Martin Leinweber
Jörg Willig

Asset-Allokation mit Kryptoassets

Das Handbuch

WILEY

WILEY-VCH GmbH

Inhalt

2 Der Bitcoin – eine kurze Historie

»Breeding homing pigeons that could cover a given space with ever increasing rapidity did not give us the laws of telegraphy, nor did breeding faster horses bring us the steam locomotive.«
Edward J. v. K. Menge, 1930

Das Jahr 2009 hielt einen reichen Fundus an guten und weniger guten Nachrichten für die Menschheit bereit. In Sri Lanka endete der 25 Jahre lang andauernde Bürgerkrieg, die Schweinegrippe wurde von der WHO zu einer globalen Pandemie erklärt und Politiker in Zimbabwe nahmen mit dem mittlerweile dritten Zimbabwe-Dollar einen erneuten Anlauf zur Eindämmung der Hyperinflation. Außerdem beendete Tiger Woods seine Karriere als Profigolfer, der Autor Terry Pratchett wurde von der Queen geadelt und Uri Geller erwarb eine unbewohnte Insel, weil er Gerüchten zufolge dort einen ägyptischen Schatz vermutete. Auf globaler Ebene wurde Christiano Ronaldo für seine Leistungen im Vorjahr zum Weltfußballer gekürt, die Slowakei führte den Euro ein und die Volksrepublik China machte das Hanyu Pinyin zur offiziellen latinisierten Umschrift der chinesischen Sprache.

Die meisten dieser Geschehnisse sind nach einem kurzen Aufflackern im obligatorischen Jahresrückblick rasch in Vergessenheit geraten. Ein Ereignis, das bis heute nachwirkt, hat es seinerzeit gar nicht erst in eine Rückblende geschafft. Am 3. Januar 2009 startete ein unbekannter Entwickler das Bitcoin-Netzwerk.

Das Jahr 2009 war das zweite Jahr der größten Finanzmarktkrise der vergangenen 100 Jahre. Während auch tiefgreifende Krisen an den Börsen und Kreditmärkten nichts Ungewöhnliches sind, stellt das Ausmaß der im Zuge der Entwicklungen der Jahre 2008 und 2009 durchgesetzten Eingriffe in den Kapitalmarkt eine Zäsur dar.[1] Seither stehen die Finanzmärkte unter dem Einfluss immer umfangreicherer Aktionen von Notenbanken, die an vielen Stellen die Mechanismen der freien Preisfindung ausgehebelt haben. Die einsetzende Gewöhnung der Marktteilnehmer an Zinssenkungen und regelmäßig aufgestockte Ankaufprogramme für Anleihen und Kreditverbriefungen, sobald das ökonomische Fahrwasser unruhiger wird, führte zu einem völlig verschobenen Anreizsystem. Ergänzend führen die niedrigen und teils negativen Zinssätze die klassischen Bewertungsansätze des Kapitalmarktes an ihre Grenzen. Die Resultate von Methoden, die seit Dekaden selbstverständlich genutzt wurden, sind nun oft kaum mehr anwendbar oder sogar irreführend und damit nicht nur nutzlos, sondern gefährlich.

Nahezu sämtliche Ventile, durch die sich der von Zeit zu Zeit entstehende Druck an den Finanzmärkten entladen konnte, wurden sukzessive geschlossen. Als finaler Druckbegrenzer verbleibt der größte aller Märkte, der globale Währungsmarkt mit

1 Siehe McDonald/Robinson (2009).

einem täglichen Handelsvolumen von mehr als 6,5 Billionen US-Dollar.[2] Auch in diesem Segment nutzen Zentralbanken seit jeher ihren Spielraum, Kursbewegungen zu beeinflussen, mal mit mehr und mal mit weniger Erfolg. Zwar erscheint der Einfluss der Zentralbanken kurzfristig oft übermächtig, doch den wichtigsten Faktor können auch diese Institutionen nur bis zu einem gewissen Grad beeinflussen: das Vertrauen der Menschen in eine Währung. Schwindet dieses Vertrauen, dann beginnen die Menschen, sich nach möglichen Alternativen umzuschauen.

Seit dem Beginn der Finanzkrise hat das Vertrauen in die globalen Finanzinstitutionen großen Schaden genommen. Die anhaltenden Markteingriffe der Zentralbanken und die ins Surreale abdriftenden eingesetzten Geldbeträge untergraben langsam aber stetig den Glauben der Menschen an die langfristige Stabilität vieler Währungen und greifen so das Fundament des globalen Finanzsystems an.[3] So wurde in den vergangenen Jahren der Boden für die Akzeptanz möglicher Alternativen bereitet. Was fehlte, war die Ausweichmöglichkeit. Mit dem Start des Bitcoin-Netzwerkes und der Entstehung einer neuen Assetklasse begann die Entwicklung einer möglichen Alternative. Bevor das erste Kryptoasset das Licht der Welt erblicken konnte, mussten jedoch einige Giganten ihre Arbeit erledigen, auf deren Schultern der Entwickler des Bitcoin später steigen sollte.

Von der Tankkarte zum Trustless Payment System

Neben allen technischen Problemen, die es auf dem langen Weg hin zur Einführung eines funktionierenden, dezentralen Zahlungssystems zu überwinden galt, mussten auch die Menschen vom Nutzen digitaler Zahlungsmittel in der Praxis überzeugt werden. Auch der bargeldlose Zahlungsverkehr hatte zu Beginn mit viel Skepsis zu kämpfen.

Ein frühes Beispiel für den sinnvollen Einsatz bargeldlosen Zahlungsverkehrs lieferten in den 1980er-Jahren einige Tankstellenbesitzer in den Niederlanden. Zahlreiche Überfälle, bei denen das Bargeld geraubt wurde, führten zur Schaffung eines bargeldlosen Zahlungssystems. Die Eigner der Tankstellen wollten zum einen das finanzielle Risiko, aber auch die persönlichen Gefahren reduzieren und führten die Kartenzahlung ein. Die Kunden nahmen das System an und konnten an den teilnehmenden Tankstellen fortan per Karte bargeldlos bezahlen. Was heute selbstverständlich klingt, war seinerzeit ein bemerkenswerter Schritt.

Während die Kartenzahlung noch greifbar ist, existieren virtuelle Währungen nur noch innerhalb von Rechnern. Als solche startete im Jahr 1998 die Internet-Währung »Flooz«, deren Funktionsweise bekannten Bonuspunkt-Systemen ähnelt. Anwender konnten durch webbasierte Einkäufe Flooz verdienen, die sie dann bei Einkäufen über

2 Siehe Mallo (2019); Schrimpf/Sushko (2019).
3 Siehe Booth (2020).

teilnehmende Webseiten wieder gegen Waren tauschen konnten. Ein Flooz entsprach dem Gegenwert von einem US-Dollar. Wie vergleichbare Projekte erreichte auch der Flooz nie die für einen Erfolg notwendige kritische Masse. Das Ende des ersten Internet Hypes zur Jahrtausendwende überlebte das System nicht.

Sowohl das Modell der Kartenzahlung in den Niederlanden als auch das Konzept des Flooz waren Unternehmungen, die sich an der Lösung spezifischer Probleme versuchten. Es gab jedoch schon zu Beginn der 1980er-Jahre Projekte, die einen wirklich großen Wurf wagten. Eines davon konzipierte David Chaum, ein bekannter Informatiker, der mehr als dreißig einschlägige Patente hält. Eines davon trägt den Titel »Blind Signature Systems«[4] und stammt aus dem Jahr 1988. Schon Jahre zuvor hatte der damals bei der University of California, Berkeley, tätige Forscher und Entwickler mit der Veröffentlichung seines Papers »Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms« einen Meilenstein in der Geschichte der verschlüsselten digitalen Kommunikation gesetzt. Auch wenn die Titel der beiden Patente nicht auf digitale Währungen hinweisen, sind die von Chaum entwickelten Methoden elementare Bausteine von Kryptoassets.

Im Jahr 1989 finalisierte Chaum die Arbeit an einem Protokoll für eine digitale Währung, deren Namen eCash er für sein Unternehmen DigiCash schützen ließ. Das Konzept nutzte zahlreiche seiner Erkenntnisse, darunter die der »blind signature«[5]. Dieses Verfahren ermöglicht die Verifikation des Absenders einer Nachricht ohne die Offenlegung des enthaltenen Inhaltes und ist ein wichtiges Element bekannter Kryptoassets. Dem Unternehmen DigiCash und dessen digitaler Währung war dennoch kein langfristiger Erfolg beschieden. Der Aufstieg des E-Commerce hatte gerade erst begonnen, und die Anzahl der Nutzer konnte trotz der ausgezeichneten technischen Umsetzung nicht in ausreichendem Maße gesteigert werden. Technisch ähnelte eCash dem Aufbau von PayPal. Als problematisch stellte sich vor allem die Abhängigkeit von den für die Nutzung von eCash lizensierten Banken heraus. Zwar konnten durch die feste Anbindung an das bestehende Finanzsystem Schwierigkeiten bei rechtlichen Themen wie der Verhinderung von Geldwäsche vermieden werden. Andererseits wurde eCash dadurch für die Nutzer nicht attraktiver, denn es stellte durch die starre Anbindung an die existierenden Systeme kein unabhängiges Geldsystem dar.

Im Jahr 1998 meldete DigiCash Insolvenz an. Die Arbeit von David Chaum war jedoch nicht umsonst. Die von ihm entwickelten und in der Praxis erprobten Konzepte bereiteten den Boden für die nachfolgenden Entwicklungen. Vor allem die Notwendigkeit einer zentralen Autorität und die Abhängigkeit vom existierenden Banksystem stellten Hürden dar, die es zukünftig zu überwinden galt. Eines wurde allen Befürwortern einer digitalen Währung durch die zentrale Natur des eCash-Systems und die anhaltenden Probleme mit den Regulierungsbehörden spätestens zu dieser Zeit klar. Ein robustes und unabhängiges Geldsystem muss dezentral konzipiert sein.

