crypto research .report

Oktober 2018
Edition IV.

Smart Contracts
Liechtensteins Blockchain Strategie
Der “Network Effect” als Bewertungsmethode

Demelza Kelso Hays
Mark J. Valek

incrementum

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

Vontobel

bitpanda

www.cryptofunds.li

Inhaltsverzeichnis

Editorial **4**

In Case You Were Sleeping: Handy Theft Edition **5**

Ein Diebstahl im rechten Moment 6
Ihr Telefon könnte mehr kosten als Sie denken 6
Bitcoin lagern, aber wie? 8
Von China bis Liechtenstein 10
ETF oder kein ETF? 11
Ein Game Changer namens BAKKT 13
Die “echte” Welt entdeckt Bitcoin 14
Der finale Showdown 15

Crypto Concept: Smart Contracts **19**

Smart Contracts, Decentralized Applications, und Decentralized Autonomous Organizations 20
Smart Contract Theory in der Praxis 22
Krypto Firmen die Smart Contracts, DApps, und DAOs verwenden 23
When Smart Contracts Are Dumb 24

Liechtensteins Blockchain Strategie: Regierungschef Hasler im Interview **31**

Der Netzwerkeffekt als Bewertungsmethode **39**

Der Netzwerk Effekt 41
Metcalfe’s Gesetz für Krypto Assets 41
Network-Value-to-Metcalfe Ratio 43
Network-Value-to-Transaction-Value Ratio 47
Network-Value-to-Transaction-Value-to-Growth 50

Liechtensteins Blockchain Strategie: Einblicke in die Finanzmarktaufsicht **53**

Coin Corner: ETH, NEO, ADA & EOS **58**

Falsche Dichotomie 60
Ein dezentraler Weltcomputer 61
Wozu eine programmierbare Blockchain? 62
Gas – eine unerlässliche Komponente Ethereums 63
Kann sich Ethereum auf dem Thron behaupten? 64
Cardano: Wenn Wissenschafter Blockchains bauen 65
China nimmt es mit Ethereum auf 67
Die Unterschiede sind nicht zu übersehen 68
EOS - Ethereum's grösster Konkurrent? 70
Inflationierung als Belohnung 71
Angriff auf Ethereums derzeitige Raison d’ être 73
Wie hast du’s mit der Dezentralisierung? 74
Ein Kampf, der eigentlich keiner ist? 77

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 (wie auch die Incrementum AG) 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: 2018 Incrementum AG. All rights reserved.

Editorial

Liebe Leser!

Liechtenstein, die Heimat der Incrementum AG und des Crypto Research Reports, steht im Mittelpunkt dieser Ausgabe. Ein Highlight dieses Berichts ist ein exklusives Interview mit dem liechtensteinischen Regierungschef Adrian Hasler. Darüber hinaus behandeln wir das neue Blockchaingesetz und diskutieren mit der Finanzmarktaufsicht, wie sich dieses Gesetz auf auswirken wird. Obwohl die Steuern auf die Erstausgabe von Tokens in anderen Ländern niedriger sind, signalisiert die liechtensteinische Regierung Anlegern und Unternehmern, dass das Land sich als Standort für den Krypto-Sektor profilieren will. So wurde beispielsweise der weltweit erste regulierte Security Token in Liechtenstein auf den Markt gebracht.

Nach **In Case You Were Sleeping**, unserer traditionellen Zusammenfassung des letzten Quartals, vergleicht das Kapitel **Coin Corner** Ethereum, NEO und das neue EOS-Protokoll. Langfristig bezweifeln wir, dass der Markt Hunderte von Blockchains mit sehr ähnlichen Eigenschaften unterstützen wird. Stattdessen werden einige wenige ausgeprägte Blockchains mit starken Entwicklerteams dominieren. Ergänzend zum Kapitel Coin Corner enthält das Kapitel **Crypto-Concept** eine detaillierte Analyse von Smart Contracts.

Abschließend diskutieren wir den "Network Effect" als mögliche Bewertungs-methode für Krypto-Token. Bitcoin ist in seinem dritten Bärenmarkt, der bereits über sechs Monate andauert. Die Rendite seit Jahresbeginn liegt für den Kryptomarkt bei etwa -50%, die Einjahresrendite bei rund +150%. **Die vorgestellten Bewertungskennzahlen deuten jedoch darauf hin, dass der Kryptomarkt immer noch überbewertet ist. Dieser Bewertungsmethode zufolge könnten weitere Korrekturen anstehen.**

Diese Ausgabe beendet unser erstes Jahr der Veröffentlichungen und wir freuen uns auf ein weiteres Jahr des Crypto Research Reports. In den nächsten Monaten werden Airdrops, dezentrale Börsen und Atomswaps für Investoren und Aufsichtsbehörden zunehmend an Bedeutung gewinnen Unsere Dezemberausgabe wird besondere Einblicke in die rechtlichen Folgen dieser technologischen Fortschritte geben. Darüber hinaus werden wir die Marktstimmung für die Blockchain-Technologie im Nahen Osten analysieren.

Unser Stammleserschaft danken wir, dass Sie und treu bleiben und wir heissen Erstleser herzlich willkommen! **Wie immer wird die vierte Ausgabe des Berichts kostenlos in deutscher und englischer Sprache auf unserer Homepage CryptoResearch.report verfügbar sein.**

Nun wünschen wir Ihnen eine erkenntnisreiche Lektüre des Reports und freuen uns auf Ihr Feedback!

Demelza Kelso Hays und Mark Valek

In Case You Were Sleeping: Handy Theft Edition

Key Takeaways

- **CBOE plant die Einführung von Ethereum-Futures, die Weltbank hat den ersten Bitcoin-"Bond" aufgelegt und die NASDAQ wird Bitcoin, Ethereum und andere Kryptos 2019 listen und handeln.**

- **Der Capgemini-World Wealth Report zeigt, dass mehr als die Hälfte der vermögenden Privatpersonen (HNWIs) weltweit zumindest marginal an Bitcoin interessiert ist. Allerdings sind Investoren nach wie vor nicht in der Lage, Kryptowährungen sicher zu speichern. Coinbase schätzt, dass in diesem Jahr 20 Milliarden USD in die Depotbankdienste für Kryptowährungen fließen werden.**

- **Kryptowährung-Wallets sind sicherer, wenn die Zwei-Faktor-Authentifizierung (2FA) aktiviert ist. die Verwendung einer Telefonnummer für 2FA kann Konten jedoch anfällig für Hacker machen. Google Authenticator und Authy sind bevorzugte 2FA-Anwendungen.**

Ein Diebstahl im rechten Moment

Im Nachhinein ist man immer klüger. Heute wissen wir, dass man als Bitcoin-Investor ruhig hätte verkaufen können als der Preis im Jänner 2018 noch weit über 15.000 USD stand. Oder dass man zumindest nicht am Höhepunkt der letzten Manie hätte einsteigen sollen, in der Hoffnung auf 25.000, 30.000 oder 50.000 USD pro Bitcoin.

"It's a fascinating market… a $400 billion market that nobody owns… we've never seen that before…the industry as a whole could easily go to $4 trillion, $40 trillion is definitely possible. It's the ten-year forecast, it's not going to happen overnight."

Dan Morehead
CEO Pantera Capital

Eines wussten wir aber schon immer: Auf diese digitalen Wertgegenstände namens Bitcoin, Ethereum oder Ripple muss man gut aufpassen. In der Praxis ist das aber gar nicht einfach. Niemand weiß das heute besser als Michael Terpin.

Der amerikanische Unternehmer und Investor ist schon lange im Bitcoin-Business. Er gehörte zu den Mitgründern der allerersten Gruppe an Angel Investoren, die seit 2013 in junge Bitcoin-Firmen investiert. Ihr Name: BitAngels. Aus BitAngels ist auch einer der ersten Fonds für digitale Währungen entstanden. Das war im März 2014. Heute ist Terpin auch Berater bei Alphabit Fund, einer der größten Hedge Funds im Krypto Bereich.

Aber das ist alles egal. Denn Schlagzeilen macht Terpin jetzt vor allem durch sein Pech – und seinen juristischen Einfallsreichtum. Ihm wurden nämlich ausgerechnet im Jänner Bitcoin und andere Kryptowährungen im damaligen Gegenwert von rund 23 Millionen USD gestohlen.[1]

Ihr Telefon könnte mehr kosten als Sie denken

Der Investor wurde das Opfer einer neuen besonders perfiden Form des Betrugs, **bei der die Betrüger die Kontrolle über die SIM-Karte des Mobiltelefons ihrer Opfer erlangen.** Viele Online-Portale nutzen die Handynummer der Nutzer als zusätzliche Sicherheitsbarriere, indem sie etwa SMS schicken, wenn jemand sich einloggen will. Dies wird als Two-Factor Authentication (2FA) bezeichnet, was ua. von Google Authenticator und Authy angeboten wird.

Leider kann dieses Feature aber auch missbraucht werden, wenn es Hackern gelingt, die Kontrolle über das Handy zu übernehmen. **Diese Form des digitalen Identität-Diebstahls wird auch angewandt, um sich illegal besonders beliebte Social Media Accounts zu sichern.** Die werden dann im Darkweb weiterverkauft – gegen Bitcoin. Im Fall von Terpin wurden direkt Bitcoin und andere Kryptowährungen gestohlen.[2]

Woher wir das wissen? Vom Opfer selbst. Der sieht die Schuld für sein Unglück nämlich bei seinem Handybetreiber AT&T und will nun vor Gericht gehen. Seine Anwälte haben eine Schrift im Umfang von 69 Seiten vorgelegt, die

—

[1] Vgl. "U.S. investor sues AT&T for $224 million over loss of cryptocurrency," Gertrude Chavez-Dreifuß, *Reuters*, August 15, 2018. https://www.reuters.com/article/us-cryptocurrency-at-t-lawsuit/u-s-investor-sues-att-for-224-million-over-loss-of-cryptocurrency-idUSKBN1L01AA

[2] Vgl. "The SIM Hijackers," Lorenzo Franceschi-Bicchierai,*Motherboard,* July 17, 2018. https://motherboard.vice.com/en_us/article/vbqax3/hackers-sim-swapping-steal-phone-numbers-instagram-bitcoin

die angebliche Verantwortung des Netzbetreibers darlegt. Terpin verklagt AT&T nicht nur auf die Schadenssumme von 23,8 Millionen USD – berechnet auf der Basis des Bitcoin-Preises vom 7. Jänner 2018, als ein Bitcoin ein knapp über 17.000 USD wert war.

"...bitcoin could definitely see $50,000 in 2018...we will probably go through a suffering period of volatility."

Jeet Singh

Das war der Tag, an dem Terpin bestohlen wurde. Es war auch der Tag, an dem sich der Preis zum letzten Mal aufgebäumt hat. In den nächsten vier Wochen ist er um mehr als 60 Prozent gefallen. Den Boden hat der Bitcoin-Preis in der Gegend von 6.000 USD gefunden. Das hoffen zumindest die Anleger, die einen Absturz fürchten**. Denn wenn eine Unterstützung nach unten durchbrochen wird, taucht sie am Weg nach oben als Widerstand wieder auf.** Seit unserem letzten Report gab es zwar eine Preisrally, aber "higher highs" wurden nicht erreicht. **Der Bärenmarkt geht weiter.**

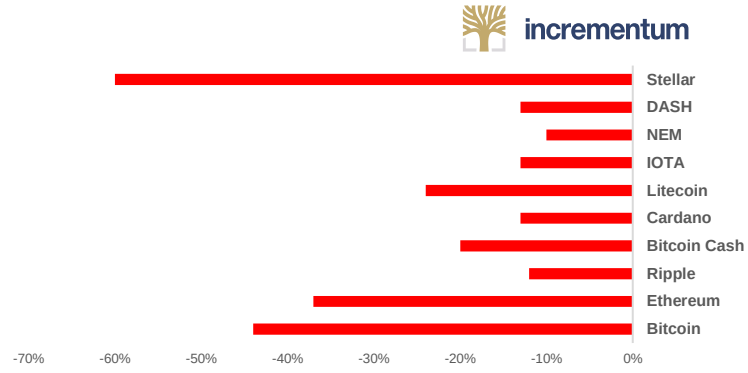
Grafik 1: Bitcoin Preis seit Jahresbeginn

Quelle: Coinmarketcap.com, Incrementum AG

Michael Terpin hat ohnehin andere Probleme. Er verlangt von AT&T nicht nur den Gegenwert seiner Bitcoins zurück, zusätzlich will er noch 200 Millionen USD als Schadenersatz. Sollte Terpin damit durchkommen, hätte er also nicht bloß einen Weg gefunden, seinem Portfolio den Bitcoin-Abverkauf des Jahres 2018 zu ersparen. Nein, er würde sein Kapital fast verzehnfachen. Dass AT&T jede Verantwortung von sich weist, versteht sich von selbst.

Was sagt uns diese Episode? Dass selbst erfahrene Bitcoin-Investoren, die seit Jahren im Geschäft sind und Millionen angehäuft haben, mit der sicheren Lagerung ihrer Coins überfordert sind. Zwar sind die Details des Diebstahls nicht ganz klar, aber die Indizien weisen stark darauf hin, dass hier einer oder mehrere von Terpins Trading-Accounts ausgeräumt wurde. **Eine weitere Möglichkeit ist, dass er seine Private Keys in schlecht gesicherter Form etwa in seinem E-Mail-Account oder einem Cloud-Dienst gespeichert hatte.** Beides sind keine sehr sicheren Optionen. Aber Terpin ist nicht alleine.

Grafik 2: Year-To-Date Rendite der Top 10 Coins



Quelle: Coinmarketcap.com, Incrementum AG

Bitcoin lagern, aber wie?

Die Frage nach der sicheren Lagerung von Bitcoins beschäftigt Anleger, seit es die Kryptowährungen gibt. Das ist auf den ersten Blick überraschend. Bitcoin braucht keine Bank, keine Zentralbank, keine Anmeldung und keine Genehmigung. Es ist ein in sich geschlossenes Geldsystem, das eine verlässliche und sichere Wertübertragung über das Internet ermöglicht.

"No one has ever hacked the bitcoin blockchain, it is the most secure place to put your money and as a stored value it is a great place to be."

Tim Draper

Den technisch versierten Früheinsteigern war all das Argument genug. Und wir können auch beobachten, dass Bitcoin seine Rolle als Geld und Fluchtwährung in Extremfällen sehr wohl weiterhin spielt. Da reicht ein Blick nach Venezuela, wo die Staatswährung aktuell eine Hyperinflation durchmacht.[3] Aber in den einigermaßen stabilen Finanzmärkten des Westens, wo Bitcoin vor allem ein Spekulationsobjekt ist, stellt sich die Situation anders dar.

Die Frage des einfachen Zugangs und der Lagerung von digitalen Assets ist größtenteils unbeantwortet. Der Mainstream-Investor will sich nicht um Private Keys oder Hardware Wallets kümmern. Auch der Einstieg institutioneller Investoren in den Sektor wird dadurch behindert. Erst langsam kommen ausgereifte Modelle für Bitcoin-Custodianship auf den Markt. Die Investmentbank Nomura hat ein Konsortium mit den Firmen Ledger und Global Advisors gegründet und bastelt an einer Lösung. Der Name: Komainu. Indes arbeiten drei Großbanken an ihren eigenen Angeboten: Bank of New York, JPMorgan und Northern Trust.[4]

Ein weiterer Player ist –natürlich – Coinbase. Kyle Samani, ein Partner beim Krypto-Hedgefund Multicoin Capital, testet gerade deren neu angebotenen Custodian-Dienst. Bloomberg spricht diesbezüglich gar von einem "game changer". "Es gibt viele Investoren, für die Custodianship die letzte Hürde darstellt", so Samani und ergänzt: **"Im Laufe des Jahres wird der Markt**

—

[3] Vgl. "Bitcoin Trading in Venezuela is skyrocketing amid 14,000% inflation," John Detrixhe, *Quartz,* June 8, 2018. https://qz.com/1300832/bitcoin-trading-in-venezuela-is-skyrocketing-amid-14000-inflation/

[4] Vgl. "Regulated Crypto Custody Is (Almost) Here. It's a Game Changer," Olga Kharif and Sonali Basak, *Bloomberg,* June 18, 2018. https://www.bloomberg.com/news/articles/2018-06-18/regulated-crypto-custody-is-almost-here-it-s-a-game-changer

kapieren, dass Custodianship ein gelöstes Problem ist. Das wird eine große Welle an Kapital bringen."

Coinbase verlangt für seine Angebot eine Einmalzahlung von 100.000 USD und danach eine Gebühr von 0,1 Prozent pro Monat bei einer Mindesteinlage von 10 Millionen USD. Dennoch geht man bei Coinbase davon aus, dass Assets im Gegenwert von rund **20 Mrd. USD in Custodian Services** fließen könnten. Das Problem ist auch nicht ganz neu. Auch für traditionelle Assets wie Cash, Goldbarren oder Diamanten braucht es Custodians, die sich seit Jahrzehnten oder sogar Jahrhunderten am Markt etabliert haben. Aber Kryptowährungen sind vor möglichen Hackerangriffen zu schützen. Und oft ist ihre juristische Behandlung noch nicht geklärt. Etablierte Player wie JP Morgan und Northern Trust sind deshalb sehr zurückhaltend. Sie wollen in den Markt, warten aber noch ab und gehen "extrem vorsichtig" vor, wie eine Quelle gegenüber Bloomberg sagte.

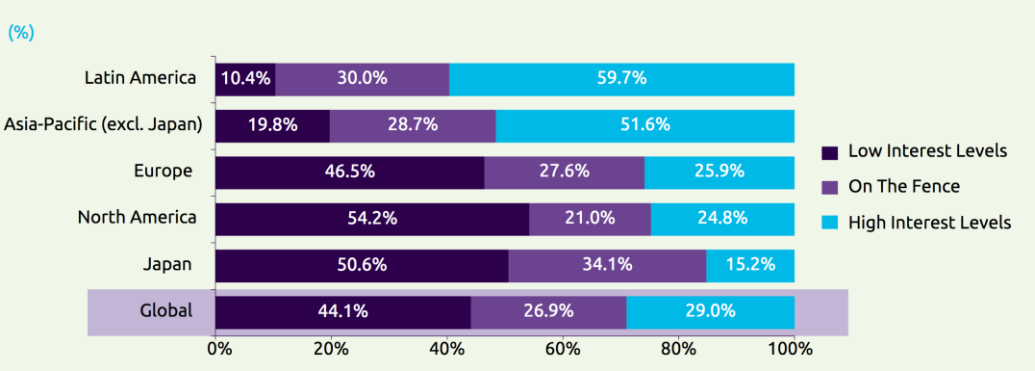
Wir werden die Entwicklung der Custodian-Angebote für Bitcoin und andere Kryptowährungen weiterhin genau beobachten. **Bärenmärkte sind der ideale Zeitpunkt, um die Infrastruktur zu verbessern.** Die zaghaften Fortschritte im Custodian-Sektor sind für uns ein Hinweis darauf, wie jung dieser Markt noch ist – und wie lange er noch brauchen könnte, um erwachsen zu werden.

"In different countries Bitcoin is qualified differently…but to me it's more than a currency."

Jeet Singh

Ein weiterer Hinweis: Der Preisboom von 2017 hat die Aufmerksamkeit der Millionäre auf Bitcoin gelenkt. Und wie der jährliche Capgemini-World Wealth Report zeigt, sind **mehr als die Hälfte der weltweiten "high net worth individuals" (HNWIs) zumindest oberflächlich an Bitcoin interessiert.** Aber nur ein Drittel von ihnen fühlt sich von den Vermögensberatern ausreichend informiert und betreut. Anders gesagt: Zwei von drei Beratern haben noch keine Ahnung von Bitcoin. Jetzt, da ihre reichen Kunden sich darüber beschweren, sollte sich das rasch ändern. Das ist ein Hauptgrund, warum Incrementum den Crypto Research Report veröffentlicht. **Wir sind bestrebt, die Anleger zu informieren und bieten auch Investmentlösungen wie einen AIF-geregelten Kryptowährungsfonds an**.

