21.07.2023 – 06:15 Uhr

Bitcoin und Kryptowährungen - Hype oder Hoffnung der Technologie

Wir besprechen genauer, wie Bitcoin und Kryptowährungen funktionieren.

Bitcoin und Kryptowährungen - Hype oder Hoffnung der Technologie

Um diese Frage besser beantworten zu können, müssen wir zunächst verstehen, was Kryptowährungen sind und wie sie funktionieren. Lassen Sie uns daher sowohl die technischen als auch die kommerziellen Aspekte von Kryptowährungen betrachten.

Beginnen wir mit den technischen Aspekten, um die Frage nach dem Hype oder der Hoffnung zu beantworten.

Eine Kryptowährung ist eine Währung, die aus digitalen Münzen besteht, die auf einer Blockchain verwaltet werden. Wie der Name schon sagt, besteht eine Blockchain aus Blöcken, die in einem festen Intervall erstellt werden und eine Kette bilden.

Jeder Block enthält eine bestimmte Anzahl von Transaktionen. Für jede Transaktion, die Sie auf dieser Blockchain durchführen, müssen Sie Gasgebühren bezahlen. Das sind die Preise, die Sie für die Kosten der Verarbeitung Ihrer Transaktion und deren Speicherung in der Blockchain zahlen.

Ein Argument für Blockchain-Transaktionen ist oft die Distributed-Ledger-Technologie. Es wird argumentiert, dass das Vertrauen in Institutionen durch das Vertrauen in die Distributed-Ledger-Technologie ersetzt wird. Kryptowährungen werden daher oft als dezentralisiert bezeichnet. Ein Missverständnis ist jedoch der Unterschied zwischen dezentralisiert und verteilt.

Ein dezentralisiertes System bedeutet, dass die Kontrolle und die Macht auf verschiedene Instanzen verteilt sind, aber es gibt immer noch eine Hierarchie zwischen den Knotenpunkten. Verteiltes System bedeutet, dass jeder Knoten auf der Blockchain gleichberechtigt ist, es gibt also überhaupt keine Hierarchie.

Oft wird von dezentralen Systemen gesprochen, obwohl sie verteilte Systeme meinen. Im Allgemeinen lassen sich Kryptowährungen in zwei Kategorien einteilen. Die erste sind stabile Münzen. Das sind Münzen, die an eine Währung oder ein Bündel von Währungen mit einem festen Wechselkurs zu diesen Währungen oder einem Pool oder Korb von Vermögenswerten/Waren gebunden sind. Sie können jederzeit erstellt werden, um mit den Marktveränderungen Schritt zu halten.

Außerdem sind diese Münzen durch Sicherheiten gedeckt. Diese Sicherheiten können Fiat-Geld, Gold/Silber, andere Kryptowährungen usw. sein. Das macht sie zu einem hervorragenden Tauschmittel. Bei der zweiten Kategorie handelt es sich um die volatilen Münzen. Ihr Wechselkurs zu normalen Währungen kann schwanken. Dies ist die prominentere Gruppe von Münzen, zu der auch Bitcoin und Ethereum gehören.

Aber wie werden sie erzeugt und gibt es Unterschiede? Das erste, was einem in den Sinn kommt, ist "Mining". Und für die meisten Währungen stimmt das auch, aber das Mining kann sich je nach dem zugrunde liegenden Konsensalgorithmus unterscheiden. Offensichtlich geht es hier darum, dass irgendjemand entscheiden muss, welche Transaktionen im nächsten Block gespeichert

werden und welche nicht.

Der Platz ist begrenzt und es kann sein, dass mehr Transaktionen warten, als Platz in einem Block vorhanden ist. Dafür gibt es die verschiedenen Algorithmen. Die bekanntesten sind wohl Proof of Work und Proof of Stake, aber auch Proof of Space und andere mögliche Algorithmen können dafür verwendet werden.

