Drescher & Cie Consult

Bitcoin und andere Kryptowährungen

Ein Praxisüberblick für Finanzberater

von Thorsten Pörschmann

Inhaltsverzeichnis

Die Blockchain

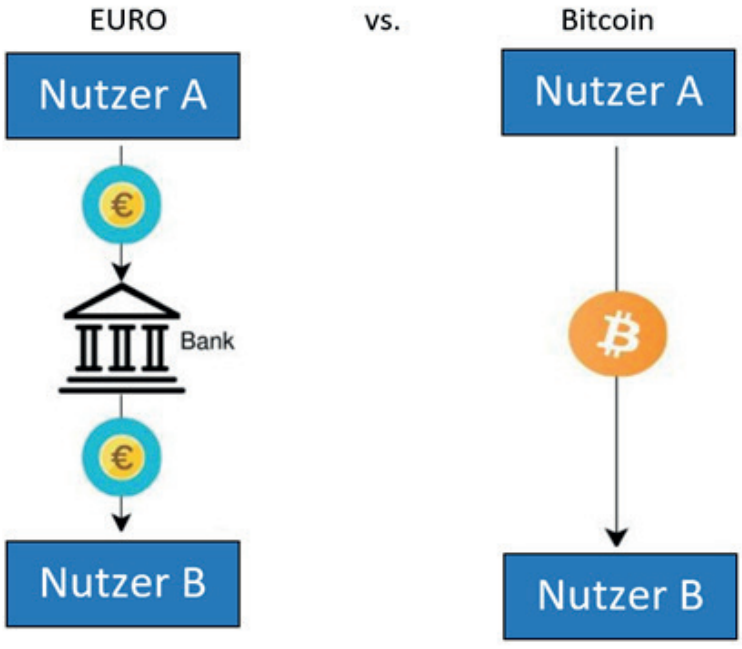
Eine Blockchain ist eine vollständige und unveränderliche Transaktionshistorie alle Transaktionen einer dezentralen Gemeinschaft, der jeder Teilnehmer zustimmt.

Diese Transaktionshistorie wird in regelmäßigen Zeitabschnitten aktualisiert. Neue Transaktionen werden in Blöcken zusammengefasst und hinzugefügt. Die Blockchain wird damit immer länger. Da jeder Teilnehmer die komplette Blockchain auf dem eigenen Rechner hat und damit ständig eine Überprüfung der Integrität der Blockchain stattfindet, gilt diese als fälschungssicher. Unzulässige Änderungen würden nicht zur gespeicherten, bestehenden Blockchain passen und entsprechend zurückgewiesen werden. Kryptowährungen sind nur ein Beispiel für den Einsatz einer Blockchain. So könnte man auch Grundstückseigentum z.B. über die Blockchain sicher verbriefen. Wichtig dabei zu wissen: es gibt keine zentrale Instanz. Das Netzwerk kontrolliert sich gegenseitig rund um die Uhr.

Einfach ausgedrückt ist das Netzwerk ein Verbund von Millionen von Buchhaltern, die sich gegenseitig kontrollieren und eine unveränderliche, von allen akzeptierte Historie durch neue Buchungen ergänzen, die auch wieder von allen akzeptiert werden müssen, bevor sie Gültigkeit erlangen.

Das Bitcoin-Netzwerk hatte seit seinem Entstehen eine Ausfallzeit von 0%. Es funktionierte mal schneller und mal langsamer (siehe Marktentwicklung), aber funktioniert hat es 24/7 ohne Ausfall. Um die Blockchain zu hacken, wären 51% der Rechenpower des Netzwerkes erforderlich. Die größten 500 Supercomputer der Welt kommen derzeit auf ca. 0,01% der Rechenleistung des Netzwerkes. Mit dem Wachstum eines Netzwerkes wird, wie man sieht, die Sicherheit so erhöht, dass sich die notwendigen Ressourcen für einen erfolgreichen Angriff dafür nicht aufbringen lassen. Zentralrechner im Bankwesen erfordern hier ungleich weniger Aufwand.

Eine Transaktion von Bitcoins im Vergleich zu einer herkömmlichen Zahlungsmethode sieht so aus:



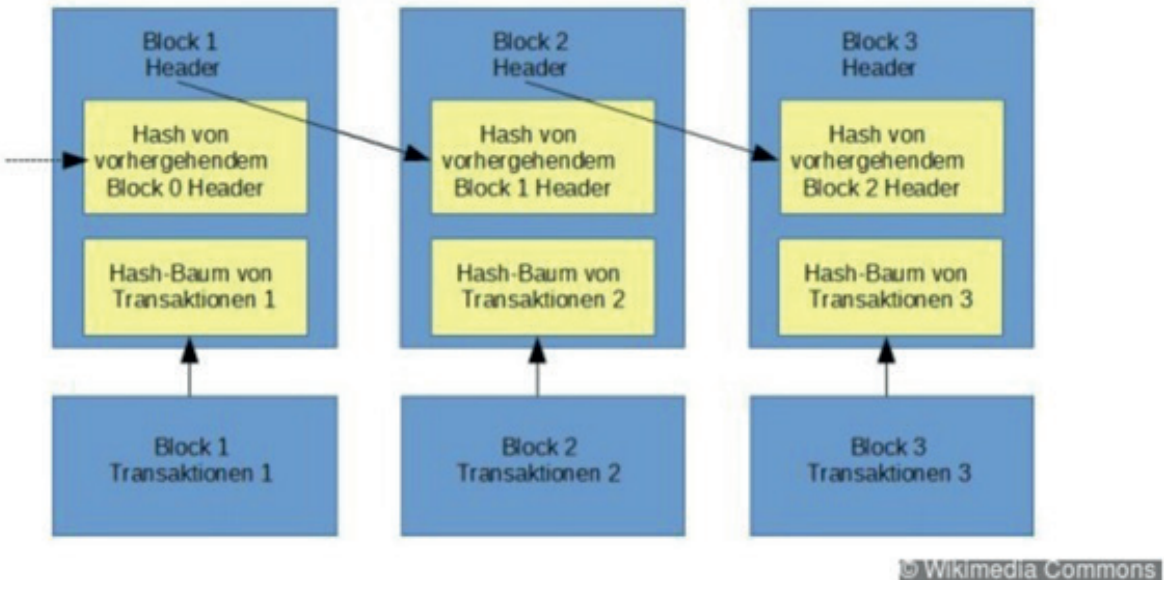
Quelle: 1Sigma GmbH

Die erste Anwendung der Blockchain war die Kreation der Cyberwährung Bitcoin durch einen Programmierer namens Satoshi Nakamoto, dessen Identität bis heute nicht wirklich geklärt ist. Bitcoin ist eine freie Peer-to-Peer-Währung, die ohne staatlichen Einfluss auf der Basis einer fälschungssicheren Blockchain betrieben wird. Durch diese wird das Vertrauen in eine Notenbank durch das Vertrauen in einen Netzwerkalgorithmus ersetzt. Weiterer Unterschied: Im Gegensatz zu herkömmlichen Währungen ist die maximale Anzahl von Bitcoins durch den Algorithmus begrenzt (siehe Mining).

Die Blockchain ist also eine Art und Weise, um Daten zu speichern. Auch verlässt ein Bitcoin nie die Blockchain, um auf einem Rechner gelagert zu werden. Der Zugang zum Bitcoin lässt sich lagern, die Bitcoins selbst sind immer in der Blockchain gespeichert - sowie die Zuordnung, wem diese gerade gehören (= dem, der Zugang dazu hat). Die Transaktionsdaten werden in so genannten Blocks gespeichert.

Mehrere Transaktionen werden zu einem Block zusammengefasst. Wenn ein Block „voll“ ist, kommen die folgenden Transaktionen in den nächsten Block. Jeder Block verweist auf den vorherigen. Die Blockchain ist also eine Kette von Blöcken. Dabei spielt das Hashing eine wichtige Rolle. Ein Hash ist eine Art digitaler Fingerabdruck von Daten. Jeder Datensatz, also jede Transaktion, hat einen eigenen Fingerabdruck, der ihn von anderen Datensätzen unterscheidet.

