crypto research .report

Juni 2020

Edition X.

Modellierung des Bitcoin Preises mit Irving Fishers Quantitätsgleichung

Eine Absolute Bewertung von Bitcoin & Co.

Ist Tether ein Schwarzer Schwan für Bitcoin?

Coin Corner: Privacy Coins und MimbleWimbleCoin

Wir bedanken uns herzlich bei unseren „Premium-Partnern“ für die Unterstützung des „Crypto Research Report“.

coinfinity

mwc Extremely scarce ghost money

bitpanda pro

Contents

Ein Absoluter Bewertungsansatz für Krypto-Assets 7

Annahmen im Detail 11
Adressierbarer Zielmarkt für Krypto-Assets 16
Tauschmittel und Rechnungseinheit 16
Offshore-Konten 18
Reservewährung 19
Wertspeicher 20
Online-Transaktionen 21
Überweisung 24
Steuerflucht 26
Kleinere Zielmärkte und Anwendungsfälle 27
Akzeptanzrate 29
Szenarien 33
Bewertungsergebnis 35
Kritik an der Quantitätsgleichung 35
Alternative Erklärung gesucht 43
Tether als Retter in der Not 43
Nachfrage nach Tether, nicht Bitcoin 44
Alle wollen US-Dollar 46

Exklusives Interview mit dem MWC Team 49

Was Sind Privacy Coins? 50
Was im Digitalen Zeitalter Gutes Geld Macht 54
Wie Eine MWC-Transaktion Durchgeführt Wird 56
Kamingespräch mit dem MWC-Team 59

Crypto Research Report Buchempfehlung 65

Disclaimer:

Diese Publikation dient ausschließlich zu Informationszwecken und stellt weder eine Anlageberatung, eine Anlageanalyse noch eine Aufforderung zum Erwerb oder Verkauf von Finanzinstrumenten dar. Insbesondere dient das Dokument nicht dazu, eine individuelle Anlage- oder sonstige Beratung zu ersetzen. Die in dieser Publikation enthaltenen Angaben basieren auf dem Wissensstand zum Zeitpunkt der Ausarbeitung und können jederzeit ohne weitere Benachrichtigung geändert werden. Die Autoren waren bei der Auswahl der verwendeten Informationsquellen um größtmögliche Sorgfalt bemüht und übernehmen keine Haftung für die Richtigkeit, Vollständigkeit oder Aktualität der zur Verfügung gestellten Informationen bzw. Informationsquellen bzw. daraus resultierend Haftungen oder Schaden gleich welcher Art (einschließlich Folge- oder indirekte Schaden, entgangenen Gewinn oder das Eintreten von erstellten Prognosen).

Copyright: 2020 Crypto Research Report. Alle Rechte vorbehalten.

Editorial

Liebe Leser,

das erste Mal in Bitcoins junger Geschichte ist die Weltwirtschaft in eine Rezession gestürzt. Im Zuge von Covid-19 haben 40 Millionen US-Amerikaner ihre Arbeit verloren (15 %). In Österreich sind es 571.477 Arbeitslose und in Deutschland 2,639 Millionen (5,8 %). Obwohl das BIP eines ganzen Quartals von 2020 ausgelöscht wurde, singen alle Hedgefonds-Manager den Slogan: **„All Time High by Fourth of July."** Dieser Slogan bedeutet, dass der S&P 500 voraussichtlich bis Juli ein neues Allzeithoch erreichen wird. Obwohl dies unglaublich klingt, haben Zentralbanken weltweit die Macht, dies zu erreichen, und sie scheinen alles ihnen Mögliche zu tun, um ihre Währungen zu schwächen und ihre Vermögenspreise künstlich zu stützen.

Wenn wir beispielsweise Amerika nehmen, so sanken sowohl der S&P 500 als auch der Dow Jones im März um zweistellige Prozentsätze. Als Reaktion darauf schuf die Federal Reserve $3 Billionen aus dem Nichts, und die Finanzmärkte erholten sich wieder. Der Stimulus, für dessen Injektion die Federal Reserve gerade zwei Monate brauchte, ist größer als der gesamte Stimulus, den sie als Reaktion auf die „Groβe Rezession" 2008 injizierte. Die Federal Reserve handelte so schnell, weil sie wusste, wie fragil das Finanzsystem ist und wie abhängig die Märkte von billigem Geld sind. Noch vor sechs Monaten lachten Verfechter des harten Geldes über die Abgeordnete des US-Repräsentantenhauses Alexandria Ocasio-Cortez, eine Advokatin der modernen Geldtheorie (Modern Money Theory, MMT), und nun hat die Fed versprochen, eine unbegrenzte quantitative Lockerung vorzunehmen, „bis wir uns erholen." Das bedeutet, **im Grunde gibt es keinen Unterschied zwischen MMT und quantitativer Lockerung.** Der einzige Unterschied ist, dass wir bei ersterer die Täuschung sein lassen und nicht mehr so tun, als würden wir die Schulden eines Tages zurückzahlen.

Trotz beispielloser quantitativer Lockerung, Billionen von kurzfristigen Krediten an den Pensionsgeschäftsmarkt und die Senkung der Zinssätze auf null **bewegte sich der US-Dollar-Index (DXY) kaum.** Das bedeutet, dass der Dollar den Druckmaschinen weitaus mehr Missbrauch abnehmen kann, bevor er gegenüber anderen Fiatwährungen abgewertet wird. Auch die 5-Jahres-Inflationserwartung des US-Dollars liegt bei niedrigen 1,43 %. Dies wiederum bedeutet, dass die Märkte trotz massiver Abwertung des US-Dollars erwarten, dass die Inflation unter dem Ziel der Federal Reserve von 2 % liegt. Traditionelle Märkte spiegeln nicht mehr die Wirtschaftslage wider, stattdessen die Bemühungen der Zentralbank, das Rentensystem am Leben zu erhalten und Trump wiedergewählt zu bekommen. **Leider gibt es nun kein Zurück mehr.** Jeder Schluckauf in der Wirtschaft muss mit einer stärkeren Inflation bewältigt werden, was zu einer noch größeren Kluft zwischen Realität und Finanzen führt.

Vergessen wir nicht, dass jedes Mal, wenn die Zentralbank neue nicht gedeckte Währungseinheiten schafft, dies auf Kosten aller geht, die derzeit über die Währung verfügen. Leider ist dieser Aufwand nicht gleich verteilt. Im Alleingang ist die Inflation die größte Ursache für die Ungleichheit des Wohlstands im Westen. Google Cantillon-Effekt.

Und wo war Bitcoin während all dem? Von $3.600 im März auf $10.000 im Mai und wieder runter auf $9.000 – die Fahrt mit der Bitcoin-Achterbahn hat so einigen Übelkeit verschafft und anderen Reichtum. Viele Kryptowährungsunternehmen sind aufgrund des Lockdowns und dem Mangel an Kunden in einer schlechten Verfassung, aber Bitcoin-Besitzer halten einfach an der Hoffnung auf einen Bullenmarkt nach der Halbierung fest. Bislang ist die Halbierung ein Non-Event gewesen. Bitcoiner auf der ganzen Welt nahmen an Zoom-Webinaren teil, um Bitcoins besonderen Tag zu feiern, aber der Bitcoin-Preis bewegte sich kaum. Die Unsicherheit in Bezug auf die Wirtschaft hat den Kryptomarkt definitiv gedämpft. Dennoch gibt es noch Hoffnung. Während Regierungen auf der ganzen Welt Währungskriege führen, um ihre Exportmärkte zu schützen und ihre belastenden Schulden abzubauen, wenden sich einige Haushalte vielleicht Plan B zu.

Wir hoffen, dass Ihnen diese Jubiläumssonderausgabe des Crypto Research Reports gefällt! In der letzten Ausgabe ging es um Plan Bs Stock-to-Flow-Modell. In dieser Ausgabe stellen wir ein weiteres beliebtes Modell vor, mit dem der zukünftige Preis von Bitcoin prognostiziert wird: die Quantitätsgleichung. Wir diskutieren, wie Vitalik Buterin von Ethereum und Kyle Samani von Multicoin Capital sich dieser Gleichung näherten, und wir diskutieren eine vernichtende Kritik von Scott Locklin von Basic Attention Token. In dieser Sonderausgabe finden Sie auch einen Gastartikel von Pascal Hügli von Schlossberg&Co's zum Thema Tether. Hügli untersucht, ob Tether tatsächlich dazu verwendet wird, um den Preis von Bitcoin zu manipulieren oder nicht. Seit Beginn dieses Jahres wurde Tether USDT im Wert von $5 Milliarden ausgegeben. Wenn der neue Tether nicht vollständig gesichert ist und der Tether schließlich zusammenbricht, dann wird dies höchstwahrscheinlich mindestens eine Börse stürzen und den Preis von Bitcoin in Mitleidenschaft ziehen. Schließlich enthält diese Ausgabe des CRR ein exklusives Interview mit dem Entwicklerteam von MimbleWimbleCoin, einer neuen Privacy Coin, die im Dezember kostenlos an Bitcoin-Besitzer ausgegeben wurde. Seit Dezember ist der Preis um 6.000 % hochgeschnellt, und die Autoren argumentieren, dass ihre Token-Ökonomie der Privacy Coin Grin überlegen ist, dass sie skalierbarer als Monero ist und dass sie im Gegensatz zu Zcash ihr Gesamtangebot nachweisen können.

Weiterhin freuen wir uns, Ihnen mitteilen zu können, dass der *Crypto Research Report* eine strategische Partnerschaft mit CoinTelegraph eingegangen ist, einer der größten Krypto-Nachrichtenunternehmen der Welt. Die Septemberausgabe des *Crypto Research Report* wird auf der CoinTelegraph-Webseite veröffentlicht, welche monatlich 10 Millionen Mal abgerufen wird. Das Ziel dieser Zusammenarbeit ist es, die Ergebnisse einer wegweisenden Studie zur institutionellen Nachfrage nach Kypto-Assets im deutschsprachigen Raum zu veröffentlichen. Diese Studie wird von Professor Dr. Philipp Sandner der Frankfurt School of Finance and Management, Professor Dr. Alfred Taudes der Wirtschaftsuniversität Wien und der Herausgeberin des *Crypto Research Report*, Demelza Hays, durchgeführt. Wenn Sie unter den ersten sein wollen, die diesen Report erhalten, abonnieren Sie den kostenlosen Quartalsbericht auf unserer Webseite.

Schließlich möchten wir uns beim laufenden Premium-Partner des *Crypto Research Report*, Coinfinity in Graz, bedanken. Coinfinity ist ein österreichischer Broker, der für die Schaffung der benutzerfreundlichen Bitcoin-Wallet The Card Wallet bekannt ist. Mittels seines Bitcoinbon-Programms hat Coinfinity auch Bitcoin-Einkäufe in 4.000 Einzelhandelsgeschäften in Österreich ermöglicht. Zusätzlich zu Coinfinity freuen wir uns

sehr, dass nun auch Bitpanda zu den Premium-Partnern des *Crypto Research Report* gehört! Bitpanda ist eine voll lizensierte Börse mit Sitz in Österreich. Erst kürzlich haben sie noch Bitpanda Pro hinzugefügt, das mehr Liquidität für geringere Gebühren bietet. Wir persönlich freuen uns über Bitpanda Metals, mit dem Anleger ihr Portfolio mit physisch abgesicherten und zu 100% versicherten Edelmetallen diversifizieren können.

Demelza Kelso Hays

Ein Absoluter Bewertungsansatz für Krypto-Assets

„Es ist weltweit so schnell passiert, dass es selbst einem Marktveteran wie mir die Sprache verschlagen hat. Wir erleben die große Geldinflation – eine beispiellose Ausweitung jeder Form von Geld, wie sie die Industrieländer noch nie gesehen haben.“

Paul Tudor Jones, CEO Tudor Investment Corp.

Key Takeaways

- **Die On-Chain-Geschwindigkeit nimmt für die meisten Münzen ab, während die Off-Chain-Geschwindigkeit zunimmt. Dies zeigt, dass das Wachstum spekulativer Transaktionen an der Börse schneller ist als das Wachstum bei der Verwendung von Kryptowährungen zum Kauf von Waren und Dienstleistungen.**

- **Nach unseren Untersuchungen gibt es weltweit mehr als 40 Millionen Kryptowährungsbenutzer. Überraschenderweise korreliert deren Anzahl in einem Land mit dem Pro-Kopf-BIP dieses Landes. Ein hohes BIP bedeutet eine stärkere Akzeptanz der Kryptowährung.**

- **Der adressierbare Zielmarkt für Krypto-Assets liegt bei ungefähr $212 Billionen. Die größten Anwendungsfälle umfassen das Tauschmittel einschließlich aller globalen Fiatwährungen im Wert von $126 Billionen und Konsumentenkredite mit einem globalen Wert von $42 Billionen. Wenn Bitcoin in den nächsten zehn Jahren 10 % dieses Marktes durchdringen würde, wäre jeder Bitcoin im Jahr 2030 $397.000 wert.**

Die Off-Chain-Geschwindigkeit von Bitcoin ist auf einem Allzeithoch. Fiatwährung mit einer hohen Geschwindigkeit ist normalerweise ein schlechtes Zeichen, aber gilt diese Regel auch bei Krypto?

Eine der gebräuchlichsten Methoden zur Schätzung des Preises einer Kryptowährung ist die Quantitätsgleichung. Die Gleichung stammt vom Ökonomen Irving Fisher aus dem 20. Jahrhundert. Eine der wichtigsten Erkenntnisse dieser Gleichung ist, **dass die Währung umso weniger Wert hat, je öfter eine Währung den Besitzer wechselt.** Geld wechselt häufiger den Besitzer, wenn die Leute glauben, dass es an Wert verliert. Wenn zum Beispiel eine hohe Inflation herrscht, halten die Leute so kurze Zeit wie möglich am Geld fest, bevor sie die heiße Kartoffel jemand anderem zuwerfen.

„Gold is up 12% year-to-date and Bitcoin is up 25% in the same time period.

I won't hold my breath for the media to write articles stating, ‚Bitcoin proving to be the best safe haven asset in the economic crisis.‘

But even their silence can't change the truth.“

Anthony Pompliano
Morgan Creek Digital
Mai 2020

In den letzten Jahren hat die Off-Chain-Geschwindigkeit von Bitcoin zugenommen. Aber was bedeutet das? Vitalik Buterin hat dieses Modell 2017 bekanntermaßen auf Krypto-Assets angewendet, um zu argumentieren, dass Münzen Geschwindigkeitsabnahmen benötigen, die das Horten fördern. Kyle Samani, Partner von Multicoin Capital, schrieb einen Artikel in Übereinstimmung mit Vitalks Verständnis von Geschwindigkeit. Er schrieb,

> *„Wie ich in* Understanding Token Velocity *erwähnt habe, ist das V in der Wechselkursgleichung ein großes Problem für praktisch alle proprietären Zahlungswährungen. Proprietäre Zahlungswährungen sind im Allgemeinen anfällig für das Geschwindigkeitsproblem, das einen anhaltenden Preisdruck nach unten ausübt. Aufgrund dieses Effekts erwarte ich, dass Utility-Token, bei denen es sich nur um proprietäre Zahlungswährungen handelt, eine Geschwindigkeit von 100 überschreiten. Geschwindigkeiten von 1.000 sind sogar möglich.“*

Scott Locklin, Ingenieur bei Brave Attention Token, erklärt jedoch in einem kürzlich erschienenen Artikel, dass sowohl Buterin als auch Samani falsch liegen. In diesem Artikel wird der Preis von Bitcoin anhand der Quantitätsgleichung erläutert und warum die Beziehung möglicherweise nicht so einfach ist, wie Buterin und Samani erörtert haben.

Einleitung in die Quantitätsgleichung

Jedes verteilte Hauptbuchnetzwerk bietet seinen Kryptowährungsbenutzern eine Reihe von Funktionen. **Der Grundwert einer Münze kann als die Gesamtsumme der Bewertung des Netzwerks durch jeden einzelnen Benutzer definiert werden.** Die kurzfristigen Preise von Kryptowährungen werden von Angebot und Nachfrage bestimmt und spiegeln möglicherweise nicht

ihre Grundwerte wider. Der Preis kann jedoch langfristig ein verrauschtes Signal für den Grundwert einer Kryptowährung sein. Langfristig bezieht er sich auf mehrere Perioden makroökonomischer Zyklen, einschließlich Erweiterungen und Rezessionen, die der Kryptowährungsmarkt noch nicht abgeschlossen hat.

Mehrere Studien haben die Quantitätsgleichung verwendet, um den Bitcoin-Preis in 5 Jahren, 10 Jahren und sogar für längere Zeithorizonte zu schätzen. Zum Beispiel schätzten Kraken und der Economist den Preis von Bitcoin bis 2022 auf $1,91 Millionen,[1] Satis bis 2023 auf $96.000[2] und Vision & bis 2028 auf $65.000[3]. Der Hauptgrund dafür, dass jeder Bericht unterschiedliche Preise hat, ist die Schätzung der zukünftigen Nachfrage nach Bitcoin und anderen Münzen basierend auf Annahmen. Die Gleichung ist ein absoluter Ansatz zur Bewertung von Krypto-Assets. Dies bedeutet, dass es einen Zielpreis angibt, zu dem Krypto-Assets auf der Grundlage von Annahmen bezüglich Änderungen von Angebot und Nachfrage bewertet werden sollten.

Die Quantitätsgleichung beruht auf der Theorie, dass der Wert jeder Kryptowährung direkt mit dem Dollarvolumen der von ihr unterstützten Wirtschaft korreliert sein sollte. Eine Krypto-Asset-Wirtschaft mit einem Handelsvolumen von $1.000 pro Jahr und 10 im Umlauf befindlichen Münzen hat einen fairen Münzwert von $100, wenn jede Münze in diesem Jahr einmal gehandelt wird. Der Wert jedes Krypto-Assets steht in umgekehrter Beziehung zu seinem Vorrat, d. h. der Anzahl der im Umlauf befindlichen Münzen und seiner Geschwindigkeit, also der Häufigkeit, mit der jede Münze pro Jahr gehandelt wird. Das BIP-Wachstum jeder Münze oder der Krypto-Asset-Wirtschaft wird durch die Anpassung des Produktmarktes bestimmt. **Die Wahrscheinlichkeit einer zukünftigen Marktakzeptanz ist heute das, was Spekulationen antreibt.**

Der absolute Bewertungsansatz ist von Mills Wechselkursgleichung inspiriert, die später von Irving Fisher formuliert wurde.[4] In diesem Modell kann der Prozentsatz des gesamten adressierbaren Marktes (Target Addressable Market, TAM) verwendet werden, um den implizierten zukünftigen Preis eines Krypto-Assets zu schätzen. Die traditionelle Gleichung MV = PQ wurde erstmals von Chris Burniske in seinem ursprünglichen Bericht 2016 für Coinbase auf Bitcoin angewendet.[5] Die Wechselkursgleichung MV = PQ beschreibt das Gleichgewicht zwischen Geld in der Wirtschaft und der Nachfrage nach diesem Geld für den Kauf von Waren und Dienstleistungen.

Interaktive Excel-Tabellen
Dieses Kapitel beinhaltet Excel-Tabellen, mit deren Hilfe unsere Leser den Preis von Krypto-Assets basierend auf ihren Recherchen und Annahmen schätzen können.

—

1 Rodrigo Cherniauskas, Beatrice Gorski und David Murchland, *Kraken Investment Proposal*, The Economist, Oktober 2016. Abgerufen von https://www.economist.com/sites/default/files/fia__the_navigators__kraken_investment_case_analysis__full_submission.pdf

2 Sherwin Dowlat, „Cryptoasset Market Coverage Initiation: Valuation August 30, 2018“, *Satis Group*, 2018. Abgerufen von https://research.bloomberg.com/pub/res/d37g1Q1hEhBkiRCu_ruMdMsbc0A

3 Dr. Lidia Bolla und Christian Schüpbach, *The Blockchain Story. What's it all worth?* [Report], Vision&, Mai 2018. Abgerufen von https://www.visionand.ch/wp-content/uploads/2018/06/vision_Valuation.pdf

4 John Stuart Mill, *Principles of Political Economy*, London, John W. Parker, 1848.

5 Chris Burniske and Adam White, „Bitcoin: Ringing The Bell For A New Asset Class“ [Whitepaper], *Ark Invest*, Januar, 2017. Abgerufen von https://research.ark-invest.com/hubfs/1_Download_Files_ARK-Invest/White_Papers/Bitcoin-Ringing-The-Bell-For-A-New-Asset-Class.pdf

"What is the one investment all of these investors have in common?

Paul Tudor Jones

Marc Lasry

Bill Miller

Mike Novogratz

Raoul Pal

Chamath Palihapitiya

Peter Thiel"

Barry Silbert
CEO Digital Currency Group
Mai 2020

Um die Größe der von Krypto-Assets unterstützten Wirtschaft abzuschätzen, werden die folgenden Schritte ausgeführt:

- Die wirtschaftliche Größe aller relevanten Anwendungsfälle für ein Krypto-Asset wird summiert. Dies wird als TAM bezeichnet. **Dies beinhaltet drei Annahmen:**
  - Welche Anwendungsfälle gelten für Kryptowährungen?
  - Wie hoch ist die Gesamtkapitalisierung in USD für jeden Anwendungsfall? **(PQ)**
  - Wie hoch ist das Wachstum der gesamten Marktkapitalisierung in USD für jeden Anwendungsfall in den nächsten zehn Jahren?
- Es wird eine Schätzung des Prozentsatzes jedes adressierbaren Zielmarkts berechnet, der über einen Zeitraum von zehn Jahren von Krypto-Assets durchdrungen wird. **Dies beinhaltet zwei Annahmen:**
  - Wie viel von jedem Anwendungsfall wird von Kryptowährungen durchdrungen?
  - Wie hoch ist die Penetrationswachstumsrate für Kryptowährungen in den nächsten zehn Jahren? **Dies beinhaltet eine Annahme**:
    - Um die Wachstumsrate der Penetration für Kryptowährungen im nächsten Jahrzehnt abzuschätzen, kann eine angenommene Akzeptanzrate von Kryptowährungen einer S-Kurve, einer linearen Kurve, einer Exponentialkurve, einer Mittelwertumkehrkurve oder einer logarithmischen Kurve folgen. **In diesem Artikel wird eine S-Kurve für alle Kryptowährungen angenommen.**
- Jeder jährliche TAM wird durch die Geschwindigkeit jeder Münze geteilt, um die Marktkapitalisierung der Münze zu bestimmen. **Dies beinhaltet drei Annahmen:**
  - Wie hoch ist das Angebot **(M)** jeder Kryptowährung im nächsten Jahrzehnt?
    - Einige Kryptowährungen folgen Lieferplänen, z. B. Bitcoin, das einer Poisson-Verteilung folgt.
    - Andere Münzen haben Vorräte, die von einem Abstimmungsmechanismus abhängen, wie z. B. EOS.
    - Ersteres weist daher einen geringeren Prognosefehler auf als Letzteres. In dieser Analyse wird angenommen, dass das Angebot jeder Kryptowährung die durchschnittliche Größe der Krypto-Asset-Basis im Laufe des Jahres ist, was aufgrund des inflationären Charakters der meisten Krypto-Asset-Protokolle, einschließlich Bitcoin, erforderlich ist.
  - Wie hoch ist die Geschwindigkeit **(V)** für jede Kryptowährung??

- Wie hoch ist das Geschwindigkeitswachstum für jede Kryptowährung im Laufe der Zeit?

- Um den Preis pro Münze zu bestimmen, wird der gesamte TAM multipliziert mit der Penetrationsrate durch sein zirkulierendes Angebot geteilt.

- Sobald der Preis pro Münze für jedes Jahr im nächsten Jahrzehnt prognostiziert ist, muss der Abzinsungssatz angewendet werden, um den Barwert des Preises jeder Münze für jedes Jahr zu berechnen. **Dies beinhaltet die folgende Annahme:**
  - Der Abzinsungssatz sollte das Risiko jeder Münze und die nominale Inflationsrate widerspiegeln. **In diesem Bericht wird ein Standardabzinsungssatz von 30% für jede Münze angenommen.**

Geschwindigkeit – Beispiel
Wenn der Gesamtbetrag der mit Bitcoin in einem Jahr bezahlten wirtschaftlichen Transaktionen $100 Milliarden beträgt und jeder Bitcoin im Laufe des Jahres durchschnittlich zehnmal den Besitzer wechselt, beträgt der Gesamtwert der Münzen $10 Milliarden, und wenn es 18 Millionen Bitcoin im Umlauf gibt, dann würde dies bedeuten, dass der Nutzpreis für jeden Bitcoin ungefähr $555 beträgt. Wenn sie 100 Mal im Umlauf sind, sind die Sammelmünzen $1 Milliarde wert, was $55 pro Bitcoin entspricht.

Annahmen im Detail

Geldversorgung
Das (M) in MV = PQ wird durch die im Umlauf befindliche Lieferung eines Krypto-Assets gemessen. **(M) ist die Geldbasis, die zur Unterstützung einer Wirtschaft erforderlich ist.** Das Angebot einiger Kryptowährungen ist leicht abzuschätzen, wenn ihr Angebot vorgegebenen Prozessen folgt (Bitcoin and Poisson, etc.). Das Angebot kommt aus zwei Hauptbereichen: neue Münzen, die entweder durch Mining, Absteckung oder Reserveverkäufe in Umlauf gebracht werden, und Münzen, die aus Walltes auf dem Markt verkauft werden. Das Ziel von „M“ ist es, die Anzahl der Münzen zu schätzen, die jedes Jahr im Umlauf sind und auf dem Markt verfügbar sein werden. Dies wird oft als Float bezeichnet, welche aus zwei Teilen besteht: „Stock“ und „Flow“. Der Flow ist der Betrag des Krypto-Assets, der jedes Jahr ausgegeben wird, und Stock gibt an, wie viel bereits ausgegeben wurde.