Grafik 3: Capgemini World Wealth Report: Interesse an Krypto



Quelle: https://www.capgemini.com/service/world-wealth-report-2018/

Von China bis Liechtenstein

Nochmal zurück zur Frage des Custodianship: Auch Fidelity, einer der größten Anbieter für Finanzprodukte in den USA, will sich in diesem Markt etablieren. CEO Abigail Johnson gilt als eine der berühmtesten Bitcoin-Fürsprecherinnen im US-Mainstream. Johnson hat sich bereits im Mai 2017 öffentlich für Bitcoin ausgesprochen. Sie will es auch nicht bei der Lagerung von Coins belassen, sondern hat sich zum Ziel gesetzt, den Zugang für Investoren zu vereinfachen. Ein möglicher Weg: Fidelity dürfte an einer eigenen Kryptobörse basteln und zwar schon seit einem Jahr.[5]

Die schweizer Bahngesellschaft SBB verkauft Bitcoin und wirbt nun mit dem Bitcoin Logo auf Plakaten.

Auch das Wettrennen um die nächste große Bitcoin-Börse ist längst voll im Gang. Die Schweizer Börse arbeitet an einer Krypto-Trading-Plattform. Sie soll die "erste ihrer Art" werden und schon Anfang 2019 an den Start gehen. **"Das ist der Beginn einer neuen Ära", kündigte Jos Dijsselhof, CEO des Betreibers SIX, an: "Für uns ist vollkommen klar, dass vieles von dem, was in der digitalen Welt geschieht, die Zukunft unserer Industrie bestimmen wird."**[6]

Die Börse in Toronto, Kanada, hat ähnliche Pläne. Auch die Börse Stuttgart in Deutschland will in den Markt. Man bastelt an einer eigenen App, genannt "Bison", die es Anlegern erlauben soll, ohne Gebühren digitale Assets zu kaufen. Auch eine Trading-Plattform ist geplant. Die Deutschen gehen aber noch ein Stück weiter. **Sie wollen auf ihrer Plattform auch ICOs möglich machen,** deren Coins dann sofort handelbar sind.[7]

Bisher wird der Markt von der ursprünglich in China gegründeten Börse Binance dominiert. Binance selbst ist aber kaum mehr als ein Jahr alt. Die Schnelllebigkeit des Bitcoin-Marktes und teils unklare gesetzliche Regelungen habe dazu geführt,

—

5 Vgl. "Fidelity, a household name in American investing, is plotting a big move into cryptocurrency trading," Frank Chaparro, *Business Insider*, June 6, 2018. https://www.businessinsider.de/fidelity-a-household-name-in-american-investing-is-plotting-a-big-move-into-cryptocurrency-trading-2018-6?r=US&IR=T

6 Vgl. "A Traditional Stock Exchange Is Also Going to Trade Cryptocurrencies Like Bitcoin," David Meyer, *Fortune*, July 6, 2018. http://fortune.com/2018/07/06/swiss-stock-exchange-cryptocurrencies/

7 Vgl. "Boerse Stuttgart to develop ICO platform and MTF for cryptocurrency trading," *Finextra*, August 2, 2018. https://www.finextra.com/newsarticle/32477/boerse-stuttgart-to-develop-ico-platform-and-mtf-for-cryptocurrency-trading

dass Binance nach China und Hong Kong auch in Malta Fuß gefasst hat und zuletzt auch in Liechtenstein, in der Heimat von Incrementum. **Eine Kooperation zwischen der Liechtensteiner Kryptobörse LCX soll Anlegern ein Fiat-Gateway in Euro und Schweizer Franken eröffnen.** Gleichzeitig hat die Regierung in Liechtenstein ein neues Gesetz auf den Weg gebracht, das Kryptofirmen und ICOs anlocken soll.[8]

Ziel ist es, dem Krypto Valley in der Schweiz Konkurrenz zu machen. Lt. Anwalt und Softwareentwickler Thomas Nägele, prüfen immer mehr Blockchain-Firmen die Gesetzeslage in Malta, Gibraltar, der Schweiz und Liechtenstein und entscheiden sich dann für Vaduz.[9] Der sogenannte "Blockchain Act", der Mitte 2019 in Kraft treten soll, ist die Idee des liechtensteinischen Regierungschefs Adrian Hasler, der sogar dem Bitcoin-Medium Cointelegraph ein Interview gegeben hat.[10] "Wir können eine global orientierte und gut ausgebildete Szene sehen, die sehr stark in den Fortschritt bei Blockchain-Technologien involviert ist. Wir glauben, dass wir erst am Anfang einer aufregenden und langfristigen Entwicklung stehen", sagte Hasler. **In dieser Ausgabe unseres Reports finden Sie auch ein ausführliches Interview mit dem Regierungschef Liechtensteins.**

ETF oder kein ETF?

"We observe a remarkable, globally oriented, and well-educated scene that is very much involved in the advancement of blockchain technology, and we believe that we are only at the beginning of an exciting and long-term development."

Regierungschef Adrian Hasler

Welche drei Buchstaben sind im Bitcoin-Sektor derzeit am wichtigsten? Nein, nicht FUD (Fear Uncertainty Doubt), sondern ETF (Exchange Traded Funds). Nichts bewegt den Preis derzeit so sehr wie die Frage, ob und wann die US-Aufsicht SEC einen Bitcoin-ETF genehmigen könnte. Es dürften unzählige Anträge vorliegen. Bisher hagelte es aber nur Absagen, **erst Ende August gleich für neun potenzielle ETFs.** Die Entscheidung sei kein Urteil über Bitcoin an sich, so die SEC. Vielmehr gehe es darum, Anleger vor den unsicheren und manipulierten Kryptomärkten zu schützen. Übersetzung: Bitcoin ist der SEC noch nicht erwachsen genug. [11]

Woher aber kommt die Aufregung rund um einen möglichen Bitcoin-ETF? So ein ETF wäre die wohl bequemste Form für ein Bitcoin-Investment, weil zumindest alle technischen Unsicherheiten für den Anleger beseitigt wären. Man kann die Situation bei Bitcoin am besten mit Gold vergleichen. Wer das Edelmetall physisch kaufen will, braucht einen Händler, einen Safe und eine Versicherung.

—

[8] Vgl. "Binance LCX Launches Fiat-toCrypto Exchange in Liechtenstein," Ana Alexandre, Cointelegraph, August 16, 2018. https://cointelegraph.com/news/binance-lcx-launches-fiat-to-crypto-exchange-in-liechtenstein

[9] Vgl."Krypto-Start-ups entscheiden sich selten gegen Liechtenstein," Pascal Züger, *Cash,* August 13, 2018. https://www.cash.ch/news/politik/blockchain-vaduz-krypto-start-ups-entscheiden-sich-selten-gegen-liechtenstein-1199004

[10] Vgl. "PwC's Pierre-Edouard Wahl: Blockchain Can Bring Positive Competition to Swiss Banking Space," Molly Jane Zuckerman, *Cointelegraph*, August 8, 2018. https://www.cash.ch/news/politik/blockchain-vaduz-krypto-start-ups-entscheiden-sich-selten-gegen-liechtenstein-1199004

[11] Vgl. "Bitcoin ETFs Aren't Coming Any Time Soon Thanks to the SEC," Rachel Evans and Lily Katz, *Bloomberg,* August 23, 2018. https://www.bloomberg.com/news/articles/2018-08-23/bitcoin-etfs-won-t-be-coming-any-time-soon-thanks-to-the-sec

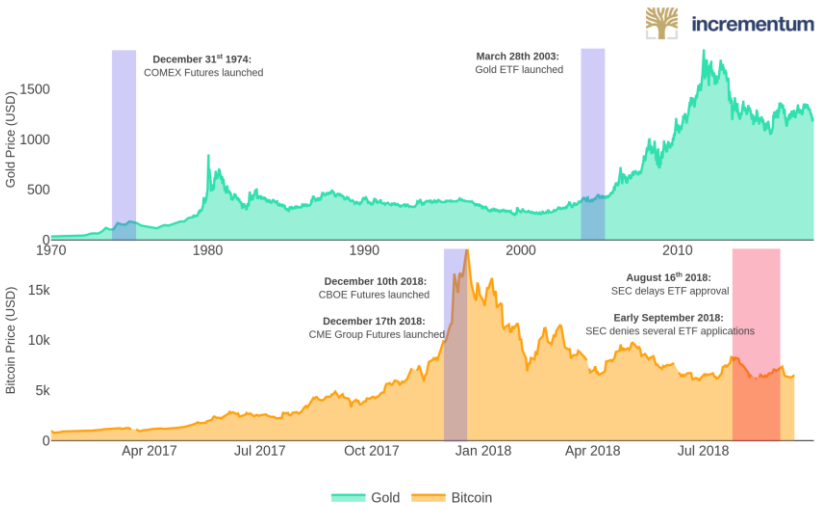
In Partnerschaft mit der Commonwealth Bank of Australia nutzte die Weltbank eine private Ethereum-Blockchain, um eine zweijährige Anleihe im Wert von 110 Millionen australischen Dollar (79 Millionen Dollar) an sieben

Wer es wiederverkaufen will, muss das Gold aus dem versicherten Safe nehmen und einen Käufer finden. Das ist zwar für überzeugte Goldbugs, die auf ein physisches Investment schwören, die bis heute beliebteste, wenngleich durchaus aufwendige Methode. Aktien kann man ja auch per Knopfdruck kaufen. Und ein ETF ermöglicht das eben für Edelmetalle und in Zukunft vielleicht für Bitcoin. Die mühselige Arbeit des physischen Kaufs und der Lagerung übernimmt der ETF-Betreiber. Der Anleger muss nur noch auf einen Knopf drücken.

Einige Beobachter meinen, dass **die Einführung eines Gold-ETF im Jahr 2004 sehr wichtigfür den Bullenmarkt von Gold war. Jetzt hoffen viele Bitcoin-Anleger auf denselben Effekt für ihr bevorzugtes Asset.** Allerdings lässt der ETF auf sich warten und jede Ablehnung oder Verschiebung einer Entscheidung durch die US-Aufsichtsbehörden drückt auf den Preis.[12] Unserer Meinung nach macht es keinen Sinn, ein Bitcoin-Investment allein von der ETF-Frage abhängig zu machen. Es wird mittel- bis langfristig einen oder mehrere solche Vehikel geben. Aber die laufende Debatte ist vor allem bedeutend, weil sie auf Basis der Fundamentaldaten von Bitcoin geführt wird. Soll heißen: Nur wenn die Märkte für die Kryptowährung tief und "erwachsen" genug sind, kann die Aufsicht einem ETF auch zustimmen.

Die Ende 2017 eingeführten Bitcoin-Futures waren ein wichtiger Schritt in diese Richtung. Die Börse CBOE ist auch im Rennen um einen ETF und hat unserer Meinung nach die besten Chancen, Teil der ersten genehmigten Tranche zu sein. Bitcoin sollte von den Aufsichtsbehörden wie Gold und andere Rohstoffe behandelt werden, sagt die CBOE. **Aber wann der erste ETF genehmigt wird, lässt sich aktuell nicht abschätzen. Es kann sich um Wochen, Monate und sogar Jahre handeln.** Alles hängt davon ab, wie schnell sich die Märkte entwickeln.

Grafik 4: Bitcoin vs. Gold Einführung von Futures & ETFs



Quelle: Incrementum AG

[12] Vgl. "Are Bitcoin ETFs Back on the Table Again?," Crystal Kim, *Barron's*, March 27, 2018. https://www.barrons.com/articles/are-bitcoin-etfs-back-on-the-table-again-1522179678

In einer Reaktion auf die SEC haben sich einige amerikanische Börsen zusammengetan, um Regeln und Standards für die junge Industrie auszuarbeiten. Diese "Virtual Commodity Association" wurde von den Gemini-Gründern Cameron und Tyler Winklevoss ins Leben gerufen.[13]

Ein Game Changer namens BAKKT

Manche Betreiber werden gar nicht auf die ETF-Entscheidung der US-Aufsicht warten wollen. Das Ziel, mehr Investoren in den Sektor zu locken, lässt sich auch auf anderem Wege erreichen. Der vielleicht wichtigste Game Changer könnte direkt von der Intercontinental Exchange (ICE) kommen, die mit der New York Stock Exchange (NYSE) die größte Börse der Welt betreibt.

Schon im November will man **einen Futures-Kontrakt mit "physical delivery" auflegen. Es sollen also "echte" Bitcoins fließen**. Als Basis soll die bestehende Infrastruktur der ICE dienen. Später soll eine eigene Firma, genannt BAKKT, die Kryptopläne der Börse übernehmen. Auf Basis der Microsoft Cloud soll eine neue Krypto-Handelsplattform entstehen. Aber die Pläne gehen noch viel weiter.[14]

"Asia dominates cryptos because they're very used to trading digital assets. South Korea has been trading digital goods related to gaming for two decades. When you move to a purely money based digital currency they understand that culturally, so they get on board quickly."

Arthur Hayes, BitMEX CEO

"Durch die Verbindung einer regulierten Infrastruktur mit institutionellen und privaten Anwendungen für digitale Assets, wollen wir das Vertrauen in die Assetklasse global stärken", sagte der CEO von ICE, Jeffrey Sprecher, der auch nicht davor zurückschreckt, das Potenzial von Bitcoin konkret anzusprechen: **"Bitcoin könnte die Bewegung von Geld global massiv vereinfachen. Es hat das Potenzial, die erste weltweite Währung zu werden."** An dieser Stelle sind wir zwar geneigt darauf hinzuweisen, dass Gold seit Jahrtausenden als global akzeptierte Währung fungiert. Wir wissen die Offenheit von Sprecher gegenüber der Innovation Bitcoin aber zu schätzen.[15] Sprecher merkt an, dass der Handel mit Bitcoin und anderen Kryptowährungen klare Regeln braucht und eine verlässliche Infrastruktur. Hier stehen wir ganz klar noch am Anfang der Entwicklung.

Einer der ersten Partner von BAKKT soll Starbucks werden. **De facto dürfte es darauf hinauslaufen, dass man seinen Iced double tall decaf peppermint cafe latte bald mit digitalem Geld kaufen kann.** "Starbucks soll eine wichtige Rolle dabei spielen, praktische, vertrauenswürdige und regulierte Anwendungen für Konsumenten zu entwickeln, um ihre digitalen Assets in USD zu tauschen, um sie bei Starbucks zu verwenden", sagte Maria Smith, Vizepräsidentin für Partnerschaften und Zahlungsverkehr bei Starbucks.[16]

—

[13] Vgl. "The Biggest Digital Exchanges Are Teaming Up To Police the Crypto Space," Matthew Leising, *Bloomberg,* August 20, 2018. https://www.bloomberg.com/news/articles/2018-08-20/winklevoss-effort-to-police-bitcoin-signs-up-more-exchanges

[14] Vgl. "NYSE-owner ICE to form new company for digital assets," John McCrank and Anna Irrera, *Reuters*, August 3, 2018. https://www.reuters.com/article/us-ice-cryptocurrency-bakkt/nyse-owner-ice-to-form-new-company-for-digital-assets-idUSKBN1KO1QN

[15] Vgl. "Breaking: World's Biggest Stock Exchange Operator is Launching a Bitcoin Market," *CNN,* August 3, 2018. https://www.ccn.com/breaking-worlds-biggest-stock-exchange-operator-is-launching-a-bitcoin-market/

[16] Vgl. "New Starbucks partnership with Microsoft allows customers to pay for Frappuccinos with bitcoin," Sarah Whitten and Kate Rooney, *CNBC,* August 3, 2018. https://www.cnbc.com/2018/08/03/starbucks-partners-with-microsoft-ice-on-new-cryptocurrency.html

Die “echte” Welt entdeckt Bitcoin

Phasen fallender Preise sind gut für Grundlagenarbeit. Deshalb kommen aktuell immer mehr Meldungen, die die fundamentale Situation der Bitcoin- und Kryptomärkte zwar verbessern, die Preise aber nicht sofort beeinflussen. FUD und ETF sind keineswegs die einzigen Abkürzungen, die die Kryptowelt bewegen. Viele Wege führen in Richtung einer größeren Verbreitung und Akzeptanz von Bitcoin. Und so wie in unseren bisherigen Reports können wir auch in dieser Ausgabe eine ganze Reihe von Belegen aufzählen, dass Bitcoin in der "richtigen Welt" angekommen ist. Und wenn nicht dort, dann zumindest an der Wall Street.

Großinvestoren äussern vermehrt Interesse an der neuen Anlageklasse

Das CFA-Institute, wo zehntausende Menschen diffizile Prüfungen zu Finanzthemen ablegen, um sich später "zertifizierte Experten" nennen zu dürfen, ist jetzt auch auf den Bitcoin-Zug aufgesprungen und hat Fragen zu den Themen Krypto und Blockchain in ihre Materialien integriert. **"Der Sektor entwickelt sich viel schneller als andere"**, so Stephen Horan, Managing Director für Ausbildung beim CFA-Institute in Charlottesville, Virginia, und ergänzt: "Das ist keine vorübergehende Modeerscheinung." Offenbar reagiert das CFA-Institute auch auf die steigende Nachfrage aus Asien, wo ein Großteil des Krypto-Handels stattfindet.[17]

Was haben Ripple und die Clintons gemeinsam? Dies sieht nach einem teurem Werbeengagement aus.

Noch ein paar Abkürzungen gefällig? Fangen wir mit IMF an. Der Internationale Monetary Fund ist so etwas wie das Zentrum des internationalen Mainstream-Geldsystems. Es versteht sich von selbst, dass man dort lange skeptisch war gegenüber Bitcoin. Aber inzwischen gibt es ein Umdenken. Die Chefin des IMF, Christine Lagarde, ging sogar soweit zu sagen, dass Bitcoin und andere Kryptowährungen das Finanzsystem "sicherer" machen könnten. Allerdings nur im Idealfall. Sie warnte, wie es sich für die Chefin des IMF gehört, im selben Satz vor "einem neuen Vehikel für Geldwäsche und Terrorfinanzierung". Immerhin kann sich der IMF nun eine Welt vorstellen, in der traditionelle Banken und private Gelder wie Kryptowährungen existieren.[18]

Auf der Ebene der Zentralbanken ist man sich uneinig. Die Bank for International Settlements (BIS), die oft als "Zentralbank der Zentralbanken" bezeichnet wird, hat sich als harter Bitcoin-Gegner positioniert. In einem 24 Seiten langen Report rechneten die Ökonomen der BIS im Juni mit Bitcoin ab. Das sei schon heute ein "Umweltdesaster" und werde nie die Versprechen erfüllen, die seine Erfinder abgegeben haben.[19]

Die dezentrale Struktur von Kryptowährungen sei eine Schwäche und keine Stärke für Währungen, so die BIS. Es sei "einfach zu riskant", die globale Wirtschaft ohne

—

[17] Vgl. “‘This Is Not a Passing Fad’: CFA Exam Adds Crypto, Blockchain Topics,” Michael Patterson and Andrea Tan, *Bloomberg,* July 16, 2018. https://www.bloomberg.com/news/articles/2018-07-16/cfa-exam-adds-crypto-blockchain-topics-as-wall-street-dives-in?srnd=cryptocurriences

[18] Vgl. “Bitcoin tools could make finance system safer, says IMF boss,” Richard Partington, *The Guardian*, April 16, 2018. https://www.theguardian.com/technology/2018/apr/16/bitcoin-tools-could-make-finance-system-safer-says-imf-christine-lagarde

[19] Vgl. “Bitcoin Could Break the Internet, Central Bank Overseer Says,” Edward Robinson, *Bloomberg,* June 18, 2018. https://www.bloomberg.com/news/articles/2018-06-17/bitcoin-could-break-the-internet-central-banks-overseer-says

ein Zentrum zu betreiben. "Das dezentrale Konsensprinzip ist so fragil, dass das Vertrauen in das System jederzeit verschwinden kann", so der Report, der fortsetzt: "Das bedeutet, dass Kryptowährungen einfach aufhören können zu existieren, was zu einem totalen Verlust ihres Wertes führen würde." Zudem bestehe die Gefahr, dass Bitcoin das gesamte Internet zum Stillstand bringen könnte.

