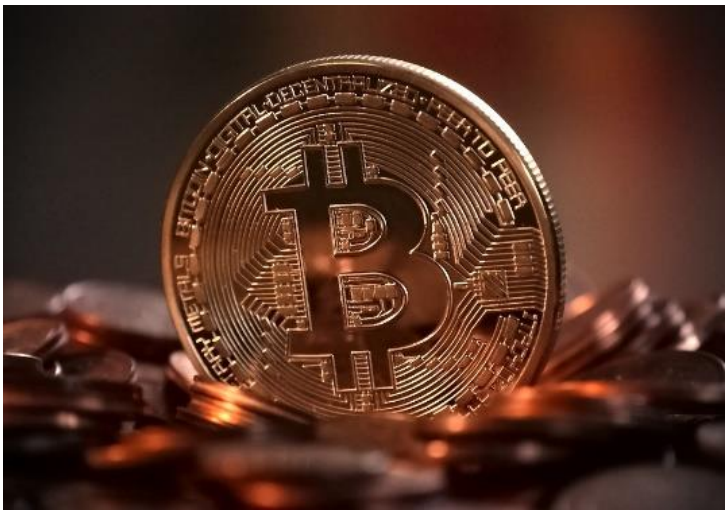
Bitcoin

Eine kurze Einführung



Inhalt

http://www.janda.io

Allgemein

Der Artikel ist für Einsteiger geschrieben und soll eine Einführung in die Terminologie und Technologie des Bitcoins geben. Er ist der erste Teil einer Serie, die einen Überblick über die neue Welt des Krypto-Geldes geben will.

Unter dem Begriff Bitcoin versteht man umgangssprachlich die Werteinheiten dieser digitalen Währung. Vielmehr verbirgt sich hinter dem Begriff aber die Technologie und das Protokoll, welches den Bitcoin als Zahlungsmittel ermöglicht.

In dem Artikel werden Gemeinsamkeiten und Unterschiede des so genannten „digitalen Goldes“ (Bitcoin) mit unseren vertrauten Währungen (dem so genannten Fiat-Geld) aufgezeigt.

Fiat-Geld: Dieser Begriff bezieht sich auf den Erschaffungsprozess des Geldes. Eine Analogie gibt es zu der Terminologie der Sekte FIAT-Lux „es werde Licht“. Es geht darum etwas ohne inneren Wert aus dem Nichts zu erschaffen. Dies trifft auf das Drucken von Euro-Banknoten und auf die Giralgeld-Schöpfung der Banken zu. Wenn man es genau nimmt, müsste man den Begriff auch auf den Bitcoin anwenden. Gebräuchlich ist aber eine Unterscheidung von Fiat-Geld zu Kryptowährungen.

Die Geschichte des Bitcoins

Der Bitcoin entstand Anfang 2009. Die Finanzkrise hatte zu diesem Zeitpunkt das Vertrauen in unser Geldsystem schwer erschüttert. Dadurch entstand der Wunsch nach alternativen Zahlungssystemen. Dabei denken die meisten zunächst an Gold. Aber Gold eignet sich eben nur als Wertaufbewahrungsmittel. Es ist kaum teilbar und ein Einkaufen mit Goldstücken oder Münzen ist quasi nicht möglich. Der Bitcoin versucht die entstandene Lücke zu schließen. Seine große Innovation ist die so genannte Blockchain. Diese erlaubt es Transaktionen extrem sicher, transparent und ohne die Nutzung einer zentralen Kontrollinstanz zu speichern.

Viele Kritiker tragen immer wieder vor, dass Bitcoin keinen inneren Wert habe. Es wäre lediglich eine Anzahl von Einsen und Nullen, deren Wert sich nur auf das

Vertrauen der Anwender stützt. Diese Kritik ist auch absolut zutreffend. Doch bleibt hierbei unerwähnt, dass dies auch auf unser vertrautes Papier- und Giralgeld (Bankguthaben) zutrifft.

Das konventionelle Geld wird von Banken und Regierungen kontrolliert. Zuweilen bleiben die Handlungen und Entscheidungen der Banken und Regierungen im Verborgenen. Das Vertrauen, dass die Akteure immer im Sinne des Gemeinwohls handeln, ist erschüttert. Der Bitcoin ist hier völlig transparent, zudem gibt es keine Kontrollinstanz. Die Geldmenge und Schöpfung der Bitcoin-Einheiten ist in den Protokollen festgelegt. Dies zeigt aber auch auf, dass der Bitcoin das konventionelle Geld niemals ersetzen kann. Kredite mit längeren Laufzeiten wären bei einer deflationären Währung wie dem Bitcoin nicht abbildbar.

