MARKUS MILLER

KRYPTONOMICS

Von der Digitalisierung
zur Tokenisierung der Welt.
So investieren Sie in Bitcoin,
Ethereum, FinTechs und Co.

FBV

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://d-nb.de abrufbar.

Für Fragen und Anregungen:
info@finanzbuchverlag.de

Originalausgabe, 1. Auflage 2021

Türkenstraße 89
80799 München
Tel.: 089 651285-0
Fax: 089 652096

Redaktion: Ulrich Wille
Korrektorat: Manuela Kahle
Umschlaggestaltung: Karina Braun
Satz: Müjde Puzziferri, MP Medien, München
Druck: GGP Media GmbH, Pößneck
Printed in Germany

ISBN Print 978-3-95972-471-5
ISBN E-Book (PDF) 978-3-96092-890-4
ISBN E-Book (EPUB, Mobi) 978-3-96092-891-1

I. Vorwort

Kryptonomics: Das neue Digitalzeitalter der Tokenisierung

In den 80er-Jahren wurde die expansive Wirtschaftspolitik unter dem damaligen US-Präsidenten Ronald Reagan als »Reaganomics« bezeichnet. In Großbritannien gab es, diesem Vorbild folgend, den »Thatcherismus« und in Japan die »Abenomics«. In den kommenden Jahren wird ein neuer politischer Treiber große Veränderungen in der Weltwirtschaft herbeiführen. Dabei handelt es sich allerdings nicht um einen einzelnen Politiker oder Staat, sondern um die Entwicklungen und Maßnahmen, die auf dem Coronavirus aufbauen. Weltweit werden Regierungen, Unternehmen und ganze Gesellschaften mittlerweile von der Corona-Pandemie in ihrem Handeln getrieben.

Diese wirtschaftliche Ära wird vermutlich als »Coronanomics« in die Geschichtsbücher eingehen. »Coronanomics« wird zu massiven staatlichen Eingriffen führen, zu einer weiteren Explosion der Schulden, auf denen unser derzeitiges Geldsystem basiert, und ebenso zu dynamischen Entwicklungen und großen Chancen im Bereich der Digitalisierung. Ich bin davon überzeugt, dass wir derzeit am Beginn des Zeitalters einer neuen Krypto-Ökonomie stehen, die ich als »Kryptonomics« bezeichne.

Jede Bank wird eine Krypto-Strategie benötigen!

Wir leben in einem Zeitalter der digitalen Disruption, die sich im letzten Jahr beschleunigt hat. Die Zentralbanken setzen rekordverdächtige geldpolitische Stimuli frei, während die Technik unsere globale Wirtschaft immer schneller umgestaltet. Es hat uns gezeigt, dass konventionelles Denken nicht die Antworten auf das bringt, was vor uns liegt. Inmitten dieses Wandels entwickeln sich Krypto-Assets zu einem »sicheren Hafen« für institutionelle Investoren, die nach alternativen Wertaufbewahrungsmitteln für ihre Anlageportfolios suchen. In diesem Zusammenhang entstehen auch zahlreiche junge Unternehmen (Fintechs), die sich zu vielversprechenden Krypto-Playern entwickeln.

Krypto-Assets: Es entsteht eine neue Anlageklasse rund um Bitcoin und Co.

Es entsteht derzeit eine neue Anlageklasse namens »Krypto-Assets«. Es ist eine Anlageklasse, die für das neue digitale Zeitalter konzipiert wurde, in das wir jetzt eintreten. Bitcoin und andere Krypto-Assets haben die Aufmerksamkeit von Privatanlegern und nun auch von institutionellen Anlegern auf sich gezogen, die von der Unabhängigkeit dieser Assets von der Politik der Zentralbanken und Regierungen und der Blockchain-Technologie, die die Zukunft des Finanzwesens gestaltet, angezogen werden. Banken müssen sowohl die Infrastruktur für Krypto-Assets schaffen als auch als vertrauenswürdige Berater für Kunden agieren, die an Investitionen in diese Anlageklasse interessiert sind. Dies führt zu einer herausfordernden Dualität und Koexistenz: Das aktuelle Finanzsystem bleibt bestehen, und ein neuer Finanzsektor im Bereich der Krypto-Ökonomie entsteht für digitale Werte und Vermögenswerte auf Basis der Blockchain-Technologie.

