30 Köpfe
Dreißig Perspektiven
zu Bitcoin & Blockchain

Texte von der Blockchain Community für die Community.

Ein Taschenbuch für alle Blockchain-Interessierte.

Version: v0.2

Ein Projekt von chainist.de

Vorwort

Schön. Schön, dass du dieses e-Book schon mal aufgemacht hast und angefangen hast zu lesen. Bitcoin und Blockchain sind kontrovers. Es gibt Wissende, Halbwissende und Bullshit-Wisser. Egal ob du Neuling bist und das Thema gerade erst erkundest oder dich selbst Vollprofi nennst. Um die Spreu von Weizen zu unterscheiden, musst du viel lesen, das Thema nah verfolgen, um am Ball zu bleiben. Und idealerweise auch selbst etwas damit gemacht haben. So hat meine Reise in die Bitcoin und Blockchain-Welt angefangen und wie es aussieht, wird die Reise noch eine Ewigkeit andauern.

Warum gibt es dieses Buch? Einen Blogbeitrag zur Idee und dem Warum findest du hier http://bit.ly/dltebook.

Achso, wer bin ich? Mein Name ist Trí Nhân Vũ und mache Dinge offline und online. Bloggen, programmieren, designen und bin Vater von zwei tollen Kindern und habe eine super Frau, die mich manchmal positiv zur Weißglut bringt ;). Das ist die Kurzform. Eine Langform findest du hier.

Was erwartet dich in diesem e-Book?
Du bekommst verschiedene persönliche, unzensierte Meinungen und Texte zu Bitcoin und Blockchain. Alle Texte wurde in Abstimmung mit den Co-Autoren erstellt. Das Buch ist ein „lebendes" Buch. Kontinuierlich werde ich mit neuen Co-Autoren das Buch erweitern bis wir 30 Co-Autoren erreicht haben. Danach sehen wir weiter. Viel Spaß beim Lesen!

Wenn du die Texte liest, bleibe kritisch. Es handeln sich um *persönliche Meinungen und Perspektiven*. Nutze dieses e-Book, um in die Welt von Kryptowährungen und Distributed Ledger Technologien einzutauchen. Für Neulinge dienen die Texte als Einstieg, für Bitcoin Maximalisten und Blockchain Oldtimern dient es seinen eigenen Horizont zu erweitern.

„Der Kluge lernt aus allem und von jedem, der Normale aus seinen Erfahrungen und der Dumme weiß alles besser." (Sokrates)

Die Texte der Co-Autoren habe ich gegengelesen. Da ich kein professioneller Lektor bin, gehe ich davon aus, dass in den Texten Satzzeichen- und Grammatik-Fehler vorkommen. Verbesserungen können im Google Doc als Kommentar hinterlegt werden. Das wäre der einfachste und schnellste Weg Verbesserungsvorschläge zu geben, um diese in die nächsten Versionen einzuarbeiten. Chapeau jetzt schon an alle Crowd-Korrekturleser!

So, jetzt geht es aber wirklich los!

– ✻ –

Dominik Weil

Ich halte „Blockchain" im Großen und Ganzen für einen maßlos „overhyped" und verwässerten Begriff.

Wenn jemand mir sein „Blockchain Projekt" vorstellen oder mich zu einer „Blockchain Konferenz" einladen möchte, winke ich persönlich in der Regel augenrollend ab. Es gibt dabei bestimmte Ausnahmen wo der Begriff aus „strategischen Gründen" verwendet werden muss, weil „Bitcoin" auf der „bad word list" steht und man mitunter taktisch vorgehen muss, um seine Message unterzubringen.

Die Popularisierung des Begriffes „Blockchain" fand runds ums das Jahr 2015 statt; damals durchaus auch von vielen „Original Bitcoinern" geduldet, um die ansteigende Aufmerksamkeit der globalen regulatorischen Agenturen durch einen Haufen „Techno Babble" zu verwirren und um ihnen weiß zu machen, dass dort in diesem Bereich großartige Innovationspotenziale vorliegen. Man möge daher doch bitte vorsichtig und bedacht vorgehen, bevor man mit der regulatorischen Keule das kleine Pflänzlein „Blockchain" zerschlägt und man sich den Schritt zur Teilhabe an den Möglichkeiten, die durch diese technische Innovation entstehen frühzeitig verbaut.

Diese „Innovationspotenziale" sind in der Tat vorhanden – und ich glaube nach wie vor, dass Bitcoin und vielerlei Dinge die drumherum stattfinden eine der der wichtigsten technischen Errungenschaften des 21.

Jahrhunderts darstellt und darstellen wird.

Die Krux an der Sache ist lediglich: Bitcoin greift fundamental einer der Basisbausteine zentralisierter, staatlicher Macht an, welche es der jeweiligen Herrscherklasse ermöglicht auf Kosten ihrer Untertanen allerlei unsinnige, kostspielige und wohlstandszerstörende Projekte zu unternehmen. Während sie zugleich auf Grund der systematischen Vorteile die ein zentralisiertes Fiat-Geldsystem ermöglicht ihre eigene Macht und Einfluß nahezu unbegrenzt mehren können.

Die Zeche bezahlt seit jeher der „einfache Bürger", welcher fast keinerlei Chance hatte diesem parasitären System der monetären Ausbeutung durch die Hintertüre (und immer öfter auch ganz offen und frei durch die Fronttüre!) zu entkommen.

Bitcoin ändert dies und verschiebt die Machtbalance zurück zum Individuum – und „the powers that be" sind „not amused".

