BITCOIN & CO. VERSTEHEN UND HANDELN

LERNEN SIE ALLES, WAS SIE ÜBER KRYPTOWÄHRUNGEN WISSEN MÜSSEN

VON SASCHA HUBER UND OLIVER BARON



eBook powered by GodmodeTrader

Inhalt

1. Bitcoin – Entstehung, Gegenwart und Zukunft Seite 4
2. Bitcoin: Die ersten Schritte – Wallet einrichten und los gehts! Seite 9
3. Blockchain: So funktioniert die Zukunftstechnologie Seite 12
4. Bitcoin & Co.: Welche Kryptowährungen gibt es eigentlich? Seite 15
5. Wo und wie kann man Kryptowährungen handeln? Seite 20
6. Bitcoin-Mining: 59% Rendite im Jahr? Seite 24
7. ICO-Hype: Jetzt geht es auch in Deutschland los? Seite 27
8. Der Krypto-Trader: Sascha Huber stellt sich und seinen neuen Börsenbrief vor Seite 30
9. Impressum Seite 32

Liebe Leserinnen und Leser,

hört man auf die Kritiker des Bitcoin, dann dürfte dieser revolutionären Kryptowährung, die in den vergangenen Jahren die Welt im Sturm erobert hat, keine große Zukunft beschieden sein. Der ehemalige US-Notenbankchef Ben Bernanke etwa sieht im Bitcoin den „Versuch, Fiat-Währungen zu ersetzen und damit Regulierungsmaßnahmen und staatliche Kontrolle zu umgehen." Befürworter des Bitcoin betrachten jedoch gerade die Tatsache, dass die Währung keiner staatlichen Kontrolle unterliegt, sondern von einem emotionslosen Netzwerk gelenkt wird, als entscheidenden Vorteil.

Die Wahrheit dürfte, wie so oft, irgendwo in der Mitte liegen. Wahr ist, dass die neuen Kryptowährungen unbestreitbare Vorteile gegenüber traditionellen Währungen haben. Wegen der seit der Finanzkrise immer hemmungsloseren Ausweitung der Geldmenge erfüllen Euro oder Dollar die Wertaufbewahrungsfunktion einer Währung schon lange nicht mehr. Angesichts Niedrigzinsphase und versteckter Inflation wird derjenige, der sein Vermögen in Form von Bargeld oder auf Bankkonten aufbewahrt, auf lange Sicht ärmer.

Beim Bitcoin ist die Geldmenge von vornherein beschränkt. Noch werden zwar ständig neue Einheiten der virtuellen Währung erzeugt, doch die Geldmenge wird auch langfristig nie die Grenze von 21 Millionen Einheiten überschreiten. Dadurch fällt der wichtigste Grund für die Verteuerung von Vermögens- und Verbraucherpreisen, nämlich die ständige und unkontrollierte Ausweitung der Geldmenge, weg. Die Begrenzung der Geldmenge beim Bitcoin bedeutet aber nicht, dass dadurch langfristig auch die Ausbreitung der Währung gefährdet ist, denn jeder Bitcoin lässt sich bis auf acht Nachkommastellen teilen.

Gefährlich könnten dem Bitcoin und anderen Kryptowährungen natürlich staatliche Regulierungsmaßnahmen werden. Durch den Bitcoin lassen sich etwa Geldwäschevorschriften relativ einfach umgehen. Denn die Kryptowährungen existieren völlig unabhängig vom traditionellen Finanzsystem, gewissermaßen in einem wirtschaftlichen Paralleluniversum. Nur dort, wo beide Systeme miteinander verknüpft sind, also zum Beispiel an Bitcoin-Handelsplätzen, an denen die Währung mit Fiat-Geld erworben oder verkauft werden kann, macht sich schon heute staatliche Kontrolle bemerkbar. Aber auch die von staatlichen Stellen erzwungenen Schließungen von Bitcoin-Börsen etwa in China und Südkorea konnten der Kryptowährung bisher nicht ernsthaft etwas anhaben. Das Damoklesschwert eines weltweiten Verbots schwebt aber trotdem langfristig über Bitcoin & Co.

Doch selbst wenn die heute existierenden Kryptowährungen auf lange Sicht nicht überleben sollten, wird die mit dem Bitcoin eingeführte Blockchain-Technologie wohl unsere Welt nachhaltig verändern. Eine Blockchain ist nichts anderes als eine Datenbank an Transaktionen, die nicht an einer zentralen Stelle, sondern von einem offenen Netzwerk verwaltet und dezentral im gesamten Netzwerk gespeichert wird. Die Einsatzmöglichkeiten von Blockchains sind beinahe unbegrenzt und erstrecken sich keineswegs nur auf das Finanzwesen, sondern können auch gewinnbringend zum Beispiel bei der automatischen Verwaltung von ganz realen Gütern eingesetzt werden. Die technologische Basis hierfür bietet dabei schon heute das Ethereum-Netzwerk mit den sogenannten Smart Contracts (intelligenten Verträgen). Bei Smart Contracts handelt es sich um Computerprotokolle, die Verträge abbilden, kontrollieren und sogar automatisch umsetzen können.

Dass die Blockchain unsere Welt wohl ähnlich nachhaltig verändern dürfte wie die Erfindung des Internets bedeutet aber nicht, dass es nicht in den vergangenen Jahren zu dramatischen spekulativen Übertreibungen kam. So mancher Computer-Nerd, der früh vom Bitcoin hörte und auf den fahrenden Zug aufsprang, wurde praktisch über Nacht zum Multimillionär. Aktuell herrscht in der Szene eine Goldgräberstimmung, die geradezu nach einer nachhaltigen Korrektur oder einem Crash verlangt. Das Konzept der Blockchain und die Idee einer Währung, die keiner staatlichen Kontrolle unterliegt, sondern von einem unabhängigen und auf Konsens basierten Rechnernetz gelenkt wird, dürfte sich aber nicht mehr aus der Welt schaffen lassen.

Die Welt der Kryptowährungen ist aber nicht nur revolutionär, sondern auch sehr unübersichtlich. Mit diesem E-Book wollen mein Kollge Sascha Huber und ich etwas Licht ins Dunkel von Bitcoin & Co. bringen. Wir hoffen, dass Ihnen die Lektüre der folgenden Seiten dabei helfen wird, den Hype um Bitcoin & Co. etwas besser zu verstehen.

Ihr Oliver Baron

Bitcoin – Entstehung, Gegenwart und Zukunft

Die virtuelle Währung Bitcoin könnte unser Geldsystem auf den Kopf stellen. Doch um zu verstehen, wie es seinerzeit überhaupt zur Entstehung des Bitcoin kam, muss man zunächst einen Blick auf unser aktuelles Geldsystem und seine Defizite werfen. Erst dann kann man verstehen, was am Bitcoin so revolutionär ist.

Was ist Geld?

Unter Geld versteht man im Prinzip zunächst einmal jedes anerkannte Tausch- und Zahlungsmittel. Das in der Währungsverfassung eines Landes als gesetzliches Zahlungsmittel bestimmte Geld bezeichnet man dann als Währung. Bei uns in der Bundesrepublik Deutschland war dies früher die Deutsche Mark und ist es heute bekanntlich der Euro.

Bei Geld unterscheidet man grundsätzlich zwischen **zwei Formen**:

- **Bargeld** (Banknoten und Münzen) sowie
- **Buch- oder Giralgeld** (Zahlungsansprüche einer Nichtbank gegenüber einer Bank).

Darüber hinaus ist noch wichtig zu wissen, dass Geld gleich **drei Funktionen** gleichzeitig zu erfüllen hat:

1. ist Geld eine **Recheneinheit** und dient somit als **Wertmaßstab** (Stichwort: Kaufkraft)
2. dient Geld als **Wertaufbewahrungsmittel** (Stichwort: sparen)
3. hat Geld eine **Zahlungsmittelfunktion** (Stichwort: kaufen)

Die Entstehung von Geld: Geldschöpfung

Geld wird in unserem heutzutage üblichen zweistufigen Bankensystem durch die Zentralbank oder die Geschäftsbanken geschöpft. In einem ersten Schritt emittiert die Zentralbank dabei sogenanntes **Basisgeld**, indem sie **Kredite an Geschäftsbanken vergibt oder Aktiva wie bspw. Wertpapiere erwirbt** (Stichwort: Offenmarktpolitik). Im Gegenzug schreibt die Zentralbank dann den Geschäftsbanken entsprechende Guthaben auf ihren Konten, die bei ihr geführt werden, gut.

In unserem Mindestreserve-System erzeugen die Geschäftsbanken dann weiteres Buchgeld auf Basis dieser Basisgeldguthaben. Eine beliebige Ausweitung der Geldmenge durch die Geschäftsbanken wird dabei dadurch verhindert, dass diese für jeden Euro ihrer Kundeneinlagen einen gewissen Prozentsatz bei der Zentralbank in Form von Zentralbankguthaben vorhalten müssen. Dieser sogenannte **Mindestreservesatz** liegt bei der EZB zurzeit bei nur 1%, so dass im gesamten Bankensystem aktuell maximal die 100fache Menge des Basisgeldes als Giralgeld erzeugt werden kann. Zum Vergleich: Bei der Schweizerischen Nationalbank (SNB) liegt der Mindestreservesatz zurzeit bei 2,5%, bei der US-Notenbank Federal Reserve (Fed) bei 10% und bei der chinesischen Notenbank People‘s Bank of China (PBoC) sogar bei 20%.

Fiat Money

Unsere Währung, der Euro, verfügt also über keinen inneren Wert. Der Euro ist ungedeckt und wird alleine durch die Macht der Regierung abgesichert. Dennoch wird der Euro letztlich erst durch die allgemeine Akzeptanz der verschiedenen Handelspartner zu Geld mit den entsprechenden, eben ja bereits angesprochenen, Geldfunktionen (Recheneinheit/Wertmaßstab, Wertaufbewahrungsmittel, Zahlungsmittelfunktion). Solch ungedecktes Geld nennt man in der Fachsprache auch Fiat Money. (Fiat = Es werde)

Festzuhalten bleibt also: Ohne Absicherung durch die Regierung sowie ohne Akzeptanz der verschiedenen Handelspartner wären insbesondere unsere Euro-Banknoten im Prinzip nichts anderes als bedrucktes Papier. Daraus folgt im Umkehrschluss, dass der Euro und jede andere Fiat Money-Währung (wie bspw. auch der US-Dollar) ohne Vertrauen nicht existieren kann.

Die Finanzkrise erschüttert das Vertrauen

Durch die beinahe zu einer neuen Weltwirtschaftskrise mutierte Finanzkrise 2007/2008 wurde das Vertrauen der Bevölkerung in das Bankensystem sowie die Fiat Money-Währungen nachhaltig erschüttert. Dies galt zwar nicht nur, aber insbesondere auch für den Euro. Vielleicht erinnern Sie sich noch daran, wie einst Bundeskanzlerin Merkel und ihr damaliger Finanzminister Peer Steinbrück vor die Kameras treten mussten, um den Deutschen ihre Spareinlagen staatlich zu garantieren.

Ohne diese Staatsgarantie bestand seinerzeit nämlich die reale Gefahr, dass große Teile der Bevölkerung ihre Guthaben von ihren Bankkonten abgehoben hätten, es also zu einem sogenannten „Bankrun“ gekommen wäre. Dies hätte jedoch einen Zusammenbruch des Bankensystems zur Folge gehabt, denn wie wir ja eingangs gelernt haben, müssen die Banken nur eine Mindestreserve in Höhe von 1% ihrer Kundeneinlagen als Sicherheit vorhalten.

Entstehung des Bitcoin als Antwort auf die Finanzkrise 2007/2008

Aufgrund der Finanzkrise 2007/2008 machten sich einige Leute Gedanken über die Einführung einer alternativen Währung. Dabei ist es nicht besonders verwunderlich, dass es im Zeitalter des Internets letztlich eine virtuelle Währung wurde. Wichtig war dem oder den Erfinder/n, der/die sich hinter dem Pseudonym „Satoshi Nakamoto“ versteckt/verstecken, dass diese virtuelle Währung alle Vorteile einer herkömmlichen Währung bieten sollte, nicht jedoch deren Nachteile. Nakamoto baute mit seiner neuen Währung dabei auf Konzepten für unabhängige Internetwährungen auf, die zum Teil bereits vor der Jahrtausendwende diskutiert worden waren.

Um die Defizite von Fiat-Währungen zu vermeiden, wurde der Bitcoin als ein dezentrales Netzwerk ohne Zentralbank entworfen. Für die Geldmenge wurde eine durchaus clever festgelegte Obergrenze an Bitcoins fixiert. Diese Obergrenze wird beim Bitcoin dadurch erreicht, dass sich die Anzahl der neu geschöpften (bei Bitcoin nennt sich dies geminten) Bitcoins nach Erreichung bestimmter Ziele halbiert („Halving“).

Dies funktioniert vereinfacht erklärt so: In einem ersten Schritt konnten auf Basis bestimmter Algorithmen noch relativ einfach ca. 10,5 Mio. Bitcoins gemint werden. Im Laufe der Zeit wird dann die Schwierigkeit zum Minen von Bitcoins beständig erhöht (indem die Algorithmen hierzu immer aufwendiger werden)

und sich die Menge der neu zu erzeugenden Bitcoins nach Erreichung bestimmter Ziele jeweils halbiert. Durch diesen Prozess gibt es letztlich maximal ca. 21 Mio. Bitcoins oder wie Mathematiker es formulieren würden: Die maximale Menge erzeugbarer Bitcoins konvergiert gegen (den Grenzwert) 21 Millionen.