Außerdem wird jeder Block durch einen Header beschrieben. Jeder Header enthält den Hash des vorherigen Block-Headers, damit verweist er auf den entsprechenden Block. Auf diese Weise bilden die Blöcke eine Kette. Die so genannten Miner, die diese Transaktionen ausführen, Di



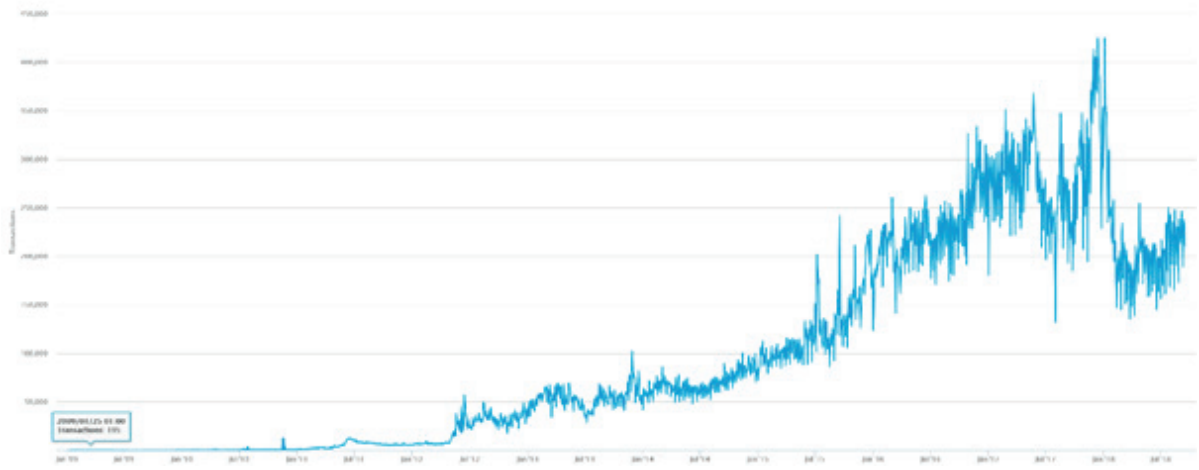
Jeder Knoten (Rechner) im Bitcoin-Netzwerk verfügt über eine Kopie der Blockchain, so dass er den „Kontostand“ eines jeden Bitcoin-Nutzers sowie die gesamte Transaktionshistorie kennt. Außerdem darf jeder Knoten der Blockchain einen neuen Block hinzufügen, indem er aktuelle Transaktionen bündelt.

Die so genannten Miner, die diese Transaktionen ausführen, bekommen als Belohnung Bitcoins ausgezahlt. Diese werden also durch den Betrieb der Blockchain generiert. Allerdings halbiert sich der Belohnungsbetrag regelmäßig, bis er eben dann gegen Null tendiert und ca. im Jahr 2030 der letzte Bitcoin geschürft wurde.

Bis zum November 2012 wurden 50, anschließend bis zum Juli 2016 25 und seitdem 12,5 Bitcoins mit jedem neuen Block ausgezahlt.

Es besteht in diesem Zusammenhang häufiger das Argument, dass, wenn die maximale Anzahl der Bitcoins geschürft ist, eben nur eine Programmanpassung erforderlich ist und es dann eben mehr davon gibt. Das geht bei einem fest verankerten Rechenalgorithmus genau so wenig, wie aus der Gleichung 2+2=4 irgendwann 5,5 herauskommt. Es geht mathematisch eben nicht. Der Bitcoinalgorithmus steht fest. Das hat, was Flexibilität und Geschwindigkeit angeht, Nachteile. Im Bereich des Vertrauensschutzes - aber eben auch unabänderliche Vorteile.

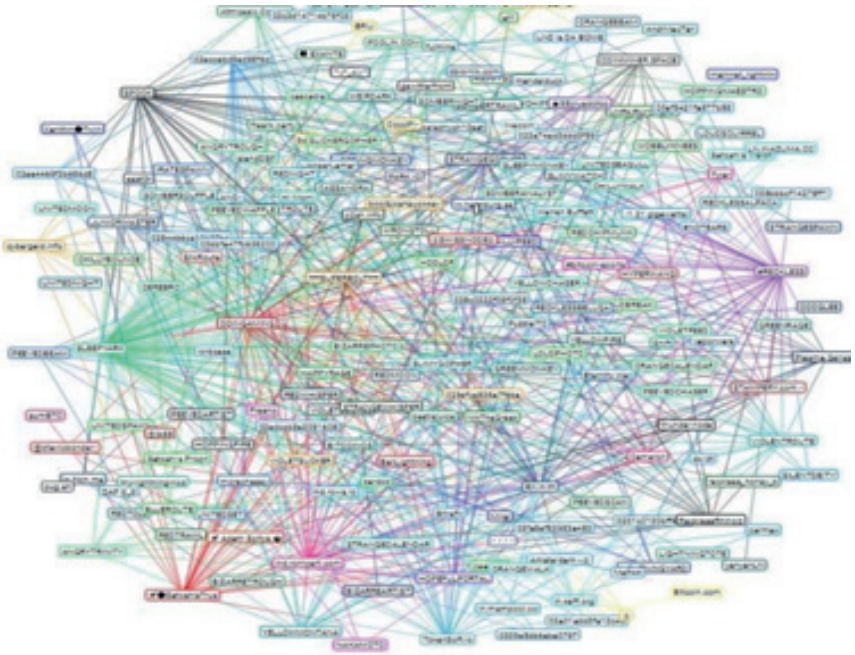
Der Anfangswert eines Bitcoins betrug 0,1 US$. Die erste Transaktion lief am 01.03.2009. Durchschnittlich wurden im Jahr 2010 etwa 150 Transaktionen pro Tag verzeichnet. Heute (Februar 2019) sind es etwa 350 000 Transaktionen pro Tag. Der gigantische Anstieg in der Bitcoin-Nutzung, der auch von Kursrückschlägen bisher nicht deutlich zu bremsen war, hat das Netzwerk an seine Leistungsfähigkeitsgrenze gebracht und insbesondere Ende 2017 verlangsamt. Die feststehende Blockgröße von 1 MB, in dem immer die gesamte Blockchain mit allen (!) historischen Transaktionen untergebracht werden musste (in Verbindung mit dem Transaktionslimit von max. 7 pro Sekunde), verzögerte Ausführungsbestätigungen um Stunden, wenn nicht Tage, und die Transaktionskosten stiegen extrem an (von wenigen Cent auf z.B. bis zu 80 US$).



Anzahl der Transaktionen pro Tag, Quelle: blockchain.com

In den Jahren 2009-2018 gab es schon verschiedene Zeitpunkte, zu denen man annehmen konnte, Bitcoin schafft es nicht und geht wieder unter. Da sich das Netzwerk bisher mit etwas Verzögerung immer an die Marktverhältnisse angepasst hat, ist dies aus technischer Sicht wenig wahrscheinlich. Die letzte bemerkenswerte Errungenschaft ist das Lightning-Netzwerk. Ein Ergänzungsnetzwerk, das Mini-Transaktionen außerhalb der Bitcoin-Blockchain zusammenfasst.

Das Lightning-Netzwerk hat per Konstruktion mehrere wünschenswerte Eigenschaften, um das Problem der Skalierbarkeit von Bitcoins zu lösen. Zu diesen zählen geringe Gebühren, welche insbesondere Micro-Payments ermöglichen. Außerdem ist die Privatsphäre der Teilnehmenden im Netzwerk höher als im Bitcoin-Netzwerk. Das Lightning-Netzwerk ermöglicht es, innerhalb eines Zahlungskanals gebührenfrei Geld hin und her zu überweisen. Daher lassen sich mit dem Lightning-Netzwerk erstmals weltweit Geldbeträge praktisch gebührenfrei in Echtzeit übertragen. Die Überweisungsgebühren im Bitcoin-Netzwerk sanken im Jahr 2018 wieder dramatisch. Die Transaktionsgeschwindigkeit hat sich gegenüber Herbst 2017 drastisch verbessert.



Visualisierung von Zahlungskanälen im Lightning-Netzwerk (Mitte 2018, Quelle: github.com)

Bitcoin

Aufbewahrung

Der sicheren Aufbewahrung von Bitcoin und anderen Kryptowährungen fällt eine Schlüsselrolle zu.

Aufbewahrt werden im Fall von Bitcoin und anderen nicht die Coins selbst, sondern der Zugang dazu. Das Verständnis, dass sich die Coins immer in der Blockchain befinden und nicht auf dem Rechner/Handy etc. des Eigentümers, ist ein wesentlicher Punkt bei der Betrachtung von Kryptowährungen als Asset. Die Problematik in der Aufbewahrung hat bis zum Jahr 2018 viele institutionelle Anleger davon abgehalten, sich näher mit diesem Segment als Anlagemöglichkeit zu beschäftigen. Das Jahr 2018 brachte auch hier sehr viele Veränderungen und selbst etablierte Börsen erweitern nun den Handel um Kryptowährungen und deren Aufbewahrung (z.B. die Börse Stuttgart mit dem Handelsprogramm BISON, Start Januar 2019).

Das Wallet-Prinzip

Kryptowährungen erfordern eine spezielle Verwahrungsform. Diese wird als „Wallet“ bezeichnet. Von diesen Wallets gibt es bestimmte Ausprägungen. Die Kenntnisse im Bereich Wallets und deren Funktionen und Schwachpunkten ist sehr wichtig, um einen Verlust der Coins zu verhindern. Es gab und gibt tausende von Betrugsfällen im Bereich Wallet-Hacking und die Schadensumme liegt sicherlich im Mrd. US$-Bereich. Bevor man den ersten Schritt in Richtung Krypto macht, ist die Beschäftigung mit der Verwahrung die absolut wichtigste.

Eine Wallet

Wir beziehen uns in der Folge auf den Bitcoin. Andere Kryptowährungen sind in der Regel identisch oder zumindest ähnlich. Eine Wallet ist eine elektronische Brieftasche. Darin liegen nicht die Coins, die sich immer in der Blockchain befinden, sondern die Zugangsdaten, um einen Coin zu bewegen. Die Daten bestehen aus 2 Teilen. Der öffentlichen und der privaten Adresse.