Bislang wurden Kryptowährungen eher als Ersatz für den globalen Geldbestand eingesetzt. Das wird sich im Laufe der kommenden Jahre nachhaltig verändern. Die Überwindung regulatorischer Hürden wird ihre Attraktivität steigern und das Potenzial erhöhen, Bargeld zu ersetzen. Wir stehen nicht nur inmitten des Zeitalters der Digitalisierung, sondern auch der Tokenisierung der unterschiedlichsten Werte und Anlageklassen. Doch nicht nur im Finanzbereich und im Zahlungsverkehr, sondern auch im Bereich des Internets der Dinge (IoT = Internet of Things), der Künstlichen Intelligenz und der Cloud-Anwendungen wie auch bei der Cybersecurity spielen Kryptowährungen eine Rolle.

Das neue Krypto-Ökosystem wird in Koexistenz mit unserem konventionellen Geldsystem existieren

Ich bin davon überzeugt, dass es ein mehrdimensionales Krypto-Geldsystem in der digitalisierten Welt der Zukunft geben wird. Dezentrale Kryptowährungen wie der Bitcoin werden zu einer Art digitalem Gold. Zentrale Stablecoins von Privatunternehmen – wie beispielsweise Facebooks Diem – werden in Koexistenz neben zentralen Kryptowährungen von Notenbanken existieren.

Securitytoken werden darüber hinaus zahlreiche Vermögenswerte digitalisieren und fungibel handelbar machen. Utility Token (funktionale Kryptowährungen) werden zusätzlich Einzug halten in die Industrie und den Handel der Realwirtschaft wie als digitale Währungen in die Finanzwirtschaft. Kryptowährungen – allen voran der Bitcoin – sind für mich somit eine ganz wichtige Säule, ein Grundbaustein für jeden vorausschauenden, zukunftsorientierten Kapitalanleger. Zumindest als Beimischung für sein Gesamtportfolio.

In den letzten Jahren habe ich bereits zwei Bücher geschrieben, die sich mit der erodierenden Kaufkraft unseres Geldes befassen. In meinem Buch Die Welt vor dem Geldinfarkt belegte ich im Jahr 2017 die damals schon besorgniserregenden Risiken unseres schuldenbasierten und ungedeckten Geldsystems. Mein Praxis-Ratgeber Finanzielle Selbstverteidigung baute im Jahr 2019 auf diesen sich weiter verschärfenden politischen und rechtlichen Rahmenbedingungen auf.

Bitcoin-Publikationen oder Bücher zu Kryptowährungen gibt es bereits zahlreiche. Mir ist es sehr wichtig, mit Kryptonomics nicht nur ein weiteres »Krypto- oder Bitcoin-Erklärbuch« zu schreiben mit angeblichen Geheimtipps für Kryptowährungen, sondern den Blick auf das große Ganze der Digitalisierung und Tokenisierung zu richten. Dabei geht es mir bei Weitem nicht nur um die scheinbar so hochspekulativen Kryptowährungen wie den Bitcoin, sondern um die Megatrends der Digitalisierung und der Tokenisierung. Ich bin davon überzeugt, dass klassische Wertpapierbörsen die Tokenisierung, also die digitale Verbriefung von Wertpapieren wie Aktien, Anleihen oder Derivaten auf Basis der Blockchain-Technologie, in naher Zukunft massiv vorantreiben werden. Wichtig ist mir ebenso der Praxisnutzen.

Mein Anspruch an *Kryptonomics:* Wissensvermittlung mit Praxisnutzen!

Auch physische Vermögenswerte wie Edelmetalle oder Immobilien werden in Form von Token zukünftig verstärkt digitalisiert und fungibel in kleinen Stückelungen handelbar. Es gibt mittlerweile zahlreiche Konzepte und Plattformen in diesen Zukunftsbereichen, über die Sie beispielsweise Anteile an realen Werten als gedeckte Blockchain-Token (Securitytoken) bereits ab wenigen Euro erwerben können.