Bitcoin als die beliebteste Kryptowährung verwendet Proof of Work, während Ethereum von Proof of Work zu Proof of Stake übergegangen ist. Proof of Work bedeutet, dass jeder Miner für die geleistete Arbeit belohnt wird. Im Fall von Bitcoin bedeutet das, dass jeder Miner Transaktionen aus dem Pool der Transaktionen auswählt, die darauf warten, auf der Blockchain gespeichert zu werden. Dann berechnet der Schürfer den Hash seines Blocks plus den Hash des vorherigen Blocks plus eine Zahl.

Sie können sich das wie das Lösen eines mathematischen Rätsels vorstellen, um den Platz der Transaktion in einer Bibliothek zu bestimmen. Auf diese Weise wird eine sehr eindeutige Nummer erzeugt, die sich ändern würde, wenn eine der Transaktionen oder der Hash des vorherigen Blocks geändert wird. Da der Hash des vorherigen Blocks ebenfalls geändert wird, wenn eine Transaktion in diesem Block geändert wird, wird eine Kette gebildet, die frühere Blöcke davor schützt, später geändert zu werden. Nun muss ein Gewinner aus allen Minern ausgewählt werden. Dies geschieht z.B. durch die Festlegung der Anzahl der Nullen, mit denen der Hash beginnen muss. Ein Miner mit einem passenden Ergebnis kann dann sein Ergebnis veröffentlichen, damit es von den anderen Knoten in der Blockchain überprüft werden kann.

Der Block von Transaktionen, den der Miner zusammengestellt hat, wird dann in die Blockchain geschrieben und der Miner wird mit Münzen belohnt. Dies kann allerdings ein sehr teurer Prozess mit hohem Stromverbrauch sein.

Beim Proof of Stake hingegen wird die Person, die den nächsten Block auswählt, auf der Grundlage der Anzahl der Münzen dieser Person und eventuell anderer Faktoren je nach Münze bestimmt. Je mehr Münzen Sie besitzen, desto höher ist Ihre Chance, als so genannter "Validator" ausgewählt zu werden. Das macht diesen Prozess effizienter, aber ein Miner muss eine Mindestmenge an Ethereum besitzen, um überhaupt an der Validierung teilnehmen zu können.

Lassen Sie uns nun unsere Hype- oder Hoffnungsfrage von einem technologischen Engel aus betrachten.

Kryptowährungen stehen vor einem Trilemma. Sie können sich nur für zwei der drei Ziele entscheiden: Sicherheit, Dezentralisierung und Skalierbarkeit. Bitcoin zum Beispiel hat ein geringes Transaktionsvolumen mit vielen Minern und Validierern. Bitcoin erstellt alle 10 Minuten einen Block mit 3000-4000 Transaktionen. Das bedeutet, dass Bitcoin im Durchschnitt nicht mehr als 4000 Transaktionen alle zehn Minuten verarbeiten kann, da sich sonst immer mehr Transaktionen anhäufen würden, die darauf warten, in die Blockchain geschrieben zu werden. Da es mehrere Miner und viele Validierer gibt, ist es ein langsamer, aber dezentraler und sicherer Prozess.

Es löst auch das Problem der doppelten Ausgaben, indem es verhindert, dass dieselben Münzen in zwei verschiedenen Transaktionen verwendet werden, indem es nur bis zu einer von ihnen verarbeitet. Aber da die Miner ihre Ressourcen in Pools zusammenfassen und die Dezentralisierung verringern, könnte dies zu einem Problem werden, sobald ein Pool 51% der Knotenpunkte hat. Dies wirft die Frage auf, ob eine solche Kryptowährung oder Kryptowährungen überhaupt eine brauchbare Alternative zu unserem derzeitigen Zahlungssystem sind, das sicher und skalierbar, aber zentralisiert ist.