Dieser Bericht geht von einem stabilen Angebot jedes Krypto-Assets für jedes Jahr aus und prognostiziert das Angebot über das Jahrzehnt basierend auf dem programmierten Versorgungsplan jedes Krypto-Assets in seinem Protokoll. Eine eingehendere Analyse würde jedoch versuchen, das zukünftige zirkulierende Angebot vorherzusagen, indem der Float oder das zirkulierende Angebot jeder Kryptowährung berechnet wird. Um den Float zu berechnen, „hodled“ Vermögenswerte oder Vermögenswerte, die gehortet werden, müssen abgezogen werde. Wenn beispielsweise 100 Millionen Münzen ausgegeben und 60% in Wallets aufbewahrt werden, die sich nie bewegen, entspricht das M 40 Millionen Münzen. Dies galt für Coinbase-Benutzer, die Bitcoin im Jahr 2016 gekauft hatten. 57 % der Coinbase-Benutzer hielten ihren Bitcoin im Jahr 2016 als Wertspeicher und spekulatives Gut, anstatt Bitcoin als Tauschmittel zu verwenden.[6]

—

6 Ibid.

Geschwindigkeit

(V) ist die Geschwindigkeit jeder Geldeinheit auf der Geldbasis. Wenn Alice einmal im Jahr einen Bitcoin an Bob weitergibt, entspricht dies einer jährlichen Geschwindigkeit von 1. Wenn Bob denselben Bitcoin an Eve weitergibt, entspricht dies einer jährlichen Geschwindigkeit von 2. Der Wert einer Münze ist umgekehrt proportional zum gesamten reduzierten Angebot und umgekehrt proportional zur Geschwindigkeit. Somit verliert eine Währung, die ihre Geschwindigkeit erhöht, gegenüber jeder anderen Währung, deren Geschwindigkeit nicht so stark zunimmt, an Wert.

Die Geschwindigkeit ist eine Schlüsselvariable, bei der viele Berichte voneinander abweichen. Die Geschwindigkeitsschätzung von Vision & war 10. Um dies ins rechte Licht zu rücken, hat die M1-Geldmenge der USA eine Geschwindigkeit von ungefähr 5. Was die Geschwindigkeit verringert, ist Reibung. Da Krypto-Assets von Haus aus digital sind, ist ihre Reibung geringer als bei physischem Geld, was die Geschwindigkeit im Vergleich zu physischen Währungen nach oben drückt. Auf der anderen Seite weisen physische Fiatwährungen hohe Inflationsraten auf, die eine hohe Geschwindigkeit fördern. Kryptowährungen mit niedrigen Inflationsraten und Kaufkraftsteigerung werden einen Abwärtsdruck auf die Geschwindigkeit haben.

„In 2012, I paid 5 BTC for 1lbs of coffee beans. The coffee wasn't good. Everyone in bitcoin has had a ‚pizza day' spending moment. Some of you just haven't realized it yet."

Andreas Antonopoulos
Mai 2020

Dieser Bericht geht von einer stabilen Geschwindigkeit jeder Münze im nächsten Jahrzehnt aus. Die Geschwindigkeitszahl wird basierend auf der Chain-Geschwindigkeit 2019 jeder Münze berechnet. Die Geschwindigkeit wird berechnet, indem das jährliche Handelsvolumen in US-Dollar durch das On-Chain-Transaktionsvolumen des Netzwerks dividiert und dann ein Jahresdurchschnitt für 2019 gebildet wird. Eine eingehendere Analyse würde versuchen, die durchschnittliche Menge an gehorteten Assets vorherzusagen, die jede Münze jedes Jahr haben wird. Gehortete Krypto-Assets senken die durchschnittliche Jahresgeschwindigkeit jeder Münze, da sie eine Geschwindigkeit von Null haben. Wie bereits erwähnt, hatten 57 % der Coinbase-Benutzer, die 2016 Bitcoin besaßen, eine Geschwindigkeit von Null. Bei Staking-Münzen wie Dash muss auch die Geschwindigkeit angepasst werden, da Staking-Münzen eine Geschwindigkeit von Null haben.

Adressierbarer Zielmarkt

- **(P)** ist der durchschnittliche Preis von Waren in der Wirtschaft. In Bezug auf Währung, Nützlichkeit und Stablecoins entspricht der Preis den Kosten der bereitgestellten Ware oder Dienstleistung.
- **(Q)** ist die Warenmenge in der Wirtschaft.

Die globale Gesamtnachfrage nach Krypto-Assets **(PQ)** wird berechnet, indem die Größe jedes adressierbaren Zielmarkts (Target Addressable Market, TAM) für jede Münze für jedes Jahr und der prozentuale Anteil der Münze an der TAM pro Jahr bestimmt wird.

Es können jedoch nicht alle Anwendungsfälle von allen Münzen bedient werden. Zunächst müssen wir also zwischen vier Arten von Münzen unterscheiden:

- Ein Wertspeicher ist eine verteilte Ledger-Technologie, mit der der Wert im Laufe der Zeit sicher gespeichert werden kann. Währungsmünzen **verfügen häufig nicht über Turing-vollständige Protokolle**, die anspruchsvolle intelligente Verträge auf der ersten Ebene ihres verteilten Netzwerks ermöglichen. Dazu gehören Kryptowährungen der ersten Generation wie Bitcoin, Litecoin und Bitcoin Cash.
- Utility Coins und Token, die Smart Contracts ermöglichen, gelten als Kryptowährungen der zweiten Generation. Smart Contracts sind automatisierte Vertragsvereinbarungen, die von einer Gruppe verschiedener Computer gespeichert werden, die häufig von Konfliktparteien und Fremden gesteuert werden. Diese Gruppe umfasst Münzen wie Ethereum, EOS und Stellar.
- Die dritte Generation von Kryptowährungen sind stabile Münzen, oder Stablecoins. Stablecoins sind normalerweise ERC-20-Token, die auf der Blockchain von Ethereum aufbauen und im Laufe der Zeit eine relativ stabile Kaufkraft in Bezug auf reale Güter und Dienstleistungen in der Wirtschaft aufrechterhalten. Zu den stabilen Münzen gehören Tether, USDC und auch Münzen, die in öffentlichen und erlaubnislosen verteilten Netzwerken wie MakerDao Sai ausgegeben werden.
- Privacy Coins sind ein Ableger der Kryptowährungen der ersten Generation. Sie sind häufig preislich volatil und verfügen über zusätzliche Funktionen, die Informationen zu jeder Transaktion verschleiern, darunter die Wallet-Adressen des Absenders und Empfängers sowie die Transaktionsmenge. Dies schließt Münzen wie Dash, Monero, Zcash, Beam, Grin und MimbleWimbleCoin ein.

„Technology evolves in a 14-year cycle around advances in computing power

'54 – Mainframe

'68 – Microchip

'82 – PC

'96 – Internet

'10 – Mobilenet

'24 – Trustnet

Imagine investing in $IBM in '50, Fairchild in '64, $MSFT in '78, $CSCO in '92, $AAPL in '06

That's #Bitcoin today...."

Mark Yusko
Morgan Creek Capital Management
April 2020

Tabelle 1: Münzkategorien

Wertspeichermünzen	**Bitcoin, Litecoin, Bitcoin Cash**
Utility Coins und Token	**Ethereum, EOS, Stellar**
Stablecoin	**MakerDao Dai, Tether**
Privacy Coin	**Monero, Dash, Zcash,** MimbleWimbleCoin

Sobald wir wissen, welche Münzen für welche Anwendungsfälle benötigt werden, müssen wir die Nachfrage für jeden Anwendungsfall berechnen. Die Werte für jeden Zielmarkt können additiv oder kannibalisch sein, d. h., dass es entweder doppelte Anforderungen an ein einzelnes Angebot geben kann oder dass sich die Anforderungen gegenseitig ausschließen und nicht hinzugefügt werden sollten. In

Tabelle 2 sind die angenommenen TAMs für Kryptowährungen aufgeführt, einschließlich Überweisung, Steuerflucht, Offshore-Konten, Wertspeicher, Online-Transaktionen, Mikrozahlungen, STO- und ICO-Finanzierung, Krypto-Handel, Glücksspiel, Online-Glücksspiel, Nichtbanken, Konsumentenkredite, Rechnungseinheit und Tausch- und Reservewährungsmedium.

Um den TAM der kommenden Jahre zu prognostizieren, ist eine vernünftige Annahme über das künftige Wachstum dieses Marktes erforderlich. **In diesem Artikel wird für jeden TAM eine durchschnittliche jährliche Wachstumsrate angenommen.** Für einige der oben aufgeführten Kategorien fehlen zuverlässige CAGR-Daten. **Für diese haben wir eine Schätzung angenommen, die auf der CAGR des S&P 500-Index im Zeitraum von 2000 bis 2018 basiert**, da eine vernünftige Annahme der Wachstumsrate das langfristige Wachstum der Weltwirtschaft sein könnte. Darüber hinaus glauben wir, dass einige der CAGR-Werte für die anderen Kategorien aufgrund des langen Bull Runs in den letzten 10 Jahren möglicherweise überhöht sind. Eine überfällige Marktkorrektur dürfte sie um mindestens 20 bis 30 % senken. **Die V-förmige Erholung des Corona-Virus wird offensichtlich durch die Abwertung von Fiatwährungen unterstützt, was selbst nicht nachhaltig ist.** Daher ist die Marktkapitalisierung für jeden TAM höchstwahrscheinlich eine Obergrenze.

(PQ) wird in traditionellen Wirtschaftsmodellen normalerweise als BIP gemessen. Spekulationen über finanzielle Vermögenswerte werden jedoch üblicherweise nicht in die BIP-Kennzahlen einbezogen. Das Devisenvolumen ist beispielsweise nicht im BIP enthalten. Schätzungen zufolge stammen ungefähr 30 % des On-Chain-Transaktionsvolumens eines Krypto-Assets aus Anlegerspekulationen, wenn Kryptowährungen zwischen Börsen transferiert werden. Daher ist die Berechnung von PxQ anhand des On-Chain-Transaktionsvolumens ein verrauschtes Signal. Auch die Vorhersage von PxQ in der Zukunft nach dem heutigen Transaktionsvolumen weist einen großen Schätzfehler auf. Stattdessen ist es besser, sich auf die adressierbaren Zielmärkte und das Wachstum in diesen Märkten zu konzentrieren.

Tabelle 2: TAMs für Krypto-Assets in Milliarden USD

Adressierbarer Zielmarkt (TAM)	Aktuelle Kapitalisierung	Implizierte Kapitalisierung zum Jahresende 2020	Implizierte Kapitalisierung zum Jahresende 2029	CAG-Daten	Münze
Rechnungseinheit und Tauschmittel[7]	126.800	136.094	187.101	3,60 %	Stablecoin, Wertspeicher
Konsumenten-kredite[8]	42.263	46.489	71.381	4,9 %	Stablecoin

—

7 Jeff Desjardins, „All of the World's Money and Markets in One Visualization", *Visual Capitalist*, 26. Oktober 2017. Abgerufen von http://money.visualcapitalist.com/worlds-money-markets-one-visualization-2017/

8 „Global consumer lending: size, segmentation and forecast for the worldwide market", *The Free Library*, 4. Mai 2016. Abgerufen von https://www.thefreelibrary.com/Global+consumer+lending%3A+size%2C+segmentation+and+forecast+for+the...-a0451297122

Offshore-Konten[9][10]	19.000	19.684	27.061	3,6 %	Wertspeicher, Stablecoin, Privacy Coin
Reservewährung[11, 12][13]	11.737	13.290	23.247	6,4 %	Wertspeicher
Wertspeicher[14]	7.070	7.112	7.307	0,30 %	Wertspeicher
Online-Transaktionen[15][16]	3.403	3.869	13.971	13,7 %	Alle
Überweisungen[17][18][19]	706	755	1.389	7,0 %	Stablecoin, Wertspeicher
Mikrozahlungen[20]	617	934	6.020	23,0 %	Alle
Steuerhinter-ziehung[21,22][22][23][24]	600	769	1.346	6,4 %	Wertspeicher, Stablecoin, Privacy Coin
Ohne Bankkonto[25]	380	388	429	1,1 %	Wertspeicher, Stablecoin

—

9 Kenneth Rapoza, „Tax Haven Cash Rising, Now Equal To At Least 10% Or World GDP“, *Forbes*, 15. September 2017. Abgerufen von https://www.forbes.com/sites/kenrapoza/2017/09/15/tax-haven-cash-rising-now-equal-to-at-least-10-of-world-gdp/#2678190870d6; „Global GDP (gross domestic product) at current prices from 2010 to 2022 (in billion U.S. dollars)“, *Statista*, 2019. Abgerufen von https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/

10 Jannick Damgaard, Thomas Elkjaer, und Niels Johannesen, „Piercing the Veil“, *IMF,* Juni 2018. Abgerufen von https://www.imf.org/external/pubs/ft/fandd/2018/06/inside-the-world-of-global-tax-havens-and-offshore-banking/damgaard.htm

11 Richard Leong, „U.S. dollar share of global currency reserves fall further – IMF“, *Reuters*, 1. Juli 2018. Abgerufen von https://www.reuters.com/article/uk-forex-reserves/u-s-dollar-share-of-global-currency-reserves-fall-further-imf-idUSKBN1JR21G

12 Verwendung von S&P CAGR, aufgrund fehlender Daten.

13 IMF, „Currency composition of official foreign exchange reserves“. Abgerufen von http://data.imf.org/?sk=E6A5F467-C14B-4AA8-9F6D-5A09EC4E62A4

14 Sean Williams, „How Does Bitcoin's Market Cap Stack Up Next to Gold, the S&P 500, and the U.S. Dollar?“, *The Motley Fool*, 17. August 2017. Abgerufen von https://www.fool.com/investing/2017/08/17/how-does-bitcoins-market-cap-stack-up-next-to-gold.aspx; Martin Fridson, "Time To Go For Gold?," *Forbes*, August 12, 2016. Abgerufen von https://www.forbes.com/sites/investor/2016/08/12/time-to-go-for-gold/#74f2f6622969

15 „Digital Payments“, *Statista*, 2019. Abgerufen von https://www.statista.com/outlook/296/100/digital-payments/worldwide

16 Digital Payments Market – Growth, Trends and Forecast (2020–2025). Abgerufen von https://www.mordorintelligence.com/industry-reports/digital-payments-market

17 Toby Shapshak, „Global Remittances Reach $613 Billion Says World Bank“, *Forbes*, 21. Mai 2018. Abgerufen von https://www.forbes.com/sites/tobyshapshak/2018/05/21/global-remittances-reach-613bn-says-world-bank/#6d1d2d625ddc

18 2019 World-Bank-Daten. Abgerufen von https://www.worldbank.org/en/topic/migrationremittancesdiasporaissues/brief/migration-remittances-data

19 World Bank Group, „Migration and Remittances“, April 2019. Abgerufen von https://www.knomad.org/sites/default/files/2019-04/Migrationanddevelopmentbrief31.pdf

20 Medici Team, „Payment Entrepreneurs go after MicroPayments segment; $13 B+ Opportunity globally“, *Medici*, 1. February 2014. Abgerufen von https://gomedici.com/payment-entrepreneurs-go-micropayments-segment-13-b-opportunity-globally/

21 Niall McCarthy, „The Global Cost of Tax Avoidance“, *Statista*, 24. März 2017. Abgerufen von https://www.statista.com/chart/8668/the-global-cost-of-tax-avoidance/

22 Verwendung von S&P CAGR, wegen fehlender Daten

23 Nicholas Shaxson, „Tackling Tax Havens“, *IMF,* September 2019. Abgerufen von https://www.imf.org/external/pubs/ft/fandd/2019/09/tackling-global-tax-havens-shaxon.htm

24 Petr Janský, „Hearing on Evaluation of Tax Gap“, Karls-Universität, Prag, Tchechische Republik, 23. Januar 2019. Abgerufen von http://www.europarl.europa.eu/cmsdata/161049/2019%2001%2024%20-%20Petr%20Jansky%20written%20questions%20-%20Ev_TAX%20GAP.pdf

25 Jeff Desjardins, „Banking the Unbanked is a $380B Opportunity“, *Visual Capitalist*, 20. Juli 2017. Abgerufen von https://www.visualcapitalist.com/banking-unbanked-emerging-markets/

Glücksspiel[26][27]	149	181	397	10,3 %	Utility Coins und Token
Online-Glücksspiel [28][29]	59	70	149	8,8 %	Utility Coins und Token, Privacy Coin
Krypto-Handel[30,31]	18,25	20.665	36.147	6,4 %	Alle
ICO-Finanzierung[32,33][34]	7,3	7,8	14,6	6,4 %	Utility Token
STO-Finanzierung[35][36]	0,57	0,61	1,1	6,4 %	Alle

Adressierbarer Zielmarkt für Krypto-Assets

In diesem Abschnitt werden die wichtigsten Anwendungsfälle von Kryptowährungen beschrieben: Wertspeicher, Überweisung, Steuerflucht, Offshore-Einlagen, Glücksspiel, Online-Glücksspiel, Bereitstellung von Finanzdienstleistungen für alle ohne Bankkonto weltweit, Kreditvergabe, Online-Transaktionen, Tauschmittel und Rechnungseinheit, Reservevermögen , Mikrozahlungen, Krypto-Handel sowie ICO- und STO-Investitionen.

Tauschmittel und Rechnungseinheit

Ein Tauschmittel ist ein zwischengeschaltetes Instrument oder System, das den Verkauf, Kauf oder Handel von Waren zwischen Parteien erleichtert. Damit ein System als Tauschmittel fungieren kann, muss es einen Wertstandard darstellen. Die Verwendung eines Tauschmediums ermöglicht eine höhere Effizienz in einer Volkswirtschaft und stimuliert eine Steigerung der gesamten Handelsaktivität. In einem traditionellen Tauschhandelssystem kann der Handel zwischen zwei Parteien nur stattfinden, wenn eine Partei eine Ware hat, die eine andere Partei wünscht, und umgekehrt. Die Möglichkeit, dass dies gleichzeitig als Kreuzereignis geschieht – wenn jede Partei etwas wünscht, das die andere Partei hat – ist unwahrscheinlich. Dank eines Tauschmittels wie Gold kann ein Kuhbesitzer, der

—

26 Tom Wijman, „Mobile Revenues Account for More Than 50% of the Global Games Market as It Reaches $137.9 Billion in 2018“, Newzoo, 30. April 2018. Abgerufen von https://newzoo.com/insights/articles/global-games-market-reaches-137-9-billion-in-2018-mobile-games-take-half/

27 Teodora Dobrilova, „How Much Is the Gaming Industry Worth?“, 4. April 2019. Abgerufen von https://techjury.net/stats-about/gaming-industry-worth/#gref

28 „Global Gambling Industry: State of Play in 2018“, *Casino.org*, 2018. Abgerufen von https://www.casino.org/gambling-statistics/

29 „Online Gambling Market – Growth, Trends and Forecast (2019–2024). Abgerufen von https://www.mordorintelligence.com/industry-reports/online-gambling-market

30 „Global Charts“, *CoinMarketCap*, 2019. Abgerufen von https://coinmarketcap.com/charts/

31 Verwendung von S&P CAGR, aufgrund fehlender Daten

32 „Cryptocurrency ICO Stats 2018“, *CoinSchedule*, 27. Januar 2019. Abgerufen von https://www.coinschedule.com/stats.html?year=2018

33 Verwendung von S&P CAGR, aufgrund fehlender Daten

34 PwC, *5th ICO / STO Report*, Sommer 2019. Abgerufen von https://www.pwc.ch/en/publications/2019/Strategy&_ICO_STO_Study_Summer_2019.pdf

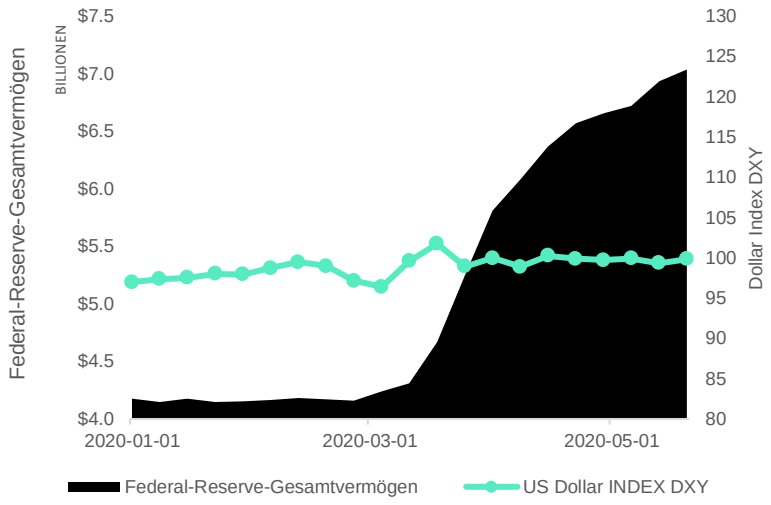
35 Ibid.

36 Token-Verkaufsstatistik. Abgerufen von https://www.coinschedule.com/stats/

auf dem Markt ist, um einen Rasenmäher zu kaufen, seine Kuh gegen Goldmünzen verkaufen, die er wiederum zum Kauf eines Rasenmähers verwenden kann.

Die Rechnungseinheit und das Medium der Devisenmärkte werden derzeit auf rund 126,8 Billionen geschätzt.[37] Wir könnten argumentieren, dass jede Krypto technisch gesehen ein Tauschmittel ist, jedoch nicht mehr als Bitcoin, da es sich um die primäre Kryptowährung handelt. Wenn wir alle BTC berücksichtigen, die derzeit für diesen Zweck verwendet werden, ergibt sich eine aktuelle Marktdurchdringung von 0,13%.

Abbildung 1: Federal-Reserve-Assets Verdoppeln Sich Fast und Dollar-Index Bleibt Unverändert



Quelle: St. Louis Federal Reserve Fred, Yahoo Finance, und CryptoResearch.Report

„Gentlemen, you can calm down. The printing presses run day and night again in three shifts.“

Rudolf Havenstein
President der Deutschen Reichsbank während der Hyperinflation der Weimarer Republik
1921–1923

Trotz beispielloser quantitativer Lockerung, Billionen kurzfristiger Kredite an den Pensionsgeschäftsmarkt und Senkung der Zinssätze auf Null **bewegte sich der US-Dollar-Index (DXY) kaum.** Dies bedeutet, dass der Dollar den Druckmaschinen viel mehr Missbrauch abnehmen kann, bevor er gegenüber anderen Fiatwährungen abgewertet wird. Auch die 5-Jahres-Inflationserwartung für den US-Dollar liegt bei niedrigen 1,43 %. Dies bedeutet, dass die Märkte trotz massiver Abwertung des US-Dollars erwarten, dass die Inflation unter dem Ziel der Federal Reserve von 2 % liegt. Fed-Vorsitzender Powell weiß, dass er mehr drucken kann und dies höchstwahrscheinlich auch tun wird.

Glücklicherweise hat die Blockchain-Technologie die Kosten für den Wechsel zwischen Währungen gesenkt. Telefonapplikationen wie Crypto.com erlauben den Menschen bereits, Zinsen für verschiedene Arten von Kryptowährungen und Stablecoins zu verdienen, die verschiedene Fiatwährungen darstellen. In Zukunft können Benutzer Portfolios mit Token-Währungen auf ihrem Bankkonto und

—

37 Jeff Desjardins, „All of the World's Money and Markets in One Visualization“, *Visual Capitalist*, 26. Oktober 2017. Abgerufen von http://money.visualcapitalist.com/worlds-money-markets-one-visualization-2017/

Telefon halten und Währungen einfach durch das Drücken einiger Tasten tauschen. Wenn die türkische Lira an Wert verliert, können sie in einen sicheren Hafen für stabile Münze wie einen tokenisierten Schweizer Franken wechseln. Wenn türkische Banken hohe Zinssätze anbieten, um Kapital anzuziehen, können die Menschen leicht zur türkischen Lira zurückkehren, um höhere Zinssätze für ihre Einlagen zu erzielen. Dies ist bereits aufgrund der Dollarisierung öffentlicher Blockchains möglich, die später in diesem Bericht in *Tether or Not to Tether* von Pascal Hügli erörtert wird.

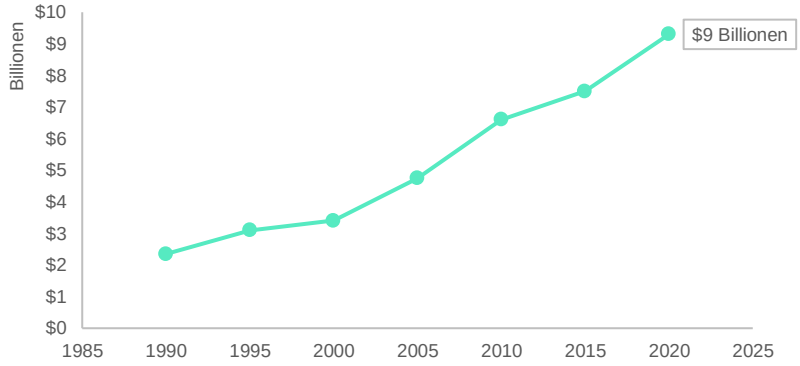
Offshore-Konten

„MALL of AMERICA in Minnesota announced it will miss 2nd payment on its $1.4 billion mortgage. An intelligent question is "Who is not getting paid?" Dominos starting to fall. IMF says debt will rise from $6 trillion to $66 trillion by end of 2020. Buy Gold Silver & Bitcoin."

Robert Kiyosaki
Mai 2020

The Tax Justice Network schätzt, dass Regierungen jährlich $180 Milliarden von den $21–32 Billionen Privatvermögen auf Offshore-Konten verlieren.[38] Der Internationale Währungsfonds schätzt die Steuerflucht weltweit auf etwa $12 Billionen pro Jahr.[39] Der Satis-Bericht analysierte die adressierbaren Zielmärkte für den gesamten Krypto-Asset-Markt und stellte fest, dass die implizite Gesamtmarktkapitalisierung bis 2028 $3,6 Billionen betragen würde, wobei ein ähnliches Modell verwendet wurde wie das in diesem Forschungsbericht entwickelte. Laut dem Satis-Bericht sind Offshore-Einlagen die Hauptanwendung von Kryptowährungen. **Sie schätzen, dass Kryptowährungen in den nächsten zehn Jahren etwa 91 % des Offshore-Einlagenmarktes durchdringen werden.**[40] Sie schätzen auch, dass der Offshore-Einlagenmarkt aufgrund von Kapitalkontrollen, Staatsverschuldung, unbeliebter Finanzpolitik und Abwertung der nationalen Fiatwährungen wachsen wird.