Ich gebe Ihnen mit Kryptonomics eine Vielzahl an Empfehlungen an die Hand, die Sie direkt umsetzen oder zumindest auch mit kleinen Anlagesummen einmal testen können. Ich verzichte dabei aber ganz bewusst auf seitenfüllende Trivialitäten, über die Sie sich auch ganz einfach und kostenlos über eine Google-Abfrage informieren können, wie beispielsweise: Was ist der Bitcoin, oder: Was ist eine Blockchain?

Weitere Megatrends und Zukunfts-Investments sowie die sich massiv verändernde Welt unseres Geldes und die damit verbundenen Gefahren und Digitalschutz- beziehungsweise Cybersecurity-Strategien sind ebenfalls Themenbereiche von Kryptonomics, denen ich mich ebenso intensiv wie praxisbezogen widme. Jetzt wünsche ich Ihnen viel Spaß und Mehrwert bei der Lektüre und freue mich über Ihre positive Rezension von Kryptonomics auf Amazon!

Mit den besten Grüßen
Ihr
Markus Miller

PS: Meine Maxime der Stunde: Positionieren Sie sich jetzt für die digitale Zukunft und bleiben Sie auch weiterhin am Ball und am Puls der digitalisierenden Zeit. Über meine regelmäßigen Blogs auf meinen beiden Online-Portalen www.geopolitical.biz und www.krypto-x.biz bleiben Sie ergänzend und weiterführend zu Kryptonomics auch in der Zukunft über aktuelle Entwicklungen, Chancen und Risiken in unserer sich dynamisch verändernden Welt bestens informiert. Nutzen Sie diese kostenlosen Möglichkeiten!

I. Kryptonomics: Das neue Digitalzeitalter

1. Keine Angst vor Krypto-Werten

Krypto-Investments sind kein Sprint, sondern ein Marathon!

Ich habe den großen Vorteil, dass ich nicht nur öffentlich zugängliche Zahlen und Informationen in meine Analysen einfließen lassen kann, sondern auch eine Vielzahl von Zuschriften, die mich täglich erreichen. Diese sind für mich sehr wertvoll, weil sie reale Entwicklungen aus der Praxis widerspiegeln. Zusätzlich lese ich täglich mindestens eine Stunde Diskussionen in Internetforen, auch hier erhalte ich fortlaufend wichtige Anregungen und Erkenntnisse. Dabei musste ich zuletzt verstärkt feststellen, dass viele Neueinsteiger die Krypto-Welt ganz offensichtlich nicht als strategischen Baustein bewerten, der die Risiken unseres konventionellen Geldsystems reduziert und die Chancen in der Welt der Digitalisierung optimiert, sondern als eine Art »Lottoschein« oder ein »Spielcasino«.

Die Jagd nach dem nächsten Cryptocoin, der innerhalb weniger Tage 100 Prozent plus x macht, überlagert dabei häufig nicht nur den gesunden Menschenverstand, sondern führt nicht selten zu großen psychischen Belastungen und finanziellen Risiken. Wenn Sie Leser meiner Publikationen auf KRYPTO-X sind oder meine YouTube-Interviews für Börse Stuttgart TV verfolgen, kennen Sie mich und meine strategische Herangehensweise, bei der Werte wie Besonnenheit und Geduld sehr wichtig sind. Das gilt nicht nur für die Phasen massiver Markteinbrüche, die wir auch in Zukunft immer wieder sehen werden, sondern auch für die Zeiten der starken Kursanstiege, die keine Einbahnstraßen sind. Für mich ist es Lebensqualität und Luxus, nicht wie ein hektischer Trader fortlaufend auf Charts und Handelssignale blicken

zu müssen, die sich an den Kryptomärkten mehrheitlich – bei kurzfristigem Anlagehorizont – als Fehlsignale erweisen.

Warnung vor den Dauerwarnern!

So sicher wie das Amen in der Kirche gibt es täglich pauschale Warnungen vor Kryptowährungen. Von Präsidenten von Notenbanken wie der Bank of England über Aufsichtsbehörden wie der deutschen BaFin oder der Finanzmarktaufsicht FMA in Österreich bis hin zu Verbraucherzentralen. Ebenso von den zahlreichen destruktiven Dauerwarnern, die seit Jahren den Fortschritt und die Transformation unserer Wirtschaft hin zu einer Digital- und Plattform-Ökonomie verschlafen haben.