Kritisiert wird in diesem Zusammenhang gerne, dass der/die Initiator/en des Bitcoin wahrscheinlich große Mengen selbst noch einfach erzeugter Bitcoins halten und der Kurs zusammenbrechen könnte, wenn er/sie diese unkontrolliert auf den Markt werfen würden. Dies halte ich jedoch für absurd, da sich der Verkäufer durch solch einen „Fire Sale" ja den eigenen Verkaufskurs zerstören würde.

Ähnliche Gedankenspiele gab es vor einigen Jahren übrigens auch mal im Bezug auf die Chinesen und den US-Dollar. Da China seinerzeit zum größten Halter von US-Staatsanleihen und somit de facto größten Gläubiger der USA aufgestiegen war, wurde der damalige Fed-Chef Alan Greenspan von einem Journalisten gefragt, ob China damit nicht die Macht habe den US-Dollar zu zerstören. Was könne er, Greenspan, denn tun, wenn die Chinesen ihre riesigen Pakete an US-Staatsanleihen über Nacht auf den Markt werfen würden?

Greenspan antwortete seinerzeit kühl: „Sie (also die Chinesen) können es ja mal versuchen". Der erstaunte Journalist hakte nach und Greenspan erklärte, dass dieser Gedanke völlig absurd sei, weil ein solches Vorgehen die größte absichtliche Vernichtung von Volksvermögen in der Geschichte der Menschheit darstellen würde. Was er damit meinte? Nun, klar hätten die Chinesen den US-Dollar so zu Fall bringen können. Aber damit wären ihre eigenen auf US-Dollar lautenden Währungsreserven ja quasi über Nacht nichts mehr wert gewesen. Sie würden sich somit letztlich ins eigene Fleisch schneiden. Gleiches gilt für die größten Halter von Bitcoin natürlich auch.

Die Verwaltung der Währung – Blockchain

Nun wissen wir also grob, wie die Geldschöpfung beim Bitcoin funktioniert. Doch was nützt es schon, wenn ein Bitcoin erzeugt, also gemint wurde? Interessant wird es ja erst, wenn man mit dieser Währung auch Transaktionen durchführen kann. Wie aber funktioniert da die Verwaltung, die ja in unserem Finanzsystem Aufgabe der Banken ist?

Nun, tatsächlich können Nutzer jederzeit Transaktionen mit Bitcoins durchführen und jede einzelne Transaktion wird aufgezeichnet. Wäre dem nicht so, wäre das ganze System dem Untergang geweiht. Denn ohne eine solche Aufzeichnung einer Transaktion, könnte man ja nicht feststellen wer wem wie viele Bitcoins übertragen hat und wer daher zurzeit wie viele Bitcoins besitzt. Sie können sich das in der realen Welt etwa so vorstellen, als ob sie auf jede Banknote immer den aktuellen Besitzer (jedoch anhand seiner Kontonummer, nicht mit seinem richtigen Namen, denn grundsätzlich sind Bitcoins pseudonym) drauf schreiben würden.

Dabei wird nur festgehalten wie viele Bitcoins auf welches „Konto" transferiert werden. Transaktionen, die in einem gewissen Zeitfenster stattfinden, werden dann zu einem Block zusammengefasst. Ein Block besteht somit aus den Transaktionen, die über einen bestimmten Zeitraum hinweg durchgeführt wurden. Dokumentiert werden diese Blocks in einem öffentlich zugänglichen Register, das aus einer langen Kette von Blocks besteht und sich folgerichtig Blockchain (zu Deutsch: Block-Kette) nennt. Sie können diese Blockchain

ganz einfach unter: http://www.blockchain.info einsehen. Und wenn Sie die richtige „Kontonummer“ kennen, können Sie dort mit Hilfe der Suchfunktion sogar den aktuellen Kontostand jedes beliebigen Kontos einsehen, nicht nur den ihres eigenen Kontos.

Dank dieser Datenbank namens Blockchain gibt es somit stets den Beweis, wer welchen Bitcoin besitzt. Grundsätzlich wäre es zwar möglich, dass ein Hacker die Blockchain nachträglich manipuliert. Allerdings ist eine solche Manipulation sowohl aus technischer Sicht wie auch vom „Preis-Leistungs-Verhältnis“ her schwierig. Denn jeder Block wird, sobald er abgeschlossen ist (d.h. die maximale Anzahl an Transaktionen in einem bestimmten Zeitraum ist erreicht), in eine willkürliche Reihe von Buchstaben und Zahlen umgewandelt.

Diese Reihe wird Hash genannt und dieser Hash wird zusammen mit dem Block in der Blockchain abgespeichert. Da niemand die konkrete Formel zur Umwandlung der Transaktionsdaten in einen Hash kennt, ist es für Hacker nahezu unmöglich, die Blockchain zu manipulieren. Zumal in die Berechnung des aktuellen Hashs zusätzlich auch noch der Hash des vorherigen Blocks mit einfließt. Der Hash ist somit quasi ein fälschungssicheres Siegel.

Das eigentliche Bitcoin Mining ist somit letzten Endes nichts anderes wie die Versiegelung eines Blocks durch die Erzeugung eines Hashs. Und derjenige, der ein solches Siegel als Erstes erzeugt, bekommt Bitcoins als Belohnung. Dieser Anreiz ist angesichts der hohen Stromkosten für das Mining allerdings auch absolut gerechtfertigt.

Der Wert eines Bitcoins

Wie wir eingangs gelernt haben, verfügt unsere aktuelle Währung, der Euro, über keinerlei inneren Wert (Fiat Money). Es handelt sich letztlich um bedrucktes Papier, dass erst durch die Akzeptanz und das Vertrauen der verschiedenen Handelspartner zu Geld wird, wobei der Staat das Vertrauen fördert und den Euro somit absichert.

Ähnlich ist es auch beim Bitcoin. Zwar fördert und sichert hier kein Staat das Vertrauen, aber die seit Jahren erprobte und bis heute nicht gehackte Blockchain. Seinen jeweils aktuellen Wert erhält auch der Bitcoin nur durch die Akzeptanz und das Vertrauen seiner Anwender/Verwender. Insofern gibt es einen stets aktuellen Marktpreis für den Bitcoin, wenn man so will ist er die frei konvertierbarste Währung der Welt (anders als bspw. der chinesische Renminbi-Yuan).

Anfangs war die Akzeptanz und das Vertrauen in den Bitcoin noch sehr gering, so dass 2009 jemand noch 10.000 Bitcoins für eine Pizza bezahlen musste. Heute sind die Akzeptanz und das Vertrauen hingegen gestiegen, so dass 10.000 Bitcoins aktuell rund 70 Millionen US-Dollar wert sind. Solange die Akzeptanz und das Vertrauen in den Bitcoin weiter steigt, wird auch der Wert des Bitcoins weiter steigen. Denn mehr Anwender/Verwender bei einer auf 21 Millionen begrenzten Geldmenge bedeutet eine steigende Nachfrage nach einem begrenzten Gut. Insofern ist es nicht ganz falsch, wenn manche Bitcoin als virtuelles Gold (statt Geld) bezeichnen. Darum werden Bitcoins übrigens auch gemint (→ Goldmine) und nicht wie bspw. der Euro „geschöpft“.

Der Kampf gegen den Bitcoin

Weil die Akzeptanz und das Vertrauen und somit der Wert des Bitcoin anfangs noch sehr gering war, ließen Notenbänker und Politiker die Entstehung des Bitcoin zu. Sie nahmen diese neue virtuelle Währung einfach nicht ernst. Zudem wäre ein Verbot aufgrund der dezentralen Struktur des Bitcoin-Netzwerks auch schwierig gewesen. Dies hat sich inzwischen jedoch geändert, denn immerhin beträgt die Marktkapitalisierung des Bitcoin aktuell schon über 100 Mrd. US-Dollar.

Kein Wunder also, dass JPMorgan Chef Jamie Dimon den Bitcoin kürzlich als „Betrugssystem“ verunglimpft hat und die Chinesen inzwischen verstärkt versuchen, ihn unter Kontrolle zu bringen. Auch wurde der Bitcoin in der Vergangenheit von vielen Politikern gerne attackiert, weil er aufgrund seiner angeblichen Anonymität Kriminalität und Terrorismus begünstige. So möchte man die virtuelle Währung, wenn man sie schon nicht mehr aufhalten oder gar besiegen kann, zumindest regulieren und somit kontrollieren.

Banken möchten die Blockchain adaptieren

Auch die Banken sehen ihr Geschäftsmodell als Intermediäre durch den Bitcoin natürlich bedroht. Daher versuchen sie die Blockchain zu adaptieren, nachdem sich dieses Konzept über die letzten Jahre hinweg bewährt hat. So möchten die Banken zukünftig Transaktionen mit den bekannten staatlichen Währungen ebenfalls über eine Blockchain verwalten und somit ihre Kosten deutlich reduzieren. Ich kann verstehen, warum die Banken dies möchten (Vorteile der Blockchain nutzen), sehe jedoch keinen Sinn darin. Denn wenn man einfach nur die „normalen“ Währungen über eine Art Blockchain verwaltet, würden die Nutzer ja nahezu alle ihre Vorteile der virtuellen Währung aufgeben. Warum aber sollten sie das tun?

Zusammenfassung: Vor- und Nachteile des Bitcoin

Vorteile	Nachteile
frei zugänglich	hohe Volatilität
kaum staatliche Kontrolle	teilweise starke Konzentration des Besitzes
dezentral organisiertes Netzwerk	teilweise umständliche Verwendung (offline)
Pseudonymität	Netzwerk-Übernahme (→ Quantencomputer)
ständige und stetige Verfügbarkeit	mögliche Verbote (siehe zuletzt China)
hohe Sicherheit (→ Blockchain)	Überlastung des Netzwerks (→ Blocksize Debatte, Entstehung von Bitcoin Cash)
freie Konvertierbarkeit	Aufbewahrung (→ Sicherheitsrisiken)
teilweise niedrige Transaktionskosten (bei Bitcoin nur bedingt)	extrem hoher Energieverbrauch durch die Miner
relativ schnelle Transaktionen (gegenüber Banküberweisungen)	Überregulierung/Markteingriffe (→ staatliche Regulierung)
begrenzte Geldmenge (→ Inflationsschutz)	„Deflationsgefahr“

Bitcoin: Die ersten Schritte – Wallet einrichten und los geht`s!

Wenn man Bitcoins über eine Kryptowährungsbörse oder einen anderen Online-Handelsplatz kauft, hat man in der Regel auch die Möglichkeit, die erworbenen Coins dort zu „lagern". Allerdings sind in der Vergangenheit schon einige Kryptowährungsbörsen, bspw. Cryptsy oder MtGox, in die Insolvenz gerutscht. Damit sind dann in der Regel auch die dort gelagerten Coins weg. Doch wer die Coins in einer eigenen Wallet aufbewahrt, kann dieses Risiko minimieren.

Beim Handel mit Aktien gibt es eine klare Trennung. Es gibt die Börsen wie die Deutsche Börse AG oder Tradegate, die für den Handel zuständig sind. Dies sind grundsätzlich private Einrichtungen, die zum Teil jedoch durch den Staat reguliert werden (Stichwort: Handelsüberwachung). An diesen Börsen können Sie jedoch in der Regel nicht direkt handeln, sondern nur über eine dort zum Handel zugelassene Bank respektive einem Broker. Dieser lagert anschließend auch die erstandenen Wertpapiere für Sie (im Depot), die ebenfalls besonders gesetzlich geschützt sind (Stichwort: Sondervermögen). Weil diese als Sondervermögen gelten, kommen Sie im Falle einer Insolvenz nicht in die Insolvenzmasse.

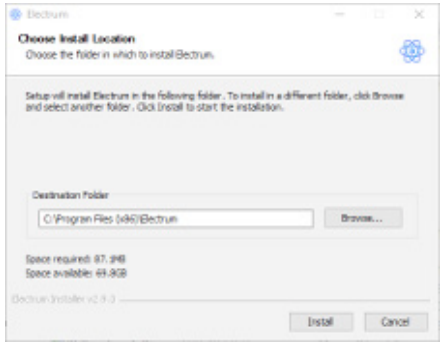
Da Kryptowährungen noch weitestgehend unreguliert sind, gilt dies hier nicht. Daher können sie dort auch direkt (ohne Bank oder Broker) handeln und die Börsen können die Coins auch für sie lagern. Rutscht aber eine Börse in die Insolvenz, fallen die dort gelagerten Coins eben auch in die Insolvenzmasse, sie sind kein Sondervermögen. Darum ist es hier besonders wichtig auf die Integrität und Seriosität der Kryptowährungsbörsen zu achten. Jede Medaille hat also immer ihre zwei Seiten. Aufgrund der fehlenden Banken/Broker spart man sich Gebühren, dafür ist die Unsicherheit höher.

Jetzt aber die gute Nachricht! Sie sind nicht dazu verpflichtet, die Coins dort zu lagern. Wenn Sie natürlich traden möchten, geht es kaum anders. Denn dann brauchen sie ja einen schnellen Zugriff darauf. Wenn sie sich dann also schützen möchten, sollten sie stets ihre Coins veräußern bevor sie den Rechner verlassen und bspw. schlafen gehen. Wenn Sie sie aber sicher behalten möchten und keinen schnelle Zugriff benötigen, können sie die Coins auf eine eigene Wallet ziehen. Natürlich sollten Sie den entsprechenden Rechner gut vor Viren schützen und regelmäßig Backups machen, aber dies gilt ja generell.