Abbildung 2: Kryptowährungen Werden Einen Teil des Globalen Offshore-Vermögensmarkets Absorbieren



Quelle: Forbes, IMF, CryptoResearch.Report

—

38 „Estimates of tax avoidance and evasion", tax justice network, 2020. Abgerufen von https://www.taxjustice.net/topics/more/estimates-of-tax-avoidance-and-evasion/

39 Jannick Damgaard, Thomas Elkjaer, und Niels Johannesen, „Piercing the Veil", *Finance and Development,* Juni 2018. Abgerufen von https://www.imf.org/external/pubs/ft/fandd/2018/06/inside-the-world-of-global-tax-havens-and-offshore-banking/damgaard.htm

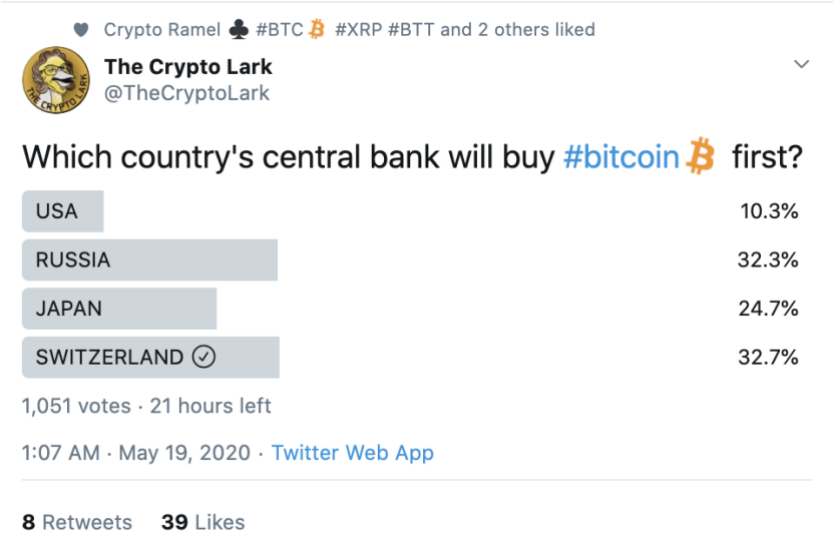
40 Sherwin Dowlat, „Cryptoasset Market Coverage Initiation: Valuation August 30, 2018", *Satis Group*, 2018. Abgerufen von https://research.bloomberg.com/pub/res/d37g1Q1hEhBkiRCu_ruMdMsbc0A

„According to Chainalysis, cryptocurrency e-commerce transactions account for $6 million daily.“

Obwohl der Satis-Bericht „Offshore-Konten“ und „Steuerflucht“ synonym verwendet, können Offshore-Konten auch für nicht illegale Zwecke wie die Eröffnung eines Geschäfts im Ausland und die Erzielung von Einkommen verwendet werden. Viele multinationale Unternehmen verfügen im Falle einer Bankenkrise in ihrer Landeswährung über Reserven im Ausland. Um ihr Vermögen vor finanziellen Katastrophen zu schützen, nutzen institutionelle Anleger die Verwendung von Offshore-Krypto-Einlagenkonten. Nach mehreren Schätzungen machen Offshore-Steueroasen 10 % des globalen BIP aus.[41] Zehn Prozent des globalen BIP liefern die Schätzungen für Offshore-Konten in der Excel-Tabelle. Eine durchschnittliche jährliche Wachstumsrate von 3,6 wird angenommen, um das zukünftige BIP und das Wachstum der Nachfrage nach Offshore-Depots vorherzusagen.

Reservewährung

Reservewährungen sind Fremdwährungen, die von Zentralbanken gehalten werden. Wenn ein Land Reserven erwirbt, stellt es die Währung nicht in den allgemeinen Umlauf. Stattdessen werden die Reserven in der Zentralbank geparkt. Die Reserven werden durch Handel erworben, wobei das erwerbende Land Waren gegen Währung verkauft.



Vielen Zentralbanken wird nachgesagt, sie hätten bereits Kryptowährungen gekauft. Gerüchten zufolge geben sie dies in der Öffentlichkeit nicht zu. Quelle: Twitter

Reservewährungen schmieren somit die Räder des internationalen Handels, indem sie Ländern und Unternehmen helfen, Transaktionen mit derselben Währung durchzuführen. Dies ist eine viel einfachere Aufgabe als die Abwicklung von Transaktionen mit verschiedenen Währungen. Ihre Popularität ist leicht zu erkennen: Zwischen 1995 und 2011 stieg der Betrag der in Reserve gehaltenen Währung um über 730 % von rund $1,4 Billionen auf $10,2 Billionen.

Reservewährungen werden in der Regel von entwickelten, stabilen Ländern ausgegeben. Die am häufigsten als Devisenreserve gehaltene Währung ist der US-Dollar, der nach Angaben des Internationalen Währungsfonds (IWF) Ende 2012 fast 62 % der zugewiesenen Reserven ausmachte. Weitere in der Reserve gehaltene Währungen sind der Euro und der japanische Yen, Schweizer Franken und Pfund Sterling. Der Dollar ist zwar immer noch die am weitesten verbreitete Reservewährung, hat jedoch eine verstärkte Konkurrenz durch den Euro erfahren. Der Euro ist von

—

41 Kenneth Rapoza, „Tax Haven Cash Rising, Now Equal To At Least 10% Or World GDP“, *Forbes*, 15. September 2017. Abgerufen von https://www.forbes.com/sites/kenrapoza/2017/09/15/tax-haven-cash-rising-now-equal-to-at-least-10-of-world-gdp/#2678190870d6/

etwas weniger als 18 % der zugewiesenen Reserven, als er 1999 an den Finanzmärkten eingeführt wurde, auf 24 % Ende 2011 gestiegen.

Der IWF meldet sowohl zugewiesene Reserven, was bedeutet, dass ein Land die in Reserven gehaltenen Währungen identifiziert hat, als auch die gesamten Devisenbestände. Der Gesamtprozentsatz der zugewiesenen Reserven ist im Laufe der Jahre stetig gesunken, von 74 % im Jahr 1995 auf 55 % im Jahr 2011. Ein Großteil dieser Verschiebung lässt sich durch die Änderung der Devisenbestände in Schwellen- und Entwicklungsländern erklären. 1995 hielten die Industrieländer rund 67 % der gesamten Devisenreserven, von denen 82 % zugewiesene Reserven waren. Bis 2011 war das Bild auf den Kopf gestellt worden: Schwellen- und Entwicklungsländer hielten 67 % der Gesamtreserven, weniger als 39 % wurden zugewiesen. Die Schwellenländer halten jetzt rund $6,8 Billionen in Reservewährung.[42] Derzeit liegen die Reservewährungen bei ca. $11,7 Billionen[43]. Keine Zentralbank hat bislang offiziell zugegeben Reserven in Form von Kryptowährung zu halten.

Wertspeicher

„The majority of Bitcoins have been held for more than 6 months. This provides evidence that the main use case for Bitcoin is not speculation and day trading."

Wie **Tabelle 2** zeigt, beträgt der Wertspeicher-TAM über $7 Billionen.[44] Diese Zahl stammt hauptsächlich aus der globalen Marktkapitalisierung von Gold. Menschen speichern den Wert jedoch auch in Fiatwährung. Allein der US-Dollar hat eine Marktkapitalisierung von $3,8 Billionen, was 20-mal mehr ist als die Marktkapitalisierung von Bitcoin. Die Menschen speichern ihr Vermögen auch in Aktien, Anleihen und Immobilien, sodass $7,07 Billionen eine Untergrenze für den größten Zielmarkt für Kryptowährungen darstellen. Wenn es um Wertspeicher geht, scheint die Kryptowährung Bitcoin am beliebtesten zu sein. Wenn wir bedenken, dass Wertspeicher-Suchende ihre Bitcoin nicht oft bewegen, können wir sehen, dass sich rund 11 Millionen BTC innerhalb fast eines Jahres nicht bewegt haben.[45] Dieser Betrag enthält unweigerlich einige verlorene Schlüssel. Zum Zeitpunkt der Erstellung dieses Berichts waren dies rund $98,6 Milliarden, was einer Penetration von 1,4 % entspricht.

Einige Kritiker argumentieren, dass Kryptowährungen nicht als Wertspeicher verwendet werden. Sie argumentieren, dass Kryptowährungen nur für Tageshandel und Spekulation verwendet werden. Ein gutes Maß dafür, ob Münzen als Wertspeicher oder für kurzfristige Spekulationen verwendet werden, ist das „Alter" jeder Münze. 20% aller existierenden Bitcoin haben ein Durchschnittsalter von über 5 Jahre.[46] Wir gehen davon aus, dass diese Münzen als Wertspeicher verwendet werden. Die Mehrheit der Bitcoins wird seit mehr als 6 Monaten

—

42 Brent Radcliffe, „A Primer on Reserve Currencies", *Investopedia,* 19. März 2020. Abgerufen von https://www.investopedia.com/articles/economics/13/reserve-currencies.asp

43 „Currency composition of official foreign exchange reserves", IWF. Abgerufen von http://data.imf.org/?sk=E6A5F467-C14B-4AA8-9F6D-5A09EC4E62A4

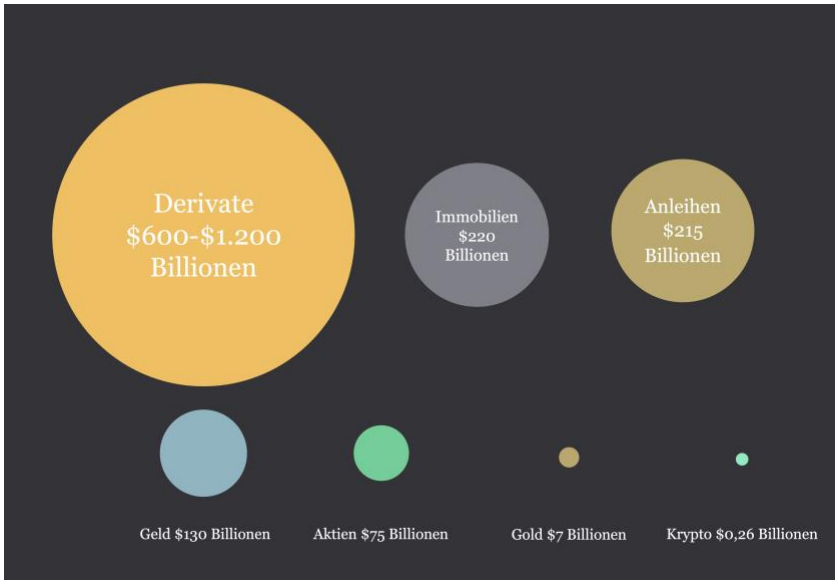
44 Sean Williams, „How Does Bitcoin's Market Cap Stack Up Next to Gold, the S&P 500, and U.S. Dollar?", *The Motley Fool*, 17. August 2017. Abgerufen von https://www.fool.com/investing/2017/08/17/how-does-bitcoins-market-cap-stack-up-next-to-gold.aspx

45 Jamie Redman, „Close to 11 Million BTC Haven't Moved in Over a Year", *Bitcoin.com*, 13. Januar 2020. Abgerufen von https://news.bitcoin.com/close-to-11-million-btc-havent-moved-in-over-a-year/

46 „Bitcoin UTXO Age Distribution", *Hodlwave*, 2020. Abgerufen von https://hodlwave.com/

gehalten, was belegt, dass Bitcoin-Besitzer Bitcoin **nicht für den Tageshandel verwenden, sondern für eine langfristige Aufwertung halten.** Zu den Faktoren, die die Verwendung und Akzeptanz von Krypto als Wertspeicher fördern, gehören Knappheit, Transparenz, globale Verfügbarkeit, Pseudonymität und Unveränderlichkeit.

Abbildung 3: Bitcoins TAM ist $1.247 Billionen Wert



Quelle: CryptoResearch.Report

„The best profit-maximizing strategy is to own the fastest horse. If I am forced to forecast, my bet is it will be Bitcoin."

Paul Tudor Jones
CEO Tudor Investment Corp.
Mai 2020

Einer der Faktoren, die zu einem Anstieg der Popularität beitragen, ist die Tatsache, dass die meisten digitalen Währungen ein begrenztes Angebot haben, was zu Knappheit führt. Währungen, die von zentralen Behörden kontrolliert werden, unterliegen häufig einer willkürlichen Inflation, insbesondere in Schwellenländern (Folkinshteyn & Lennon 2016). Paul Tudor Jones, der den Tudor BVI-Fonds verwaltet, hält aufgrund der massiven Haushaltsausgaben und des Anleihekaufs durch die Zentralbanken zur Bekämpfung der Coronavirus-Pandemie einen niedrigen einstelligen Prozentsatz seines Vermögens in Bitcoin-Futures. **Nach seiner Berechnung wurden seit Februar 2020 $3,9 Billionen gedruckt, was 6,6 % der globalen Wirtschaftsleistung entspricht.**

Online-Transaktionen

Laut einem Bericht von Mordor Intelligence über den digitalen Zahlungsmarkt und Daten von Statista machen Online-Transaktionen zwischen $4,4 Billionen und $3,4 Billionen pro Jahr aus.[47] Das Forschungsunternehmen Chainalysis schätzt, **dass Kryptowährungstransaktionen täglich $6 Millionen ausmachen.**[48]

—

47 „Digital Payments Market – Growth, Trends and Forecasts (2020–2025)", *Mordor Intelligence*, 2020. Abgerufen von https://www.mordorintelligence.com/industry-reports/digital-payments-market

48 Olga Kharif, „From Online Gambling to Pot, Crypto Commerce Takes Off This Year", *Bloomberg*, 6. November 2019. Abgerufen von https://www.bloomberg.com/news/articles/2019-11-06/crypto-commerce-jumps-65-as-tether-s-use-takes-off-this-year

Dies bedeutet, dass Kryptowährungszahlungen nicht einmal 1 % der Online-Transaktionen durchdrungen haben. Laut demselben Bericht von Chainalysis stieg der Betrag an digitalem Geld, der an 16 Händlerdienstleister wie BitPay gesendet wurde, zwischen Januar und Juli 2019 um 65 %. Dies liegt daran, dass Kryptowährungstransaktionen vergleichsweise schneller sind und optimalerweise nur einige Sekunden brauchen oder ungefähr eine Stunde, wenn Netzwerke überlastet sind. Es gibt auch keine Rückbuchungen bei Kryptowährungen, wodurch es zu weniger Online-Betrugsfällen kommt.
Transaktionsplattformen wie BitPay verzeichneten ein konstantes jährliches Wachstum der Transaktionsraten (DeVries, 2016). Laut einem BitPay-Jahresbericht im Jahr 2017 verzeichnete die Plattform gegenüber 2016 einen Anstieg des Zahlungsvolumens in US-Dollar um 328 % gegenüber dem Vorjahr. In diesem Zeitraum erhielten Händler, die die Plattform nutzen, monatlich mehr als $1 Million an Bitcoin-Zahlungen. Insgesamt war der Dienstleister auf dem Weg, in den Jahren 2017 und 2018 jährlich **über $1 Milliarde** durch Bitcoin-Zahlungsakzeptanz und -Auszahlungen zu verarbeiten.[49] Das B2B-Geschäft von BitPay wuchs zwischen 2017 und 2018 um 255 %, da sich Anwaltskanzleien, Rechenzentrums- und IT-Anbieter für die Akzeptanz von Bitcoin angemeldet hatten. BitPay beauftragte außerdem Rolf Haag, ehemaliger Geschäftsführer von Western Union und PayPal, als Head of Industry Solutions, der für das B2B-Geschäft verantwortlich ist.

Die Copay-Wallet, die BitPay-Wallet und andere Wallets, die den Bitcore Wallet Service (BWS) von BitPay verwenden, verfügen über mehr als 1,5 Millionen Wallets. Im vergangenen Jahr kam mit der BitPay-Wallet noch die Zusammenarbeit mit großen Geschenkkartenmarken hinzu, die es Benutzern ermöglicht, In-App-Geschenkkarten für Reisen, Essen und Shopping mit Bitcoin und Bitcoin Cash zu kaufen. Berühmte Händler wie Microsoft, CheapAir (Flüge), Travala (Hotelbuchungen)[50] und das Basketballteam von Dallas Mavericks akzeptieren Zahlungen in Kryptowährung, um Nischenmärkte von Kryptowährungsbesitzern zu erreichen. Zum Beispiel akzeptieren auch lokale Regierungen wie Tessin und Zug in der Schweiz und Seminole County, Florida, in den USA akzeptieren auch Kryptowährungszahlungen.

Der stationäre Handel, der Online-E-Commerce, Casinos und Steuereintreiber benötigen einen Zahlungsabwickler, um das Währungsrisiko der Akzeptanz von Kryptowährungen zu bewältigen. Aus diesem Grund sind Point-of-Sale-Systeme (PoS) für Software und Hardware ein interessantes Geschäftsmodell mit steigender Nachfrage. Der The Crypto Research Report befasste sich kürzlich mit der Einführung von PoS-Systemen durch Worldline und Ingenico in Europa im Sommer 2020. Weitere Unternehmen, die Kryptowährungszahlungen abwickeln, sind Salamantex, AnyPay, CryptoBuyer, GoCoin, Coinpayments und Coingate. Diese Unternehmen bieten Hardware- und Softwarelösungen für Händler an. Zum Beispiel verfügt Salamantex über eine Hardware, die Händler zu ihrem

—

49 Jan Jahosky, „BitPay Sees Record Year for Revenue in 2018, with $1 Billion in Transactions“, *BusinessWire*, 16. Januar 2019. Abgerufen von https://www.businesswire.com/news/home/20190116005701/en/BitPay-Sees-Record-Year-Revenue-2018-1

50 „Travala.com Monthly Report: October 2019“, *Travala.com*, 1. November 2019. Abgerufen von https://blog.travala.com/travala-com-monthly-report-october-2019/

vorhandenen Hardware-Point-of-Sale-System hinzufügen können. Gocoin, Coinpayments und Coingate bieten Plugins für E-Commerce-Webseiten wie Woocommerce, Shopify und Wordpress.

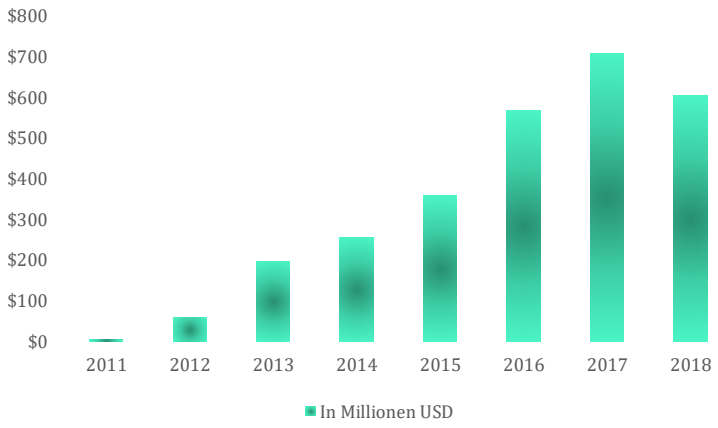
Der größte Start-up in diesem Bereich ist Spedn, das Flexa gehört, in welchen die Winklevoss-Zwillinge investiert haben. Damit können alle Starbucks-Coffeeshops in den USA seit 2020 Kryptowährungszahlungen akzeptieren. Coinbase bietet auch den Service der Zahlungsabwicklung an. Einer der jüngsten Neulinge in diesem Bereich ist Crypto.com. Es wird erwartet, dass sie für Furore sorgen werden.

„Still hilarious that oil went to $0 and Bitcoin didn't."

Anthony Pompliano
Morgan Creek Digital
Mai 2020

Obwohl Kryptowährungen ursprünglich als digitales Bargeld konzipiert wurden, haben Online-Transaktionen mit Kryptowährungen nicht wirklich an Bedeutung gewonnen. In einem kürzlich von Experten begutachteten Zeitschriftenartikel stellte Nicole Jonker fest, dass die Krypto-Akzeptanz bei Online-Händlern nur bescheiden ist (2 % aller Online-Shops).[51] Dies liegt hauptsächlich daran, dass die meisten Kryptowährungen deflationär sind und die Anleger sie nicht ausgeben möchten. Die meisten Händler konvertieren Krypto-Zahlungen in Fiat, um Volatilitätsprobleme zu vermeiden. Online-Transaktionen können jedoch mit Stablecoins akzeptiert werden, da sie nicht deflationär sind. Beispielsweise hat BitPay 2018 die Abwicklungsunterstützung für stabile US-Dollar-Münzen von Circle, Gemini und Paxos hinzugefügt.

Abbildung 4: Darknet-Volumen von $600 Millionen pro Jahr



Quelle: Chainanalysis, CryptoResearch.Report

Kryptowährungen werden nicht nur in stationären Geschäften und für Online-Einkäufe verwendet, sondern auch online für illegale Waren und Dienstleistungen ausgegeben. Laut Chainalysis wurde das **Darknet-Handelsvolumen 2017 auf $700 Millionen und 2018 auf $600 Millionen geschätzt.**[52,53]

—

51 Nicole Jonker, „What drives the adoption of crypto-payments by online retailers?", *Electronic Commerce, Research and Applications*, 35, Mai-Juni 2019. Abgerufen von https://www.sciencedirect.com/science/article/pii/S1567422319300250

52 Aaron van Wirdum, „Following the Waves Of Shutdowns, Remaining Darknet Markets Fill The Void (Again)", *Bitcoin Magazine*, 17. Juni 2019. Abgerufen von https://bitcoinmagazine.com/articles/following-wave-of-shutdowns-remaining-darknet-markets-fill-the-void-again

53 Chainalysis Team, „Crypto Crime Series: Decoding Darknet Markets", *Insights*, 18. Januar 2019. Abgerufen von https://blog.chainalysis.com/reports/decoding-darknet-markets

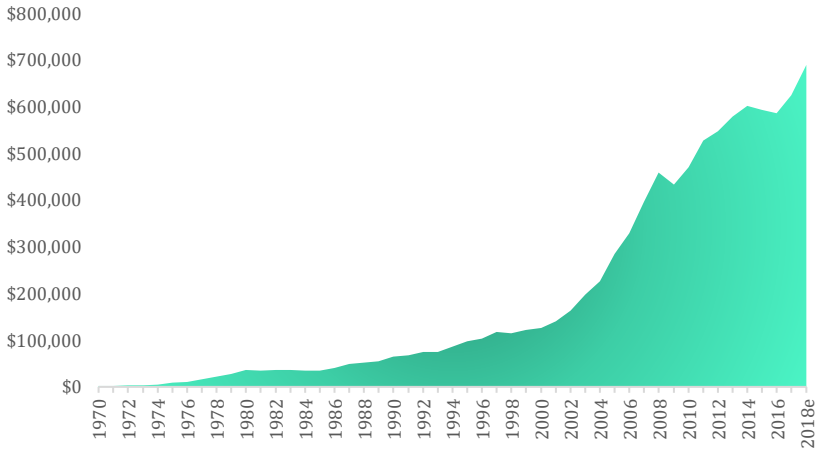
Überweisung

„A firefighter has never been criticized for using too much water.“

Stephen Poloz
Governeur, Bank of Canada

Im Jahr 2018 schickten Migranten in verschiedenen Teilen der Welt mehr als $613 Milliarden in ihre Heimatländer. Die Nutzung traditioneller Bankdienstleistungen bedeutet jedoch hohe Transaktionsgebühren und eine langsame Verarbeitung. Auf den Philippinen, einem der weltweit führenden Überweisungsmärkte, gibt es bereits Lösungen wie Coins.ph, die Krypto- und Blockchain-Technologie verwenden und es Einzelpersonen ermöglichen, Geld mit geringeren Gebühren nach Hause zu senden.

Abbildung 5: Überweisungsmarkt Wächst Jährlich



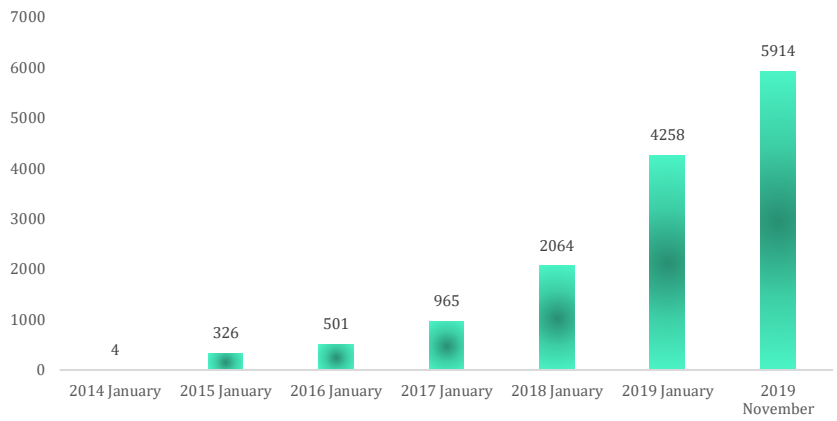
Quelle: World Bank, CryptoResearch.Report

Viele Überweisungen werden über Bitcoin-Geldautomaten mit Überweisungsfunktion ausgeführt. Diese Funktion ermöglicht es einer Person, britische Pfund in einen Geldautomaten in London einzuzahlen und einen Code zu erhalten, welchen sie Code an einen Verwandten oder Freund in New York senden können. Der Verwandte oder Freund kann mit diesem Code zu einem Bitcoin-Geldautomaten in New York gehen, ihn dort eingeben und dann US-Dollar erhalten. Diese Funktion funktioniert derzeit für über 100 Länder und 35 verschiedene Währungen.