4 Das Patent ist unter https://www.chaum.com/patents/US4759063.pdf abrufbar.
5 Siehe Chaum (1983).

Rund zehn Jahre nach dem Start von DigiCash konzipierte Wei Dai, ein chinesischer Hardware Entwickler, das digitale Geld b-Money[6]. In seinem Paper beschrieb Dai ein Protokoll, das schon viele Punkte des Bitcoin vorwegnahm. Beschrieben wurden beispielsweise die Möglichkeiten, den Rechenaufwand zur Lösung eines mathematischen Problems als proof-of-work zu nutzen und den beteiligten Rechner für seine geleistete Arbeit zu vergüten. Auch die Nutzung eines gemeinsamen Buchhaltungssystems (distributed legder), dessen Einträge kollektiv verifiziert und akzeptiert werden, wurde von Dai erwähnt. Über die Konzeptionsphase kam sein Protokoll zwar nie hinaus, es beeinflusste jedoch spürbar die nachfolgenden Entwicklungen. Zu Ehren von Wei Dai wurde die kleinste Einheit des Ether[7], der wei, nach ihm benannt.

Ein weiterer bedeutender Pionier der digitalen Währungen ist der aus Ungarn stammende Nicholas Szabo. Im Jahr 1998 entwickelte der Informatiker mit dem bit gold-Protokoll einen direkten Vorläufer des Bitcoin, der essenzielle Bausteine seines Nachfolgers bereits erkennen ließ.[8] Der Kern des bit gold-Protokolls ist das proof-of-work-Konzept, bei dem Szabo sich an der Arbeit von Adam Back orientierte. Dieser hatte ein Jahr zuvor einen entsprechenden Algorithmus geschaffen, der zur Vermeidung von Spam-Nachrichten und zur Vorbeugung gegen Distributed-Denial-of-Service Attacken[9] in Netzwerken eingesetzt werden konnte. Das Konzept verhindert die unlimitierte Kommunikation von Netzwerkteilnehmern, indem es als Voraussetzung für die Akzeptanz einer übermittelten Nachricht eine vorher verrichtete Arbeit voraussetzt. Für DDoS-Angreifer oder Absender von Spam-Nachrichten entstünden somit bei jeder Anfrage oder versandten Nachricht ein Rechenaufwand. Die damit einhergehenden Kosten würden solche Angriffe teuer und damit unattraktiv machen.

Das Konzept des Nachweises geleisteter Rechenarbeit, das proof-of-work, ist ebenso einfach wie genial. Die Teilnehmer eines Netzwerks stellen Rechenleistung für die Lösung mathematischer Probleme zur Verfügung. Hat ein Rechner die Lösung einer Aufgabe gefunden, kann er diese in das Netzwerk kommunizieren. Da der Rechner seinen Arbeitseinsatz durch die Lösung der Aufgabe unter Beweis gestellt hat, kann nun ein Eintrag in das öffentliche Verzeichnis des Netzwerks erfolgen. Jeder Eintrag wird dann ein Teil der nächsten zu lösenden Aufgabe. So entsteht eine stetig länger werdende Kette an Einträgen, die durch den enormen investierten Rechenaufwand de facto unveränderlich ist. Diese Kette, mit allen jemals auf dem Netzwerk erfolgten Transaktionen, ist der Kern der global verteilten dezentralen Buchhaltung des Netzwerks, der distributed ledger.

Der Beitrag von Szabo zur Schaffung eines dezentralen Geldsystems ist außerordentlich. Lediglich das double-spend-Problem konnte Szabo mit seinem bit gold-Protokoll nicht zufriedenstellend lösen. Dabei handelt es sich um die Frage, wie sich in einem

6 Den Text von Wei Dai zu b-money finden Sie unter http://www.weidai.com/bmoney.txt.
7 Der Ether ist der native Token des Ethereum Netzwerks.
8 Siehe Szabo (2021).
9 Distributed Denial of Service-Attacke: Bei einem DDoS-Angriff führen Angreifer die Nichtverfügbarkeit eines Dienstes oder Servers durch eine enorme Anzahl von Anfragen gezielt herbei.

Zahlungssystem die mehrfache Ausgabe derselben Geldeinheit verhindern lässt. Bezahlt beispielsweise ein Käufer einen Musikdownload und kann die Dienstleistung nutzen, bevor die Transaktion final abgerechnet wurde, kann die selbe Geldeinheit für die Zahlung einer weiteren Dienstleistung genutzt werden oder einfach an eine andere Adresse gesendet werden. Die Lösung dieser schwierigen Aufgabe blieb vorerst offen. Wenn aber Nakamato sagen würde, er habe wie Newton auf den Schultern von Riesen gestanden, dann ist Szabo einer dieser Riesen.

Enter Satoshi Nakamoto

»If I have seen further it is by standing on the shoulders of Giants.«

Isaac Newton

Der nächste große Schritt war Satoshi Nakamotos Bitcoin-Protokoll, das der Entwickler in einem Whitepaper als Peer-to-Peer Bezahlsystem beschrieb. Das Protokoll kombiniert verschiedene Bausteine seiner Vorgänger und löst als Blockchain Anwendung auch das Problem des double spend. Alle Transaktionen finden direkt Peer-to-Peer zwischen den Teilnehmern in einem Netzwerk ohne zentrale Autorität und ohne zentrale Buchhaltung statt. Alle notwendigen Informationen sämtlicher Transaktionen werden in Daten-Blöcken gespeichert, die sequenziell zu einer Kette von Blöcken verknüpft werden, einer *Blockchain*. Die einzelnen Blöcke sind dabei über eine kryptografische Hashfunktion miteinander verkettet. Jeder Block beinhaltet so transformierte Informationen des vorangegangenen Blocks. Da sich dies durch die gesamte Kette hindurchzieht, kann kein einzelner Block verändert oder aus dieser Kette herausgelöst werden.

Die Mehrheit der Rechenleistung des Netzwerks einigt sich auf eine einzige valide Kette aus Blöcken. So entsteht eine stetig wachsende Reihe an Transaktionen, die mehrheitlich akzeptiert der korrekten Historie aller Transaktionen entspricht. Das Netzwerk übernimmt somit eigenständig die Schaffung neuer Einträge, die Überprüfung von Transaktionen auf Konsistenz mit der Transaktionshistorie und deren Fortschreibung. Eine zentrale Instanz ist ebenso überflüssig wie eine dritte, prüfende Partei. Auch die Datenhaltung ist ungewöhnlich. Die gesamte Blockchain ist auf jedem Knoten (full node) des Netzwerks vorhanden. Anstelle einer zentralen Datenhaltung werden die Daten im Netzwerk redundant vorgehalten. Die Datenmenge ist daher größer als bei einer zentralen Speicherung. Die Redundanz führt aber zu einer robusten Datenhaltung, denn der Ausfall einzelner Netzwerkknoten spielt für die Datensicherheit keine Rolle.

Enter Bitcoin

Der 31. Oktober 2008 markiert das Datum der Veröffentlichung des Bitcoin Whitepapers mit dem Titel »Bitcoin: A Peer-to-Peer Electronic Cash System«.[10] Es ist bis

10 Das Paper ist unter https://bitcoin.org/bitcoin.pdf abrufbar.

heute nicht bekannt, ob sich hinter dem Decknamen Satoshi Nakamoto eine einzelne Person oder eine Gruppe von Entwicklern verbirgt.[11]

Während der Arbeit am Paper und bereits zwei Monate vor der Veröffentlichung registrierte Nakamoto die Domain »bitcoin.org« (siehe Abbildung 2.1). Das Eigentum an dieser Domain gab Nakamoto umgehend an mehrere Personen weiter, die nicht zum Kern der Bitcoin-Entwickler zählten. Nicht nur auf Ebene der Programmierung wurde die Gefahr einer Zentralisierung des dezentralen Projektes so von Beginn an minimiert.[12]

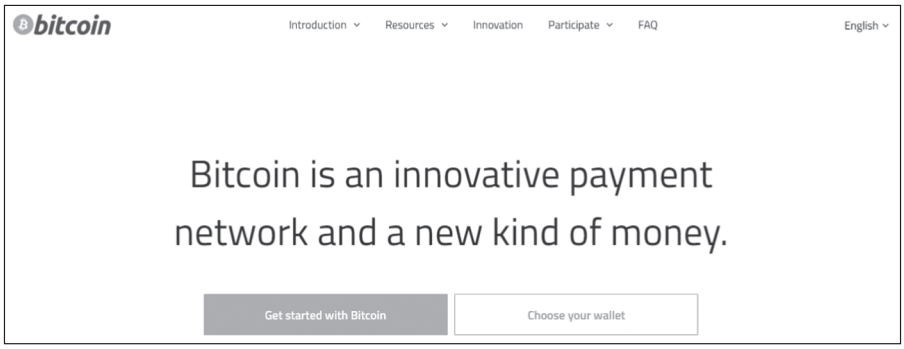

Abb. 2.1: Webseite Bitcoin.org

Am 3. Januar des Jahres 2009 war es soweit. Mitten in der größten Finanzkrise seit den 1930er-Jahren[13] wurde mit dem Genesis Block der Ursprung der Bitcoin Blockchain gelegt. Dieser Block ist der erste Block, der jemals auf dem Bitcoin-Netzwerk erzeugt wurde. Da die Belohnung für Erstellung des Blocks im Rahmen des Mining seinerzeit bei 50 Bitcoin lag, entstanden zeitgleich mit diesem ersten Block auch die ersten 50 Bitcoin.