Und während der Begriff „Blockchain" eine Weile seinen Dienst verrichtete, um als „trojanisches Pferd" Zeit zu erkaufen und Bitcoin in der Zwischenzeit größer, stärker und ultimativ schwieriger „zu vernichten" werden zu lassen; sah die „Consulting" Industrie als auch in Folge zahllose Tech-Startup Gründer im konfusen Begriff „Blockchain" eine formidable Möglichkeit mit ziellosem, futuristischem Techno Babble dicke Gagen aus der „Corporate World" einzustreichen (im Allgemeinen mehr eine PR-Ausgabe, um sich selbst als innovativ und „cutting edge" gegenüber der Öffentlichkeit und den Shareholders zu präsentieren) oder aber noch dickere Schecks fürs „Blockchain Startup Funding" zu kassieren. Da die meisten Investoren auch keine wirkliche Ahnung zum

Thema „Blockchain" hatten und nur NPC-like die leeren, aber verheißungsvoll klingenden Sprechblasen anderer „Blockchain thought leaders" wiederholten und dementsprechende „FOMO" in der Investoren-Community einsetzte („All die anderen Leute in meiner Branche haben 'Blockchain' in ihrem Portfolio ↠ Wir müssen auch in 'Blockchain' investieren!„) ein ultimativ sehr lohnender Schachzug für viele der „Blockchain Project" Gründer rund um das Jahr 2017.

„Everybody got to make a living" – fair enough. Aber diese Umtriebe sind definitiv nicht, was mich dazu bewegte in 2013 zu entscheiden meinen regulären Job an den Nagel zu hängen (was dann ein Jahr später in 2014 in die Tat umgesetzt wurde) und ein Großteil meiner Zeit seitdem dem Thema Bitcoin zu widmen.

Leseempfehlung: „Denationalisation of Money: The Argument Refined" – Friedrich A. von Hayek

Über Dominik Weil

Twitter | LinkedIn | Facebook

Aufgewachsen in Frankfurt am Main; seit 6 Jahren in Vietnam's wirtschaftlichem Zentrum Ho Chi Minh Stadt („Saigon„) lebend. Freund der österreichischen Schule der Nationalökonomie. Gegen Ende 2012 von „Bitcoin" infiziert worden. Im Sommer 2013 Mitbegründer der Frankfurter Bitcoin Community. Ende 2013 Mitgründer des ersten und ältesten Bitcoin Exchange Services in Vietnam; BitcoinVN.

– ✻ –

Marius van der Wijden

Verteilte Systeme, Systeme die aus mehreren Computern bestehen, gab es schon seit mehreren Jahrzehnten. Beispielsweise verteilt Google alle Suchanfragen auf viele verschieden Server, um möglichst schnell und redundant zu sein. Sollte ein Server im Google-Netzwerk ausfallen, können andere für ihn einspringen. Diese verteilten Systeme hatten allerdings einen großen Nachteil, sie sind „permissioned", d.h. nur authentifizierte Server können ihnen beitreten. *Aber wieso?*

Nehmen wir folgendes Szenario an:

Alice besitzt 5 Bitcoins. Sie schickt an einen Computer im Netzwerk die folgende Nachricht „Alice sendet 4 Bitcoins an Bob". Gleichzeitig schickt sie an einen anderen Computer die Nachricht „Alice sendet 4 Bitcoins an Charlie". Da Alice nur 5 Bitcoins hat, können nicht beide Transaktionen ausgeführt werden.

Nun kommt es zwischen den beiden Computern zu einem Problem, sie müssen sich entscheiden welche der beiden Transaktionen ausgeführt werden soll. Sie können andere Computer im Netzwerk fragen welche Transaktion zuerst ankam. Da Charlie allerdings Computer im Netzwerk simulieren kann, könnte er die Abstimmung beeinflussen, indem er neue Fake-Identitäten im Netzwerk etabliert.

In „permissioned" Netzwerken wird dieses Problem gelöst, indem alle Parteien die abstimmen können, bekannt sind. Allerdings ist es dabei nicht mehr möglich anonym dem Netzwerk beizutreten oder auszutreten. Es gibt auch Systeme in denen es eine „Master-Node" gibt, einen Computer der alle Entscheidungen trifft. Beide Ansätze sind nicht dezentral und nicht anonym.

Nakamoto-Style Konsensus löst dieses Problem durch den Proof-of-Work (PoW). Hierbei stimmen Nutzer sozusagen mit ihrer Rechenleistung ab. Wird ein Block an Transaktionen generiert, ergibt sich daraus ein Rätsel. Dieses Rätsel wird schwerer je mehr Rechenleistung im Netzwerk verfügbar ist. Das Rätsel hat keine eindeutige Lösung, der Rechner der die erste akzeptable Lösung findet, gewinnt und bekommt ein Entgelt (Mining-Reward). Werden zwei Lösungen parallel gefunden, wird die schwerer zu berechnende Lösung genommen. Dieser Prozess wird auch Mining genannt, da hierbei neue Bitcoins erstellt werden.

Ein Computer mit mehr Rechenleistung hat eine höhere Chance der erste zu sein, der eine akzeptable Lösung findet. Würde Charlie in unserem Beispiel jetzt das Netzwerk beeinflussen wollen, müsste er viel Geld investieren um Hardware zu kaufen, um diese Rätsel zu lösen.

Bei Bitcoin wird davon ausgegangen, dass keine einzelne Person mehr als 50% der Rechenleistung des Netzwerkes kontrollieren kann. Wird diese Annahme (auch honest-majority assumption genannt) verletzt, könnte Charlie auch die Vergangenheit umschreiben, indem er bessere Lösungen für alte Blöcke entwickelt. Auch wird davon ausgegangen, dass jemand der viel Hardware gekauft hat um Bitcoin zu minen und viel Strom

investiert hat, kein Interesse daran hat Bitcoin zu zerstören, da damit seine Investitionen wertlos werden würden.