„Swiss banks have been extremely reticent with regard to blockchain-based business models. As a result, it was almost impossible for entrepreneurs from the Zug Crypto Valley to open a company account for payment transactions (salaries, rent, accounts payable) We view ourselves as being significantly ahead of our competitors. We have now welcomed about 300 of these blockchain-friendly firms as clients here at Bank Frick.“

Bank Frick

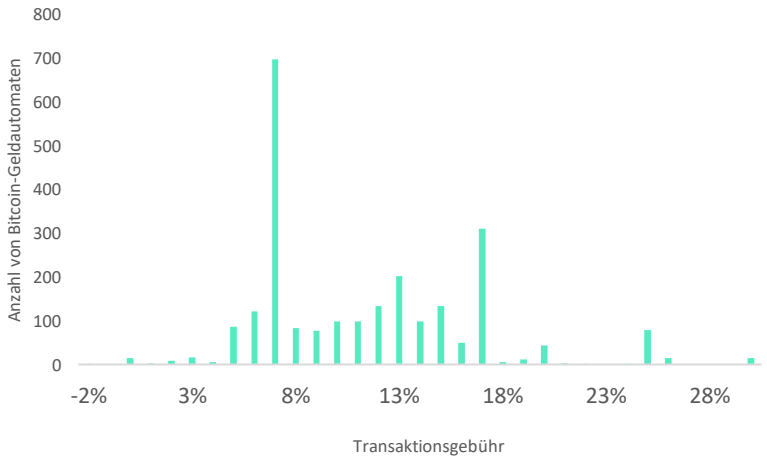
Abbildung 6: Die Anzahl der weltweit installierten Bitcoin-Automaten



Quelle: Coinatmradar.com, CryptoResearch.Report

Statistische Daten zur Anzahl der Bitcoin-Geldautomaten weltweit zeigen einen stetigen Anstieg im Laufe der Jahre. Im Januar 2016 zeigte Coinatmradar, dass es weltweit nur 501 von ihnen gab, aber bis Januar 2017 war die Zahl auf 965 gestiegen.

Abbildung 7: Die durchschnittliche Gebühr für Bitcoin-Automaten beträgt 10%



Quelle: Coinatmradar.com, CryptoResearch.Report

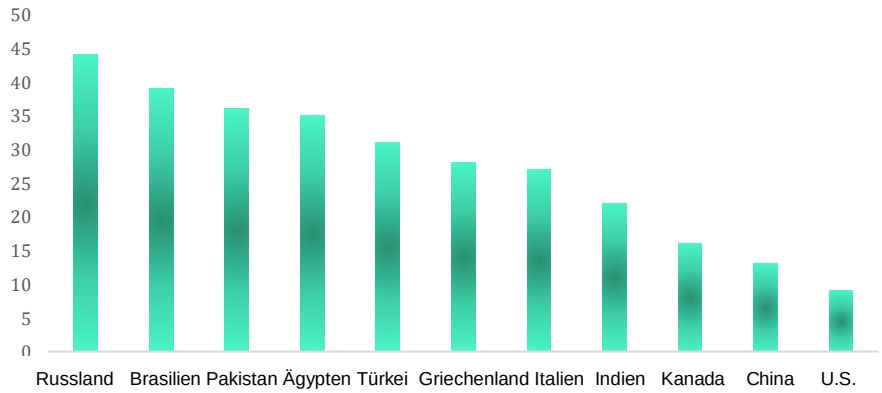
Im Januar 2018 hatten sie sich auf 2.073 mehr als verdoppelt und sich bis Januar 2019 fast nochmals, auf 4.112. Die durchschnittliche Gebühr für Bitcoin-Geldautomaten beträgt jedoch 10 %. In der Schweiz gibt es 84 Bitcoin-Geldautomaten, in DACH 296, ohne SBB- und Kiosk-Geldautomaten.

Steuerflucht

„Even if KYC/ AML is implemented on every exchange via the Travel Rule, money can still be laundered and hidden with cryptocurrencies by mining newly minted coins.“

Das ursprüngliche Ethos von Krypto war libertär, und diese Haltung ist in der Branche immer noch vorherrschend. Es ist keine Überraschung, dass einige Benutzer von Kryptowährungen ihre Gewinne nicht vollständig melden und dass einige Steuerflüchtlinge zu diesem Zweck Kryptowährungen einsetzen. Jedes Land hat ein einzigartiges Maß an Steuerflucht, und dieses Niveau ist im Laufe der Zeit dynamisch und hängt von Variablen wie Steuersätzen, Staatsschuldenbetrag, Verstaatlichungsgeschichte der Industrie, Kultur usw. ab. Kryptowährungen bieten Steuerflüchtlingen eine neue Möglichkeit, Vermögenswerte zu verbergen und sie werden auf diese Weise verwendet. **Selbst wenn KYC / AML bei jedem Umtausch über die Reisebestimmungen implementiert wird, kann Geld durch Mining neu geprägter Münzen gewaschen und mit Kryptowährungen versteckt werden.** Eine Möglichkeit, den Zugriff auf nicht verfolgte oder „schmutzige“ Bitcoin- und andere Kryptowährungen sicherzustellen, besteht darin, ein Kryptowährungs-Miner zu werden. Kryptowährungs-Miners können aus einfachen Grafikkarten und Strom nicht nachverfolgbare Assets machen. Es gibt Hinweise darauf, dass Miners in Asien in die Mining-Industrie eintreten, um ohne das Wissen der Steuerbehörden Kapital aus China und Indien herauszuschaffen. Eine andere Möglichkeit besteht darin, Münzen mit Bargeld zu kaufen. Der Krieg gegen Bargeld (Geldentwertung großer Denominationen) und die Inflation haben jedoch die Fähigkeit verringert, mit großen Mengen an Bargeld zu handeln. Daher wird sich ein großer Teil der Steuerflucht und Geldwäsche in diesem Bereich auf das Mining konzentrieren. Dies ist eine Form der Steuerflucht für vermögende Privatpersonen und Unternehmen.

Abbildung 8: Größe der Unversteuerten „Schatten“-Wirtschaft in Ausgewählten Ländern 2010 als Anteil am BIP



Quelle: Tax Justice Network, Bloomberg Businessweek, CryptoResearch.Report

Aufgrund der Schwierigkeit, das Ausmaß der Steuerflucht weltweit abzuschätzen, und der Schwierigkeit, diese Variable für die Zukunft vorherzusagen, wird in diesem Report die Wachstumsrate des S&P 500 verwendet und davon ausgegangen, dass der Prozentsatz der Steuerflucht in der Wirtschaft über die Zeit konstant ist. **In diesem Report wird der Markt für Steuerflucht basierend auf Schätzungen der Universität der Vereinten Nationen auf $600**

Milliarden geschätzt.[54] Steuerflucht durch Institute und vermögende Privatpersonen wird aufgrund der Beträge eher auf Datenschutzmünzen und Münzen mit geringer Volatilität wie Stablecoins und Bitcoin als auf physisches Fiatbargeld abzielen. Dies ist jedoch auch ein großer Teil der Steuerflucht durch „schwarze Volkswirtschaften", in denen die unteren und mittleren Schichten keine Gewinne ausweisen. Physisches Fiatbargeld ist möglicherweise besser für die Steuerflucht auf dem Schwarzmarkt durch Arbeitnehmer der Mittelklasse und der unteren Klasse, da es keine Aufzeichnungen gibt und die Volatilität begrenzt ist. Schwarzmärkte in Ländern, in denen dies eine starke Inflation in der Landeswährung ist, wechseln jedoch eher zu Krypto-Assets.

„We do not interpret bitcoin's popularity as having a relationship with the public view of the Federal Reserve's conduct of monetary policy."

Janet Yellen
Ehemalige Vorsitzende
Federal Reserve

In dieser Hinsicht sind Privacy Coins der nächste Stellvertreter, den wir in der Krypto-Welt dafür finden können. Es liegt auf der Hand, dass sich jeder, der Krypto zur Steuerflucht verwendet, in erster Linie auf vollständig nicht nachvollziehbare Münzen konzentrieren würde. Mit Blick auf die beiden größten – Monero und Dash – haben sie eine kombinierte Marktkapitalisierung von $1,8 Milliarden. Selbst wenn sie alle ausschließlich für diesen Zweck verwendet werden, ergibt sich dennoch eine Penetration von weniger als 0,3 %.

Kleinere Zielmärkte und Anwendungsfälle

Mikrozahlungen and ohne Bankkonto

Kryptowährungen, die stabil sind und niedrige Transaktionsgebühren haben, eignen sich gut für Mikrozahlungen, da sie die Unannehmlichkeiten und das Sicherheitsrisiko der Übermittlung von Kreditkartendaten für jede kleinere Transaktion beseitigen (Spilka, 2018). In bestimmten Fällen wurden Händler durch die hohen Gebühren, die mit kostengünstigen Transaktionen auf herkömmlichen Systemen verbunden sind, abgeschreckt. Mit niedrigeren Gebühren, höherer Sicherheit und schneller Transaktionsverarbeitung könnten mehr Unternehmen Mikrotransaktionen mithilfe von Krypto durchführen (Spilka, 2018). Dies könnte es neuen Geschäftsmodellen ermöglichen, wie einem Browser, der online neue Websites bezahlt, um Werbung zu blockieren. Laut Business Insider helfen Mikrozahlungen dabei, ein Problem für Anbieter von Online-Inhalten zu lösen, z. B. digitale Musik und App-Käufe.[55]

Weltweit gibt es fast 2 Milliarden Menschen ohne Bankkonto; ein Drittel davon lebt in Afrika südlich der Sahara (Bank4YOU, 2018). In einigen Ländern dieser Region ist die Verbreitung von Smartphones recht hoch („Banking is only the beginning", 2018). Über eine Internetverbindung können sie problemlos auf Krypto-Dienste zugreifen und unter anderem Finanzierungs- und Überweisungsdienste erhalten.

—

54 Niall McCarthy, „The Global Cost of Tax Avoidance", *Statista*, 24. März 2017. Abgerufen von https://www.statista.com/chart/8668/the-global-cost-of-tax-avoidance/

55 Jaime Toplin, „The Micropayments Report: Problems and solutions for low-value payments", *Business Insider*, 12. Januar 2017. Abgerufen von https://www.businessinsider.com/micropayments-report-2017

ICO- und STO-Finanzierung und Krypto-Handel

Ethereum hat zum Aufstieg eines alternativen Fundraising-Modells geführt. Obwohl diese häufig mit Betrug und schlechtem Anlegerschutz verbunden sind, haben sie neue Kapitalflusswege mit einem breiteren Zugang für Anleger geschaffen. Durch die Erstellung digitaler Darstellungen von Vermögenswerten können die Kosten und die Reibung bei der Verwaltung, Übertragung und Ausgabe traditioneller Vermögenswerte verringert werden. Sie haben daher dazu beigetragen, die Liquidität und Transparenz im Lebenszyklus solcher Vermögenswerte zu verbessern (Nagaraj, Hunter & Captain, 2018). Diese praktischen Technologieanwendungen bleiben sehr wahrscheinlich relevant und fördern die Akzeptanz.

„Grayscale's Bitcoin Trust is on a whole new level in 2020.

Average weekly investment (Q1 2019): $3.2 million

Average weekly investment (Q1 2020): $29.9 million

Institutional money has arrived.“

Kevin Rooke
Mai 2020

Die ICO-Finanzierung hat auch die Einführung von Krypto gefördert, trotz der schlechten Presse, die sich aus Betrügereien in diesem Sektor ergibt. Durch die Senkung der Markteintrittsbarriere, um Finanzmittel für Start-ups zu erhalten und in diese zu investieren, können Start-ups nun frühzeitige Startkapitalinvestitionen umgehen oder zusätzlich zu frühen Startkapitalinvestitionen Crowdfunding einsetzen (Davis, 2018). Interessanterweise haben ICOs traditionelles Risikokapital nicht eliminiert, sondern dessen Anpassung und Weiterentwicklung gefördert (Town, 2018). Start-ups sammelten 2017 weltweit $5,5 Milliarden durch die Ausgabe von Token im Rahmen von ICOs. In diesem Jahr ist der Gesamtbetrag bereits auf $14,3 Milliarden gestiegen.[56]

Es muss nicht erwähnt werden, dass Krypto diesen Markt bereits vollständig durchdringt, da Token-Verkäufe, die nur Fiatwährungen akzeptieren, praktisch nicht existieren.

Glücksspiel

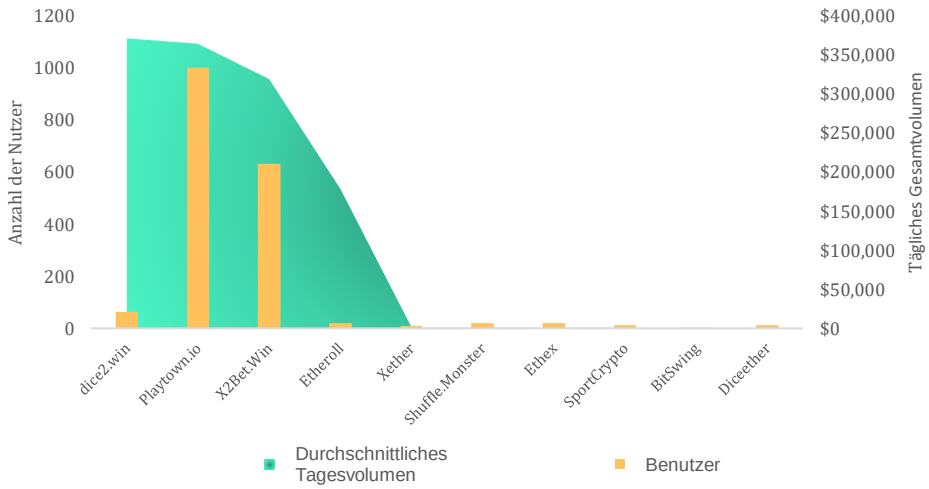
Neben dem Online-E-Commerce ist das Online-Glücksspiel auch ein wichtiger Markt für Kryptowährungen. In wenigen Jahren ist Ethereum zum Zuhause von über 400 dezentralen Glücksspielanwendungen geworden. Das Gameplay reicht von traditionellen Casino-Slots bis hin zu Märkten für den Handel mit Spieloptionen und Prognosemärkten. Es gibt mehrere Online-Casinos, die Zahlungen in Kryptowährungen anbieten.[57] Casinoanbieter.com gibt an, dass die Nachfrage seiner Kunden nach Krypto-Glücksspielen steigt.

—

56 Zahlen laut Coindesk ICO Tracker, abgerufen am 19. September 2018.

57 Frank Sellingen, „Beste Online Bitcoin Casinos im Überblick“, *Casinoanbieter.com*, 2020. Abgerufen von https://casinoanbieter.com/einzahlen-auszahlen/bitcoin/

Abbildung 9: Top 10 der Dezentralen Glücksspielapplikationen Haben ein Tägliches Gesamtvolumen von Über $1 Million



Quelle: DappRadar, CryptoResearch.Report

Obwohl sich die Online-Glücksspielbranche in einem Aufwärtstrend befindet („Banking is only the beginning“, 2018), müssen ihre Kernthemen im Zusammenhang mit Transparenz noch Lösungen finden. Die Verwendung von Krypto hat es jedoch ermöglicht, Vertrauen, Transparenz und Fairness wiederherzustellen. Es bremst das Laster der Rekordmanipulation und schließt das Mantra „The house always wins“ aus.

„I've been wrong in thinking you could really have the developments you've had without inflation taking hold.“

Warren Buffet
Mai 2020

Die globale Glücksspielbranche, die 2020 voraussichtlich auf $143 Milliarden wachsen wird (Wolfson, 2018), ist ein weiterer reifer Markt für die Einführung virtueller Währungen. Virtuelles Geld ist in der Tat nichts Neues für den Sektor, da digitales Gold seit über einem Jahrzehnt für Einkäufe im Spiel verwendet wird. Mit dem Aufkommen von Krypto können Spieler nun jedoch einfacher virtuelle Spielgegenstände miteinander tauschen (Wolfson, 2018). Es hat auch das Problem des Besitzes von Assets im Spiel durch Tokenisierung gelöst. Nach diesem Modell behalten Spieler das Eigentum an ihren erworbenen Vermögenswerten in einer digitalen Geldbörse, bis sie sich entscheiden, diese zu handeln oder zu verkaufen.

Dem folgenden Report zufolge[58] verzeichnet die krypto-spezifische Glücksspielszene in ihren Top-Glücksspiel-Apps ein Volumen von fast $2,5 Milliarden pro Jahr. Im Vergleich zu geschätzten $59 Milliarden für die gesamte Branche[59] ist Krypto mit 4,2 % einer der am stärksten durchdrungenen Märkte.

Akzeptanzrate

Sobald M, V, P und Q geschätzt sind, wird die Penetrationsrate jedes TAM durch jede Kryptowährung berechnet. Dies wird als Akzeptanzrate bezeichnet und basiert

—

58 *The Crypto Betting Industry* [Research Report], The Crypto Community. Abgerufen von https://thecrypto.community/wp-content/uploads/2019/10/The-Crypto-Betting-Industry-TheCrypto.Community-3.pdf

59 „Global Gambling Industry: State of Play in 2018“, *Casino.org*, 2018. Abgerufen von https://www.casino.org/gambling-statistics/

auf einer Annahme hinsichtlich der zukünftigen Verwendung der Währung für jeden Anwendungsfall. Um die Akzeptanz abzuschätzen, gibt es zwei Hauptmethoden: 1) Schätzung des Anstiegs der Anzahl der Personen pro Jahr, die Krypto besitzen und 2) Anpassung einer Kurve an das historische Wachstum der aktiven Wallet-Adressen.

Prognose der Akzeptanz mithilfe historischer Daten zum Wachstum der Zahl an Menschen weltweit, die Krypto nutzen

Laut unserer Recherche gibt es weltweit mehr als 40 Millionen Kryptowährungsbenutzer. Die Anzahl der registrierten Konten an den größten Krypto-Börsen dient als verwendbarer Proxy. Coinbase hat zum Beispiel mehr als 30 Millionen Benutzer.[60] Der Gründer von Binance, Changpeng Zhao (CZ), sagte kürzlich in einem Interview, dass er ungefähr 12 bis 15 Millionen registrierte Benutzer und ungefähr 0,5 bis 2 Millionen aktive Benutzer pro Tag hat. Es gibt mehrere andere ähnlich große Börsen wie Kraken, Bitstamp, Bitfinex, Bittrex, Huobi und OKEx. Unter der Annahme, dass Coinbase die meisten Benutzer hat, müssen mindestens 30 Millionen Kryptowährungsbenutzer vorhanden sein. **Binance und Coinbase haben zusammen etwa 45 Millionen Benutzer**. Dies entspricht durchschnittlich 22,5 Millionen Benutzern pro Börse.
Für die acht größten Börsen würden so 180 Millionen (22,5 x 8) Benutzer herauskommen. Unter der Annahme, dass die meisten Benutzer an mehreren Börsen registriert sind, scheint diese Zahl zu groß zu sein. **Die richtige Antwort liegt wahrscheinlich zwischen 35 und 70 Millionen Benutzern.**

„Good and bad coin cannot circulate together."

Sir Thomas Gresham
Brief an Königin Elizabeth I.
1558

Schaut man sich verschiedene Umfragen an, besitzen etwa 5–8 % der Erwachsenen in den USA Kryptowährungen (Statista Global Consumer Survey, Finder.com). Es gibt Länder wie die Türkei, die mehr Nutzer haben, und Länder wie Japan, die weniger haben. Laut der Umfrage hat Spanien im Vergleich zu anderen westeuropäischen Ländern einen höheren Anteil an Kryptowährungsbenutzern – 10 % der Erwachsenen besitzen dort Kryptowährungen.[61]

Eine endgültige Schätzung der Gesamtzahl der Benutzer könnte mit dem folgenden Experiment erfolgen. Es gibt ungefähr 4,3 Milliarden Menschen, die Zugang zum Internet haben und als mögliche Krypto-Besitzer infrage kommen. Lassen Sie uns 1,5 Milliarden wegen gesetzlicher Beschränkungen abziehen (d. h. China, Pakistan und andere). Die folgende Tabelle zeigt die Anzahl potenzieller Kryptowährungsbenutzer in Abhängigkeit von der Weltbevölkerung.

—

60 Helen Partz, „Coinbase Added 8 Million New Users in the Past Year", *Cointelegraph*, 23. Juli 2019. Abgerufen von https://cointelegraph.com/news/coinbase-added-8-million-new-users-in-the-past-year

61 Mathias Brandt, „So verbreitet sind Kryptowährungen", *Statista*, 25. Mai 2019. Abgerufen von https://de.statista.com/infografik/18102/nutzung-von-kryptowaehrungen/

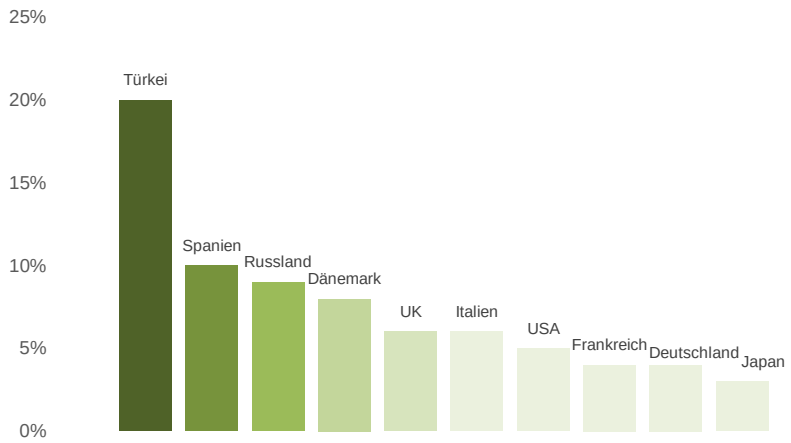
Tabelle 3: Schätzung des Anteils an Krypto-Benutzern an der Weltbevölkerung

Prozentzahl	Weltbevölkerung
1 %	28.000.000
2 %	56.000.000
3 %	84.000.000

Quelle: CryptoResearch.Report

Laut dem CEO von Binance, SZ, korreliert die Anzahl der Konten eines Binance-Landes positiv mit dem Pro-Kopf-BIP (hohes BIP – mehr Konten).

Abbildung 10: Prozentsatz der Kryptowährungsbenutzer pro Land



Quelle: Statista.com[62], CryptoResearch.Report

Prognose der Akzeptanz mit historischen Daten zum Wachstum aktiver Adressen

„You can print more money, but you can't print more hard work. That takes time, effort and energy."

The Bitcoin Rabbi

Ein anderer Ansatz besteht darin, die Anzahl der Wallets zu zählen. Laut BitInfoCharts gibt es derzeit mehr als 43 Millionen Bitcoin-Adressen. Wenn wir dies als Proxy verwenden und die Bitcoin-Dominanz berücksichtigen, die derzeit bei 67 % liegt (CoinMarketCap), können wir davon ausgehen, dass es für Bitcoin und alle Altcoins ungefähr 64 Millionen Adressen (43 / 0,67) geben muss. Einige Benutzer haben möglicherweise sowohl Bitcoin als auch Altcoins, daher gibt es ungefähr 37 bis 52 Millionen Benutzer von Kryptowährungen.

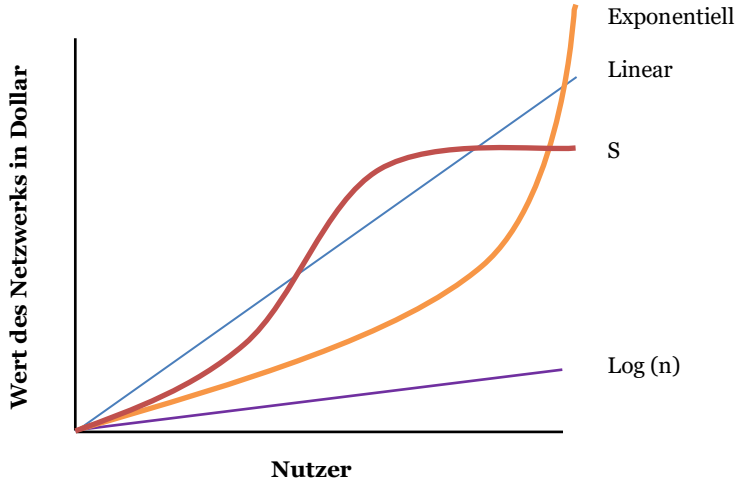
Die meisten Studien verwenden eine S-Kurve, die mit dem Start des Netzwerks beginnt. Es gibt verschiedene mögliche Akzeptanzkurven für die Kryptowährungsakzeptanz, z. B. S-Kurve und linear. Andere Kurvenoptionen sind

—

62 Ibid.

exponentiell und Log. Alle Kurvenannahmen sind in der folgenden Grafik dargestellt.

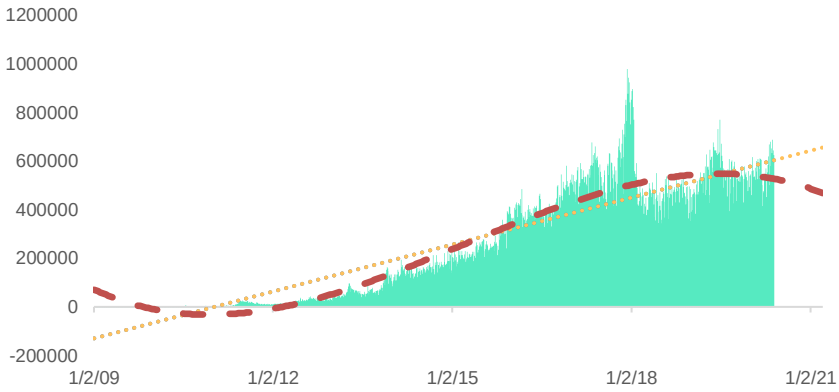
Abbildung 11: Akzeptanzkurve für die Netzwerkutzung



Quelle: CryptoResearch.Report

Nach dem Anpassen der täglichen Daten zur Verwendung von Wallets mit einem Guthaben ungleich Null **scheint die Verwendung von Bitcoin als Tauschmittel einer linearen Kurve oder einer S-Kurve zu folgen und hat derzeit ungefähr 600.000 aktive Benutzer pro Tag.**

Abbildung 12: Bitcoins Akzeptanzkurve Wird als S-Kurve Angenommen



Quelle: Blockchain.info, CryptoResearch.Report

Aus verhaltensökonomischer Sicht wirken sich viele Variablen auf die Akzeptanz aus, z. B. Pfadabhängigkeit, Netzwerkeffekte, überlegene Technologie, Marktpräsenz und Ambiguitätsaversion von Investoren und Benutzern. Die Akzeptanz ist schwer zu messen, da Entwickler und Investoren von Kryptowährungen, sobald eine Metrik standardisiert ist, versuchen, diese Metrik zu spielen oder diese Metrik auszutricksen, um den Markt zu manipulieren.