Cyber-Wallet/Web-Wallet oder lokale Wallet

Beginnen wir mit der lokalen Wallet. Dazu brauchen Sie natürlich eine entsprechende Software. Eines der meistgenutzten Programme ist dabei Electrum, welches Sie hier herunterladen können: https://electrum.org/#download

Anschließend installieren Sie die Software einfach auf Ihrem Rechner, ich habe die Windows Version heruntergeladen und installiert.

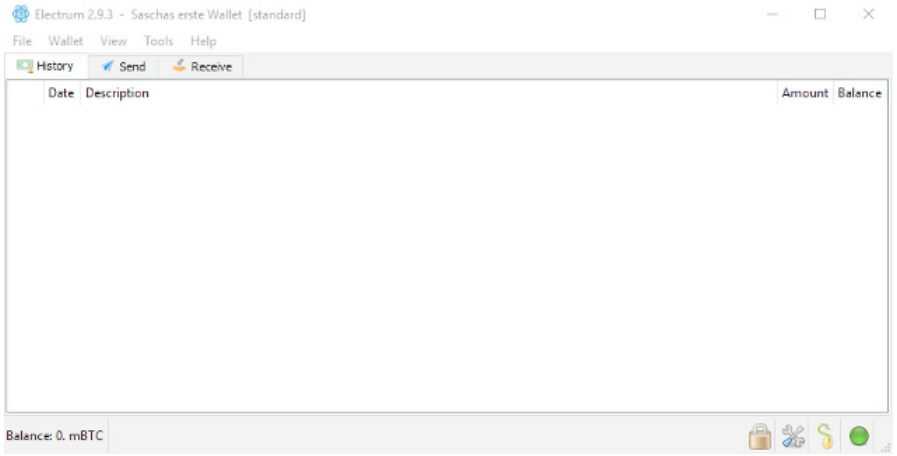


Anschließend können Sie das Programm öffnen, auf „Auto Connect" klicken und ihrer Wallet einen Namen zuweisen, z.B. „Saschas erste Wallet". Als Nächstes müssen Sie noch auswählen was für eine Wallet sie gerne erstellen möchten, aus Sicherheitsgründen wäre mindestens eine Wallet mit Zwei-Faktor-Authentifizierung

empfehlenswert. Ich habe aber zunächst einmal die „Standard Wallet“ genommen. Wenn Sie ein gutes Passwort vergeben und diese verschlüsseln, ist auch die Standardvariante sehr sicher.

Danach müssen Sie dann einen Sicherheitscode (12 Wörter) via „Create a new seed“ erstellen lassen. Wenn Sie später mehr Erfahrung haben, können Sie auch „Public oder Private Keys“ auswählen. Diesen Sicherheitscode dürfen Sie niemals vergessen, da Sie sonst den Zugriff auf ihre Wallet und somit ihre Coins komplett verlieren könnten!

Diesen Sicherheitscode geben Sie im nächsten Feld komplett ein, das geht am einfachsten per Kopieren/Einfügen (Copy/Paste). Anschließend vergeben Sie noch zusätzlich ein eigenes Passwort, dass Sie ebenfalls nicht verlieren sollten. Nehmen Sie dort bitte keine Passwörter wie „qwertz“ oder „123456“, die leicht zu knacken sind. Es sollte ein Häkchen bei „Encrypt Wallet File“ sein, damit Ihre Wallet-Datei verschlüsselt wird. Danach sind Sie fertig und Ihre Wallet sollte so aussehen:



Im Prinzip haben Sie damit eine Art Homebanking-Software. Die wichtigsten beiden Funktionen sind nun natürlich „Send“ („Senden“) und „Receive“ („Empfangen“) von Coins, in diesem Fall natürlich Bitcoins. Voreingestellt ist die Sprachversion „English“, diese können Sie unter „Tools“, „Preferences“, „Appearance“ und dann „Language“ auf „German“ (Deutsch) umstellen. Danach ist aber ein Neustart inkl. Eingabe ihres Passworts (hoffentlich nicht qwertz oder 123456) notwendig.

Wenn jemand Ihnen nun Bitcoins überweisen möchte, finden Sie ihre „Bitcoin-Kontonummer“ (ein langer Code aus diversen Zeichen, beachten Sie das Groß- und Kleinschreibung hier wichtig sind!) unter „Empfangen“. Weisen Sie der angeforderten Transaktion eine Beschreibung (müssen Sie aber nicht unbedingt!) sowie einen Betrag in mBTC (Milli-Bitcoins, also 0,001 Bitcoins) zu (für einen ganzen Bitcoin also 1000 mBTC eintragen) zu. Drücken Sie anschließend auf „speichern“ und geben Sie demjenigen, der Ihnen Bitcoins senden möchte, diese Daten (insbesondere natürlich ihre Bitcoin-Kontonummer). Am einfachsten wird das natürlich, wenn Sie die Möglichkeit haben, ihm den von der Software generierten QR-Code zukommen zu lassen.

Sie können prinzipiell beliebig viele Bitcoin-Konten (für jede einzelne Transaktion ein eigenes!) anlegen, was Sie auch tun sollten. Denn über http://www.blockchain.info kann man anhand Ihrer Bitcoin-Kontonummer abfragen, wer Ihnen Bitcoins zugeschickt hat (nicht den Namen, sondern „nur“ seine Bitcoin-Kontonummer, aber trotzdem) und wie ihr aktueller Kontostand aussieht. In der Software wird ihr Kontostand unten links unter „Balance“ (respektive „Guthaben“) angezeigt. Dabei wird natürlich der Kontostand all Ihrer Bitcoin-Konten addiert. Negative Salden sind ja beim Bitcoin nicht möglich.

Wenn Sie irgendwelche Probleme haben, hilft (unter Windows) die Taste F1 (Sie brauchen dafür allerdings eine Verbindung zum Internet). Für den Anfang reicht das, später können Sie natürlich noch viel mehr Funktionen der Software nutzen. Natürlich gibt es auch andere Software-Lösungen als Electrum, aufgrund Ihrer Einfachheit gehört diese jedoch zu den beliebtesten.

Cyber- bzw. Web-Wallet

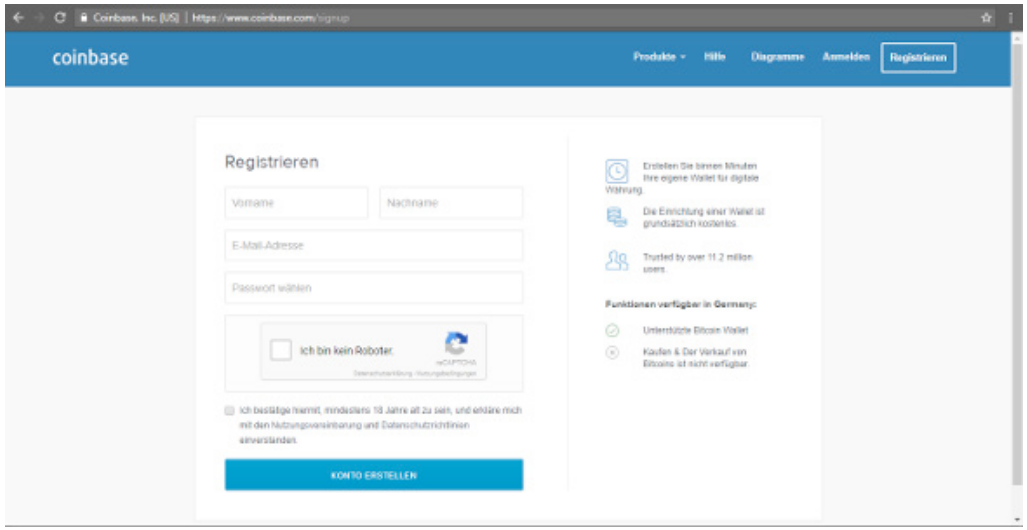
Alternativ können Sie auch eine Cyber- oder Web-Wallet anlegen. Dies geht bspw. bei Coinbase, einem Unternehmen, dem man Stand heute durchaus Vertrauen schenken kann. Denn schließlich hat man ja mehrere Finanzierungsrunden mit Risikokapitalgebern aus dem Silicon Valley hinter sich und gilt zurzeit als eines der am besten durchfinanzierten „Startups“ in diesem Bereich.

Der Nachteil einer solchen Cyber- oder auch Web-Wallet ist, dass Sie a) dem Anbieter Vertrauen schenken und sich b) natürlich dennoch vor Attacken (Stichwort: „Phishing“) schützen müssen. Denn hackt jemand ihren Account, kann er mit den dort gelagerten Coins machen, was er möchte. Zwar können Sie alle Transaktionen via http://www.blockchain.info verfolgen, aber leider ist der Bitcoin pseudonym (nicht, wie fälschlicherweise immer in den Medien berichtet wird anonym). Sie hätten also theoretisch die Chance den Angreifer irgendwann (wenn er mal einen Fehler macht und seine Identität irgendwo offen legt) zu ermitteln, aber das dürfte Ihnen wenig helfen, wenn Ihre Coins z.B. in Nigeria gelandet sind.

Der Vorteil einer solchen Cyber- oder Web-Wallet ist dagegen, dass Sie prinzipiell von jedem Ort der Welt darauf zugreifen (wenn Sie eine Verbindung zum Internet haben) und auch frei über Ihre Coins verfügen können. Das Grundprinzip ist also vergleichbar mit der eMail, auch dort gibt es ja sogenannte Webmail-Anbieter wie GMX, Hotmail oder Web.de.

Um sich eine solche Cyber- oder Web-Wallet bei Coinbase anzulegen, gehen Sie einfach auf http://www.coinbase.com. Die Internetseite erkennt automatisch, dass Sie in Deutschland sind und zeigt alles in deutscher Sprache an. Zuerst müssen Sie auf „Registrieren“ klicken und Ihre Daten eingeben.

Anschließend müssen Sie auswählen, ob Sie ein das Konto für eine Einzelperson oder aber ein Geschäftskonto eröffnen möchten, in der Regel müssen Sie also wohl Einzelperson anklicken und auf „Weiter“ klicken. Dann müssen Sie, schon aus Sicherheitsgründen, Ihre Handynummer eingeben. Wenn Sie dann noch Ihre Identität bestätigen und eine Zahlungsmethode hinzugefügt haben, sind Sie fertig.



Beachten Sie, dass Sie mit der Registrierung auch Bitcoins über den Handelsplatz von Coinbase kaufen und verkaufen können. Dabei ist aktuell, neben dem Handel mit Bitcoins, auch der Handel mit Ethereum und Litecoins möglich. Ansonsten funktioniert die Cyber- bzw. Web-Wallet ähnlich wie Electrum, nur eben im World Wide Web. Sie können sich sogar ein paar Dollar hinzu verdienen, wenn Sie Coinbase Freunden empfehlen (10 US-Dollar je Registrierung).

Beachten Sie, dass Sie sich auch hier ein wenig einarbeiten müssen, prinzipiell ist alles jedoch sehr leicht verständlich. Leider kann ich Ihnen an dieser Stelle nur die ersten Schritte erläutern, ein wenig Arbeit von Ihrer Seite zur Einarbeitung ist erforderlich. Das wird aber nicht zu Ihrem Nachteil sein!

Paper Wallet

Wer ganz auf Nummer sicher gehen und jedes Verlustrisiko ausschalten will, kann seine Bitcoins sogar in Papierform aufbewahren. Dies wird auch als Paper Wallet bezeichnet. Jede Wallet besteht im Wesentlichen aus zwei Elementen, dem public key und dem private key. Der public key ist öffentlich und wird dazu benutzt, Transaktionen von anderen zu empfangen. Der private key ist nur dem Inhaber der Wallet bekannt. Wer über den private key verfügt, weist sich damit gegenüber dem Netzwerk als Besitzer einer Wallet aus.

Eine Paper Wallet besteht nun aus nichts anderem als aus public key und private key einer Wallet. Die Keys können dabei entweder als lange Buchstaben- und Zahlenkolonnen und/oder in Form eines QR-Codes ausgedruckt und zum Beispiel in einem Bankschließfach aufbewahrt werden. Wichtig ist allerdings, dass tatsächlich niemand Einblick in den private key einer Wallet erhält. Denn wer den private key einer Wallet kennt, kann über die Coins verfügen.

Wie Sie konkret eine Paper Wallet erstellen können, wird in diesem Tutorial von CoinDesk erklärt. Wegen des nicht unerheblichen Aufwands lohnt sich dies vor allem für größere Beträge, die man nicht kurfristig in Transaktionen verwenden, sondern für längere Zeit aufbewahren will.

Kurse von Kryptowährungen, Indizes, Aktien und Rohstoffen/Währungen auch unterwegs jederzeit abrufen.

Machen Sie die Guidants App zu IHRER App. Jetzt kostenlos downloaden!

Blockchain: So funktioniert die Zukunftstechnologie

Was verbirgt sich hinter der geheimnisvollen Zukunftstechnologie Blockchain, die als wichtigste technologische Grundlage der Kryptowährungen dient und derzeit die Finanzbranche durcheinander wirbelt? Auch wenn der mathematische und informationstechnische Hintergrund recht kompliziert ist, so lässt sich das Blockchain-Konzept in seinen Grundzügen doch ganz ohne höhere Mathematik oder ausgefeilte IT-Konzepte beschreiben.

