

Bitcoins & Co.

Wie Blockchain und Kryptowährungen die Welt verändern (Teil 1)

Seit dem 03.01.2009 um 18:15 Uhr (Weltzeit) gibt es eine Technologie, welche die Welt grundlegend verändern wird – die „Blockchain-Technologie“. Sie wurde zusammen mit der Kryptowährung Bitcoin gestartet. Wer glaubt, Blockchain wurde nur erfunden, um Bitcoins für Nerds zu erzeugen, liegt falsch. Es wurde damit eine technische Revolution ausgelöst, die nicht mehr aufzuhalten ist.



Quelle: H. Leidenroth

1 Bitcoin-Akzeptanzstelle

Autor

Dipl.-Ing. (FH) Hannes Leidenroth,
LeiTech GbR, Sandkrug, unterstützt
von Co-Autor Dipl.-Ing. (FH) Thomas
Imhoff.

Bereits heute können Unternehmer ihren Kunden die Zahlungsoption anbieten „Bitcoin accepted here“ (Bild 1). Laut der Postbank-Digitalstudie 2018 hält etwa jeder dritte Deutsche Kryptowährungen für eine interessante Geldanlage, trotz der hohen Kursschwankungen. Bei den unter 35-jährigen ist es sogar fast jeder Zweite. Diese Beitragsreihe soll grundlegende Informationen und praktische Hinweise zum Thema liefern, wobei auch die Fallstricke nicht zu kurz kommen sollen.

Prämissen des Autors

Der Autor findet das Thema so spannend, dass es unbedingt auch den ep-Leser errei-



2 Symbolischer ep-Bitcoin

Quelle: A. Purwin

chen soll. Er gibt dabei aber folgendes zu bedenken:

1. Das Thema kann nur aus seiner rein subjektiven Sicht beschrieben werden. Neutrale Formulierungen würden eine Allgemeingültigkeit vortäuschen, die nicht existiert und für die „er oft keine Beweise vorlegen könnte“.
2. Für im Beitrag genannte praktische Lösungsvorschläge gibt es stets zahlreiche

GIRA



Gira E2 Schwarz matt, die neue Oberfläche.

Bestechende Optik, ganz einfach montiert. Das bewährte Schalterprogramm Gira E2 wurde jetzt um eine neue trendige Oberfläche erweitert: Schwarz matt. Diese Schalter-Variante passt nicht nur in jedes gehobene Interieur, sondern ist auch besonders flexibel zu installieren. Mit dem Gira System 55 in standardmäßigen Unterputz- oder Hohlwanddosen oder den Gira Gerätedosen bzw. Unterputzdosen. Weitere Informationen: www.gira.de/e2

Alternativen. Daher sind die Vorschläge als Beispiele von vielen zu verstehen.

- Es gibt über 1 000 verschiedene Kryptowährungen. Bitcoin BTC ist daher nur eine unter vielen – und es ist völlig offen, welche Coins sich durchsetzen werden.

Dennoch startet dieser Beitrag mit der Mutter aller Kryptowährungen – dem Bitcoin BTC (Bild 2), denn das Prinzip lässt sich an diesem Beispiel gut erklären. Später werden auch andere Coins vorgestellt, es wird auf Wallets (sichere Aufbewahrung) eingegangen und ebenso auf die Themen Steuern und Regulierung. Erscheinen plötzlich keine weiteren ep-Folgebeiträge, ist die Krypto-Blase geplatzt. Das wird aber nicht passieren.