„The best way to think about Bitcoin is as a non-correlated asset most similar to gold, except that it's much more easily transportable than gold."

Bill Miller
Gründer und Vorsitzender
Miller Value Partners
2018

Szenarien

Um die Robustheit der Analyse der Akzeptanzrate zu verbessern, können mehrere Szenarien für die Akzeptanzrate jeder Kryptowährung für ihre jeweiligen TAMs berechnet werden. **In diesem Bericht werden drei verschiedene Szenarien angenommen:**

- Pessimistisch
  a. Die Kryptowährung wird nur 1 % des gesamten TAM einnehmen.
  b. Die Kryptowährung wird zwei Jahre brauchen, um 10 % der Akzeptanzrate von 1 % zu erreichen.
  c. Die Anzahl der Jahre, die eine Kryptowährung benötigt, um 90 % der Akzeptanzrate von 1 % zur erreichen, ist sieben.
- Moderat
  a. Die Kryptowährung wird nur 10 % des gesamten TAM einnehmen.
  b. Die Kryptowährung wird zwei Jahre brauchen, um 10 % der Akzeptanzrate von 1 % zu erreichen.
  c. Die Anzahl der Jahre, die eine Kryptowährung benötigt, um 90 % der Akzeptanzrate von 1 % zur erreichen, ist fünf.
- Optimistisch
  a. Die Kryptowährung wird nur 20 % des gesamten TAM einnehmen.
  b. Die Kryptowährung wird zwei Jahre brauchen, um 20 % der Akzeptanzrate von 1 % zu erreichen.
  c. Die Anzahl der Jahre, die eine Kryptowährung benötigt, um 90 % der Akzeptanzrate von 1 % zur erreichen, ist fünf.

Diskontsatz

Ein Dollar ist heute mehr wert als ein Dollar in einem Jahr. Aktienbewertungsmodelle wie das Discounted-Cashflow-Modell können basierend auf dem Risiko der Branche und des Unternehmens Abzinsungssätze von 10–50 % pro Jahr verwenden. Nehmen Sie den zukünftigen aktuellen Wert und reduzieren Sie ihn auf die Gegenwart. Wenn man den Wert von $7,45 nimmt und ihn 10 Jahre mit einer Rate von 40 % zurückzählt, ergibt sich ein rationaler Marktwert von $0,26. Die Berechnung beträgt $7,45 / ($1,40^{10}$). Ein alternativer Ansatz besteht darin, jeden Periodennutzungswert abzuzinsen und den gewichteten Durchschnitt zu verwenden, indem größere Perioden auf Perioden angewendet werden, die näher liegen. Der Satis-Bericht argumentiert, dass für die TAM-Analyse keine Diskontierung erforderlich ist[63]; die meisten Berichte enthalten jedoch einen Abzinsungssatz. Chris Burniske verwendet Raten zwischen 30 % und 40 %.[64] Der

—

63 Sherwin Dowlat und Michael Hodapp, „Cryptoasset Market Coverage Initiation: Valuation August 30, 2018", *SatisGroup*, 2018. Abgerufen von https://research.bloomberg.com/pub/res/d37g1Q1hEhBkiRCu_ruMdMsbc0A

64 Burniske and White, 2017.

2015 Wedbush Securities Report verwendet einen Abzinsungssatz von 40 %.[65] In diesem Bericht wenden wir 30 % an. Es sind jedoch zusätzliche Untersuchungen zum Immobilienabzinsungssatz jeder Münze erforderlich, um unterschiedliche Risikoprofile widerzuspiegeln.

Der Gewinner bekommt alles

Da diese Analyse fünf Münzen statt nur einer untersucht, ist **eine weitere Annahme vonnöten.**

Viele der Top-5-Münzen konkurrieren miteinander, um globale Hauptbücher für die Speicherung und den Handel digitaler Assets zu werden. Daher ist eine Annahme zu treffen, **ob es einen Gewinner gibt**, der alle übernimmt, **oder ein Oligopol von Krypto-Assets für jeden Hauptanwendungsfall** oder nicht. Mehrere Studien gehen davon aus, dass jedes Protokoll eine isolierte Wirtschaft ist, um die Berechnungen zu vereinfachen. Der Kryptowährungsmarkt ist jedoch einer der wettbewerbsfähigsten Märkte der Welt. Er weist weniger regulatorische Markteintrittsbarrieren auf, und die Kosten für den Wechsel zwischen Kryptowährungen sind niedrig. Diese Annahme ist relevant für die Akzeptanzrate, die Szenariowahrscheinlichkeit und den Abzinsungssatz.

„It's the single best hedge against traditional financial infrastructure. Whether you support the fiscal and monetary policy or not, it doesn't matter. This is the schmuck insurance you have under your mattress."

Chamath Palihapitiya
Gründer und CEO
Social Capital
2019

Man könnte argumentieren, dass die Gewinnerprotokolle dieser digitalen Ressourcen zu globalen Standards werden und globale Standards in der Regel Szenarien sind, in denen „der Gewinner die meisten nimmt". **In diesem Bericht werden daher folgende Annahmen getroffen:**

- Bitcoin wird Ethereum, Bitcoin Cash, und Litecoin in der Währungsmünzengruppe schlagen.
  - Dies spiegelt sich im „Abzinsungssatz" wider. Für Bitcoin wird ein Abzinsungssatz von 30 % **angenommen**, während für Bitcoin Cash und Litecoin ein Abzinsungssatz von 50 % **angenommen** wird.
- Ethereum wird Stellar in der Utility-Coin-Gruppe schlagen.
  - Dies spiegelt sich im „Abzinsungssatz" wider. Für Ethereum wird ein Abzinsungssatz von 30 % **angenommen**. Für Stellar wird ein Abzinsungssatz von 50 % **angenommen**.

Diese Annahmen basieren auf den aktuellen technologischen und regulatorischen Stärken von Bitcoin und Ethereum. Die für Bitcoin bestimmte Hash-Rate ist um Größenordnungen höher als bei jeder anderen Kryptowährung. Schließlich hat der dezentrale Charakter von Bitcoin die SEC-Beamten dazu veranlasst, Bitcoin inoffiziell als keine Sicherheit zu betrachten. Dies bietet einen gewissen regulatorischen Schutz für Bitcoin, der neue Blockchain-Starts behindern kann. Bitcoin Cash und Litecoin haben jedoch auch Vorteile. Beide Münzen bieten im Vergleich zu Bitcoin schnellere Bestätigungszeiten und niedrigere Transaktionsgebühren. Sie sind mit großen Anlegernetzwerken ausreichend

—

65 Gil Luria and Aaron Turner, *Bitcoin Investment Trust (GBTC)*, Wedbush Securities, 9. Juli 2015. Abgerufen von https://www.scribd.com/doc/271095696/GBTC-Initiation-2015-07-09?campaign=SkimbitLtd&ad_group=100652X1574425Xb33e774d2adb3cb7ff048b89c1f5ae1e&keyword=660149026&source=hp_affiliate&medium=affiliate

dezentralisiert, und bei Bitcoin Cash arbeiten viele Entwickler an Protokoll-Upgrades. Anstelle eines Gewinners, der in den nächsten zehn Jahren alles nimmt, dürfte ein Oligopol der Zahlungsmünzen bestehen bleiben. Darüber hinaus verwenden mehrere Anleger naive 1 / n-Strategien, um in Kryptowährungen zu investieren, und investieren daher gleichermaßen in Münzen mit der höchsten Währung, um das Risiko zu verringern und den Markt zu erobern.

Bewertungsergebnis

Unter Berücksichtigung aller Variablen und TAMs haben wir für jede der untersuchten Kryptowährungen eine Schätzung des Utility-Preises erstellt. Es bringt nichts, dass jede dieser Schätzungen auf einer nicht-abgezinsten Basis und mit entweder pessimistischen oder moderaten Marktdurchdringungsannahmen erfolgt.

Tabelle 4: Quantitätsgleichung-Prognose für den Krypto-Asset-Preis

Nicht-diskontierte Utility-Preis-Prognosen					
	Aktuell	**2020**	**2025**	**2030**	**2033**
Bitcoin	$9.263	$19.044	$341.000	$397.727	$395.270
Ethereum	$208	$331	$3.549	$3.644	$3.441
Litecoin	$44	$83	$1.216	$2.252	$2.299
Bitcoin Cash	$235	$414	$6.690	$13.016	$12.941
Stellar	$0,07	$0,09	$2,40	$7,81	$8,26

Quelle: CryptoResearch.Report

„We should be happier to have a job than to have our savings protected.“

Christine Lagarde
Präsidentin der Europäischen Zentralbank und ehemalige Leiterin des IWF
2019

Es ist erwähnenswert, dass zum Zeitpunkt der Erstellung dieses Berichts die gesamte Marktkapitalisierung für Krypto (alle Währungen, nicht nur die oben aufgeführten 5) bei $256 Milliarden liegt. In der Zwischenzeit liegt der TAM aller oben diskutierten potenziellen Märkte bei über $188 Billionen, wodurch die derzeitige Krypto-Penetration in diesen Märkten 0,136 % beträgt.

Wie aus den obigen Diagrammen hervorgeht, glauben wir, dass Bitcoin noch am Anfang seiner Akzeptanzkurve steht. Der Preis von $7.200 Ende 2019 deutet darauf hin, dass Bitcoin weniger als 0,44 % seiner gesamten TAMs durchdrungen hat. Wenn diese Durchdringung 10 % erreicht, sollte der nicht abgezinste Utility-Preis fast $400.000 erreichen.

Kritik an der Quantitätsgleichung

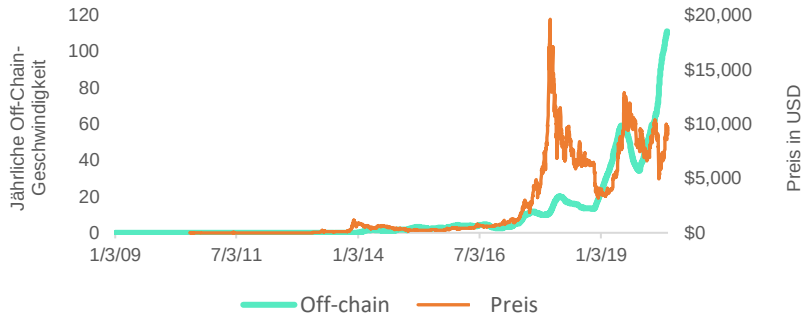
Die im Modell der Wechselgleichung vorgestellte Geschwindigkeitstheorie, die üblicherweise auf Krypto-Assets angewendet wird, **würde das Geschäftsmodell von Utility Coins und Zahlungsmünzen in Frage stellen, die keine Anreize zum Horten mittels Staking bieten, und es wird erwartet, dass sie eine hohe Geschwindigkeit haben, da die Leute ihre Münzen häufig ausgeben.** Zur Unterstützung dieser Theorie und der Analyse von Buterin und

„The dollars that you work hard for are always buying less and less, yet the government tells you there's ‚not enough inflation'. The Fed is a government-created monopoly that counterfeits dollars by the trillions, and you're supposed to believe that this is capitalism."

Ron Paul
Ehemaliher US-Kongressabgeordneter und Präsidentschaftskandidat

Samani zeigte Coin Metrics' State of the Network #37, wie die On-Chain-Geschwindigkeit von Bitcoin stetig gesunken ist und der Preis gestiegen ist. **Wir haben jedoch auch die Off-Chain-Transaktionsgeschwindigkeit von Bitcoin berechnet und das entgegengesetzte Muster gefunden.** Wir haben festgestellt, dass der Preis von Bitcoin und die Handelsaktivität von Bitcoin in den letzten Jahren gleichzeitig gestiegen sind. Die On-Chain-Geschwindigkeit ist die Geschwindigkeit, die ausschließlich durch Transaktionen in der Blockchain erzeugt wird, während die Off-Chain-Geschwindigkeit die Geschwindigkeit ist, die durch Handelsaktivitäten an Kryptowährungsbörsen erzeugt wird.

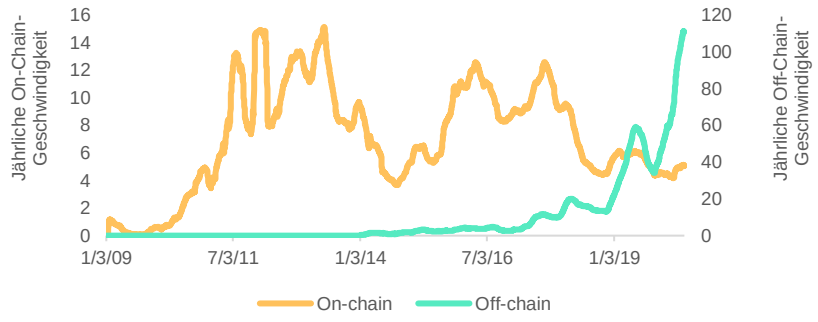
Abbildung 13: Bitcoins Off-Chain-Geschwindigkeit Korrekliert Positiv mit dem Bitcoin-Preis



Quelle: Coinmetrics.io, CryptoResearch.Report

Wir wollten diese Ergebnisse mit anderen Münzen überprüfen, also berechneten wir die On-Chain- als auch die Off-Chain-Geschwindigkeit für Ethereum, Bitcoin Cash, Litecoin und Stellar, um festzustellen, ob Münzen häufiger On-Chain gehandelt wurden (Austausch und Off-Exchange) oder Off-Chain (Intra-Exchange).

Abbildung 14: Gleitender 90-Tages-Durchschnitt Bitcoin On-Chain- und Off-Chain-Geschwindigkeit

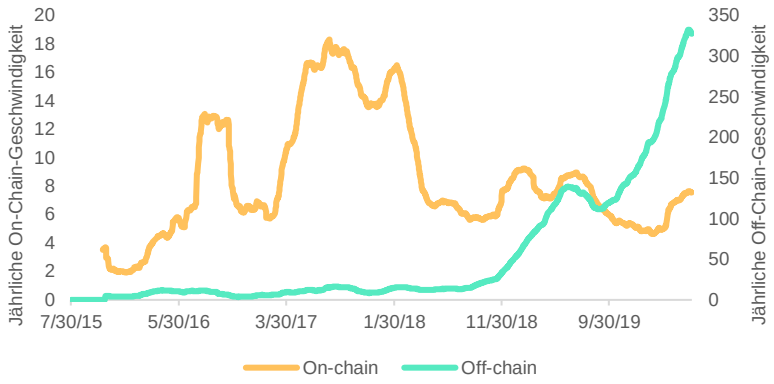


Quelle: Coinmetrics.io, CryptoResearch.Report

Wir haben festgestellt, dass bei fast allen Münzen die On-Chain-Geschwindigkeit abnimmt, während die Off-Chain-Geschwindigkeit zunimmt. Wir interpretieren

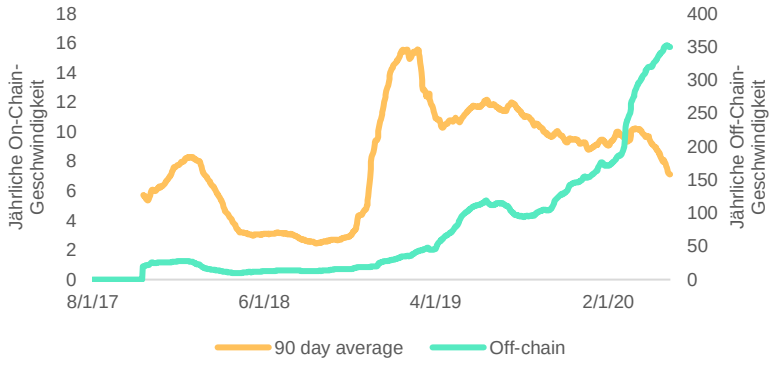
dies so, dass das Wachstum der Anzahl spekulativer Transaktionen an Börsen schneller ist als das Wachstum von Versorgungstransaktionen zum Kauf von Waren und Dienstleistungen.

Abbildung 15: Gleitender 90-Tages-Durschnitt Ethereum On-Chain- und Off-Chain-Geschwindigkeit



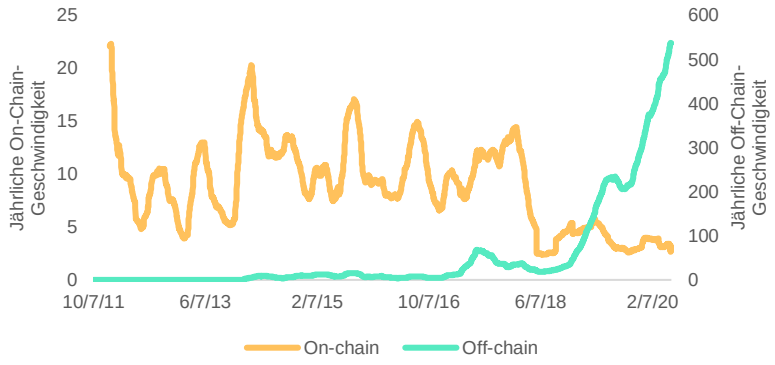
Quelle: Coinmetrics.io, CryptoResearch.Report

Abbildung 16: Gleitender 90-Tages-Durschnitt Bitcoin Cash On-Chain- und Off-Chain-Geschwindigkeit



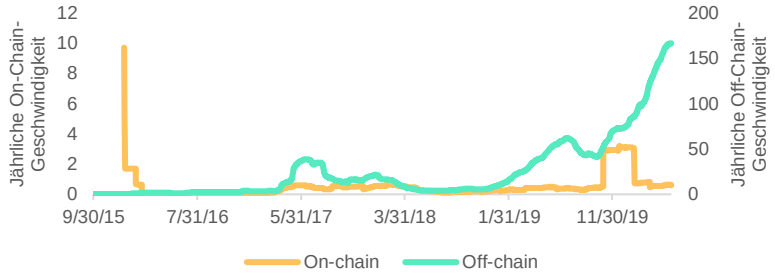
Quelle: Coinmetrics.io, CryptoResearch.Report

Abbildung 17: Gleitender 90-Tages-Durschnitt Litecoin On-Chain- und Off-Chain-Geschwindigkeit



Quelle: Coinmetrics.io, CryptoResearch.Report

Abbildung 18: Gleitender 90-Tages-Durschnitt Stellar On-Chain- und Off-Chain-Geschwindigkeit



Quelle: Coinmetrics.io, CryptoResearch.Report

„The key value proposition of blockchain is minimizing the cost of trust down to almost zero. The cost of trust is roughly 35 % of global GDP or $28 trillion dollars. Therefore, the target addressable market for blockchain is $28 trillion dollars.“

Lasse Clausen
Gründer 1kx
Mai 2020

Es ist interessant, dass sich bei fast allen Kryptowährungen ähnliche Geschwindigkeitstrends beobachten lassen. Höhere Geschwindigkeiten bevor die Kryptowährung reift und später stabilere und niedrigere Geschwindigkeiten. Stellar scheint eine Ausnahme von dieser Regel zu sein (hauptsächlich im Hinblick auf den enormen Geschwindigkeitssprung Ende 2019), aber wie wir wissen, ist Stellars Coinbase stark zentralisiert und es ist wahrscheinlich, dass dies eine Grundtransaktion ist, die die Zahlen verzerrt.

Erwähnenswert ist auch der enorme Anstieg der Off-Chain-Geschwindigkeiten unter allen Kryptowährungen in den Jahren 2019-2020, der mit dem Rückgang der On-Chain-Geschwindigkeit zusammenfällt. Dies deutet darauf hin, dass Händler, die ausschließlich an Börsen tätig sind und mit hohen Volumina handeln, die dominierende Kraft auf dem Markt für Krypto-Assets werden, anstatt langfristige Holder.

Die Ergebnisse, die wir gefunden haben, widersprechen der Theorie von Buterin und Samani, da wir festgestellt haben, dass die Geschwindigkeit steigt und der Preis steigt, obwohl ihr Modell besagt, dass der Preis fallen sollte. Scott Locklins Kritik an ihrer Arbeit könnte die Antwort enthalten. Wie Locklin

betont, funktioniert die direkte Anwendung der MV = PT-Austauschgleichung von Fisher auf Krypto-Assets aus zwei Hauptgründen nicht:

„Die Umkehrung der [durchschnittlichen] Token-Geschwindigkeit ist keine durchschnittliche Haltezeit. Nehmen wir zum Beispiel eine Geldmenge von 10 Token in einer Volkswirtschaft mit einer Geschwindigkeit von 10 Mal pro Tag an. Wenn 9 der Token einmal alle 1000 Tage und einer der Token 99,991 Mal am Tag gehandelt werden, ergibt dies 10 Mal pro Tag die mittlere Token-Geschwindigkeit. Die durchschnittliche Haltezeit für eine Münze in diesem Ökosystem beträgt jedoch 900,001 Tage, nicht 1/10 Tage pro Transaktion."

„Auch wenn Fishers Quantitätsgleichung ein Gleichgewichtsmodell ist [das vermutlich als ‚stationärer Zustand' bezeichnet werden könnte], hängt sie nicht von der Anzahl der Benutzer ab."

Locklin nimmt einige Änderung an der Gleichung vor und argumentiert, dass die Benutzerakzeptanz für den Preis einer Münze wirklich wichtig ist. Je mehr Leute ins Netzwerk kommen und die Münze verlangen, desto höher ist der Preis. Locklins Kritiker ist sehr direkt. Wenn mehr Menschen Bitcoin und Ethereum zum Kauf von Kaffee oder zum Spekulieren verlangen, ist das Ergebnis ähnlich. In beiden Fällen tauschen die Menschen wirtschaftliche Ressourcen gegen Kryptowährungen und bieten ihre Preise an. Zur Verteidigung von Buterin und Samani werden Spekulationen über finanzielle Vermögenswerte normalerweise nicht in die BIP-Kennzahlen einbezogen. Das Devisenvolumen ist beispielsweise nicht im BIP enthalten, und daher ist eine Analyse der Geschwindigkeit der Spekulation mit Krypto-Assets möglicherweise nicht angemessen.

Letztes Wort. Vitaliks wirtschaftliche Konzepte von Geschwindigkeit und Geschwindigkeitssenken, die das Horten fördern, sind wichtig. Die Analyse ist jedoch statisch und berücksichtigt nicht die Akzeptanz neuer Benutzer und die wachsende Nachfrage. Wenn Kryptowährungen für langfristige Hortungszwecke oder für kurzfristige Ausgaben für Spekulationen oder Kaffee eingesetzt werden, steigt der Preis für Krypto-Assets. **On-Chain mit hoher Geschwindigkeit und Off-Chain mit niedriger Geschwindigkeit deuten darauf hin, dass Krypto-Assets zunehmend für Spekulationen und nicht als Wertspeicher verwendet werden.**

Es ist immer wieder davon zu lesen: Bitcoin-Wallets sind das Ziel von Hacker-Angriffen, Passwörter werden vergessen und Festplatten gehen kaputt.

Bitcoin langfristig zu sichern ist kompliziert.
Die Card Wallet macht es einfach.

Alles, was Sie tun müssen, ist die Karte an einem sicheren Ort aufzubewahren – wir kümmern uns um den Rest. Die Card Wallet ist eine Co-Produktion von **Coinfinity** und der **Österreichischen Staatsdruckerei** und bietet Ihnen

- die Möglichkeit, Bitcoin physisch zu verwahren
- Schutz vor Hacker-Angriffen durch offline-Lagerung
- einfache Handhabung, auch ohne technisches Vorwissen
- problemloses Schenken, Übertragen oder Vererben von Bitcoin

Kombinieren Sie die Card Wallet mit dem Bitcoin-Sparplan, dem regelmäßigen Bitcoinkauf per Dauerauftrag ohne jegliche Bindung.

Mehr unter www.cardwallet.com

coinfinity

BRINGING BITCOIN TO THE PEOPLE

Coinfinity steht seit Jahren für Vertrauenswürdigkeit und individuelle Beratung beim Kauf und Verkauf von Bitcoin und anderen Kryptowährungen.

Eine umfassende Kundenbetreuung ist uns wichtig. Kontaktieren Sie uns, wir beraten Sie gerne!

+43 316 711 744 | office@coinfinity.co

Für Käufe über 100.000 € kontaktieren Sie bitte direkt unsere Compliance-Abteilung unter compliance@coinfinity.co

www.coinfinity.co

Tether oder Nicht-Tether

„Im April 2019 gab der General Counsel von Bitfinex, Stuart Hoegner, in Gerichtsdokumenten zu, dass Tether nur zu 74 % durch ‚Zahlungsmittel und Zahlungsmitteläquivalente' gedeckt war, was der Theorie Glauben schenkt, dass Tethers zunehmend aus dem Nichts geprägt werden. Bitfinex wird von der New Yorker Generalstaatsanwaltschaft untersucht. Er machte diese Behauptung geltend, als Tether im Wert von nur $2,8 Milliarden im Umlauf war. Jetzt gibt es das Dreifache dieses Betrags."