Bei jeder Art von Buchgeld oder elektronischem Geld besteht das Problem, dass irgendwo gespeichert werden muss, über welche Guthaben die einzelnen Kontoinhaber verfügen. Nehmen wir eine x-beliebige Bank, bei der es drei Kunden mit den Namen A,B und C gibt. Die Bank führt elektronisch in einer Datenbank Buch, über welches Guthaben die einzelnen Kunden auf ihren Girokonten verfügen. Auch wenn Banken in der Regel gut gegen Cyberangriffe und andere Gefahren gerüstet sind, ist dieses Vorgehen inhärent unsicher:

WELCHEN BROKER HÄTTEN SIE DENN GERN?

JFD BROKERS

Consors bank ! by BNP PARIBAS

FXCM *

flatex ONLINE BROKER *

VITRADE *

JETZT VIA GUIDANTS HANDELN!

WWW.GUIDANTS.COM/HANDELN



* Die Handelsmöglichkeit ist eine Dienstleistung der Guidants Trading GmbH. Risikohinweis: Der Handel mit Devisen und Differenzkontrakten (CFDs) birgt ein hohes Risiko für Ihr eingesetztes Kapital.

Guidants

Wer immer die Listen oder Datenbanken kontrolliert, in denen die Guthaben vermerkt sind, kontrolliert auch die Guthaben! Kriminelle, oder auch ein böswilliger Staat, der in einer Nacht- und Nebel-Aktion eine Zwangsabgabe auf Spareinlagen beschließt, können sich zumindest theoretisch Zugriff auf das Vermögen der Bankkunden verschaffen.

In einem auf einer Blockchain basierenden Zahlungssystem werden Informationen über die Guthaben der einzelnen Teilnehmer dagegen nicht in einer zentralen Datenbank, sondern dezentral bei ALLEN Teilnehmern des Zahlungssystems gespeichert. Die Blockchain ist dabei nichts anderes als eine Liste über alle jemals getätigten Transaktionen. Überweist Teilnehmer A einen Betrag von 100 Geldeinheiten an Teilnehmer B, dann teilt Teilnehmer A dem gesamten Netzwerk öffentlich und gleichzeitig anonym diese Transaktion mit. Die Transaktion wird in der Blockchain gespeichert. Die Blockchain ist nichts anderes als eine Liste aller Transaktionen, wobei jeder Block aus einer Transaktion besteht. Dabei enthält jeder Block in Form einer Prüfsumme des vorhergehenden Blocks und der gesamten Blockchain einen Verweis auf die zuvor getätigten Transaktionen. Dadurch sind nachträgliche Modifikationen der Blockchain ausgeschlossen. Einmal getätigte Transaktionen, die vom Netzwerk verifiziert wurden, können nicht mehr rückgängig gemacht werden. Um die Blockchain zu manipulieren, müsste sich ein Hacker Zugriff auf mehr als die Hälfte aller an einem Netzwerk beteiligten Computer verschaffen. Es gibt keine zentrale Instanz, von der die Blockchain kontrolliert wird. Stattdessen übernimmt das Netzwerk als Ganzes die Kontrollfunktion und sorgt dafür, dass die dezentral gespeicherte Blockchain immer konsistent ist. Guthaben in einem auf der Blockchain basierenden Zahlungssystem werden in einer sogenannten Wallet, also einer (meist elektronischen und softwarebasierten) „Geldbörse“ aufbewahrt. Die Wallet besteht aus der Kombination aus einem öffentlichen und einem privaten Schlüssel. Der öffentliche Schlüssel entspricht der Kontonummer in einem traditionellen Zahlungssystem. Allerdings muss die Identität eines Inhabers einer Wallet niemandem bekannt sein – es handelt sich also um das elektronische Äquivalent zu einem anonymen Schweizer Nummernkonto. Der Besitzer einer Wallet erhält durch seinen privaten Schlüssel Zugriff auf sein elektronisches Konto. Jede Transaktion, die er tätigt, muss er mit seinem privaten Schlüssel signieren. Der private Schlüssel ist nur ihm bekannt. Obwohl der öffentliche Schlüssel und der private Schlüssel mathematisch ein fest verbundenes Paar bilden, ist es mathematisch so gut wie unmöglich, allein aus dem allgemeinen bekannten öffentlichen Schlüssel den privaten Schlüssel zu erraten.

Welche Vorteile bietet die Blockchain?

- **Dezentralität:** Es gibt keine zentrale Kontroll- oder Überwachungsinstanz. Willkürliche Eingriffe in das System, zum Beispiel von Kriminellen oder staatlichen Stellen, sind ausgeschlossen.
- **Pseudonymität:** Kontoinhaber in einem auf der Blockchain basierenden Zahlungssystem sind pseudonym. Das bedeutet: Bei Transaktionen sind nur öffentliche Schlüssel beziehungsweise Adressen sichtbar. Welche Person sich hinter einem Schlüssel bzw. einer Adresse verbirgt, wird nirgendwo in der Blockchain gespeichert. Der Besitzer einer Wallet weist sich ausschließlich durch den Besitz des privaten Schlüssels als Inhaber einer Wallet aus.
- **Transparenz:** Transaktionen sind öffentlich, weil sie dem gesamten Netzwerk mitgeteilt werden und für alle sichtbar in der Blockchain vermerkt werden. In einigen fortschrittlichen Blockchain-Konzepten wird die Transparenz allerdings eingeschränkt, um echte Anonymität bei Transaktionen zu verwirklichen.
- **Unmöglichkeit von Manipulationen:** Nachträgliche Veränderungen der

Blockchain sind in der Praxis ausgeschlossen, weil jede Transaktion fest mit einer vorhergehenden Transaktion verkettet ist. Transaktionen können, nachdem sie einmal verifiziert wurden, nicht mehr rückabgewickelt werden.

- **Schnelligkeit:** Transaktionen können schneller abgewickelt werden als in vielen anderen elektronischen Zahlungssystemen, weil die Verifikation bereits ein Teil des Systems ist.
- **Smart Contracts:** Einige Blockchains können nicht nur finanzielle Transaktionen bewältigen, sondern auch mit sogenannten Smart Contracts verknüpft werden, bei denen die Gegenleistung einer Zahlung ebenfalls auf elektronischem Wege abgewickelt wird. So kann der Download einer gekauften Musikdatei in Form eines Smart Contracts mit der Zahlung des fälligen Preises verknüpft werden. Erst, wenn der User eine Transaktion per Blockchain getätigt hat, erfolgt automatisch die Auslieferung der bestellten Musikdatei – und zwar unabhängig vom Verkäufer, der in einen einmal gestarteten Smart Contract nicht mehr eingreifen kann. Umgesetzt wird das Konzept der Smart Contracts beispielsweise im Ethereum-Protokoll.

Liebe Krypto-Trader: Wie wäre es mit Aktien?

Scannen Sie tausende Werte nach technischen und fundamentalen Kriterien und finden Sie so einfach und schnell lukrative Chancen. Legen Sie Vorlagen und Listen Ihrer Kandidaten an. Richten Sie Alarme ein, die Sie in real-time über neue Signale und Chancen informieren. Das und mehr bietet Ihnen der Screener! Abonnenten von Guidants PROup und PROmax profitieren ganz besonders davon: Sie können sich ab sofort beispielsweise die historische Performance von Aktien ausrechnen lassen und Dividenden dabei entweder einbeziehen oder unberücksichtigt lassen.

Bitcoin & Co.: Welche Kryptowährungen gibt es eigentlich?













Die Welt der Kryptowährungen wird immer unübersichtlicher. Auf der Internetseite www.coinmarketcap.com sind fast alle existierenden Kryptowährungen aufgelistet. Insgesamt gibt es inzwischen weit über 1.000 Kryptowährungen – Tendenz steigend. Die allerwichtigsten sollen an dieser Stelle vorgestellt werden: Bitcoin, Bitcoin Cash, Bitcoin Gold, Ethereum und Ethereum Classic, Ripple, Litecoin, DASH, Monero und Dogecoin.

Bitcoin – der „First Mover“, Bitcoin Cash und Bitcoin Gold

Der Bitcoin genoss als erste bekannte Kryptowährung („First Mover“) natürlich einen gewissen Vorteil („First Mover Advantage“). Allerdings gibt es auch innerhalb der Bitcoin-Community seit längerer Zeit Reibereien. So ist durch die zunehmende Nutzung des Bitcoin das System recht träge und auch teuer (Transaktionskosten) geworden, was man gerne ändern würde. Durch ein Update namens SegWit2x, das in Kürze aktiviert wird, dürften diese Schwierigkeiten aber zumindest teilweise beseitigt werden.

Ein Teil der Community wollte aber nicht auf dieses Update warten. So entstand im Sommer 2017 Bitcoin Cash als ers-

ter sogenannter „hard fork“ (harte Abspaltung) von Bitcoin. Hauptunterschied von Bitcoin zu Bitcoin Cash ist dabei die Blockgröße. Während diese beim Bitcoin nämlich auf 1 MB festgezurrt ist, erlaubt Bitcoin Cash hier bis zu 8 MB. In Kürze soll es mit Bitcoin Gold eine weitere solche Abspaltung geben. Sollte es dann Ende November auch noch zu einem SegWit2x-Fork kommen, gäbe es neben dem Original-Bitcoin bereits drei Alternativ-Bitcoins: Bitcoin, Bitcoin Cash, Bitcoin Gold und Bitcoin SegWit2x.

Der Vorteil solcher Abspaltungen ist, dass Bitcoin-Besitzer die durch die Spaltung neu entstehenden Bitcoin-Alternativen automatisch eingebucht bekommen. Im Falle von Bitcoin Cash stieg der Wert des neuen, alternativen Bitcoins (Bitcoin Cash) in der Spitze auf knapp 900 US-Dollar. Insofern wirkt jede Abspaltung quasi wie eine Gelddruckmaschine („free money“). Aber natürlich bietet eine solche Abspaltung nicht nur Vorteile.

	Bitcoin	Ethereum	Ripple
Anzahl tägliche Transaktionen	278.000	361.000	600.000
Marktkapitalisierung	95,4 Mrd. Dollar	29,1 Mrd. Dollar	7,9 Mrd. Dollar
Tägliches Transaktionsvolumen	9,0 Mrd. Dollar	3,1 Mrd. Dollar	63,6 Mio. Dollar

Denn wenn es in Zukunft zu immer mehr solcher Abspaltungen kommt, könnte dadurch letztlich der Wert des Original-Bitcoin sinken – ganz einfach weil Investoren durch die Inflation an alternativen Bitcoins das Vertrauen verlieren. Möglich wäre natürlich auch, dass sich einer dieser alternativen Bitcoins als die beste Alternative herauskristallisiert – und alle Investoren ihr Geld umschichten, sich also auf diese eine Alternative konzentrieren. Dann ginge der Original-Bitcoin womöglich unter und an seine Stelle würde dieser eine Alternativ-Bitcoin treten.

Litecoin – wenn Bitcoin Gold ist, ist Litecoin Silber

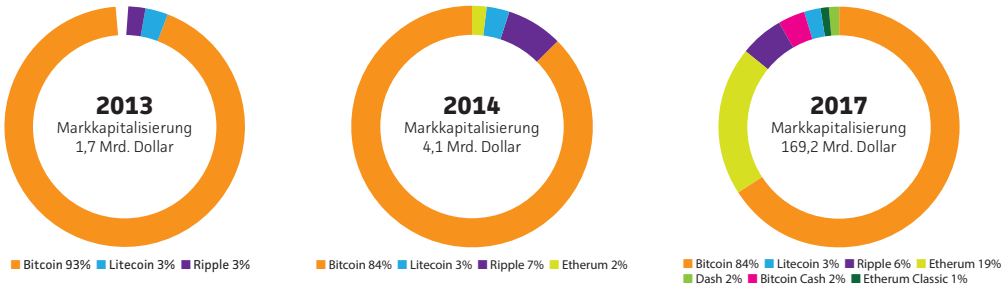
Litecoin wurde am 7. Oktober 2011 von Charles Lee veröffentlicht. Technisch betrachtet ist das Litecoin-Netzwerk ähnlich wie das Bitcoin-Netzwerk aufgebaut. So halbiert sich beim Litecoin die Menge der neu zu erzeugenden („minenden“) Litecoins ebenso wie beim Bitcoin und auch ein Litecoin kann in 100.000.000 kleinere Einheiten unterteilt werden. Anders als beim Bitcoin werden hier jedoch durchschnittlich alle 2,5 Minuten (anstatt wie beim Bitcoin durchschnittlich alle zehn Minuten) neue Coins erzeugt, was einerseits Transaktionen beschleunigt, aber andererseits auch dazu führt, dass es am Ende viermal so viele Litecoins wie Bitcoins geben wird (rund 84 Millionen Stück gegenüber rund 21 Millionen Stück). Zudem versucht man durch Verwendung eines anderen Proof-of-work-Algorithmus (Scrypt versus SHA256 beim Bitcoin) das Mining gleichmäßiger zu verteilen und somit einer Zentralisierung entgegenzuwirken, wie es sie beim Bitcoin durch Entstehung großer Miningpools leider schon – in einem zunehmenden Maße – gibt.