Bitcoin ist nicht skalierbar genug, um alle internationalen Währungstransaktionen abzuwickeln, und Ethereum ist möglicherweise nicht sicher genug (wir alle erinnern uns an die DAO-Sicherheitslücke im Jahr 2016). Es gibt zentralisierte Blockchains in Privatbesitz, die Münzen ausgeben, die skalierbar und sicher sind, aber sie sind zentralisiert. Dann befinden wir uns wieder in dem alten zentralisierten System - mit mehr Transparenz, aber diese zusätzliche Transparenz gilt nur für den Eigentümer der Blockchain und nicht unbedingt für Sie. Dass Kryptowährungen in der Lage sein werden, den internationalen Zahlungsverkehr abzuwickeln, scheint aus heutiger Sicht eine unbegründete Hoffnung zu sein.

Ein weiteres wichtiges Thema ist die Anonymität. Anonymität wird oft als Vorteil von Kryptowährungen genannt, was in gewisser Weise richtig ist, aber im Grunde genommen falsch. Für einen normalen Menschen ist es im Grunde unmöglich herauszufinden, wer wie viele Münzen besitzt, aber für jemanden, der über wahnsinnige Mengen an Ressourcen verfügt, ist es tatsächlich möglich, was dazu führt, dass Bitcoin und die absolute Mehrheit der Kryptowährungen eher pseudoanonym als anonym sind. Das sagen nicht wir, sondern eine der größten Bitcoin-Kaufplattformen. Letztendlich läuft alles auf die Anwendungsfälle hinaus. Nach Einschätzung des IT-Unternehmens Gartner haben die Kryptowährungen das "Tal der Enttäuschung" verlassen und befinden sich bereits auf halbem Weg zum "Hang der Aufklärung". Und Smart Contracts sind bereits heute ein sehr plausibler Anwendungsfall. Aber da könnte noch mehr kommen.

Zusammenfassend lässt sich sagen, dass Kryptowährungen im Moment außer der Spekulation mit den hochvolatilen Kryptowährungen nicht viel Wert haben, aber es gibt echte Anwendungsfälle, die sich weiterentwickeln und weitere Verbesserungen der Lebensqualität und Innovationen schaffen.

Andere entscheidende Faktoren auf dem Weg, Bitcoin könnte seinen Wert aufgrund des Entstehungsprozesses und der Tatsache, dass er begrenzt ist, zugeschrieben bekommen. Durch die Schaffung von ETFs oder anderen Produkten darauf, stellt sich jedoch die Frage, ob das Argument der Begrenztheit ganz richtig ist. Auf jeden Fall ist es nur wahr, wenn Sie echte Bitcoins besitzen.

Und das führt uns zu der nächsten Frage: Wer ist der Verwahrer dieses Bitcoins (oder einer anderen Kryptowährung). Wenn Sie den Bitcoin auf der Plattform halten, befindet er sich in einem "heißen Speicher", der internetfähig und online ist, wenn Sie ihn offline auf Ihrem Stick haben, befindet er sich in einem kalten Speicher. Bei der kalten Lagerung sind Sie der Verwahrer, eine Funktion, die normalerweise eine Bank oder ein Vermögensverwalter für Sie übernimmt.

Kryptowährungen existieren nur in digitaler Form. Schließlich haben Sie einen Code, in dem die Rechte verankert sind. Es gibt keine

physischen Münzen oder Scheine, die Sie in der Hand halten.

Einer der wichtigsten Punkte, warum eine erlaubnisfreie Blockchain in der Lage ist, Krypto-Token zu schaffen, die als Kryptowährung auf der Blockchain dienen, anstatt Institutionen und von der Zentralbank geschaffenes Fiatgeld zu verwenden, ist die Tatsache, dass Kryptowährungen wie Bitcoin in der Lage sind, das Double Spend Problem zu lösen. Das Double Spend Problem beschreibt die Schwierigkeit, sicherzustellen, dass digitales Geld nicht einfach dupliziert werden kann. Im traditionellen Bankensystem verhindern vertrauenswürdige Dritte, wie z.B. Banken, doppelte Ausgaben, indem sie jede Transaktion privat verifizieren.