Amy Castor

Key Takeaways

- **Ursprünglich wurde angenommen, dass die USD-gebundene Tether-Stablecoin eine Bitcoin-Rampe ist. Dies ist heute jedoch nur ein kleiner Anwendungsfall. Stattdessen wird Tether als Abwicklungsinstrument für Handelsstrategien, Arbitraging zwischen Kryptowährungsbörsen und zur Umgehung von Kapitalkontrollen verwendet. Dieser Trend kann als Dollarisierung öffentlicher Blockchains bezeichnet werden.**

- **Der Trend der „Hyper-Krypto-Dollarisierung" dürfte die Nachfrage nach Tether und anderen Fiat-Pegged-Stablecoins erhöhen. Seit Januar wurden $4,7 Milliarden an Tether geschaffen. Derzeit sind fast $9 Milliarden im Umlauf.**

- **Tether ist nicht vollständig gesichert, und es gibt Hinweise darauf, dass nicht gesicherte Tether künstliche Preisbewegungen in Bitcoin unterstützen. Bitfinex-Kredite an Miners können auch den Preis von Bitcoin künstlich stützen.**

Pascal Hügli

Pascal Hügli ist Chief Research Officer bei Schlossberg&Co, einem Schweizer Vermögensverwalter, der sich darauf konzentriert, das Vermögen seiner Kunden vor einem beispiellosen und zunehmenden Geldsozialismus auf der ganzen Welt zu schützen. Schlossberg&Co hat Bitcoin seit 2013 in seine Portfolioallokation integriert. Sie beobachten den Bitcoin-Markt seit Jahren genau.

Im September 2018 erreichte US-Tether (USDT) einen vorübergehenden Höchststand bei der Marktkapitalisierung von etwas über 2,8 Milliarden US-Dollar. Bis Mitte November korrigierte die Marktkapitalisierung dann auf unter zwei Milliarden US-Dollar – danach folgte auch der Bitcoin-Preis und fiel bis kurz vor Jahresende auf beinahe dreitausend Dollar pro Bitcoin.

„New York does not like $USDT as it competes with their upcoming $22 trillion IEO to pay off US debt.“

Simon Dixon

Heute ist der Bitcoin-Preis höher und auch die Marktkapitalisierung von Tether ist seither kontinuierlich auf über acht Milliarden US-Dollar gestiegen. Nicht nur ist die ausstehende Menge an Tether kaum jemals auch nur vorübergehend gesunken, die Emissionsrate neuer Tether zeigt zudem seit Beginn des Jahres plötzliche, sprunghafte Anstiege; insgesamt drei an der Zahl, von denen jeder grösser ist als der vorhergehende.

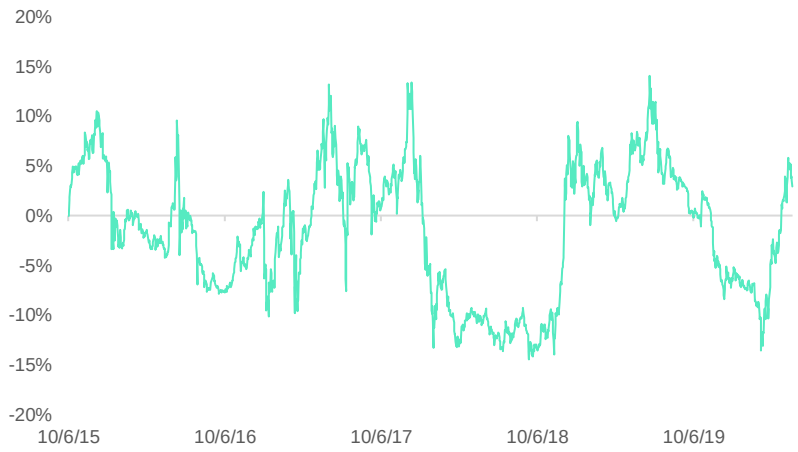
Gewissermassen als einer der grossen Blackboxen der Kryptowelt ranken sich um Tether viele Geheimnisse und Spekulationen – abrupte Wachstumsschübe in der Marktkapitalisierung heizen letztere noch an. Abseits der Gerüchte und Mutmassungen wird USDT nach wie vor als sogenannter “On-ramp” angesehen. Gemeint ist, dass Tether Investoren dazu dienen würde, einfach und schnell in Bitcoin zu investieren.

„Tether has a real-world use case: Chinese importers of cheap goods in Russia use it to send millions home daily.“

Anna Baydakova

In der Tat mag Tether für einige Investoren das Eingangstor zur Bitcoin-Welt darstellen. Wäre Tether allerdings ausschliesslich eine “On/Off-Ramp”, müsste die Marktkapitalisierung Tethers in der Theorie zwischenzeitlich auch wieder fallen, da USDT in Abständen durch das Tether-Treasury vernichtet, bzw. “geburnt” **werden** müssten – dann nämlich wenn in Fiat gewechselt würde. Die Marktkapitalisierung von Tether steigt aber in den vergangenen 18 Monaten konstant an, ohne zwischendurch zu fallen. Dieser Umstand deutet darauf hin, dass Tether nicht in erster Linie als On- oder Off-Ramp fungiert.

Abbildung 19: Negative Korrelation Zwischen Änderung des Tether-Angebots und Bitcoin-Preis



Quelle: Coinmetrics.io, CryptoResearch.Report

Dagegen spricht nämlich, dass die Nachfrage nach Bitcoin sehr volatil ist. Während der letzten zwei Jahre hat es immer wieder Zeiten geben, in denen Bitcoin kaum Aufmerksamkeit geniesst und der Preis gefallen ist, während die Marktkapitalisierung Tethers gleich geblieben oder gar gestiegen ist. Würde USDT vor allem als On-Ramp gebraucht, müsste seine positive Korrelation zu Bitcoin viel stärker sein. Das ist nicht der Fall, zumal es sogar Hinweise gibt, dass die Korrelation negativ ist.

Alternative Erklärung gesucht

Gemeinhin wird von einigen Marktbeobachtern vermutet, dass USDT geschaffen werden, ohne diese zu besichern – frei nach dem Prinzip der Teilreservehaltung. US-Tether würden dabei von Tether Limited und der Mutterfirma BitFinex gezielt kreiert, um den Bitcoin-Preis hochzutreiben.

Auf diese Weise würde versucht, Aufregung unter den Retail-Investoren zu generieren, die dann bestenfalls in eine Hysterie des "Fear of Missing out" (FOMO) übergeht und der Kryptowelt einen neuen Bullenrun bescheren soll. So und nicht anders erklären sich einige Analysten den Umstand, dass die Tether-Marktkapitalisierung am 14. Mai ein paar Tage nach dem Halvening schlagartig von etwas über sechs Milliarden auf beinahe neun Milliarden US-Dollar angestiegen ist.

„The coming crash of Tether/USDT will cause the crash of Bitcoin as the former was used to manipulate the latter."

Nouriel Roubini

Was sich für einige nach einer Verschwörungstheorie angehört, halten andere für einen Fakt: Denn letztlich hätten die beiden Firmen BitFinex und Tether Limited starke Anreize, derartige Spiele zu betreiben. Wie der Justizminister von New York festgestellt haben soll, seien ausstehende Tether nur zu ungefähr 70 Prozent mit Cash und anderen Barwerten besichert. Dieses Loch in der Besicherung, so die Skeptiker von Tether, könnte natürlich Schritt für Schritt gestopft werden, wenn sich Bitcoin durch Privatanleger gestützt auf einem höheren Niveau stabilisiert und die Besicherung, die BitFinex zum Teil auch in Bitcoin hält, damit mehr Wert hat. Mehr US-Dollar könnten mit dieser Besicherung gekauft werden, was den Reservesatz verbessern würde.

Tether als Retter in der Not

Eine andere Hypothese zur Erklärung des abrupten Anstiegs der Tether Marktkapitalisierung vom 14. Mai geht auch dahin, dass BitFinex mit USDT-Krediten gewissen Minern das Überleben sichern will. Bitcoin-Miner betreiben heute hochspezialisierte ASIC-Prozessoren, wovon gegenwärtig vor allem zwei verschiedene in Verwendung sind: der Antminer S9 sowie der Antminer S17.

Der grosse Unterschiede dieser beiden Mining-Hardware liegt hauptsächlich in der Effizienz. Obschon der S17 gegenüber dem S9 einen ungefähr 50 Prozent höheren Stromverbrauch hat, erreicht ein Miner mit ersterem eine 300 Prozent höhere Hashrate. Diese höhere Effizienz hat zur Folge, dass Antminer S17 heute mit etwas

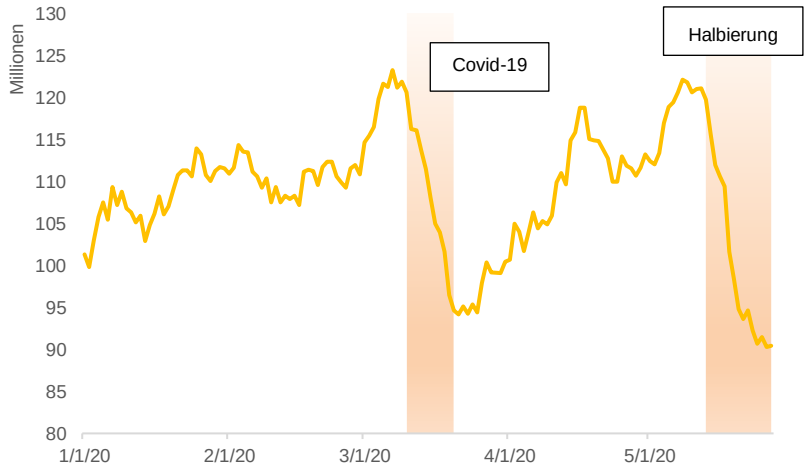
über 61 Prozent einen weitaus höheren Anteil am Bitcoin-Mining ausmachen. Die Verwendung des S9-Typen liegt indes bei etwas mehr als 38 Prozent.

And it is precisely these miners, so the argument goes, that are dependent on support, as they have become unprofitable after the halving. However, in order to not have to empty out their Bitcoin treasuries and generate downward pressure on the Bitcoin price, these miners could be buying time with USDT loans - time to renew their hardware equipment that had become unprofitable.

Speculations and theories of this kind always sound tempting. It is also difficult to refute them completely. But it is just as difficult to provide definitive evidence. In the end, it is argument against argument.

What stands against the BitFinex miner thesis is the fact that miners today are farsighted, long-term invested players. As rational players in a very competitive, highly innovative and little-regulated field, it can be assumed that precisely those miners with older Antminer S9 have taken precautions. They could have moved to a location with much lower electricity costs so that their Antminer S9s are still profitable even after the block reward was halved.

Abbildung 20: Miner Hash Rate Ist Gefallen



Quelle: Blockchain.com, CryptoResearch.Report

Wiederum gibt es in der realen Welt Friktion und Ungewissheit. Unvorhersehbares könnte beispielsweise zur Folge haben, dass man sich bei Langzeitverträgen mit Stromanbietern verschätzt hat und deswegen nicht über Nacht die Mining-Farmen dislozieren kann. Es ist und bleibt eine Tatsache: Wir können nur spekulieren.

Nachfrage nach Tether, nicht Bitcoin

Der kontinuierliche Anstieg der Tether-Marktkapitalisierung muss aber nicht zwingend die Folge vermehrter USDT-Nachfrage als Bitcoin-On-Ramp sein. Wie sich immer stärker abzeichnet: Es scheint wahrscheinlicher, dass Tether an und für sich nachgefragt werden. Als eine Art Settlement-Vehikel für Arbitrageure zwischen Kryptohandelsbörsen findet der Stablecoin rege Verwendung.

Über die vergangenen Jahre haben sich die Handelsbörsen für Kryptoassets professionalisiert, womit auch das Geschäft der Arbitrage professioneller geworden ist. So wird mit immer grösseren Summen arbitragiert – eine stabile Settlement-Währung wie der USDT scheint dafür prädestiniert zu sein.

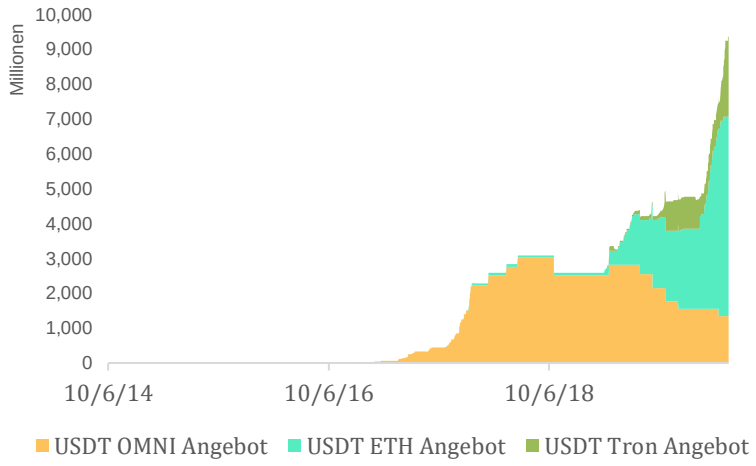
„Allow me to present the only piece of news in crypto that's worth your while. It's about what's really backing Tether's stablecoin. It's not dollars. It's not Bitcoin either - not entirely, at least. It's loans to miners, backed by Bitcoin.“

Trolly McTrollface

Doch geht es nicht nur um Arbitrage. Eine stabile Kryptowährung hilft Kryptohandelsbörsen auch, ihre Aktivitäten effizienter durchzuführen. Die Tetherisierung der Kryptobörsen-Industrie ist in vollem Gange. Bitcoin wurde durch Tether als Basiswährung verdrängt. Mehrere Börsen wie Binance, OKEx oder Huobi haben sogar auf Tether lautende Futures-Produkte eingeführt.

Als Konsequenz hat die Menge von auf Börsen gehaltenen Tether erheblich zugenommen. Nicht nur Börsen machen sich allerdings die stabilen Eigenschaften von Tether zunutze, USDT wird auch von Trader immer intensiver zu Absicherungszwecken verwendet. Fällt der Bitcoin-Preis, wechseln diese Akteure in den Stablecoin, damit sie Verluste minimieren und sich später zu einem tieferen Preis wieder einkaufen können.

Abbildung 21: In den Letzten Zwei Jahren ist das Tether-Angebot an den Börsen von Millionen auf Milliarden Angewachsen



Quelle: Coinmetrics.io, CryptoResearch.Report

Doch nicht nur der Arbitrage-Handel zwischen Kryptobörsen, auch der “Handel” zwischen einzelnen Ländern vereinfacht ein Stablecoin wie Tether. So ist allgemein bekannt, dass einer der ersten grösseren Anwendungsfälle von Bitcoin das Umgehen von Kapitalverkehrskontrollen gewesen ist. Der erste grosse Preisanstieg

Ende 2013 soll vor allem auf Chinesen zurückzuführen sein, die ihre Ersparnisse ausser Land bringen wollten.

Die Volatilität Bitcoins war Kapitalflüchtlingen jedoch seit jeher ein Dorn im Auge. Und tatsächlich scheint wenig gewonnen zu sein, wenn man sein Kapital ausser Land bringt, die Bitcoin-Volatilität in der Zwischenzeit allerdings mehr als die Hälfte des "geretteten" Kapitals aufgefressen hat.

Mit der Lancierung von Tether haben sich für die Kapitalflucht plötzlich neue Möglichkeiten aufgetan. Nachvollziehbar also, dass USDT in diesem Fall als Killerapplikation entdeckt worden ist. Insbesondere bei chinesischen Händlern und Geschäftsleuten, die nach Russland exportieren, ist Tether als grenzübergreifender Kryptodollar im Einsatz.

Alle wollen US-Dollar

„Crypto is an insanely powerful tailwind for the US Dollar, many people haven't understood this yet. Far from being crushed by bitcoin or cryptocurrency, the dollar will be its primary beneficiary (assuming the MMTers don't obliterate it first)."

Nic Carter

Dass chinesische Geschäftsleute mit USDT einen auf Dollar lautenden Stablecoin halten, hat seinen Grund. Der US-Dollar ist heute die globale Leit-, Reserve- und Handelswährung. Alle namhaften Rohstoffe werden über den US-Dollar abgerechnet, weshalb er heute das 4,7-Fache an weltweiten Importen und das 3,1-Fache an globalen Exporten ausmacht. Für Nicht-US-Unternehmen ergibt es deshalb häufiger mehr Sinn, gleich in US-Dollar zu fakturieren.

Doch werden nicht nur Rechnungen in US-Dollar ausgestellt und abgerechnet. Unternehmen auf der ganzen Welt haben gegenwärtig in US-Dollar denominierte Schulden von fast 60 Billionen. Das schafft eine anhaltende Nachfrage nach US-Dollar zur Bedienung der Schulden durch Schwellen- aber auch Entwicklungsländer, die nicht spurlos an deren Währungen vorbeigehen wird. Letztere dürften gegenüber dem Dollar eher abwerten, was vermehrt verstärkte Kapitalverkehrskontrollen zur Folge haben wird.

Jüngstes Beispiel liefert Libanon. Lokale Banken stehen dort derzeit mitten in einem Kampf gegen die Kapitalflucht, weshalb beispielsweise die Restriktionen für Fremdwährungsbezüge, allen voran in US-Dollar, verschärft worden sind. Verschärfte Kapitalverkehrskontrollen dürften aber nicht nur in unterentwickelten Ländern zunehmen, auch der Euroraum könnte diesbezüglich auf absehbare Zeit restriktiver werden.

Anders als mit dem japanischen Yen und dem Schweizer Franken, die als Währungen noch immer den Charakter des sicheren Hafen geniessen, korreliert die Nachfrage nach Euro hauptsächlich mit der Nachfrage nach Exporten aus der Eurozone. Je eher die im Zuge der ultra-expansiven Geldpolitik der Europäischen Zentralbank geschaffene Euro-Liquidität die internationale Nachfrage nach Euro relativ zum Dollar übersteigt, desto schneller verliert ersterer an Wert.

Verschärfte Kapitalverkehrskontrollen zur Stützung des Euros würden vor allem europäische Banken treffen. Noch immer führen diese grosse US-Dollar-Positionen in ihren Bilanzen. Ohne eine über ausreichende US-Dollar-Einlagen zu

verfügen, brauchen sie ständig offene Wege, um an US-Dollar zukommen. Verschärfte Kapitalverkehrskontrollen wären ein Hindernis.

Die Verwendung von Kryptodollar, allen voran Tether, können hier Abhilfe schaffen. Nicht nur können damit potenzielle Kapitalverkehrskontrollen umgangen werden, Transaktionen mit Kryptodollar lassen sich im Vergleich zur traditionellen Finanzinfrastruktur grundsätzlich leichter initiieren und abwickeln.

Die Nachfrage nach Tether dürfte also heute schon mehrere reale Bedürfnisse stillen. Angesichts der US-Dollar-Nachfrage, die immer stärker von den unterschiedlichsten Teilen dieser Erde ausgehen wird, dürfte die "Hyper-Crypto-Dollarisierung" erst begonnen haben. Ironischerweise kommt damit die Dollarisierung öffentlicher Blockchains.

bitpanda pro

Europas sichere Exchange für Krypto-zu-Fiat-Märkte.

Rechtskonform mit den Richtlinien der EU

Bitpanda Pro ist AML5-konform und besitzt eine PSD2-Lizenz, die von der österreichischen Finanzmarktaufsicht ausgegeben wird. Durch die Einhaltung der aktuellsten Richtlinien für Kryptowährungen haben wir eine stabile Grundlage für sicheres und zuverlässiges Trading geschaffen.

Beliebte europäische Fiat-Märkte

Wir bieten Tradern Zugang zu den beliebtesten europäischen Trading-Paaren mit hoher Liquidität wie BTC/EUR, BTC/CHF, ETH/EUR und vielen weiteren. Unsere unterstützten Fiat-Märkte werden bald um GBP und TRY erweitert.

Hochmoderne Trading API

Über REST und Websocket-APIs können sich Trader mühelos mit unserer Plattform verbinden, Trading Bots verwenden und erhalten Zugang zu allen aktuellen und relevanten Marktdaten, um ihre Investitionsziele bestmöglich zu erreichen.

Fortgeschrittene Orderarten & niedrige Gebühren

Neben Market und Limit Orders bietet Bitpanda Pro auch fortgeschrittene Orderarten wie GtC, GtT, IoC und FoK an. Außerdem zählen unsere Tradinggebühren zu den niedrigsten der Branche.

Jetzt www.bitpanda.com/pro besuchen

Exklusives Interview mit dem MWC Team

Key Takeaways

- MimbleWimbleCoin ist ein neuer Privacy Coin. Zu den Privacy Coins gehören außerdem Dash, Monero, Zcash, Zcoin, Beam, und Grin. MimbleWimbleCoin ist skalierbarer als Monero, aber weniger privat.

- MimbleWimbleCoin (MWC) hat sich im November 2019 von Grin abgespaltet und erreichte Anfang Dezember ein Tief von $0,25 pro Münze mit einer Marktkapitalisierung von weniger als $2 Millionen. Seit Dezember ist die Marktkapitalisierung von MWC jedoch um 6.100 % gestiegen. Die MWC-Marktkapitalisierung liegt derzeit bei rund $125 Millionen. Damit ist sie die 13. größte Proof-of-Work-Münze nach Bitcoin Gold und Decred.

- Im Gegensatz zu Grin hat MWC eine feste Obergrenze für das Gesamtangebot von 20 Millionen. Schaut man sich die Anzahl der pro Tag erstellten Münzen an, so bilden MWC, Monero, Bitcoin und Bitcoin Cash die Schlusslichter. In Bezug auf den US-Dollar-Wert der Anzahl der pro Tag erstellten Münzen liegt MWC immer noch am niedrigsten, gefolgt von Monero und Dash. Schließlich ist der US-Dollar-Wert neuer Münzen, die pro Jahr im Verhältnis zu ihrer US-Dollar-Marktkapitalisierung erstellt wurden, auch der niedrigste für MWC mit 1,2 %, gefolgt von Bitcoin mit 1,7 %, Monero mit 2,8 %, Litecoin mit 6,1 %, Dash mit 8,4 % und Zcash mit erstaunlichen 35,1 % (!).

MimbleWimbleCoin Team

Wir möchten dem MWC-Team herzlich für dieses Interview danken. Die Gründer möchten anonym bleiben; Sie einigten sich jedoch auf ein exklusives Interview mit dem Crypto Research Report zum Thema Online-Datenschutz im digitalen Zeitalter. Weitere Informationen zu MWC finden Sie unter mwc.mw .

Einer der Hauptgründe für den Erfolg und die Popularität von Bitcoin ist das **nicht vertrauenswürdige Design**. Anstatt Menschen die Freigabe und Abwicklung von Finanztransaktionen anzuvertrauen, vertrauen Bitcoiners Softwareprotokollen. Besonders revolutionär an Bitcoin war, wie das Netzwerk Arbeitsnachweise verwendete, um Angriffe mit doppelten Ausgaben zu stoppen, und wie jeder auf der ganzen Welt neue Transaktionen validieren und eine Kopie des Datenbankverlaufs speichern konnte. Stellen Sie sich vor, die Credit Suisse oder die Bank of America erlaubten nicht nur jedem, ihre gesamte Transaktionsdatenbank einzusehen, sondern auch jedem, über die Gültigkeit neuer Transaktionen abzustimmen.

Im Laufe der Zeit wurde es jedoch aufgrund der Größe der Bitcoin-Blockchain immer teurer und exklusiver, ein Validierungsknoten im Bitcoin-Netzwerk zu werden. Ohne hohe Investitionen in die Rechenleistung ist es unmöglich, neue Transaktionen weiterzuleiten und eine Kopie der Datenbank zu speichern. Ein Newcomer in der Bitcoin-Blockchain muss ungefähr eine Woche damit verbringen, die 277-Gigabyte-Datenbank vorhandener Transaktionen herunterzuladen, um an der Validierung neuer Transaktionen teilnehmen zu können. Die mit Bitcoin verknüpfte „Blockchain“ ist jedoch nur eine Art von verteilter Ledger-Datenbankarchitektur. Es gibt auch andere Arten von verteilten Hauptbuchdatenbanken, wie z. B. die gerichteten azyklischen Graphen von IOTA, die wir in der Juni-2018-Ausgabe des *Crypto Research Report* untersucht haben. Dieser Artikel beschreibt eine andere Art von verteilter Hauptbucharchitektur namens MimbleWimble, die im Vergleich zur Bitcoin-Blockchain spezifische Vor- und Nachteile hat.

„In economics, fungibility is the property of a good or a commodity whose individual units are essentially interchangeable, and each of its parts is indistinguishable from another part.“

MimbleWimbleCoin

Was Sind Privacy Coins?

In einem kürzlich veröffentlichten Bericht des Blockchain Observatory and Forum der Europäischen Union mit dem Titel *„Legal and Regulatory Framework of Blockchains and Smart Contracts“* erklären die Autoren ausdrücklich, dass Regulierungsbehörden Blockchain-Explorer verwenden sollten, um Transaktionen zu verfolgen und persönliche Informationen über die Absender und Empfänger von Bitcoin-Transaktionen herauszufinden.[66]

„Obwohl dies zum Zeitpunkt der Transaktion nicht immer erkennbar ist, können bei ausreichender Zeit und Mühe viele Parteien einer Transaktion entlarvt werden. Daher besteht zu diesem Zeitpunkt keine Frage der völligen Straflosigkeit für Blockchain-Akteure.

Drittens kann jedoch nicht geleugnet werden, dass einige privacy-orientierte Blockchains, beispielsweise Monero oder ZCash, schlechten Schauspielern wirksame Werkzeuge für echte Anonymität bieten können. Es ist wichtig zu beachten, dass anonyme Transaktionen in der Praxis

—

66 *Legal and Regulatory Framework of Blockchains and Smart Contracts* [Thematischer Report], The European Union Blockchain Observatory and Forum, 27. September 2019. Abgerufen von https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf

derzeit nicht weit verbreitet sind: Bitcoin und Ethereum, die beliebtesten Plattformen, unterstützen keine Anonymität.