Der Wert des Bitcoins ist darauf zurückzuführen, dass die Anzahl der Personen, die den Bitcoin als Alternative entdeckt haben, stetig steigt. Solange das Vertrauen in das konventionelle Finanzsystem weiterhin niedrig bleibt, wird der Kurs des Bitcoins steigen.

Eine der Aufgaben der Europäischen Zentralbank (EZB) ist es, die Inflationsrate bei einem Wert von ca. 2% zu halten. Die wirtschaftspolitischen Auswirkungen einer Deflation wären gravierend. Die EZB versucht dies durch eine expansive Geldpolitik zu erreichen.

Das ganze Geld wird buchhalterisch gesehen durch eine Bilanzverlängerung der Geschäftsbanken in den Markt gebracht. Im letzten Jahr hat die EZB hierzu quasi 60 Milliarden Euro pro Monat sinnbildlich „gedruckt“. Demzufolge stiegen die Schulden jeden Monat um diese Summe.

Daher ist es sehr wahrscheinlich, dass mittelfristig weitere Länder ähnlich wie Griechenland in Zahlungsschwierigkeiten kommen werden.

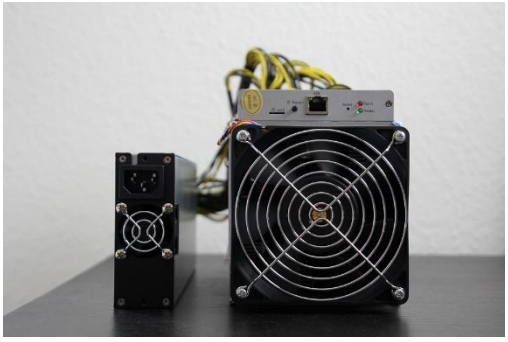
Dies alles stützt die Wertentwicklung des Bitcoins. Die Zukunft wird zeigen, ob sich die Banken oder das quelloffene Bitcoin-Protokoll als vertrauenswürdiger erweisen.

Die Blockchain

Viele betrachten die Blockchain als die eigentliche Innovation des Bitcoins. Die Blockchain ist eine Art verteiltes Kontenbuch, in dem alle Transaktionen (und damit alle Bitcoin-Bestände) enthalten sind. Die Integrität wird durch sicherere kryptografische Verfahren gewährleistet. Alle bestätigten Transaktionen sind nicht umkehrbar. Entgegen aller Kritik ist der Bitcoin nicht anonym. In dem Kontenbuch (der Blockchain) sind alle Transaktionen enthalten, die jemals getätigt wurden. Da die Kontennummern (Bitcoin-Adressen) aus kryptischen Zeichenfolgen bestehen, spricht man hier von „Pseudonymität“.

Um den Bitcoin zu verstehen, muss man die Blockchain verstehen:

Im Bitcoin Ökosystem gibt es die Benutzer (User), die Miner (Rechner, die die Blockchain absichern) und die Blockchain (dezentrales Kontenbuch aller Transaktionen die jemals getätigt wurden).



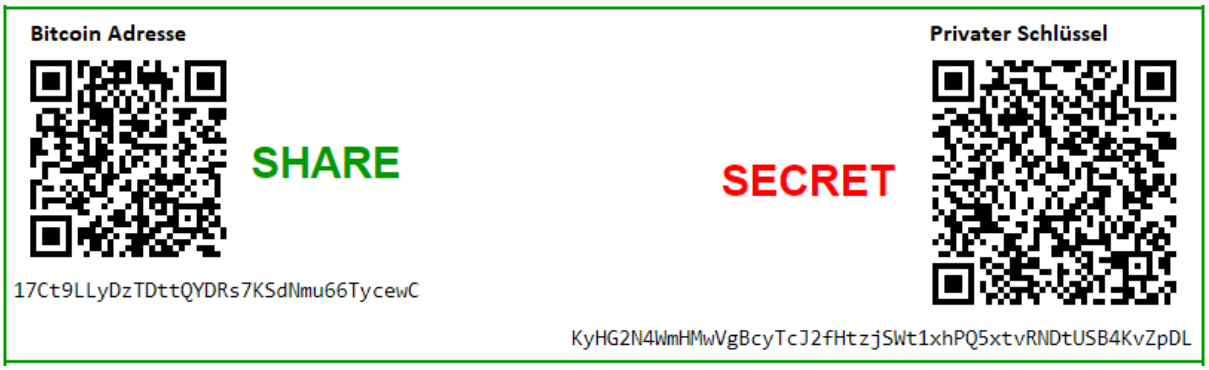
Eine spezielle Bitcoin Mining-Hardware

Wenn jetzt neue Transaktionen erstellt werden, dann versuchen die Miner diese Transaktionen in einem neuen Block zu bündeln. Neben den Transaktionen wird auch der Hashwert des Vorgängerblocks (eine kryptografische ID, die diesen Block und dessen Inhalt identifiziert) in dem aktuellen Block gespeichert. Durch die Referenz auf den Vorgängerblock entsteht logisch gesehen die Kette der Blöcke (Blockchain). Die Miner errechnen dann einen neuen Hashwert, der noch weitere Kriterien erfüllen muss. Das Bitcoin-Protokoll stellt sicher, dass ca. alle zehn Minuten ein Block der Blockchain hinzugefügt wird.