Im Gegensatz zum traditionellen System mit vertrauenswürdigen Dritten wie Banken und Notaren ist das System dezentralisiert oder verteilt und jedes Bitcoin-Mitglied ist Teil des Verifizierungsprozesses. Das Bitcoin-Netzwerk verhindert Doppelausgaben, indem es für jede Transaktion ein mathematisches Puzzle erstellt (um den nächsten Block zu finden), das von jedem Mitglied der Bitcoin-Gemeinschaft verifiziert werden muss. Dieser Prozess wird als Proof of Work bezeichnet und ist recht energieintensiv.

Daher sind einige Parteien in anderen Kryptowährungen - wie Ethereum - zu Proof of Stack übergegangen, was wir in einem unserer nächsten Artikel erklären werden. Auf diese Weise wird das Vertrauen in eine dritte Partei durch Vertrauen in die Technologie ersetzt. Bei Bitcoin muss jedes Mitglied das gleiche Ergebnis für das mathematische Rätsel berechnen.

Der Markt hat sich von Kryptowährungen zu Krypto-Assets weiterentwickelt, die man als elektronische Wertpapiere oder im Fachjargon als Security Tokens bezeichnen kann. Schließlich - wenn die Liquidität hoch genug ist, um einen echten Marktpreis wie für ein Wertpapier an der Börse zu bilden - sollte es einem Anleger gleichgültig sein, ob er einen Wertpapier-Token oder eine Aktie in seinem Portfolio hält (lassen wir die Frage der Verwahrung für einen Moment beiseite, denn es gibt professionelle Verwahrer wie Banken, die jetzt Verwahrungsdienste anbieten).

Jedes Unternehmen kann also heute über seine Börsenstrategie entscheiden, sei es in Form eines Initial Public Offering von Aktien (IPO) oder in Form eines Security Token Offering (STO). Es wird erwartet, dass es in den nächsten 10-20 Jahren zu einer Verschmelzung von STOs und traditionellen Aktien kommen wird, die sogar auf demselben Markt gehandelt werden könnten. Die US-Aufsichtsbehörde SEC (Security Change Commission) trennt derzeit die Geschäfte an Krypto-Börsen.

Nehmen wir an, wir sind "durch die Ernüchterung hindurch" und auf halbem Weg zum "Hang der Erleuchtung", wie Gartner es ausdrückt.

Es gibt noch viel mehr über Kryptowährungen und Krypto-Assets zu sagen und über die Vor- und Nachteile von Kryptowährungen und Krypto-Assets. Dieser Artikel soll mit einigen Mythen aufräumen, die über Kryptowährungen existieren. Schließlich glauben wir, dass es Hoffnung gibt, insbesondere wenn man sich mit Krypto-Assets und Blockchain und Kryptographie als Technologien beschäftigt. Es gibt auch strenge Protokolle und Protokollverifizierungsmodelle, die derzeit etabliert sind, und es gibt Appetit auf Krypto-Assets, zumindest bei institutionellen Anlegern.

Ob dezentralisierte oder verteilte Kryptowährungen als zusätzliche Zahlungsmethode auf dem Vormarsch sind - wir glauben es - aber ohne ihr Zahlungspotenzial zu übertreiben und ohne in den Hype-Modus zu verfallen. Wie Gartner es formuliert hat: Die Erleuchtung ist auf dem Weg. Vielleicht sind Bitcoin und andere Kryptowährungen jetzt jenseits der Krypto-Blase, die Verhaltensökonomen haben kommen sehen.

Lassen Sie uns einen frischen und aufgeklärten Blick auf die Frage werfen, ob Krypto-Assets das Richtige für Sie sind, und diskutieren Sie die Vor- und Nachteile von Kryptowährungen und Krypto-Assets in unseren kommenden Artikeln.

Karen Wendt

President of SwissFinTechLadies

Medieninhalte