Hierzu zählt auch der als »Mister Dax« öffentlich sehr bekannt gewordene Dirk Müller, der sich nach meiner Einschätzung längst zu einem fragwürdigen Crashpropheten und Verschwörungstheoretiker entwickelt hat. Zu Jahresbeginn 2021 gab es ein Interview von Dirk Müller bei Focus Online, auf das ich sehr häufig angesprochen wurde. Dirk Müller vertrat hier unter anderem die Hypothese, dass hinter dem Bitcoin kein Wert stehe und die führende Kryptowährung innerhalb von 24 Stunden auf null fallen könne, wenn Justizbehörden wegen Geldwäsche dagegen vorgehen. Das ist schlicht eine unqualifizierte Angstmacherei!

Ein weiterer Aspekt, der immer wieder als Kritikpunkt an Kryptowährungen angeführt wird, ist der angeblich so hohe Stromverbrauch, als wenn das konventionelle Geld- und Bankensystem oder die Förderung von Gold energielos funktionieren würde.

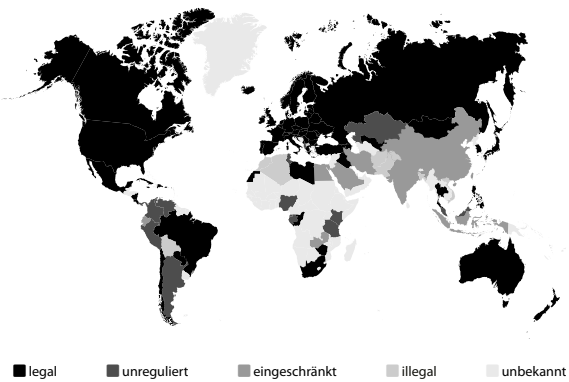
Fakt ist: In Bezug auf den Stromverbrauch liegt der Bitcoin auf Rang 39 zwischen Bangladesch und Chile, Ethereum lediglich auf Rang 81, zwischen Syrien und Turkmenistan. Die Energieeffizienz von Bitcoin und Ethereum wird durch technologische Verbesserungen – Lightning Network, Ethereum 2.0 – immer besser, nicht schlechter!

Informationen: www.digiconomist.net

Der Bitcoin ist bereits in 132 von 257 Ländern beziehungsweise Regionen legal

In vielen Medien ist immer wieder zu lesen, dass der Bitcoin in zahlreichen Ländern verboten sei. Gegen Ende des Jahres 2017 schlug beispielsweise ein Bitcoin-Verbot in China hohe Wellen. Längst sind der Bitcoin und andere Kryptowährungen jedoch in China als Zahlungsmittel anerkannt, auch wenn es – wie auch in Indien – Einschränkungen gibt. Ich kann somit klar feststellen, dass tendenziell negative Medienberichte zu Verboten von Kryptowährungen die Mär von der angeblichen Illegalität des Bitcoin nach wie vor sehr häufig befeuern und zu Ängsten führen. Ein rationaler Faktencheck führt allerdings zu einem ganz anderen Ergebnis.

In 132 von 257 Ländern ist der Bitcoin heute bereits absolut legal und als Zahlungsmittel beziehungsweise Vermögenswert anerkannt. Lediglich in zehn Ländern ist der Bitcoin verboten. Dabei handelt es sich um Afghanistan, Algerien, Bangladesch, Bolivien, Katar, Pakistan, die Republik Mazedonien, Saudi-Arabien, Vanuatu und Vietnam. Diese Staaten bewerte ich als vollkommen unbedeutend im Hinblick auf die zukünftige Adaption von Kryptowährungen in der weltweiten Finanz- und Realwirtschaft, wenn der Bitcoin in großen Volkswirtschaften wie Japan, Deutschland, Großbritannien, Russland, Brasilien oder allen voran in den USA legal ist.