Der Zeitpunkt für den Start des Netzwerkes wurde nicht zufällig gewählt. Das globale Finanzsystem stand seinerzeit vor einem Komplettversagen. Ein Detail lässt einen Blick auf die Beweggründe Nakamotos zu, der mit der Erzeugung des ersten Blocks der Bitcoin Blockchain eine kurze Textnachricht übermittelte. Bei dieser Botschaft handelt es sich um das Zitat der Überschrift eines Artikels aus der englischen Tageszeitung *The Times* vom 3. Januar 2009, in dem über die Pläne des damaligen Finanzministers Alistair Darling berichtet wird, die britischen Banken im Rahmen einer erneuten Rettungsaktion mit hunderten Milliarden britischen Pfund zu stützen. Der kurze Text lautete »The Times 03/Jan/2009 Chancellor on brink of second bailout for banks«. Für Nakamoto stellte das Bitcoin-Netzwerk als bankenunabhängiges Peer-to-Peer-System für den globalen Zahlungsverkehr eine Alternative zum bestehenden, zentralisierten System dar.

11 Siehe Frisby (2014).
12 Siehe Champagne (2014).
13 Zahlen zur Finanzkrise erhältlich bei bpb (2017).

Bitcoin versus Blockchain

Der Bitcoin ist als nativer Token des Bitcoin-Netzwerks nur eine Ausprägung einer Kryptowährung. Daher ist die bekannteste Kryptowährung kein Synonym für die Blockchain, sondern lediglich ihre bislang bekannteste Anwendung. Obwohl die folgenden Ausführungen sich spezifisch auf Nakamotos Entwicklung beziehen, gelten nachfolgend dargestellte Prinzipien auch für andere Kryptoassets.

Das System Bitcoin besteht aus mehreren Komponenten. Zum einen ist es die Client-Software, die jeder auf einem Computer installieren kann. Rechner, die diese Software nutzen, bilden die Knoten eines verteilten Netzwerks, über das die Kommunikation der Computer untereinander erfolgt. Neben der installierten Client-Software hält jeder Netzwerkknoten eine vollständige Version der aktuellen Blockchain mit allen jemals erfolgten Bitcoin Transaktionen in seinem Speicher.

Die Regeln des Netzwerks sind im Bitcoin-Protokoll definiert. Die Client-Software implementiert diese codierten Regeln, die unter anderem festlegen, wie neue Bitcoin entstehen, wer diese erhält und wie Transaktionen im Netzwerk verifiziert werden können. Die Mining-Rechner sind die Buchhalter des verteilten Netzwerks, die gemeinsam in einem dezentralen, redundant abgelegten Hauptbuch arbeiten. Für ihren Beitrag zur Aufrechterhaltung einer fehlerfreien und unabänderlichen Buchhaltung werden die Miner mit neu geschaffenen Bitcoin belohnt. Zusätzlich können sie Transaktionsgebühren vereinnahmen.

Die Nutzung einer Blockchain und das ökonomische Anreizsystem für die Miner ermöglichen eine dezentrale und unabhängige Überprüfung sämtlicher Eigentumsverhältnisse und Transfers im Netzwerk. Die Übertragung von Bitcoin zwischen zwei Teilnehmern erfolgt direkt bilateral. Eine Rückabwicklung von Transaktionen im Falle von Fehleingaben oder Streitigkeiten ist nicht möglich. Bitcoin Transaktionen sind endgültig. Die Unabhängigkeit von jeglicher Drittpartei und die Finalität einmal ausgeführter Transaktionen sind die grundlegenden Unterschiede zwischen Blockchain-basierten und konventionellen Transaktionssystemen.

Im Gegensatz zu typischen Finanztransaktionen, bei denen sich die beteiligten Personen oder Organisationen durch einen Ausweis oder eine eindeutige ID identifizieren müssen, gibt es für die Nutzung des Bitcoin-Netzwerks keine derartige Anforderung. Um eine Transaktion ausführen zu können, muss eine Person oder Organisation nur einen privaten Schlüssel[14] und eine Bitcoin-Adresse[15] besitzen.

14 Ein privater Schlüssel ist eine 256-Bit-Zeichenfolge. Im Hexadezimalsystem hat sie entsprechend 64 Zeichen. Ein Beispiel für einen solchen Schlüssel ist: 1b9cdf53588f99cea61c6482c4549b0316bafde19f76851940d71babaec5e569.

15 Eine Bitcoin-Adresse besteht je nach Format aus einer 34- bzw. 42-stelligen Zeichenfolge im Hexadezimalsystem. Ein Beispiel für eine Adresse im alten Format P2PKH ist: 1MbeQFmHo9b69kCfFa6yBr7BQX4NzJFQq9; ein Beispiel für eine Adresse im modernsten Format Bech32 ist bc1qc7slrfxkknqcq2jevvvkdgvrt8080852dfjewde450xdlk4ugp7szw5tk9.

Anonymität jedoch, wie vielfach hervorgehoben, bietet der Bitcoin nicht. Vorsichtige Nutzer können zwar versuchen, die Transparenz der eigenen Transaktionen zu verschleiern. Der erreichbare Grad an Anonymität im Netzwerk wird jedoch überschätzt. Nach Aussagen von Forschern der Cornell Universität können bereits simple Webtracker und Cookies, die in viele Websites eingebettet sind, die Zuordnung von Bitcoin Transaktionen zu einer Person ermöglichen. In mehr als 60 % der untersuchten Fälle sei eine eindeutige Verknüpfung möglich.[16] Es erfordert nur wenig Fantasie, sich vorzustellen, wie einfach die Zuordnung der meisten Transaktionen zu den ausführenden Personen ist, wenn nur genügend Daten systematisch zusammengefasst werden können. Schon jetzt gibt es Beispiele von Strafverfolgungsbehörden, die Straftäter auf Grund der von diesen im Zusammenhang mit den ausgeübten Vergehen durchgeführten Bitcoin-Transaktionen überführen konnten.[17]

Einsatzfelder

Ironischerweise ist Bitcoin auf Grund technischer Restriktionen und der unvermeidlichen Transaktionskosten kaum als Zahlungsmittel für eine Vielzahl kleiner Transaktionen geeignet. Nakamotos ursprüngliche Vision eines »Peer-to-Peer Electronic Cash System« erfüllt die von ihm geschaffene Kryptowährung in der aktuellen Form nicht. Inspiriert vom Bitcoin entwickelten sich jedoch andere Projekte, die für diesen Einsatzzweck besser geeignet sind. Trotz der Möglichkeiten, auch unter Nutzung des Bitcoin-Netzwerks eine Lösung für den alltäglichen Zahlungsverkehr zu schaffen, liegen dessen Stärken anderswo.

In den letzten Jahren kristallisierte sich die Vorteilhaftigkeit des Bitcoin-Netzwerks vor allem für zwei Anwendungen heraus. Zum einen sind dies grenzüberschreitende Großtransaktionen, die sich mit Kryptowährungen schnell und unbürokratisch, sehr günstig und ohne Settlement-Risiken[18] durchführen lassen. Es spielt weder für die Kosten noch für die Dauer eines Transfers eine Rolle, ob sie einen einzigen oder 10 000 Bitcoin transferieren. Es spielt auch keine Rolle, ob sich diese Transaktion zwischen Ihnen und Ihrem Nachbarn oder einer Person auf der anderen Erdhalbkugel abspielt. Das Internet hat keine Grenzen und das Auslösen einer beliebig großen Transaktion ist nicht schwieriger als eine E-Mail zu versenden. Abwicklungssysteme werden ebenso wenig benötigt wie zwischengeschaltete Organisationen und das Settlement der Transaktion erfolgt umgehend. Die Bitcoin befinden sich entweder noch beim Sender oder bereits beim Empfänger. Zwischen diesen beiden Zuständen gibt es nichts, keinen Intermediär und damit auch kein entsprechendes Risiko.

16 Siehe Goldfeder et al. (2017).
17 Siehe Manager Magazin (2021).
18 Als Settlement-Risiko bezeichnet man das Risiko, dass eine getätigte Transaktion gar nicht oder nicht rechtzeitig abgewickelt wird, da der Vertragspartner bis zum beiderseitigen Erfüllungstag seinen Verpflichtungen nicht nachkommt, während die eigene Verpflichtung bereits erfüllt wurde.

Zudem entwickelt sich Bitcoin auf Grund des tendenziell abnehmend inflationären bis leicht deflationären Charakters zunehmend als zentralbankunabhängige Anlage ohne Zinsänderungs- oder Adressausfallrisiko. In Zeiten, in denen Zentralbanken nicht mehr die Geldwertstabilität, sondern mit der Steigerung der Inflationsrate den Kaufkraftverlust als primäres Ziel verfolgen, gewinnt dieser Punkt an Bedeutung.

Die Bausteine des Bitcoin

Während Blockchains und Bitcoin bereits seit einem Jahrzehnt existieren, nimmt die Aufmerksamkeit institutioneller Investoren erst seit einigen Jahren zu. Der starke Anstieg des Bitcoin-Kurses und die damit verbundenen Schlagzeilen im Jahr 2017 führten erstmals zu einer Wahrnehmung von Kryptoassets durch breitere Bevölkerungsschichten. Während private Anleger vor allem von hohen Kursgewinnen angezogen wurden, galt das Interesse professioneller Anleger zunächst eher den Einsatzmöglichkeiten von Blockchain-Anwendungen in der Finanzbranche. Die neue Technologie hat offensichtliche disruptive Elemente, die einerseits enorme Prozessverbesserungen für Finanzunternehmen, vor allem für Asset-Manager, mit sich bringen. Andererseits stellt ein ausgereiftes und skalierbares Blockchain-basiertes System die Notwendigkeit klassischer Intermediäre und die mit diesen zwangsläufig verbundenen Kosten in Frage. Um sich den relevanten Fragen widmen zu können, ist ein grundlegendes Verständnis der Bitcoin-Terminologie notwendig.