Dieses System erlaubt es neuen Rechnern Teil des Netzwerkes zu werden und an Abstimmungen teilzunehmen ohne ihre Identität preisgeben zu müssen. Durch den Mining-Reward ist ein Anreiz geschaffen worden um mehr Rechenleistung für das Netzwerk zur Verfügung zu stellen. Pro Block werden zurzeit etwa 80.000€ ausgeschüttet. Allerdings hat dieses System auch Nachteile.

Da sehr viele Firmen Bitcoin Mining betreiben, ist es als Privatmensch fast unmöglich einen Block zu generieren. Um ihre Rechenleistung trotzdem beizusteuern, treten die meisten Miner in sogenannte Pools ein. In Mining-Pools arbeiten alle Rechner an dem gleichen Rätsel. Findet ein Miner die Lösung wird der Gewinn auf alle Miner im Pool verteilt. Dies hat den Nachteil, dass die Betreiber der Mining-Pools viel Macht besitzen. Somit sind Mining-Pools wieder ein zentralisiertes Element in dem dezentralen System, das zum potentiellen Angriffspunkt wird.

Ein weiteres Problem ist der hohe Stromverbrauch des ganzen Systems. Die gesamte Rechenleistung geht verloren, da am Ende nur eine einzige Lösung für das Rätsel Bestand hat.

Bitcoin verbraucht momentan etwa 73 TW/h im Jahr, somit etwa genau so viel wie Österreich. Umgerechnet auf Transaktionen sind das etwa 671 KW/h für jede einzelne Transaktion. Dies ist etwa ein Sechstel des Jahresverbrauchs einer dreiköpfigen Familie.

Um dieses System effizienter zu machen, sind sogenannte Off-Chain Technologien entwickelt worden (wie etwa das Lightning Netzwerk), die mehr Transaktionen zusammenfassen können.

Über Marius van der Wijden

Twitter | LinkedIn | GitHub

Ich beschäftige mich mit der Skalierbarkeit der Blockchain durch Off-Chain Techniken mit dem Schwerpunkt auf Payment und State Channels. Des weiteren arbeite ich an diversen Open Source Projekten im Bereich Blockchain mit, unter anderem auch bei Ethminer, der Open Source Mining Software für Ethereum. Ich konzeptionierte auch eine eigene Kryptowährung, die auf Festplattenspeicher nicht reiner Rechenleistung basiert und somit weitaus energiesparender wäre als bestehende Währungen.

– ✻ –

Severin Schell

„Blockchain, aber ohne Cryptowährungen!„

„Blockchain macht Daten praktisch unveränderbar„[1]

Diese oder ähnliche Sätze, sind euch sicherlich schon häufiger begegnet. Leider entspringen diese Sätze aus dem vollkommen falschen Narrativ. Sie reduzieren das System einer Cryptowährung auf lediglich einen Bestandteil: auf die Blockchain.

Die Blockchain ist nichts anderes als eine Datenbank mit Zeitstempeln (im Bezug auf Bitcoin auch gerne als Timechain bezeichnet), die den vorangegangen Stand ihres Inhaltes in jedem neuen Block referenziert und somit das willkürliche austauschen vorangegangener Blöcke (oder ändern deren Inhalt) sofort auffliegen lassen würde. Dies bedeutet, man kann sehr wohl Daten ändern, man muss nur die nachfolgenden Blöcke wieder dementsprechend anpassen. Bei Cryptowährungen wie bspw. dem Bitcoin wird dies durch ökonomische und spieltheoretische technische Implementierungen so stark erschwert, dass der Gewinn den ein Angreifer einfahren könnte geringer ausfallen würde – als wenn er sich dem System gegenüber wohlgesonnen verhält und somit direkt profitiert.

Gleichzeitig lebt das System davon, dass es selbst für seinen Fortbestand bezahlt (in Form eines virtuellen Assets), von jedem vollständig

[1] Quelle: BSI für Bürger

auditierbar ist und jeder Teilnehmer des Netzwerkes derart unabhängig ist, dass selbst ein Ausfall aller anderen Netzwerkteilnehmer nicht die Anwendbarkeit und die Datenintegrität des eigenen Knoten beeinträchtigen würde.

Wenn heutzutage über "Blockchain" gesprochen wird, blenden viele Leute die genannten Aspekte aus. Sie verstehen jedoch nicht, dass dadurch auch die beworbenen Vorteile verschwinden:

1. Dezentralität
2. Zensurresistenz
3. Offene Nachvollziehbarkeit der Integrität
4. Neutralität gegenüber den Inhalten
5. Keine Notwendigkeit jemandem zu vertrauen
6. Keine Notwendigkeit um Erlaubnis zu fragen
7. Die größtmögliche Ausfallsicherheit

Denn: Ohne den Wettbewerb um ein natives Asset (bspw. Bitcoin), welcher über einen Konsens-Mechanismus (Proof Of Work, Proof Of Stake) realisiert wird, gibt es keine echte Dezentralität und somit entfallen auch die anderen oben genannten Aspekte.

Kann eine Blockchain auch außerhalb von Cryptowährung angewendet werden?

Selbstverständlich gibt es auch Anwendungsfälle für eine Blockchain außerhalb der Funktion als Währung, wichtig ist hierbei jedoch zu verstehen, dass wenn die Blockchain als "unveränderbare Datenbank" (immutable Ledger) genutzt wird, dieser Ledger auch nur so sicher ist wie seine "Währung" – sein natives Asset.