Weg zum ersten Bitcoin oder Teilen davon

Dazu sind nur wenige Schritte notwendig:

- Man kann bei der Münchner Fidor-Bank ein Online-Konto anlegen, was etwas Zeit erfordert, inklusive dem Postident-Verfahren. Dafür gibt es aber auch schon passende Apps, sodass die Kontoeröffnung in 10 min zu schaffen ist.
- Dann eröffnet man beim größten europäischen Onlinemarktplatz „bitcoin.de“ ein eigenes Account und stimmt dem dort vorgeschlagenen „Express-Handel“ mit der Fidor-Bank zu. Das ist sozusagen ein heißer Draht zwischen Onlinehändler und einer echten Bank. Somit gestaltet sich der Authentifizierungsvorgang bei **bitcoin.de** sehr kurz und schmerzlos, denn die Daten von Fidor werden praktisch übernommen.
- Dann zahlt man z. B. 6 600 Euro auf sein Fidor-Konto ein und kann sich anschließend über bitcoin.de den ersten Bitcoin von einer anderen Privatperson kaufen (Stand per

23.05.2018 um 17:50 Uhr); oder man erwirbt für den Anfang nur 0,01 Bitcoin.

- Datenpflege: Zugangsdaten, Passwörter usw. sind absolut sicher zu notieren.
- Wichtig:** Zurzeit gelten solche Investitionen als „hochspekulativ“. Deshalb ist es sinnvoll, zu Testzwecken nur mit kleinen Beträgen zu üben.

Ist das geschafft, entsteht die Frage nach dem praktischen Nutzen von Bitcoins im täglichen Geschäftsleben. U. a. nutzt der Autor heute schon die Möglichkeit, mit Bitcoins seine Strom- und Gasrechnung zu bezahlen. Enercity in Hannover bietet das bereits an.

Kryptowelt trifft klassisches Bankenwesen

Die Partnerschaft zwischen der Fidor-Bank und bitcoin.de feierte gerade ihr fünfjähriges Bestehen. Im Jahr 2013 war es eine Sensation, als die weltweit erste „Direktverbindung“ zwischen der klassischen Bankenwelt und der Kryptowelt entstand. Verkauft man zum Beispiel Bitcoin (BTC) über den Handelsplatz bitcoin.de, wird durch den automatischen Express-Handel zwischen den beiden Institutionen der Erlös sofort in Euro dem normalen Fidor-Konto gutgeschrieben; also dort, wo noch die staatliche Einlagensicherung herrscht. Beim Express-Handel fallen Markplatzgebühren von 0,8 % an.

In Zukunft soll es weitere einfache Handelswerkzeuge geben. Beispielsweise startet die Stuttgarter Börse ab dem Herbst 2018 das Projekt „Bison-App“ (gebührenfrei), was man durchaus im Auge behalten sollte. Die zweitgrößte deutsche Finanzbörse wagt den Kontakt zur Kryptowelt. Außerdem gibt es laut Bafin schon sechs deutsche Banken, die ebenfalls mit Kryptowährungen handeln.

Irren ist menschlich

In den typischen Online-Medien liest man täglich Statements zum Thema Kryptowährungen – aktuell beispielsweise von Warren Buffett: „Bitcoin ist Rattengift zum Quadrat“. Daher lohnt ein Blick in die Geschichte [2], insbesondere hinsichtlich der Auffassungen und Aussagen berühmter Persönlichkeiten:

- 1876 Henry Preece** (Elektroingenieur, British General Post Office): „Die Amerikaner mögen eine Verwendung für das Telefon haben, wir aber nicht. Wir haben viele Kuriere.“
- 1889 Thomas Edison:** „Mit Wechselstrom herumzuspielen, ist Zeitverschwendung. Niemand wird dies jemals nutzen.“
- 1966 Time Magazine:** „Obwohl technisch machbar, wird Shopping von Zuhause floppen.“
- 2007 Steve Balmer** (bis 2014 CEO von Microsoft): „Das iPhone wird niemals einen signifikanten Marktanteil erlangen.“

Zurück zu Warren Buffett, der nur in Dinge investiert, „die er versteht“. Das ist ja auch gut und richtig. Mit 87 Jahren muss man Blockchain auch nicht mehr verstehen, aber dann sollte man sich in seiner Position mit solchen öffentlichen Äußerungen auch entsprechend zurückhalten.

