklungen im Zentrum der Artikel. Inwiefern Bitcoin es jemals schaffen kann, eine alternative Währung zu werden und wirklich, wie anfangs euphorisch proklamiert, das Ende der Banken und Finanzinstitute bedeuten kann, wird angesichts der hohen Investitionen, die Banken selbst in die Blockchaintechnologie machen, um ihre internen Prozesse zu optimieren, hinterfragt. Ob Bitcoin wirklich für die Anwendung in der Masse taugt, steht genauso auf dem Prüfstein, wie auch die Fragestellung, warum trotzt hoher Investitionen von Risikokapital in Bitcoin-Startups noch keine leicht anwendbaren Applikationen für die breite Masse existieren.

Bis Nov. 2016 sind 115 Todesmeldungen verzeichnet. Es ist höchst interessant in diesen großteils erstklassig recherchierten Artikeln zu schmökern. Nichtsdestotrotz muss man festhalten, dass Bitcoin nach wie vor existiert. Der Kurs für einen Bitcoin lag beim ersten gelisteten Eintrag vom 15.12.2010 bei 0,23 $ - beim aktuell letzten Eintrag vom 21.11.2016 bei 735,54 $. Auf der Bitcoin-Blockchain werden aktuell täglich rund um die 200.000 Transaktionen im Wert von gesamt rund um die 300.000 Bitcoins festgehalten[5].

Und auch, wenn es natürlich gute Argumente dafür gibt, dass man die Entwicklung von Bitcoin und Blockchain nicht mit der Entwicklung des Internets in den 1990er Jahren vergleichen kann, muss man sagen, dass es auch damals viele Stimmen gab, warum das Internet niemals skalieren kann und wird, eine jede neue Entwicklung wurde als Gefahr gesehen, die das Internet nicht überleben wird. Auch damals gab es gute Argumente, warum E-Mail, das WWW, Voice over IP oder Netflix den Tod des Internet bedeuten wird. Und dann kam doch eine neue Entwicklung, die plötzlich neue Möglichkeiten eröffnete… insofern kann man gespannt sein, was die Zukunft bringt.

[5] Die Statistiken wie auch die Transaktionen sind öffentlich einsehbar unter https://blockchain.info/.

Die FMA Warnung – Zum Nachdenken

Die europäischen Finanzmarktaufsichten warnen Banken und Privatpersonen davor, Bitcoins zu kaufen, zu halten oder zu verkaufen. Bitcoin wird nicht beaufsichtigt, außerdem könnte die quasi Anonymität von Transaktionen dazu führen, dass Bitcoin zur Bezahlung von kriminellen Aktivitäten genutzt wird – wie Geldwäsche, Drogenhandel oder Kinderpornographie. Auch die Globalität der Währung wird als Risiko angeführt.[6] Und die anderen vorgebrachten Argumente sind ebenfalls nicht von der Hand zu weisen, wie die fehlende Einlagensicherung, die Möglichkeit von Kursschwankungen, die Möglichkeit von Hackerangriffen, die fehlende zentrale Speicherung der Daten, die Möglichkeit von einem Totalverlust, wenn man seinen privaten Schlüssel verliert – denn ohne dem ist ein Zugriff auf die Bitcoins nicht mehr möglich. An diesen Argumenten ist nichts Falsches, es ist jedoch fragwürdig, ob man mündige und erwachsene Bürger wirklich warnen muss, oder ob es sich hierbei vielleicht auch nur um ein, auch bei anderen disruptiven Innovationen, Aufbäumen des bestehenden Systems handelt, wie es beispielsweise die Telefonnetze beim Internet gemacht haben, wo Modemverbindungen einfach vom Telefonanbieter getrennt wurden:

- Kriminelle sind sehr rasch dabei, neue Technologien für sich zu nutzen, das war schon immer so und wird auch immer so sein. Nur ist es nicht die Technologie, die das menschliche Verhalten bestimmt. Die Bedeutung von Bargeld wurde in diesen Kreisen sicher nur in geringen Ausmaß geschmälert. Auch wenn das Lösegeld für Ransomware in Bitcoin verlangt wird, bedeutet dies nicht, dass es diese Verschlüsselungstrojaner ohne Bitcoin nicht geben würde. Schwarzgeld existiert ebenfalls vorrangig in Bargeld, ein Grund, warum das Bargeld in Indien erst kürzlich abgeschafft wurde. Dem gegenüber steht der legale Gebrauch von Bitcoin als Zahlungsmittel und zahlreiche Möglichkeiten, wie Bitcoin Nutzen für einen jeden von uns stiften könnte.
- Der Kurs von Bitcoin schwankt und das teilweise beträchtlich. Im Prinzip ist auch ein Totalverlust möglich, denn der Bitcoin-Kurs entsteht aus dem Verhältnis von Angebot und Nachfrage. Jedoch muss man dazu sagen, dass der Wert von Geld immer davon abhängt, inwieweit man darauf vertrauen kann, am nächsten Tag noch etwas von Wert dafür zu bekommen. Dies gilt auch für alle anderen, auch die staatlich kontrollierten Währungen. Auch bei uns gab es Zeiten, wo wertlos gewordene Geldbündel den Kindern zum Spielen dienten oder per Scheibtruhe nach Hause