Die Regierungen versuchen auch, die Verwendung von Anonymisierungstechniken in Blockchain-Netzwerken zu unterbinden, indem sie beispielsweise AML-Regeln auferlegen und damit das Tor zwischen den Welten der Kryptowährungen und des Fiatgeldes überwachen (siehe auch nächster Abschnitt). Obwohl die Anonymisierung derzeit kein signifikantes Durchsetzungsrisiko für Blockchains ohne Erlaubnis darstellt, könnte die Verwendung anonymer Blockchains zu einem Problem werden, sollte sie sich erheblich verbreiten.

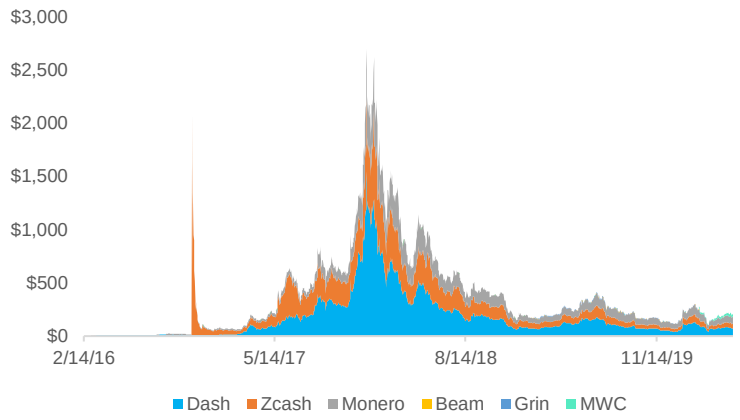
„A civilized society involves total transparency for institutions and full privacy for individuals.“

Marco Ricca

Es scheint, dass die Bereitstellung von Identifizierungsinstrumenten für Staaten (möglicherweise unter der Kontrolle von Gerichten oder durch den privaten Sektor auf Zahlungsbasis) eine Mindestbedingung sein sollte, damit ein Staat die Verantwortung durchsetzen und damit die Wirkung des Gesetzes auf das menschliche Verhalten im Blockchain-Bereich sicherstellen kann.“

Viele Marktteilnehmer halten Fungibilität für ein Merkmal guten Geldes. Bitcoin ist nicht fungibel, was bedeutet, dass Bitcoins auf ihre ursprüngliche Transaktion zurückgeführt werden können, als sie gemined wurden. Privacy Coins sind Münzen, die versuchen, die Privatsphäre von Bitcoin zu verbessern, indem sie die gehandelten Beträge und die an der Transaktion beteiligten Wallet-Adressen verbergen. Privacy Coins verwenden Technologien wie das Mischen von Münzen und vertrauliche Transaktionen. Zu den größten Privacy Coins gehören Dash, Monero, Zcash, Grin, Beam und MimbleWimbleCoin. Im Jahr 2014 wurde Dash eingeführt, die erste Privacy Coin auf dem Markt. Dash gibt jedem Benutzer die Wahl, ob er seine Transaktion privat machen will oder nicht. Die Dash-Technologie verwendet das Mischen von Münzen, um Informationen über die Sende- und Empfangsadressen zu verschleiern. Nur 2 % der Dash-Transaktionen verwenden die Datenschutzoption von Dash. Die restlichen Transaktionen von Dash sind genauso nachvollziehbar wie Bitcoin-Transaktionen. Einige Monate nach dem Erscheinen von Dash wurde eine neue Privacy Coin namens Monero auf den Markt gebracht. Im Gegensatz zu Dash ist jede Monero-Transaktion privat. Blockchain-Explorer sehen die in Monero-Transaktionen gesendeten Beträge nicht. Monero führte vertrauliche Ringsignaturen ein, die Monero-Benutzern eine sehr starke Privatsphäre bieten. Einige Jahre später kam Zcash im Jahr 2016 heraus, und in jüngerer Zeit, im Jahr 2018, kamen die MimbleWimble-Base-Layer-Münzen Beam und dann Grin heraus.

Abbildung: Performance von Privacy Coins, 2016–2020



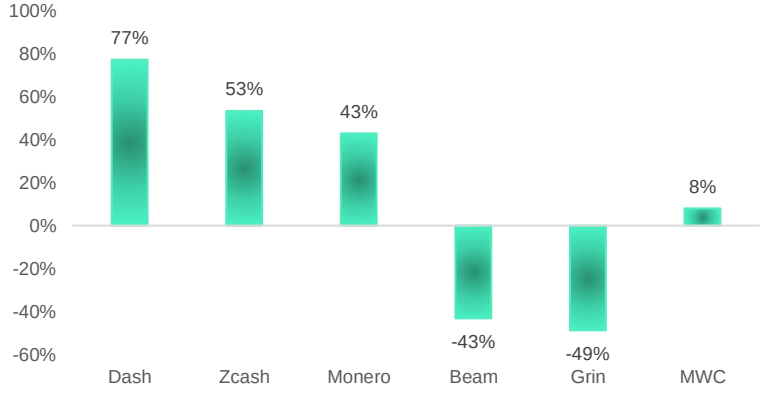
Quelle: Coinmarketcap.com, CryptoResearch.Report

„In October, eight months after discovery, the bug was surreptitiously patched during a planned network upgrade. Although Zcash have stated that they do not believe the bug was exploited, they cannot be certain.“

The Bitcoinist

Die Entwickler von Privacy Coins stehen jedoch vor Designentscheidungen, die jeweils spezifische Kompromisse aufweisen. Beispielsweise ist Monero privater als Dash, da der Transaktionsbetrag ausgeblendet ist, Monero ist jedoch weniger skalierbar, da mehr Ressourcen für die Ausführung eines vollständigen Knotens erforderlich sind, wodurch er weniger zensurresistent ist. Ein weiterer Kompromiss besteht darin, nachweisen zu können, dass eine Münze knapp ist, und über Datenschutzfunktionen zu verfügen. Blockchains, die die abgewickelten Beträge verdecken, haben Schwierigkeiten, die Gesamtmenge der im Umlauf befindlichen Münzen zu bestimmen. In einem kürzlich im Academic Blockchain Podcast mit dem Chief Technology Officer von Ledger geführten Interview diskutierte Demelza Hays Zcashs „Inflationsfehler“. Der Inflationsfehler von Zcash macht es unmöglich, die tatsächliche Gesamtmenge der vorhandenen Münzen zu berechnen. Dies bedeutet, dass es unendlich viele Münzen geben könnte, was einer der Säulen eines guten Geldes im digitalen Zeitalter widerspricht, nämlich der Knappheit. Das MimbleWimble-Protokoll verwendet jedoch mathematische Beweise mit Überwerten von Zwischentransaktionen, um zu beweisen, dass alle Belastungen und Gutschriften im Hauptbuch Null ergeben.

Abbildung 23: Rendite von Privacy Coins Seit Jahresbeginn



Quelle: Coinmarketcap.com, CryptoResearch.Report

Vertrauliche Transaktionen auf den Punkt gebracht

Wenn in Bitcoin Person A eine Transaktion an Person B sendet, wird ein nicht ausgegebenes Transaktionsoutput erstellt. Wenn Person B eine Transaktion an Person C senden möchte, verwendet Person B diese nicht ausgegebenes Transaktionsoutput als Eingabe für die Transaktion.

In MimbleWimbleCoin fasst die Blockchain diese beiden Transaktionen zu einer zusammen, indem die Zwischentransaktion von A nach B und von B nach C übersprungen wird.

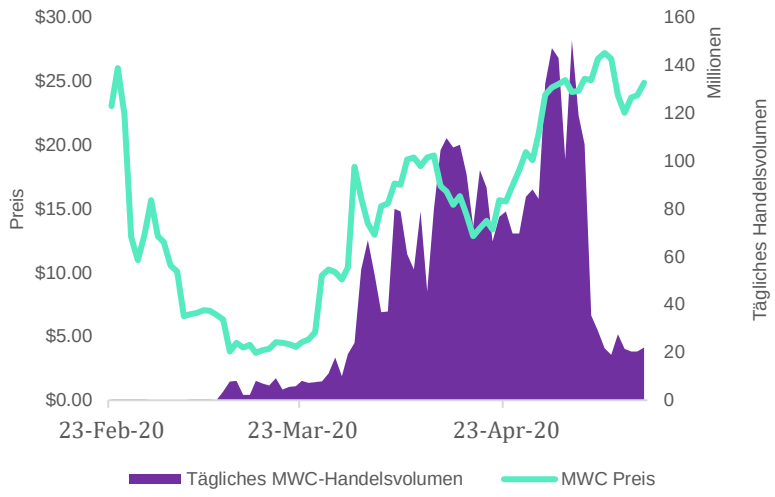
Obwohl nicht die gesamte Transaktion gespeichert wird, gibt es ein kleines Artefakt von Transaktion B, das in der MimbleWimbleCoin-Blockchain gespeichert wird. Dies wird als "Überschuss" bezeichnet. Durch Entfernen von B verbessern gleichzeitig Skalierbarkeit und Datenschutz.

Aber was ist MimbleWimble? Im Jahr 2016 veröffentlichte eine anonyme Person das MimbleWimble-Protokoll, um die **Skalierbarkeit und** den **Datenschutz** von Bitcoin zu verbessern. MimbleWimble ermöglicht es, Transaktionen zu signieren und zu validieren, ohne dass jede historische Transaktion validiert und die Eingaben einer Transaktion in den Hash einer neuen Transaktion aufgenommen werden muss. Dies reduziert die Größe der Blockchain drastisch. Befürworter hatten MimbleWimble ursprünglich als Sidechain oder Soft Fork für Bitcoin vorgeschlagen. Die aktuellen Implementierungen des MimbleWimble-Protokolls basieren jedoch auf neuen Kryptowährungen, die neue Blockchains wie Grin, Beam und MimbleWimbleCoin (MWC) erstellt haben, die MimbleWimble elegant in der Base Layer anwenden.

Während des Jahres 2019 und bis in das Jahr 2020 hinein klang ein Großteil des MimbleWimble-Hypes zusammen mit den Marktkapitalisierungen von Grin (derzeit etwa $19 Millionen) und Beam (derzeit etwa $16 Millionen) ab. MimbleWimbleCoin (MWC) spaltete sich im November 2019 von Grin ab und erreichte Anfang Dezember ein Tief von $0,25 pro Münze mit einer Marktkapitalisierung von weniger als $2 Millionen. Seit Dezember ist die Marktkapitalisierung von MWC jedoch um 6.100 % gestiegen. Die MWC-Marktkapitalisierung liegt derzeit bei rund $125 Millionen und hat sich in den letzten zwei Monaten größtenteils über $100 Millionen konsolidiert. Nach Marktkapitalisierung ist MWC derzeit die drittgrößte Privacy Coin hinter Monero und Zcash und die 13. größte Proof-of-Work-Münze hinter Bitcoin Gold und Decred. MWC wird derzeit auf Hotbit, Bitforex, Whitebit, Trade Ogre und Toktok gehandelt.

Die beiden Ideen, die die Grundlage für MimbleWimble bilden, stammen aus der Arbeit des Blockstream-Mitbegründers Gregory Maxwell zu „Confidential Transactions“ und „CoinJoin“. Vertrauliche Transaktionen verwenden Verschlüsselung, sodass in der öffentlichen Blockchain nicht die Anzahl der Münzen angezeigt wird, die in einer Transaktion gesendet oder empfangen werden. In Bitcoin kann beispielsweise jeder die Menge an Bitcoin sehen, die in jeder Transaktion gesendet wird. In MWC kann die Öffentlichkeit jedoch nicht sehen, wie viel gesendet wird, obwohl überprüft werden kann, ob die Transaktion den Konsensregeln entspricht, um beispielsweise doppelte Ausgaben zu verhindern und die Gesamtzahl der Münzen durchzusetzen. Die zweite Innovation, die das MimbleWimble-Protokoll verwendet, ist CoinJoin. Dies bedeutet, dass mehrere Transaktionen im Netzwerk zu einer Transaktion zusammengeführt werden, sodass die Blockchain-Forensik den tatsächlichen Absender und den tatsächlichen Empfänger einer bestimmten Transaktion nicht erkennen kann.

Abbildung 24: Die Neueste Privacy Coin auf dem Markt: MimbleWimbleCoin



Quelle: Coinmarketcap.com, CryptoResearch.Report

Es gibt jedoch auch Nachteile des MimbleWimble-Protokolls. Beispielsweise erlaubt es kein umfangreiches Scripting. Glücklicherweise wurden seitdem umfangreiche Untersuchungen durchgeführt, und mit MimbleWimble sind diese Arten von Skripten und Anwendungen möglich: Transaktionen mit mehreren Signaturen, Zeitsperren, Atomic Swaps und zeitlich gesperrte Hash-Verträge, die den Baustein für Zahlungskanäle und Lightning Network bilden. Ein weiterer großer Nachteil von Münzen, die das MimbleWimble-Protokoll verwenden, einschließlich Grin, Beam und MWC, besteht darin, dass diese Blockchains derzeit nicht weit verbreitet sind. Solange nicht mehr Menschen diese Münzen verwenden und mehr Menschen Transaktionen senden, kann der Nutzen der Privatsphäre durch ihre Verwendung eingeschränkt sein.

Wo Sie mehr über MimbleWimble erfahren

Eine gute Erklärung für die Funktionsweise von MimbleWimble finden Sie auf der Smith & Crown-Website. Darüber hinaus ist der ursprüngliche Vortrag von Andrew Poelstra über die Durchführung der MimbleWimble-Validierung auf YouTube.

Was im Digitalen Zeitalter Gutes Geld Macht

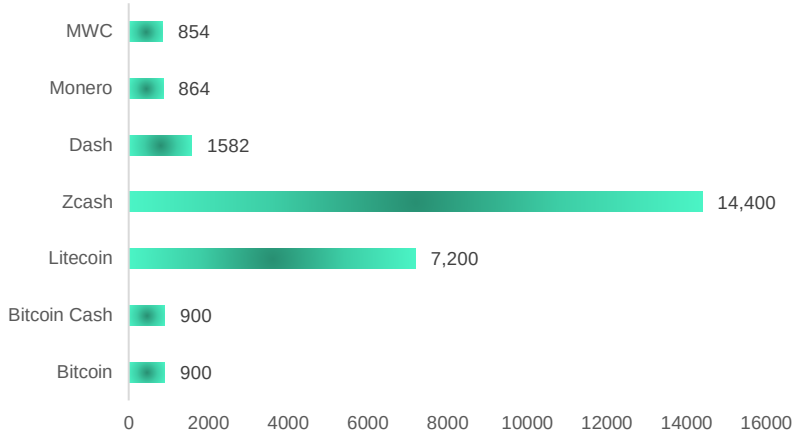
Gutes Geld im digitalen Zeitalter muss (1) **erkennbar**, (2) **knapp**, (3) **zensurresistent**, (4) **langlebig und unzerstörbar**, (5) **erweiterbar**, (6) **verkaufsfähig**, (7) **tragbar**, (8) **fungibel**, (9) **privat** und (10) **teilbar** sein.[67] Die meisten Kryptowährungen erfüllen diese Kriterien jedoch nicht. Im Jahr 2019 war Grin eine der am meisten diskutierten Münzen. Die Anleger stellten jedoch schnell fest, dass die hohe Inflationsrate von Grin und das Fehlen einer festen Obergrenze für das Angebot schlechter waren als die Inflation im US-Dollar. Dies führte dazu, dass die Leute sich fragen, warum sie Grin mit US-Dollar kaufen sollten, wenn Grin ein schlechterer Wertspeicher ist. Die Grin-Emissionsrate beträgt 1 Grin pro Sekunde auf unbestimmte Zeit. Pro Jahr werden 31.536.000

—

67 „What Makes Good Money in the Information Age?“, *MWC*, 2020. Abgerufen von https://www.mwc.mw/good-money

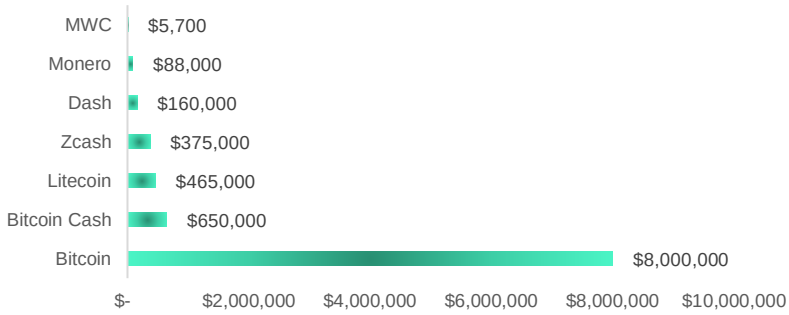
Grin erzeugt. Derzeit gibt es ungefähr 43 Millionen Grin. Dies führt in den Anfangsjahren zu einem sehr niedrigen Verhältnis von Bestand zu Durchfluss. Im Jahr 2020 beträgt das Stock-to-FLow-Verhältnis von Grin ungefähr das 1,19-fache oder ungefähr 43.000.000 Grin geteilt durch die neue Produktion von 31.536.000. Dies dient als Übertragung von Vermögen von Besitzern auf Miners.

Abbildung 25: Die Anzahl der pro Tag neu erstellten Münzen



Quelle: Coinmarketcap.com, diverse Whitepapers, CryptoResearch.Report

Abbildung 26: US-Dollar-Wert der Neu Erstellten Münzen pro Tag



Quelle: Coinmarketcap.com, diverse Whitepapers, CryptoResearch.Report

Wie Saifedean Ammous erklärt, führt ein niedriges Stock-to-Flow-Verhältnis zu einer Wertübertragung von den Besitzern der Assets an die Produzenten, während ein hohes Stock-to-Flow-Verhältnis zu niedrigeren Kosten führt, gemessen am Vermögenswert selbst für die Besitzer. Vor dem Start von Grin schlug ein MWC-Entwickler eine Angebotsobergrenze und Änderung der Emissionsrate vor, was jedoch von der Grin-Community, die als grünes Licht fungierte und Teil der Inspiration für das Forking von Grin war, schnell abgelehnt wurde. Bei Finanzinnovationen geht es schließlich darum, viele verschiedene Ansätze auszuprobieren, um Geldprodukte auf den Markt zu bringen, damit die Verbraucher sie genießen können. Alle vier Jahre erfolgt eine Bitcoin-Halbierung, und nach der Halbierung im Mai 2020 betrug das Bitcoin-Aktien-Flow-Verhältnis ungefähr 55. Dies macht Bitcoin vergleichbar mit Gold. MWC ist das Problem der festen Obergrenze und des niedrigen Stock-to-Flow-Verhältnisses angegangen,

indem sie der Münze eine feste Obergrenze von 20.000.000 gegeben hat und damit eine viel langsamere Emissionsrate erzielen konnte. Wie Bitcoin verwendet MWC einen reinen Proof-of-Work-Algorithmus und hat das höchste Stock-to-Flow-Verhältnis einer beliebigen Base Layer MimbleWimble-Münze. Bis Oktober 2020 wird MWC ein Stock-to-Flow-Verhältnis haben, das nahezu dem von Bitcoin entspricht, und bis Februar 2021 sogar ein deutlich höheres.

„Despite some common misconception, Bitcoin offers a very weak level of privacy."

Georg Fuchsbauer, Michele Orrù und Yannick Seurin

Bei der Anzahl der pro Tag erstellten Münzen liegen MWC, Monero, Bitcoin und Bitcoin Cash am niedrigsten. In Bezug auf den US-Dollar-Wert der Anzahl der pro Tag erstellten Münzen liegt MWC immer noch am niedrigsten, gefolgt von Monero und Dash. Schließlich ist der US-Dollar-Wert neuer Münzen, die pro Jahr im Verhältnis zu ihrer US-Dollar-Marktkapitalisierung erstellt wurden, auch der niedrigste für MWC mit 1,2 %, gefolgt von Bitcoin mit 1,7 %, Monero mit 2,8 %, Litecoin mit 6,1 %, Dash mit 8,4 % und Zcash mit erstaunlichen 35,1 % (!).

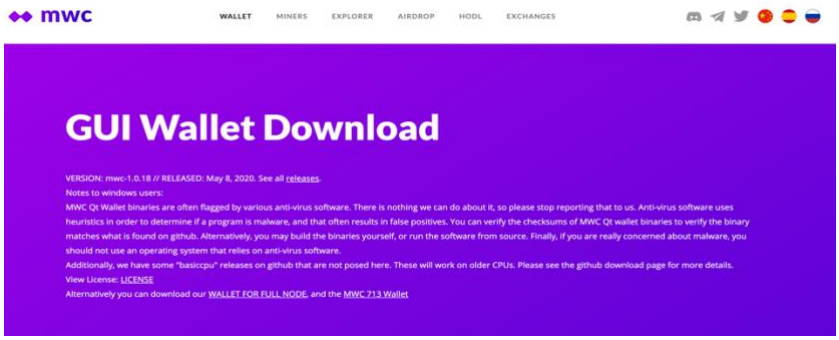
MWC hat jedoch aufgrund der Art und Weise, wie der anfängliche Bestand erstellt wurde, einen Pushback von der Kryptowährung-Community erhalten. Gemäß dem Whitepaper und dem Protokoll sollte die Hälfte des gesamten MWC-Angebots mit Proof-of-Work-Nachweis gemined werden, und die andere Hälfte wurde im Genesis-Block erstellt. Von diesem anfänglichen Bestand von 10.000.000 MWC, der bei seiner Erstellung wertlos war, wurden 2.000.000 MWC sofort an das Entwicklerteam verteilt, 2.000.000 MWC wurden dem HODL-Programm zugewiesen und 6.000.000 MWC wurden an alle Bitcoin-Besitzer abgeworfen, die sich über einen Zeitraum von drei Monaten erfolgreich registriert und ihre MWC-Zuteilung im Dezember 2019 in Anspruch nahmen. Über 5,4 Millionen MWC wurden erfolgreich kostenlos an Bitcoin-Besitzer abgeworfen und hatten zu diesem Zeitpunkt einen Gesamtwert von weniger als $2 Millionen. MWC verwendet hauptsächlich den C31-Proof-of-Work-Algorithmus, und die neue monatliche Emission von MWC aus einem reinen Proof-of-Work-Algorithmus beträgt ca. $500.000.

Wie Eine MWC-Transaktion Durchgeführt Wird

„The most important thing Bitcoin is missing right now is privacy."

Edward Snowden

MWC wurde geschaffen, um die Nachfrage nach Online-Geldtransfers mit voller Privatsphäre zu befriedigen, da Bitcoin-Transaktionen nicht so privat oder fungibel sind. MWC-Zahlungen unterscheiden sich geringfügig von Bitcoin-Transaktionen, **so gibt es beispielsweise nur Outputs und keine Adressen**. Schließlich wird alles mit vertraulichen Transaktionen verbunden, und dann werden die Signaturen in den Blöcken zusammengefasst. Um loszulegen, müssen Sie eine MimbleWimbleCoin-Wallet herunterladen. Um einen gewissen Kontext zu schaffen, stützt sich die andere Privacy Coin, Grin, hauptsächlich auf Befehlszeilenschnittstellentools, deren Verwendung jedoch für nicht technische Personen schwierig sein kann. Aus diesem Grund hat MWC eine sehr benutzerfreundliche Brieftasche erstellt, die hier heruntergeladen werden kann: https://www.mwc.mw/downloads



Nachdem Sie Ihre Wallet erfolgreich eingerichtet haben, gibt es zwei Methoden zum Senden und Empfangen von Transaktionen: die MWCMQS-Methode und die File-Methode. Im Allgemeinen umfasst dies sechs Schritte:

- Der Sender erstellt die Transaktion mit Output(s)
- Der Empfänger signiert die Transaktion
- Der Empfänger gibt dem Sender die Transaktion zurück
- Der Sender signiert die Transaktion
- Der Sender übermittelt dem Netzwerk die Transaktion
- Die Miners bestätigen die Transaktion als Block und fügen sie der Blockchain hinzu

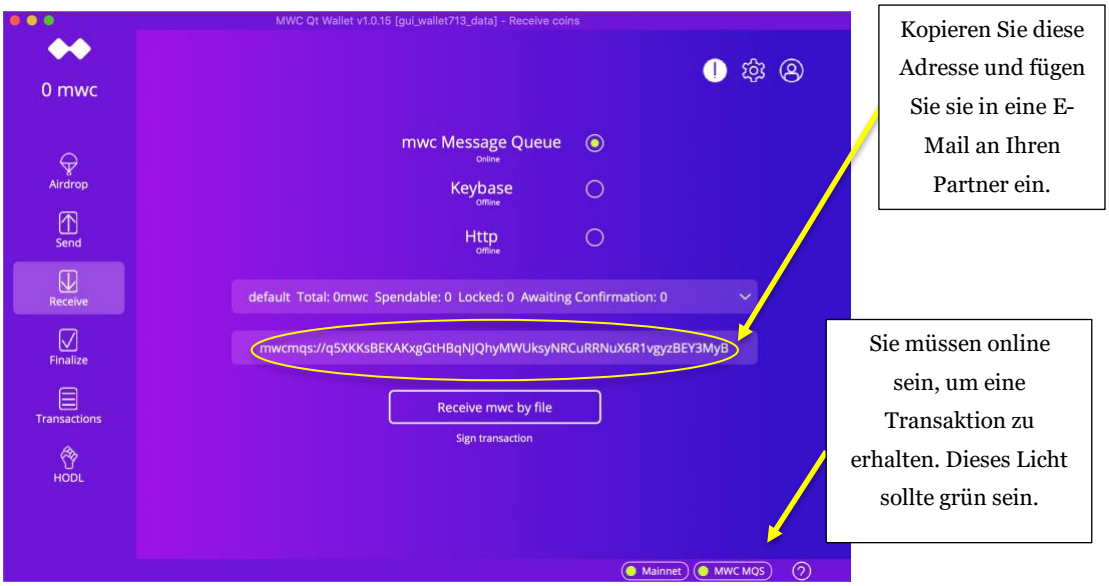
Die MWCMQS-Methode

„While privacy coins offer bad actors a level of anonymity, the liquidity issues and barriers to entry for buying and selling privacy coins make them impractical for most dark market purchases.“

John Jefferies
CipherTrace

Das Senden und Empfangen über die MWCMQS-Methode ist einer Bitcoin-Transaktion am ähnlichsten. Sowohl der Sender als auch der Empfänger müssen jedoch in der Lage sein, miteinander zu interagieren. **Dies bedeutet, dass der Empfänger online sein und mit der Adresse “hören” muss, an die der Absender zu senden versucht.** Dies bedeutet, dass Sie nicht einfach eine Adresse angeben, Ihren Laptop ausschalten und wie mit BTC, LTC usw. ins Bett gehen können.