Auch Bill Gates rudert inzwischen etwas zurück – im Gegenteil: Sein lobenswertes Projekt der „Bill & Melinda Gates Foundation“ basiert sogar selbst auf einer Art Krypto (Ripple), siehe <http://mojaloop.io/>.

Idee von Währungs-Alternativen

Als Vertreter der Wiener Schule für Volkswirtschaft hatte Friedrich August von Hayek im Jahr 1975 in London einen Vorschlag unterbreitet – und dafür den Nobelpreis kassiert [3]. Im Jahr 1976 erschien sein Buch „Entnationalisierung des Geldes“. Er zeigt darin in aller Klarheit die großen Schwächen und Gefahren des staatlichen Geldmonopols sowie dessen Folgen und beschreibt eine alternative Lösung. Das Dumme war nur, dass ihm damals die technischen Mittel zur Umsetzung fehlten.

World Wide Web bietet nötige Infrastruktur

Sein Problem ist mittlerweile gelöst, es gibt das Internet, was die erforderliche Infrastruktur bietet. Staaten wie Argentinien, Zypern oder Venezuela kennen Hyperinflation und eine Übernacht-Enteignung. Zu Beginn des Jahres 2013 verloren die Zyprer plötzlich ihre gesamten Ersparnisse. 2015 durften die

Häufig verwendete Begriffe und hilfreiche Links zum Thema

Begriffe

- Nocoiner:** Jemand, der keine Coins hat (Schimpfwort)
- BTC:** Offizielles Bitcoin-Kürzel
- FIAT-Geld:** Übliche staatliche Währungen, z. B. in Euro oder US-Dollar (USD)
- Open-Source-Software:** Sie gehört der Allgemeinheit (keinem Konzern)
- Blockchain:** Dezentrale, verschlüsselte Datenbank
- Mining:** (Gold) Schürfen, neue Datenblocks freigeben.

Links

- www.bitcoin.de
- www.btc-echo.de
- www.coinmarketcap.com
- www.blockchain.info
- www.bitcoinblog.de
- www.bisonapp.de
- www.coin-hero.de
- www.coinspondent.de
- www.coincierge.de
- www.kryptoszene.de

Griechen zeitweise nur 60 Euro/Tag abheben. Dort haben Staaten und Notenbanken versagt. Dort stehen die Menschen Kryptowährungen – als alternativen Hafen – sehr offen gegenüber.

Schulden machen, das ist im Bitcoin-System übrigens nicht möglich. Wer über kein Guthaben verfügt, kann keine Transaktionen/Zahlungen ausführen – so einfach ist das. Kryptowährungen müssen sich auf dem freien Markt durchsetzen, staatliches Geld muss das nicht.

Vier Probleme waren zu knacken

Es gab unzählige Versuche, E-Cash auf digitalem Wege ins Leben zu rufen, aber alle scheiterten an vier Problemen:

- Double-spending:** Was könnte der PC gut ausführen? Digitales Geld kopieren, sodass man es häufiger ausgeben kann.
- Wo** wird der **zentrale Computer** aufgestellt, der das digitale weltweite Geld hauptverantwortlich verwalten soll? Unter den Schweizer Alpen – schwer bewacht, atom-bombensicher?
- Wem gehört** die **Software**, die das digitale Geld verwaltet?

d) Wie kann man das System absolut **sicher vor Hackerangriffen** machen?

Erfinder der Kryptowährung

Das ist Satoshi Nakamoto – doch seine/ihre Identität ist bis heute nicht bekannt. Selbst wenn sie jemand kennen sollte (z. B. die NSA), gibt es kein Interesse, diese öffentlich zu machen.