[6] https://www.fma.gv.at/fma-themenfokusse/bitcoin/

befördert wurden, um direkt als Heizmaterial zu dienen. Interessante Bilder dazu findet man im Netz[7]. Und das trotzt der staatlichen Kontrolle und Aufsicht. Die höchste bekannte Inflationsrate betrug 1945/46 in Ungarn 41,9 Trillionen Prozent pro Monat[8]. Auch wenn durch Währungsreformen gegengesteuert wurde, einen Großteil der Ersparnisse war in dieser Zeit wertlos geworden. Aktuell ist es so, dass die Geldmenge aus geldpolitischen Gründen ständig erhöht wird, in besonders hohem Maße beim Dollar. Mehr Geld im System ohne entsprechendes Wirtschaftswachstum bringt automatisch Inflation bzw. Spekulationen. Warum sollte also eine staatlich gesicherte Währung bei der aktuellen Geldpolitik wertsicherer sein? In Staaten mit hoher Inflation und eingeschränktem Devisenhandel wie Argentinien werden Bitcoin als sicherere Wertanlage gesehen, Gehälter werden teilweise in Bitcoin bezahlt.[9]
Das Risiko eines Totalverlustes gibt es auch bei anderen Anlageformen, die durchaus auch von Banken gehandelt werden. Rund um das Jahr 2000 bei der Dotcom-Blase[10] haben auch viele kleine Sparer ihr gesamtes Kapital an der Börse verspekuliert, aktuell kommt dies immer wieder beim gerade recht hippen Crowdinvesting vor[11] [12], ohne dass hier ein Anlegerschutz besteht.

- Ganz ähnlich wie mit der Stabilität einer Währung verhält es sich auch mit staatlichen Einlagensicherungen – zu 100 Prozent garantiert ist hier nichts. Unsere Kontostände auf der Bank sind eigentlich keine Guthaben sondern nur Schuldversprechen der Bank an uns. Die Bank verspricht uns, das Geld auf Verlangen auszuzahlen. Auch wenn dies in der Regel funktioniert, sollte man sich nicht darauf verlassen. Die Bank besitzt nicht so viel Geld, um alle ihre Schuldner bezahlen zu können. Ob eine Bank Geld auszahlen kann und will oder nicht, liegt bei ihr bzw. auch beim Staat. Griechenland hat beispielsweise 2015 die Bargeldbehebungen auf maximal 60 € pro Tag beschränkt, um ein Zusammenbrechen des Finanzsystems zu verhindern. Die staatliche Einlagensicherung ist in den meisten Ländern der EU auf 100.000 € begrenzt. Die

[7] http://www.akg-images.de/C.aspx?VP3=SearchResult&ALID=2UMEBMYFANUKT
[8] https://de.wikipedia.org/wiki/Peng%C5%91
[9] https://www.youtube.com/watch?v=e__m-w4N7NI
[10] http://www.manager-magazin.de/finanzen/artikel/a-186368.html
[11] https://futurezone.at/b2b/oesterreichisches-startup-woodero-meldet-konkurs-an/125.661.323
[12] http://crowd-investment.de/crowd-pleiten/

Sicherung erfolgt über einen Fond, in den alle Banken einzahlen werden. Inwiefern ein solcher Fond eine große Finanzkrise abdecken kann ist äußerst fraglich. Der österreichische Fond befindet sich gerade im Aufbau und sollte 2024 das Zielvolumen von 1,5 Milliarden Euro erreichen. Das reicht dann, um 130.000 Sparer mit einer durchschnittlichen Einlage von 11.700 € zu befriedigen.[13] Ob das ausreicht, um eine große Finanzkrise zu überstehen oder die Insolvenz einer Großbank abzufedern ist fragwürdig. Ob der Staat in einem solchen Fall die Einlagensicherung übernehmen kann, wer weiß… wenn, dann wahrscheinlich nur auf Kosten von Steuerzahler oder durch die Aufnahme neuer Schulden, also letztlich zahlt wieder die Gemeinschaft der Bürger. Und ein Staat hat immer die Möglichkeit, Bankrott zu gehen. Bitcoin kennt keine Schulden, niemand kann Geld schöpfen, indem er Kredite vergibt.