Ein wenig entspannter sieht Jay Powell, Chef der US-Notenbank Fed, die Sache. Der Kryptosektor sei nicht groß genug, um eine Gefahr für das Finanzsystem darzustellen, so Powell in einer Anhörung Mitte Juli. Die Fed habe keine Aufsicht über Kryptowährungen und wolle sie auch nicht regulieren, so Powell.[20]

Der finale Showdown

"The key thing is that the more [bitcoin] grows, the more it will deprive governments of the ability to print more money...I think, in the long run, this is going to be a very good thing for everywhere in the world, particularly places in the Middle East."

Saifedeam Ammous

Der Preis von Bitcoin und allen Altcoins befindet sich seit Beginn des Jahres in einem Abwärtstrend. Wie wir gesehen haben, nutzen viele seriöse Player diese Zeit für den Aufbau neuer Infrastruktur. Ganze Staaten, wie etwa Liechtenstein, bereiten sich auf die nächste Phase der Blockchain-Revolution vor. Auch traditionelle Player wie der IMF, die Fed und die BIS haben Bitcoin und Co. im Auge.

Gleichzeitig wird der Sektor weiterhin von Kinderkrankheiten geplagt. Zentral ist hier die ICO-Bubble, vor der wir schon in unserem allerersten Report gewarnt haben. Die ist noch nicht verschwunden. Niemand geringerer als Jihan Wu, CEO des Bitcoin Mining-Giganten Bitmain, erwartet aber genau das: "Ich glaube, dass ICOs eine nicht nachhaltige Finanzblase sind, die irgendwann platzen wird. In einem oder zwei Jahren. Das ist nur eine Frage der Zeit. Sie wird einfach verschwinden."[21]

Wu glaubt zwar daran, dass traditionelle Assets in Zukunft in Form von Tokens handelbar sein werden, nicht aber an Crowdfunding in Form von ICOs. Freilich: Er will seine Firma Bitmain durch einen klassischen IPO an die Börse bringen, hat also seine eigene Agenda. Aus unserer Sicht hat er dennoch Recht. ICOs waren der Hype des Jahres 2018 und haben vor allem den Preis von Ethereum in die Höhe getrieben. Wie weit die Preise fallen können, wenn diese Blase endgültig platzt, wollen wir uns gar nicht vorstellen. Wobei Wu vor allem Aufmerksamkeit verdient, weil er im Unterschied zu vielen anderen, die sich zu Kryptowährungen äußern, weiß, wovon er spricht.
Die tiefste Preisprognose, die wir finden konnten, stammt dieses Mal vom berühmten Ökonomen Joseph Stiglitz. Der sagte im Juli, dass die Staaten irgendwann den "Hammer" gegen Bitcoin einsetzen werden und die Kryptowährung zu Tode regulieren werden. "Die Mächtigen werden anonyme

—
[20] Vgl. "Powell Says Cryptocurrencies Aren't Big Enough to Pose a Threat," Olga Kharif, *Bloomberg*, July 18, 2018. https://www.bloomberg.com/news/articles/2018-07-18/powell-says-cryptocurrencies-aren-t-big-enough-to-pose-a-threat?srnd=cryptocurriences
[21] Vgl. "ICOs an ‚Unsustainable Financial Bubble': Jihan Wu," *CCN*, August 22, 2018. https://www.ccn.com/icos-an-unsustainable-financial-bubble-jihan-wu/

Transaktionen regulieren. Da kann man sich sicher sein. **Bitcoin kann in 10 Jahren nur 100 USD wert sein."**[22]

Vor wenigen Jahren kannten die wenigsten den Begriff Fiat Money. Dies hat scheinbar nichts mit der italienischen Automarke zu tun…

Dem können wir nicht direkt widersprechen, weil niemand in die Zukunft sehen kann. Eigenartig ist aus unserer Sicht aber die konkrete Zahl. Vor 10 Jahren gab es Bitcoin noch nicht mal. Manch frühe Bitcoin-Anleger können sich noch an eine Zeit erinnern, in der 100 USD eine verrückt hohe Prognose waren. Dass der Skeptiker Stiglitz Bitcoin überhaupt einen Wert zugesteht und sogar sagt, dass es in 10 Jahren noch existieren wird, ist unserer Meinung nach Sensation genug. Aus Anlegersicht sind solche extremen Prognosen immer mit Vorsicht zu genießen, sowohl die der Bären, als auch die der Bullen.

Auftritt Tim Draper. Der Milliardär und Gründer der Venture Capital Firma Draper Fisher Jurvetson sieht für die Zukunft eine völlig andere Welt als Stiglitz und andere Skeptiker: "Ich glaube, dass Kryptowährungen die Fiat-Währungen in den nächsten fünf bis sieben Jahren überholen werden. Ich halte viele Kryptowährungen – hauptsächlich Bitcoin. Ich kaufe noch viel mehr. Ich glaube, dass das die Zukunft ist. Fiat ist die Vergangenheit. Ich habe noch ein bisschen Fiat für die alltäglichen Transaktionen. Aber ich glaube, dass sich das in den nächsten paar Jahren ändern wird."[23]

Dass es in der Kryptowelt weiterhin zu Hacks und Diebstählen kommt, wie zuletzt beim Ethereum-basierten Netzwerk Bancor, beunruhigt Draper nicht. Hacks gäbe es auch in der traditionellen Bankenwelt. Er sieht diese Angriffe aber als Argument für die Sicherheit von Bitcoin. "Je größer das Netzwerk von Wallet Besitzern, Minern und Stakeholdern, desto sicherer ist die Kryptowährung. **Bitcoin ist also die sicherste."**[24]

Draper hat eine faszinierende Vision für die Zukunft der Finanzwelt. Er glaubt, dass Kryptowährungen die Umlaufgeschwindigkeit (Velocity) des Geldes erhöhen werden: "Der aktuelle Markt für Währungen ist 86 Billionen USD groß. Ich erwarte, dass er in den nächsten 10 Jahren auf rund 140 Billionen anwachsen wird. Dieses Wachstum wird in Krypto geschehen. Ich gehe davon aus, dass die Verwendung von Fiat-Währungen zurückgehen wird und dass der Kryptosektor bis zu 100 Billionen dieses Marktes einnehmen könnte. Bitcoin sollte davon 10 Prozent abbekommen, also 10 Billionen. Es gibt also noch viel Luft nach oben." Da hat er Recht. Am absoluten Höhepunkt, als Bitcoin bei fast 20.000 USD stand, war der gesamte Markt nicht einmal eine Billion USD groß. Viele Analysten gehen kurz- und mittelfristig dennoch davon aus, dass wir Bitcoin im Bereich von 5000, 4000 oder sogar 3000 USD sehen könnten, bevor der Bärenmarkt vorbei ist.

—

[22] Vgl. "Bitcoin price warning: BTC will drop to '$100' after being 'regulated into oblivion'," David Dawkins, *Express*, July 9, 2018. https://www.express.co.uk/finance/city/985964/Bitcoin-price-ripple-cryptocurrency-ethereum-BTC-to-USD-XRP-Joseph-Stiglitz

[23] Vgl. "Billionaire Investor Bill Draper Explains Why Bitcoin Will Hit $250,000 in 2022," Jordan French, *The Street*, July 25, 2018. https://www.thestreet.com/investing/bitcoin/billionaire-tim-draper-super-bullish-on-bitcoin-14603011

[24] Vgl. "Another Crypto Fail: Hackers Steal $23.5 Million from Token Service Bancor," Jeff John Roberts, *Fortune*, July 9, 2018. http://fortune.com/2018/07/09/bancor-hack/

"Bitcoin is a hedge against the whole world falling apart."

Peter Thiel

Langfristig wird es faszinierend zu beobachten, ob Stiglitz oder Draper Recht behalten. Bitcoin und Krypto haben wahrscheinlich das Potenzial, Drapers Vision Wahrheit werden zu lassen. Aber auf dem Weg dorthin werden vermutlich viele traditionelle Finanzinstitutionen, die derzeit über unvorstellbare Macht verfügen, einfach verschwinden. Wir können also nachvollziehen, dass Stiglitz mit massiver Gegenwehr rechnet. Um Bitcoin tatsächlich zu stoppen, wäre aber wohl internationale Kooperation auf einem bisher nicht vorstellbaren Niveau nötig. Die Vision von Satoshi Nakamoto scheint also intakt. **Bitcoin bläst tatsächlich zum Endkampf gegen Fiat. Neu gegen Alt. Online gegen Offline. Zentral gegen Dezentral. Und egal wie es ausgeht, spannend wird es auf jeden Fall.**

Vontobel

Investment Banking

Driven by the power of possibility

vontobel.com

Crypto Concept: Smart Contracts

“A smart contract is a computer program that directly controls some kind of digital asset… The smart contract approach says instead of a legal contract, immediately transfer the digital asset into a program, the program automatically will run code, validate a condition, and determine whether the asset should go to one person or back to the other person, or whether it should be immediately refunded to the person who sent it or some combination thereof. ”

Vitalik Buterin, Gründer von Ethereum

Key Takeaways

- **Kryptotoken von Plattformen wie Ethereum und EOS stellen im Vergleich zu Bitcoin, Monero und Litecoin eine besondere Investitionsmöglichkeit dar. Dennoch sind diese Utility Tokens (derzeit) immer noch hochgradig korreliert (0,8) mit Payment Tokens. Sie wiesen im vergangenen Jahr ein höheres Beta zu Payment Token auf.**
- **Utility Token stellen jene Geschäftsmodelle in Frage, die auf Vermittler wie Crowdfunding-Websites, bspw. Kickstarter angewiesen sind. Schweizer und US-Regulierungsbehörden argumentieren jedoch, dass zwischen 95% und 100% von ihnen rechtlich als Wertpapiere einzustufen sind.**
- **Zu den bemerkenswerten Utility-Tokens, die online für Furore sorgen, gehören Etherisc, PolkaDot, ShareRing, Dfinity und Cosmos.**

Smart Contracts sind dynamisch, komplex und unglaublich leistungsstark. Diese Technologie hat das Potenzial, die Art und Weise, wie Geschäfte abgewickelt werden, grundlegend zu verändern. Sie verspricht Regierungen und Unternehmen Kosten zu senken, die Vertragsdurchsetzung zu automatisieren und eine nachprüfbare Kontrollmöglichkeit zu bieten. Ihr langfristiges Potenzial ist unvorstellbar, doch stellen sie bereits heute Branchen wie Crowdfunding, das Rechtswesen und den Versicherungssektor auf den Kopf. Allerdings werden intelligente Verträge von Menschen gestaltet und deshalb sind sie nicht perfekt. **Über 2,4 Milliarden USD sind bereits durch fehlerhafte Smart Contracts verloren gegangen.** Der zukünftige Erfolg von Utility-Tokens hängt von der Fähigkeit der Entwickler ab, sicherere Anwendungen zu erschaffen, denen Benutzer auch vertrauen können.

Vor- und Nachteile von Smart Contracts

Smart Contracts haben mehrere Vorteile, darunter:

1.) Geringere Fehlerquote. Anstatt Menschen zu vertrauen, verlagern Smart Contracts das Vertrauen auf die Mathematik, was jene Fehler reduzieren soll, die auf böswillige oder fahrlässige menschliche Verwaltung zurückzuführen sind.
2.) Automatische Implementierung neuer Daten und sichere Speicherung historischer Daten.
3.) Die Transparenz und Überprüfbarkeit von Smart Contracts erhöht auch die persönliche Verantwortung der Menschen, die den Smart Contract verwalten, da jede Transaktion zusammen mit dem Vertrag und dem Konto, das die Transaktion ausgelöst hat, erfasst wird.
4.) Durch die Verwendung eines Smart Contract verpflichten sich die Parteien auf die Regeln des zugrundeliegenden Codes. Theoretisch sollte dies das Potenzial für Streitigkeiten und Schiedsgerichtskosten verringern, da sich beide Parteien vorab auf das im Smart Contract programmierte Ergebnis einigen.

Zu den Nachteilen gehören:

1.) Die Rechtmäßigkeit von Smart Contracts ist fraglich. Da die Struktur digital ist, kann sie die staatlichen Genehmigungsanforderungen umgehen. Staatliche Gerichte müssen die Rechte der Anleger nicht anerkennen.
2.) Smart Contracts sind nicht sehr flexibel. Sobald ein Smart Contract auf einer öffentlichen Blockchain ausgeführt wurde, ist der Vertrag anfällig für Hacker. Fehlerbehebungen und Änderungen der Vertragsbedingungen sind schwierig bis unmöglich.

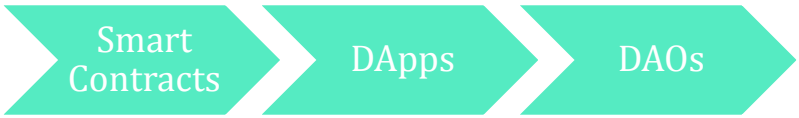
Smart Contracts, Decentralized Applications, und Decentralized Autonomous Organizations

Mit dem Aufkommen von Kryptowährungen und Blockchains werden Smart Contracts, Dezentrale Anwendungen (DApps) und Dezentrale Autonome Organisationen (DAOs) zu immer wichtigeren Technologien, die Investoren verstehen sollten. Das alles begann, als Nick Szabo 1994 den Begriff "Smart Contract" prägte. Ein **Smart Contract ist eine Software, die ein Regelwerk darstellt, das unter bestimmten Umständen automatisch ausgeführt wird. Mit anderen Worten: ein Smart Contract ist eine "wenn-dann"-Anweisung, die in einem verteilten Peer-to-Peer-Netzwerk ausgeführt wird**.

Da jeder Vertrag auf mehreren Computern auf der ganzen Welt gespeichert ist, haben Smart Contracts keinen zentralen Point-of-Failure. Ähnlich wie bei BitTorrent bedeutet das Fehlen eines einzelnen Point-of-Failure, dass beim Ausfall eines Computers das gesamte Netzwerk nicht ausfällt. Niemand hat die Macht, den Smart Contract zu ändern – auch nicht die Person, die den Smart Contract abgeschlossen hat. Das gilt auch für Hacker und Regierungen!

Smart Contracts haben die gleichen Privilegien wie Kryptowährung-Wallets, außer dass sie nicht von privaten Schlüsseln oder Benutzern gesteuert werden. Stattdessen wird ein Smart Contract durch den im Smart Contract enthaltenen Code gesteuert. Dieser kann Kryptowährungen senden und empfangen, einen Saldo speichern oder einen Saldo von Null haben. Er kann mit anderen Smart Contracts interagieren, aber die Nutzer

müssen eine kleine Gebühr für diese Interaktion an das Blockchain-Netzwerk zahlen, da jede Änderung von jedem Computer, der an das Netzwerk angeschlossen ist, genehmigt und aufgezeichnet werden muss. Das ähnelt dem Mining-Prinzip bei Bitcoin.



Eine DApp ist eine Sammlung vieler Smart Contracts, die zusammenarbeiten, um ein Produkt für Benutzer zu bereitzustellen. Eine DApp muss vier Kriterien erfüllen. Erstens muss die Anwendung Open-Source sein, was bedeutet, dass jeder sie herunterladen und sich den zugrundeliegenden Code ansehen kann. Zweitens muss die Anwendung auf einer Blockchain- oder Ledger-Technologie, wie beispielsweise einem gerichteten azyklischen Graphen, basiert sein. Drittens muss der Anwendung ein Token zugeordnet sein. Dieser Token kann aus der Anwendung heraus geboren werden wie beispielsweise Augur oder die Anwendung kann eine andere Kryptowährung wie Bitcoin oder Ethereum verwenden. Schließlich muss die Anwendung einen kryptographischen Algorithmus verwenden, um jene Änderungen an den Smart Contracts zu bestätigen, welche die DApp steuern.

Weitere Ressourcen zu Smart Contracts, DAOs und DApps

Im Jahr 2014 veröffentlichte Vitalik Buterin im Ethereum Blog einen Artikel, der beschreibt, wie Smart Contracts funktionieren und wie sie sich von DAOs unterscheiden. Außerdem wurde 2014 von David Johnston ein umfassender Leitfaden zu DApps verfasst. Schließlich erklärt ein beliebter YouTuber, Evan on Tech, den Unterschied zwischen Smart Contracts und dezentralen Anwendungen.

Anfängern steht ein kostenloser Kurs online zur Verfügung, der eine Einführung in die Programmierung von Smart Contracts bietet. Der Kurs umfasst acht Einheiten auf Grundlage der intelligenten Programmiersprache Solidity von Ethereum.

Ein DAO ist eine Art von DApp, die es Eigentümern ermöglicht, Geschäftsentscheidungen durch elektronische Abstimmung zu treffen und das Management durch Smart Contracts zu automatisieren. DAOs nutzen Smart Contracts, um die digitale Abstimmung zu erleichtern und die Abstimmungsergebnisse zu verifizieren. **Ziel eines DAO ist es, den Verwaltungsaufwand zu reduzieren und Vorschriften, die speziell für geografische Regionen gelten, zu umgehen.**

Wesentlich ist, dass ein DAO eine Unternehmensstruktur für eine weltweit verteilte Eigentümergruppe ist. Die Kryptographie und Blockchain ermöglicht es einer Gruppe von Fremden, gemeinsam Kapital zu investieren und finanzielle Entscheidungen zu treffen. Smart Contracts ermöglichen es, das Unternehmen autonom zu führen, da sie die Regeln des Unternehmens einhalten und als Grundlage für operative Entscheidungen anstelle eines Menschen dienen. So könnte beispielsweise ein Smart Contract programmiert werden, um Dividenden an Investoren auszuschütten, sobald eine bestimmte Bedingung wie ein Gewinn über einem bestimmten Schwellenwert erfüllt ist, könnte der Smart Contract automatisch die Dividende an die Wallets der Aktieninhaber senden.

Smart Contract Theory in der Praxis

"There is a lot of intermediaries that end up charging 20–30%, if the concept of decentralization takes off and does well, those fees are going to decline to almost zero."

Vitalik Buterin

Die beliebteste Kryptowährung, die Smart Contracts enthält, ist Ethereum. Der Gründer von Ethereum, Vitalik Buterin, schlug Ethereum 2013 als Blockchain vor, die speziell für Smart Contracts entwickelt wurde. Ethereum ist ein weltweites Netzwerk von Computern, das Smart Contracts ausführt, durchsetzt und validiert. Wie bereits in der letzten Edition des Crypto Research Report beschrieben, wird die Validierung durch ein dezentrales Netzwerk von Tausenden von Ethereum-Knoten auf der ganzen Welt erreicht. Die zentrale Natur des Netzwerks ermöglicht es dezentralen Anwendungen (DApps), ohne Ausfallzeiten, Zensur oder Eingriffe Dritter zu laufen, was die Anwendungen unveränderlich oder manipulationssicher macht.