„Er“ hat in den Jahren 2008/2009 nur mittels Mail und Foren mit beteiligten Informatikern zusammengearbeitet. Warum er diese Anonymität gewählt hat, weiß letztendlich niemand. Eventuell wollte er nicht gleich „mitverhaftet“ werden, falls der Bitcoin ausschließlich für kriminelle Zwecke zum Einsatz kommen würde. Studien zufolge sind das maximal 10 %. Damit muss man leben, auch mit dem Darknet. Trotzdem ist niemand gezwungen, das Darknet zu verwenden.

Open-Source-Software für jedermann

Am 31.10.2008 veröffentlichte Satoshi sein Whitepaper – also sein Konzept für die Block-

chain-Technologie und den Bitcoin. Seine Software ist ein Open-Source-Produkt, jeder kann die Software analysieren und verwenden. Somit ist der **Punkt c)** gelöst: Die Software ist für alle Menschen nutzbar.

Bereits andere Open-Source-Produkte sind weltweit extrem erfolgreich: Sämtliche Internetserver basieren zum Beispiel auf dem Betriebssystem Linux. Der Browser Firefox ist beispielsweise auch ein Produkt, was alle Internetuser nutzen können.

Am 3. Januar 2009 startete Satoshi Nakamoto „seine“ Software mit dem sogenannten ersten Datenblock, dem „Genesis-Block“. Dort verewigte er den aktuellen Titel der Londoner Times – sinngemäß: „Schatzkanzler steht kurz vor zweiter Bankenrettung“.

Eine Botschaft an alle: Diese Zeiten werden für den Steuerzahler bald vorbei sein.

Bitcoin-Handel erstmals dokumentiert

Und dann gibt es noch ein legendäres Datum: Am **21.05.2010** hatte der Programmierer Laszlo Hanyecz für 10 000 Bitcoins zwei Pizzas gekauft – der erste dokumentierte Bitcoin-Handel. Ein neues Zeitalter

WILLKOMMEN ZUHAUSE

Wenn nach Hause kommen immer ein gutes Gefühl ist – Einfach **WISER™**.

schneider-electric.de/wiser



Connected
Technology
for Homes



Life Is On

Schneider
Electric

war angebrochen. Satoshi Nakamoto wurde auch für den Nobelpreis vorgeschlagen, aber leider ist das für anonyme Personen nicht möglich.

Größtes weltweites Vertrauensnetzwerk

Satoshi Nakamoto hat das weltweit größte Vertrauensnetzwerk geschaffen, das ohne Mittelsmänner funktioniert:

<https://bitnodes.earn.com/nodes/network-map/>

Vision: Open-Source und Transparenz

Seine Vision war, dass Menschen in Zukunft lieber neutralen, nicht korrumpierbaren Open-Source-Algorithmen vertrauen, statt Politikern, Notenbanken, zentralen Katastern oder Tresoren unter den Schweizer Alpen.

Die Deutschen haben zwar noch wenig Vertrauen zu Algorithmen, sie hängen zu sehr am Bargeld – aber das ist ihr spezifisches Problem – die Welt wartet nicht auf sie.

In der Schweiz gibt es Bitcoin-Automaten am Hauptbahnhof, in Deutschland keinen einzigen, da die Bafin das nicht genehmigt. Das muss aber niemanden ärgern, denn Automaten sind auch noch Relikte der Vergangenheit, denn eine Handy-App reicht.

Satoshi hat eine digitale, rein virtuelle Währung entwickelt, indem er viele bereits bewährte Open-Source-Softwareprodukte geschickt kombinierte und zusätzlich die o. g. Hauptprobleme lösen konnte. Dabei hat er sich konsequent am Edelmetall Gold orientiert. Was dort über Jahrtausende gut funktioniert hat, muss auch in der digitalen Welt funktionieren, so die Annahme. Und nach zehn Jahren weiß man jetzt: Es funktioniert.

