Warum Kryptowährung nicht gleich Kryptowährung ist

Der Konkurs von FTX hat den Glauben an „Krypto“ erschüttert. Dies wird sich wahrscheinlich auch auf die Akzeptanz von Bitcoin und BTC (die Währung von Bitcoin) sowie auf Investitionen in BTC und das Bitcoin-Ökosystem auswirken. Obwohl es gravierende Unterschiede zwischen Krypto und Bitcoin gibt, hängt der Kurs aller Kryptowährungen stark mit dem von Bitcoin zusammen. Wenn BTC steigt, steigt auch Krypto.

An Kryptowährungen führt kein Weg mehr vorbei, – die globale Marktkapitalisierung von Krypto beläuft sich heute schon auf ca. €769.80 Milliarden. Kritiker behaupten, dass hinter Bitcoin kein Wert liegen würde, weil andere Kryptowährungen wertlos sind. Das zeigt deutlich, dass sie Bitcoin und Kryptowährungen nicht auseinanderhalten können.

Fangen wir von vorne an.

Das Konzept der Blockchain als verteiltes Datenbankmanagementsystem wurde erstmals 2008 von einer Person/Personengruppe unter dem Pseudonym Satoshi Nakamoto im White Paper zu Bitcoin beschrieben.

Die ersten Grundlagen zur kryptografisch abgesicherten Verkettung einzelner Blöcke wurden aber schon 1991 von Stuart Haber beschrieben. Bitcoin, die erste und einzige echte Kryptowährung, hat die längste Erfolgsbilanz und die größte Sicherheit. Sie hat in ihrem ersten Jahrzehnt einen bemerkenswerten Aufschwung erlebt und unterscheidet sich grundlegend von allen anderen Kryptowährungen.

Bitcoin, die erste und einzige echte Kryptowährung, hat die längste Erfolgsbilanz und die größte Sicherheit. Sie hat in ihrem ersten Jahrzehnt einen bemerkenswerten Aufschwung erlebt und unterscheidet sich grundlegend von allen anderen

Kryptowährungen. Sie hat in ihrem ersten Jahrzehnt einen bemerkenswerten Aufschwung erlebt und unterscheidet sich grundlegend von allen anderen Kryptowährungen.

Auch wenn Kryptowährung generell als dezentral gelten, ist außer Bitcoin keine wirklich dezentral. Anders als bei Bitcoin, gibt es bei allen anderen Kryptowährungen ein Gründerteam und Geschäftsführung, die Entscheidungen treffen und zum Beispiel bestimmen, ob beliebig mehr oder weniger von einer Kryptowährung in Umlauf gebracht. Es ist also eigentlich ein Unternehmen, das digitale Währungen anbietet und in Theorie so viel Angebot wie sie wollen bereitstellen könnten. Das hat große Ähnlichkeiten zu dem bestehendem Finanz-System, in dem bei Krisen, für eine kurzfristige Besserung, Geld aus dem Nichts in Umlauf gebracht wird.

Längerfristig reduziert monetäre Inflation aber den Wert von Geld. Die monetäre Inflation ist für die meisten Menschen nicht erkennbar und wird erst durch die preisliche Inflation spürbar. So wie Zentralbanken mehr Geld innerhalb des Fiat Geldsystems in Umlauf bringen, so agieren auch Entscheider an der Spitze der “Kryptounternehmen”.

Das hat große Ähnlichkeiten zu dem Fiat-System,

Bei Bitcoin ist die maximale Anzahl von BTC festgelegt und im Code fest verankert. Die Blockchain ist das Register des Bitcoin-Netzwerks, dass den Verlauf bestätigter Transaktionen speichert. Der Akt des Mining eines Blocks ist die Suche (durch Raten) nach einer Kombination bedeutungsloser Daten (die in den Block aufgenommen werden sollen), um eine schwierige mathematische Herausforderung zu lösen, die das Bitcoin-Protokoll stellt. Wenn das Problem gelöst ist, wird der Block (Transaktionen + bedeutungslose Daten) gültig und an die Spitze der Blockchain hinzugefügt. Wenn ein Miner erfolgreich ist, erhält er eine Belohnung für seine Bemühungen in Form von neuen BTC und Transaktionsgebühren.