Der Bitcoin ist der derzeit bekannteste Anwendungsfall einer Blockchain. Die Blockchain ist die zentrale Komponente des Bitcoin-Netzwerks, sie ist jedoch nicht gleichbedeutend mit dem Bitcoin. Blockchain-Anwendungen lassen sich für viele Zwecke nutzen, und das gesamte Bitcoin-System besteht nicht allein aus der Blockchain, sondern aus mehreren Komponenten. Das von Nakamoto ins Leben gerufene Zahlungssystem ist ein eher simpler Spezialfall der Nutzung einer Blockchain. Die Genialität des Bitcoin-Systems liegt nicht in der Blockchain allein, sondern in der sinnvollen Kombination verschiedener existierender Technologien zu einem effizienten Ganzen. Gerade in der Simplizität und der Beschränkung auf das Wesentliche liegen die Stärken des Protokolls. Je einfacher ein System ist, desto weniger Angriffspunkte bietet es.

Im folgenden Abschnitt werden wir auf die Grundlagen der Blockchain und des Bitcoin-Netzwerks eingehen. Für technisch Interessierte gibt es zahlreiche Bücher, die auch die Konstruktionsmerkmale von Bitcoin und Kryptowährungen detailliert beschreiben.[19] Leser mit Vorkenntnissen können diesen Abschnitt überspringen.

Die Blockchain

Im Kern handelt es sich bei einer Blockchain um eine verteilte Datenbank, die von mehreren Benutzern in einem Netzwerk gemeinsam genutzt werden kann. Die

19 Siehe Bashir (2020); Schär/Berentsen (2017); Voshmgir (2019).

Datenhaltung erfolgt nicht in einer zentralen Instanz, sondern redundant auf jedem einzelnen Rechner, der Teil des Netzwerks ist. Einzelne Daten, beim Bitcoin-Netzwerk sind es Transaktionsdaten, werden in Blöcken (block) zusammengefasst, die dann unverrückbar und eindeutig zu einer wachsenden Historie verkettet (chain) werden. Um dies zu ermöglichen, werden verschiedene Technologien wie das Internet, kryptografische Methoden und Hashfunktionen eingesetzt.

Eine Blockchain kann in verschiedenen Ausprägungen gestaltet werden. Eine öffentliche Blockchain (public blockchain), wie die des Bitcoin-Netzwerks, hat keine Hürden hinsichtlich der Nutzung. Jeder kann dem Netzwerk beitreten und es vollumfänglich nutzen. Eine private Blockchain (private blockchain) ist vergleichbar mit einem Intranet, erfordert eine Nutzerverifikation und kann je nach Konstruktion sämtliche Mechanismen vom Mining bis hin zu Manipulationen einzelner Einträge auf der Blockchain über eine zentrale Instanz beeinflussen. Private Blockchains repräsentieren daher eine dezentral konstruierte, aber zentral koordinierte Anwendung. Die dritte Kategorie sind die permissioned blockchains, die Elemente aus den privaten und öffentlichen Blockchains kombinieren. Ein Beispiel für eine solche Blockchain ist Ripple (XRP). Es gibt keine guten oder schlechten Blockchains. Die jeweilige Konstruktion hängt vom Einsatzzweck und von anderen Parametern, etwa dem Datenschutz, ab.

Kryptografie

Die Kryptografie beschäftigt sich als Teilgebiet der Kryptologie mit Verfahren zur Verschlüsselung von Daten. Obwohl alle historischen Bitcoin-Transaktionen unverschlüsselt und damit für jedermann einsehbar sind, spielen Verschlüsselungsalgorithmen eine unverzichtbare Rolle. Im Bitcoin-Netzwerk kommt ein klassisches asymmetrisches Verschlüsselungsverfahren mit privaten und öffentlichen Schlüsseln zum Einsatz. Wie diese Schlüssel generiert werden, hängt vom kryptografischen Algorithmus ab. Beispiele für asymmetrische Systeme sind der RSA (Rivest-Shamir-Adleman) und der ECC (Elliptic-Curve Cryptography) Algorithmus, der beim Bitcoin eingesetzt wird. Die asymmetrische Kryptografie erhöht auf skalierbare Weise die Sicherheit der Kommunikation in nicht vertrauenswürdigen Netzwerken.

Einen ausreichend langen *privaten Schlüssel* zu knacken, ist praktisch nicht möglich. Nur derjenige, der im Besitz dieses Schlüssels ist, kann Transaktionen im Netzwerk anstoßen und Bitcoin von einer Adresse an eine andere senden. Durch die Freigabe einer Transaktion mit dem privaten Schlüssel wird gleichzeitig die Authentizität des Absenders sichergestellt. Die Bedeutung des privaten Schlüssels im Netzwerk kann man daher nicht überbewerten. Wer den privaten Schlüssel zu einer bestimmten Adresse im Netzwerk besitzt, kann frei über die mit dieser Adresse assoziierten Bitcoin verfügen. Es ist kein weiterer Nachweis der Identität oder des Besitzrechtes notwendig. Ohne diesen Schlüssel hingegen geht nichts mehr. Dieses Vorgehen mag kompliziert klingen, wird jedoch vollständig von der Wallet-Software des Anwenders übernommen. Die Aufgabe des Nutzers besteht lediglich darin, seinen privaten Schlüssel nicht zu verlieren.

Hashfunktionen

Die meisten Menschen haben bereits von verschiedenen Verschlüsselungsverfahren gehört. Schon Kinder machen spielerische Experimente mit Geheimtinten oder stecken sich Zettel mit einfach verschlüsselten Botschaften zu. Mit Hashfunktionen aber haben wohl nur die wenigsten Menschen bereits zu tun gehabt. Daher kann sich kaum jemand vorstellen, was sich hinter diesem essenziellen Baustein des Bitcoin-Netzwerks verbirgt.

Eine Hashfunktion ist eine mathematische Funktion. Sie ordnet jedem gegebenen Eingangswert eine Ausgabe, den Hashwert oder kurz »Hash« der Eingabe, zu. Dabei erfüllt sie mehrere Kriterien.

- Eine Hashfunktion ist unumkehrbar. Aus einem Eingangswert kann leicht eine Ausgabe berechnet werden. Aus dieser Ausgabe sind jedoch keinerlei Rückschlüsse auf die Eingabe möglich. Wie bei einer Zigarette ist es ein Leichtes, diese zu einem Häufchen Asche umzuwandeln. Der Rückweg ist, zum Leidwesen aller Raucher, ausgeschlossen.
- Auch bei zwei Eingangswerten, die sich nur marginal unterscheiden, sind keinerlei Ähnlichkeiten beim Ergebnis sichtbar.
- Die Zuordnung muss eindeutig sein. Jede Eingabe resultiert exakt in einem Hashwert und zwei unterschiedliche Eingaben führen immer zu unterschiedlichen Hashwerten.
- Das Ergebnis einer Hashfunktion hat unabhängig von der Länge des Inputs immer die gleiche Länge.
- Eine Hashfunktion muss schnell berechenbar sein, damit sie in der Praxis eingesetzt werden kann.

Es gibt verschiedene Hashfunktionen. Ein bekannter Vertreter dieser Gattung hört auf den schönen Namen *SHA-512*. Wir wollen uns diese Funktion einmal bei der Arbeit anschauen, übergeben ihr daher einen einfachen Satz und werfen einen Blick auf das Ergebnis. Das erste der beiden folgenden Beispiele zeigt den Hashwert eines Zitats des Physikers Richard P. Feynman, der sagte: »I would rather have questions that can't be answered than answers that can't be questioned.«

Die Funktion liefert als Hashwert dieses Satzes die folgende Zeichenkette:

```
adbdc0b3741d344597b7049bff22f72e0ba629e5a68be081b210f74bbd9f429046c7c845f9a
956859b08b7802e68f80d0ac4c4c3d9637df92aa87f5bf3dbdedd
```

Nun ändern wir die Eingabe, indem wir den abschließenden Punkt des Zitats streichen. Wir übergeben nun den Satz »I would rather have questions that can't be answered than answers that can't be questioned« an die Funktion. Diese minimale Änderung der Eingabe resultiert in folgendem, stark vom ersten Ergebnis abweichenden Hashwert:

f1fa8a235ff0947058678928e6cc614b3803b5db30e0f813de6d738779fdb2b8e98150d2540
62b84f525f80f9118ea14bd1d8ff1405e534ad102d2d7d7bc2c49.

Niemand kann aus den Ausgabewerten Rückschlüsse auf die Eingaben ziehen. Eine minimale Änderung der Eingabe, hier der Punkt am Satzende, führt zu nicht kalkulierbaren Veränderungen der Ausgabe. Die Funktion SHA-512 hat Ihre Aufgabe erfüllt.

Die treibenden Kräfte hinter Bitcoin

> *»It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self fulfilling prophecy.«*
>
> *Satoshi Nakamoto im Jahr 2009*

Viele, die sich eine Weile mit Kryptowährungen im Allgemeinen und dem Bitcoin im Besonderen beschäftigt haben, können die sich bietenden Möglichkeiten nur erahnen, sind aber fasziniert von der Idee eines dezentralen Geldsystems. Wie revolutionär diese Idee ist, dürfte vor allem Fachleuten bewusst sein, die täglich mit den technischen und juristischen Wirren des Finanzalltags zu tun haben. Ein System, in dem Transaktionen ohne Gegenparteirisiko und Zeitverzug abgewickelt werden können, das unabhängig von politischen Einflüssen und einer zentralen Autorität ist und alle historischen Transaktionen mit exaktem Zeitstempel öffentlich und kostenlos verfügbar macht, ist ein großer Wurf.