Dezentralität – Stärke des Systems

Wie Blockchain funktioniert

Anhand des folgenden stark vereinfachten Beispiels soll das Prinzip der Blockchain-Technik verdeutlicht werden:

Annahme. Es wurde ein neuer Verein mit fünf Mitgliedern gegründet. Ein Kassenswart notiert alle Einnahmen und Ausgaben, damit der jährliche Ausflug finanziert werden kann. Falls jemand den Rasen mäht oder sich irgendwie einbringt, erhält er auch mal Geld aus der Kasse zurück. Aber die Geldbeträge

werden lediglich notiert, erst einmal nicht tatsächlich gezahlt, um es einfach zu halten und Wechselgeldprobleme zu vermeiden. Warum soll heute jemand 10 Euro einzahlen, wenn er morgen Rasen mäht und schon wieder 10 Euro der Kasse entnimmt. Erst am Jahresende wird festgestellt, wer noch Guthaben hat oder noch etwas einzahlen muss.

Problem. Der Kassenswart ist unzuverlässig, die Buchführung ist immer falsch.

Lösung. Satoshi hatte die Idee, das Kassensbuch (Blockchain-Datenbank) auf alle fünf Leute (weltweite Knotenrechner im Netzwerk) zu verteilen. Jeder Zahlvorgang (Transaktion) wurde sofort per E-Mail an alle fünf Partner gemeldet und jeder notierte sich diesen Vorgang im eigenen Kassensbuch. Einmal pro Tag (beim Bitcoin: etwa alle 10 min) gab es eine Telefonkonferenz, in der alle Buchungen verglichen wurden (Konsens herstellen). Somit verfügten alle Leute (Knotenrechner) stets über ein aktuelles Kassensbuch. Ginge ein Kassensbuch versehentlich verloren, wäre das kein Problem für das Netzwerk, denn es existieren ja noch vier korrekte Exemplare.

Somit hat Satoshi auch **Hürde b)** überwunden: Ein zentraler Computer zur „Verwaltung des Kassensbuchs“ wird nicht benötigt und somit gibt es auch keinen Verantwortlichen dafür.

Diese Dezentralität ist die große Stärke des Systems. Eine stets aktuelle Datenbank, in tausendfacher Ausfertigung auf ebenso viele Knotenrechner weltweit verteilt, ist die geniale Innovation des Erfinders.

Blockchain – Verketteten von Datenblöcken

Jede Seite im Kassensbuch stellt einen Datenblock in der Datenbank dar. Ist die Seite mit Transaktionen gefüllt, wird eine Art fälschungssichere Checksumme („Hash“, dazu später) dieser Seite berechnet. Diese komplett gefüllte Seite wird für alle Zeiten „in Gießharz“ konserviert – im übertragenen Sinne. Exakt dieses Hash-Ergebnis wird auf

der nächsten neuen leeren Kassensbuchseite als Starteintrag (Übertrag) vermerkt. Somit besteht eine Art unveränderliche Verlinkung zwischen den Seiten. Die Datenblöcke werden also durch diesen Hash-Wert untereinander verkettet (chain), daher der Begriff Blockchain.

Was die Datenblöcke für Daten enthalten, wäre prinzipiell erst einmal egal – dazu später. Gedanklich wird hier zunächst von Geldbeträgen in Bitcoin ausgegangen.

Daten mithilfe Kryptographie absichern

Eine weitere Richtschnur für Satoshi war sein extremes Misstrauen gegenüber Hackerangriffen und Datenmanipulationen. Daher verwendet er eine unüberwindliche Verschlüsselungstechnik (Kryptographie) für die Blockchain. Auch hier hat er das Rad nicht komplett neu erfunden, sondern greift auf ausgereifte Open-Source-Produkte zurück.

Zum Beispiel wird beim Bitcoin der **Hash-SHA256-Verschlüsselungsalgorithmus** verwendet, der ursprünglich von der NSA entwickelt worden ist. Hintertürchen kann es trotzdem nicht geben, sonst wäre es keine Open-Source-Anwendung, für jedermann einsehbar. Aber was machen manche Medien daraus – der Schlagzeile wegen: „der Bitcoin kommt von der NSA“.