In der Vergangenheit gelang es dem Litecoin phasenweise, zur zweitwichtigsten Kryptowährung hinter dem Bitcoin aufzusteigen. Der Kurs stieg während des Hypes um den Bitcoin im Jahr 2013 von wenigen Cent auf mehr als 40 US-Dollar. Anscheinend wurde der Bitcoin damals einigen Anlegern zu teuer und so entdeckten sie den Litecoin als Alternative. Anschließend brach der Litecoin jedoch stärker als der Bitcoin ein, im Tief auf weniger als drei US-Dollar ein. Zwar erholte auch er sich inzwischen – wenngleich mit einiger Verzögerung – deutlich, jedoch bei weitem nicht so stark wie der Bitcoin. Erst zuletzt markierte er neue Hochs, als es der Litecoin Community gelang, das SegWit2x-Update innerhalb kurzer Zeit durchzusetzen.

Monero und DASH – das Zauberwort heißt Anonymisierung

Das Wort Monero stammt aus der Plansprache Esperanto und bedeutet übersetzt so viel wie Währung. Anders als Litecoin, der ja grundsätzlich auf Bitcoin basiert und nur ein wenig angepasst wurde, wurde Monero von Grund auf neu programmiert. Hauptziel war dabei ein möglichst hoher Anonymisierungsgrad. Als Proof-of-work-Algorithmus hat man sich für CryptoNight entschieden, was zwar sehr speicherintensiv ist, sich dafür aber gut für den Einsatz auf normalen PCs eignet. Das Zielintervall zur Blockgenerierung beträgt zwei Minuten und der Mining-Schwierigkeitsgrad (Difficulty) passt sich kontinuierlich an (beim Bitcoin passiert dies alle zwei Wochen).

Nach Erreichung einer Geldmenge von 18,132 Mio. Moneros (Kürzel: XMR) wird die Erzeugung neuer Moneros auf 0,6 XMR je 2-Minuten-Block eingefroren, so dass ab diesem Zeitpunkt eine konstante Menge an neuen XMR erzeugt wird. Dadurch steigt die Geldmenge prinzipiell stetig an, wobei die Inflationsrate wegen der immer größeren Geldbasis aber trotzdem gegen 0% tendiert. Die Entwickler vermuten jedoch, dass sich die Zahl neu erzeugter Moneros sowie die Zahl verlorengehender Moneros (zum Beispiel durch Hardware-Defekte, Viren etc.) langfristig etwa ausgleicht, so dass Monero letztlich eine perfekt inflations- aber auch deflationsfreie Währung werden könnte. Mithilfe von Ring-Signaturen werden Transaktionen in der Monero-Blockchain stets stark verschleiert, so dass Geldströme nicht verfolgt werden können. Optional kann eine Transaktion jedoch als transparent gekennzeichnet werden.
DASH, zuvor bekannt als Darkcoin und XCoin, nutzt dagegen X11 als Proof-of-work-Algorithmus. Der Hauptunterschied gegenüber anderen Kryptowährungen ist, dass DASH ein Netzwerk aus Servern nutzt, die mehr Aufgaben durchzuführen haben als die typischen Nodes wie sie bspw. beim Bitcoin verwendet werden und daher Masternodes heißen. Innerhalb des dezentralen Netzwerks kann prinzipiell jeder seinen eigenen Masternode starten. Dank dieses ausgeklügelten Systems dauern Transaktionen bei DASH nur knapp zwei Sekunden. Zusätzlich sorgt DASH, ähnlich wie Monero, für einen hohen Grad an Anonymisierung. Prinzipiell geben Masternodes den Nutzern sogar die Möglichkeit, die Transaktionsgeschichte einzelner Coins komplett zu löschen und damit die ohnehin hohe Fungibilität der Währung noch weiter zu erhöhen.



Aufgrund des zunehmenden Vertrauens der Anleger haben diese beiden Kryptowährungen zuletzt ihren Wert deutlich steigern können, DASH sogar noch stärker als Monero.

Ethereum, Ethereum Classic und Ripple – etwas andere Kryptowährungen

Ethereum, Ethereum Classic und Ripple verstehen sich nicht als Kryptowährungen im klassischen Sinne. So versucht die Firma Ripple Labs (an der u.a. Google Ventures sowie Andreessen Horowitz und andere Risikokapitalgeber beteiligt sind) ein Zahlungsnetzwerk und in letzter Konsequenz quasi ein privates Geldsystem aufzubauen. Zwar ist das Protokoll für dieses Zahlungsnetzwerk Open Source, so dass sich prinzipiell jeder an der Entwicklung beteiligen

kann. Grundsätzlich behält jedoch Ripple Labs hier die Kontrolle, was schon daran erkennbar wird, dass das Unternehmen die Hälfte aller erzeugten Ripples (XRP) selbst behält, um von deren möglicher Wertsteigerung profitieren zu können. Insgesamt existieren aktuell 100 Milliarden XRP und Stand aktuell sollen es auch nicht mehr werden, Mining ist also nicht vorgesehen.

Aktuelle Kurse und Charts für Bitcoin, Ether, Ripple und andere Kryptowährungen, übersichtlich zusammengefasst finden Sie auf Guidants auf einem speziellen Desktop. **Jetzt auch mit Experten-Streams**

Ethereum dagegen versteht sich als verteiltes System, das eine Plattform zum Ausführen von Smart Contracts bietet und auf einer eigenen, öffentlich zugänglichen Blockchain basiert. Die Kryptowährung Ether wird dabei eigentlich nur als Zahlungsmittel für Rechenleistung genutzt, die Teilnehmer des Netzwerks zur Verfügung stellen. Zunächst sah es tatsächlich danach aus, als könne Ethereum dem Bitcoin den Rang ablaufen. Durch einen Fehler im Smart Contract einer sogenannten dezentralen autonomen Organisation (The DAO) gelang es jedoch einem unbekannten Hacker, 3,6 Millionen Ether im damaligen Wert von rund 65 Mio. Euro unbrauchbar zu machen. Schließlich beschloss die Ethereum-Community, diesen Angriff mit Hilfe einer harten Abspaltung abzuwehren. Allerdings existieren seitdem zwei Ethereum-Blockchains. Die Anhänger der ursprünglichen Blockchain führen diese nämlich einfach als Ethereum Classic weiter.

Dogecoin – die Charity-Kryptowährung

Ursprünglich war der Dogecoin, der auf Litecoin basiert, als Parodie auf den Bitcoin gedacht. Daher war die maximale Menge von Dogecoin mit 100 Milliarden Stück von Anfang an extrem hoch (diese wurde bereits Anfang 2015 erreicht). Im Februar 2014 wurde dann diese Begrenzung durch den Gründer Jackson Palmer sogar ganz aufgehoben. Stattdessen werden nun jährlich konstant 5,256 Milliarden Dogecoin neu erzeugt („gemint“), wodurch die Inflationsrate im Laufe der Zeit sinkt. Zurzeit liegt die Inflation noch über 5%. Um 2030 wird sie dann bei ca. 3% liegen und um 2050 auf unter 2% sinken.

In der Vergangenheit nutzte die sehr aktive Dogecoin-Community diese virtuelle Währung bereits mehrfach zur Unterstützung von – aus ihrer Sicht – interessanten Projekten. So sammelte man 2014 Geld zur Unterstützung des jamaikanischen Bobteams, damit es an den Winterspielen in Sotchi teilnehmen konnte (qualifiziert hatten sie sich bereits). Darüber hinaus wurde auch noch Geld zur Unterstützung des indischen Rodlers Keshavan gesammelt, sodass auch dieser bei den Olympischen Winterspielen dabei war. Später gab es Spenden für ein Wasserprojekt in Kenia, bekannt unter dem Namen „Doge4Water“, bei dem von etwa 4000 Spendern umgerechnet rund 40.000 US-Dollar zusammenkamen. Zuletzt rückte der Dogecoin im Jahr 2014 in den Fokus einer breiten Öffentlichkeit, als die Community dem NASCAR-Rennfahrer Josh Wise durch Spenden die Teilnahme an mehreren Rennen ermöglichte. Als Wertanlage eignet sich der Dogecoin allerdings somit wohl kaum.

Das sind die wertvollsten Kryptowährungen

Die folgende Tabelle zeigt die wertvollsten Kryptowährungen mit einer Marktkapitalisierung von mindestens einer Milliarde Euro. Die Marktkapitalisierung ergibt sich dabei als Produkt aus Anzahl der aktuell existierenden Währungseinheiten und dem Marktwert je Währungseinheit in Euro (Stand: 23.10.2017).

Name	Marktkapitalisierung in Euro	Name	Marktkapitalisierung in Euro	Name	Marktkapitalisierung in Euro
Bitcoin	84,104 Mrd.	Litecoin	2,527 Mrd.	NEO	1,369 Mrd.
Ethereum	23,351 Mrd.	DASH	1,746 Mrd.	Monero	1,307 Mrd.
Ripple	6,437 Mrd.	NEM	1,825 Mrd.	IOTA	1,031 Mrd.
Bitcoin Cash	4,595 Mrd.	BitConnect	1,482 Mrd.	Ethereum Classic	1,007 Mrd.

Wichtige Begriffe

Kryptowährung: Kryptowährungen sind Fiatgeld in Form digitaler Zahlungsmittel. Dabei werden Prinzipien der Kryptographie angewandt, um ein dezentrales, verteiltes, sicheres Zahlungssystem zu realisieren. Die Geldschöpfung erfolgt dabei nicht durch eine (staatliche) Zentralbank, sondern durch Privatleute.

Proof-of-work-Algorithmus: Unter Proof-of-Work versteht man in der Informatik eine Methode, die den übermäßigen Gebrauch eines Dienstes verhindern soll. Dies geschieht, in dem man vor der Nutzung eine kleine Aufgabe lösen muss. Ursprünglich eingeführt wurde die Idee, um Spam Mails zu erschweren.

Blockchain: Die Blockchain (zu deutsch: Blockkette) ist eine Datenbank, deren Integrität (Sicherung gegen Manipulation) durch Speicherung des Hashwertes des vorhergehenden Datensatzes im jeweils nachfolgenden Datensatz gesichert wird (eben eine Kette). Die Blockchain, in Form einer dezentralen Datenbank, ist die technologische Basis von Kryptowährungen und somit des Bitcoin. Für jede Kryptowährung existiert eine eigene Blockchain.

Blocksize: In diese Datenbank (Blockchain) werden die Daten in Form von Blöcken hinein geschrieben. In einem solchen Block werden zahlreiche Transaktionen zusammengefasst und dieser anschließend mit einem Hash versiegelt. Das ist im Prinzip die Aufgabe der Miner, wofür diese zum einen durch neue Coins und zum anderen durch Transaktionsgebühren entlohnt werden. Dabei ist die Blockgröße (Blocksize) vorher festgelegt worden, beim Bitcoin auf maximal 1 MB, bei Bitcoin Cash bspw. auf maximal 8 MB.

Mining: Unter Mining (zu deutsch: schürfen) versteht man bei Kryptowährungen im Prinzip die Geldschöpfung. Anders als bei den Notenbanken unterliegt die Geldschöpfung jedoch strengen Regeln und funktioniert nur unter Aufwendung von Rechnerleistung. Daher sehen sich die meisten Kryptowährungen in der Tradition von Edelmetallen wie Gold, so dass man den Prozess der Geldschöpfung in Anlehnung an diese Edelmetalle eben als Mining bezeichnet.

Node: Ein Node (zu deutsch: Knoten bzw. Netzwerkknoten) ist ein Element eines Netzwerks und dient als Austauschpunkt für den Datenverkehr.

Smart Contract: Smart Contracts sind Computerprotokolle, die Verträge abbilden oder überprüfen bzw. die Aushandlung oder Abwicklung eines Vertrages technisch unterstützen. Dadurch wird eine schriftliche Fixierung eines Vertrages unter Umständen überflüssig. Sie haben üblicherweise auch eine Benutzerschnittstelle und bilden somit die Logik vertraglicher Regelungen auf technischem Weg ab. So versuchen sie eine höhere Vertragssicherheit bei gleichzeitiger Reduktion der Kosten zu erreichen.

Ring-Signatur: Eine Ring-Signatur ist eine bestimmte Art einer digitalen Signatur, die von jedem Mitglied einer Gruppe ausgeführt werden kann, dass über den jeweils entsprechenden Schlüssel verfügt. Eine der Sicherheitseigenschaften einer solchen Signatur ist, dass es rechnerisch nicht möglich ist festzustellen, welcher der jeweiligen Schlüssel verwendet wurde, um die Signatur zu erzeugen. Der Name Ring-Signatur kommt aus der ringförmigen Struktur des Signaturalgorithmus.

Wo und wie kann man Kryptowährungen handeln?

Grundsätzlich ist die Mutter aller Kryptowährungen, also der Bitcoin, oftmals sehr einfach gegen verschiedene Währungen wie Euro oder US-Dollar handelbar. Ansonsten kann man die anderen Kryptowährungen an diversen Kryptowährungsbörsen kaufen oder verkaufen, braucht dazu aber meistens Bitcoin (weil sie dort nur gegen Bitcoin und nicht gegen Euro oder US-Dollar gehandelt werden).

Wer in Deutschland Bitcoins kaufen möchte, kann dies jedoch leider (noch) nicht an einer deutschen Kryptowährungsbörse tun. Denn es gibt schlicht keine deutsche Kryptowährungsbörse. Allerdings steht ihnen der Handelsplatz bitcoin.de zum Kauf von Bitcoin, Bitcoin Cash und zukünftig auch Ethereum zur Verfügung. Optimal wäre es dabei, wenn man gleichzeitig ein Bankkonto bei der **Fidor Bank** (eine reine Online Bank) besitzt. Denn dies kann man dann in seinem bitcoin.de-Account hinterlegen und so Direkthandel betreiben.