Eine öffentliche Adresse sieht z.B. so aus:

1F4NFmUvRqraiCMiJebzCRk3f8nExgtk8B

An diese Adresse lassen sich Bitcoins überweisen oder - falls Guthaben vorhanden ist - auch wegüberweisen. Ob auf dieser Adresse Guthaben ist, lässt sich auf blockchain.info leicht überprüfen:

Da diese Wallet für die Ausarbeitung neu erstellt wurde, enthält diese keine Coins und auch null Transaktionen. Die Wahrscheinlichkeit, dass es zwei Wallets mit identischer Kombination gibt, ist unwahrscheinlicher als das sich ein Sandkorn auf der Erde wiederholt. Um Bitcoins bewegen zu können, braucht man neben dem öffentlichen Schlüssel (Wallet-Adresse) auch noch den privaten Schlüssel. Dieser lautet für die erzeugte Wallet:

5KNPDmwWazkyKy32cJardDdQVgAT7rSevDhzKAv7WVHDshWZH7W

Der private Schlüssel ist nicht auf Blockchain.info einsehbar. Diese privaten Schlüssel müssen sehr sorgfältig und geheim aufbewahrt werden.

Verwahrung von Coins an der Börse

Hier hat, ähnlich wie beim normalen Geld, die Börse/Bank sowohl den öffentlichen als auch privaten Schlüssel und setzt ihn ein, wenn man eine Transaktion für seine Wallet aufgibt. Ähnlich einer Überweisung bei einer Bank. Ohne die Bank/Börse geht hier nichts. Ist die Bank offline, gehackt worden oder das Konto gesperrt, geht hier genauso wenig, wie bei einem Euro-Guthaben bei einer normalen Bank. Die Bank ist Herr des Geldes und nicht der vermeintliche Eigentümer. Das widersprach von Anfang an der Grundidee des Bitcoins. Es ist freies aber limitiertes Geld und verfügen kann der Inhaber ohne zentrale Instanz und ohne Möglichkeit der Blockierung von Konten, Zahlungswegen, etc.

Die Verwahrung von Coins an der Börse ist bequem - wenn man allerdings Pech hat und die Exchange gehackt wird, eben auch nicht sicher. Dass Exchanges gehackt werden, passiert mehrmals pro Jahr. Einlagensicherung hier: Fehlanzeige.

Trotzdem folgt hier ein Bild, wie so etwas aussieht: Ansicht eines Guthabens bei bitcoin.de, der bisher führenden Bitcoin-Börse in Deutschland (Stand Jan. 2019)

Meine Guthaben

Währung	Ihr Guthaben	Aktueller Gegenwert	Reserviertes Guthaben	Verfügbares Guthaben	Aktionen
BTC	1,07019782 BTC	3.195,70 €	0,00000000 BTC	1,07019782 BTC	
BCH	0,00000000 BCH	0,00 €	0,00000000 BCH	0,00000000 BCH	
BTG	1,03827044 BTG	8,92 €	0,00000000 BTG	1,03827044 BTG	
ETH	2,21745900 ETH	206,38 €	0,00000000 ETH	2,21745900 ETH	
BSV	0,00000000 BSV	0,00 €	0,00000000 BSV	0,00000000 BSV	
Gesamt		3.411,00 €			

Quelle: Bitcoin.de/Privataccount

Der Zugang ist zwar auch durch 2-Faktor-Identifizierung abgesichert, aber die privaten Schlüssel hält bitcoin.de stellvertretend für den Inhaber. Ist bitcoin.de nicht erreichbar, nützt die bisherige 100% Verfügbarkeit des Bitcoin-Netzwerkes nichts.

Verwahrung in einer Desktop- oder Handy-Wallet
Bei diesen Wallet-Typen werden öffentliche und private Schlüssel in einer Applikation verwaltet. Das hat Komfortgründe, denn Transaktionen können mit einem Klick ausgeführt werden, weil bei der Transaktion die beiden Schlüssel zusammengeführt werden. Wichtig zu wissen: Die Schlüssel befinden sich damit ausschließlich im Besitz des Inhabers der Wallet. Geht das Handy verloren, wird es zerstört oder entwendet, ist die Wallet mit den Coins weg. Daher ist es erforderlich, eine Widerherstellungsphrase zu generieren, aus der sich die Wallet wiederherstellen lässt.

Diese sollte an einem sicheren Ort aufbewahrt werden. Die Phrase wird in der Applikation meist unter dem Punkt Backup erstellt und sieht dann so aus:

Mit genau dieser im Zufallsverfahren erstellten Wortreihenfolge lässt sich eine Wallet wiederherstellen. Ohne: Die Coins sind nicht weg, aber man kommt nicht mehr dran.

Die Oberfläche einer Desktop-Wallet (hier EXODUS) sieht z.B. so aus:

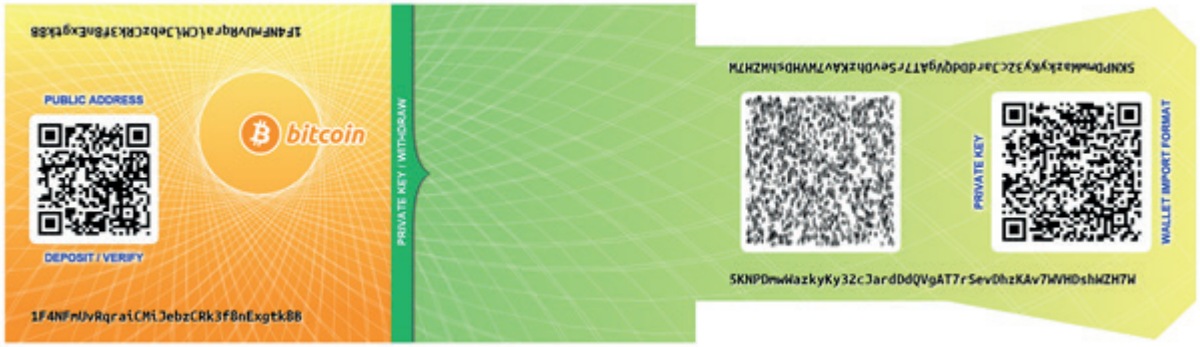
In dieser Wallet lassen sich verschiedenste Coins lagern und mit einem Service mit Namen „Shape Shift“ auch gegeneinander austauschen (handeln).

Lagerung für Profis

Es gibt die Möglichkeit, Wallets zu erzeugen, die gar keine Online-Verbindung haben und damit als ausgesprochen sicher gelten. Die Daten werden quasi kalt gehalten – also ohne Verbindung zum Internet. Daher heißt diese Verwahrungsart auch „cold-storage“.

Cold Storage

Eine Möglichkeit ist es, quasi einen „Bitcoin-Geldschein“ auf Papier zu erstellen. Eine so genannte Paper-Wallet:



Links steht die öffentliche Adresse und rechts (wenn eingeklappt und verklebt nicht sichtbar) der private Schlüssel. Überweist man nun z.B. einen Bitcoin von einer Exchange auf die öffentliche Adresse, kann der Inhaber dieses Scheins mit der Hilfe des privaten Schlüssels Abhebungen oder Bezahlungen mit dem Bitcoin oder eben Bruchteilen (z.B. 0,01) vornehmen. So lassen sich auch Bitcoins im Fluchtfall über Grenzen transportieren, z.B. auf den Arm eines Familienmitglieds die private Adresse mit Kugelschreiber geschrieben und die öffentliche Adresse per E-Mail vorab an eine Vertrauensperson im Zielland. Vorsichtshalber lassen sich noch ein paar Stellen verändern, die vor Einsatz wieder in die richtige Form gebracht werden. Ganz ohne Aufzeichnungen geht es auch. Das nennt sich dann „Brain-Wallet“ und besteht im Auswendiglernen des Codes. In Ländern mit instabilen Währungen ist der Bitcoin äußerst beliebt, um sich vor der kollabierenden staatlichen Währung zu retten. Dies wurde bisher sichtbar in Venezuela und Simbabwe.

Die beliebteste Cold-Storage-Methode ist aber nicht eine Paper-Wallet, sondern spezielle Formen von USB-Sticks, die als Tresore für die Schlüssel benutzt werden. Beispiele sind hier TREZOR oder auch LEDGER Nano S. Auf diesen wird mit hochgradiger Verschlüsselung der Zugang zu den Wallets gespeichert und die Sticks an einem sicheren Ort verwahrt. Auch diese lassen sich im Notfall mit einer Passphrase auf einem anderen Stick wiederherstellen. Die Sticks selbst sind passwortgeschützt und generieren beim Einsatz eine komfortable Benutzeroberfläche zum Verwalten von verschiedenen Kryptowährungen.

Handel

Der Handel mit Kryptowährungen wird hauptsächlich über so genannte Exchanges - also Börsen - durchgeführt.