Die Konzeption eines digitalen Assets klingt abstrakt und wirkt technisch komplex. Für Menschen ohne nennenswerte Technikaffinität und mit nur geringem Interesse an der Funktionsweise der Finanzmärkte ist so eine Entwicklung schwer zu greifen. Die mangelnde Regulatorik und der in den Anfangsjahren sprichwörtliche Wilde Westen mit seinen extremen Preisschwankungen schreckten viele Menschen ab. Medienberichte, die vor diesem »gefährlichen Zeug« warnten, erhöhten die Attraktivität ebenso wenig wie die Kursrückgänge nach dem Preisanstieg im Jahr 2017. Auch die oft an Desinteresse grenzenden Wissenslücken manchen Verfassers solcher Artikel halfen nicht weiter, die Angst der Anleger blieb. Gerade in Deutschland kam mit den Erinnerungen an das Aktiendebakel des »Neuen Marktes« ein Trauma wieder zum Vorschein.

Auch in der Finanzbranche arbeitete man zunächst nicht auf eine Adoption hin, sondern operierte vielerorts nach dem alten Prinzip, erst einmal abzuwarten, was die anderen wohl tun mögen. An einer Stelle also, die zum logischen Berührungspunkt interessierter Kunden und der neuen Kryptowelt hätte werden können, herrschte weitgehend Stille.

Auch in den Jahren 2020 und 2021 herrschte kein Mangel an kritischen Stimmen. Fundierte Argumentationen waren selten zu finden und oft gefielen sich die Opponenten in einer aggressiven Generalkritik.[20]

20 Thomas Straubhaar auf welt.de: »Der Bitcoin ist ein Spielzeug für Zocker.« (Straubhaar, 2021) oder Mark Schieritz auf Zeit.de mit dem Artikel »Bitcoin? Kann weg. Die Digitalwährung ist weder krisensicher noch nachhaltig. Auch wenn sie gerade boomt: Ihre Tage sind gezählt.« (Schieritz, 2021).

Auch die Bundesanstalt für Finanzaufsicht (BaFin) teilte potenziellen Anlegern ihre Sicht der Dinge unter anderen im BaFin Journal 09/2020 mit.[21] Dort heißt es »Belastbare Prognosen über die Wertentwicklung von Payment-Token können Anleger kaum treffen – dafür sind virtuelle Währungen zu komplex. Dies ist insbesondere darauf zurückzuführen, dass Payment-Token kein realwirtschaftlicher Wert zugrunde liegt. Sie haben keinen intrinsischen Wert und sind dadurch Spekulationen ausgesetzt. Für die Stabilität eines Payment-Tokens ist ihre Reputation und Akzeptanz enorm wichtig – insbesondere vor dem Hintergrund, dass Payment-Token nicht von Zentralbanken ausgegeben werden und kein gesetzliches Zahlungsmittel darstellen.«

Diese Stellungnahme ist in zweierlei Hinsicht bemerkenswert. Zum einen ist es eine Eigenschaft von Fiat-Währungen, keinerlei intrinsischen Wert aufzuweisen und nur auf Vertrauen zu basieren. Zum anderen ist es gerade der Vorteil eines dezentralen Systems, nicht von einer zentralen Instanz wie einer Notenbank abhängig zu sein. Man kann die Sichtweise der BaFin teilen oder nicht. Es ist jedoch unstrittig eine Sichtweise, die den Status quo zum Maß aller Dinge macht. Eine solche Haltung kollidiert früher oder später mit der fortschreitenden Realität.

Über den Nutzen und die möglichen Risiken wird diskutiert und wie bei anderen Themen sollte es niemanden überraschen, wenn die Interessen von Unternehmen, Regierungen und Privatpersonen nicht immer deckungsgleich sind. Daher ist es wichtig, bei der Einordnung jeglicher Kritik die Ziele des Kritikers zu beachten. Wer sich eine möglichst umfassende staatliche Kontrolle über persönliche Daten und Finanzmarkttransaktionen wünscht, der favorisiert eine zentrale Behörde. Aus Sicht einer Privatperson hingegen bringt ein dezentral organisiertes Finanzsystem ohne Intermediäre und ohne zentrale Kontrollstelle mehr Selbstbestimmung über die persönlichen Finanzen und auch über die persönlichen Daten. Zudem können Werte außerhalb der komplexen Strukturen des Finanzsystems gehalten werden und so die Sicherheit des Vermögens vor systemimmanenten Risiken erhöht werden. Andreas Antonopoulos, Informatiker und ein früher Fürsprecher einer zunehmenden Bitcoin-Adoption, spricht daher nicht nur vom Schweizer Bankkonto, sondern von einer Schweizer Bank in der Hosentasche.[22] Das mag für manchen arg ambitioniert klingen, ist jedoch angesichts der technischen Möglichkeiten dezentraler Finanzapplikationen ein treffender Vergleich.

Es gilt wie so oft, die Wahrheit in der Mitte zwischen quasireligiösen Fans auf der einen und den Vertretern einer fundamentalen Opposition auf der anderen Seite zu suchen. Dabei hilft es nicht, so zu tun, als gäbe es so etwas wie eine alleinstehende Attraktivität oder ein alleinstehendes Risiko einer Anlageklasse. Sowohl die Beurteilung der Attraktivität als auch die Einstufung der Risiken eines Assets sind nur innerhalb eines Bezugssystems möglich. Wenn jemand den Bitcoin als nutzlos bezeichnet, dann sollte er den Token auf einer Skala der Nutzlosigkeit einordnen und eine Aussage darüber

21 BaFin (2020).
22 Siehe Antonopoulos (2019).

treffen, ob negativ rentierliche Staatsanleihen auf dieser Skala höher oder niedriger angesiedelt sind. Wenn jemand sagt, der Bitcoin sei auf ewig die beste aller Assetklassen und er würde niemals auch nur einen Teil seiner Bitcoin verkaufen, dann stellt sich die Frage, wie sinnvoll eine Aussage über die zukünftige Attraktivität eines Assets sein kann, wenn das Verhältnis zu anderen Anlagen ignoriert wird.

Professionelle Marktteilnehmer erkennt man an fundierten Aussagen und der Fähigkeit, in Anbetracht sich verändernder Rahmenbedingungen geistig handlungsfähig zu bleiben und, falls es angeraten ist, die Richtung zu ändern.

Bitcoin-Mythen

> *»Cryptocurrencies basically have no value and they don't produce anything. I don't have any cryptocurrency and I never will.«*
>
> *Warren Buffett*

Technologische Entwicklungen wirken ebenso wie gesellschaftliche Veränderungen oft erst im Rückblick folgerichtig. Heutzutage findet sich kaum jemand, der nicht den Aufstieg des Onlinehandels oder die vollständige Digitalisierung der Musik- und Videobranche für einen logisch zwingenden Weg hält. Zu Beginn eines Wandels benötigt es Visionäre, die die Attraktivität sowie das Potenzial einer neuen Technologie erkennen. Neue Entwicklungen haben nicht nur Befürworter und auch der Bitcoin, oder genereller gesagt die Kryptoassets, stehen noch immer von vielen Seiten unter Beschuss. So gab es neben erfolglosen Versuchen, das Netzwerk selbst zu attackieren, auch Gegenwind von Regulierungsbehörden und Vertretern des klassischen Finanzwesens. Dabei sind oft die gleichen Argumente zu hören, warum der Bitcoin nicht funktionieren könne oder sich aus sonstigen Gründen nicht durchsetzen werde.

Wir gehen im Folgenden auf die gängigsten Argumente gegen den Bitcoin ein.

Bitcoin wird verboten

Schon häufig riefen die Auguren der Finanzbranche nach einem Verbot des Bitcoin. So auch Jamie Dimon, CEO von J.P. Morgan. Noch im Jahr 2017 warnte er in einem Interview Anleger und Interessierte vor möglichen staatlichen Sanktionen.[23]

Im Februar 2019 sah die Welt bereits anders aus. Die von Dimon geführte Bank legte mit dem JPM Coin selbst eine digitale Währung auf, die den US-Dollar abbilden sollte. Geplant war der Einsatz im Zahlungsverkehr. Nur ein Jahr später erweiterte J.P. Morgan sein Kundenspektrum und bot Bankdienstleistungen für die amerikanischen Krypto-Börsen Coinbase und Gemini an. Diese Wendung der Dinge sollte man nicht belächeln, sondern als Ausdruck der professionellen Fähigkeit zum Umdenken werten.

23 Siehe Buck (2017).

Ein Verbot des Bitcoin ist nicht mal eben so und schon gar nicht ohne Nebenwirkungen zu realisieren. Dies ist nicht die Hoffnung einzelner Krypto-Enthusiasten, sondern entspricht der Einsicht des US-Gesetzgebers. Der Vorsitzende des Bankenausschusses des Senats, Mike Crapo, teilte in einer Anhörung zur Regulierung von Kryptowährungen und Blockchain-Technologie mit, dass die Vereinigten Staaten nicht in der Lage sein würden, ein Verbot von Bitcoin durchzusetzen.[24] Das Bitcoin-Protokoll ist Open Source. Jeder kann es implementieren und betreiben. Ein technisch umsetzbares Verbot ist nahezu unmöglich. Auch die Verbreitung der notwendigen Client Software lässt sich zumindest in einem Rechtsstaat nicht einfach unterbinden, denn offen verfügbarer Programmcode wird wie ein Prosatext behandelt. Schon in den 1990er-Jahren hat der oberste US-Gerichtshof dazu ein Urteil gesprochen.[25] Damals ging es um eine kryptografische Verschlüsselungssoftware. Demnach ist Open-Source-Software nichts anderes als ein normaler Text. Damit fällt auch der Code des Bitcoin-Clients unter die Redefreiheit und hat damit den gleichen verfassungsrechtlichen Schutz wie ein Gedicht oder ein Zeitungsartikel. Der Regulierer kann lediglich auf Drittanbieter Einfluss nehmen. Diese erleichtern Interessenten den Zugang zu Bitcoin und sind somit die Schnittstelle zwischen der Welt der Fiat-Währungen und den digitalen Assets. Eine Regulierung dieser Marktteilnehmer ist jedoch nicht zwingend ein Malus. Intelligent reguliert, können alle Beteiligten davon profitieren, die Unternehmen und deren Kunden von gestiegener Rechtssicherheit, der Staat von einer mit vergleichsweise wenig Aufwand zu erreichenden Kontrolle.