Neben dem Bitcoin gibt es noch über 1 000 andere Kryptowährungen, aber noch nie wurde eine Bitcoin-Blockchain gehackt. Gehackt werden Privatrechner, Online-Börsen und übrigens regelmäßig auch Banken und Unternehmen. Das darf aber eben nicht mit der Bitcoin-Blockchain verwechselt werden. Die Blockchain im klassischen Sinne gilt als nicht hackbar, sofern sie den höchsten Sicherheitsstandards genügt – Proof of Work PoW – wie beim Bitcoin BTC benutzt.

Allein diese Tatsache der extremen Sicherheit im IT-Bereich müsste auch den letzten Skeptiker aufrütteln. So etwas gab es noch nie. Somit ist auch der o. g. **Punkt d)** erfüllt.



3 Suche in der Blockchain

Quelle: H. Leidenroth

Problem: Double-Spending

Dann verbleibt noch **Punkt a)** das Double-Spending-Problem: Geld kopieren und mehrfach ausgeben. Auch dafür hat Satoshi eine Lösung gefunden, die hier aber nicht im Detail beschrieben werden soll.

Nur so viel: Werden Datenblöcke als „ungültig“ erkannt, werden diese nicht einfach gelöscht, sondern zusätzlich zur einzig gültigen und eindeutigen Blockchain gespeichert, damit jederzeit eine Nachvollziehbarkeit der Entstehungsgeschichte der Blockchain ermöglicht wird. Auch dieser Punkt ist eine geniale Lösung dieses Informatikers, an der sich andere vergeblich die Zähne ausgebissen haben. Allerdings lauert hier im Hintergrund noch eine Gefahr, die sogenannte 51 %-Attacke, – darauf wird später noch eingegangen.

Kassenbuch: transparent für jedermann

Und noch eine Sache ist durchaus erwähnenswert: Die Datenbank, das „Kassenbuch“, ist vollkommen transparent und für jedermann einsehbar, der einen normalen Browser bedienen kann, auch wenn die Einträge/Transaktionen in anonymer Form vorliegen.

Ausprobieren kann man es, indem man im Browser **blockchain.info** eingibt. Danach wird im Eingabefeld der Suche (Bild 3) die gezeigte Adresse eingegeben. Das ist sozusagen eine Art Kontonummer, der „öffentliche Schlüssel“ der Smartphone-App, um Bitcoin empfangen zu können.

Dorthin hatte der Autor selbst einmal eine kleine Summe überwiesen. Wie hoch diese war, kann jeder im öffentlichen Kassenbuch erkunden. Um es vorwegzunehmen: Abbuchen kann derjenige von dieser Adresse nicht. Jeder Neugierige sollte sich auch stets dessen bewusst sein: Wenn man als Dritter das weltweit größte „Kassenbuch“ öffnet und nachsieht, welchen Kontostand beispielsweise der Autor auf seiner Smartphone-App ausweist, dann bleibt diese Empfangsadresse bestehen. Hatten einige nicht einmal irgendwo gelesen: „Bitcoin sei etwas für Verbrecher“? Was glaubt der Leser: Welche Kriminellen verewigen sich freiwillig in solch einem transparenten System? Zu Übungszwecken könnte man aber durchaus kleine Summen überweisen und anschließend prüfen, ob die Transaktion erfolgreich war. Doch mit einer Tatsache muss man sich in diesem Fall ebenfalls abfinden:

Die Blockchain-Datenbank wird wohl die von Geheimdiensten am besten analysierte und gescannte Datenbank der Welt sein.