Diese wurden ab 2017 international stark reguliert und Dutzende geschlossen. Eine vollständige Legitimation, Einhaltung von Geldwäschegesetzen und KYC- (Know your Costumer) Regeln sind heute die üblichen Rahmenbedingungen für die Genehmigung einer Handels-Lizenz. Um einen Eindruck zu bekommen, welche Volumina auf bitcoin.de in verschiedenen Zeiträumen gehandelt wurden:

Aktuelles Handelsvolumen

Zeit	Volumen (BTC)	Volumen (EUR)	Preis Durchschnitt
15min	0	0	—
1h	0	0	—
4h	6.74	37,160.82	5516.0894
12h	21.55	118,628.26	5505.2931
1d	148.82	805,595.22	5413.0533
2d	247.26	1,339,805.13	5418.6964
7d	807.64	4,440,497.37	5498.0978
30d	4,727.60	27,213,381.50	5756.2812
6m	34,582.94	214,765,967.01	6210.1714
1y	185,075.73	1,485,059,108.06	8024.0618

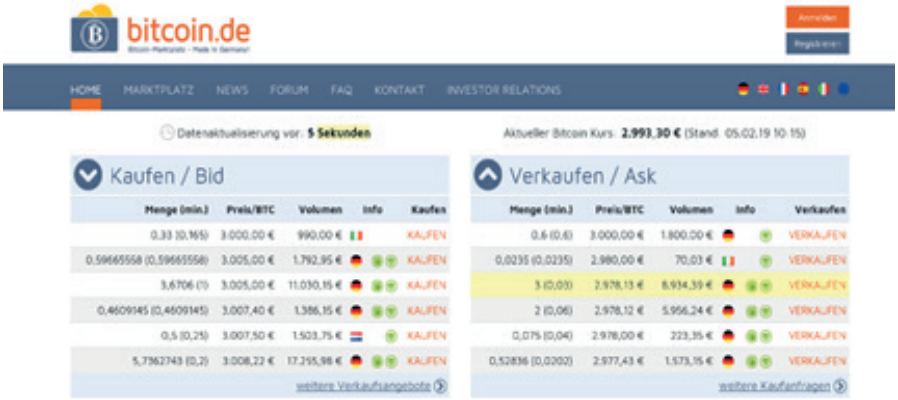
Quelle: Daten www.bitcoincharts.com Grafik: 1Sigma GmbH

Das Handelsvolumen von 1,48 Milliarden Euro innerhalb eines Jahres zeigt, dass Bitcoin auch im Inland mehr ist als ein Nischenprodukt. Verglichen mit einer der größeren asiatischen Börsen relativiert sich aber die Bedeutung des deutschen Handelsplatzes. So setzt z.B. Bithumb (Korea) etwa 240 Mio. US$ am Tag nur in Bitcoin um, d.h. der Jahresumsatz von bitcoin.de ist in nur wenigen Tagen an einer (!) asiatischen Börse erreicht. Insgesamt ist der gesamteuropäische Anteil am globalen Krypto-Umsatz kein wesentlicher Faktor, ebenso ist die europäische Berichterstattung zum Thema nicht marktrelevant.

Im Jahr 2018 hat sich zwar im Kryptobereich ein massiver Bärenmarkt ereignet, jedoch verbreiterten sich in Deutschland dessen ungeachtet die Möglichkeiten zum Handel. Sogar eine regulierte Börse stieg in den Handel mit Kryptowährungen im Februar 2019 mit ein (Börse Stuttgart mit BISON).

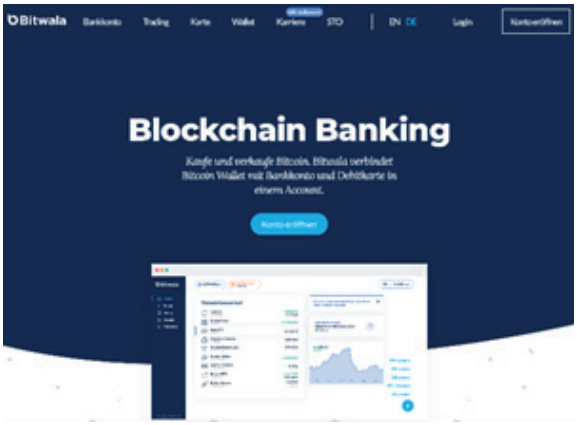
Handelsplattformen in Deutschland ein Überblick:

1. Bitcoin.de (www.bitcoin.de)



Der Handelsplatz bitcoin.de der zur börsennotierten Bitcoin Group SE gehört (Erstnotiz am 31.05.2013) ist der älteste regulierte Anbieter von Bitcoinhandel in Deutschland und kooperiert eng mit der FIDOR Bank. Auf der Handelsplattform werden Käufer und Verkäufer quasi aneinander vermittelt. Im sog. Sekundenhandel bei der Benutzung eines FIDOR-Kontos zur Abwicklung ist sofortiger Handel möglich. Die möglichen Handelsvolumina richten sich nach der Handelshistorie des Nutzers. Mit dem sog. erreichten Trust-Level erhöhen sich im Laufe der Zeit mit Anzahl der durchgeführten Transaktionen und deren Volumen auch die Möglichkeiten für die Akteure. Die Anzahl der registrierten User liegt bei über 500.000, das Transaktionsvolumen lag im guten Kryptojahr 2017 bei weit über einer Milliarde Euro. In den letzten 6 Monaten waren es ca. 160 Mio. Euro allein im Bereich Bitcoin. Der Handelsplatz hat im Kryptobereich schon einige Haussen und Baissen gesehen, gilt als etabliert und bisher skandalfrei. Im Jahr 2018/2019 kommt in Deutschland nun zum ersten Mal Wettbewerb für den Marktführer auf.

2. Bitwala (www.bitwala.com)



Im Dezember 2018 ging Bitwala aus Berlin in Kooperation mit der Solaris-Bank (als sog. tied agent) und 40.000 vorregistrierten Interessenten an den Start. Bitwala bietet neben dem Kryptohandel ein voll reguliertes Blockchain-Konto mit SEPA-Überweisungsmöglichkeiten, einer Debitkarte sowie Einlagensicherung in Höhe von 100.000 EURO (bezieht sich auf Kontoguthaben bei der SOLARIS Bank). Quasi ein Girokonto mit angeschlossener Kryptowallet, Handelsmöglichkeit und der Möglichkeit Kryptowährung zu verkaufen und damit die Debitkarte mit EURO zu laden. Ähnelt ein wenig der Grundidee von TENX aus Singapore, nur dass es zum einen nun verfügbar ist und der deutschen Regulierung unterliegt.

3. BISON-App (www.bisonapp.de)

Medial die größte Aufmerksamkeit bekam das Projekt der Börse Stuttgart: BISON.
In der Tat dürfte es der erste Handelsplatz für Kryptowährungen sein, der unter der Obhut einer regulierten herkömmlichen Wertpapierbörse steht (Börse Stuttgart). Das sorgt für einen Vertrauensvorschuss und die einfach gestalteten APPs für Smartphones lassen sich quasi intuitiv bedienen. Die Kontoeröffnung mit Legitimation über IDNOW dauerte im Selbsttest keine 10 Minuten. Angeboten werden zum Start Bitcoin, Etherium, Litecoin und Ripple. Leider erlaubt BISON nicht (!) die Übertragung von bestehenden Kryptoguthaben. Man kann dort zwar Krypto gegen EURO kaufen und verkaufen und auch Krypto wegtransferieren, aber eben nicht einbringen. Schlagen wir einen Bogen in unsere Fondswelt: Eine neue Depotbank erlaubt den Wertpapierhandel, aber bestehende Bestände von einer anderen Plattform können nicht dahin eingebracht werden – also Depotübertrag nicht möglich. Das mag hier regulatorische Gründe haben, aber kann sich als deutlicher Wettbewerbsnachteil darstellen.

Fazit:

„Krypto ist unreguliert“ stimmt für Deutschland so als Aussage nicht mehr. Sogar in Verbindung mit einem SEPA-fähigen EURO Konto, Debitkarte mit Chip und kontaktloser Bezahlfunktion und Handelsmöglichkeiten für Kryptowährungen gibt es ein Angebot im regulierten Bereich.

Andere Möglichkeiten, Kryptowährungen zu kaufen und zu verkaufen, ergeben sich über Austauschservices wie z.B. shapeshift, was auch in eine Wallet mit eingearbeitet werden kann. Andere Anbieter sind webbasiert und erlauben den Erwerb nach Identifizierung mit Kreditkarte, Überweisung etc. und senden die Coins dann an eine Wallet-Adresse, die der Käufer beim Erwerb angibt (z.B. www.bitpanda.de). Diese Formen sind einfach gehalten, weil eine aufwändige Kontoeröffnung nicht erfolgen muss (Legitimation allerdings schon), sind allerdings gegenüber dem Handel auf Exchanges teurer.