In der Praxis kann Ethereum verwendet werden, um eine dezentrale Crowdfunding-Website ohne Vermittler wie Kickstarter zu erstellen. Ethereum- Nutzer können in eine Geschäftsidee investieren, indem sie ihr Geld an die Ethereum-Wallet-Adresse eines Smart Contracts senden. Wenn der Unternehmer nicht in der Lage ist, innerhalb eines bestimmten Zeitraums eine bestimmte Summe an Finanzmitteln aufzubringen, kann der Smart Contract allen Investoren automatisch ihr Geld zurückschicken. Anstatt 10% an Kickstarter zu zahlen, müssen sie nur eine 5-Cent-Gebühr an das Ethereum-Netzwerk entrichten, um die Transaktion mit dem Smart Contract abzuwickeln. Wenn das Unternehmen 10 Millionen USD mit Ethereum anstelle von Kickstarter sammelt, spart es 1 Million USD an Gebühren.

Tabelle 1: Korrelation der Renditen von Utility Token und Payment Token

Korrelations Matrix

	BTC	ETH	XRP	NEM	ETC	LTC	DASH	STRAT	XMR	WAVES	UP	PP
Bitcoin	1											
Ethereum	0.61	1										
XRP	0.36	0.52	1									
NEM	0.34	0.48	0.44	1								
Ethereum Classic	0.52	0.68	0.45	0.44	1							
Litecoin	0.59	0.66	0.42	0.48	0.62	1						
Dash	0.50	0.6	0.38	0.38	0.48	0.52	1					
Stratis	0.55	0.61	0.4	0.44	0.57	0.5	0.49	1				
Monero	0.58	0.62	0.47	0.39	0.57	0.55	0.66	0.57	1			
Waves	0.62	0.66	0.43	0.44	0.52	0.58	0.52	0.71	0.57	1		
Utility Porfolio	0.64	0.82	0.55	0.75	0.78	0.69	0.6	0.83	0.66	0.82	1	
Payment Portfolio	0.74	0.77	0.72	0.53	0.78	0.79	0.79	0.64	0.84	0.69	0.81	1

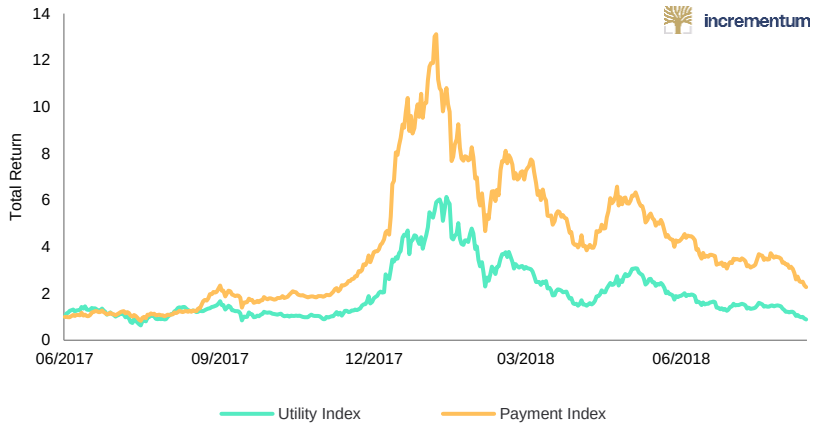
Quelle: Coinmarketcap.com, Incrementum AG

Der dezentrale Charakter von Ethereum ermöglicht es Investoren auch, Vorschriften zu umgehen, die die Investitionsbereitschaft von Investoren in Crowdfunding-Projekte einschränken. So dürfen beispielsweise in den USA nicht akkreditierte Anleger mit einem Jahreseinkommen oder einem Nettovermögen von weniger als 107.000 USD maximal 5% ihres Vermögens investieren. Diejenigen mit einem Jahreseinkommen oder einem Nettovermögen von mehr als 107.000 USD dürfen höchstens 10% des niedrigeren der beiden Beträge investieren. Diese Regeln gelten jedoch nicht für Ethereum und andere Smart Contract-Platformen wie NEO und EOS.

Blockchains, die Smart Contracts ermöglichen, werden oft als Utility-Blockchains bezeichnet, und die damit verbundenen Vermögenswerte werden als Utility-

Cryptoassets oder Utility-Token bezeichnet. Tabelle 1 vergleicht die relative Rendite von Utility-Tokens und Payment-Tokens wie Bitcoin, Monero und Litecoin. Obwohl ein Portfolio, das vollständig aus Payment-Tokens besteht, eine höhere kumulative Rendite von 227% aufweist, besitzen die Portfolios einen starken Korrelationskoeffizienten von 0,81. Kryptoinvestoren, die im Juni die fünf größten Payment-Tokens gekauft und im Januar verkauft haben, erzielten einen Halbjahresgewinn von über 1.200%. Leichtes Geld in Retrospektive!

Grafik 5: Historische Performance von Utility vs. Payment Tokens



Quelle: Incrementum AG

"(A DAO) ...is an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do."

Vitalik Buterin

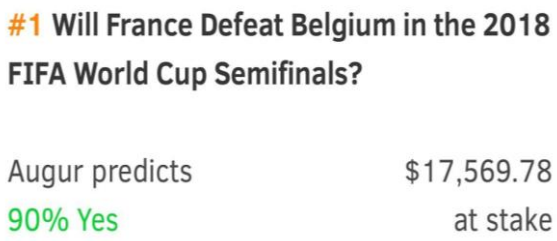
Krypto Firmen die Smart Contracts, DApps, und DAOs verwenden

Es gibt bereits viele Projekte, die darauf abzielen, Smart Contracts über Blockchains in der Praxis umzusetzen. Ethereum ist eines der prominentesten Beispiele, aber auch eine Vielzahl anderer Unternehmen nutzen die Vorteile automatischer digitaler Verträge wie Cosmos, Dfinity, Etherisc, Polkadot und ShareRing.

Tabelle 2: Nennenswerte Tokens die Smart Contracts, dApps, und DAOs verwenden

Token	Vorteile
Cosmos	Blockchain-Interoperabilität mit einem Netzwerk von unabhängigen parallelen Blockchains. Von den Schöpfern von Tendermint, Niedrigenergie-Konsensmechanismus klassische byzantinische Fehlertoleranz. Polychain Capital investierte in Cosmos.
Dash	Obwohl Dash nicht oft als Smart Contract-Plattform angesehen wird, ist Dash eine Art DAO, da die Governance von den Masternodes kontrolliert wird, die es den Benutzern ermöglicht, über Vorschläge abzustimmen.
Dfinity	Das Team aus Informatikern, Mathematikern und Ökonomen, gegründet in Zug mit Sitz in Palo Alto, will Technologievermittler wie Uber, eBay und Facebook enthronen.
Ethereum	Großes Netzwerk von Anwendern und Entwicklern, größtes Versorgungs-Kryptoasset nach Marktkapitalisierung.
Etherisc	Dezentrale Versicherung, einer der führenden Anbieter von Blockchain-basierten Versicherungsprodukten.
EOS	Skalierbare, flexible, nutzbare Infrastruktur für dezentrale Anwendungen.
Polkadot	Parity Technologies als Lead Developer, verbesserte Anonymität und Skalierbarkeit.
ShareRing	P2P Carsharing, Teil der MOBI-Initiative, australisches Entwicklerteam.
Starcards.my	Ähnlich wie Cryptokitties ermöglicht Starcards Ethereum-Benutzern das Sammeln und Tauschen von seltenen digitalen Celebrity-Karten, die auf der Blockchain gespeichert sind.

Quelle: Incrementum AG



Der Preis für diese Wette lag bei 0,9 $ pro Aktie, "Frankreich wird gewinnen", aber sobald das Ergebnis der Veranstaltung bekannt gegeben wurde, war jede Aktie 1 $ wert, die Anleger erzielten einen sicheren Gewinn von 0,1/0,9 = 11,1%.

Ein umstrittenes Beispiel ist der dezentrale Prognosemarkt Augur. Ende Juli berichtete CNN über Augur-Nutzer, die darauf wetteten, ob Präsident Trump bis Ende dieses Jahres ermordet werden würde. Da Augur eine DApp ist, kann niemand die Nutzer davon abhalten, auf kriminelles und unethisches Verhalten zu wetten. Sobald sich eine Gegenpartei finden lässt, entsteht ein Markt. Selbst die Schöpfer von Augur können solche Wetten nicht verhindern, da es sich um ein Open-Source-Projekt handelt. Nicht nur die Rechtmäßigkeit der Prognosemärkte ist fragwürdig, auch das Leben von Menschen könnte direkt an finanzielle Gewinne gebunden sein. Sollte dieser Prognosemarkt zu unethischen Handlungen führen, wird der Preis des Augur Tokens höchstwahrscheinlich in Mitleidenschaft gezogen werden.

Das Risiko von Orakeln

Smart Contracts versprechen, Verträge automatisch durchzusetzen und Intermediäre zu ersetzen. Allerdings verlassen sich viele Anwendungen von Smart Contracts auf so genannte "Orakel", um ihnen Informationen über die reale Welt zur Verfügung zu stellen. Orakel beliefern Smart Contracts mit Daten über die Welt wie Daten zum Wetter, Wechselkurse und Wahlergebnisse. Smart Contracts führen Finanztransaktionen automatisch auf der Grundlage der Daten des Orakels durch. Orakel können jedoch gefährdet sein, da sie nicht dezentralisiert sind. Ein Orakel kann als Gegenparteirisiko angesehen werden, was zu unwiderruflichen Geldverlusten führen kann.

Es wurden mehrere Lösungen vorgeschlagen. Vor allem Augurs Forschung zu Orakeln ist richtungsweisend. Das Modell ermöglicht es Augur-Anwendern, über die Wahrheit abzustimmen und die Ergebnisse der Abstimmung zu diskutieren.

Dennoch geht die Suche nach einem sicheren Orakel weiter, und die zukünftige Adoption von Smart Contracts auf öffentlichen dezentralisierten Blockchains hängt davon ab.

Obwohl Augur es Anwendern ermöglicht, beispielsweise über die Wahrscheinlichkeit abzustimmen, ob Donald Trump oder Warren Buffett dieses Jahr überleben werden, sind die meisten Prognosen von Augur im Sport angesiedelt. So konnten die Nutzer beispielsweise während der Fußball-Weltmeisterschaft über das Ergebnis bestimmter Spiele abstimmen und Ethereum verdienen.

When Smart Contracts Are Dumb

Seit 2011 wurden Kryptotokens im Wert von insgesamt 2,4 Milliarden USD durch Angriffe zerstört, eingefroren, gestohlen oder anderweitig kompromitiert. Die zwei an Marktkapitalisierung gemessen grössten Kryptowährungen haben in den letzten sieben Jahren Verluste von rund 1,7 Millionen BTC und 4,54 Millionen ETH erlitten. Auf der Ethereum Platform sind die drei prominentesten Hacks der Vergangenheit: der DAO-Hack, der Parity WalletHack und der Parity Wallet-Suicide Hack.

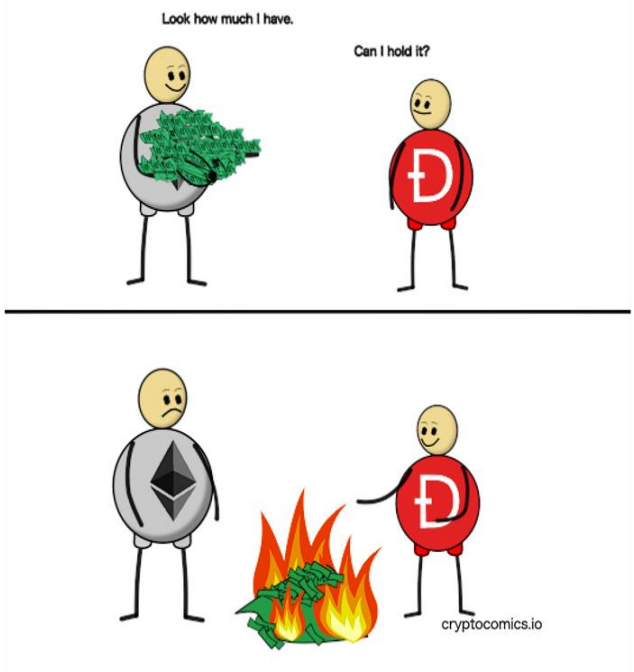
DAO Hack

Die Decentralized Autonomous Organization (DAO) war ein lang herbeigesehntes Krypto-Projekt und sollte ein Musterstück der revolutionären Kraft von Smart Contracts sein. Einige der Ur-Entwickler von Ethereum lösten sich von dem Team um ein Unternehmen namens Slock.it zu gründen und bauten im April 2016 das erste DAO auf der Ethereum Blockchain.[25] **Die DAO-Anwendung funktionierte wie ein Investmentfonds, allerdings ohne die sonst dazu nötige Fondsverwaltung.** Anleger konnten sich an dem Fonds beteiligen, indem sie die Währung der Ethereum Platform, Ether, in den Fonds einzahlten, was ihnen wiederum Stimmrechte einräumte. Die Investitionsentscheidungen sollten

—
[25] See " Jentzsch, C. (2016). Decentralized Autonomous Organization to Automate Governance. Final Draft – Under Review [white paper]. Retrieved fromDecentralized Autonomous Organization to Automate Governance. Final Draft – Under Review https://www.scribd.com/document/317501611/White-Paper" [white paper], Christoph Jentzsch, 2016.

zusammen im Rahmen einer Abstimmung getroffen werden. Jeder der eine Geschäftsidee hatte, konnte diese der DAO-Community präsentieren und eventuell Kapital aus einem Pool von Ether erhalten, der von der DAO.[26] kontrolliert wurde. Nachdem sich die Community für ein Investitionsprojekt entschieden hat und das Projekt sich als profitabel herausstellt, sollten die Inhaber der Token Rendite auf diese erhalten -ähnlich wie Dividenden oder Zinszahlungen.

Die DAO wurde im Mai 2016 als Smart Contract auf der Ethereum Platform ins Leben gerufen. Damals brachte das Projekt Ether im Wert von 162 Millionen US-Dollar auf und kürte sich damit bis dato zum größten Crowdfunding aller Zeiten. Dennoch infiltrierte ein Hacker am 17. Juni 2016 das DAO-Netzwerk, indem er sich einer Software Lücke verhalf, die ihm den Abzug von ETH Tokens aus dem Pool des DAO-Netzwerks ermöglichte. In den ersten Stunden des Angriffs wurden 3,6 Millionen ETH-Token gestohlen, was damals einem Gegenwert von 70 Millionen Dollar entsprach (heute 1,2 Milliarden Dollar). Eigenartigerweise beendete der Hacker bald seinen Angriff obwohl er das DAO Netzwerk noch problemlos weiter auspressen hätte können.



Die DAO ist bis heute der größte Crowdfund in der Geschichte mit über 162 Millionen Dollar. Weniger als einen Monat nach dem Start wurde die DAO von 50 Millionen Dollar durch einen Hack erleichtert.

Das Team und die Community hinter Ethereum waren sehr bald von dem Angriff alarmiert und reagierten schnell indem sie mehrere Vorschläge zur Abwehr vorlegten. Aufgrund der Architektur der DAO wurden die gestohlenen Token in Form von Ether zunächst in einem so genannten „child“ DAO festgehalte. Dieser „child“ DAO war ein weiterer Smart Contract, der eine 28-tägige Aufbewahrungsfrist vorschrieb, bevor der Angreifer das Geld vollständig abheben und in Umlauf bringen konnte. Dieser Sicherheitsmechanismus verschaffte dem Ethereum-Team genügend Zeit, um über die nächsten Schritte zu entscheiden.

Vitalik Buterin, der Vater von Ethereum, war sich über den Ernst der Lage bewusst und gab kurz darauf ein Statement heraus, in der er Anleger davon vergewisserte, dass ihre Gelder vorerst sicher aufbewahrt seien. Die Ethereum-Community entschied sich dann, jede Transaktion für ungültig zu erklären, die vom Konto des Angreifers mit dem Hash Code

0x7278d050619a624f84f51987149ddb439cdaadfba5966f7cfaea7ad44340a4ba

stammten und verhinderten so, dass der Angreifer auch nach Ablauf der 28-tägigen Haltedauer Geld abhebt.

Der Hacker veröffentlichte später einen offenen Brief an die Ethereum-Community, indem er das rechtmäßige Eigentum an den erworbenen Geldern beanspruchte. Das Originalschreiben ist hier zu finden. Eine Entschädigung der

—
[26] See “The Story of the DAO–Its History and Consequences,” Samuel Falkon, *The Startup,* December 24, 2017. https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

Investoren wäre nach den einprogrammierten Regeln des Ethereum-Netzwerks zu diesem Zeitpunkt nicht möglich gewesen und stellte somit eine existenzielle Bedrohung für das gesamte Netzwerk dar.

"Just goes to show that any centralized entity will be pushed in that direction, which is why lightning network, atomic swaps and Decentralized Exchanges are the only way to resist surveillance economics."

Andreas M. Antonopoulos

Die Lösung, welche die Ethereum Stiftung nun im Endeffekt vorschlug war zu der Zeit höchst umstritten[27]. Sie entschieden sich dazu einen "Hard Fork" zu implementieren, indem sie eine neue Version der Ethereum-Software veröffentlichten, die die gehackten Transaktionen nicht enthielt. Dies muss man sich als eine Rückversetzung in einen früheren Stand der Blockchain vorstellen, in dem der Angriff noch nicht vollzogen wurde und die Software Lücke beseitigt ist. Nicht alle Mitglieder des Netzwerks stimmten mit der Entscheidung überein, die Blockchain mit roher Gewalt aufzuspalten. Einige Kritiker verließen Ethereum vollständig, andere nutzten einfach weiterhin die ursprüngliche Ethereum-Blockchain, auf der auch die Hacker-Transaktion aufgezeichnet war. Diese ursprüngliche Blockchain wurde dann unter dem Namen 'Ethereum Classic' mit dem Ticker ETC weitergeführt.

Wie bei all den in diesem Artikel beschriebenen Missgeschicken ist keines davon aufgrund der grundlegenden Auslegung der Ethereum-Plattform entstanden. Stattdessen traten die Hacks aufgrund von Problemen in der Gestaltung von Anwendungen auf, die auf der Ethereum-Plattform gebaut wurden. Die Art des Angriffs, der die DAO zu Fall brachte wird als Wiedereintrittsangriff[28] bezeichnet. Bei diesem Angriff sendete der Angreifer zunächst Ether an den Smart Contract (DAO) und konnte dann wiederholt nach Ether "fragen" (ähnlich wie Wechselgeld), noch bevor der Smart Contract sein Guthaben aktualisieren konnte. Wenn ein Smart Contract sein Guthaben (das Guthaben eines Benutzers) vor dem Senden von Tokens nicht aktualisiert, kann der Angreifer die Abhebungsfunktion kontinuierlich aufrufen, und den Smart Contract somit leerräumen[29]. Das für die DAO geschriebene Programm hatte mehrere Fehler, darunter den rekursiven Aufruf-Fehler sowie die Tatsache, dass die Smart Contracts ETH-Gelder geschickt haben, bevor sie das interne Token-Guthaben aktualisiert haben.