Dieses native Asset – im Falle von Bitcoin: BTC, im Falle von Ethereum: ETH, ... sichert die Blockchain dadurch, dass durch die Belohnung (Coinbase-Transaktion) mit jedem neu generierten Block, ein spieltheoretischer und ökonomischer Anreiz geschaffen wird, sich fair und ehrlich zu verhalten.

Da es für jeden Teilnehmer wirtschaftlich sinnvoller ist das Netzwerk positiv zu unterstützen, trägt dies wesentlich zur Sicherheit des Netzwerkes bei. Nur so kann auch sichergestellt werden, dass es sich auch in Zukunft nie lohnen wird die Blockchain wieder auf einen bestimmten Stand zurückzusetzen.

Dieses wesentliche Sicherheitsmerkmal entfällt allerdings bei einer sogenannten privaten Blockchain, da hier kein freier Markt für das native Asset existiert, sofern es überhaupt eines gibt, und daher kann ein solches Projekt auch nicht mit den oben angeführten Kriterien werben (Dezentralität, Zensurresistenz, Neutralität gegenüber den Inhalten, ...).

Wenn man nun auf jene Kriterien keinen Wert legt, dann braucht man wiederum auch keine Blockchain, sondern kann eine effizientere Datenbank verwenden, darf sich umgekehrt aber auch nicht mit den oben genannten Merkmalen schmücken. Wenn ein Kunde bspw. eine Lieferkette, die für Ihn „auf der Blockchain„ nachvollziehbar gespeichert

wurde, nur über ein Web-Frontend des (Software-)Herstellers einsehen kann, und nicht mit einem eigenen Node deren Integrität validieren kann, da Ihm der Zugang zum Netzwerk, der Software, o.ä. verwehrt wird, bleibt das Ergebnis genau so als hätte man im Hintergrund, der Webseite, eine PostgreSQL, MySQL oder andere Datenbank verwendet.

Über Severin Schell

Ich gebe Schulungen und Support rund ums Thema Bitcoin (und bei Bedarf auch anderen Altcoins) und lege meinen Fokus mehr auf die Befähigung des Einzelnen, statt auf die (erneute) Abhängigkeit des Einzelnen von zentralisierten Institutionen.

Twitter | LinkedIn | Webseite

– ✻ –

Tobias Schwarz

Vertrauen 2.0

Die frühen Jahre des Web waren nicht nur geprägt von der Dot-Com-Blase, sondern auch vom Glauben an die frohe Botschaft einer allseits verfügbaren und für alle gleichermaßen zugänglichen, enthierarchisierenden globalen Informations- und Transaktionsstruktur. Die Cyber-Utopien dieser Tage, der Glaube an die Programmierbarkeit einer besseren Welt – das, was der Baseler Soziologe Oliver Nachtwey als „Solutionismus" bezeichnet – hatten nicht selten sogar einen religiösen Einschlag.

Mittlerweile ist diese in der Rückschau etwas naive Hoffnung angesichts der ökonomischen Realität und der gesellschaftlichen Konsequenzen einer durch Netzwerkeffekte entstandenen oft quasi-monopolistischen Plattformökonomie, zumindest außerhalb des Silicon Valley, einer gewissen Skepsis gewichen, manchmal resignativ verbunden mit der Erkenntnis, dass es ohne fortschreitende Digitalisierung eben auch nicht mehr geht.

Als ich mich in der hoffnungsfrohen Phase im Rahmen meiner Diplomarbeit in Organisationstheorie mit der Frage beschäftigte, wie sich ein Kompressionsalgorithmus namens „mp3" auf die Wertschöpfungskette der Musikindustrie auswirken könnte, war die These nicht weniger Branchenexperten die einer weitgehenden Disintermediation, die oft auch als „Demokratisierung" des Marktes bezeichnet wurde. Das Internet würde es Musikschaffenden erlauben,

ihre Musik direkt an ihre Fans zu verkaufen. Kostentreibende und inhaltlich einengende Mittelsmänner wie Plattenfirmen oder Plattenläden wären dann nicht mehr notwendig.

In den folgenden Jahren wurde dann zwar die gesamte Wertschöpfungskette einmal durch den Reißwolf gedreht und das Urheberrecht weltweit an die neue digitale Realität angepasst, aber statt der alten Intermediäre gibt es nun neue. Re-Intermediation statt Disintermediation. Apple und Spotify statt Media-Markt und dem Plattenladen um die Ecke. Der direkte Kontakt von Künstlern zu Fans beschränkt sich doch zumeist auf Instagram.

Aber warum ließ sich die Utopie nicht verwirklichen? Zum einen, weil eine musikalische Idee nicht gleichzusetzen ist mit einem musikalischen Produkt, da haben nicht wenige Experten zu kurz gedacht. Und zum anderen, weil selbst bei Vorhandensein eines vermarktbaren Produkts das Internet als Kommunikationsprotokoll allein nicht das komplexe Gewebe aus Verträgen abbilden oder überflüssig machen konnte, das die wirtschaftliche Verwertbarkeit von Musik noch immer erfordert.

Einer ganz anderen Utopie folgend stellte 1937 ein junger sozialistischer Ökonom namens Ronald Coase, bei dem Versuch zu beweisen, dass ein Staat wirtschaftliche Aktivität besser steuern könne als der Markt, eine sehr entscheidende Frage: wenn es so sein sollte, wie zumeist angenommen, dass Märkte die effizienteste Form wirtschaftlicher Organisation sind, *warum gibt es dann überhaupt Unternehmen?*

Coase hatte erkannt, dass Unternehmen ihre Existenz der Tatsache verdanken, dass die Verwendung des Preismechanismus des Marktes

selbst einen Preis hat. Und dass dieser mitunter höher sein kann als die Kosten anderer Organisationsformen. Er konnte zwar nicht belegen, dass Planwirtschaft immer effizienter ist als Marktwirtschaft, aber er legte mit seiner Einsicht nicht nur den Grundstein für seinen Nobelpreis, sondern auch für die Analyse dessen, was heute als „Transaktionskosten" bezeichnet wird.