Quelle: coin.dance

Informationen: www.coin.dance

Die regulatorischen Rahmenbedingungen sind besser als die Medienberichterstattung

Wenn ich aktuell und in den letzten Jahren in zahlreichen Medien immer sehr oberflächliche und undifferenzierte Berichte zur angeblich so unsicheren Rechtslage von Kryptowährungen in Deutschland – oder auch anderen Ländern – lese, die meist verbunden sind mit der Forderung nach einer klaren Regulierung, dann frage ich mich, ob die jeweiligen Journalisten beziehungsweise Autoren überhaupt die realen Entwicklungen und Fakten kennen.

Die Regulierung ist beispielsweise in den USA, aber auch in Europa in der Praxis sehr weit fortgeschritten. Zum einen durch die mächtige US-Wertpapieraufsichtsbehörde United States Securities and Exchange Commission (SEC). Zum anderen im Mekka der Hochfinanz, dem Bundesstaat New York, durch die Regierungsbehörde des New York State Department of Financial Services (NYSDFS). Bereits im Jahr 2015 wurde dem ersten US-Unternehmen (Circle) durch die US-Behörde eine BitLicense erteilt, um als Bitcoin-Börse aktiv zu werden beziehungsweise Krypto-Dienstleistungen reguliert anzubieten. Mittlerweile verfügen auch börsennotierte US-Techkonzerne wie Square, die sich auf Zahlungsverkehrsdienstleistungen spezialisiert haben, über eine BitLicense.

Securitytoken sind in Deutschland eine eigene Wertpapiergattung

Auch in Deutschland ist die Regulierung längst viel weiter, als der überwiegend negative Tenor in den Medien vermuten lässt. Am 15. April 2019 hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) eine umfassende Stellungnahme zur »Tokenisierung« veröffentlicht. Bei der Tokenisierung handelt es sich um die digitalisierte Abbildung eines (Vermögens-)Wertes inklusive der in diesem Wert enthaltenen Rechte und Pflichten sowie dessen hierdurch ermöglichte Übertragbarkeit.

Bereits zu Jahresbeginn 2019 hat die BaFin den ersten Wertpapierprospekt zu einem Security Token Offering (STO) in Deutschland genehmigt. Das war der erste Schritt eines rechtlichen Paradigmenwechsels in der Praxis. Durchgeführt wurde das STO durch das Unternehmen Bitbond mit Sitz in Berlin. Seither sind eine Vielzahl an liberalen Regulierungsschritten weltweit

erfolgt, die die Rechtssicherheit fördern und somit zu einer weiter steigenden Marktakzeptanz und Marktdurchdringung von Kryptowährungen führen werden.

Zentralbankgeld: Bundesbank setzt auf Blockchain[1]

»Die Deutsche Börse, die Deutsche Bundesbank und die Finanzagentur des Bundes haben gemeinsam mit weiteren Marktteilnehmern eine Abwicklungsschnittstelle für elektronische Wertpapiere entwickelt und erfolgreich getestet. Die auf der Distributed-Ledger-Technologie (DLT) basierenden Wertpapiere können mithilfe einer sogenannten Trigger-Lösung und eines Transaktionskoordinators in TARGET2, dem Zahlungsverkehrssystem des Euro-Systems für Großbeträge, abgewickelt werden.

Damit bewiesen die Teilnehmer, dass eine technische Brücke zwischen der Blockchain-Technologie und dem konventionellen Zahlungsverkehr grundsätzlich zur Wertpapierabwicklung in Zentralbankgeld genutzt werden kann, ohne dass digitales Zentralbankgeld geschaffen werden muss. Im Verlauf des Tests emittierte die Finanzagentur des Bundes eine Bundesanleihe mit zehnjähriger Laufzeit im DLT-System, deren Primär- und Sekundärmarkt-Transaktionen auch auf DLT abgewickelt wurden. Die getätigten Geschäfte des Tests sind rechtlich nicht bindend.« [...] »Bei der Durchführung des Experiments waren Barclays, die Citibank, die Commerzbank, die DZ Bank, Goldman Sachs und die Société Générale beteiligt.

Die Grundlagen für tokenisiertes Zentralbankgeld sind gelegt

DLT wie Blockchain gewinnen seit einigen Jahren zunehmend an Bedeutung. Im Projekt wurde eine Schnittstelle zwischen dem konventionellen Zahlungsverkehr und einem DLT-basierten Wertpapiersystem geschaffen. Zwei Softwaremodule, eine Trigger Chain der Bundesbank und ein Transaktionskoordinator der Deutschen Börse, verbinden TARGET2 und ein DLT-Wertpapiersystem. Wertpapiere und Zentralbankgeld wechseln erst bei erfolgreicher Bestätigung aller Parteien den Besitzer. Diese Zug-um-Zug-Abwicklung minimiert das Ausfallrisiko für Käufer und Verkäufer.