Der erfolgreiche Miner erhält eine Belohnung von aktuell 12,5 Bitcoin. Alle vier Jahre wird diese Belohnung halbiert. Da diese Belohnung das Geldmengen-Wachstum reguliert, handelt es sich beim Bitcoin um eine deflationäre Währung. Die Gesamtmenge der Bitcoins wird niemals 21 Millionen Werteinheiten erreichen bzw. überschreiten. Neben dem durch die Finanzkrise erschütterten Vertrauen in das konventionelle Geldsystem, ist dies der Hauptanreiz für eine nachhaltige Wertsteigerung des Bitcoins.

Die „Kontonummer“

Mit der „Kontonummer“ ist die Bitcoin-Adresse gemeint. Jeder Teilnehmer am Bitcoin Netzwerk kann sich beliebig viele Bitcoin-Adressen erstellen. Beim Erstellen wird immer ein Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel, erzeugt. Mit dem privaten Schlüssel kann auf das Konto zugegriffen werden. Alle ausgehenden Transaktionen müssen mit ihm signiert werden. Sollte dieser verloren gehen, gäbe es keine Chance mehr an das Geld zu kommen.



Ein Bitcoin-Konto bestehend aus der Bitcoin Adresse (öffentlicher Schlüssel) und dem privaten Schlüssel

Das Bitcoin-Konto in der Abbildung zeigt ein mit https://www.bitaddress.org neu erstelltes Konto. Wichtig ist, dass der private Schlüssel niemandem zugänglich gemacht wird und sicher gespeichert wird. Die Kontonummer (Bitcoin Adresse) kann jederzeit aus dem privaten Schlüssel errechnet werden.

Technisch gesehen ist das Guthaben nur auf der verteilten Blockchain gespeichert. Die Schlüssel werden lediglich für den Zugriff auf dieses „Konto“ benötigt.

Digitales Gold?

Der Bitcoin wird oft als digitales Gold bezeichnet. Dies verdankt er dem Umstand, dass Bitcoins einige Eigenschaften mit echtem Gold teilen. Die Menge der Werteinheiten sind in beiden Fällen begrenzt. Diese Knappheit ist ein wichtiges Merkmal, welches bei konventionellem Geld nicht garantiert werden kann.

Sowohl Gold als auch Bitcoin müssen durch einen aufwändigen Prozess gefördert („ge-mined“) werden. Wenn man es genau nimmt, ist die landläufige Meinung, dass Bitcoins errechnet werden, nicht ganz korrekt. Bitcoins werden

als Belohnung für die Arbeit im Zusammenhang mit dem Absichern der Blockchain gegen Manipulation ausgegeben. Das System verringert die Ausgabemenge mit der Zeit so, dass die festgelegte Grenze nie überschritten wird.

Die Eigenschaft der Teilbarkeit ist bei Gold nicht wirklich vorhanden. Diese findet man nur bei Bitcoin und beim konventionellen Fiat-Geld.

Chancen und Risiken

Durch Nutzung des Bitcoin Netzwerks können innerhalb von Minuten Werte international und mit geringen Transaktionskosten übermittelt werden. Der deflationäre Charakter der Bitcoin-Währung ist ein Argument für die Nutzung als Wertaufbewahrungsmittel.

Es gibt keine zentrale Instanz, die diese Währung kontrolliert. Wikileaks wäre beispielsweise durch eine Sperrung der PayPal-Konten fast pleitegegangen. Die Existenz von Bitcoin hat es ermöglicht, die Arbeit von Wikileaks weiter durch Spenden zu unterstützen.

„There is no free lunch“ – Alles hat seinen Preis. Bislang könnte man den Text als Plädoyer für den Bitcoin missverstehen. In dem ganzen Bitcoin Umfeld stecken aber auch Risiken. Im Folgenden werden die wichtigsten Risiken aufgezeigt.