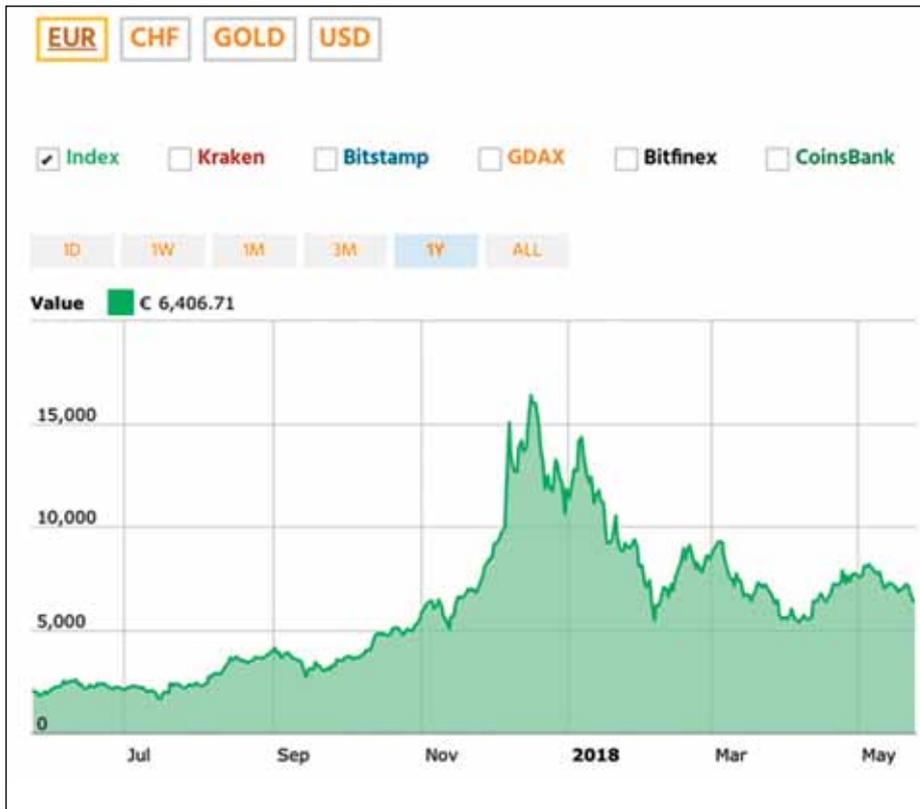


Zeitenwende: Aus top2 wird top3 Digitale Zeitschaltuhren top3

Die neuen digitalen Zeitschaltuhren top3 von Theben setzen den nächsten Meilenstein hinsichtlich Funktionsvielfalt, Programmierbarkeit und Energieeffizienz.

Erstellen Sie Ihre Programme komfortabel per App, speichern Sie sie in der Cloud oder versenden Sie sie per E-Mail. Übertragen Sie die Programme manipulationssicher via Bluetooth Low Energy OBELISK an die Uhr. Nutzen Sie vorhandenes top2-Zubehör und Programme einfach weiter. Für effizienteres Arbeiten und mehr Zeit fürs Wesentliche.





Quelle: BTC-echo.de

4 Kursverlauf des BTC eines Jahres in Euro

Bitcoin im Stresstest

Schaut man sich den zurückliegenden Kursverlauf des Bitcoin (BTC) an, ist der beispiellose Hype zur Jahreswende erkennbar, gefolgt von einem deutlichen Rückwärtsgang (Bild 4 – Kursverlauf BTC eines Jahres in Euro, Quelle: BTC-Echo.de). Dieser Hype war von größtem Nutzen. Durch den Massenansturm wurde die Technik bei allen Beteiligten aufs äußerste gefordert und förderte ohne Gnade alle Schwachstellen zutage, was normalerweise der Sinn eines (hier ungeplanten) Stresstests ist. Das läßt aber auch darauf schließen, welches Potential und welches öffentliche Interesse mittlerweile mobilisiert werden kann.