In diesem Zusammenhang ein Hinweis zur angeblichen Anonymität von Bitcoin etc.:

Es handelt sich um eine Pseudoanonymität. Da die Blockchain jederzeit transparent ist, lassen sich Zahlungen von Wallet zu Wallet verfolgen und damit auch rückverfolgen. Da Wallets keinen Klarnamen der Eigentümer tragen, ist das bis dahin anonym. Allerdings lassen sich die Coins auch auf Wallet-Adressen verfolgen, die von einer Exchange stammen. Hier sind den Wallet-Adressen aber die Kundennamen zugeordnet (Geldwäschegesetze). Wird eine Transaktion bis zu einer solchen Wallet durch Finanz-Forensiker zurückverfolgt (z.B. bei Geschäften im Darknet), wird der Name bei der Exchange aufgedeckt (die Börsen kooperieren hier quasi alle). Strafverfolgung ist hier also alles andere als unmöglich. Die Verschleierungsservices wie z.B. Coinmixer gingen durch Regulierung im Jahr 2018 vom Netz. Die Kryptowährungen Monero und Dash sind durch eingebaute Anonymisierungsfunktionen hier eher Exoten, ziehen derzeit aber die Aufmerksamkeit von Regulierern auf sich.

DATENSCHUTZ | Von Daniel Mützel | Aug. 1 2017, 2:04pm

Exklusiv: Die größte deutsche Bitcoin-Plattform gibt Kundendaten an die Polizei weiter

Für die Polizei ist es ein Leichtes, an Nutzerdaten der größten deutschen Bitcoin-Börse zu gelangen. Kunden der Plattform können mit einem weit geringeren Schutz rechnen als bisher angenommen.

Quelle: motherboard.vice.com

Einsatz als Währung

Die Nachfrage nach Kryptowährungen stieg im Zusammenhang der Akzeptanz als Zahlungsmittel im Laufe der Jahre an. In Deutschland gab es vor einigen Jahren nur wenige Akzeptanzstellen, die Güter und Dienstleistungen gegen Bitcoin angeboten haben. Besonders zu erwähnen ist die Szenenkneipe Room 77 in Berlin, die bis heute ein Szenetreffpunkt für Kryptofans ist und Bier & Burger seit Jahren auch gegen Bitcoin anbietet. Die Akzeptanz von Bitcoin als Zahlungsmittel feierte größere und kleinere Erfolge. DELL Computer erlaubte vor einigen Jahren den Erwerb von Computern über seine Webseite in Bitcoin. Der Durchbruch geschah allerdings im Frühjahr 2017, als die Bank of Japan Bitcoin als zulässiges inländisches Zahlungsmittel akzeptierte. In einer der führenden Industrienationen mit über 160 Mio. Einwohnern ist Bitcoin im Straßenbild nichts Ungewöhnliches mehr. Der Bitcoinkurs, der vor der Ankündigung der BOJ bei etwa 1000$ lag, hat sich nach der Ankündigung sehr schnell vervielfacht.

In Deutschland stufen die Bankenaufsicht und das Finanzministerium Bitcoin als privates Geld ein. Steuerlich gilt es als digitales, nicht abnutzbares Wirtschaftsgut, was es im Vergleich zu anderen Finanzanlagen privilegiert. Wie bei physischem Gold gilt keine Abgeltungssteuer und Wertzuwächse sind nach einer Spekulationsfrist von 12 Monaten steuerfrei. Dies gilt im Moment für alle Coins, die keine Erträge durch Ausschüttungen oder Zinszahlungen erwirtschaften. Bei nunmehr etwa 2100 Kryptowährungen gibt es immer Ausnahmen, die sich in einem Grundsatzartikel nicht erfassen lassen.

Regulierung

Bitcoin war bis zum Jahr 2017 vergleichsweise wenig reguliert und der Handel wenig beaufsichtigt. Ende 2018 lässt sich hingegen feststellen, dass es quasi kein Land mehr gibt, in dem Kryptohandel unreguliert ist. In der Regel haben die Finanzministerien Rahmenbedingungen definiert, Lizenzpflicht für Börsen eingeführt und bestimmte Formen der Kryptowährungen schlicht verboten.

Venezuela lancierte die erste staatliche Kryptowährung mit Hinterlegung von Erdölreserven, den Petro. Nordische Länder, in denen Bargeld auch heute schon eher ein exotisches Zahlungsmittel ist, treiben die Überlegungen von staatlichem Kryptogeld voran. Echtzeitüberweisungen ohne Gebühren und ohne Bankenapparat zur Ausführung können ein globaler Wettbewerbsvorteil sein.

Es gibt bereits 3 an den US$ gebundene Kryptowährungen (1:1 mit US$ hinterlegt), die quasi weltweite Blitzüberweisungen von Wallet zu Wallet ermöglichen, eben ohne Banken als Zwischenstation. Diese Kryptos werden auch als „Stablecoins“ bezeichnet. Die bekannteste ist Theter mit einer Marktkapitalisierung von 2,0 Milliarden US$.

Weltweit existieren einige tausend Unternehmen im Kryptobereich. Auch in Europa ist eine eigene Industrie entstanden und siedelt sich in kryptofreundlichen Staaten wie der Schweiz oder auch Malta an. Dabei geht es häufig nicht um Finanztransaktionsgesellschaften/Börsen, sondern um den Einsatz von neuen Technologien im Bereich Verbriefung, Fälschungssicherheit, etc. Die Wahrscheinlichkeit, dass Krypto als Zeitgeisterscheinung wieder ganz verschwindet, liegt etwa bei null.

Zunehmende Regulierung hatte für den Kryptomarkt auch eine gute Seite. Institutionelle Anleger haben den Markt entdeckt und handeln meist über für sie geschaffene Instrumente mittelbar am Kryptomarkt. Im Laufe des Jahres etablierten sich auch einige Treuhandsysteme für Währungsverwahrung, die Bestände auch gegen Verlust versichern. Diese Unternehmen erlauben es nun auch institutionellen Investoren, Bestände direkt am Markt aufzubauen, weil das Problem der sicheren Verwahrung nun Lösungen hervorgebracht hat. Nach der letzten Retailhausse in 2017 (siehe Kursentwicklung) ist der Markt im Jahr 2018 zunehmend von institutionellen Teilnehmern dominiert, die bisher seit 2009 eben keine große Rolle spielten.

3. Andere Kryptowährungen, ICO und digitale Token

Neben Bitcoin existieren derzeit weitere ca. 2000 Coins und digitale Token. Die Masse davon entstand 2017/2018. Die zweitbekannteste Kryptowährung heißt Ethereum und wurde durch eine Crowdfunding-Aktion im Jahr 2015 für 1$ pro Stück ins Leben gerufen (Kurs derzeit ca. 100$).

Ethereum basiert, wie auch Bitcoin, auf der Blockchain-Technologie. Im Unterschied zu Bitcoin ist Ethereum jedoch keine reine Kryptowährung, sondern auch eine Plattform für sogenannte Dapps (Distributed Apps), die aus Smart Contracts bestehen. Für Smart Contracts gibt es eine Vielzahl von Anwendungen, unter anderem E-Voting-Systeme, virtuelle Organisationen, Identitätsmanagement und Crowdfunding.

Wird ein neuer Coin angeboten, spricht man auch von einem so genannten ICO = Initial Coin Offering, also die Erstausgabe eines digitalen Tokens. Eine Flut dieser Coins erreichte 2017/2018 den Markt mit desaströsen Kursentwicklungen, Betrugssystemen oder schlicht keinem Geschäftsmodell dahinter. Branchenkenner schätzen, dass sich 95% aller Kryptowährungen kursmäßig wieder der Nullmarke nähern (Stand Feb.19: Wir sind auf einem guten Weg dahin). Die Ausgabe von Token basiert bis heute auch nicht auf einem Wertpapierverkaufsprospekt, sondern einem so genannten White Paper, einer unverbindlichen Absichtserklärung mit Werbecharakter.

Regelmäßig erhalten Tokeninhaber keine Firmenanteile, keine Gewinnausschüttungsansprüche und sind auch an nichts rechtlich beteiligt. Der Coin ist damit quasi eine digitale Spendenquittung, die in der Hoffnung gehalten wird, dass es Marktteilnehmer gibt, die dafür mehr bezahlen, da deren Anzahl limitiert ist.

Wird eine Kryptowährung weltweit als Zahlungsmittel akzeptiert, entsteht ein Wechselkurs zu anderen Währungen. Dies ist bei Bitcoin, Ethereum und einigen anderen der Fall. Bei allen anderen müssen sich dauerhaft genügend Liebhaber finden, die bereit sind „echtes Geld“ für digitale Liebhabertoken einzusetzen. Da der Markt für Liebhabertoken aber mit Milliarden Coins geflutet wurde, ist das Segment im Moment eher von einem drastischen Überangebot geprägt. Als Beispiel für einen erfolgreichen ICO aus dem Jahr 2017 mit dann doch eher unerwartetem Verlauf soll einmal TENX gelten.