Öffnen Sie zunächst die Brieftasche und klicken Sie im linken Menü auf „Empfangen“. Kopieren Sie die Adresse mwcmqs: // und senden Sie diese Adresse an Ihren Partner. Das Senden per E-Mail oder über eine Messaging-Anwendung ist in Ordnung. Damit Ihr Partner Ihnen eine Transaktion senden kann, **muss Ihre Wallet online sein** und auf diese bestimmte Adresse warten (unten rechts muss das MWCMQS grün sein).



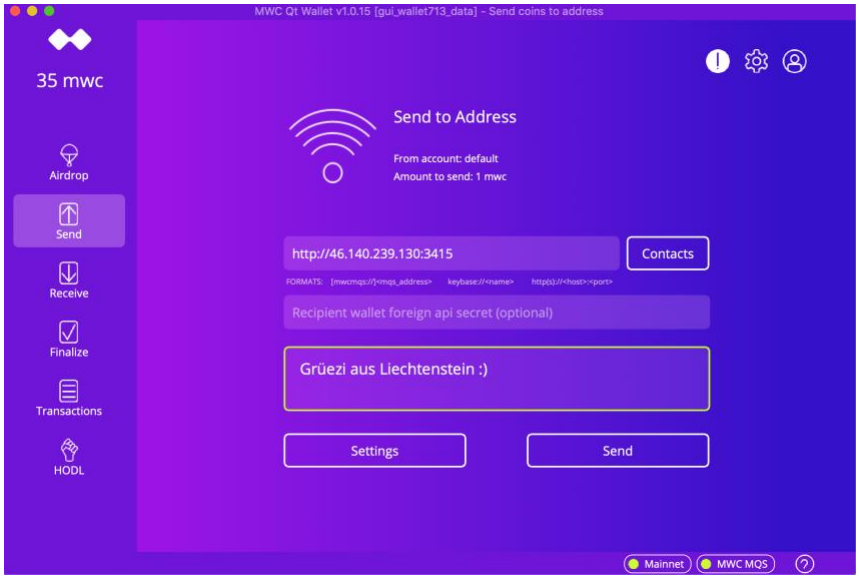
Sobald Ihr Absender die von Ihnen gesendete Adresse kopiert hat, kann er die Adresse in die Wallet einfügen, indem er im linken Menü auf die Option "Senden" klickt. Sie können auch eine Nachricht zusammen mit der Transaktion senden.

Die File-Methode

Obwohl die MWCMQS-Methode die einfachste Methode für Personen ist, die Bitcoin-Transaktionen gesendet haben, ist die Dateimethode die privateste Methode zum Senden von MWC-Transaktionen.

Das Senden und Empfangen per File erfordert fünf Schritte.

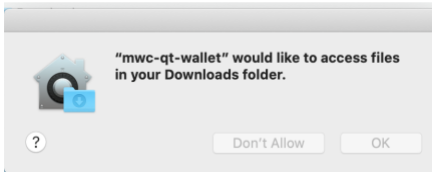
- Der Sender erstellt eine Transaktion und generiert eine .tx-Datei
- Der Sender übermittelt die .tx-Datei an den Empfänger
- Der Empfänger signiert die Transaktion und generiert die .tx-Antwort-Datei
- Der Empfänger übermittelt dem Sender die .tx-Antwort-Datei
- Der Sender signiert die Transaktion und übermittelt sie an das Netzwerk und schließt die Transaktion ab



„In cashless societies like Sweden, 95 % of all transactions are done using a plastic card. Every single one of those transactions is under full surveillance, not just by one intelligence agency, but you can assume by all simultaneously and surreptitiously. We already have a digital money future, which is a totalitarian surveillance nightmare.“

Andreas Antonopoulos

Zu Beginn hängt ein Sender die Datei mwc-fee.tx an eine E-Mail an und sendet diese Datei dann per E-Mail an den Empfänger. Dies umfasst die ersten beiden Schritte. Der Empfänger muss dann die Datei aus der E-Mail herunterladen und dann in seine MWC-Wallet gehen und die Datei einfügen. Abhängig von Ihrem Betriebssystem wird möglicherweise ein kleines Feld angezeigt, wenn Sie auf „MWC per Datei empfangen“ klicken. In diesem Feld werden Sie um die Erlaubnis gebeten, auf Dateien in Ihrem Download-Ordner zuzugreifen. Sobald Sie auf „OK“ klicken, müssen Sie die spezifische .tx-Datei finden, die der Sender Ihnen geschickt hat.



Anschließend muss der Empfänger eine neue mwc-payment.tx-Antwort-Datei per E-Mail zurücksenden, die die nächsten beiden Schritte darstellt. Der letzte Schritt ist dann der Abschluss der Transaktion auf der Seite des Absenders. Der Sender und der Empfänger können die Transaktion im Block-Explorer überprüfen: https://explorer.mwc.mw/. Durch Klicken in die obere rechte Ecke des Zahnrads können MWC-Benutzer ihre Transaktionen in der Blockchain anzeigen, indem sie auf die Ausgabe doppelklicken. Was cool ist, ist, dass nur Sie und die Person, mit der Sie die Transaktion abgewickelt haben, wissen, wie viele MWCs mit dieser bestimmten Ausgabe verbunden sind.

Kamingespräch mit dem MWC-Team

- Sind Sie von Austrian Economics inspiriert? Wenn ja, von welchem Vertreter besonders? Was ist Ihr Lieblingsbuch Austrian Economics? Und zu guter Letzt, was ist Ihr Lieblingszitat?

„Individual privacy online has decreased for the last nine consecutive years in a row.“

Freedom on the Net Report 2019

- ***„Ja, wir mögen Austrian Economics wegen ihrer Objektivität. Es geht darum zu verstehen, wie die Dinge im Gegensatz zu dem stehen, was wir viele wollen. Mises, Rothbard, Gordon, Block und andere haben hervorragende Arbeit geleistet. Human Action ist ein grundlegender Text in diesem Bereich. Wir sind Maximalisten der Währungssouveränität und große Fans aller Mittel, die dazu beitragen, diesen Zweck zu erreichen oder zu erreichen, ob dies nun in Form von Gold, Silber, Bitcoin, Dogecoin, MWC oder was auch immer geschieht. Mises erklärte: ‚Es ist unmöglich, die Bedeutung der Idee des gesunden Geldes zu erfassen, wenn man nicht erkennt, dass sie als Instrument zum Schutz der bürgerlichen Freiheiten gegen despotische Eingriffe der Regierungen konzipiert wurde. Ideologisch gehört es in dieselbe Klasse mit politischen Verfassungen und Grundrechten. Die Forderung nach verfassungsmäßigen Garantien und nach Gesetzentwürfen war eine Reaktion gegen willkürliche Regeln und die Nichtbeachtung alter Bräuche durch Könige. Das Postulat des gesunden Geldes wurde zuerst als Reaktion auf die fürstliche Praxis der Entwertung der Münzprägung angesprochen. Es wurde später sorgfältig ausgearbeitet und perfektioniert in der Zeit, in der – durch die Erfahrung der amerikanischen Kontinentalwährung, des Papiergeldes der Französischen Revolution und der britischen Restriktionsperiode – gelernt wurde, was eine Regierung mit dem Währungssystem einer Nation tun kann … Das Prinzip des soliden Geldes hat somit zwei Aspekte. Dies ist eine positive Bestätigung für die Wahl des Marktes für ein häufig verwendetes Tauschmittel. Es ist negativ, wenn es die Neigung der Regierung behindert, sich in das Währungssystem einzumischen.“***

- Sie erwähnen, dass das MWC-Team in Bitcoin investiert hat. Haben Sie auch in andere Privacy Coins investiert??

- ***„Wir wissen nicht. Das MWC-Team besteht aus einer beträchtlichen Anzahl von Personen, die durch den Zweck oder das Ziel der Währungssouveränität vereint sind. Und das bedeutet auch, dass jeder von uns mit seinem eigenen Geld macht, seine eigene Angelegenheit ist und nicht die anderer.“***

- Was sagen Sie zu dem Argument: „Nur Kriminelle verwenden Privacy Coins“?

- ***„Ohne die Fähigkeit, Geheimnisse zu bewahren, verlieren Individuen die Fähigkeit, sich von anderen zu unterscheiden, ein unabhängiges Leben zu führen, vollständige und***

autonome Personen zu sein. Dies bedeutet nicht, dass eine Person tatsächlich Geheimnisse bewahren muss, um autonom zu sein, sondern nur, dass sie die Fähigkeit dazu besitzen muss. Die Fähigkeit, Geheimnisse zu bewahren, setzt die Fähigkeit voraus, Geheimnisse selektiv offenzulegen. Daher ist die Fähigkeit zur selektiven Offenlegung nach eigenem Ermessen auch für die individuelle Autonomie wichtig.

„While privacy coins may intuitively appear likely to be preferred by malicious actors due to their purported anonymity-preserving features, there is little evidence to substantiate this claim.“

Rand Corporation

Geheimhaltung ist eine Form von Macht. Die Fähigkeit, ein Geheimnis zu schützen und die Privatsphäre zu wahren, ist eine Form der Macht. Die Fähigkeit, Geheimnisse zu durchdringen, sie zu lernen, sie zu nutzen, ist auch eine Form von Macht. Geheimhaltung stärkt, Geheimhaltung schützt, Geheimhaltung tut weh. Die Fähigkeit, die Geheimnisse einer Person ohne ihr Wissen zu lernen – die Privatsphäre einer Person im Verborgenen zu durchdringen – ist noch eine größere Macht.

Wir möchten der Menschheit helfen, ihr unveräußerliches Recht auf Geheimhaltung auszuüben, oder mit anderen Worten, Sie und Ihr Eigentum in Ruhe zu lassen. Dies ist umso wichtiger, als wir über Tools wie Bitcoin und MWC verfügen, die auf der Verschlüsselung mit öffentlich-privaten Schlüsseln basieren.“

- Wer ist die Zielgruppe für Privacy Coins? Was ist Ihrer Meinung nach die durchschnittlichen demographischen Eckpukte eines Privacy-Coin-Benutzers? Ich meine, denken Sie, dass Privacy Coins hauptsächlich in Industrieländern oder in Entwicklungsländern verwendet werden? Denken Sie, dass sie von relativ reichen oder relativ armen Menschen benutzt werden?

- ***„Wir sind uns nicht sicher, da wir neben der persönlichen Selbstbeobachtung nicht viel Marktanalyse durchgeführt haben. Zum größten Teil sind wir seit vielen Jahren bedeutende Bitcoin-Besitzer, sind uns jedoch seiner Eigenschaften bewusst und wissen, dass es nicht unbedingt alle Aufgaben erfüllt, die wir uns wünschen. Wir sahen die Möglichkeit, ein Produkt zu bauen, das wir selbst verwenden wollten, extrem knappes*** Ghost Money, ***und die anderen Geldunternehmer auf dem Markt vernachlässigten derzeit diese Marktnachfrage oder wählten Designmerkmale, die wir*** bei ***einem Produkt nicht als überzeugend empfanden. Also haben wir die Art von Geldprodukt gebaut, die wir selbst verwenden wollten.“***

- Was sind die wichtigsten Punkte auf der Roadmap für MWC in den nächsten 12 Monaten?

- ***„Vollständige Verteilung der ursprünglichen Aktien über den nicht beanspruchten Airdrop-Fonds und das HODL-Programm, zusätzliche Börsenintegrationen, größere Marktliquidität, zusätzliche Grin-Rebases, Freigabe einer mobilen Geldbörse, Atom-Swaps, eine dezentrale Börse, Multisig, Lightning-Netzwerk und andere Funktionen.“***

Fazit

Das MWC-Netzwerk wurde im November 2019 gestartet und hat mit 100 % Betriebszeit einwandfrei funktioniert. Das MWC-Team betrachtet das Protokoll als „verknöchert“ und sieht derzeit keine Notwendigkeit für eine zukünftige Hard oder Soft Fork, es sei denn, eine Schutzmaßnahme wäre erforderlich, um das Netzwerk zu schützen. Wir sind der Ansicht, dass der MimbleWimble-Sektor möglicherweise vernachlässigt wird, ein erhebliches störendes technologisches Innovationspotenzial aufweist und eine erhebliche Informationsasymmetrie auf dem Markt besteht. Diese Art von Technologie ist im Zeitalter der Überwachung besonders wichtig.

Disclaimer: Der Autor dieses Artikels ist der Inhaber von MWC.

Introducing...

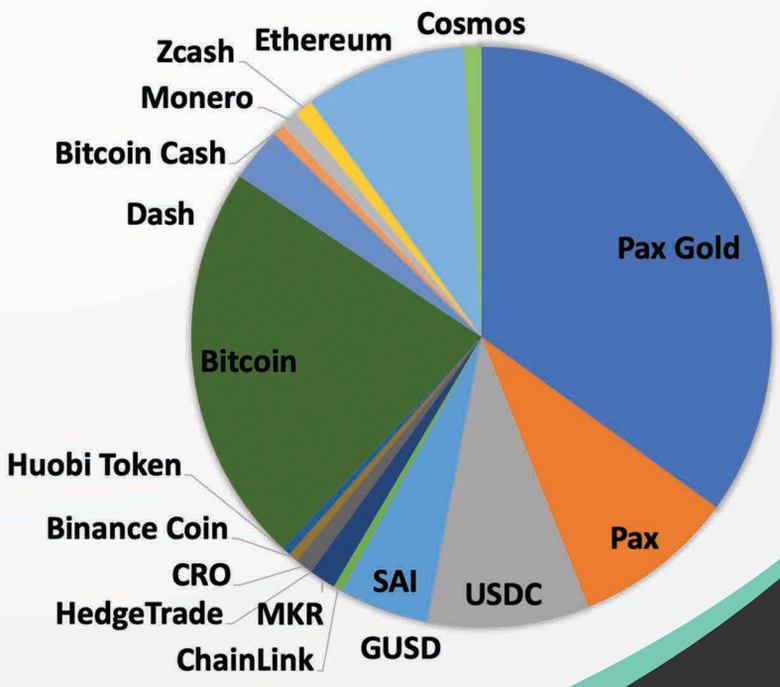
Crypto Research Newsletter

Professional Financial Analysis of Cryptocurrencies

See what our portfolio holds and follow our weekly trades for the price of a coffee!

Sign up for our newsletter!

CRR Portfolio Jan 31st 2020



crypto research .report

Crypto Research Report Buchempfehlung

Mit dem Buch *Das liechtensteinische Steuerrecht* von Matthias Langer kommt 2019 eine bisher noch fehlende Fachlektüre auf den Markt. Neben den Grundlagen des Steuerrechts in Liechtenstein trifft Matthias Langer mit dem Aufgreifen der Besteuerungsregelungen von Blockchain- und FinTech-Unternehmen den Nerv der Zeit und schafft steuerrechtliche Klarheit.

Nach einer Einführung zu Geschichte, Staatswesen und Wirtschaft des Fürstentums Liechtenstein, wird das Gesellschafts-, Stiftungs- und Trustrecht thematisiert. Dabei werden die einzelnen existierenden Rechtsformen sehr prägnant mit ihren Charakteristiken und rechtlichen Grundlagen vorgestellt. Anschliessend folgt ein Überblick zu Art und Umfang der liechtensteinischen Prüfungs-, Review- und Offenlegungspflichten, sowie zu den vorhandenen Rechnungslegungsvorschriften. Beginnend mit einer ersten Darstellung der Struktur des liechtensteinischen Steuersystems taucht Matthias Langer, der seit elf Jahren in Liechtenstein als Steuerberater tätig ist und mittlerweile eine eigene Kanzlei in Triesen unterhält, nun tiefer in steuerrechtliche Thematiken ein. So werden beispielsweise Vermögens- und Erwerbssteuer, Schenkungen und Erbschaften oder die Ertragssteuer mit Hilfe von anschaulichen Beispielen verständlich erklärt. Darüber hinaus vermittelt die Lektüre mit dem Aufgreifen der Besteuerung von Investmentfonds und Stiftungen, sowie den verschiedenen Strafmassen auch spezifische Bestimmungen des Steuersystems in Liechtenstein. Um die Darstellung des Themenkomplexes zu vervollständigen, findet das Internationale Steuerrecht mit seinen Regelungen zu Anrechnungen und Sitzverlegungen, sowie internationalen Abkommen seinen Platz in der Lektüre. Da Liechtenstein ausserdem als einer der Vorreiter in Sachen Blockchain und FinTech gilt, ist deren Handhabung der Besteuerung international von grossem Interesse. Nach einer kurzen Erklärung der Grundbegriffe und des Bilanzansatzes von Kryptowährungen, werden Besonderheiten der Erwerbs-, Ertrags- und Mehrwertsteuer thematisiert. Dabei lernt der Leser neben der Differenzierung verschiedener Coin-Arten, die steuerliche Bedeutung der Übertragung, des Handels und der Aufbewahrung von Coins/Tokens kennen. Zusammenfassend lässt sich sagen, dass sich das Buch mit allen wesentlichen Aspekten des Steuerrechts in Liechtenstein beschäftigt und darüber hinaus Einblicke in angrenzende Themengebiete gibt. Besonders zu erwähnen ist dabei die Behandlung steuerrechtlicher Besonderheiten von Blockchain- und FinTech-Unternehmen. Der Leser wird in der Lektüre auf tiefer Ebene abgeholt und bekommt einzelne Sachverhalte mit der Unterstützung von Beispielen veranschaulicht. Es ist dementsprechend zu bemerken, dass sich die Lektüre durch die strukturierte Gliederung, die kurzen, treffenden und leichtverständlichen Erklärungen, sowie die Verwendung von Beispielen, hervorragend lesen und verstehen lässt. Hinzukommend wird dadurch ein schnelles Nachschlagen und Nachvollziehen ermöglicht, ohne dass der Leser tiefgreifende Steuerkenntnisse besitzen muss. Auch wenn sich das Buch zwar hauptsächlich an angehende Unternehmer in Liechtenstein richtet, beinhaltet es auch Informationen, die für diejenigen interessant sind, die mehr über das Leben in Liechtenstein und das Land selbst erfahren möchten. Die deutsche Ausgabe des Buchs Das liechtensteinische Steuerrecht kann auf der Webseite des Verlags gekauft werden: Springer Verlag's Website.

Dipl.-Kfm Matthias Langer, LL.M.

Advisors

Um Ihnen stets genaue Informationen zu den wichtigsten und aktuellsten Entwicklungen im Krypto-Bereich liefern zu können, haben wir ein vielfältiges Team von Vordenkern, Akademikern und Finanzexperten für unser Advisory Board zusammengestellt. Die Aufgabe unseres Boards ist es, die Diskussion über die dringendsten Risiken und Chancen im Krypto-Währungsmarkt anzuregen. Unsere Berater kommen aus verschiedenen Ländern, haben unterschiedliche Bildungswege und Karrieren durchlaufen. Eines haben sie jedoch gemeinsam: Sie alle haben ein großes Interesse an der Blockchain-Technologie und den Kryptowährungen. Um stets auf dem Laufenden zu bleiben, treffen sich die Mitglieder des Advisory Board regelmäßig, um über die aktuellen Themen und Aussichten bezüglich des nächsten Quartals zu diskutieren. Alle Sitzungsprotokolle werden als Transkript veröffentlicht und kostenlos auf unserer Website unter www.CryptoResearch.Report. veröffentlicht. Zum Advisory Board gehören:

Max Tertinegg

Max Tertinegg ist CEO und Mitbegründer von Coinfinity in Graz. Seit 2014 arbeitet Herr Tertinegg mit Händlern, Investoren und Aufsichtsbehörden in Österreich zusammen, um Menschen innerhalb der Krypto-Welt näher zusammenzubringen. Max hat ein „Card Wallet“ designed.

Oliver Völkel

Oliver Völkel ist Partner bei StadlerVölkel Rechtsanwälte. Das Unternehmen hat seinen Sitz in Wien. Er begleitet Unternehmen und Banken in zahlreichen Phasen einer Kapitalmarktemittierung und Privatplatzierungen (national und international). Sein Schwerpunkt liegt auf den neuen Finanzierungsformen (Initial Coin Offerings, Initial Token Offerings) und der Gestaltung und Verhandlung von grenzüberschreitenden Fazilitätenverträgen und Sicherheitsdokumentationen – auch im Zusammenhang mit Kryptowährungen und Token.

Falls Sie unseren letzten Crypto Research Report verpasst haben und eine angenehme Lektüre wünschen, folgen Sie bitte den untenstehenden Links.

Crypto Research Report - Dezember 2017 Edition

- Eine Einführung in die Blockchain-Technologie und Kryptowährungen
- ICOs: Geld, Scams und große Hoffnungen
- US-regulierte Bitcoin- Derivate: Fluch oder Segen?
- Ein Index für Krypto-währungen
- Besteuerung von Kryptowährungen in Europa

Crypto Research Report - März 2018 Edition

- In Case You Were Sleeping: Ikarus-Edition
- Finanzblase oder Hyperdeflation?
- Coin Corner: Krieg um Bitcoin
- Technische Analyse: Droht uns ein Krypto-Winter?
- Crypto-Concepts: Forks
- 10 Fragen an Max Tertinegg, den CEO von Coinfinity
- Incrementum Insights: Krypto-währungen und das Finanzwesen

Crypto Research Report - Juni 2018 Edition

- In Case You Were Sleeping: Wall Street macht sich bereit
- Crypto Concept: Konsens-Mechanismen
- Währungswettbewerb & digitales Geld: Wie aktuell ist Hayeks Vorschlag?
- Coin Corner – Blockchain 3.0 Die Zukunft der DLT?

Crypto Research Report - Oktober 2018 Edition

- In Case You Were Sleeping: Handy Theft Edition
- Crypto Concept: Smart Contracts
- Liechtensteins Blockchain Strategie: Regierungschef Hasler im Interview
- Der Netzwerkeffekt als Bewertungsmethode
- Liechtensteins Blockchain Strategie: Einblicke in die Finanzmarktaufsicht
- Coin Corner: ETH, NEO, ADA & EOS

Crypto Research Report - Januar 2019 Edition

- In Case You Were Sleeping: Krypto-Winter Edition
- Crypto Concepts: Verwahrungslösungen für Kryptowährungen
- Ist ein Bitcoin Standard denkbar? Saifedean Ammous im Austausch mit dem Crypto-Research-Report
- Anforderungen an einen investierbaren Krypto-Index von institutionellen Investoren
- Equity Tokens
- Security Token Offerings: Rechtliche Herausforderungen für einen Kapitalmarkt auf der Blockchain

Crypto Research Report - April 2019 Edition

- In Case You Were Sleeping: Wenn die Ebbe kommt...
- Gold & Bitcoin im Duett: Eine Krypto Strategie, auch für institutionelle Investoren
- Technische Analyse: Frühlingserwachen?
- Crypto Concepts: Mining – Theorie und Praxis
- John Tromp: Making Computer Science Great Again

Crypto Research Report – Juli 2019 Edition

- In Case You Were Sleeping: Facebook Edition
- Libra: Das Ende des Geldmonopols?
- Coin Corner: Ripple Labs Inc. und XRP
- Kaminfeuergespräch mit Nick Szabo zur Skalierung Bitcoins
- Goldgedeckte Tokens

Crypto Research Report – Oktober 2019 Edition

- In Case You Were Sleeping: Banking auf der Blockchain
- Wie Krypto-Broker und -Fonds Liquidität bereitstellen
- Ein Leitfaden zur Kryptoregulierung in der Schweiz
- Die Tokenisierung des Schweizer Frankens; ein Interview mit Armin Schmid
- Incrementums Buchrezension

Crypto Research Report – Februar 2020 Edition

- In Case You Were Sleeping: Iran, Gold und ein kleiner Bitcoin Boom
- Das „Plan B"-Modell: Heiliger Gral der Bitcoin Bewertung?
- Das Stock-to-Flow-Modell: Mark Valek im exklusiven Gespräch mit „Plan B"
- Verwahrung von KryptoVermögenswerten: Was gibt es Neues?
- Bitcoin vs. Gold – ein fiktives Streitgespräch
- Incrementums Buchrezension

Wir möchten uns bei folgenden Personen für die Mitarbeit bei der Erstellung des CRR bedanken:

Bei unseren sachkundigen Beratern, darunter Max Tertinegg und Oliver Völkel und den Autoren, die zu diesem Bericht beigetragen haben, darunter Pascal Hügli. Unser Dank gilt auch unserem großartigen Webmaster Mark Mason und unserer Editorin Bianca Sayers

Kontakt:

Crypto Research Report
9492 – Eschen/Liechtenstein
http://www.cryptoresearch.report
E-Mail: info@cryptoresearch.report

Disclaimer:

Diese Publikation dient ausschließlich zu Informationszwecken und stellt weder eine Anlageberatung, eine Anlageanalyse noch eine Aufforderung zum Erwerb oder Verkauf von Finanzinstrumenten dar. Insbesondere dient das Dokument nicht dazu, eine individuelle Anlage- oder sonstige Beratung zu ersetzen. Die in dieser Publikation enthaltenen Angaben basieren auf dem Wissensstand zum Zeitpunkt der Ausarbeitung und können jederzeit ohne weitere Benachrichtigung geändert werden. Die Autoren waren bei der Auswahl der verwendeten Informationsquellen um größtmögliche Sorgfalt bemüht und übernehmen keine Haftung für die Richtigkeit, Vollständigkeit oder Aktualität der zur Verfügung gestellten Informationen bzw. Informationsquellen bzw. daraus resultierend Haftungen oder Schäden gleich welcher Art (einschließlich Folge- oder indirekte Schäden, entgangenen Gewinn oder das Eintreten von erstellten Prognosen).

Copyright: 2020 Crypto Research Report. Alle Rechte vorbehalten.