Im Durchschnitt findet ein Miner alle 10 Minuten die Lösung und erhält dann BTC als Belohnung. Der Algorithmus, der beim BTC Mining verwendet wird heißt: Proof-of-Work. Miner müssen Arbeit leisten und werden dafür belohnt. So wird auch Konsens im Bitcoin Netzwerk ohne eine zentrale Autorität erreicht. Wenn ein Miner einen gültigen Transaktionsblock erfolgreich bestätigt hat, kann jeder im Netzwerk davon ausgehen, dass die anderen ihn als wahr akzeptieren. Dies ermöglicht es allen, zu einem Konsens zu gelangen, ohne sich auf eine vertrauenswürdige dritte Partei verlassen zu müssen. So kann das Bitcoin-Netzwerk ohne zentrale Autorität oder Vertrauen funktionieren. Die Regel, der Nachricht mit der größten Arbeit zu vertrauen, kann nicht geändert werden und ist im Bitcoin-Protokoll eingebettet (Wankum L.,2022) .

Bei der Entwicklung von Bitcoin legte Satoshi Nakamoto nicht nur die maximale Anzahl der verfügbaren BTC auf 21.000.000 fest, sondern auch wann diese herausgegeben werden. Bei der Einführung von Bitcoin im Jahr 2009 waren es 50 BTC die alle 10 Minuten als Belohnung herausgegeben wurde. Diese Anzahl halbiert sich alle 4 Jahre („Halving“), bis es dann im Jahr 2140 keine neuen BTC mehr gibt. Das erste „Halving“ fand im Jahr 2012 statt. Damals halbierte sich die Anzahl der BTC die im Durchschnitt alle 10 Minuten geschürft werden können, von 50 auf 25. Das zweite Halving fand 2016 statt (25 zu 12,5 BTC). Das dritte „Halving“ fand 2020 statt (12,5 zu 6.25 BTC). Insgesamt werden momentan 900 BTC pro Tag gemined. Alle 10 Minuten 6.5 = 900 in 24 Stunden. Voraussichtlich ab Sommer 2024 sind es dann nur noch 3.25, 2028 (1.625) bis es dann im Jahr 2140 keine mehr gibt. Das nächste Halving wird, basierend auf der 10-minütigen Blockzeit des Bitcoin-Protokolls errechnet. Alle 210.000 Blocks halbiert sich die Block Belohnung. Aufgrund des Halvings steigt der BTC Preis in etwa alle 4 Jahre. Weniger Angebot und gleichbleibende oder steigende Nachfrage bedeutet, dass der Preis steigt.

Die meisten anderen Kryptowährungen, allen voran Ethereum,

nutzen den Proof-of-Stake Mechanismus. Proof-of-Stake-Netzwerke sichern sich durch Validatoren ab, die per Zufallsverfahren zum Signieren neuer Blöcke ausgewählt werden. Doch, je nach hinterlegtem Kapital (Stake) erhöhen sich die Chancen, dieses Los zu ziehen. Arbeiten Validatoren sauber, erhalten sie nicht nur Transaktionsgebühren, sondern erhöhen auch ihre Reputation im Netzwerk und damit die Wahrscheinlichkeit, weitere Blöcke zu signieren. Bei versuchtem Missbrauch werden sie hingegen vom Algorithmus abgestraft und vom Netzwerk ausgeschlossen. Validatoren setzen somit ihren Stake aufs Spiel.

Das in Netzwerk, in dem ein paar Hände voll Nodes darüber entscheiden, welche Transaktionen durchgehen und ob alle Kontostände korrekt sind, führt den Gedanken von dezentralem Geld ad absurdum. Je größer das Krypto-Vermögen, das man zum Staking entbehren kann, desto größer die Chance, einen Block zu produzieren und den Staking Reward einzustreichen. So konzentriert sich die Macht im Netzwerk auf immer weniger Player.

Validator Nodes können aber auch durch Solo Staking, Staking-as-a-Service, Pooled Staking oder zentralisierte Börsen betrieben werden. Ein ETH-Validator-Node nimmt am Konsens teil und generieren wertvolle ETH-Einsatzprämien. Es ist aber sehr kostenaufwendig für eine Einzelperson, da Validatoren 32 ETH (oder ein Vielfaches von 32 ETH) einsetzen müssen. 32 ETH sind heute 36746,12 Euro. Resultierend daraus und den hohen Kosten für Ethereum Validations Hardware, ist es sehr schwer für den Otto Normalverbraucher eine Node zu betreiben. Es gibt nicht so viele Nodes im Netzwerk, was dadurch weniger dezentralisiert ist. Bei Bitcoin wiederum ist es sehr viel einfacher und günstiger eine Node im Netzwerk zu betreiben. Dies trägt zur Dezentralisierung und des Netzwerks bei. Das Mining ist bei Bitcoin von der Validierung von Transaktionen getrennt, weswegen es einfacher ist eine Bitcoin Node zu betreiben.