Exkurs: ICO TENX

TENX ist ein in Singapore ansässiges Unternehmen, das sich der Idee, Kryptowährungen ausgebbar zu machen, gewidmet hat. Eine App-basierte Krypto-Wallet mit verschiedenen Krypotwährungsoptionen in Verbindung mit einer VISA Kreditkarte. Mit der Kreditkarte lassen sich alle Güter und Dienstleistungen in normalen Währungen wie EUR oder US$ erwerben und im Hintergrund wird bei der Zahlungstransaktion Kryptowährungsguthaben (zu Beginn nur Bitcoin) getauscht. Der Händler bekommt beim Bezahlvorgang nicht mit, dass z.B. der Einkauf bei LIDL quasi mit Bitcoin bezahlt wurde. Die Idee war nicht neu. Zum Zeitpunkt des ICO gab es bereits ca. 8 weitere Unternehmen mit Krypto-Kreditkarten. Die bekannteste heißt WIREX, u.a. mit deutscher Webseite und deutschem Kundensupport.

Das Besondere an dem ICO von TENX war, dass dem Zeichner im White Paper „versprochen" wurde, ihn an den Umsätzen von TENX über die Ausschüttung von weiteren Token zu beteiligen. Der Token von TENX heißt PAY. Hält man PAY, bekommt man einen Anteil der von TENX vereinnahmten Kreditkartengebühren dann als Ausschüttung wieder als PAY Token, bzw. Bruchteile davon auf der Wallet gutgeschrieben. Man ist zwar nicht an der Firma beteiligt, hat mit dem PAY Token aber so etwas wie einen digitalen Genussschein. Soweit die Idee.

Im Vorfeld des ICO gab es mächtiges Marketing auf Social Media-Kanälen und die möglichen Umsätze des Geschäftsmodells wurden in die Aber-Milliarden hochgerechnet. Immer unter der Prämisse, dass die etablierten Kreditkartenanbieter sich das alles nur vom Seitenrand anschauen und den neuen Karten den Markt überlassen. Vergessen wurde dabei, dass keiner der Krypotkartenanbieter eigener Kartenemittent ist, sondern gelabelte Karten von VISA oder MASTERCARD benutzt werden. Der ICO war in 7 Minuten ausplatziert.

Kursmäßig wurde PAY erst gefeiert, bis die ersten Schwierigkeiten auftauchten. Die Regulierer sahen in einem Token, auf dem eine Ausschüttung erfolgt, ein wertpapierähnliches Konstrukt, was dann aber möglicherweise eine Börsenzulassung benötigt. Daher bleiben auch erst einmal die erwarteten Ausschüttungen auf den Token aus, um Ärger mit den Finanzbehörden zu vermeiden. Am Jahresanfang 2018 traf es dann quasi alle Kryptokreditkartenunternehmen, deren Karten bis dahin reibungslos funktionierten. Der quasi einzige Provider für alle Kryptokarten war Wavecrest aus Gibraltar, die gelabelte VISA Karten zur Verfügung stellten. Wavecrest verlor von einem auf den anderen Tag seine Kreditkartenlizenz und alle Kryptokarten wurden ungültig. Zunächst wurde kommuniziert, dass die Nachfolgekarte bei TENX bis Ende des ersten Quartals 2018 verfügbar ist. Bis Dezember 2018 ist dies aber nicht der Fall. Fazit: Das Versprechen aus dem White Paper wurde nicht gehalten und keine Karten sind nicht gut für den Kursverlauf des Tokens. Und dies ist noch ein harmloses Beispiel mit einer Firma, die es noch gibt und die nach wie vor an einer Lösung arbeitet. Andere haben außer einem White Paper gar nichts abgeliefert. WIREX schaffte es übrigens im 2. Quartal 2018 tatsächlich, die Nachfolgekarte auf den Markt zu bringen. Nun sogar mit kontaktloser Zahlungsmöglichkeit und ETHEREUM als weiterer Währungsoption.

Der PAY Token stieg von unter 1 US$ in der ersten Euphorie auf über 5 US$. Das zweite Hoch folgte in der Retail-Kryptohausse im Dezember 2017 (knapp 5 US$), beträgt zurzeit etwa 0,25 US$ und ist damit als ein ICO des Jahres 2017 noch vorzeigbar. Andere verzeichneten Verluste bis 99,5%.

Das „Hochjubeln“ der Preise von Kryptowährungen über gezielte Käufe und begleitet von medialer Marschmusik auf Social-Media-Kanälen wird als PUMP bezeichnet. Eine Fangruppe auf Facebook für einen Coin auch als PUMP-Group. Das gezielte Hochziehen von Kursen mit dem Abladen an das unbedarfte Publikum wird als DUMP bezeichnet. Der gesamte Vorgang als „Pump and Dump“. Der Laie hat hier keine Chance. Insideraufsicht gibt es nicht und eine Marktmissbrauchsverordnung ebenfalls nicht. Die großen Coins, wie z.B. Bitcoin mit einer Marktkapitalisierung von über 100 Milliarden US$, sind nicht mehr leicht beeinflussbar. Bei den Kleineren und Kleinsten kommt so etwas täglich vor.

4. Marktentwicklung seit 2009

Die Grundidee stammt aus der Hackerszene, im Angesicht der Finanzkrise eine von Regierungen und Notenbanken unabhängige, nicht verwässerbare Währung zu schaffen, die mit nur geringsten Transaktionskosten weltweit ohne Eingriffsmöglichkeiten von Staaten transferierbar ist. Wenn es um die Umsetzung dieser Gedanken geht, ist es mit Bitcoin gelungen.

Für Programmierer und Systemkritiker ist der Auftrag damit erfüllt. In fast 10 Jahren eine Ausfallzeit von null aufzuweisen und einen Transfermechanismus erschaffen zu haben, der seit Beginn 24 Stunden am Tag, 7 Tage die Woche läuft, ist im Geldwesen einzigartig. Es gibt keinen zentralen Angriffspunkt zum Hacken, keine Firma Bitcoin, die Regeln aufstellt und keine heimliche Gebührenmaschinerie, keine Bestandspflegen, sondern nur Bits und Bytes, öffentliche und private Schlüssel und die hohe Eigenverantwortung des Nutzers. Hat er keine Ahnung, macht einen Fehler oder arbeitet nicht sorgfältig, dann ist das Geld unwiederbringlich verloren. Es haftet hier niemand außer einem selbst. Faires System, aber eben weit davon entfernt, endkundentauglich zu sein.

Es gibt aus der Anfangszeit des Bitcoins Wallets mit tausenden Coins, die sich seitdem nicht bewegt haben. Als Bitcoin noch bei wenigen Cents notierte, waren tausend Bitcoin gerade 100 US$. Wenn da der private Schlüssel abhandenkam oder die Festplatte weggeworfen wurde, war es nicht wirklich tragisch.

Diese Coins sind zwar in der Blockchain noch vorhanden, aber quasi gestorben, weil man diese weder bewegen noch handeln kann. Diese Coins gibt es also nur noch theoretisch. Man spricht hier auch von so genannten Zombiecoins. Diese muss man gedanklich auch alle von der maximal möglichen Anzahl von Bitcoins abziehen. Die maximale Geldmenge ist durch das Netzwerkprotokoll auf 21 Millionen Einheiten festgelegt und kann nicht durch einzelne Teilnehmer beeinflusst werden. Die maximale Menge ist um 2030 erreicht. Aktuell etwa 17,5 Mio. Stück.
Ein Bitcoin ist im Vergleich zu den weltweiten Geldmengen in den Währungen US$, EUR, YEN etc. ein seltenes Vehikel. Verschiebungen von Geld in oder aus dem winzigen Kryptomarkt führen zu erheblichen Kursbewegungen. Die letzte Abwärtsbewegung von ca. 20.000 US$ auf 3.400 US$ lässt die Finanzindustrie vom „Krypto-Crash“ sprechen. Allerdings ist eine solche Bewegung im Bereich Bitcoin eher als durchschnittliche Korrektur zu sehen, zumindest wenn man lange genug dabei ist und schon mehrere Korrekturen von bis zu über 90% gesehen oder mitgemacht hat. Aktuell steht der Kurs noch bei einer Verzehnfachung in 3 Jahren und einer Verdreitausendfachung in nicht einmal 10 Jahren.

So richtig gecrasht ist hier nichts, im Gegenteil: der Langfristchart weist steigendende Böden auf und in dieser Perspektive ist die außerordentliche Entwicklung deutlicher zu sehen. Im Grundmuster hat sich der Bitcoinkurs vom Ausgangspunkt immer mindestens verzehnfacht (also z.B. von 10 auf 100) und korrigierte dann um 80-90%, um sich danach vom Hochpunkt (also hier den 100) wieder zu verzehnfachen.

Die nächste Korrektur führte von 1.100 auf 170 zurück, von da ging es dann auf 20.000 und zurück auf 3.300. Hier die Haussen und Baissen in der großen Perspektive:

Quelle: Tradingview

Der letzte so genannte Kryptowinter begann 2014 und endete im Dezember 2016. Der Kursverlust betrug hier insgesamt ca. 80%. Dann begann der Anstieg von 280 US$ auf 20.000 US$. In den Jahren des Kryptowinters ist der Bitcoin medial mehrmals gestorben. Es war aber nur eine Korrektur der vorher aufgetretenen blasenhaften Erscheinung. Im Prinzip ist die Entwicklung (bisher) eine Abfolge von Preisblasen mit anschließenden scharfen Korrekturen. Im Moment steht der Bitcoinkurs trotz des Absturzes etwa beim mehr als dem zwölffachen des letzten Börsenmarkttiefs von 2016.