Bei DLT-basierter Abwicklung werden üblicherweise entsprechende Werte und Geld in Form von Token dargestellt, also als Abbildung in der DLT-Um-

gebung. Mit der vorgestellten Lösung kommt es nicht zum Einsatz von tokenisiertem Geld. Stattdessen wurde eine Schnittstelle geschaffen, die zwischen der DLT und dem konventionellen Zahlungsverkehr vermittelt und die Zahlung auslöst (›triggern‹). Da die im Projekt getestete Lösung in verschiedenen DLT-basierten Abwicklungssystemen eingesetzt werden kann, ist sie ein wichtiger Schritt für die weitere Verwendung der DLT im Finanzsektor und in der Realwirtschaft.

Zentralbanken werden auch mit Krypto-Projekten kooperieren

Burkhard Balz, der im Vorstand der Bundesbank für die Bereiche Zahlungsverkehr und Abwicklungssysteme zuständig ist, sagte: ›Nach dem erfolgreichen Test dürfte die Implementierung einer entsprechenden Lösung durch das Euro-System in relativ kurzer Zeit möglich sein, zumindest deutlich schneller als etwa die Emission von digitalem Zentralbankgeld.‹«

Es gibt mittlerweile auch Staaten beziehungsweise Notenbanken, die bereits bestehende Blockchains mit ihren Kryptowährungen für derartige Anwendungen nutzen beziehungsweise testen. Hierzu zählt beispielsweise die Kryptowährung Stellar. Kryptowährungen beziehungsweise Blockchain-Anwendungen vermitteln in den Medien häufig den Eindruck einer schnelllebigen Zockerei. Besinnen Sie sich darauf, dass Ihre Krypto-Investments kein Sprint, sondern ein Marathon sind, bei dem es auf Ihre Ausdauer ankommt!

Musa al-Chwarizmi: Der unbekannte Krypto-Urvater der Kryptowährungen

Kennen Sie den Urvater aller Kryptowährungen? Nein, ich spreche nicht von Satoshi Nakamoto, der das Bitcoin-Konzept als Whitepaper im Jahr 2008 in das Internet gestellt hat und der nicht wirklich »Satoshi Nakamoto« heißt, sondern eine unbekannte Einzelperson oder eine Entwicklergruppe mit diesem Pseudonym ist. Ich spreche von der Person mit dem echten Namen »Musa al-Chwarizmi«, die zu einer Zeit lebte, in der die Digitalisierung noch eine reine Zukunftsmusik war.

Wir alle kennen die großen griechischen Mathematiker der Antike wie Pythagoras von Samos, Euklid von Alexandria, Archimedes von Syrakus, Eu-

doxos von Knidos, Diophant von Alexandria oder Thales von Milet. Ich bin mir sicher, jeder unter Ihnen hat sich in der Schule mit dem Satz des Pythagoras befasst und Begriffe wie »Hypotenuse« oder »Kathete« heute noch in Erinnerung.

Der Name »Musa al-Chwarizmi« ist nach meiner Einschätzung hingegen leider weitgehend unbekannt. Ich habe einige meiner Bekannten und Freunde gefragt – die teilweise Mathematik studiert haben –, ob Sie Musa al-Chwarizmi kennen. Kein Einziger konnte den Namen zuordnen. Von »Fußballspieler« über »Musikproduzent« und »Notenbankchef« bis hin zu »Terrorist« war unter den Antworten so ziemlich alles dabei. Musa al-Chwarizmi (circa 780 bis 850 nach Christus) war ein iranischer Mathematiker, auf den die weltbekannten Begriffe »Algebra« und »Algorithmus« zurückzuführen sind.