Tabelle 3: Berüchtigte Hacks in der Smart Contract Welt

Berüchtigte Hacks		
	Jahr	Menge USD
Fehlkonfigurierte Ethereum Clients	2018	20,000,000
MyEtherWallet DNS hack	2018	152,000
Parity Wallet Suicides	2017	160,000,000
Parity Wallet Hack	2017	30,000,000
Veritaseum's Ether wallet	2017	8,400,000
DAO Hack	2016	60,000,000
Shapeshift	2016	230,000
King of the Ether Throne	2015	2,000

Quelle: Incrementum AG

—
[27] Vgl. "To fork or not to fork," Jeffrey Wilcke, *Etherum Blog*, July 15, 2016. https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork/
[28] Vgl. "Smart Contract Attacks [Part 1] – 3 Attacks We Should All Learn From The DAO," Pete Humiston, *Hackernoon*, July 5, 2018.
[29] Finden Sie eine detaillierte Beschreibung hier

Parity Wallet Hack

Parity Technologies ist ein Software Hersteller von Anwendungen und versorgt einen großen Teil der Infrastruktur des öffentlichen Ethereum-Netzwerks[30]. Am 19. Juli 2017 griff ein unbekannter Hacker eine kritische Schwachstelle des auf dem Ethereum-Netzwerk laufenden Parity Multi-Signature Wallet an und plünderte in wenigen Minuten drei massive Wallets mit einem Gesamtwert von 31 Millionen Dollar[31]. Eine Gruppe heldenhafter White-Hat Hacker aus der Ethereum-Community reagierte unverzüglich darauf, indem sie Ethereum-Nutzer kurz darauf über Social Media alarmierten und tastächlich die übrigen fehlerhaften Wallets hackten, bevor sie in die Finger des Angreifers gelangten. Diese Form des Hackens wird als White Hat Hacking bezeichnet, weil sie für den guten Zweck gehackt wurden. Hätten die sogenannten White-Hat Hacker nicht so schnell reagiert, hätte der Hacker Ethereum im Wert von über 180.000.000.000 Dollar aus fehlerhaften Wallets hacken können. Natürlich wurden die Token, die von den White-Hats „gestohlen“ wurden, am Ende sicher an die rechtmäßigen Inhaber verteilt.

Der Hacker fand einen Programmierfehler im Code, der es ihm ermöglichte die Parity Multisignature Wallet neu zu initialisieren, fast so wie wenn man ein iPhone auf seine Werkseinstellungen zurücksetzen würde. Nachdem er das getan hatte, konnte er sich als neuer Besitzer konfigurieren und über die Token frei verfügen.

“Bitcoin is not unregulated. It is regulated by algorithm instead of being regulated by government bureaucracies. Un-Corrupted.”

Andreas M. Antonopoulos

Aufgrund der Architektur von Ethereum besteht für Programmierer ein Anreiz, Code so auszulegen, dass Transaktionskosten minimiert werden. Immer wenn ein gewisses Programm, ein Smart Contract, auf Ethereum ausgeführt wird und somit eine Transaktion im Netzwerk darstellt, ist dies mit einer Transaktionsgebühr verbunden. Eine effiziente Art, die Kosten für Transaktionen zu senken, besteht darin, offene Bibliotheken von Programmen zu verwenden, die bereits im Netzwerk veröffentlicht wurden.

Die Standardeinstellungen für die Multisignatur-Wallets von Parity hatten eine Konfiguration, die genau das tat. Diese verwies auf eine gemeinsam genutzte externe Bibliothek, die eine Wallet-Initialisierungslogik enthielt, nämlich initWallet(). Sobald diese aufgerufen, wurde, war man im Stande den Smart Contract, dem das Wallet zugrunde Lag war, neu zu initialisieren. Jeder der diesen Fehler ausnutzte, konnte somit zum neuen Inhaber des Wallets werden. Dies einmal geschafft konnte ein Hacker das Geld einfach an jede Adresse seiner Wahl überweisen.

—

[30] Erfahren Sie mehr über Parity hier. https://parity.io

[31] Vgl. “A hacker stole $31M of Ether – how it happened and what it means for Ethereum,” Haseeb Qureshi, *Medium*, July 20, 2017. https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce

Das neue Ethereum Logo?

Aber warum hat Ethereum diesen Hack nicht einfach rückgängig gemacht, wie sie es beim DAO-Hack getan hatten? Leider war diese äußerste Lösung nicht einmal mehr eine Option. Als der Angreifer damals das Guthaben der DAO in einen child DAO übertrug, wurden die gehackten Token für einen Zeitraum von 28 Tagen eingefroren, bevor sie an den Angreifer freigegeben werden konnten. Dies verhinderte, dass das gestohlene Geld in Umlauf kam. Andererseits gab es der Ethereum-Community genügend Zeit, sich untereinander abzusprechen wie sie mit dem Angriff umgehen sollen. Im Parity Wallet Angriff zog der Angreifer das Geld jedoch direkt ab und konnte sofort darüber voll verfügen. Einmal im Umlauf, war es fast unmöglich, die ETH Token zurück zu gewinnen, ähnlich wie bei einer riesigen Summe an Falschgeld, das in den Wirtschaftskreislauf gelangt.

Parity Wallet Selbstmorde

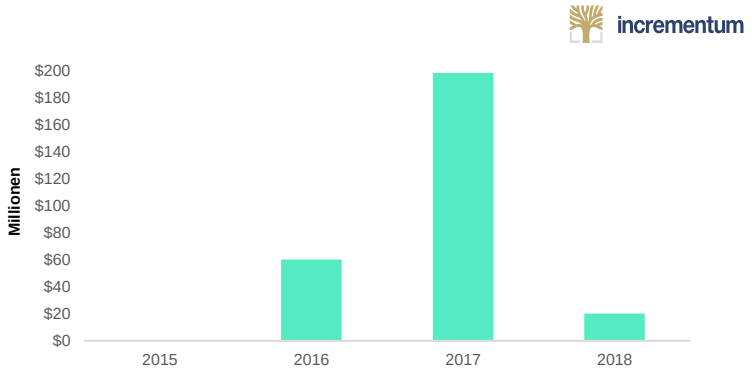
Am 6. November 2017 fiel die Parity Multisignature Wallet einem weiteren Angriff[32], zum Opfer, diesmal allerdings in einem viel gravierenden Ausmaß. Ein Github-Nutzer namens 'devops199' schrieb einen Beitrag mit dem Titel **“anyone can kill your contract”.** Devops199's Beitrag schien gute Absichten zu haben[33]. Er wollte das Parity-Team auf einen Fehler in jenem Smart Contract aufmerksam machen, auf dem die Multisignature Wallets gebaut waren. Die Sicherheitslücke ließ zu, dass jeder Hacker, sich selbst zum "Eigentümer" dieses Smart Contracts ernennen konnte und so die Erlaubnis zukam, mit der Wallet nach freiem Belieben zu verfügen. Bis zum heutigen Zeitpunkt ist noch unklar, was die ursprüngliche Absicht war, aber der folgenden Tat von devops199 wurde weitgehend Unverständnis entgegengebracht: Er löste „versehentlich" den Kill-Switch des Smart Contracts aus, wodurch alle Parity Multisig Wallets nicht mehr zugänglich waren. Nur wenige Minuten nachdem die Bibliothek ausgelöscht wurde, hängte devops199 einen Folgepost an seinen Beitrag **“anyone can kill your contract”** auf Parity's Github mit dem Titel **“I accidentally killed it”**an.

—

[32] Vgl. “Security Alert,” *Parity*, November 8, 2017.https://paritytech.io/blog/security-alert.html

[33] Vgl. “Yes, this kid really just deleted $300 MILLION by messing around with Ethereum’s smart contracts,” Thijs Maas, *Hackernoon*, November 8, 2017. https://hackernoon.com/yes-this-kid-really-just-deleted-150-million-dollar-by-messing-around-with-ethereums-smart-2d6bb6750bb9

Grafik 6 Jährliche Verluste durch Ethereum Smart Contracts



Quelle: Incrementum AG

Das Ausmaß dieses Parity-Hacks errodierte insgesamt 514,000 Ethereum-Token, die damals an die 155 Millionen Dollar oder 1% der Gesamtbewertung von Ethereum ausmachten. Als Folge des Hacks kann aus allen Parity Multisig-Wallets, die nach dem 20. Juli 2017 aufgesetzt wurden, kein Geld ausgezahlt werden.

Ein erneuter „hard-fork" könnte die eingefrorenen Multisig Wallets technisch retten, aber dies würde der Grundauslegung von Ethereum als eine dezentrale, verteilter, *unveränderliche* und manipulationssichere Platform im krassesten Gegensatz stehen. Die Forderungen nach einem hard-fork sind darum weitgehend unwirksam geblieben.

Smart Contracts stellen für Investoren ein deutlich anderes Exposure dar als Bitcoin

"Bear markets are for builders. The calm, the quiet, the disillusionment… while the fickle and fair-weather peer around with nervous insecurity, the builders become the market's foundation, preparing the mortar and stone of tomorrow's towers."

Erik Voorhees

Smart Contracts haben das Potenzial ganze Branchen auf den Kopf zu stellen, indem sie den Mittelsmann umgehen und Vertragsparteien direkt zusammenbringen, ohne das ein Vertrauensverhältnis zwischen diesen herrschen muss. Sie können Vertrauen schaffen und Transaktionskosten senken. Trotz der Vorteile kritisiert *The Economist* das Konzept der Smart Contracts, indem er auf den unreifen Zustand derer hinweist.[34] Sie argumentieren weiter, dass Smart Contracts nicht flexibel genug für eine Wirtschaft sind, die auf ständig wechselnde Bedingungen reagieren muss.

Bei Incrementum sind wir der Meinung, dass Smart Contracts eine zukunftsträchtige Technologie sind. Aus finanzieller Sicht bieten Utility Blockchains wie Ethereum, NEO oder EOS ein deutlich anderes Risiko-Rendite-Profil als Payment Blockchains wie Bitcoin, Dash oder Monero. Aufgrund der Komplexität von Smart Contracts sind Utility Blockchains von Natur aus anfälliger für Technologierisiken. Da deren Token das derzeitige Währungssystem nicht zu stören drohen, ist das Wettbewerbsrisiko mit souveränen Währungen im Vergleich zu öffentlichen Payment Blockchains geringer. Viele Aufsichtsbehörden sagen jedoch, dass ICOs und Utility Tokens gegen die Finanzmarktregulierung verstoßen.

—

[34] Vgl. "Not-so-clever contracts," Schumpeter, *The Economist*, July 28, 2016. Schumpeter. (2016, July 28). Not-so-clever contracts. *The Economist*. Retrieved from http://www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted

Fällt Ihnen etwas auf?

"Dieses **'Telefon'** hat zu viele Schwächen, als dass man es ernsthaft für die Kommunikation in Erwägung ziehen kann."

WILLIAM ORTON, WESTERN UNION PRÄSIDENT, 1876

"Es gibt keinen Grund, warum irgendjemand einen **Computer** in seinem Haus haben wollen würde."

KEN OLSON, DIGITAL EQUIPMENT CORPORATION, 1977

"**Das Internet** wird wie eine spektakuläre Supernova im Jahr 1996 in einem katastrophalen Kollaps untergehen."

ROBERT METCALFE, ETHERNET ERFINDER, 1995

"**Bitcoin** ist was für Spekulanten, aber keine Währung."

EWALD NOWOTNY, GOUVERNEUR DER OeNB, 2017

Weitblick **zahlt sich aus.**

bitpanda

Home of **Cryptocurrency**

Liechtensteins Blockchain Strategie: Regierungschef Hasler im Interview

“Mit dem ‚Token‘ führen wir ein neues Konstrukt ein, um die Transformation der „realen“ Welt auf die Blockchain-Systeme rechtssicher zu ermöglichen.”

Liechtenstein‘s Regierungschef Adrian Hasler

Key Takeaways

- **Liechtenstein’s Regierung hat aktiv eine blockchainfreundliche Strategie eingeschlagen.**
- **Das Blockchaingesetz tritt voraussichtlich im Sommer 2019 in Kraft**
- **Die Liechtensteiner Finanzmarktbehörde hat zuletzt massiv Know-how und Ressourcen aufgebaut, um aufsichtsrechtliche Rahmenbedingungen rund um die „Tokenized Economy“ zu schaffen.**

Seit zwei Jahren arbeitet die liechtensteinische Regierung an dem neuen Blockchaingesetz. Das Gesetz signalisiert Unternehmern, dass Liechtenstein ein idealer Standort für den Krypto-Sektor sein will. Federführend für das Projekt steht niemand geringerer als Regierungschef Adrian Hasler. Die Gesetzesinitiative ist Teil einer umfangreichen Strategie zur "Digitalisierung Liechtensteins" durch Verbesserung aller staatlichen Dienstleistungen und Förderung der Innovation im Land.

Mark Valek: Vielen herzlichen Dank Regierungschef Hasler und Dr. Dünser, dass Sie sich die Zeit nehmen und uns exklusiv für den *„Crypto Research Report“* ein Interview geben. Unsere erste Frage: Der Standort Liechtenstein zeichnet sich zunehmend durch seine blockchainfreundliche Politik aus. Dies hat sich bis jetzt an den vielen hier angesiedelten ICOs, an dem Engagement der Universität Liechtenstein aber auch an einigen regulierten Crypto Fonds und nun schließlich auch an der anstehenden Verabschiedung des Blockchaingesetzes[35] merklich gemacht. Welche langfristige Vision verfolgen Sie mit dieser blockchainaffinen Strategie im Zusammenhang mit dem Fürstentum?

Incrementum Partner Mark Valek mit Liechtenstein's Ministerpräsident Adrian Hasler. Photo: Andres Coronado.

Regierungschef Hasler: *Grundsätzlich geht es bei diesen ganzen Maßnahmen, die wir setzen, um den Erhalt und die Schaffung von neuen Arbeitsplätzen und damit um den Erhalt der Lebensqualität in Liechtenstein für die Zukunft. Dies ist die Hauptstossrichtung, die wir verfolgen. Die Blockchain-Technologie hat aus unserer Sicht das Potenzial, eine wichtige Basis für digitale Wirtschaftsprozesse und auch Finanzdienstleistungen zu werden. Dieses Potenzial geht weit über das hinaus, was wir heute beobachten können und bietet auch für den Kleinstaat Liechtenstein entsprechende Chancen. Wir haben uns bereits in der letzten Legislatur intensiv mit dem Thema Innovation in der Finanzbranche beschäftigt und mit „Impuls Liechtenstein“ verschiedene Initiativen entwickelt. Das Blockchaingesetz ist ein weiterer Meilenstein und passt natürlich hervorragend in diese Strategie. Dabei ist uns wichtig, dass wir stets offen sind für Neues, dass wir Chancen frühzeitig erkennen und diese Chancen auch nutzen. Ebenso wichtig ist, dass wir Rechtssicherheit schaffen, nicht nur im traditionellen Finanzbereich, sondern gerade auch bei diesen neuen Technologien.*

Mark Valek: Vergangenen Juni wurde an der Universität Liechtenstein unter großem Interesse das Blockchaingesetz erstmals vorgestellt. Dies ist weltweit eine der ersten umfänglichen Legislativen, welche einen erweiterten rechtlichen Rahmen für Anwendungsfälle der neuen Blockchaintechnologie formuliert. Welches sind die wesentlichen Eckpfeiler dieses Gesetzes?

Regierungschef Hasler: *Uns geht es darum, dass wir mit diesem Gesetz die grundlegenden Fragen klären, die für die Rechtssicherheit in der Token-Ökonomie wichtig sind. Wir haben in anderen Staaten gesehen, dass dort vielfach ganz konkrete Bereiche wie zum Beispiel ICOs oder Kryptowährungen geregelt werden. Wir haben in Liechtenstein bewusst einen umfassenden Ansatz gewählt, der die ganze Bandbreite der Token-Ökonomie erfasst. Mit dem Token führen wir*

—

35 Vgl.“Vernehmungslassungsbericht Blockchain-Gesetz,” *Ministerium für Präsidiales und Finanzen*, August 29, 2018.

ein neues Konstrukt ein, um die Transformation der „realen" Welt auf die Blockchain-Systeme rechtssicher zu ermöglichen. Es geht darum, Token als Möglichkeit zu nutzen, alle Arten von Rechten auf Blockchain-Systemen zu verkörpern. Um den Kundenschutz zu verbessern, werden Mindestanforderungen an Tätigkeiten auf einem Blockchain-System definiert. Ebenso klar ist, dass die Anwendbarkeit der Geldwäschereigesetze und somit die Einhaltung der Sorgfaltspflichten elementare Teile dieses neuen Erlasses sind, den wir in Planung haben.

Mark Valek: Ist schon bekannt ab wann das Blockchain Gesetz in Kraft tritt?

Regierungschef Hasler: *Der Vernehmlassungsbericht wurde auf der Homepage der Regierung publiziert und ist dort downloadbar. Eine Version in englischer Sprache sollte in Kürze verfügbar sein. Sobald das Gesetz verabschiedet und in Kraft getreten ist, wird es auch in englischer Sprache übersetzt werden.*

Mark Valek: Und wo bzw. auch ab wann können sich interessierte Unternehmen oder Bürger über das Gesetz informieren und Folgefrage wird das Gesetz auch in englischer Sprache verfügbar sein?

Regierungschef Hasler: *Vorerst wird* ***die Vernehmlassung publiziert und diese ist auf der Homepage der Regierung downloadbar.***[36] *Diese wird jedoch nicht in englischer Sprache erhältlich sein.* ***Wenn das Gesetz dann verabschiedet ist, wird es sicher auch in englischer Sprache übersetzt werden.*** *Wir haben viele Gesetze schon auf Englisch übersetzt welche auch auf unserem Portal verfügbar sind und ich gehe davon aus, dass auch dieses Gesetz, wenn es dann verabschiedet ist und in Kraft ist auf diesem Portal auf Englisch verfügbar sein wird.*

"Bitcoin was the first engineering solution that allowed for digital payments without having to rely on a trusted third-party intermediary. By being the first digital object that is verifiably scarce, Bitcoin is the first example of digital cash"

Saifedean Ammous

Mark Valek: Welche Auswirkungen wird das Gesetz ihrer Meinung nach auf das heimische Bankenwesen haben?

Regierungschef Hasler: *Ich gehe davon aus, dass das Blockchain-Gesetz positive Auswirkungen auf unseren Finanzplatz haben wird. Das Gesetz wird es Banken und anderen Finanzintermediären erleichtern, sich mit der Blockchain zu beschäftigen. Wir stellen jetzt schon fest, dass Banken, Treuhänder und Rechtsanwälte sehr interessiert an unserem Gesetzesentwurf sind und grosses Potenzial für neue Geschäftsmodelle erkennen. Mittlerweile haben sich auch schon verschiedene Unternehmen aus dem FinTech-Bereich in Liechtenstein angesiedelt. Das strahlt nach aussen und führt dazu, dass sich weitere Unternehmen für unseren Standort interessieren. Wir stellen fest, dass in Liechtenstein ein neues Ökosystem entsteht, welches sicher noch weiter wachsen wird.*

Mark Valek: Gibt es bereits Unternehmen, die angekündigt haben vom Gesetz Gebrauch zu machen?

—

36 Vgl."Vernehmlassung zum Blockchain-Gesetz gestartet," *Regierung des Fürstentums Liechtenstein*, August 29, 2018. https://www.llv.li/files/srk/vnb-blockchain-gesetz.pdf

Regierungschef Hasler: *Wir haben in den letzten Wochen immer wieder Rückmeldungen erhalten von Unternehmen, und diese Rückmeldungen sind sehr positiv. Mit Dr. Thomas Dünser haben wir zudem einen kompetenten Ansprechpartner im Ministerium. Es steht in engem Austausch mit der Szene und spürt den Puls. Dabei zeigt sich, dass einige dieser Unternehmen darauf warten, dass das Gesetz in Kraft tritt.*

"There is a major revolution taking place that is now allowing for a better currency, one that is more secure, that is decentralized, that is more effective, more useful, it is global, it is open to everyone, it allows people sending money to their families without any big friction, it is a far better currency than fiat currency."

Tim Draper

Mark Valek: Gibt es so etwas wie einen Verband oder mit wem waren Sie da bilateral in Gesprächen oder gab es da eine zentrale Ansprechstelle?