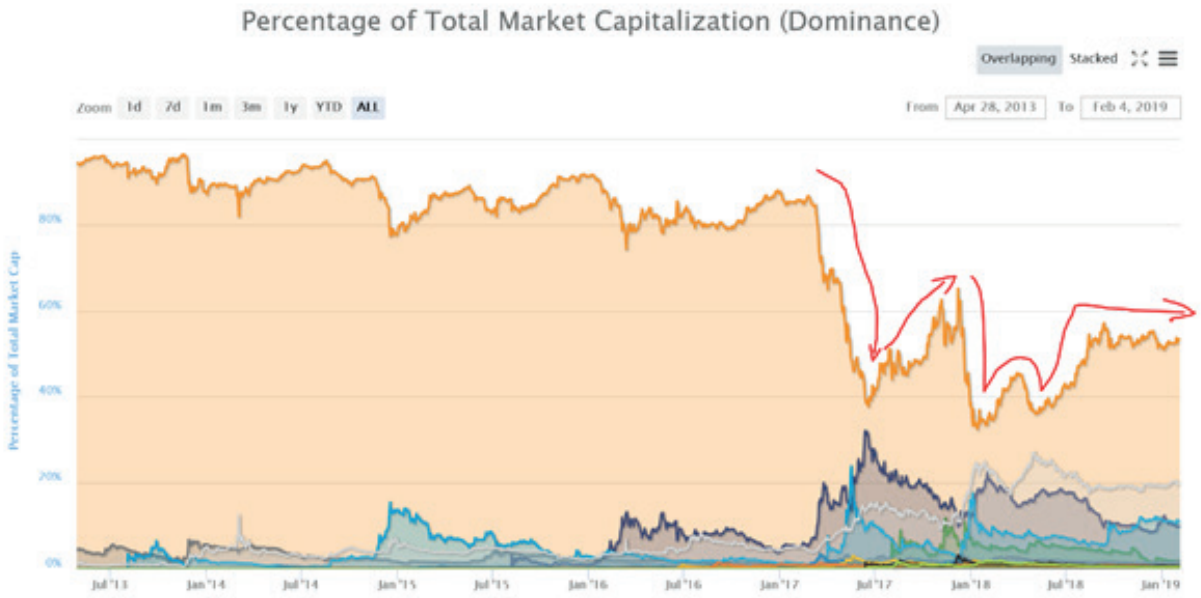
Es gibt sogar eine eigene Webseite „Bitcoin is dead“, die die Anzahl der medialen Beerdigungen zählt, bei denen der Bitcoin nun aber endgültig untergegangen ist.

https://99bitcoins.com/bitcoinobituaries/

Aktuell steht der Zähler bei 342-mal. Gestimmt hat es bisher nicht.

Die Chancen für einen Privatanleger angesichts der Volatilität und des medialen Sperrfeuers mit Kryptowährungen Geld zu verdienen, sind also nicht sonderlich hoch. Zudem darf bei der Aufbewahrung und dem Handel kein Fehler unterlaufen und diese sind selbst für fortgeschrittene User leicht möglich.

Im Jahr 2017 sah es einige Zeit so aus, als würde der Bitcoin von anderen Kryptowährungen in der Führungsrolle abgelöst werden. Ablesbar an der so genannten Bitcoin-Dominanz, also wieviel Prozent der gesamten Marktkapitalisierung ist Bitcoin. Das waren ursprünglich 100%, weil es keine anderen Coins gab. So sieht die Kurve aktuell aus:



Quelle: coinmarketcap.com

Im Sommer und Winter 2017 kam es zu einer gigantischen Hausse bei den alternativen Coins (ALT-Coins). Die Haussen verpufften, viele ALT-Coins nähern sich der Null-Marke und Bitcoin gewinnt wieder an Bedeutung zurück. Das liegt zum einen daran, dass er als einziger Coin ein offizielles Zahlungsmittel in einem Industrieland ist (Japan), zum anderen klassische Finanzprodukte (siehe nächster Abschnitt) auf Bitcoin aufgelegt wurden. Wenn es denn irgendwann stirbt, dürfte der Erste Coin auch der Letzte sein.

Im Moment sieht das Kryptouniversum so aus:

Cryptocurrencies: 2104 • Markets: 15831 • Market Cap: $113.588.203.168 • 24h Vol: $15.813.978.399 • BTC Dominance: 53.3%

Die wichtigsten Inhalte dieser Zeile sind: Es gibt 2104 verschiedene Kryptowährungen, die insgesamt zu 15.831 Währungspaaren an verschiedenen Börsen gehandelt werden. Die Marktkapitalisierung des Gesamtmarktes beträgt 113,5 Mrd. US$ (also als Vergleich nur ca. 1/7 der Kapitalisierung von Apple). Das Handelsvolumen des gezeigten Tages betrug 15,8 Mrd. US$ und die Bitcoinmarktkapitalisierung entspricht 53,3% des Gesamtmarktes (also knapp 60,5 Mrd. US$).

5. Klassische Finanzinstrumente auf Kryptowährungen

Es dauerte relativ lange, bis Produkte der klassischen Finanzindustrie mit Bezug auf Kryptowährungen emittiert wurden. Das war und ist weniger ein Nachfrageproblem, sondern in der Schwierigkeit zu suchen, die Position für den Emittenten berechenbar zu machen. Nehmen wir z.B. ein Zertifikatetracker auf Bitcoin. Im Prinzip ist das nichts anderes als eine 1:1-Abbildung des Bitcoinkurses abzüglich von durchaus erheblichen Zertifikatsgebühren. Der Emittent wird versuchen, das Zertifikat mit Bitcoins zu hinterlegen. Dabei tritt dann das Problem der sicheren Verwahrung auf (siehe Wallets) und der ständig erforderlichen Anpassung des Underlyings (Anzahl Bitcoins) an das Zertifikatevolumen.

Das führte dazu, dass Trackerzertifikate in der letzten Hausse mehrere Wochen „ausverkauft" waren, weil die Rückdeckung am Markt nicht möglich war.

Weiterhin besteht das Problem eines möglichen so genannten Forks. Das ist eine Aufspaltung der Blockchain in 2 verschiede Ketten unter Generierung einer neuen Währung. Bei Bitcoin gab es im Jahr 2017 mehrere so genannte Hardforks. Die erfolgreichste war die Abspaltung von Bitcoin CASH. Ein Bitcoin-Inhaber besaß nach dem Fork sowohl einen Bitcoin als auch einen Bitcoin Cash. Was steht in diesem Fall dem Anleger eines Trackerzertifikates zu?

Während beim Besitz von Bitcoin nach einer Haltefrist von 12 Monaten eine steuerfreie Wertsteigerung im Privatvermögen zu verzeichnen ist, verliert man dieses Privileg beim Einsatz von Finanzprodukten auf Krypto und muss sich der Abgeltungssteuer unterwerfen.

Das nächste Problem tritt auf, weil Krypto rund um die Uhr und 7 Tage die Woche gehandelt wird, andere Finanzprodukte jedoch nicht. Kommt es zum Beispiel in einer Nacht am Wochenende zu drastischen Kursbewegungen und Marktverwerfungen, können diverse Klauseln in den Wertpapierprospekten der Tracker und Derivate auf Krypto zum Tragen kommen. Es gibt dann schlicht keine Geld- oder Brief-Kurse mehr – der Handel wird ausgesetzt. Bei Hebelprodukten nützen dann auch Stoppkurse nichts.

Der Durchbruch an der Börse – der Bitcoin Future

Eine leichte Adelung des Bitcoins geschah mit der Zulassung des Bitcoin Futures an der CBOT. Ein stark reguliertes Finanzprodukt auf eine Kryptowährung. Dies war neben der Anerkennung des Bitcoins als Zahlungsmittel in Japan durch die BOJ eine der weiteren wichtigen Anerkennungen, um die Sterbewahrscheinlichkeit von Bitcoin weiter drastisch zu reduzieren. Es gibt zu viele Marktteilnehmer mit Interesse, dass es ein Erfolg bleibt, darunter eben eine Volkswirtschaft mit 160 Millionen Menschen sowie die Wall Street. Hier der Handelsausschnitt vom 19.09.2018 (Volumen übersichtlich):

Cboe XBT Bitcoin Futures Trading Daten 19.09.2018

Symbol	Verfall	Letzter	Änderung	Hoch	Tief	Schluss	Volumen
GXBT	-	6385.10	+4.93	0.0	0.0	-	-
XBT/V8	10/17/2018	6360.00	-37.50	6405.00	6345.00	6397.50	313
XBT/X8	11/14/2018	6370.00	-42.50	6400.00	6355.00	6412.50	11
XBT/Z8	12/19/2018	6350.00	-50.00	6385.00	6340.00	6400.00	19

Quelle: Daten: Chicago Board of Trade, Grafik 1Sigma GmbH

Der Bitcoin Future hat jedoch Positionseinschränkungen, so dass ein unlimitiertes Spekulieren von Anfang an nicht möglich ist. Den Bitcoin „in Grund und Boden" zu shorten ist technisch nicht möglich. Zum einen existieren bei einem Short-Future genauso viele Long-Kontrakte auf der Gegenseite, zum anderen darf jeder Marktteilnehmer nur folgende Maximalposition halten:

1 Kontrakt = 1 Bitcoin

Maximale Anzahl Kontrakte pro Teilnehmer in allen Laufzeiten: 5.000

Maximale Netto- (!) Long- oder Shortposition in einer Laufzeit: 1.000

Übersetzt heißt das: z.B. kann ein Teilnehmer nur mit 1.000 Bitcoins in einem Verfallstermin Netto- Long oder Short gehen. Das ist angesichts einer Marktkapitalisierung von 60 Mrd. US$ keine wirklich relevante Größe, selbst kumuliert nicht. Aber: Auch der Future handelt am Wochenende nicht, der Bitcoin schon. Das kann im Risikomanagement zu erheblichen Überraschungen führen, da man die Position eben zeitlich nicht immer parallel managen kann.