Das nächste Halving steht, basierend auf der 10-minütigen Blockzeit des Bitcoin-Protokolls am 4.5.2024 an.

Ziel von Bitcoin war es, ein dezentrales Geld und Zahlungsnetzwerk zu schaffen, dass, im Gegensatz zum bestehenden Finanzsystem ein größeres Maß an Transparenz und Fairness bietet. Sein(e) Schöpfer zielten darauf ab, den Menschen Souveränität über Finanzen zu ermöglichen, anstatt einer zentralen Autorität – wie einer Bank – die Kontrolle zu geben/vertrauen zu müssen. Alle Kryptowährungen, die nach Bitcoin kamen, machen den Anschein, als würden Sie den Menschen Macht geben, was letztendlich aber ein Trugschluss ist, weil sie oft stärker zentralisiert als das bestehende Finanzsystem sind.

Wie unterschiedlich Bitcoin und Krypto sind, zeigt sich auch in der Art und Weise, wie Behörden Bitcoin und andere Kryptowährungen betrachten. Gary Gensler, Vorsitzender der SEC (U.S. Finanzaufsicht) zum Beispiel, betrachtet Bitcoin als digitalen Rohstoff und die „große Mehrheit“ der Krypto-Token als unregistrierte Wertpapiere. Als Grundlage hierfür bezieht er sich auf den Howey Test. Dies macht jedoch deutlich, wie sich Bitcoin von anderen Kryptowährungen unterscheidet, aber eine finale Entscheidung zu der Regulierung von Kryptowährungen steht noch nicht fest.

Natürlich gibt es auch Gemeinsamkeiten zwischen Bitcoin und Kryptowährungen. Primär die Nutzung einer Blockchain als dezentralisierte Datenbankmanagementsystem zum Aufzeichnen von Transaktionen, aber es kommt kein anderes Projekt außer Bitcoin ohne CEO, Gründer und zentraler Autorität aus, die alleinig Entscheidungen treffen. Insbesondere Ethereum ist in der Vergangenheit negativ aufgefallen, weil die Regeln des Projekts am ständig von den Gründern, allen voran Vitalik Buterin, verändert werden.

Satoschi Nakamoto verschwand vor 12 Jahren, am 13. Dezember 2010, von der Bildfläche. Das war das Klügste, was er/sie

hätte tun können. Seitdem existiert Bitcoin unabhängig, ohne der Kontrolle einer zentralen Autorität zu unterliegen. Das ist die Innovation. Alle anderen Krypto-Projekte sind ein Rückschritt und werden langfristig nicht mit Bitcoin konkurrieren können, da sie von einem CEO, Vorstand oder einer anderen zentralisierten Einheit kontrolliert werden.

Strenggenommen schaffen Kryptowährungen ein Problem, das Bitcoin schon gelöst hat. Vor Bitcoin gab es unzählige Unternehmen, die digitales Privatgeld herausgaben. Ecash von David Chaum zum Beispiel. Das Problem dabei ist, dass jede zentral herausgegebene Währung bisher gescheitert ist. Bitcoin auf der anderen Seite wird höchstwahrscheinlich erfolgreich sein, weil es nicht von einem Unternehmen oder Organisation kontrolliert wird und es von Menschen für Menschen erschaffen wurde. Bei allen Kryptowährungen außer BTC handelt es sich schlussendlich um spekulative Vermögenswerte, in die man kurz- bis mittelfristig investieren kann, um finanzielle Gewinne zu erzielen, aber nicht um langfristig Werte zu speichern. Der Kauf von BTC hingegen ist die Entscheidung, Kaufkraft in einem soliden und digitalen Geld zu sichern und zu sparen, um es langfristig vor der Inflation zu schützen (Wankum, L 2022).

„Bitcoin ist die Entdeckung der digitalen Knappheit“ (Gigi, 2022). Regierungen und Geld hängen schon lange unerfolgreich zusammen und Bitcoin löst dieses Problem. Es ist schafft unabhängiges digitales Geld, dessen Wert nicht durch die Abhängigkeit von einer zentralen Organisation geschmälert werden kann.