Diese Kosten – die Kosten des Suchens von Tauschpartnern, des Verhandelns, von Unsicherheit und Unklarheit über Gegenstände und Kontingenzen, den Kosten der Durchsetzung im Konfliktfall und vielem anderen mehr – sind eine Konsequenz der Annahme sog. begrenzter Rationalität – den neuro-physischen Grenzen mentaler Informationsverarbeitung durch Menschen –, und der Möglichkeit von opportunistischem, d.h. ausbeuterischem, Verhalten seitens der Beteiligten.

Tatsächlich kann man alle organisatorischen Fragestellungen – vom Kauf einer Limonade am Kiosk bis zur Gestaltung komplexer zwischenstaatlicher Handelsabkommen – als Konsequenz dieser beiden Annahmen über menschliches Verhalten und der so entstehenden Transaktionskosten modellieren. Deswegen argumentieren manche Ökonomen auch, dass man Transaktionskosten einfach als „institutionelle Kosten" bezeichnen sollte.

Wir alle leben eingebettet in eine Vielzahl von impliziten und expliziten Institutionen, die helfen, die Transaktionskosten unserer Interaktionen zu reduzieren oder, wie bei den Musikern, diese überhaupt erst möglich zu machen, indem bestimmte Transaktionen anhand ihrer Eigenschaften

entsprechenden Organisationsformen zugeordnet werden. Implizite Institutionen sind z.B. gesellschaftliche Normen, die unser Handeln prägen. Beispiele für explizite Institutionen sind die Rechtsordnung, Unternehmen, Gebietskörperschaften – oder eben eine Blockchain.

In Bezug auf die Transaktionskosten von arbeitsteiliger wirtschaftlicher Aktivität sind Register von fundamentaler Bedeutung, um einen für alle Beteiligten als *vertrauenswürdig* voraussetzbaren transaktionalen Zustand dokumentieren zu können.

Eine strenge rechtliche und hierarchische Kontrolle über Register war und ist zumeist ein wesentliches Element für ihre Akzeptanz als neutrale, *vertrauenswürdige* Grundlage von Tauschbeziehungen, weswegen sie zumeist von staatlichen Institutionen gepflegt werden. Aber sie sind auch eine Einflussgröße bzgl. der effizienten Grenzen von Organisationen, bzw. des Ausmaßes der Integration verschiedener Wertschöpfungsstufen innerhalb von Unternehmen, also des Zentralisierungsgrades von Volkswirtschaften.

Blockchains sind nun eine Technologie, die zuverlässige Register ohne Vertrauen in eine die Register pflegende Institution ermöglicht: Die deutsche Wikipedia[2] definiert "Blockchain" als „eine kontinuierlich erweiterbare Liste von Datensätzen, „Blöcke" genannt, die mittels kryptographischer Verfahren miteinander verkettet sind." Wird dieses technische Prinzip innerhalb eines dezentral organisierten Netzwerks umgesetzt, entsteht ein verteiltes Datenbanksystem - oder Register -, das

[2] https://de.wikipedia.org/wiki/Blockchain - abgerufen am 28.1.2020

technisch notwendig, auf Basis des von allen Teilnehmern verwendeten Verfahrens, zu jedem Zeitpunkt den für das Gesamtsystem geltenden Zustand dokumentiert.

Und das ohne zentrale Instanz. Aufgrund der beschriebenen Bedeutung von Registern erscheint es daher nicht unplausibel, dass einer dezentralisierenden Veränderung der Registertechnologie auch eine Veränderung der Transaktionsstruktur der Wertschöpfung folgen könnte, inklusive des möglichen Wegfalls von Intermediären.

Dabei ist die mögliche Anwendungsbreite von Blockchains so groß, dass sie Einfluss auf die relativen Kosten und damit relativen Effizienzen auch aller anderen Organisationsformen haben wird. Aber, und das unterscheidet Blockchains von anderen informationstechnischen Entwicklungen, man kann eine Blockchain darüber hinaus auch als eine neue, eine Organisationsform sui generis, ansehen – als nicht nur technische, sondern auch als *institutionelle Innovation* (Davidson et al., 2018[3]).

Und es ist diese institutionelle Innovation, die heute Anlass gibt, erneut über die Machbarkeit mancher organisatorischen Utopie der frühen Tage des Web zu spekulieren. Und darüber, ob und wie es möglich sein könnte, dass dezentralere Angebote die hochintegrierten Strukturen der aktuellen Plattformökonomie aufbrechen.

[3] Sinclair Davidson, Primavera de Filippi, Jason Potts. Blockchains and the economic institutions of capitalism. Journal of Institutional Economics, Cambridge University Press (CUP), 2018, 14 (4), pp.639 - 658. 10.1017/S1744137417000200. hal-01850927

Über Tobias Schwarz

Twitter | LinkedIn
Bild (c) Tom Solo

Ich studierte Wirtschaft und Politik an der Johannes Gutenberg-Universität Mainz, der Universität Mannheim, der ESSEC Paris sowie der London School of Economics. In meinen wissenschaftlichen Arbeiten beschäftigte ich mich mit Fragen der Disruption und demokratischer Organisation aus Sicht der Institutionenökonomie. Ich bin Gründungsmitglied des 2017 gegründeten Bundesverbands Blockchain und lebe zur Zeit in meiner Heimatstadt Mainz, wo ich als Digitalstratege, Sprecher und Kommunikationsberater tätig bin.