Eine weitere europäische Möglichkeit verschiedene Kryptowährungen wie bspw. auch DASH oder Monero gegen Euro zu kaufen bietet die niederländische Anycoindirect.eu. Allerdings sollte man berücksichtigen, dass hier zwar keine Orderkosten anfallen, dafür jedoch die Spreads zum Teil sehr hoch sind.

Bitfinex.com ist die nach eigenen Angaben weltweit größte Kryptowährungsbörse. Bitfinex zeichnet sich durch eine große Anzahl handelbarer Basiswerte, unkompliziertes Margin-Trading und eine relativ einfache Anmeldung ohne langwierige Verifikation aus. Bitfinex hat seinen Sitz in der chinesischen Sonderverwaltungszone Hongkong.

bitcoin.de sowie **Anycoindirect.eu** sind zwar interessant, eignen sich jedoch nicht für Daytrader, da der Handel hier schlicht zu langsam von statten geht. Wer wirklich mit Kryptowährungen traden möchte, kommt daher an einer der fünf folgenden Kryptowährungsbörsen nicht vorbei:

Bittrex.com (USA): Bei Bittrex.com kann man gegenwärtig nahezu alle Kryptowährungen problemlos handeln. Bisher sind mir keine Probleme, bspw. mit Auszahlungen bekannt. Insofern ist diese Kryptowährungsbörse empfehlenswert.

Coinbase.com (USA): Coinbase ist ein, durch bekannte Risikokapitalgeber wie u.a. Andreessen Horowitz (insgesamt 117 Mio. US-Dollar an Finanzierungen erhalten, derzeit geschätzter Wert des Unternehmens: 1,6 Mrd. US-Dollar) finanziertes, US-amerikanisches Unternehmen, dass eine Online-Handelsplattform für Kryptowährungen betreibt. Das Unternehmen war seinerzeit das erste, das eine offizielle Genehmigung zum Handel mit Kryptowährungen von den – in den USA zuständigen – Behörden erhielt.

Der Nachteil von Coinbase ist, dass man sich nahezu ausschließlich auf die großen und bekannten Kryptowährungen wie Bitcoin, Ethereum oder Litecoin fokussiert hat. Der Vorteil jedoch ist, dass man hier auch andere Kryptowährungen wie eben Ethereum oder Litecoin nicht nur gegen Bitcoin, sondern auch gegen Euro oder US-Dollar handeln kann. Darüber hinaus bietet Coinbase auch noch eine sogenannte Web-Wallet (Cyberwallets) an, man kann also hier durchaus auch seine Bitcoins „parken“.

Von **A** wie **aktuell** bis **Z** wie **zeitlos**

ENTDECKEN SIE UNSERE **ONLINE-MAGAZINE**

Mit dem passenden Schwerpunkt für Anleger und Trader:

- Rohstoffe
- Devisen
- Zertifikate oder CFDs



GodmodeTrader

JETZT KOSTENLOS ABONNIEREN

Gemini.com (USA): Gemini.com ist ebenfalls eine US-amerikanische Kryptowährungsbörse. Diese wurde von den beiden Winklevoss-Zwillingen gegründet, die einst erfolgreich gegen Mark Zuckerberg geklagt hatten (weil sie an der Gründung von facebook beteiligt gewesen sein wollen). Von den Winklevoss-Zwillingen mag man halten was man will, Gemini.com aber gilt in der Branche als seriös.

Kraken.com (USA): Auch Kraken.com ist eine in den USA ansässige Kryptowährungsbörse. Genau wie die deutsche Handelsplattform bitcoin.de verfügt auch Kraken.com über eine Kooperationsvereinbarung mit der Fidor Bank, so dass es sicherlich nicht schadet, wenn man dort ein Konto hat. Kraken.com gilt in der Branche ebenfalls als seriös, allerdings ist das Angebot an handelbaren Kryptowährungen etwas begrenzt.

Poloniex.com (USA): Ähnlich wie bei Bittrex lassen sich bei Poloniex nahezu alle Kryptowährungen handeln und es kommen sogar laufend neue hinzu. Bis vor wenigen Monaten galt Poloniex dabei noch als sehr seriös. Leider kam es zuletzt jedoch zu Berichten, dass einige Anleger ihre Auszahlungen erst mit starken Verzögerungen erhielten. Insofern gibt es durchaus Mitglieder der Kryptowährungs-Community, die inzwischen zur Vorsicht bei dieser Kryptowährungsbörse raten.

Möglichkeit des Margin Tradings: Margin Trading bedeutet, dass man nur eine Sicherheitsleistung für den Kauf einer – im vorliegenden Fall natürlich – Kryptowährung wie bspw. dem Bitcoin leisten muss. Dadurch wird es möglich gehebelt long (auf steigende Kurse spekulierend) oder short (auf fallende Kurse spekulierend) zu gehen. Die fünf vorgestellten Kryptowährungsbörsen bieten jedoch nicht alle solches Margin Trading an. Zwar stellt sich durchaus die berechtigte Frage, ob man solch hochvolatilen Underlyings wie es Kryptowährungen nun mal sind, überhaupt gehebelt handeln sollte. Allerdings lassen sich dadurch natürlich Gewinne optimieren.

Bittrex arbeitet eigenen Aussagen zufolge derzeit daran, eine Margin Trading Möglichkeit zu schaffen. Dafür ist hier jedoch Algo-Trading (der Computer handelt nach vorgegebener Programmierung) möglich. Coinbase bietet zwar prinzipiell die Möglichkeit zum Margin Trading, allerdings nur in einem sehr begrenzten Umfang. Bei Gemini gibt es zurzeit keine Möglichkeit zum Margin Trading. Bei Kraken.com hingegen ist Margin Trading möglich, allerdings auch hier nur in einem recht eingeschränkten Ausmaß. Zu guter Letzt gibt es mit Margin Trading bei Poloniex keinerlei Probleme.

Worauf Sie unbedingt achten müssen

Das wichtigste bei der Auswahl ihrer Kryptowährungsbörse ist, dass sie auf deren Integrität und Seriosität achten. Natürlich müssen Sie auch darauf achten, dass die Kryptowährungen, die Sie gerne handeln möchten, auch gehandelt werden können. Und wenn Sie gerne die Möglichkeit des Margin Trading nutzen möchten, muss das natürlich auch angeboten werden. Allerdings sollten Sie bei Zweifel an der Integrität und/oder Seriosität lieber Abstand halten. Denn in der Vergangenheit sind bereits mehrere Kryptowährungsbörsen in die Pleite gerutscht. So nicht nur die einstmals größte und führende Kryptowährungsbörse, die japanische MtGox, sondern bspw. auch die aus den USA stammende Cryptsy. Ich selbst hatte einige Litecoins bei Cryptsy liegen, die leider im Zuge der Insolvenz verloren gegangen sind (ich hätte mich zwar an einer Sammelklage beteiligen können, aber klagen sie als Deutscher mal in den USA). Seien Sie sich darüber im Klaren, dass bei einer Insolvenz ihre Coins weg sind, ganz egal wie hoch die Buchgewinne in der Theorie auch sein mögen.

Wenn Sie Kryptocoins gerne über einen längeren Zeitraum halten möchten, sollten Sie diese nicht im Handelskonto einer solchen Kryptowährungsbörse liegen lassen. Viel besser wäre es, Sie dann an eine Ihnen gehörende Wallet zu senden. Welche Wallets (Software) es gibt und was Sie genau tun müssen, haben Sie ja bereits im Kapitel „Die ersten Schritte“ erfahren. Eine solche Wallet müssen sie zudem richtig, bspw. gegen Virenbefall, schützen.

Das Beste habe ich mir nun noch für den Schluss aufgehoben: Kryptowährungen gelten in Deutschland tatsächlich als Währungen, so dass Kursgewinne nach einer Haltedauer von einem Jahr steuerfrei sind. Zwar müssen Sie ihre Gewinne in der Steuererklärung ausweisen, der Staat wird Ihnen jedoch kein Geld weg nehmen. Wenn Sie natürlich kurzfristige Tradinggewinne einfahren, wird darauf ganz normal die Abgeltungssteuer fällig.

Handelbare Instrumente – Derivate

Tendenziell ist eher zu einem Direktinvestment zu raten. Allerdings gibt es inzwischen durchaus einige Alternativen, zum Beispiel eine Exchange Traded Note (WKN: A18KCN) auf den Bitcoin bei Tradegate. Dabei entsprechen 200 Stück dieses ETNs einem Bitcoin.

Seit November 2016 bietet die Schweizer Bank Vontobel zudem ein Partizipationszertifikat (WKN: VN5MJG) auf den Bitcoin in US-Dollar an, wobei die Kurse der US-Kryptobörsen Coinbase und Kraken.com als Referenz dienen. Zur Abbildung eines Bitcoin benötigt man hier zehn solcher Zertifikate.

Wer es besonders spekulativ mag, kann den Bitcoin auch über CFDs gehebelt handeln. Da der Kurs selbst bereits sehr volatil ist, sollten das nur erfahrene Trader in Erwägung ziehen. Anbieter sind beispielsweise AvaTrade, JFD Brokers, eToro, IG oder Plus500. Achten Sie jedoch darauf, auf welche Kryptowährungsbörse sich der CFD bezieht. Denn diese können sich von Kryptowährungsbörse zu Kryptowährungsbörse erheblich unterscheiden, was übrigens auch Arbitragegeschäfte ermöglicht.

Handeln Sie Kryptowährungen über solche Produkte, so kaufen Sie die Kryptowährung aber nicht direkt, vielmehr wetten Sie nur auf deren Kursentwicklung. Daher haben Sie in diesem Fall keinerlei Probleme mit der Sicherheit. Sie können diese Produkte ganz normal, wie bspw. auch Aktien, in ihrem Depot halten sowie kaufen oder verkaufen.

Allerdings hat dies leider einen sehr gravierenden Nachteil. Denn wenn Sie mit solchen Derivaten nur auf die Kursentwicklung wetten, die entspreche Kryptowährung damit aber ja gar nicht kaufen und verkaufen, gilt die – eben noch als positiver Faktor hervorgehobene – Steuerfreiheit nach einem Jahr leider nicht.

Auch darum schrieb ich eingangs, dass ich eher zu einem Direktinvestment raten würde. Bei allen Gefahren und (technischen) Schwierigkeiten, die das mit sich bringen mag. Ganz abgesehen vom generell noch sehr überschaubaren Angebot dieser Produkte (in erster Linie gibt es diese ja nur mit dem Bitcoin als Underlying).

Bitcoins jetzt direkt in Guidants handeln!

Bitcoins und andere Kryptowährungen können auch direkt aus der Investment- und Analyseplattform Guidants heraus gehandelt werden. So bietet der an Guidants angeschlossene CFD-Broker JFD bereits den Handel mit Bitcoins an.

Demnächst werden auch Kryptowährungsbörsen (im ersten Schritt Bitstamp und Cex.io) an Guidants angeschlossen, so dass Bitcoin & Co. dann auch ohne den Umweg über Derivate direkt über Guidants gehandelt werden können.

Hier finden Sie einen Link zum Guidants Mini-Handbuch, welches die wichtigsten Features erklärt.

Bitcoin-Mining: 59% Rendite im Jahr?

Das Bitcoin-Mining lohnt sich nicht mehr, jedenfalls nicht für Privatpersonen. Stimmt dieses Vorurteil wirklich? Der Selbstversuch zeigt: Es gibt doch noch Auswege, mit denen man sich Bitcoins und andere Kryptowährungen einfach selbst erzeugt.

Das waren noch Zeiten: Kurz nach der Erfindung des Bitcoins im Jahre 2008 brauchte es nur einen durchschnittlichen PC (und etwas technisches Know-how), um profitabel Bitcoin zu minen. Man ließ den Rechner einige Stunden oder Tage laufen und war anschließend ein paar Bitcoins reicher. In den Anfangsjahren des Bitcoins war die Mining-Funktion sogar in normalen Bitcoin-Wallets integriert. Natürlich waren die gewonnenen Bitcoins damals kaum etwas wert. Aber wer die Miningerträge bis heute aufbewahrte, der ist heute ziemlich wohlhabend. Schließlich kostetet ein Bitcoin heute mehr als 5.500 Dollar. Tendenz: Stark steigend. Es dürfte so manchen IT-Nerd geben, der durch das Mining zum Multimillionär wurde.

Bitcoin-Mining ist virtuelles Goldschürfen

Bitcoin-Mining ist der Prozess, mit dem Transaktionen im Bitcoin-Netzwerk verarbeitet und bestätigt werden. Dazu sind bewusst sehr aufwendige Rechenprozesse notwendig. Die Bitcoin-Miner werden mit den Erträgen dafür belohnt, dass sie ihre Rechenleistung zur Verfügung stellen. Und damit das Bitcoin-Netzwerk am Laufen halten.