Allerdings kommt in diesem Chart des Bitcoin (Bild 4) nicht die ganze Wahrheit ans Licht. Es ist davon auszugehen, dass dieser Hype wahrscheinlich teilweise durch Kursmanipulationen künstlich unterstützt oder gefördert worden ist [1].

Doch der Hype hatte zudem eine wichtige psychologische Funktion, was am Ende dieser Beitragsserie gezeigt wird, selbst wenn die Blase vorläufig als geplatzt gilt.

Hinweis: Beim Begriff „Blase“ sollte man aber vorsichtig sein, denn beim Bitcoin ist es oft so, dass sich die Kurse nach einer sogenannten Blase auf einem höheren Niveau wiederfinden als davor.

Ein Blick zurück in die Vergangenheit

Auch beim Begriff „Blase“ lohnt ein Blick in die Vergangenheit. Als sich im Februar 2011 zwischen US-Dollar und Bitcoin ein Paritätszustand ergab (1 USD = 1 Bitcoin BTC), wurde von einer großen Blase gesprochen. Ein Bitcoin virtueller Währung könne niemals wertmäßig gleich einem realen Dollar sein. Hätte jemand in dem Augenblick behauptet, was sich später bewahrheiten sollte (1 BTC = 20 000 US-Dollar), wäre derjenige für verrückt erklärt worden. Irgendwie muss man dann doch wieder an

Warren denken. Eine Schätzung des Weltwirtschaftsforums geht davon aus, dass im Jahr 2025 etwa 10 % des weltweiten Bruttoinlandsprodukts in Blockchain(s) gespeichert sein wird. Das entspräche einer Marktkapitalisierung von 10 Billionen US-Dollar. Sollte sich das als real erweisen, könnte 1 BTC = 288 000 USD wert sein. Aber es gibt eben nicht nur den Bitcoin, sondern noch viele ernstzunehmende „Coin-Konkurrenten“, dazu später.

Konsequenzen für die Beteiligten

Nach dem Stresstest mussten also alle Beteiligten ihre Hausaufgaben machen:

- Die Bitcoin-Entwickler sahen mit Schrecken einen riesigen Datenstau entstehen, weil nur maximal 7 Transaktionen pro Sekunde abgewickelt werden konnten. Manche Überweisungen dauerten viele Stunden, wenn nicht sogar mehr. Zum Vergleich: Bei Visa & Co. sind 47 000 Überweisungen pro Sekunde möglich. Wer eine schnellere Bearbeitung wünschte, musste hohe Gebühren zahlen. Man sagt, die „Skalierbarkeit“ des Systems sei nicht gegeben. Das System konnte nicht passend reagieren – von einem dahindümpelnden Zustand bis zum Mega-Ansturm.
- Als Reaktion darauf wird das sogenannte Lightning-Netzwerk entwickelt, was den Bitcoin im Prinzip wieder flotter, preiswerter (Gebühren) und flexibler nutzbar machen soll.
- Auch die Chip- und Hardwarehersteller konnten die Nachfrage nach speziellen Knotenrechnern nicht mehr erfüllen.
- Die Online-Händler (Börsen) kamen bei dem Ansturm in große Bedrängnis, die Server waren überlastet und die Datensicherheit blieb bei manchen auf der Strecke.

In den vergangenen Monaten wurde also ordentlich nachgerüstet, sodass man für eine neue, nachhaltigere Nachfrage hoffentlich gut gerüstet sein sollte.

Literatur

- [1] John M. Griffin and Amin Shams (University of Texas at Austin): Is Bitcoin Really Un-Tethered? Quelle: papers.ssrn.com.
- [2] Dr. Torsten Langner: Und es wurde Krypto.
- [3] Aaron Koenig: BITCOIN Geld ohne Staat.
- [4] Saifedean Ammous: The Bitcoin Standard.
- [5] Christoph Bergmann: „Bitcoin – die verrückte Geschichte vom Aufstieg eines neuen Geldes“, Moby-Verlag. ■

Anzeige