– ✻ –

Krystian Gaus

Was ist eine Blockchain?

Bei der Definition des Begriffs „Blockchain“ ist sehr oft die Rede von einer „dezentralen Datenbank“, ab und an wird noch der Begriff „verteilt“ hinzugefügt. Unabhängig von der tatsächlichen Bedeutung der Begriffe, hört sich das alles auf den ersten Blick sehr einleuchtend an. Man hat das Gefühl eine vage Vorstellung von einer Blockchain erhalten zu haben.

Doch verstehen wir den Begriff wirklich oder lügen wir uns hier selbst in die Tasche? Nicht umsonst gibt es das Zitat „If you can't explain it simply, you don't understand it well enough.“, das in ähnlicher Form Feynman oder Einstein zugeschrieben wird.

Blockchain ist nicht gleich Blockchain

Zunächst einmal muss man wissen, dass es nicht die eine Blockchain gibt. Blockchains gibt es in allen möglichen Varianten. Schnell gelangt man zu Begriffen wie Merkle Trees, verschiedenen Proof of Somethings, Hashes und Kryptographie. Meine Lieblinge hierbei sind die Begriffe public (öffentlich einsehbar), private (nur von Teilnehmern einsehbar) und permissioned (Teilnahme an eine Erlaubnis gebunden), permissionless (Teilnahme offen). Hier scheint die Verwirrung besonders groß zu sein. Bei all meinen Gesprächen mit anderen Blockchain Interessierten, mussten wir irgendwann feststellen, dass wir von zwei völlig verschiedenen Dingen sprechen. Wir hatten einfach beide ein völlig anderes Verständnis von all diesen Begriffen. Beispielsweise wird

permissionless sehr oft als Synonym für public verwendet (und dementsprechend permissioned für private). Für den einen ist eine private Blockchain eine Blockchain, die unter der Kontrolle einer einzigen Entität steht und keinerlei weitere Teilnehmer besitzt. Für den anderen erlaubt eine private Blockchain (mit dem Zusatz permissioned) weitere Teilnehmer in das Netzwerk aufzunehmen und somit die Kontrolle über das Netzwerk aufzuteilen, also eine sehr partnerschaftliche Verbindung zwischen den einzelnen Teilnehmern einzugehen. Wiederum andere verstehen unter letzterem eine Konsortium Blockchain. Nimmt man nun noch den Begriff DLT (Distributed Ledger Technology) hinzu, so wird einem in etwa das Ausmaß dieses schwammigen Begriffs Blockchain bewusst.

Was sagt die Literatur?

Lasst uns mal einen Blick in die Literatur werfen, bevor wir resignieren. Dr. Julian Hosp definiert

„Eine Blockchain ist eine dezentrale und meist öffentliche Datenbank, in der Vorgänge durch kryptografische Hashes als Merkle Tree (Hash-Baum) über viele Computer hinweg aufgezeichnet werden, so dass die Datensätze nicht rückwirkend geändert werden können, ohne nicht dieselbe Energie noch einmal hineinzustecken welche für das Kreieren der Hashes benötigt worden war."

Als Techie finde ich diese Definition spitze. Doch bei all den verwendeten Fachwörtern kann ich mir vorstellen wie nichtssagend dies für einen

Nicht-Techie sein mag. Großartig finde ich daher die folgende aus dem gleichen Buch stammende Definition:

„Eine Blockchain ist eine digitale Datei, in der dieselbe Information von allen Mitgliedern einer Gesellschaft abgespeichert und Updates in regelmäßigen Zeitblöcken an die bereits bestehende Information gehängt werden, sodass jeder Teilnehmer die gesamte Information besitzt und sich nicht auf andere verlassen muss.“

Okay, nun scheint klar zu sein was eine Blockchain ist. Oder etwa nicht? Betrachten wir die letzte Definition etwas genauer, so fällt auf, dass die erwähnte „digitale Datei“ aktualisiert wird, folglich etwas oder jemand diese Datei ändert. Doch was ist diese besagte Instanz, die Änderungen an der Blockchain vornimmt? Darf sie das überhaupt? Oder anders gefragt – ist sie vielleicht Teil der Blockchain? (An dieser Stelle könnt ihr euch mal selbst die Frage stellen, was denn überhaupt eine Datenbank ist. Klingt erstmal banal – dachte ich mir als Entwickler, der tagtäglich mit Datenbanken zu tun hat. Schließlich kann ich da Daten ablegen, abrufen und irgendeine Software kümmert sich um die Rest wie beispielsweise die Datenkonsistenz. Doch Moment mal – was tut diese Software? Und gehört der darin verwendete Konsens-Mechanismus zur Datenbank oder nicht? ;) Und genau dies führt uns zu der Kernproblematik eine Definition zu geben. Kurz gesagt: Wir müssen uns die Frage stellen, ob der Algorithmus, der für die Updates der „Blockchain-Datenstruktur“ zuständig ist, zur Blockchain gehört oder nicht. Und wir müssen uns die Frage stellen, ob eine „Blockchain-Datenstruktur“ ohne diesen Algorithmus überhaupt Sinn macht.

Daniel Drescher bringt es in einem seiner Bücher auf den Punkt. Er beschreibt, dass der Begriff Blockchain auf mehrere Arten verwendet wird:

- als Name für eine Datenstruktur,
- als Name für einen Algorithmus,
- als Name für ein Technologiepaket,
- als Oberbegriff für rein verteilte Peer-to-Peer-Systeme mit einem gemeinsamen Einsatzgebiet.

Kurz gesagt, kommt es bei der Begriffsdefinition auf den Blickwinkel an.