Doch die goldenen Anfangszeiten des Bitcoins-Mining sind längst vorbei. Das hat vor allem zwei Gründe: Da die Rechenpower, die für das Bitcoin-Mining verwendet wird, stark steigt, sinkt der Ertrag des einzelnen Miners deutlich. Denn die Schwierigkeit des Minings wird regelmäßig an die vorhandene Rechenpower angepasst, so dass trotz wachsender Rechenpower nicht mehr Bitcoins pro Zeiteinheit erzeugt werden. Zu allem Überfluss wird die Gesamtzahl der durch das Mining erzeugten Bitcoins alle vier Jahre halbiert. Beide Effekte zusammengenommen hatten zur Folge, dass die Erträge des einzelnen Miners immer stärker gesunken sind. War am Anfang das Mining noch mit normalen PC-CPUs möglich, brauchte es später Hochleistungsgrafikkarten (wie sie auch in Spiele-PCs zu finden sind), um Bitcoin-Mining profitabel zu betreiben. Heute hat man ohne speziell für den Zweck entwickelte Hardware (sogenannte Application Specific Integrated Circuits, ASIC) praktisch keine Chance mehr.

Auch unter Einsatz immer besserer Hardware wurde es für den einzelnen Miner immer unwahrscheinlicher, durch das Mining jemals etwas zu verdienen. Denn beim Mining wird immer nur der Rechner belohnt, der den jeweils zu lösenden Block als erstes löst. Welcher Rechner das ist, hängt vor allem von der Rechenpower und dem Zufall ab.

Wie wird das Mining heute betrieben?

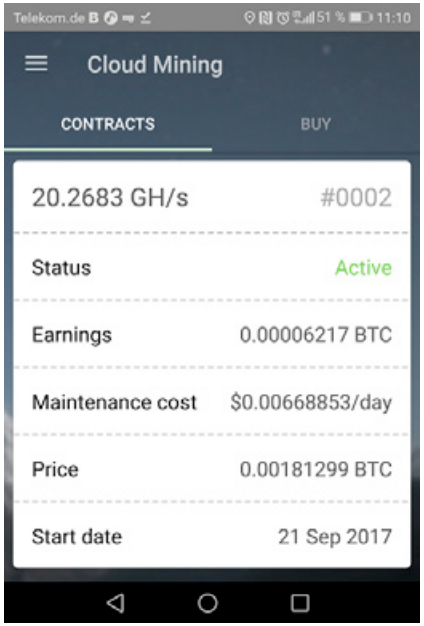
Ein erster Ausweg der Miner war, sich zu sogenannten Miningpools zusammenzuschließen. Alle Rechner eines Pools versuchen gemeinsam, einen Block

zu lösen. Gelingt dies, werden die Erträge des einen Rechners proportional zur Rechenpower unter allen am Pool beteiligten Rechnern aufgeteilt. Wer als Privatperson mit Hochleistungsrechnern und ASICs das Bitcoin-Mining über einen Pool betreibt, für den kann sich das unter Umständen auch noch heute lohnen - zumal die erzeugten Bitcoins bzw. Bruchteile davon ja im Wert stark steigen. Allerdings ist auch das Mining über einen Pool nur lohnend, wenn die Stromkosten nicht zu hoch sind. Bei den hohen Energiepreisen in Deutschland dürfte sich das Bitcoin-Mining mit privaten Hochleistungsrechnern auch dann kaum mehr lohnen, wenn man sich mit anderen zu einem Pool zusammenschließt und über geeignete Hardware verfügt.

Gibt es einen anderen Weg, mit dem auch Privatpersonen ohne großes technisches Know-how heute noch selbst Bitcoin minen können? Einen Ausweg bieten sogenannte Mining-Dienstleister. Diese Unternehmen betreiben meist riesige Rechnerparks, mit denen das Bitcoin-Mining deutlich effizienter betrieben werden kann als im kleinen Maßstab. Bekannte Namen sind etwas Genesis Mining, ein von einem Deutschen in Hongkong gegründetes Unternehmen, sowie der Miningpool Minergate, der inzwischen ebenfalls Mining-Verträge an Privatpersonen verkauft. Allerdings tummeln sich auch auf diesem Feld viele schwarze Schafe - und auch bei den genannten Unternehmen ist es wohl schon zu verspäteten oder ganz verlorenen Auszahlungen gekommen.

Lohnt sich der Abschluss eines Miningvertrages?

Welche Rendite kann man erwarten, wenn man als Privatperson einen Mining-Dienstleister beauftragt? Ein Selbstversuch bei Minergate zeigt, dass die Rendite zumindest auf den ersten Blick gar nicht so gering ist. Am 21. September wurden für diesen Artikel 0,00181299 BTC (umgerechnet zum damaligen Kurs 7,27 Dollar) in einen Mining-Vertrag bei Minergate investiert. Bis drei Wochen später wurden durch das Mining 0,00006217 BTC verdient (zum aktuellen Kurs umgerechnet rund 0,25 Dollar). Pro Tag verdient der Miningvertrag eine Rendite von ungefähr 0,16 Prozent. Auf das Gesamtjahr hochgerechnet ergibt das (ohne Reinvestition der erzielten Beträge) eine „Pseudorendite“ von 59 Prozent. Nur um eine Pseudo-Rendite handelt es sich, weil der zu Beginn investierte Betrag ja nicht mehr zurückgezahlt wird und die Miningerträge auch nicht konstant sind, sondern sehr stark schwanken können und außerdem mit der Zeit auch abnehmen, da die Rechenpower in der Blockchain insgesamt tendenziell stark steigt.



Der Miningvertrag hat theoretisch eine unendliche Laufzeit. Allerdings nur theoretisch, denn von den Miningerträgen werden jeden Tag 0,00668853 Dollar abgezogen. Damit werden die laufenden Kosten des Minings, also vor allem die Stromkosten, beglichen. Sollten die Miningerträge irgendwann drei Tage am Stück nicht mehr ausreichen, um die laufenden Kosten zu begleichen, dann endet das Mining automatisch. So ist das im Vertrag mit dem Miningdienstleister vereinbart.

Die Gefahr, dass die Miningerträge die Kosten nicht mehr decken, ist vor allem dann gegeben, wenn die Rechenpower im Bitcoin-Netzwerk weiter stark steigt (wovon langfristig auszugehen ist, besonders bei steigenden Bitcoin-Kursen)

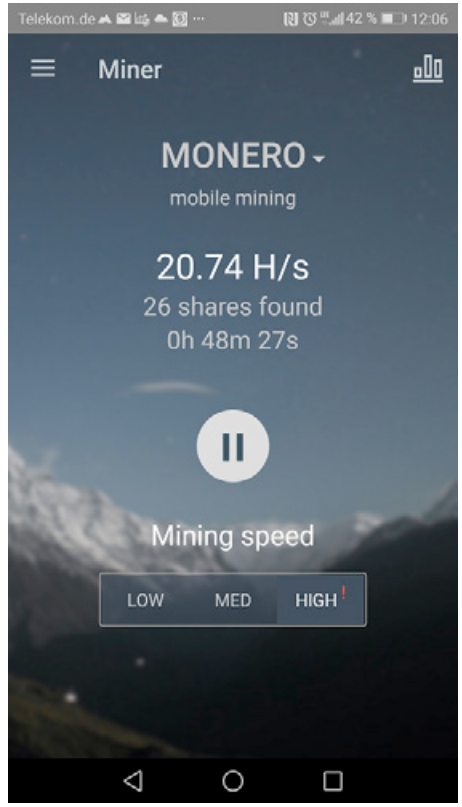
oder wenn der Bitcoin gegenüber dem Dollar an Wert verliert. Auf lange Sicht sinken die Erträge wohl so oder so. Miningverträge sind deshalb keine solide Investition, sondern haben mehr mit einem Glücksspiel gemeinsam. Die Erträge können zeitweise sehr hoch sein, aber ob der Auftraggeber eines Miningvertrags auf lange Sicht einen Gewinn erzielt, steht in den Sternen. Nur so erklärt sich die auf den ersten Blick sehr attraktive Pseudorendite von im gezeigten Beispiel 59 Prozent p.a.

Lohnt sich das Mining anderer Kryptowährungen?

Neben dem Bitcoin gibt es inzwischen unzählige andere Kryptowährungen. Bei den meisten Währungen sind die Miningerträge zu Beginn am höchsten und sinken mit der Zeit deutlich. Dadurch wird ein Anreiz geschaffen, bereits früh die entsprechende Währung zu verwenden und Rechenpower für die jeweilige Blockchain zur Verfügung zu stellen. Wer zu den ersten Minern gehört, kann hier unter Umständen große Gewinne einstreichen. Allerdings nur dann, wenn die Währung zu einem Erfolg wird und sich tatsächlich behaupten kann. Denn nur unter diesen Umständen können die erzeugten Beträge überhaupt jemals umgetauscht oder als Zahlungsmittel verwendet werden.

Für die Währung Monero kann das Mining mit der Minergate-App sogar auf einem handelsüblichen Smartphone betrieben werden. Hohe Erträge sollte man sich davon aber nicht versprechen. Im Test wurden mit einem neuen Smartphone der mittleren bis hohen Preisklasse innerhalb von 24 Stunden rund 0,04 Euro per Mining erzielt. Vor Kosten allerdings. Zieht man die Stromkosten ab oder rechnet womöglich sogar die Gerätekosten mit ein, ist das Mining nach Kosten überhaupt nicht profitabel. Jedenfalls dann nicht, wenn der Monero in den kommenden Jahren nicht mehr stark an Wert gewinnt.

Satoshi Nakamoto hatte Bitcoin eigentlich als ein dezentral verwaltetes Zahlungssystem entworfen. Durch die Konzentration der Mining-Rechenpower in den Händen großer Mining-Pools und -Dienstleister ist diese Vision aber zumindest gefährdet. Neue Kryptowährungen werden deshalb häufig so entworfen, dass das Mining möglichst auch auf handelsüblicher Hardware erfolgreich ist und sich durch den Einsatz von ASICs möglichst nur geringe Vorteile realisieren lassen. Gleichwohl gilt auch bei den zahlreichen neuen Altcoins: Das Mining lohnt sich in der Regel nur dann, wenn Coins gemint werden, die im Wert gewinnen. Die Preisentwicklung der geminten Coins bleibt der wichtigste Einflussfaktor für den Erfolg jede Mining-Operation.



ICO-Hype: Jetzt geht es auch in Deutschland los

Das erste deutsche Initial Coin Offering (ICO) ist angelaufen. „Wysker“ will das Online-Shopping revolutionieren. Lohnt sich das auch für die Anleger?

Mit Wysker hat das erste deutsche Start-Up ein sogenanntes Initial Coin Offering (ICO) gestartet. Bei einem ICO nimmt ein Unternehmen frisches Kapital auf, indem eine neue Kryptowährung emittiert wird bzw. sogenannte Token ausgegeben werden. Es handelt sich bisher um eine zumindest in Deutschland völlig unregulierte Form der Unternehmensfinanzierung über Crowdfunding. In Ländern wie China und Südkorea wurden ICOs inzwischen verboten - schließlich hat sich hier in den vergangenen Monaten ein unkontrollierter Kapitalmarkt entwickelt.

In den vergangenen Monaten gab es international einen regelrechten Hype um ICOs. In Deutschland wagte sich bisher aber noch kein Unternehmen an eine Finanzierung über die Ausgabe einer Digitalwährung. Doch inzwischen führt Wysker das erste ICO in Deutschland durch. Das junge Start-Up will das Online-Shopping revolutionieren. „Die Idee ist so kühn, dass sie entweder grandios scheitern oder zum Riesenerfolg werden muss“, schrieb die FAZ über das Konzept von Wysker.

Wichtig für Anleger: Irgendwelche Eigentumsrechte am Unternehmen erwirbt der Zeichner mit dem Kauf der neuen Kryptocoins nicht. Vielmehr sollen Werbetreibende mit „Wys Token“, so der Name der neuen Währung, künftig ihre Produkte bei Wysker präsentieren können. User könnten für die Token Rabatte bei Einkäufen erhalten oder ihre Token einfach verkaufen. Direkt bezahlen wird man mit Wys Token aber wohl nicht können. Denn Wysker will die auf der App gezeigten Produkte gar nicht selbst verkaufen, sondern jeweils zu einem Online-Shop weiterleiten.

Das Shopping der Zukunft soll nach der Vorstellung von Wysker wie im Geschwindigkeitsrausch ablaufen und dabei die Daten der User besser schützen als heute. Außerdem soll der User dafür bezahlt werden, dass er seine Daten teilt oder sich Produkte ansieht, die ihn interessieren könnten.

Auf der Wysker-App soll der User im Schnelldurchlauf Produkte angezeigt bekommen, nach denen er sucht oder die ihm gefallen könnten. Durch eine Fingerbewegung kann der User dann entscheiden, dass er den Schnelldurchlauf der Produkte stoppen und sich ein Produkt genauer ansehen will. Wie das funktionieren könnte, zeigt Wysker in dem nachfolgenden Youtube-Video.

Wysker will aber nicht nur das Shopping beschleunigen, sondern die Daten der User auch noch besser schützen als heutige Online-Shops. Die Daten sollen nur dann an die Verkäufer von Produkten weitergeleitet werden, wenn der User dem ausdrücklich zustimmt. Im Gegenzug soll der User für die Weitergabe seiner Daten (oder auch dafür, dass er sich besonders viele Produkte angesehen hat) bezahlt werden.