Dr. Dünser: *Bei der Ausarbeitung des Gesetzes haben wir eine Kerngruppe mit Experten aus verschiedenen Bereichen einbezogen, die sich bereits intensiv mit der Blockchain auseinandergesetzt haben. Zudem führe ich relativ häufig Gespräche mit Unternehmern aus der Praxis, um die aktuellen Entwicklungen zu kennen und die kommenden Problemstellungen zu erkennen.*

Regierungschef Hasler: *Spannend ist in diesem Zusammenhang auch, dass es bereits Rechtsanwälte, Treuhänder und auch Banken gibt, die sich schon einige Zeit mit diesem Thema intensiv beschäftigt haben. Auch sie stehen in engem Austausch mit Dr. Thomas Dünser und können sich aktiv an der Weiterentwicklung beteiligen. Wie bereits erwähnt hat sich bereits eine Szene mit externen aber auch mit liechtensteinischen Unternehmen gebildet. Es war ein großer Vorteil, dass wir auf diese Ressourcen und das vorhandene Know-how zugreifen konnten bei der Erarbeitung des Blockchaingesetzes.*

Mark Valek: Insbesondere bei der neuartigen Crypto Technologie ist es essenziell, dass alle beteiligten Parteien innerhalb kurzer Zeit viel neues Wissen aufbauen. Mit dem „Crypto Research Report" wollen wir dazu auch einen Teil beitragen. Stehen sie hinsichtlich der Blockchain-Thematik mit Gesetzgebern in benachbarten oder in anderen Ländern im Austausch?

Regierungschef Hasler: *Wir beobachten sehr genau, was in anderen Staaten und Jurisdiktionen diskutiert wird; das ist für uns sehr interessant. Ebenso wichtig ist, was auf internationaler Ebene angedacht wird. Auch hier tauschen wir uns regelmäßig aus.*

Mark Valek: Wie schätzen Sie den Fortschritt Lichtensteins als Standort für die Blockchain-Industrie im Vergleich zu der Schweiz oder auch zu anderen internationalen Standorten ein?

Regierungschef Hasler: *Wir arbeiten schon seit einigen Jahren intensiv daran, die Rahmenbedingungen für innovative Unternehmen in Liechtenstein zu verbessern. Das Blockchaingesetz ist jetzt ein Teil dieser Arbeit. Ich denke, wir sind aktuell sehr gut positioniert, um die vorhandenen Potenziale auszunutzen. Liechtenstein bietet sicher den Vorteil, dass wir eine innovationsfreundliche Regierung haben und eine kompetente Finanzmarktaufsicht, die mit dem Regulierungslabor ein Gefäss bietet, um die Anliegen der Unternehmen frühzeitig aufzunehmen und auch beratend zur Seite zu stehen. Dieser Ansatz hat sich als sehr erfolgreich herausgestellt. Ein weiterer ganz wesentlicher Standortvorteil sind die kurzen Wege, die wir in Liechtenstein haben. Nicht zuletzt ist neben dem*

Zollvertrag mit der Schweiz auch unsere EWR-Mitgliedschaft ein großer Vorteil. Sie sichert uns den Marktzugang zu Europa.

Mark Valek: Anbei möchte ich Sie mit folgender Aussage konfrontieren: Der Vorsitzende der SEC hat in einem Statement verlautbart, dass jede ICO, welches er bis jetzt gesehen hat einer traditionellen Kapitalbeschaffung gleicht und somit im Falle der USA ihre Aufsicht unterläge. Sehen Sie dies ähnlich?

Regierungschef Hasler: *Wir haben hierzu eine differenziertere Auffassung. Es gibt ICOs, welche wertpapierähnliche Token ausgeben. Diese unterliegen der Wertpapier- und teilweise auch der Finanzmarktgesetzgebung. Es gibt aber auch Token, die z.B. ein Nutzungsrecht für Software oder einen Gutschein für einen späteren Leistungsbezug beinhalten. Diese fallen in Liechtenstein, aber auch in anderen Staaten in Europa, eben nicht unter die Wertpapier-Gesetzgebung der Finanzmarktregulierung. Man sieht hier in dieser Diskussion das grosse Spannungsfeld der Token-Ökonomie: Einerseits ist das Anwendungsfeld für den Einsatz der Token sehr breit und geht von klassischen Wertpapieren und Finanzinstrumenten bis hin zu normalen Wirtschaftstätigkeiten wie Gutscheinen, etc. Andererseits gibt es durch die Digitalisierung direkten Zugang zu sehr vielen Personen, verbunden mit Herausforderungen für den Kundenschutz. Wenn wir versuchen, dies alles in eine bestehende Schublade zu packen, dann laufen wir Gefahr, andere – ebenfalls sinnvolle – Anwendungen zu unterbinden. Deshalb haben wir in unserem Blockchaingesetz allgemeine Anforderungen an den Kundenschutz und die Missbrauchsvermeidung gestellt, die für alle Arten von Token gelten.*

Mark Valek, Dr. Thomas Dünser, und Ministerpräsident Hasler diskutieren Liechtenstein's Blockchain Gesetz

Mark Valek: Die Einstufung des Tokens unternimmt aber die Finanzmarktaufsicht (FMA)?

Regierungschef Hasler: *Ja, das ist richtig. Die Einstufung des Tokens wird durch die Finanzmarktaufsicht vorgenommen. Da Liechtenstein Mitglied des EWR ist, orientiert sich der Geltungsbereich der Finanzmarktgesetze an den europäischen Richtlinien.*

Mark Valek: Ich nehme an die Liechtensteinische Finanzmarktaufsicht wird zwangsläufig Ressourcen aufbauen, oder gibt es bereits eine spezifische Abteilung, welche speziell für die ICO-Einstufung zuständig ist?

Regierungschef Hasler: *In der FMA wurde vor einigen Jahren das Regulierungslabor gegründet. Das Regulierungslabor ist das interne Kompetenzteam der FMA für neue Finanztechnologien. Mit dem Regulierungslabor haben Fin-Techs einen klaren Ansprechpartner und erhalten*

Unterstützung im Bewilligungsprozess. Aufgrund der vielen Anfragen hat die FMA den nächsten Schritt gemacht und das Regulierungslabor weiter professionalisiert, Es wurde nun direkt bei der Geschäftsleitung angesiedelt und mit entsprechenden Personalressourcen ausgestattet. Dennoch sind immer noch die originären Bereiche zuständig, wenn es um Bewilligungen geht.

Mark Valek: Gibt es hier eine spezielle Ansprechstelle oder eine Person, die dafür zuständig ist?

Dr. Dünser: *Ja, die Leiterin der Stabstelle für Finanzplatz Innovation und Regulierungslabor heisst Dorothea Rohlfing.*[37]

Interessante Ansprechpartner in Liechtenstein

1.) Planen Sie ein ICO oder brauchen Sie rechtliche Auskunft? Thomas Nägele von Nägele Law in Vaduz hat sich einen Ruf als Berater für Blockchain-bezogene Unternehmen aufgebaut.

2.) Haben Sie in Kryptowährungen investiert und steuerliche Fragen? Matthias Langer von der Actus-AG in Vaduz ist ausgewiesener Experte für steuerliche Themen.

3.) Sollten Sie ein Unternehmen in Liechtenstein planen und einen lokalen Treuhänder mit Krypto Know how suchen? Klaus Stark von der Ganten-Gruppe konnte bereits vielen helfen und ist in der lokalen Krypto Szene bestens vernetzt!

4.) Brauchen Sie ein Bankkonto für Ihr Krypto-Geschäft? Bank Frick, Alpinum, Bendura und Union heißen Blockchain-Unternehmer willkommen!

Regierungschef Hasler: *Die zweite Stelle ist im Ministerium bei Thomas Dünser und das ist auch sehr wichtig, dass man sowohl beim Ministerium der Regierung wie auch bei der FMA auf beiden Seiten entsprechende Einfallstore hat und sich dort orientieren kann. Und diese beiden schließen sich nämlich zusammen damit die ganzen Informationen weitergegeben werden können.*

Mark Valek: Welche der heimischen Banken bzw. Unternehmen sind Ihres Wissens nach bereit in die Crypto Welt einzudringen bzw. gibt es interessante Projekte, welche Sie speziell verfolgen?

Regierungschef Hasler: *Es ist so, dass ich jetzt natürlich keine speziellen Namen nennen möchte, aber man kann feststellen, dass das Interesse der hiesigen Banken aber auch Rechtsanwälte und Treuhänder sehr groß ist. Ich habe in den letzten Monaten festgestellt, dass dort sehr viel Zeit investiert wird, auch entsprechende Ausbildungen gemacht werden und Fachkompetenzen eingeholt werden um eben auch in diesem Bereich tätig zu sein. Es zeigt sich, dass es sehr viele interessante Projekte gibt und dass eben auch von außen Unternehmen an Liechtenstein herantreten und* ***entsprechende Geschäftspartner suchen um dann hier ihr Business in Liechtenstein aufzusetzen.***

Mark Valek: Es gibt ja auf diese Themen spezialisierte Anwälte, die sind wahrscheinlich auch erste Anlaufstelle für viele aus dem Ausland.

Regierungschef Hasler: *Genau. Einige Anwälte haben sich frühzeitig auf diese Themen spezialisiert und sind heute sehr gefragt. Übrigens haben wir bei der Ausarbeitung des Blockchaingesetzes auch auf dieses Fachwissen abgestellt.*

—

37 Vgl."Medienmitteilung: Regierungslabor wird verstärkt," *Finanzmarktaufsicht* Liechtenstein, April 20, 2018. Vgl. https://www.fma-li.li/files/fma/fma-medienmitteilung-2018-04.pdf; Email: dorthea.rohlfing@fma-li.li

"People used to use seashells as money. We can't help but think how primitive that was. Today we use paper as money. Eventually people will wonder how we could have been so primitive."

Anthony Pompliano, Founder & Partner Morgan Creek Digital Assets

Mark Valek: Zu guter Letzt gibt es weitere Blockchain-freundliche Maßnahmen, welche bereits angedacht sind?

Regierungschef Hasler: *Wir arbeiten ständig an der Verbesserung der Rahmenbedingungen. Jetzt gilt es jedoch, im nächsten Schritt dieses Blockchaingesetz umsetzen. Das heißt, die Vorlage im Parlament zu diskutieren und zu beschliessen. Das braucht sicherlich noch entsprechende Ressourcen. Dennoch sind wir laufend in Diskussion mit dem Markt, um die Bedürfnisse zu spüren und mitzubekommen, wo weitere Maßnahmen notwendig sind. Diese nehmen wir dann sehr gerne auf, um weitere Verbesserungen zu erzielen.*

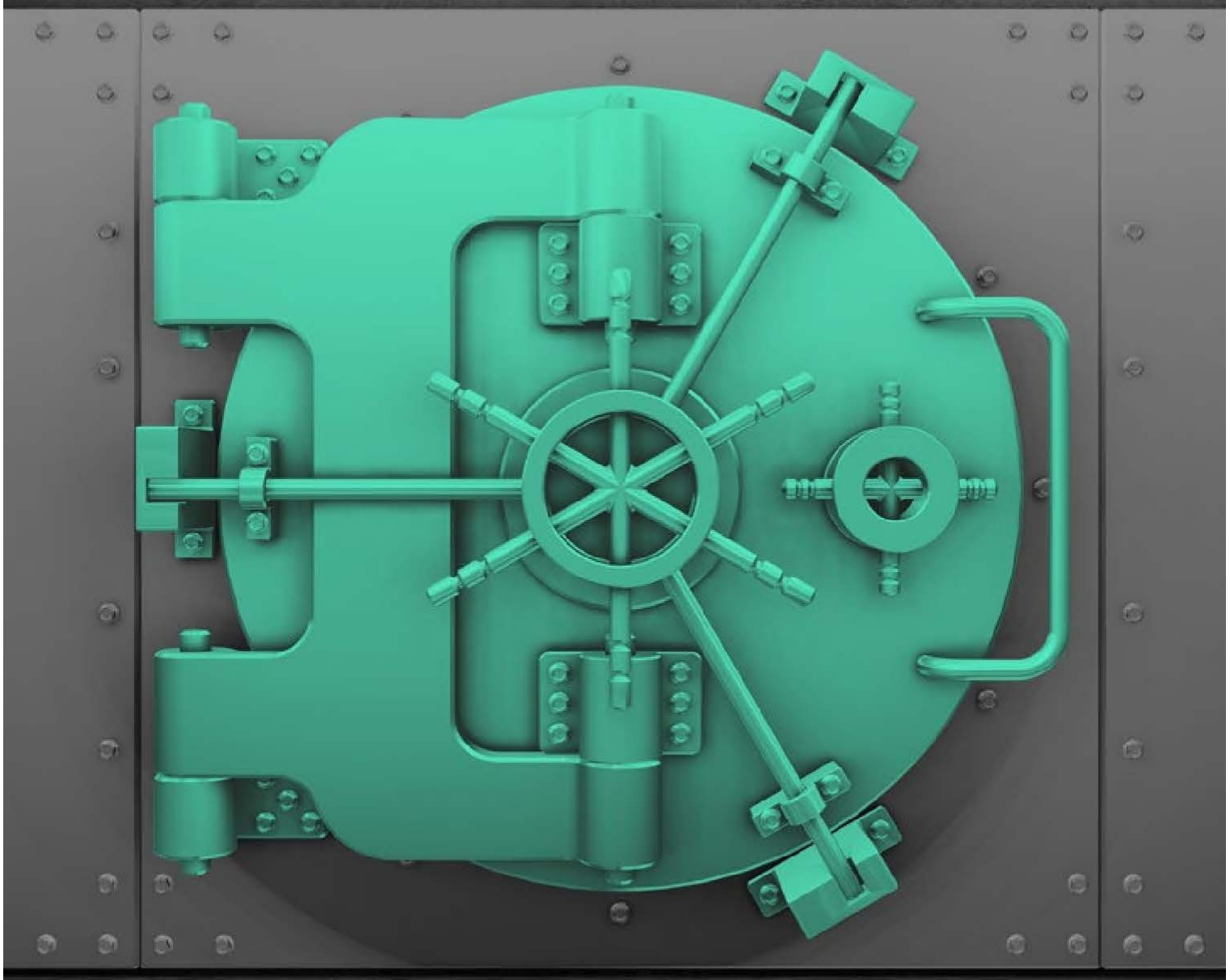
Mark Valek: Wunderbar, ich will Ihnen beiden natürlich nicht die Chance nehmen noch weitere Kommentare oder Anregungen zu erläutern.

Regierungschef Hasler: *Ich denke wir haben das Thema gut abgehandelt. Im Moment ist sehr viel im Fluss. Derzeit bin ich auf die Stellungnahmen zur Vernehmlassung sehr gespannt. Ich gehe davon aus, dass der Ansatz, den wir gewählt haben, befürwortet wird. Wir werden sehen, ob es noch weiteres Verbesserungspotential gibt. Anschliessend wird die Diskussion im Parlament wichtig sein. Interessant werden dann schliesslich auch die Auswirkungen sein, wenn das Gesetz in der Praxis angewendet wird. Da hoffe ich natürlich, dass wir gutes Feedback erhalten, Liechtenstein als attraktiver Standort wahrgenommen wird und sich somit viele Unternehmen hier niederlassen.*

Mark Valek: Hervorragend, dann sag ich Ihnen beiden, Regierungschef Hasler und Dr. Dünser vielen herzlichen Dank für die Zeit und ich wünsche viel Glück für die Vernehmlassung.

Regierungschef Hasler: *Besten Dank, Hr. Valek. Ich danke auch Ihnen für das Interesse und das Interview.*

Kryptowährungen.
Die neue Asset-Klasse.



Reguliert | Diversifiziert | Liquide

Informationen zur Fondsstrategie ausschließlich für professionelle Investoren gemäß MiFID.

www.cryptofunds.li

Der Netzwerkeffekt als Bewertungsmethode

"... ether itself will retain a strong and steady value as a cryptofuel, and as a store of value for Ethereum-based security deposits, simply because of the combination of the Ethereum blockchain's network effect (which actually is a platform network effect, as all contracts on the Ethereum blockchain have a common interface and can trivially talk to each other)"

Vitalik Buterin, Gründer von Ethereum

Key Takeaways

- **Bewertungskennzahlen sind der Schlüssel zur Fundamentalanalyse und stellen im traditionellen Finanzwesen ein bewährtes Konzept dar. Dieses ist nun auch mit der zunehmenden Reife des Marktes in der Krypto-Welt angekommen.**
- **Wir bieten eine Einleitung zu einer bestimmten Art der Bewertung, die darauf abzielt Assets zu identifizieren, die auf Grundlage einiger Fundamentalkennzahlen im Vergleich zu anderen Assets über- oder unterbewertet sind, und wenden dieses Konzept für Bitcoin, Litecoin und Bitcoin Cash an.**
- **Auch wenn die Kennzahlen noch ihre Tücken mit sich bringen, kommen sie weitgehend zu dem Schluss, dass der Bärenmarkt noch nicht vorbei ist und eine weitere Korrektur nicht auszuschließen ist.**

Ein auf Fachkonferenzen in den USA sehr aktuelles Thema ist die Bewertung von Kryptowährungen. Es gibt hierbei zwei Grundmodelle: absolute und relative Bewertung. Die absolute Bewertung versucht zu einem "fairen" Preis für jeden Vermögenswert zu gelangen sodass der Anleger den theoretisch "fairen" Preis mit dem realen, auf dem Markt gehandelten Preis vergleichen kann. Ist der Preis am Markt höher als der errechnete "faire" Preis, bedeutet dies ein Verkaufssignal für den Anleger. Dieselbe Logik gilt selbstverständlich für den umgekehrten Fall eines unterbewerteten Preises. An der Börse berechnen Analysten durchgehend den Barwert zukünftiger Unternehmensgewinne oder Dividenden, um zu einem Konsens über den heutigen Wert der Aktie zu kommen. Im Gegensatz zu dieser Form von Einzelbewertung ermöglichen relative Bewertungsmodelle dem Anleger den Vergleich mehrerer Aktienwerte untereinander. Relative Bewertungsmodelle sind oft Kennzahlen wie das Kurs-Gewinn-Verhältnis (KGV), welches den Marktpreis einer Aktie mit dem Bilanzgewinn des Unternehmens vergleicht.[38]

"Just like 20 years ago when very few institutions had exposure to hedge funds, it is now time for institutional investors to get off zero allocation to crypto assets."

Mark W. Yusko

Kryptowährungsanalysten nahmen diesen allgemeinen Bewertungsrahmen als Grundlage und erschufen das Verhältnis Network-Value-to-Metcalfe (NVM), Network-Value-to-Transactions (NVT) und eine Kennzahl die beide Konzepte kombiniert, genannt Network Value-to-Transactions-to-Growth (NVTG). Ein jeweils höheres Verhältnis suggeriert, dass eine Kryptowährung im Vergleich zu einer anderen überbewertet ist.

In diesem Kapitel konzentrieren wir uns auf die letztgenannte Form von Bewertungsmodellen. Ziel ist es Kennzahlen zu berechnen, die es Investoren ermöglichen, Kryptowährungen untereinander zu vergleichen. **Aus der Analyse dieser Kennzahlen, zeigen unsere Ergebnisse, dass der Kryptomarkt noch immer überbewertet ist, da die Markt-kapitalisierung weder durch die Zahl an täglich aktiven Nutzern noch durch das tägliche Transaktionsvolumen gerechtfertigt ist.** Wir konzentrieren unsere Analyse auf Bitcoin, Bitcoin Cash und Litecoin und stellen fest, dass Bitcoin relativ gesehen noch eine bessere Investition darstellt als Bitcoin Cash oder Litecoin. **Allerdings ist die relative Bewertungsmethode nur einer von mehreren Indikatoren ist, die wir bei Incrementum für Investitionsentscheidungen verwenden.**

[38] Fama and French, 1992

Netzwerk Wert Korrelationen

Korrelation Tabelle			Stand 21.09.2018
	BTC	LTC	BCH
Metcalfe's Gesetz	0.9653	0.9438	0.8482

Wie aus der obigen Tabelle ersichtlich ist, weist die Theorie hinter Metcalfe‘s Gesetz eine nahezu perfekte Korrelation zu empirischen Daten aus.