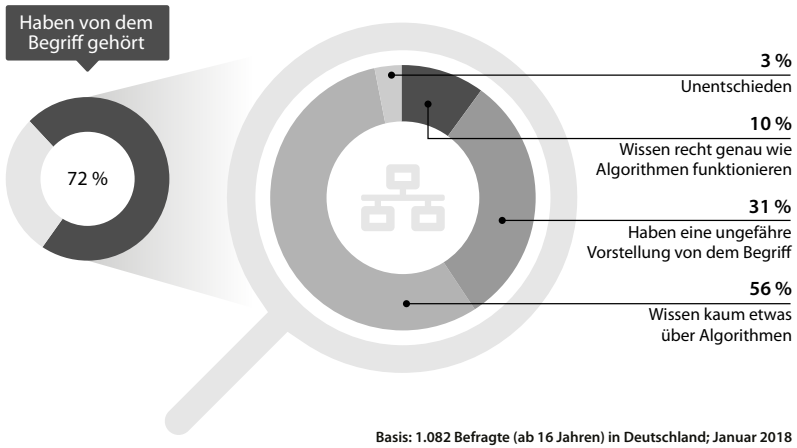
Algebra und Algorithmen sind die Grundpfeiler der Kryptowelt

Ein Algorithmus bezeichnet ein Bearbeitungsschema eines Problems in Einzelschritten, das meistens auf mathematischen Strukturen beruht und deshalb von Computern gelöst werden kann. Jede Kryptowährung basiert auf diesem Prinzip. Algorithmen bestimmen zunehmend unser aller Leben.

Selbst wer es schafft, sich – noch – vom Internet fernzuhalten, wird unweigerlich von Algorithmen beeinflusst. Das ist den meisten Bürgern allerdings überhaupt nicht bewusst. Auch diese Unwissenheit birgt gleichzeitig weiteres Potenzial für Cryptocoins. Werden Sie sich bewusst: Algorithmen sind Assets!

Digitalbildung: Wissenslücke Algorithmen

Unser Leben ist längst geprägt von Algorithmen. Hinter dem Bitcoin steht ein mächtiger und wertvoller Algorithmus, der immer mehr Anerkennung, Anwendung und Vertrauen findet. Das fehlende Verständnis für den Bitcoin liegt nach meiner Überzeugung auch darin begründet, dass viele Bürger viel zu wenig über Algorithmen wissen. Diese mathematische wie digitale Bildungslücke gilt es zu schließen.



Quelle: statista, Bertelsmann Stiftung

Krypto-Algorithmen: Sie investieren in SHA-256, Dagger-Hashimoto und ECDSA!

Wenn Sie eine Schufa-Auskunft benötigen oder einfach nur mit einem öffentlichen Verkehrsmittel wie der Bahn fahren, folgen Sie zwangsläufig einem Algorithmus. Umso verwunderlicher ist das Ergebnis einer aktuellen Studie der Bertelsmann Stiftung, aus der hervorgeht, dass die Mehrheit der Deutschen wenig bis nichts mit dem Begriff »Algorithmus« anfangen kann. 72 Prozent der befragten Bürger geben an, zumindest schon von dem Wort »Algorithmus« gehört zu haben. Wie die obige Grafik eindrucksvoll verdeutlicht, musste davon im Anschluss aber mehr als die Hälfte zugeben, kaum Fachwissen zu haben.

Der Bitcoin basiert beispielsweise auf dem Algorithmus SHA-256, Ethereum auf Dagger-Hashimoto, Ripple auf ECDSA, Litecoin auf Scrypt. Unser Leben basiert immer mehr auf Algorithmen, die Menschen sind sich dieser Entwicklung aber gar nicht bewusst! Krypto-Algorithmen und die entsprechenden Coins haben daher das Potenzial, Prozesse in den unterschiedlichsten Bereichen signifikant zu verbessern. Das wiederum wird zu steigenden Werten von Cryptocoins führen, weil Algorithmen Anerkennung und Marktakzeptanz gewinnen, wertvolle Funktionalitäten und somit Werte darstellen.

Sechs Konsensalgorithmen: Von Burnern bis Validatoren

Für die Funktionalität und Sicherheit einer Blockchain werden Regeln benötigt. In dezentralen Netzwerken gibt es dabei – im Gegensatz zu einem Konto bei einer Bank – nicht eine einzige Autorität, die für Recht und Ordnung sorgt, sondern Konsensmechanismen, die auf mathematischen Berechnungen basieren. Ein Konsensmechanismus definiert die Vorgehensweise, durch die eine bestimmte Gruppe beziehungsweise Beteiligte eines Netzwerks eine Entscheidung herbeiführen.