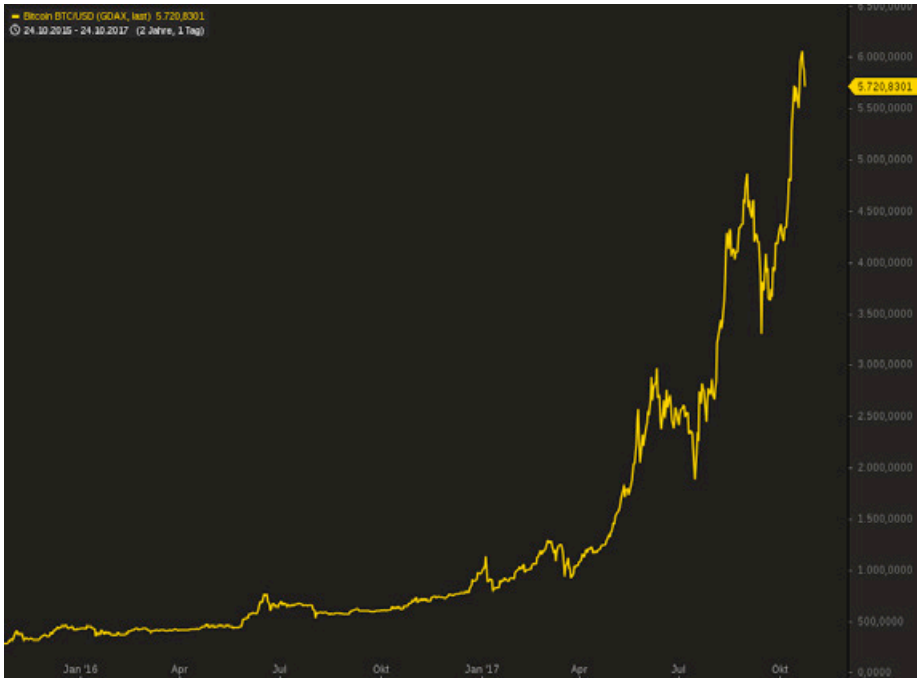
Wysker selbst erwartet, dass seine Token mit der Zeit stark an Wert zulegen werden. Mit diesem Argument sollen wohl auch die Anleger geködert werden, beim ICO mitzumachen. Der ICO soll am Montagabend starten - ein erster Starttermin am Sonntagabend wurde offenbar kurzfristig verschoben. Die Gesamtzahl der

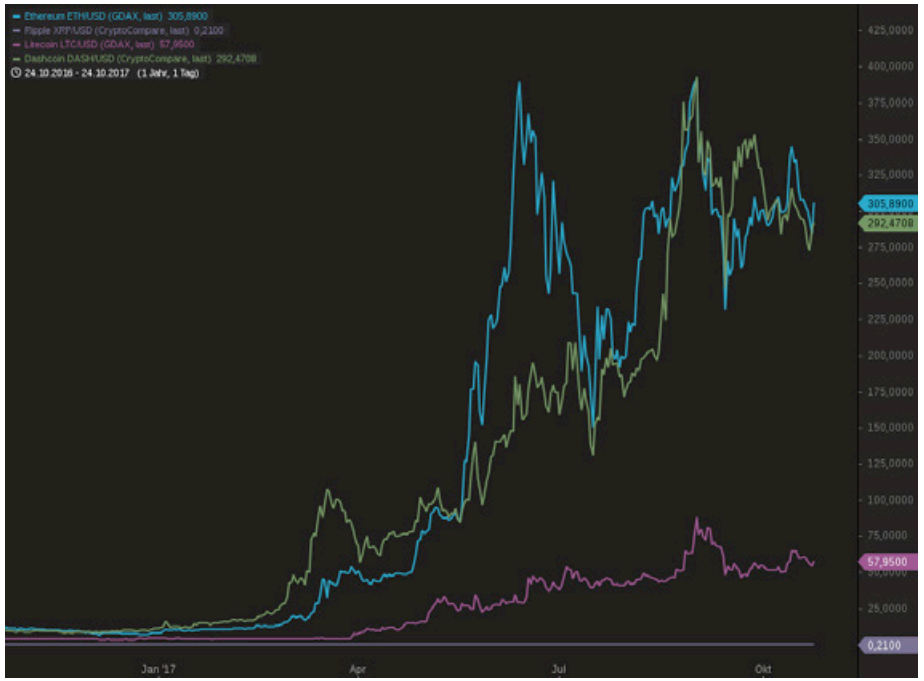
Wys Token soll für alle Zeiten auf 3 Milliarden begrenzt sein. Im Rahmen des ICOs sollen gut 1,782 Milliarden Token bei den Anlegern platziert werden.

Bezahlt wird beim ICO ausschließlich mit der Kryptowährung Ether. Für 1 ETH erhält der Anleger 18123 Wys Token. Umgerechnet kostet ein Wys Token damit ungefähr 2 Cent. Für frühe Zeichner gibt es einen Rabatt von bis zu 30 Prozent. Technisch sind die Token sogenannter Smart Contract auf der Ethereum-Plattform umgesetzt.

Ob sich das alles auch für die Anleger lohnt, ist sehr fraglich. Bisher existiert noch nicht einmal eine funktionsfähige App, geschweige denn die kritische Masse an Usern, um das Konzept von Wysker zum Erfolg werden zu lassen. Auch ist noch überhaupt nicht klar, was der Anleger irgendwann einmal für seine Token erhalten wird.

Spannend dürfte das ICO trotzdem werden. Sollte Wysker die Finanzierung per Kryptocoin gelingen, dürften bald weitere Unternehmen sich an diesem innovativen Weg der Finanzierung versuchen. Ob das auch ein Gewinn für die Anleger ist, muss sich aber noch zeigen. Große Zweifel sind auf jeden Fall angebracht.





SCANNEN SIE
TAUSENDE BASISWERTE IN
SEKUNDENSCHNELLE

Mit dem Screener auf Guidants finden Sie lukrative Investmentchancen im Handumdrehen

Technisch und fundamental

Aktien, Währungen, Rohstoffe

Alarmfunktion und Index-Matrix

JETZT SCREENER TESTEN

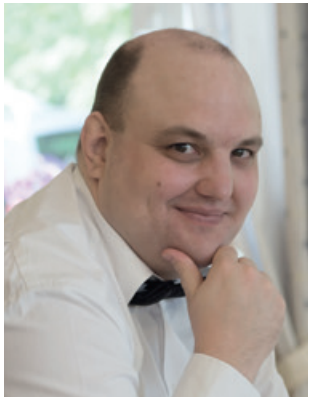
bit.ly/guidants-screener



Guidants

Der Krypto-Trader: Sascha Huber stellt sich und seinen neuen Börsenbrief vor

Liebe Leserinnen und Leser,



mein Name ist Sascha Huber, ich wurde am 13. September 1978 in Trier geboren und habe 1997, im Alter von 19 Jahren, meine Allgemeine Hochschulreife (Abitur) am Max-Planck Gymnasium in Trier absolviert. Anschließend habe ich meinen Wehrdienst abgeleistet und ein Informatikstudium begonnen. Schon während des Studiums habe ich dann den Schritt in die Selbstständigkeit gewagt (es war die Zeit der „Dotcom Bubble“ und des Neuen Marktes), was sehr erfolgreich wurde. Als dann der New Economy-Boom vorbei war, habe ich mir erst einmal die Welt angesehen, ich bin also viel gereist, u.a. nach Venezuela (Isla Magarita in der Karibik).

Auf die Dauer wurde mir das jedoch zu langweilig und so stieg ich kurz nach der Gründung beim Münchener Startup sharewise ein. Dort befasste ich mich zunächst mit Online Marketing und SEO, was spannend war. Später übernahm ich dann als Chefredakteur den sharewise Börsenbrief, der u.a. der wohl erste Börsenbrief in Deutschland mit einer Kaufempfehlung für die Tesla Aktie war (im Jahr 2012 zu unter 35,00 US-Dollar). Als sharewise von der japanischen Minkabu Gruppe übernommen wurde und jegliches Produktgeschäft einstellte, gab es dort für mich nichts mehr zu tun. So verpflichtete mich mein alter Bekannter Stephan Heibel und ich arbeitete rund 1 ½ Jahre bei seinem Börsenbrief mit.

Anschließend machte ich noch einmal etwas Urlaub und startete dann zum 1. Dezember 2016 meinen YouTube Kanal „Saschas Börsentag“: http://www.youtube.com/SaschasBörsentag

Da ich mich bereits seit 2012 mit dem Bitcoin beschäftigt hatte und Anfang 2013 zu Kursen unter 25 US-Dollar eingestiegen war, war auch der Bitcoin bzw. Kryptowährungen allgemein von Anfang an ein Thema in meinen Videos. Wer damals schon meinem Hinweis gefolgt ist, konnte Bitcoins noch zu unter 750 US-Dollar einsammeln, wo der Kurs heute steht brauche ich Ihnen nicht zu erläutern. Im Video vom Freitag, dem 3. März 2017, berichtete ich dann über meinen Einstieg bei DASH zu damals 44,29 US-Dollar. Heute, nur knapp acht Monate später, notiert DASH um die 300 US-Dollar.

Einige von Ihnen, darunter sogar der ein oder andere Banker, werden mich vielleicht auch von meinen Seminaren zum Thema „Bitcoin – kann eine Kryptowährung die Welt revolutionieren?“ auf der World of Trading 2016 oder auch von meinem Auftritt auf den IB-Days von Michael Voigt vom März diesen Jahres kennen. Zudem habe ich schon im Dezember 2013 einen ersten Artikel im „Traders Mag“ veröffentlicht und sagte damals ein langfristiges Kursziel für den Bitcoin in Höhe von mindestens 10.000 US-Dollar voraus, aber erst nach einem vorherigen starken Kursrutsch. In den folgenden Jahren kamen weitere Artikel hinzu, in denen ich den Handel mit Kryptowährungen generell erläuterte sowie einige alternative Kryptowährungen („Altcoins“) vorgestellt habe.

Mein Vorteil, wie schon damals während der „Dotcom Bubble“ ist, dass ich einst Informatik studiert habe und daher die Technologie verstehe (eine Vorlesung zum Thema „Datenbanken“ respektive „Verteilte Systeme“ ist hierfür

empfehlenswert). Zugleich bin ich aber auch schon seit inzwischen mehr als 20 Jahren an der Börse tätig und kenne daher die Finanzmärkte – und zwar nicht nur in der Theorie, sondern in der Praxis.

So konnte ich sowohl den Crash zu Zeiten der „Dotcom Bubble“ anno 2000 als auch den Crash im Zuge der „Finanzkrise 2007/2008“ nicht nur finanziell problemlos überleben, sondern zum Teil sogar davon profitieren (Kauf der Aktie der Bank of America Ende des Jahres 2009).

Nach Gesprächen mit dem Team von Godmode-Trader, die mich und mein Tun schon länger beobachtet haben, haben wir uns entschieden unsere Kräfte zu bündeln und Ihnen allen ein Angebot zu machen, dass Sie nicht ablehnen sollten, nämlich den aus unserer Sicht besten Kryptowährungs-Börsenbrief Deutschlands auf den Markt zu bringen.

Nun hoffe ich, dass es auch ein großes Interesse an diesem neuen, einzigartigen Produkt gibt und möchte Sie auf diese Weise gerne in die phantastische Welt der Kryptowährungen mitnehmen. Mein Anspruch dabei ist zu erkennen welche Kryptowährungen wirklich aussichtsreich sind – und welche man schlichtweg als Humbug oder gar Betrug klassifizieren sollte. Schon am Neuen Markt habe ich so manche Aktie frühzeitig als Insolvenzkandidaten identifiziert und daher zum Verkauf gestellt, was mir leider auch die ein oder andere Abmahnung einbrachte (so viel zur Pressefreiheit in Deutschland).

Ihr
Sascha Huber

Folgen Sie mir **kostenlos** auf meinem Guidants Experten-Desktop



Impressum

Herausgeber:

BörseGo AG

Balanstraße 73, Haus 11/3.OG

81541 München

Telefon: +49 89 76 73 69-0

Fax: +49 89 76 73 69-290

E-Mail: kundenservice@boerse-go.de

Internet: www.boerse-go.ag

Aktiengesellschaft mit Sitz in München

Registergericht: Amtsgericht München

Register-Nr: HRB 169607

Umsatzsteueridentifikationsnummer

gemäß § 27a UStG: DE207240211

Autor: Sascha Huber. Oliver Baron

Grafik: BörseGo AG

Vorstand: Robert Abend, Christian Ehmig,

Thomas Waibel

Aufsichtsratsvorsitzender: Theodor Petersen

Risikohinweis:

Soweit die BörseGo AG Börsen- oder Wirtschaftsinformationen, Kurse, Indizes, Preise, Nachrichten, Marktdaten sowie sonstige allgemeine Marktinformationen bereitstellt, dienen diese nur zur Information und zur Unterstützung Ihrer selbstständigen Anlageentscheidung. Die genannten Informationen stellen keine Aufforderung zum Kaufen, Halten oder Verkaufen von Wertpapieren und derivativen Finanzprodukten dar und begründen kein individuelles Beratungs- oder Auskunftsverhältnis. Sie sind keine Rechts-, Steuer- oder sonstige Beratung und können eine solche auch nicht ersetzen.

Bevor der Leser Investmententscheidungen trifft, sollte er sich sorgfältig über die Chancen und Risiken des Investments informiert haben. Aus einer positiven Wertentwicklung eines Finanzprodukts in der Vergangenheit kann keinesfalls auf zukünftige Erträge geschlossen werden. Die BörseGo AG übernimmt keine Haftung für die erteilten Informationen, die aus von der BörseGo AG als vertrauenswürdig erachtet wurden, für bereitgestellte Handelsanregungen sowie für deren Vollständigkeit.

Bitte beachten Sie insbesondere unsere AGB, die für alle unsere Angebote und Services gilt