Der Netzwerk Effekt

In den 1980er Jahren entwickelte ein Mitarbeiter des Xerox Palo Alto Research Center (PARC) namens Robert Metcalfe eine neue Theorie über den Wert von Kommunikationssystemen[39]. Die Theorie wurde später als Metcalfe‘s Gesetz bekannt. Seine ursprüngliche Absicht war es, die Aktivitäten und Verbindungen des Ethernets zu beschreiben, welches ein Vorläufer des Internets war.

Heutzutage wird dieselbe Theorie verwendet, um ein Netzwerk und seine Nutzer zu bewerten, prominente Beispiele sind Internetunternehmen wie Facebook und eBay. **Metcalfe´s suggeriert einen Zusammenhang zwischen dem Wert eines Netzwerks und seiner Größe, die typischerweise in der Anzahl an Nutzern gemessen wird[40].**

Er argumentierte, dass der Wert eines Netzwerks proportional zum Quadrat der Netzwerkknoten (Nutzer) sein würde. Angenommen, das Social Media Netzwerk Pinterest hat n Nutzer, dann ist der Mehrwert, den jeder Nutzer aus dem Netzwerk zieht proportional zu (n - 1), nämlich die Anzahl der potenziellen Verbindungen im Netzwerk. Diese Beziehung zwischen Nutzen und Mehrwert ist der sogenannte "Netzwerkeffekt". Wenn ein zusätzlicher Nutzer dem Netzwerk beitritt, erhöht dies den Nutzen der Übrigen und unter der Annahme, dass alle Verbindungen gleichwertig sind, sollte sich der gesamte Netzwerkwert proportional zu $n*(n-1)$ verhalten, was wiederum asymptotisch proportional zu n^2 ist.

Metcalfe’s Gesetz für Krypto Assets

Ähnlich wie Online-Netzwerke sind Kryptowährungen Netzwerke von Nutzern, die im digitalen Raum verbunden sind und mit anderen Nutzern interagieren. Das **Metcalfe-Gesetz zu Folge wird der Nutzen eines Netzwerks umso größer, desto mehr Menschen Kryptowährungen adoptieren. Letztendlich führt dies zu einem entsprechend höheren Marktwert der jeweiligen Kryptowährung.**

In einem Versuch, die Rolle von Netzwerkeffekten zu definieren und ihre Folgen im kryptoökonomischen Kontext zu verstehen, skizzierte Vitalik Buterin die Hauptgründe dafür, warum ein großes Netzwerk den Wert einer Kryptowährung erhöht[41].

—

[39] Vgl. “Metcalfe’s Law after 40 Years of Ethernet,” Bob Metcalfe, *Computer*, Vol. 46, No. 12, 2013.https://ieeexplore.ieee.org/document/6636305/?tp=&arnumber=6636305&searchWithin%3Dp_Authors:.QT.Metcalfe.%20B..QT

[40] Vgl https://ieeexplore.ieee.org/document/6636305/?tp=&arnumber=6636305&searchWithin%3Dp_Authors:.QT.Metcalfe.%20B..QT.

[41] Vgl. “On Bitcoin Maximalism, and Currency and Platform Effects,” Vitalik Buterim, *Ethereum* Blog, November 19,

John Pfeffer, Partner bei Pfeffer Capital prognostiziert einen Bitcoin Wert von $700,000.

1. Sicherheitseffekt: *Systeme, die breiter akzeptiert sind, beziehen ihren Konsens aus größeren Konsensgruppen, was Angriffe auf das Netzwerk erschwert.*

2. Netzwerk-Effekt des Zahlungssystems: *Zahlungssysteme, die von mehr Händlern akzeptiert werden, sind für Verbraucher attraktiver, und Zahlungssysteme, die von mehr Verbrauchern genutzt werden, sind wiederum für Händler attraktiver.*

3. Integrationsnetzwerkeffekt: *Drittplattformen werden eher bereit sein, sich in eine Plattform zu integrieren, die weit verbreitet ist und die größere Anzahl dieser Drittplatformen wird die Nutzung der Plattform erleichtern.*

4. Größenstabilitätseffekt: *Währungen mit größerer Marktkapitalisierung sind tendenziell stabiler, und es wird als wahrscheinlicher angesehen, dass der Wert von etablierten Kryptowährungen in der Zukunft nicht auf Null sinkt.*

5. Markttiefeffekt: *Größere Währungen haben eine höhere Markttiefe an den Börsen, sodass die Nutzer größere Mengen an Geld in und aus dieser Währung umrechnen können, ohne den Marktpreis zu beeinflussen.*

6. Interpersönlicher Präferenzeffekt für eine einzige Währung: *Die Nutzer bevorzugen es, die gleiche Währung zu verwenden, die auch andere verwenden um Wechselgebühren bei alltäglichen Transaktionen zu vermeiden.*

7. Intrapersönlicher Präferenzeffekt in einer einzigen Währung: *Nutzer, die eine Währung bereits für einen Zweck verwenden, bevorzugen es, sie für andere Zwecke zu verwenden, sowohl aufgrund niedrigerer kognitiver Kosten als auch, weil sie einen niedrigeren Gesamtliquiditätssaldo unter allen Kryptowährungen ohne Wechselgebühren aufrechterhalten können.*

Grafik 7: Historischer Bitcoin Wert gegenüber Metcalfe Wert

Vergleicht man den Marktwert von Bitcoin mit dem aus fundamentaler Sicht vom Metcalfe Gesetz suggerierten Wert, so ist der starke Zusammenhang deutlich sichtbar.

Quelle: Incrementum AG

Nachteile der Network-Value-to-Metcalfe Ratio

Auch wenn die Theorie einleuchtend scheint, blieb Metcalfe's Gesetz in der akademischen Gemeinschaft nicht unumstritten.

So äußerten Andrew Odlyzko et al. einen berechtigten Einwand über das Modell: Metcalfe's-Gesetz suggeriert, dass der Nutzen in Form potenzieller Verbindungen innerhalb eines Netzwerks, theoretisch unendlich sein kann. Allerdings gibt es in der Realität einen Punkt, ab dem jeder zusätzlicher Netzwerkteilnehmer für den einzelnen Nutzer von wenig Mehrwert ist.

Eine weitere Annahme, die stark hinterfragt wurde, war jene die besagt, dass jeder zusätzliche Nutzer einen gleich hohen Mehrwert zum Netzwerk beiträgt. Es ist sinnvoll zu argumentieren, dass für ein Netzwerk von jungen Snapchat-Nutzern der Eintritt weiterer Freunde zum Netzwerk mehr Nutzen bringt, als wenn ihre Eltern dem Netzwerk beitreten.

Verschiedene Arten von Kryptowährungen können auch unterschiedliche Arten von Netzwerkeffekten aufweisen: Ein Zahlungs-Token wie Bitcoin wird wahrscheinlich einen stärkeren *Interpersönlichen Präferenzeffekt für eine einzige Währung* aufweisen als ein Nutzen-Token wie Ethereum.

Network-Value-to-Metcalfe Ratio

Nachdem wir ein Verständnis für die Rolle von Netzwerkeffekten im Kryptogebiet gewonnen haben, können wir uns nun den konkreten Kennzahlen widmen, mit denen wir den durch Netzwerkeffekte suggerierten Wert für einzelne Kryptowährungen errechnen. Die erste Kennzahl, die wir betrachten wollen ist die Anwendung von Metcalfe's Gesetz auf Kryptowährungen, welche als Network-to-Metcalfe Kennzahl bezeichnet wird. Ihr Hauptzweck ist es, eine Einschätzung zu ermöglichen, wie über- oder unterbewertet eine Kryptowährung im Moment ist.

Je höher der Preis im Verhältnis zum Nutzen ist, den Netzwerkteilnehmer der Netzwerkeffekt-Theorie zur Folge nach beziehen, desto höher ist die zu erwartende Korrektur zurück zu dem theoretischen Wert. **Demnach impliziert das Modell, dass der Preis einer Kryptowährung in einem direkten Zusammenhang mit einem fundamentalen Wert steht,**

der langfristig vom Anwendernutzen bestimmt wird, und dass eine Form der Rückkehr zum Mittelwert stattfindet[42].

Die Network-to-Metcalfe-Kennzahl stellt die jeweilige Theorie zur Beschreibung des Netzwerkeffektes in den Nenner, während die Marktkapitalisierung als Näherungswert für den Wert des Netzwerks verwendet wird. Netzwerknutzer (n) werden durch die Anzahl der täglich aktiven Adressen geschätzt, d.h. jene die an Sende- oder Empfangsvorgängen teilnehmen. Aktive Adressen im Bitcoin-Ökosystem sind Zahlungsadressen, die einen positiven Saldo aufweisen[43]. Während die Zahl der aktiven Adressen kein perfektes Maß für die tatsächliche Nutzung an einem bestimmten Tag ist, gilt im Allgemeinen je mehr Adressen verwendet werden, desto mehr Nutzer muss das Netzwerk haben. Da wir versuchen, eine langfristig fundamentale Kennzahl zu erhalten, glätten wir zusätzlich die täglich aktive Nutzerzahl auf einen gleitenden 30-Tage-Durchschnitt, um starke tägliche Schwankungen zu beseitigen.

"The Bitcoin market price was sometimes ten times higher than predicted by the Metcalfe model."

Lidia Bolla, Vision &

Der erste Kandidat für unsere Analyse ist Bitcoin: Wenn man den Netzwerkwert von Bitcoin mit seinem NVM-Verhältnis grafisch vergleicht, zeigt sich ein interessanter Zusammenhang.

Grafik 8: Bitcoin Network-Value-to-Metcalfe Ratio

Quelle: Coinmetrics, Incrementum AG

Hohe Werte in Bitcoins NVM-Verhältnis deuten darauf hin, dass das Netzwerk im Verhältnis zur Anzahl der aktiven Nutzer überteuert ist was in der Vergangenheit fast immer zu einer Korrektur des Marktwertes geführt hat. Wir sehen das ganz deutlich in den Perioden von Anfang 2011, Mitte 2012, Anfang 2013 und Ende 2017. Der orangefarbene Bitcoin Marktwert ist auf einer logarithmischen Skala

—

[42] Hier konzentrieren wir uns auf das Verhältnis zwischen dem Netzwerkwert und einer aggregierten Benutzermetrik, mit dem Ziel, den Netzwerkeffekt so allgemein wie möglich zu halten. Um zu einer vollständigen grundlegenden Maßnahme zu gelangen, müsste weiter erforscht werden, wie die einzelnen Effekte zu beurteilen sind.

[43] Für Internetunternehmen mit starken Netzwerkeffekten ist der Daily Active Users (DAU) Indikator eine der wichtigsten Performance- und Bewertungskennzahlen.

dargestellt. Wir transformieren alle nachfolgenden historischen Marktwerte in eine logarithmische Skala zwecks besserer Visualisierung. Die y-Achse in der obigen Grafik stellt links die logarithmische Skala und rechts den aktuellen Wert der NVM-Kennzahl dar.

Die historische Betrachtung zeigt, dass sobald Bitcoins NVM sich deutlich über seinen langfristigen Mittelwert (0,21) befindet, Grund zur Sorge über die zukünftige kurz- bis mittelfristige Entwicklung des Marktwerts besteht. Umgekehrt hat ein NVM, das deutlich unter seinem Mittelwert liegt, in der Regel eine gute Kaufmöglichkeit geboten. Die aktuellen Werte der NVM Kennzahl für Bitcoin zeichnen allerdings ein negatives über die zu erwartende Marktwertentwicklung und suggerieren noch weiteren Raum für Abwärtskorrekturen.

Grafik 9: Litecoin Network-Value-to-Metcalfe Ratio

Quelle: Coinmetrics; Incrementum AG

Ähnliche Muster, wenn auch mit geringerer Vorhersagekraft, treten bei Litecoin (LTC) und Bitcoin Cash (BCH) auf. Das Signal für letztere Kryptowährung ist zudem auch wegen der kurzen Historie weniger robust.

Grafik 10: Bitcoin Cash Network-Value-to-Metcalfe Ratio

Quelle: Coinmetrics; Incrementum AG

"First off, you could argue we have had a proper correction in Bitcoin, it has had a 50 percent pull back at one point, which is healthy. But we have still not seen the full effect of the futures contract."

Kay Van-Peterson, Saxo Bank

Bei Litecoin sind hohe NVM Werte in den Folgeperioden meist von Korrekturen im Marktwert gefolgt. Es ist jedoch auffallend, dass die jüngste "Blase" Ende 2017 von keinen hohen NVM Werten begleitet wurde. Dies könnte mit den bereits angesprochenen Schwachstellen der Kennzahl zusammenhängen oder aber mit idiosynkratischen Komponenten, die dem Litecoin-Netzwerk innewohnen. Beispielsweise die Tatsache, dass die Entwicklung von Litecoin fast vollständig zum Stillstand gekommen ist, wie aus ihrer Github-Aktivität ersichtlich ist, oder aber auch die 100 %ige Liquidierung der LTC-Beteiligung durch den Litecoin-Gründer, Charlie Lee, sind Gründe für ein Auseinanderfallen von Marktwert und Fundamentaldaten**. Insgesamt scheinen die Kennzahlen von BTC & LTC mehr oder weniger im gleichen Bereich von 0,01 - 2 zu handeln, während BCH von Natur aus eine viel höhere Skala von .90 - 11 aufweist.** Die aktuellen Kennzahlen finden Sie in der folgenden Tabelle.

Tabelle 4: Aktuelle Niveaus der Network-Value--to-Metcalfe Ratio

Current NVM Multiples			as of 21.09.2018
	BTC	LTC	BCH
NVM	0.33	0.44	5.95

Quelle: Incrementum AG

Auf relativer Basis sind die Preise für BTC und LTC im Vergleich zu ihrer Benutzerbasis ähnlich hoch, während der BCH-Preis stark überbewertet zu sein scheint.

Network-Value-to-Transaction-Value Ratio

Eine weitere wertvolle relative Bewertungs-kennzahl, die der NVM Ratio ähnlich ist, ist das Verhältnis von Netzwerk Wert zu täglichem Transaktionsvolumen. Wenn wir an das KGV im traditionellen Finanzbereich zurückdenken, dienen die Erträge als Indikator für die Wertschöpfung eines Unternehmens. Wenn wir versuchen, diese Idee auf Kryptowährungen anzuwenden, stellen wir fest, dass die meisten von ihnen keine Einnahmen im traditionellen Sinne generieren. Man kann jedoch argumentieren, dass es eine positive Beziehung zwischen dem Nutzen, und damit dem Wert eines Netzwerks und dem Volumen der dadurch fließenden Transaktionen geben sollte. Diese Idee ist im Einklang mit den im vorherigen Abschnitt diskutierten interpersonellen und intrapersonellen Netzwerkeffekten nach Vitalik Buterin.

Der wichtigste Teil des NVT-Verhältnisses ist die Definition des Nenners, sprich des gesamten Transaktionsvolumens, so dass dieser den tatsächlichen Nutzen für Netzwerkteilnehmer widerspiegelt. Transaktionsvolumina von Kryptowährungen werden derzeit an zwei Stellen generiert: auf der Blockchain selbst (On-chain) und abseits davon (Off-chain). On-Chain-Transaktionen werden direkt auf der Blockchain dokumentiert, während Off-Chain-Transaktionen sich typischerweise auf Interaktionen über Drittanbieter wie Kryptobörsen beziehen, die nicht direkt auf der Blockchain dokumentiert werden.

Die Frage welche Transaktionen nun tatsächlich repräsentativ für den Nutzen in einem Netzwerk sind, ist eine wirkliche Herausforderung in der Kryptowelt.[44] Es ist davon auszugehen, dass On-Chain-Transaktionsvolumen der tatsächlichen Wirtschaftsleistung auf der Blockchain am Nächsten kommen sollte und somit unmittelbar den Nutzen eines Netzwerks für deren Teilnehmer darstellt. Wir beschreiben den Nenner in der Network-to-Transactions Ratio mit einem vom Coinmetrics-Team berechneten On-Chain-Transaktionsvolumen.

Ähnlich wie bei NVM glätten wir die täglichen Transaktionsvolumina auf einen gleitenden 30-tägigen Durchschnitt, um sicherzustellen, dass wir den langfristigen fundamentalen Trend erfassen. Abermals dient wie schon oben beschrieben die Marktkapitalisierung als Annäherung für den Wert des Netzwerks. Nachfolgend präsentieren wir unsere Ergebnisse:

Nachteile der Network-Value-to-Transaction-Value Ratio

Echten wirtschaftlichen Nutzen auf der Blockchain herauszufiltern, gestaltet sich als eine große Herausforderung und schwächt somit die Zuverlässigkeit des NVT-Verhältnisses bis zu einem gewissen Grad ab.

So ist es beispielsweise gängig, massive Transfers zwischen unterschiedlichen Börsen auf der Bitcoin Blockchain zu beobachten, welche dem Netzwerk wiederum wenig Nutzen bringen. Außerdem muss man bei der Messung des On-Chain-Transaktionsvolumens beim Vergleich verschiedenen Blockchain-Systemen äußerst vorsichtig sein, da verschiedene Protokolle auf unterschiedliche Weise Transaktionen bearbeiten (z.B. Bitcoins UTXO vs. Ethereums Account based model). Auch finden auf manchen Protokollen Aktivitäten statt die auf anderen nicht geschehen (z.B. Transaktionsvolumen auf Blockchains mit Staking-Rewards wie Dash ist im Vergleich zu Bitcoin von Grund auf inflationiert).

Darüber hinaus spielt ein von George Soros eingeführtes Konzept, namens "Reflexivity" auch eine Rolle: Transaktionsvolumen folgt tendenziell auf Preisänderungen und umgekehrt, so dass die beiden Variablen eine "reflexive" Beziehung innehaben, welche wiederum je nach Stärke jenes Effekts die Zuverlässigkeit des NVT-Verhältnisses in Frage stellt.

—
44 Vgl. "Introducing our adjusted transaction volume estimates," Coinmetrics Team, *Coin Metrics*, June 27, 2018. https://coinmetrics.io/introducing-adjusted-estimates/

Für Bitcoin erhalten wir mit dem NVT Verhältnis einen weiteren Leitindikator für dessen Marktwert, wobei ein hohes Mehrfache (zwischen 50-100) eine potenzielle Überbewertung und ein niedriges Mehrfach (zwischen 0-30) eine Unterbewertung signalisieren. Es ist interessant anzumerken, dass sich der aktuelle Wert von NVT einem Niveau zu nähern scheint, das zuletzt am Höhepunkt der letzten Blase erreicht wurde.

Grafik 11: Bitcoin Network-Value-to-Transaction-Value Ratio

Quelle: Coinmetrics; Incrementum AG

Dies gilt nicht nur für BTC, sondern auch für LTC, während sich die Bewertung von BCHs im Verhältnis zu seinem Transaktionsvolumen wieder stabilisiert zu haben scheint und sich in der Nähe des langfristigen Mittelwert befindet. Ähnlich wie das NVM-Verhältnis befindet sich das NVT-Verhältnis von BTC und LTC meist im gleichen Schwankungsbereich (20-60), während das BCH-Verhältnis typischerweise über 50 liegt und in seiner kurzen Vergangenheit bereits einige Male die 100er-Marke berührt oder überschreitet hat, was Hinweis für eine inhärente Überbewertung von BTC könnte.