Der Umgang der US-Regulierer mit Bitcoin beeinflusst die Behörden in vielen anderen Regionen der Welt. Dennoch gibt es auch Staaten, die versuchen, die Nutzung des Bitcoin einzuschränken oder sogar ganz zu verbieten. Dazu gehören afrikanische Länder wie Algerien, Ägypten und Marokko. Auch in Südamerika gibt es mit Bolivien und Ecuador Vertreter der kompromisslosen Gangart.

In vielen Schwellenländern betreffen die Verbote Banken, denen Geschäfte mit Kryptowährungen untersagt sind. Werden diese Länder Erfolg haben oder sind derartige Eingriffe lediglich das Zeichen ökonomischer Schwäche und werden von Außenstehenden auch als solche wahrgenommen? Wenn es um die Gefahren einer raschen Geldentwertung geht, die in der Regel durch Korruption oder politische Unfähigkeit zumindest begünstigt wird, dürften ab einer gewissen wirtschaftlichen Schmerzgrenze auch Verbote wenig bewirken. Viele Menschen in allen Regionen der Erde wollen zumindest einen Teil ihres Ersparten in Assets anlegen, die von der Geldpolitik entkoppelt sind. Verzweifelte und schlussendlich wohl auch erfolglose Versuche, die Bürger vom Markt für Kryptoassets abzuschneiden, fügen der Außenwirkung einer ohnehin angeschlagenen Fiat-Währung weiteren Schaden zu und erhöhen so die Attraktivität jeglicher Alternative, ob es nun Gold oder auch ein digitales Asset ist.

Eine weitere Möglichkeit staatlicher Eingriffe besteht in der Kontrolle und Regulierung von Börsen und bilateralen Handelsplätzen. Diese ist bei zentralen Organisationen

24 Siehe Brown (2019).
25 Siehe Taaki (2018).

leicht zu implementieren und durch bekannte Ziele wie der Verhinderung von Geldwäsche nachvollziehbar zu argumentieren. Ein generelles Verbot solcher Plattformen wäre hingegen kontraproduktiv, denn wie beim netzbasierten Tausch von Videos und Musikdateien haben sich auch im Segment der Kryptoassets schon jetzt eine Vielzahl von Peer-to-Peer Netzwerken etabliert, die sich auf Grund der dezentralen Organisation nicht zerstören lassen.[26]

Dennoch würde ein solcher Eingriff den Eintritt neuer Anleger und den Kapitalzufluss von außen deutlich behindern. Dies würde in den betroffenen Regionen zu einer Verlagerung des Erwerbs von Kryptoassets auf intransparentere Kanäle führen. Die Folgen wären Preisaufschläge, die die Anleger in bestimmten Ländern aufzubringen hätten. In Argentinien, Indien oder Venezuela ist dadurch bereits die Prämie für Bitcoin gestiegen. Das von einer solchen Vorgehensweise ausgehende Signal der ökonomischen Schwäche dürfte spürbare Schäden an der Reputation des betreffenden Landes verursachen. Die erwähnten Auswirkungen sind nicht theoretischer Natur. Sie lassen sich auch auf dem Goldmarkt beobachten.

Was aber ist der beste Weg für Staaten mit einem funktionierenden Rechtssystem? Schon um die Kontrolle nicht vollends aus der Hand zu geben, ist eine Regulierung sinnvoll. Dabei sollte das Ziel nicht die Verhinderung neuer Möglichkeiten sein, sondern die Schaffung eines verlässlichen, konsistenten und dauerhaften Rechtsrahmens, innerhalb dessen die Investoren eigenverantwortlich agieren können.

In Deutschland hat die Bundesregierung eine den Handel mit Kryptoassets betreffende Gesetzesnovelle beschlossen. Banken und Start-ups erhalten fortan mehr Rechtssicherheit, wenn sie den Handel mit Kryptowährungen anbieten. In den Vereinigten Staaten wurde Banken zugestanden, Kryptowährungen zu verwahren. Auch die EU stellte einen Vorschlag zur Regulierung von Kryptowährungen vor. Diese Beispiele weisen den Weg und der führt nicht in Richtung eines Verbots.

Das wahrscheinlichste Szenario ist eine fortschreitende Integration digitaler Assets in das bestehende System mit dem Ziel der Schaffung rechtlicher Klarheit für alle Beteiligten. Emittenten, Dienstleister und Handelsplätze müssen ihrer Informationspflicht nachkommen. Anleger müssen sich darauf verlassen können. Die neu entstehende Regulierung digitaler Assets wird sich am bereits bestehenden Rechtsrahmen der klassischen Kapitalmärkte orientieren. Puristen mögen den Verlust an Freiheit beklagen, jedoch bringt nur die Rechtssicherheit auch die Möglichkeit mit sich, Marktmanipulationen oder Insiderhandel zukünftig rechtlich zu ahnden.

Die Voraussetzung für eine steigende Adoption von Bitcoin & Co. ist mehr Kapital. In nennenswertem Umfang kann dies nur von institutionellen Anlegern stammen. Damit diese sich überhaupt für das Thema erwärmen können, ist die Schaffung regulatorischer Sicherheit die notwendige Voraussetzung. Eine konstruktive Regulierung ist

26 Ein gutes Beispiel sind die Filesharing-Plattformen wie BitTorrent (Alderman, 2001).

eher das Ende des »Wilden Westens« als das Ende der Welt. Für den Handel mit Kryptowährungen sollte die wachsende Rechtssicherheit einen deutlichen Vertrauensschub auslösen und neue Anlegerklassen erschließen.

Von einem Verbot der Kryptoassets sind wir weit entfernt. Die größte Gefahr für die zunehmende Akzeptanz ist eine langfristig ausgerichtete, politisch unabhängige und auf Geldwertstabilität ausgerichtete Geldpolitik. Danach sieht es momentan nicht aus.

Bitcoin kann abgeschaltet werden

Die Betriebszeit von Bitcoin seit seiner Entstehung am 3. Januar 2009 beträgt 99,985 %.[27] Damit ist das dezentrale System mit seinen mehr als 10 000 full nodes in mehr als 96 Ländern eines der stabilsten Netzwerke überhaupt. Auf Grund der dezentralen Konstruktion lässt sich das Netz nicht einfach abschalten. Es gibt genau zwei Wege, das Netzwerk zu stoppen. Der eine Weg ist die Zerstörung des Internets. Angesichts der ebenfalls dezentralen Natur dieses Netzes ein hoffnungsloses Unterfangen. Da Bitcoin kaum Bandbreite benötigt, ist die Kommunikation auch über Radiowellen oder das Telefonnetz problemlos möglich. Auch wurden schon erste Satelliten ins All geschossen, um das Netzwerk noch robuster zu machen. Das Start-up Blockstream hat bereits sechs Satelliten angemietet, die die ganze Welt abdecken. So sind auch Nodes in ländlichen Gegenden denkbar, die bislang keinen Netzwerkzugang hatten.[28]

Die zweite Möglichkeit, das Netzwerk zu zerstören, liegt in der Löschung sämtlicher full nodes und aller gespeicherten Transaktionshistorien. Auch dieser Weg ist nicht erfolgversprechend.

Bitcoin wird kopiert

Bitcoin ist Open-Source-Software. Jeder kann den Code einsehen, nutzen und verändern. Warum nicht einfach Bitcoin kopieren und die eigene Bitcoin-Blockchain gründen? Diese Frage hat sich schon mancher gestellt und das Vorhaben in die Tat umgesetzt. So einfach die technische Umsetzung ist, so schwierig gestaltet sich das Vorhaben, Nutzer für die neue Plattform zu gewinnen. Warum sollte jemand das kopierte Asset nutzen, und warum sollte jemand Rechenkapazitäten für das Mining bereitstellen, wenn die Belohnung in Coins ausgezahlt wird, die weder von vielen akzeptiert werden noch besondere Merkmale aufweisen, die diesen Zustand ändern könnten?

Dennoch gab es schon zahlreiche Abspaltungen von der Bitcoin-Blockchain, die als *Forks* bezeichnet werden. Der Begriff Fork kommt aus dem Englischen und bedeutet Gabel oder Gabelung. In der Softwareentwicklung ist ein Fork eine Aufspaltung des

27 Es gab lediglich zwei Unterbrechungen von wenigen Stunden, die auf einen Softwarefehler zurückzuführen waren. Beide Unterbrechungen wurden in der Community über Konsensus gelöst, ohne dass ein Schaden für die Teilnehmer entstanden ist. Mehr Details unter Bitcoin Uptime Tracker (2021).