Zwar gibt es immer mehr Anleger, die Bitcoin als langfristige Investition betrachten. Jedoch besteht ein größerer Teil der Eigentümer der Bitcoins aus Spekulanten und so genannten „Day-Tradern“. Dies hat zur Folge, dass der Kurs der Währung sehr volatil ist. Sollte es mal einen markanten Einbruch geben, dann könnten Stop-Loss Orders jederzeit zu einem Lawineneffekt führen, der die Währung innerhalb von Stunden viel an Wert verlieren lassen würde. Verluste von 30% an einem Tag kamen schon vor.

Auch die Abhängigkeit vom privaten Schlüssel kann ein Nachteil sein. Sollte der Key ausgespäht oder verloren werden, dann hat man keine Chance mehr, auf sein Guthaben zuzugreifen. Kein Spezialist wird in der Lage sein, den privaten Schlüssel wieder zu restaurieren.

Sollten Betrugsfälle innerhalb einer Tauschplattform vorkommen, dann würde das den Kurs nachhaltig einbrechen lassen.

Die mangelnde Skalierbarkeit des Bitcoin Protokolls ist eine Herausforderung, die noch gelöst werden muss. Wenn die Zahl der Nutzer immer weiter ansteigt, wird es zwangsläufig problematisch werden. Das Bitcoin Netzwerk erzeugt lediglich alle 10 Minuten einen neuen Block. Zudem ist der Block in seiner Größe beschränkt. Es gibt allerdings vielversprechende Lösungsansätze für dieses Problem. Letztlich ist der Wert des Bitcoins aber vom Vertrauen der Nutzer abhängig.

Über den Autor
Martin Janda hat mehr als 20 Jahre Erfahrung im Bereich der Software-Entwicklung und IT-Beratung. Er hat in zahlreichen Projekten in der Finanzbranche gearbeitet, unter anderem für Kunden wie beispielsweise Deutsche Bank, Commerzbank, Schwäbisch Hall und Allianz.
Seine Schwerpunkte sind neben der Blockchain Technologie vor allem die Entwicklung mit C# (DotNet Framework), Java (Spring Framework), C++, Oracle PL/SQL inkl. DB-Administration und IT-Security (CEHV8-Zertifizierung).

Der Bitcoin bewegt sich aktuell in stürmischem Fahrwasser. Die Tatsache, dass immer mehr Länder ihn inzwischen sogar als gesetzliches Zahlungsmittel „küren“ (beispielsweise Japan, Australien und Indien) beruhigt die Lage etwas. Allerdings sind noch viele Meilensteine zu erreichen. Eine langfristige Lösung des Skalierungsproblems würde hier einiges beitragen können. Die Tatsache, dass die Geldmenge immer langsamer wächst (durch die Halbierung der Miner-Belohnung alle vier Jahre. Das nächste Mal im Jahr 2020) und die Tatsache, dass das Interesse an dem Bitcoin ständig steigt, sorgt für günstige Impulse für den Bitcoin-Kurs.

Es darf aber nicht missachtet werden, dass der Bitcoin eine sehr neue Technologie ist. Fundierte Prognosen sind fast unmöglich und erinnern eher an einen Blick in die Glaskugel. Das Vertrauen in die neue Währung ist noch zu brüchig. Und nur davon hängt letztlich der Wert ab.

Viele sehen in dem Bitcoin eine Alternative zu bestehenden Zahlungssystemen. Neben der Kreditproblematik durch den deflationären Charakter des Bitcoin gibt es noch ein weiteres Problem. Die Bitcoin Miner verbrauchen eine sehr hohe Energiemenge für die Absicherung des Netzwerks. Dies ist auch notwendig, um

die Hürde für einen erfolgreichen Angriff extrem hoch zu setzen. Die benötigte Energiemenge pro Transaktion hängt direkt mit dem aktuellen Skalierungsproblem zusammen. All dies lässt nur den Schluss zu, dass Bitcoin lediglich eine Ergänzung des aktuellen Geldsystems sein kann. Der Bitcoin in seiner heutigen Form wird weder die Banken noch Fiat-Währungen ersetzen können. Für risikoaffine Spekulanten stellt er aber durchaus eine langfristige Investitionsmöglichkeit dar.

Haftungsausschluss

Der Inhalt dieser Einführung dient ausschließlich der Information und stellt nicht eine Anlageberatung oder sonstige Empfehlung im Sinne des Wertpapierhandelsgesetzes dar. Diese Einführung ist nicht als Zusicherung etwaiger Kursentwicklungen zu verstehen. Kursentwicklungen in der Vergangenheit bieten keine Gewähr für die Wertentwicklung in der Zukunft. Die Informationen sollen nicht als Aufforderung verstanden werden, ein Geschäft oder eine Transaktion einzugehen. Die Informationen stellen keine Aufforderung zum Erwerb und/oder Handel mit Kryptowährungen dar.