Fazit

Wie wir gesehen haben, gibt es verschiedene Arten von Blockchains und ebenso verschiedene Perspektiven zur Begriffsklärung. Bei Diskussionen kommt es daher sehr stark auf das Vorwissen der anderen Personen an und darauf, welches konkrete Problem diskutiert wird.

Ebenso ist Blockchain eine sehr junge Technologie, deren Potential wir noch nicht richtig erfasst und verstanden haben. Es müssen Learnings gesammelt und vernünftige Einsatzgebiete erschlossen werden. Die Definition wird sich im Laufe der Zeit immer wieder ändern und angrenzende Gebiete wie verteilte Systeme und DLT präzisieren.

Auch schätze ich, dass es eine Änderung im Wortgebrauch geben wird. Während ich im vorigen Absatz das Wort „Blockchain“ als technologische Disziplin verwendet habe – ähnlich wie die Mathematik als wissenschaftliche Disziplin – wird schon heute davon gesprochen Daten „in die Blockchain“ zu speichern, obwohl damit ein spezifisches Blockchain-Netzwerk gemeint ist. Letzteres erinnert sehr an die Verwendung, dass Daten „in der Cloud liegen“.

Ich persönlich sehe die Begriffe „Blockchain“ und „DLT“ als Oberbegriffe für verschiedene (aufkommende) Technologien, die mit der Zeit für unterschiedliche Use Cases optimiert und somit die Lücke zwischen den beiden Extremen verteiltes System („unter der Kontrolle einer einzigen Entität und Teilnahme an eine Erlaubnis gebunden“) und Bitcoin-Netzwerk („öffentlich einsehbar und Teilnahme offen“) schließen werden.

Also, diskutiert weiterhin über Blockchain- und DLT-Technologien, hört eurem Gegenüber gut zu, stellt Fragen, hinterfragt und bringt somit diese spannende Technologie weiter.

Über Krystian Gaus

Als Mathematiker und Software-Entwickler beschäftige ich mich mit dem Thema Blockchain auf mehreren Ebenen. Ich analysiere Whitepaper und diverse Konsens-Mechanismen, engagiere mich in der Wissensvermittlung und entwickle Apps. Zum Ausgleich treibe ich Kampfsport und habe Spaß an Dingen wie Hindernisläufen und Fallschirmspringen.

Twitter | LinkedIn | Xing

– ✻ –

Ronald Steyer

Die Geschichte wiederholt sich, oder doch nicht?

Wir werden über Blockchain reden – versprochen! Vorher möchte ich einen Umweg machen. Denn Technologien wie die Blockchain finden nicht im luftleeren Raum statt. Sie haben mit den Menschen zu tun, die sie nutzen. Und da wird es interessant, denn ob eine Technologie „erfolgreich" ist oder nicht, entscheidet sich eben auch daran, wie sie in der Gesellschaft ankommt.

Wir leben in interessanten Zeiten. Das Industriezeitalter geht zu Ende – darüber sind sich alle einig. Die derzeit reichsten Gesellschaften bezeichnen sich aber weiter als die Industrienationen. Der oft bewunderte Aufstieg Chinas zur Welt(wirtschafts)macht ist eine Geschichte der Industrialisierung. Im Kern geht es im Industriezeitalter um Skaleneffekte, also die Tatsache, dass eine große Menge ähnlicher Produkte industriell günstiger produziert werden können als eine kleine Menge. Groß ist dann besser als Klein.

Neben diesem ökonomischen Effekt gibt es noch den gesellschaftlichen Effekt: Große Unternehmen haben mehr Möglichkeiten das Wettbewerbsumfeld zu gestalten. Sie können aufwändig um Kunden werben und Politik beeinflussen, sind dann irgendwann sogar „too big to fail".

Dieses ständige Streben nach Größe hat zu ganz spezifischen Strukturen und Vorgehensweisen geführt, die sich tief eingegraben haben in die

Kultur von Industriegesellschaften. Besonders wesentlich: eine enorme Zentralisierung auch innerhalb dieser Organisationen und Unternehmen. Das führt zu Hierarchie und ständig steigen Koordinierungskosten. Viele Jobs sind so entstanden, große Mengen von Managern, die aber Verwalter sind, und ein Heer von Koordinierungsspezialisten – sehr oft ohne konkrete Verbindung zu dem Produkt oder der Leistung des Unternehmens. Das Ziel: Die immer weitergehende Verbesserungen von Produktionsprozessen, die idealerweise wie ein Uhrwerk oder eine große Maschine arbeiten sollen.

Aber wenn sie das lesen, sie spüren auch: Das hat oft gar nicht mehr so viel mit dem zu tun, was wir eben auch schon erleben. Wir leben in einer Phase des Umbruchs. Vor nicht allzu langer Zeit wurde das Informationszeitalter aufgerufen, davon ist aber immer weniger die Rede. Denn nicht Informationen sind das wesentliche, sondern die Tatsache, dass sie digital vorliegen, verarbeitet und weiterverwendet werden können. Es geht also um Digitalisierung und die Virtualisierung vieler Angebote. Skaleneffekte spielen dabei keine so große Rolle mehr, es geht jetzt darum, schnell den Kunden folgen zu können, deren Anforderungen und Erwartungen sich immer wieder ändern. Das Bild vom Uhrwerke führt jetzt in die Irre, bewegliche und anpassungsfähige, eher organische Strukturen können das eher leisten.