6. Schlussbetrachtung

Die Vertreter der Finanzindustrie traten gegenüber den Kryptowährungen recht kritisch auf. Nicht immer wurde da bisher mit Sachverstand, was Geldwäschemöglichkeiten, Anonymität etc. angeht, argumentiert. Auch dass hier ohne Regulierung quasi alles möglich ist, ist ein Argument von gestern. Da sich auch Wertpapiere auf der Blockchain emittieren lassen und auch Fondsverwaltung auf der Blockchain möglich ist, ändern sich so langsam die Blickwinkel. Sollte sich dies durchsetzen, fallen tausende von Intermediären weg, weil diese schlicht überflüssig sind.

Auf der anderen Seite stehen Programmierer, Hacker und Menschen, die Innovationen großartig finden (Geeks) und die sehr frühzeitig auf Bitcoin und Ethereum gesetzt haben und ihren Einsatz mehrtausendfach vervielfältigt haben und daher quasi kein Gegenargument gelten lassen. Dass auch der Kryptomarkt den Gesetzen von Angebot und Nachfrage folgt, akzeptieren sie nicht immer und sehen häufig hinter jeder signifikanten Kursbewegung eine Verschwörung aus dem FIAT-Lager. Wikipedia definiert FIAT-Geld als Geld ohne inneren Wert, das als Tauschmittel benutzt wird. Also z.B. EURO, US$ etc. - geschaffen von einer zentra-

len Instanz, wenn nötig in unbegrenzter Menge und daher langfristig wertlos (was währungshistorisch nicht falsch ist). Dem stehen Kryptowährungen ohne zentrale Instanz (das Geld gehört tatsächlich den Menschen und nicht dem Bankwesen) entgegen und das weltweite Netzwerk mit tausenden von unabhängigen Kontrollinstanzen sorgt für Sicherheit. Dies wird mit einer höheren Überlebenswahrscheinlichkeit eingeschätzt, als die bekannten zentralen Währungen, die einer ständigen Verwässerung ausgesetzt sind. Vertrauen benötigt jedes Währungssystem, der innere Wert eines Papierscheines ist nicht wesentlich höher als eines digitalen Token - sollte das Vertrauen, was die Kaufkraft angeht, auf null sinken.

Noch ein paar Anmerkungen zum Thema Energieverbrauch. Es gibt Kryprowährungen wie z.B. Bitcoin die werden durch sog. Mining geschaffen. Dies verbraucht in erheblichem Maße elektrische Energie. Der Kostenaufwand Energie zur Herstellung eines Bitcoins beträgt Anfang 2019 über 2000 US$. Zwei Dinge kann man daraus nicht (!) ableiten. 1. Dass dies so bleibt, weil sich die Rechengeschwindigkeit der Hardware ständig verbessert und 2. Dass es als Allgemeinaussage Gültigkeit hat, weil viele Währungen ja gar nicht gemined werden, sondern einmal per Ausgabe schlicht virtuell erschaffen.

Vergleichen wir einmal den Stromverbrauch für 1 Transaktion im herkömmlichen Zahlungsverkehr (VISA) mit Bitcoin und Ripple:

Glühbirnenbetriebsdauer (60W) als Äquivalent für den Stromverbrauch für 1 Transaktion

- VISA : 1 Stunde 28 Minuten

- Bitcoin: 9 Jahre 187 Tage

- Ripple: 11 Sekunden

- Quelle: LSP-Digitale-Recherche/Statista 2018

Die Erkenntnis daraus ist:

1. Auch herkömmliche Transaktionen verbrauchen Energie in erheblichen Umfang

2. Krypto ist Energieverschwendung oder massive Einsparung, je nachdem was man genau dort betrachtet

Der Kryptomarkt ist sehr entwicklungsfreudig und dynamisch. Was heute als Erkenntnis gilt, wie z.B. Bitcoin skaliert nicht, ist zu langsam und zu teuer im Transfer, kann morgen schon obsolet sein, weil sich schlicht das Netzwerk schnell weiterentwickelt hat. Echte Kryptoanhänger interessieren sich für die Idee des unabhängigen Geldes, die technischen Möglichkeiten und deren Weiterentwicklung, kaum jedoch für Kurse. Die Finanzindustrie schaut quasi nur auf Kursentwicklungen. Daher verstehen sich diese beiden Welten z.Zt. nicht sonderlich gut.

Exkurs:

Einer Unterhaltung folgen:
Die Finanzbranche hat eigentümliche Begriffe und Laien ist es nicht möglich, einer Unterhaltung, die sich um Benchmarks, Alphas und Betas oder NAVs dreht, zu folgen. Dies gilt aber auch für die Kryptobranche. Ohne Kenntnisse der Fachbegriffe ist ein Verständnis einer Unterhaltung selbst für Finanzberater kaum möglich.

Beispiel:

Bei einem meiner ALT-coins gab`s nen Airdrop. Die Gerüchte hatte ich für FUD gehalten. Wegen FOMO hatte ich trotzdem noch nicht verkauft.

Beim nächsten Pump geh ich dann raus.

7. Glossar

Wichtige Begriffe zum Entschlüsseln:

Adresse: Der Ort, wo Bitcoins gelagert werden. Beim Verschicken wird der Coin von einer Adresse zu einer anderen geschickt
Airdrop: Gratis-Verteilung eines Coins
ALT-coin: Wird jede andere digitale Währung neben Bitcoin bezeichnet. Beispiele Hierfür sind Dash, Ethereum, Monero...

Blockchain: Die Liste, in der alle gefundenen Blöcke einer Kryptowährung aufgelistet werden. In den Blöcken werden alle Transaktionen der jeweiligen Kryptowährung gespeichert.
BTC: Abkürzung für Bitcoin

Difficulty: Beschreibt die Schwierigkeit, mit der ein Block gefunden wird. Je größer die Rechenleistung eines Kryptowährungsnetzwerks ist, desto höher ist auch die Difficulty. Wenn die Rechenleistung abnimmt, nimmt auch die Schwierigkeit ab, neue Blöcke zu finden.

ETH: Währungsabkürzung für Ethereum
Escrow: Ein neutraler Mittelsmann, welcher zwischen zwei Parteien den Austausch von Wertsachen ermöglicht. Wichtig bei institutioneller Lagerung.

FOMO: "Fear of missing out"; beschreibt die Angst, dass einem auf Grund einer Entscheidung oder Investition ein Profit entgeht.
Fork: ist die Aufspaltung einer Blockchain in zwei verschiedene, welche dann unabhängig voneinander agieren.
FUD: „Fear, Uncertainty and Doubt" - ist eine Strategie um Leute zu verunsichern, indem man negative und falsche Informationen streut. (Fake News – eine Seuche im Kryptobereich)

Genesis-Block: Ist der allererste geminte Block jeder Kryptowährung.

Hash: Bezeichnet den mathematischen Prozess, mit dem eine große Menge an Daten auf einen gewissen Wert reduziert werden kann.
HODL: "Hold on for dear life"; wird als Aussage benutzt. Man möchte damit ausdrücken, dass man seine Kryptowährung hält, egal wie sich der Kurs entwickelt und davon ausgeht, dass sie eines Tages sehr profitabel sein wird. Nicht HOLD sondern HODL. Extra falsch geschriebenes HOLD.

ICO: Initial Coin Offering - eine Neuemission im Bereich Kryptowährungen

Mining: Wird der vom Computer (Miner) ausgeübte Vorgang bezeichnet, mit dem man neue Bitcoins & ALT-coins erzeugt, indem mathematische Probleme gelöst werden.

Pump & Dump: Künstliche Wertsteigerung (pump) eines Coins ohne Nachhaltigkeit, einzig und alleine dazu genutzt, damit andere bei hohen Kursen einkaufen, um damit die eigenen Coins bei hohen Kursen zu verkaufen (dumpen)

Satoshi: Ist die kleinste Einheit von Bitcoin: 0.00000001 BTC
Scam: engl. für Betrug
Scamcoin: Ist ein ALT-coin, der wie Falschgeld unter die Leute geworfen wird und irgendwann aufhört zu existieren.

Wallet: Ist eine digitale Geldbörse, in der Bitcoins oder andere ALT-coins gespeichert werden