28 Eine Übersicht finden Sie unter »Blockstream Satellite« (2020).

Pfads eines Projekts. Eine Version wird in Richtung A weiterentwickelt, die andere in Richtung B. Wenn Richtung A das ursprüngliche Projekt bzw. die ursprüngliche Blockchain repräsentiert, wird der Abzweig in Richtung B als *Fork von A* bezeichnet. Dieses neue Projekt baut auf einer exakten Kopie des ursprünglichen Quellcodes auf, der dann modifiziert wird.[29]

Ist die Abwärtskompatibilität einer ursprünglichen Blockchain mit einem Fork gegeben, spricht man von einem soft fork, andernfalls von einem hard fork. Ein Beispiel für einen soft fork ist die Protokollerweiterung Segregated Witness (SegWit) zur Verbesserung der Skalierbarkeit des Netzwerks. Einer der nach wie vor bekanntesten Bitcon hard forks war die Abspaltung von Bitcoin Cash (BCH) im Jahr 2017, die aus einer Veränderung der Blockgröße resultierte. Die Original-Bitcoin-Blockchain blieb erhalten und das Netzwerk lief wie gewohnt weiter. Bitcoin Cash fing als neue Kryptowährung an. Im Zuge des hard fork erhielt jeder Bitcoin Besitzer zusätzlich einen Bitcoin Cash.

Es folgten weitere hard forks und auch Bitcoin Cash war betroffen. Bereits kurz nach seiner Entstehung entstand Bitcoin Satoshi Vision (BSV). Im Oktober 2017 folgte Bitcoin Gold (BTG). Geschadet haben diese Forks dem Bitcoin nicht, denn abgesehen vom klaren Use Case und der sehr hohen Sicherheit des Bitcoin wirkt sich auch der Netzwerkeffekt aus. Dinge, die von vielen Menschen genutzt werden, haben stets einen Vorteil gegenüber Neuankömmlingen. Das ganze Bitcoin-Ökosystem muss sich bei einem Fork für eine Richtung entscheiden und in der Regel fällt diese Wahl auf die längste Blockchain. Wenn ein Miner auf die neue Chain wechselt, muss er sich sicher sein, die neuen Coins zu einem ausreichend hohen Preis verkaufen zu können. Dazu benötigt er eine Börse und diese wird den Handel mit dem neuen Coin nur dann anbieten, wenn es ausreichend Marktteilnehmer gibt. Die gleichen Überlegungen stellen auch Händler und die Anbieter von Wallet Software an. Es ist daher nicht leicht, ein funktionierendes Ökosystem von einem Fork zu überzeugen. Der neue Coin muss maßgebliche Vorteile bieten und die ökonomischen Interessen der Teilnehmer müssen gewahrt sein. Wenn sich jedoch alle über die Vorteilhaftigkeit eines Entwicklungsschritt einig sind, dann gibt es keinen Anlass für die Abspaltung einer neuen Blockchain. In diesem Fall kann die entsprechende Protokollanpassung im Rahmen des normalen evolutionären Verbesserungsprozess der Software durchgeführt werden.

Fazit: Die Geschichte schreitet voran

Für den einen ist der Bitcoin digitales Gold. Für den nächsten ist es eine Möglichkeit, sein Geld vor zunehmenden übergriffigen Regierungen zu schützen. Es ist ein Zahlungssystem und ein Spekulationsobjekt. Es ist ein Finanzinstrument, eine Währung, ein Vermögenswert, ein Tauschmittel, eine Rechnungseinheit, ein Wertaufbewahrungsmittel, ein Netzwerk und ein Abrechnungssystem.

29 Siehe Schär/Berentsen (2017).

Vor allem die rasante Weiterentwicklung des Systems ist beeindruckend. Allein wegen der dynamischen Entwicklungen im Bereich der Dezentralisierung von Finanzdienstleistungen wächst die Zahl der Regierungen und Unternehmen, die sich ernsthaft mit Kryptoassets auseinandersetzen. Die über Jahre herrschende Skepsis und das weit verbreitete Unverständnis weichen einer zunehmenden Aufgeschlossenheit. Das hat wichtige Konsequenzen für Investoren, auf die wir im Verlauf dieses Buches eingehen werden.

Viele Gegenargumente bewegen sich auf dem Niveau von Aussagen wie »Gold zahlt keine Zinsen«, einer Aussage, die in einem Umfeld negativ rentierlicher Zinspapiere etwas aus der Zeit gefallen wirkt. Investoren, die sich Gedanken um ihre Asset-Allokation machen, sollten derartige Plattitüden beiseiteschieben, die Chancen und Risiken der neuen Assetklasse im Vergleich zu anderen Anlagen bewerten und dann in Ruhe ihre eigenen Schlüsse ziehen.

Experteninterview mit Prof. Dr. Philipp Sandner

Zur Person: Prof. Dr. Philipp Sandner hat das Frankfurt School Blockchain Center (FSBC)[30] gegründet. Von 2018 bis 2020 wurde er von der Frankfurter Allgemeinen Zeitung (FAZ) als einer der »Top 30«-Ökonomen ausgezeichnet. Darüber hinaus gehörte er zu den »Top 40 unter 40«, einem Ranking des Wirtschaftsmagazins Capital. Seit 2017 ist er Mitglied des FinTechRats des Bundesministeriums der Finanzen. Er ist zudem im Verwaltungsrat von Avaloq Ventures und der Blockchain Founders Group, einem Venture-Capital-Investor für Blockchain-Startups.

Die Expertise von Prof. Sandner umfasst die Blockchain-Technologie, Kryptowerte wie Bitcoin und Ethereum, den digitalen programmierbaren Euro, die Tokenisierung von Assets und Rechten sowie die Entwicklungen auf dem Gebiet der digitalen Identität.

Wir haben heute den Experten für Blockchain-Technologie und Kryptowerte zu Gast. Herzlich Willkommen Philipp.

Vielen Dank, dass ich dabei sein kann. Freut mich wirklich sehr.

Satoshi Nakamoto spricht in seinem Whitepaper von einem Peer-to-Peer Electronic Cash System. In letzter Zeit hört man häufiger, dass es sich bei Bitcoin eher um digitales Gold handelt. Was ist Bitcoin für dich, eher eine Währung oder ein Rohstoff?

Also das ist eine Frage, über die man eine ganze Stunde diskutieren könnte. Es gibt ein, zwei wirklich tolle Artikel von einem Autor im Internet, der Plan B heißt. Der hatte die Narrative von Bitcoin analysiert und sagt: Narrative folgen verschiedenen Wellen. Das momentan bekannteste Narrativ ist das vom digitalen Gold. Auch Firmen wie Fidelity sagen beispielsweise, Bitcoin hat die Veranlagung, so zu sein wie Gold.

30 Zur Webseite Frankfurt School of Finance (2021).

Der Bitcoin ist jedoch Stand heute kein digitales Gold, hat aber von der Architektur und Funktionsweise her die Möglichkeit, so zu sein wie Gold. Dementsprechend ist es sinnvoll, Bitcoin mit Gold zu vergleichen. Derzeit entspricht die Marktkapitalisierung des Bitcoin etwa zehn bis elf Prozent des Marktwertes von Gold.

Es gab aber auch schon andere Narrative. Am Anfang stand das Peer-to-Peer Electronic Cash System als Narrativ. Der Begriff »Cash System« suggeriert die Nutzung als Zahlungssystem und ich glaube, dass daraus auch das Wort Cryptocurrency, also Kryptowährung entstanden ist, auch wenn das Wort im inhaltlichen Sinne falsch ist. Man müsste eher Cryptocommodity sagen, also eine Art Rohstoff, oder aber Kryptoasset. Ich glaube, dass damals das Wort Cryptocurrency entstanden ist, war in gewisser Weise ein Missverständnis, weil seitdem alle Leute Kryptowährung sagen. Man denkt direkt an Payment, kann den Bitcoin aber fast nirgendwo zum Bezahlen einsetzen, und deswegen denken viele Leute, dass der Bitcoin fehlgeschlagen ist. Dabei wollte er eigentlich nie unbedingt so sein wie eine Währung, aber das Wort hat sich am Anfang festgesetzt aus dem ersten Narrativ, als es darum ging, einen Prototyp für ein elektronisches Zahlungssystem aufzubauen.

Zwischendurch gab es noch andere Narrative. Zum Beispiel ist Bitcoin vor einigen Jahren die Reservewährung für das Krypto-Ökosystem geworden. Das heißt, mehr als 200 Kryptobörsen verwenden den Bitcoin als Hauptwährung zum Betrieb ihrer Systeme, und rechnen alles gegen den Bitcoin ab. Und es ist natürlich klar, dass ich im laufenden Betrieb bei mehr als 200 Kryptobörsen die Basiswährung nicht einfach mal so auswechseln kann. Das heißt, der Bitcoin ist da drin und der bleibt da drin. Das sorgt für einen Momentum-Effekt und soll das Narrativ der Reservewährung veranschaulichen.

Und dann gibt es natürlich auch noch das Narrativ einer anonymen Darknet-Währung, also einer anonymen bzw. pseudo-anonymen Währung zur Abwicklung von Kriminalitätsfinanzierung. Viele Leute hängen diesem Narrativ noch nach, wobei es weniger werden. Das heißt, vor einem Jahr war dieses Narrativ noch sehr dominant, inzwischen aber fangen die Leute an, sich eher mit dem Narrativ des digitalen Goldes zu beschäftigen.

Nicht nur institutionelle Anleger, sondern auch viele private Anleger sehen die wachsende Bedeutung des Themas ESG. So rückt beim Bitcoin der hohe Energieverbrauch der Mining-Rechner in den Fokus, der oft plakativ mit dem Stromverbrauch kleinerer Länder verglichen wird. Wie ist dieser Energieverbrauch zu rechtfertigen, der ja vor allem durch den Proof of Work-Algorithmus verursacht wird?