Und es geht darum, dass große Teile der Kommunikation zwischen Menschen nun über digitale Plattformen läuft. Und jetzt stellt man fest: Moment, schon wieder geht es doch um Größe! Wichtig ist aber zu verstehen, dass die wirtschaftliche Logik dahinter eine andere ist. Es geht jetzt nicht mehr um die Skaleneffekte bei der Produktion. Jetzt geht es

darum, dass viele dieser Angebote „soziale“ Angebote sind oder so gestaltet werden. Diese Angebote werden umso wertvoller, umso mehr Menschen daran teilnehmen. Große „Netze“ sind daher besser als „kleine“ Netze.

Damit aber diese Netze zu Geldmaschinen werden, braucht es mehr: Denn offene Standards, also z.B. das „Internet-Protokoll“ TCP/IP, haben auch solche positiven Effekte. Entscheidend ist daher: Können sich Unternehmen des digitalen Zeitalters die positiven Wirkungen des Netzwerks aneignen und in Milliardengewinne umwandeln? Das können sie derzeit, und sie machen es ausgiebig. Und nicht nur das: Sie nehmen sich auch gleich noch die Inhalte, auch die ganzen privaten Informationen, die bei der Kommunikation zwischen den Teilnehmern anfallen. Und damit haben wir wieder große, zentralisierte Unternehmen.

Wie wäre es, wenn es eine Möglichkeit gäbe, die eigenen digitalen Informationen selbst zu kontrollieren?

Wenn es für die Menschen möglich wäre, für den Nutzen, den sie in einem Netz oder auch als freiwillige Arbeit für ihre Communities schaffen, vergütet zu werden?

Wenn es eine Möglichkeit gäbe, in größeren Gruppen zusammen zu arbeiten und auch Größenvorteile zu nutzen, ohne eine Koordinierungs- und Verwaltungs-Hierarchie aufzubauen? Wenn Entscheidungen dezentraler getroffen werden können?

Ich hatte es ja versprochen, und jetzt kommt sie, die Blockchain. Denn auf diese Fragen kann schon heute die Blockchain-Technologie, oder

allgemeiner Distributed Ledger Technologie (DLT), eine Antwort geben, und die lautet: Technisch wären mit ihrer Hilfe solche Systeme möglich. Diese Technologie kann Eigentum definieren und kontrollieren helfen. Sie kann Gruppen und ihre Zusammenarbeit organisieren helfen. Sie kann Privatheit und Transparenz schaffen. Sie kann positive Beiträge zur Gesellschaft belohnen. Sie ist daher eine Technologie, die eine ungemein soziale Komponente hat. Für mich ist es dieses Element, die diese Technologie so interessant macht.

Jetzt spekuliere ich ein wenig, aber wenn in einigen Jahrzehnten auf diese Zeit zurückgeblickt wird, dann wird man nicht mehr von der Informationsgesellschaft reden, oder von Globalisierung. Die Industrie-Metapher, das Uhrwerk, funktioniert dann schon lange nicht mehr. Wenn ich die Blockchain in diesem Kontext sehe, ist sie möglicherweise die Technologie, die die wirklichen Veränderungen in einer Phase der Digitalisierung erst angestoßen hat. Weil sie Eigentumsrechte definieren kann, dabei hilft, Zusammenarbeit dezentraler zu organisieren, und neue Regeln in einer digitalisierten Gesellschaft ermöglicht.

Aber die Zukunft fährt nicht auf Schienen, schon gar nicht automatisch in eine gute Welt. Die Blockchain-Technologie hat auch das Potential, einzudringen in soziale Systeme in viel kleineren Einheiten als das bisherige Geldsystem, und soziale Beiträge und Interaktionen bewertbar zu machen. Wie überall gilt daher auch hier für die, die sich für diese Technologie begeistern, eine besondere Verantwortung. Wir legen die

Schienen für diese Technologie aus, wir können sie jetzt beeinflussen mit unseren Projekten. Wir können informieren über Möglichkeiten und

Grenzen. Und in der Blockchain Community dafür werben, mit unseren Projekten die Potenziale für Dezentralität, Persönlichkeitsrechte und persönliche Kontrolle zu stärken.

Über Dr. Ronald Steyer

Blockchain-Enthusiast, Mitglied im Board von PositiveBlockchain.io

Twitter | LinkedIn | mastodon

Nachwort

Kein Ahnung, was ich als Nachwort aktuell schreiben sollte. Wir sind noch gar nicht an Version v1.0 angelangt! Aus diesem Grund erstmal ein Dankeschön an alle Co-Autoren, die bisher sich die Zeit und Mühe genommen haben, dieses e-Book zu starten. Lust selbst teilzunehmen als Co-Autor? Lese nochmal die Hintergründe nach und melde dich auf der verlinkten Seite als Co-Autor an.

Ich freue mich auf Version v0.3, die im April 2020 erscheinen wird. Mit mehr Perspektiven, mit mehr Wissen.

Wer ist Chainist?

Wir sind Blockchain-Enthusiasten, -Educator und -Berater. Wir sind Begleiter für Menschen, Organisationen und Institutionen, um die Blockchain-Technologie zu verstehen und zu nutzen. Wir sind das Blockchain-Kompetenz-Netzwerk.

Wir bieten öffentliche Schulungen und inhouse Schulungen an und organisieren Events, Meetups im Raum Rhein-Main.

Zu unseren Kunden und bisherigen Veranstaltungs-Partnern zählen bereits das ZDF, das Wirtschaftsministerium Rheinland-Pfalz, die IHK Rheinhessen, Stadt Mainz, die Hans-Böckle-Stiftung, der Gutenberg Digital Hub e.V. und die UNECE PPP Initiative. Wenn es um Bitcoin & Blockchain Wissensvermittlung geht, dann sind wir die Anlaufstelle im Raum Rhein-Main.

Folge uns gerne auf Twitter, Facebook und LinkedIn.