- Immer wieder ist die Rede von verloren gegangenen und gestohlenen Bitcoins, von Hackerangriffen und ähnlichem. Dazu ist zu sagen, dass Bitcoin im tagtäglichem Umgang dem Bargeld gleicht. Wer Bargeld versehentlich vernichtet, verliert oder es ihm gestohlen wird, der hat keinen Anspruch auf einen Ersatz. Ähnlich ist es bei Bitcoin, wem sein Wallet mit dem privaten Schlüssel durch Löschen, Verlust des Handys oder Diebstahl abhandenkommt, kann nicht mehr über seine Bitcoins verfügen, diese bleiben ungenutzt in der Blockchain gespeichert oder werden vom Dieb weiterverwendet. Hier wird laufend daran gearbeitet, die Sicherheit und Bedienerfreundlichkeit zu verbessern.
  Missverständnisse entstehen oft auch dadurch, dass Hackerattacken und Diebstähle bei Bitcoinbörsen als Fehler in der Bitcoin-Blockchain interpretiert werden. Vergleichbar wäre es, nach einem Bankraub zu sagen, die Währung sei unsicher.
- Die US-Finanzaufsicht warnt nicht vor Bitcoins, sie hat vielmehr Bitcoin und andere Kryptowährungen seit dem 18. März 2013 als Zahlungsmittel bzw. Währung eingestuft und somit die Rechtssicherheit rund um Bitcoin erhöht.

[13] http://www.konsument.at/geld-recht/einlagensicherung-318893946533

Der Abschluss: Häufig gestellte Fragen und ein Glossar der falschen Begriffe

Was ist Bitcoin?

Bitcoin ist ein Protokoll zur sicheren Überweisung eines Wertes (=Geld) zwischen zwei Partnern, die sich nicht vertrauen müssen und keinen Mittelsmann für diese Überweisung benötigen.

Was ist ein Wallet?

Das Wallet oder die Geldbörse ist für den häufigen Gebrauch in der Regel ein Computerprogramm (oder Handyapp), in dem die privaten Schlüssel gespeichert sind, um auf das damit in der Blockchain „weggesperrte“ Geld zugreifen zu können. Wenn das Handy kaputt wird, benötigt man ein Backup, um das Wallet wiederherstellen zu können.

Was ist die Blockchain?

Eine auf tausenden Rechnern verteilt gespeicherte, laufend aktualisierte und synchron gehaltene Datenbank.

Wie entstehen Bitcoins?

Bitcoins werden mit jedem Block, der von den sog. Minern errechnet wird, geschöpft. Zurzeit bekommt der Miner, der als erster ein kompliziertes Rätsel gelöst hat, 12,5 Bitcoin als Belohnung für den betriebenen Aufwand. Damit entsteht im Gegensatz zum sogenannten Fiatgeld (z.B. Euro oder Dollar) kein Schuldverhältnis, welches auch wieder beglichen werden muss.

Was sind die Miner?

Ein Miner (Software auf einem Rechner) rechnet den nächsten Block für die Blockchain aus und investiert dafür Energie. Die Analogie ist ähnlich einem Minenarbeiter, wodurch die Arbeitskraft das Gold aus dem Berg holte.

Wer definiert den Preis von Bitcoin?

Der Preis ergibt sich nur durch Angebot und Nachfrage. Wenn die Nachfrage auf den Wechselbörsen steigt, dann steigt auch der Preis und umgekehrt.

Wem gehört Bitcoin?

Es gibt keinen Bitcoin-Eigentümer, da es sich um ein dezentrales System handelt, welches wie Linux zwar von vielen verwendet wird, aber keiner einen Besitzanspruch hat. Theoretisch könnte eine Mehrheit der Miner gemeinsam die Blockchain manipulieren, ob das bei der Offenheit des Systems und der Menge an Miner praktisch klappt, ist fragwürdig.

Kann ich eine Bitcoin Transaktion rückgängig machen?

Nein, das ist nicht möglich, da es sich verhält wie eine Bargeldtransaktion. Der Empfänger muss das Geld freiwillig zurückgeben. Diese Funktionalität wird unter „unveränderlich“ (engl. immutable) als eine der herausragenden Eigenschaften von Bitcoin gesehen.

Ist eine Bitcoin Transaktion anonym?

Wenn man etwas im Bitcoin Netzwerk überweist, dann ist diese Transaktion „Pseudonym“ und man kenn nur die Adressen des Absenders und des Empfängers in Form von langen Zahlen-Buchstaben-Kombinationen. Um zu verhindern, dass die gesamte Zahlungshistorie auf einer Adresse nachvollzogen werden kann, gibt es Wallets, wo bei jedem Bezahlvorgang eine neue Adresse generiert wird.

Worum die uns geläufigen Begrifflichkeiten in Bitcoin nicht gut funktionieren?

Ein Wallet ist eigentlich keine Geldtasche, sondern vielmehr ein Schlüsselbund, der den Zugang zu meinen Bitcoins aufsperrt. Bitcoin ist kein Coin, also keine Münze, denn im Gegensatz dazu lässt sich in Bitcoin in beliebig kleine Teile teilen. Und auf der Blockchain wird kein Guthaben niedergeschrieben wie auf einem Konto, letztlich werden nur die Änderungen, also die Transaktionen notiert, das Saldo berechnet sich erst aus der Summe aller Transaktionen über die gesamte Blockchain. Wie recht oft bei neuen Technologien versuchen wir die Begriffe der bisherigen Lösungen weiterzuverwenden, auch wenn sie nicht mehr ideal passen. Denken Sie nur an die PS für Pferdestärke. Erst in den letzten Jahrzehnten haben sich die kW durchgesetzt.