Es macht aus meiner Sicht wenig Sinn, die Stromkosten pro Transaktion zu berechnen, denn das ist eine unfaire Metrik. Man muss das Thema Stromverbrauch eigentlich aus dem Blickwinkel sehen, dass es erforderlich ist zur Sicherung des Netzwerks. Und dann muss man betrachten, wie viel Geld in diesem Netzwerk bewegt wird. Das sind teilweise hunderte Milliarden Euro pro Woche. Und dann muss ich mir den Stromverbrauch pro bewegtem Euro anschauen und von der Anzahl der Transaktionen abstrahieren. Das wäre die erste Maßnahme, die Berechnung anzupassen.

Wichtiger aber als die Frage, wie viel Strom wird verbraucht, ist aus meiner Sicht die Frage, woher denn der Strom kommt, der hier verbraucht wird. Ist es Atomenergie, ist es das Verbrennen von Öl und Gas, Kohle, oder sind es erneuerbare Energien, die hier Einsatz finden? Und wenn man hier ein bisschen tiefer gräbt, und das machen die meisten Leute eben leider nicht, gelangt man zum Ergebnis, dass der Bitcoin eigentlich immer dann profitabel erzeugt und geschürft werden kann, wenn der eingesetzte Strom sehr günstig ist. Und welcher Strom ist vom Profil her sehr günstig? Ganz einfach: Der Strom, der aus Wasserkraft und Solarkraft kommt, teilweise auch Nuklearstrom. Das ist vom Profil her der günstigste Strom und je tiefer der Preis geht, desto profitabler ist das Mining. Und das erklärt auch, dass das Bitcoin-Netzwerk eigentlich von der Tendenz her einen Hang haben sollte, zunehmend mehr erneuerbare Energien zu unterstützen und zu konsumieren, weil in diesem Segment das günstige Strompreisprofil entsteht. Das erklärt, dass es wegen des Themas Solarstrom viel Mining in Texas gibt und warum es viel Mining in Nordeuropa gibt. Dort geht es um Strom aus Wasserkraft und teilweise aus erneuerbaren Energien.

Auch bei konventionellen Energieträgern spielen die Kosten eine wichtige Rolle. Bei der Stromerzeugung in China etwa sind vielfach konventionelle Kraftwerke im Einsatz, die mit Öl, Gas und Kohle betrieben werden. Diese Kraftwerke sind bereits abgeschrieben und so wird der Strompreis nicht durch Abschreibungskosten verteuert. Man muss überlegen, welcher Strom wird eigentlich genutzt? Ist es erneuerbarer Strom oder ist es Strom aus fossilen Energien? Und dann muss man die Sache nochmal neu bewerten. Ich sage nicht, dass es dadurch gut wird, denn der Stromverbrauch ist sehr unschön und bleibt auch sehr unschön. Aber die Frage kann nur dann sinnvoll beantwortet werden, wenn man beachtet, dass die benötigte Energie nicht nur aus der Verbrennung von Öl und Kohle stammt.

Die meisten Beobachter setzen Bitcoin Mining automatisch mit China und der Energieerzeugung aus Kohle gleich. Kann man ungefähr beziffern, wie hoch der Anteil an regenerativen Energiequellen ist bei Bitcoin?

Dies ist sehr schwierig zu schätzen, weil die Mining-Anlagen nicht systematisch auf der Landkarte festgehalten werden. Aber die Schätzungen Stand heute sehen den Anteil erneuerbarer Energien am Bitcoin Mining in der Spanne zwischen 60 und 75 Prozent.

Das ist ein spannendes Thema vor allem aufgrund der Mobilität der Mining-Kapazitäten. Im Vergleich zum Unternehmen Google, das seine Rechenzentren gerne auch in der Nähe von Wasserkraftwerken platziert, ist die Mobilität des Minings enorm. Im Grunde kann das Mining den sauberen Energiequellen hinterher wandern, wenn man sie im eigenen Land nicht hat, und ich glaube, das ist auf globaler Ebene bereits sichtbar. Das heißt, diese Technologie hat in der Tat einen Hang zur Nutzung des günstigsten Stroms, weil der Energieverbrauch der größte Kostentreiber für die Miner ist.

Ganz genau, richtig. Das Bitcoin Mining tendiert definitiv zum niedrigsten Strompreis, wo auch immer der herkommt. In Zukunft wird sich zeigen, ob tatsächlich die erneuerbaren Energien den günstigsten Strom liefern. Wenn dem so sein sollte, müsste der

Bitcoin in einigen Jahren noch etwas grüner geworden sein und der Anteil des konventionell erzeugten Stroms sollte zurückgegangen sein. Man kann dies heute nur hoffen und selbst dann bleibt fairerweise die Frage offen, ob der Strom, der hier konsumiert wird, nicht anderswo besser eingesetzt werden könnte. Auch das muss man beurteilen und man sieht schnell, da wird es komplex.

Es wird erst recht komplex, wenn man überlegt, dass auch Goldminen als Förderer von Gold, Silber und Platin Ressourcen aufwenden und zwar ein Vielfaches mehr als die Bitcoin Miner. Allerdings ist es nicht so wunderschön darstellbar. So kommen bei der Goldförderung Chemikalien zum Einsatz, es werden Dieselgeneratoren, Bagger und schweres Gerät eingesetzt und natürlich wird auch Strom verbraucht. Auch das muss man berücksichtigen, wenn man den Stromkonsum von Bitcoin so plakativ verurteilt.

Kommen wir zurück zum Thema ESG. Derzeit wird über die mögliche Auflage eines ESG-orientierten Gold-ETF berichtet. Die Kryptoanleger warten ja zunächst noch auf die ersten Bitcoin-ETFs, aber kannst du dir perspektivisch auch ein ESG-Produkt für den Bitcoin vorstellen?

Das ist ein spannendes Feld, und zwar deswegen, weil das Thema Goldschürfen natürlich auch mit Umweltverschmutzung einhergeht. Die Frage ist, ob bei der Stromerzeugung für die Mine Diesel oder die Solarzelle zum Einsatz kommt. Jetzt gibt es erste Fonds, die nur dann in Goldminen investieren, wenn diese Unternehmen dort, wo es möglich ist, nachweisbar nachhaltig wirtschaften. Plastisch gesprochen geht es um die Frage, ob die Solarzelle und nicht der Dieselmotor irgendwo in irgendwelchen abgelegenen Gebieten in den Anden zum Einsatz kommt. Die Investoren zahlen eine Preisprämie dafür, dass sie sichergehen können, dass hier zwar Gold geschürft wird, aber so nachhaltig, wie es eben noch geht.

Und die Übertragung auf den Bitcoin ist sicherlich nicht schlecht. Ich bin gespannt, ob es so etwas in ein, zwei Jahren geben wird, und ich würde behaupten: ja. Die Analogie wäre, dass es Bitcoin-Mininganlagen gibt, die nachweisen können, dass der von ihnen konsumierte Strom wirklich zu 100 Prozent aus Wasserkraft oder Solaranlagen stammt und möglichst nichts verschwendet wird. Es wäre eigentlich logisch, so einen Green Bitcoin-ETF oder ein Anlageprodukt dieser Art aufzulegen. Aber vielleicht ist die Zeit noch nicht reif. Vielleicht braucht es einfach noch Zeit, weil der gesamte Bitcoin-Markt sich erst noch weiter professionalisieren muss.

Es gibt Alternativen zum reinen Proof-of-Work-Ansatz, den wir vom Bitcoin kennen. Ein Beispiel ist eine hybride Variante, wie etwa beim Decred, sprich eine Kombination aus Proof-of-Work und Proof-of-Stake. Erhöht die Diskussion um den Energieverbrauch die Chancen derartiger Ansätze oder denkst du, dass der Bitcoin auch in Zukunft das Asset der Wahl bleibt?

Meine persönliche Meinung, aber die kann natürlich falsch sein, ist folgende: Der Bitcoin ist seit Anbeginn der Kryptowährungen immer auf Position eins und ich kann beim besten Willen nicht erkennen, warum er nicht auf Position eins sein sollte.

Und zwar deswegen, weil er aus vielerlei Gründen das Schlachtross des Krypto-Ökosystems ist. Und Ethereum ist die Kryptowährung Nummer zwei, war sehr lange die Nummer zwei, und ich glaube, dass es weiterhin die Nummer zwei sein kann. Ethereum ist dabei, den Sprung von Proof-of-Work zu Proof-of-Stake zu schaffen. Warum? Weil Ethereum auf Grund der gesamten Governance eher updatefähig ist. Bei Bitcoin ist die Governance anders, sehr viel behäbiger und deswegen ist es bei Bitcoin nahezu unmöglich, signifikante Updates einzuspielen. Es gab einige, aber dass Updates eingespielt werden, die die Netzwerksicherheit gefährden, wie es bei einem Update hin zu Proof-of-Stake der Fall wäre, kann ich mir momentan nicht vorstellen. Und deswegen glaube ich, dass der Proof-of-Work-Konsensmechanismus beim Bitcoin erhalten bleiben wird und damit auch das Problem des Stromverbrauchs. Bei anderen Kryptowährungen allerdings wird es anders sein, siehe Ethereum. Da ist eine gewisse Updatefähigkeit gegeben und daher ist ein solches Netzwerk dazu in der Lage, sich quasi selbst zu überholen. Ethereum 2.0 wäre die neue Version von Ethereum, die dann auf einem anderen Konsensmechanismus basiert.

Eine Frage noch zum Schluss: Wenn unsere Leser deine Arbeit verfolgen wollen, wie können sie das am besten tun?

Ach, ich glaube, ganz gut funktioniert eigentlich LinkedIn, Twitter oder die gute, alte E-Mail. Alles, was elektronisch ist eigentlich.

LinkedIn: https://www.linkedin.com/in/philippsandner/

Twitter: https://twitter.com/philippsandner

Philipp, herzlichen Dank für deine Zeit und danke für das Interview.

Super gerne. Freut mich sehr und danke, dass ihr das Thema so tiefgründig unter die Lupe nehmt.

Stichwortverzeichnis