Dadurch wird es einander vollkommen fremden Teilnehmern möglich, sich auf bestimmte Abläufe zu einigen. Beispielsweise die Übertragung einer Kryptowährung. In der Welt der Cryptocoins gibt es zwei grundlegende Konsensprotokolle, auf denen die Blockchain-Technologie der wichtigsten Kryptowährungen aufbaut. Proof-of-Work (PoW) und Proof-of-Stake (PoS). Darüber hinaus gibt es zahlreiche weitere Konsensalgorithmen und Abwandlungen. Nachfolgend finden Sie sechs wichtige Konsensalgorithmen, beginnend mit den beiden wichtigsten, PoW und PoS:

1. Proof-of-Work (PoW)

Proof-of-Work (PoW) bedeutet, dass derjenige Rechner einen neuen Block an eine Blockchain anhängen kann, der ein vorgegebenes kryptografisches Rätsel als Erster gelöst hat und damit die Belohnung in Form von Cryptocoins beziehungsweise Token erhält. PoW ist ein Arbeitsnachweis. Beim Proof-of-Work findet somit eine Auswahl nach der Rechenleistung der Miner statt, was wiederum zu einem exorbitant hohen und deswegen häufig kritisierten Energieverbrauch führt, beispielsweise beim Bitcoin-Mining.

2. Proof-of-Stake (PoS)

Die Idee hinter dem Konsensalgorithmus von Proof-of-Stake (PoS) ist es, das energieraubende Lösen kryptografischer Rätsel durch den PoW-Ansatz massiv zu reduzieren und gleichzeitig die Geschwindigkeit der Transaktionen zu erhöhen. Beim PoS-Mechanismus ist die Wahrscheinlichkeit, dass ein Miner für die Erzeugung eines neuen Blocks den Zuschlag erhält, proportional zum wertmäßigen Anteil aller seiner Coins an der ausstehenden

Gesamtmenge der bereits existierenden Cryptocoins. PoS ist somit nicht wie PoW ein Arbeitsnachweis, sondern ein Anteilsnachweis. Die dadurch generierten Kryptowährungen und einbehaltenen Transaktionsgebühren aus der Blockchain-Aktivität werden nach dem Zufallsprinzip an die Coin-Inhaber (Anteilseigner) ausgeschüttet. Die Wahrscheinlichkeit, »Ausschüttungen« zu erhalten, steigt mit der Höhe der Bestände wie auch mit der Haltedauer.

3. Proof-of-Activity (PoA)

Bei diesem Konsensalgorithmus wird sowohl PoW als auch PoS verwendet, so dass man von einem »Hybridverfahren« spricht. Dadurch wird die Arbeit der Miner belohnt und gleichzeitig wird auch eine Art Verzinsung (Staking) der gehaltenen Cryptocoins möglich.

4. Proof-of-Authority (PoA)

Bei der Abkürzung »PoA« kommt es immer wieder zu Unstimmigkeiten und Missverständnissen, weil das Kürzel »PoA« sowohl für den Konsensalgorithmus Proof-of-Activity verwendet wird als auch für den Blockchain-Mechanismus Proof-of-Authority. In Proof-of-Authority-Blockchains werden neue Blöcke von sogenannten Validatoren erstellt. Diese haben auf Basis von Mehrheitsentscheidungen ein Stimmrecht, dass ihnen aber auch wieder entzogen werden kann, falls das Vertrauen missbraucht wird, beispielsweise durch die Verifizierung falscher Blöcke.

5. Proof-of-Capacity (PoC)

Bei Proof-of-Capacity generieren Miner für die Erzeugung von Blöcken große Datensegmente, die sich »Plots« nennen und die auf Datenträgern (Festplatten) gespeichert werden. Dadurch ist PoC energieeffizienter als PoW und PoC-Blockchains sind äußerst resistent gegen externe Angriffe wie beispielsweise automatisierte Schadprogramme (Bots).