Wie bereits für den obigen Fall von NVM erläutert, scheint die NVT von LTC seinem historisch vorhersagenden Muster während der letzten Blase Ende 2017 nicht gefolgt zu sein. Wir haben bereits einige Überlegungen angestellt, warum dies der Fall für LTC sein könnte[45].

—
45 Vgl. „Debunking Market Narratives: Litecoin ($LTC) Edition" ," Tushar Jain, *Multicoin Capital*, September 14, 2018.

Grafik 12: Litecoin Network-Value-to-Transaction-Value Ratio

Quelle: Coinmetrics, Incrementum AG

Grafik 13: Bitcoin Cash Network-Value-to-Transaction-Value Ratio

Quelle: Coinmetrics, Incrementum AG

Network-Value-to-Transaction-Value-to-Growth

"Historically, ten days comprise all the performance in any single year of Bitcoin's price...If you just took out those ten days, Bitcoin's down 25 percent a year. So as miserable as it feels holding Bitcoin at $8,000, the move from $8,000 to $25,000 will happen in a handful of days."

Tom Lee,
Co-founder Fundstrat

In den beiden vorangegangenen Unterkapiteln wurden die NVM- und NVT-Verhältnisse sehr detailliert behandelt, aber wie wir aus unseren Analysen ersichtlich ist, rufen diese in manchen Fällen widersprüchliche Ergebnisse in Bezug auf Über- oder Unterbewertung einer Kryptowährung hervor.

Beide Kennzahlen sind zweifellos die zurzeit brauchbarsten relativen Bewertungskennzahlen, aber der Ruf nach einer Kennzahl die beide Konzepte vereint, ist verständlich. NVT berücksichtigt nicht den Nutzen, den neue Teilnehmer dem Netzwerk beisteuern, während NVM nicht das tatsächliche Ausmaß der wirtschaftlichen Aktivität eines Netzwerks berücksichtigt.

Aus diesem Grund hat ein Forscherkollege[46] kürzlich abermals die Brücke zwischen der traditionellen Finanzwelt und der Kryptowelt geschlagen, indem er sich die zweithäufigste relative Kennzahl aus ersterer Welt anschaute, nämlich das Kurs-Gewinn-Wachstumsverhältnis („Price-to-Earnings-to-Growth"). Das KGW-Verhältnis ist besonders bei der Bewertung von Aktien mit hohem Wachstumspotenzial, aber nahezu inexistenten Gewinnen nützlich, was zu einem sehr hohen KGV und somit aber einer unvollständigen Bewertung führen würde. Wenn wir das KGWV-Verhältnis auf Krypto anwenden, erhalten wir das Network Value-to-Transactions-to-Growth (NVTG)-Verhältnis, das darauf abzielt, sowohl den wirtschaftlichen Mehrwert in einem Netzwerk als auch das Wachstum seiner Nutzerbasis in einer einzigen Kennzahl zu konsolidieren. Wenden wir diese Idee auf echte Netzwerke an, erhalten wir folgenden Ergebnisse:

Die NVTG-Kennzahl fasst im Großen und Ganzen die Ergebnisse zusammen, die wir aus der Analyse von NVM und NVT für die drei Kryptowährungen im Einzelnen erhalten haben. Insgesamt deuten die Kennzahlen auf einen weiteren Abwärtstrend in Richtung ihres jeweiligen Mittelwerts hin. Demnach jenen den Nutzerzahlen als auch Transaktionsvolumina für Bitcoin und Bitcoin Cash nahelegen. Wie bereits erwähnt, scheint Litecoin den Bezug zu seinen Fundamentaldaten vollständig verloren zu haben, weshalb das NVTG-Verhältnis auch in dem Fall wenig Vorhersagekraft besitzt.

—
46 Vgl. "Improvements on the Network Value to Transactions (NVT) Ratio & Introducing Network Value/Transactions to Growth (NVTG) to Value Crypto," Vikram Arun, *Medium*, March 29, 2018.

Grafik 14: Bitcoin Network-Value-to-Transaction-Value-to-Growth

Quelle: Coinmetrics, Incrementum AG

Grafik 15: Litecoin Network-Value-to-Transaction-Value-to-Growth

Quelle: Coinmetrics, Incrementum AG

Grafik 16: Bitcoin Cash Network-Value-to-Transaction-Value-to-Growth

Quelle: Coinmetrics, Incrementum AG

"Bitcoin's volatility derives from the fact that its supply is utterly inflexible and not responsive to demand changes, because it is programmed to grow at a predetermined rate"

Saifedeam Ammous

Bitcoins NVTG nähert sich dem höchsten Stand seit zwei Jahren, was unsere Schlussfolgerung bestärkt, dass es noch weiter Abwärts gehen könnte, sollte der wirkliche wirtschaftliche Nutzen des BTC-Netzwerks nicht deutlich ansteigen.

Wie ersichtlich, scheint Bitcoin im Vergleich zu seinen Konkurrenten noch die gesündesten Bewertungsniveaus zu haben, wenn sie auch im historischen Vergleich recht hoch sind. Bitcoin Cash hat eindeutig die übertriebensten Bewertungskennzahlen in Bezug auf Nutzerzahl und Transaktionsvolumen.

Zum Abschluss haben wir den aktuellen Stand nach relativer Bewertung in einer Tabelle für die ausgewählten Coins zusammengefasst.

Tabelle 5: Aktuelle Relative Kennzahlen

Aktuelle Niveaus			Stand: 21.09.2018
	BTC	LTC	BCH
NVM	0.33	0.44	5.95
NVT	56.6	62.5	65.1
NVTG*	4.6	34.4	84.2

*Hier haben wir das tatsächliche NVTG mit einem Vielfachen von 105 multipliziert, um die Zahlen optisch ansprechender zu gestalten.

Wir werden diese Kennzahlen auch in Zukunft monitoren und planen, diese auch regelmäßig zu veröffentlichen.

Wir danken Incrementum Analyst Friederich Zapke für den Beitrag.

Liechtensteins Blockchain Strategie: Einblicke in die Finanzmarktaufsicht

"... So können „payment token“ nur Unternehmen mit einer Bewilligung der FMA, also z.B. einer E-Geld Bewilligung oder einer Bankbewilligung, ausgegeben werden. Es gibt aber gewisse Ausnahmen, die keine Bewilligung benötigen. Bei „securities token“ hängt es davon ab, ob das Unternehmen mit dem Token ein Finanzinstrument für Anleger kreiert oder ob damit Fremd- oder Eigenkapital für das Unternehmen selbst aufgenommen wird.

Patrick Bont, FMA

Key Takeaways

- **In den letzten drei Jahren hat die FMA mehr als 100 Anfragen im Zusammenhang mit ICOs erhalten und bearbeitet. Allerdings wurde nur ein Bruchteil davon umgesetzt.**
- **Nach Angaben der FMA in Liechtenstein dauert die Planung, Vorbereitung und Durchführung eines ICO‘s je nach Komplexität der Coin und der erforderlichen Bewilligungen zwischen 12 und 18 Monaten.**
- **Die Einstufung der Tokens ist von aufsichtsrechlicher Relevanz und wird von der FMA vorgenommen.**

Patrick Bont ist Mitglied der Geschäftsleitung der Finanzmarkt Aufsicht in Liechtenstein, Leiter der Bankabteilung und Leiter des FinTech-Teams der FMA. In den letzten dreieinhalb Jahren war Herr Bont als Dozent am Compliance-Officer Certificate Program der Universität Liechtenstein tätig. Er absolvierte seinen Master in Rechtswissenschaften an der Universität St. Gallen. Herr Bont hat ausführlich zum Thema Kryptowährungen publiziert, und ist ein aktives Mitglied der liechtensteinischen Fintech-Community.

Mark Valek: Ein wesentlicher Aspekt von Kryptowährungen bzw. der „Tokenized Economy“ ist der Prozess des sogenannten Initial Coin Offerings (ICOs), also die Erstausgabe von Crypto Tokens. Welche wesentlichen Kategorien von Tokens gibt es hier aus aufsichtsrechtlicher Sicht?

Patrick Bont, Mitglied der Geschäftsleitung der liechtensteiner Finanzmarkt Aufsicht (FMA) spricht mit Mark Valek über rechtliche Aspekte von ICOs.

Patrick Bont: *Es gibt zahlreiche Ansätze, um Token zu kategorisieren. Unter den Regulatoren und Aufsichtsbehörden sind Diskussionen im Gange, welcher Ansatz am sinnvollsten ist. Die FMA geht im Moment von drei Kategorien aus. Das sind „utility token“, „payment token“ und „securities token“. Ganz grob kann man sagen, dass „utility token“ zum Bezug einer Ware oder Dienstleistung berechtigen, „payment token“ als Zahlungsmittel dienen sollen und „securities token“ quasi Finanzinstrumente darstellen. In der Praxis sind die Grenzen aber nicht ganz so einfach zu ziehen und es gibt zahlreiche Mischformen. Finanzmarktrechtlich sind vor allem „payment token“ und „securities token“ relevant.*

Mark Valek: Wer nimmt im Einzelfall die Token Klassifizierung des ICO vor? Liegt der Schwerpunkt der Klassifizierung auf juristischer oder technischer Ebene?

Patrick Bont: *Grundsätzlich ist der Token-Emittent dafür verantwortlich abzuklären, ob sein ICO bzw. sein Token unter das Finanzmarktrecht fällt. Es empfiehlt sich, dazu einen spezialisierten Anwalt beizuziehen. Das FinTech-Team der FMA kann im Falle von Unklarheiten natürlich auch kontaktiert werden. Für uns ist in erster Linie die juristische Einordnung wichtig. Die technischen Funktionalitäten eines Token können aber Hinweise zur Einordnung geben.*

Mark Valek: Nehmen wir an ein Unternehmen beabsichtigt ein ICO hierzulande. Wie sieht der Prozess je nach Token Klasse, die ausgegeben werden soll, aus?
Patrick Bont: *Zuerst muss sich das Unternehmen überlegen, was es mit dem ICO erreichen will. Das heisst, es muss dies wirtschaftlich, aber auch juristisch und technisch beurteilen. Man spricht auch von „ICO economics“. Wenn dann beschlossen wird, einen „security token“ oder einen „payment token“ auszugeben, dann sollte das Unternehmen, am besten mit Unterstützung durch einen Spezialisten, die entsprechenden Anträge bei der FMA einreichen.*

Mark Valek: Benötigt das emittierende Unternehmen eine aufsichtsrechtliche Konzession, und wenn ja welche?

Patrick Bont: *Das hängt wiederum vom Token bzw. dem Geschäftsmodell des Unternehmens ab und wem die Token angeboten werden. So können „payment token" nur Unternehmen mit einer Bewilligung der FMA, also z.B. einer E-Geld Bewilligung oder einer Bankbewilligung, ausgegeben werden. Es gibt aber gewisse Ausnahmen, die keine Bewilligung benötigen. Bei „securities token" hängt es davon ab, ob das Unternehmen mit dem Token ein Finanzinstrument für Anleger kreiert oder ob damit Fremd- oder Eigenkapital für das Unternehmen selbst aufgenommen wird. In letzterem Fall benötigt das Unternehmen keine Bewilligung der FMA, muss aber allenfalls den sogenannten „Prospekt" genehmigen lassen.*

Mark Valek: Welche Zeitdauer sollte für ein ICO eingeplant werden?

Patrick Bont: *Die Planung, Vorbereitung und Durchführung eines ICO benötigt nach unseren Erfahrungen zwischen 12 und 18 Monaten, abhängig von der Komplexität und den benötigten Bewilligungen.*

Mark Valek: Welche Auswirkungen wird das geplante Blockchain Gesetz auf die ICO Landschaft in Liechtenstein haben bzw. wie wirkt sich dieses nationale Gesetz auf internationale Sachverhalte aus?

Patrick Bont: *Wichtig zu verstehen ist, dass alle ICO, die heute unter das Finanzmarktrecht fallen dies auch in Zukunft tun werden. Liechtenstein übernimmt als EWR-Land die EU-Finanzmarktregulierung und setzt diese um und durch. Das Blockchain-Gesetz betrifft also alle ICO, die nicht unter das Finanzmarktrecht fallen, das heisst vor allem „utility token". Das Gesetz hat den Vorteil, dass auch diese ICO gewissen Regeln unterworfen werden und somit die Käufer der Token einen besseren Schutz geniessen. ICO sind aber nur ein Aspekt des neuen Gesetzes.*

Mark Valek: Wie viele ICOs wurden bereits von der FMA geprüft bzw. wieviel sind derzeit in Prüfung (sofern diese Information publik gemacht werden kann)?

Patrick Bont: *Die FMA hat in den vergangenen drei Jahren über 100 Anfragen in Zusammenhang mit ICOs erhalten und bearbeitet. Davon wurde aber nur ein Bruchteil umgesetzt.*

Mark Valek: Wie bereitet sich die FMA Liechtenstein ressourcentechnisch auf die neue Komplexität bzw. zunehmende Anfragen von

Wie Sie mit der liechtensteinischen FMA in Kontakt treten können:

1.) Folgen Sie Patrick Bont auf Twitter: @patrickbont

2.) Besuchen Sie die kostenlosen Blockchain-Meetups in St. Gallen, Schweiz, die von Patrick Bont und Beni Bürgi erstellt wurden!

3.) Treffen Sie Herrn Bont persönlich während einer seiner Vorträge, wie zB. auf der FinTech.li!

4.) Besuchen Sie die FMA, aber vergessen Sie nicht zuerst einen Termin zu vereinbaren!

Finanzmarktaufsicht Liechtenstein
Landstrasse 109, Postfach 279
9490 Vaduz, Liechtenstein
+423 236 73 73
info@fma-li.li

"The regulatory landscape has seen some positive developments in the last six months. Earlier in the year, South Korea highlighted that it was planning to regulate cryptocurrencies and bring them into the open, as opposed to outright banning them. In May, Japan announced that the country is working on cryptocurrency regulation and building a template for ICO and digital currency exchange regulation. Most recently, an SEC official announced that bitcoin and ether are not securities due to the decentralised nature of their networks."

CoinShares Research

Unternehmen gerade in Hinblick auf die Prüfung und Überwachung der Tokens vor?

Patrick Bont: *Die FMA hat im Juni dieses Jahres ein eigenes Team für das Thema FinTech aufgebaut. Das Team Regulierungslabor/Finanzinnovationen kümmert sich um Fragestellungen von Unternehmen und Unternehmern im Bereich Finanzinnovationen. Das sind nicht nur Start-ups sondern auch Banken oder andere Finanzintermediäre, die Projekte realisieren wollen. Zudem legen wir in der FMA grossen Wert darauf, dass unserer Mitarbeitenden sich in diesen Themen weiterbilden, damit wir auf Augenhöhe mit den Marktteilnehmern diskutieren können.*

Mark Valek: Wo kann sich ein Unternehmen über allfällige Anforderungen informieren?

Patrick Bont: *Ich empfehle, regelmässig die Website der FMA zu besuchen. Unter der Rubrik „FinTech in Liechtenstein" finden sich Informationen zum Thema. Die FinTech-Seiten werden regelmässig erneuert und ergänzt.*

bitpanda

Home of **Cryptocurrency**

TRADEN. SENDEN. LAGERN.

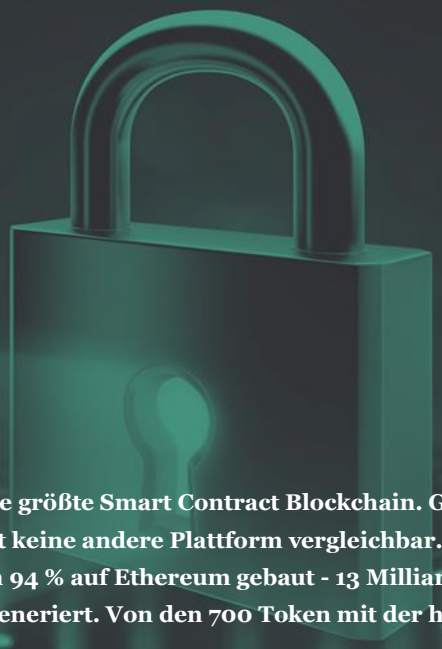
Besuchen Sie uns auf **www.bitpanda.com**

Made in **Vienna** with ♥ and care

Coin Corner:
ETH, NEO, ADA & EOS

“2019’s Trillion Dollar Question: How to merge Blockchains?”

Yanislav Malahov, Aeternity



Key Takeaways

- **Ethereum ist bis dato noch die größte Smart Contract Blockchain. Gemessen an Entwicklern, Transaktionen und DApps, ist keine andere Plattform vergleichbar. Von den Top-100 Token nach Marktkapitalisierung wurden 94 % auf Ethereum gebaut - 13 Milliarden Dollar Kapital wurden auf diese Weise über Ethereum generiert. Von den 700 Token mit der höchsten Marktkapitalisierung sind 87 % Ethereum-Token.**

- **Allerdings rühmt sich eine neue Kryptowährung, EOS als der "Ethereum Killer". EOS hält den Rekord für die größte ICO, die je auf Ethereum durchgeführt wurde: 4 Milliarden Dollar. Im Juni dieses Jahres lancierte EOS seinen Mainnet und wechselte von einem Ethereum basierten ERC-20 Token zu einer eigenen Blockchain, der EOS Blockchain.**

- **Cardano als Underperformer: Vergangenen Mai handelte Cardano noch über $0,37 und rangierte als sechstgrößter Token auf den Coinmarketcap-Listen. Seither ist es jedoch in einem Abwärtstrend und handelt heute um lediglich $0,07. Investoren kritisieren auf Reddit weiterhin scharf, dass Cardano nicht in der Lage ist, mit den niedrigen Transaktionskosten und schnellen Bestätigungszeiten von EOS zu konkurrieren.**

Als der Krypto-Markt noch im Januar bei einer Marktkapitalisierung von ungefähr 800 Milliarden USD stand, ist vielen Krypto-Enthusiasten das Wort der Bitcoin-Revolution allzu leicht über die Lippen gegangen. Heute, wo die Marktkapitalisierung nur noch etwa ein Viertel davon ausmacht und die Preise von ihren Allzeithochs in den Keller gestürzt sind, scheint die Euphorie verflogen und die Revolution aufgeschoben. Zumindest vorerst.

"The main advantage of blockchain technology is supposed to be that it's more secure, but new technologies are generally hard for people to trust, and this paradox can't really be avoided"

Vitalik Buterin

Doch wenn man seinen Fokus einmal weg von den Kursen wendet und sich vergegenwärtigt, wie jung das Krypto-Phänomen noch ist und über die bisherigen Erfolge Bilanz zieht, vermag man dessen revolutionären Errungenschaften so richtig zu erfassen. Denn obwohl die Krypto-Welt noch ganz am Anfang steht, hat sie bereits Einmaliges geschafft: Eine digitale Währung, die im Internet existiert und dabei auf einem eigenständigen Zahlungsnetzwerk ohne eine alles kontrollierende Zentralinstanz basiert, hat es vor Bitcoin noch nie gegeben. Auch der Umstand, dass Bitcoin abseits des Polit- und Wirtschaftsestablishments im Stile einer spontanen Ordnung und eines chaotischen Planes zu einem 100 Milliarden USD Projekt werden konnte, lässt einen dessen revolutionären und einzigartigen Charakter würdigen. Selbst über sein eigenes Habitat hinaus hat der Bitcoin neue Ökosysteme geschaffen – allen voran das Ethereum-Imperium. So war es die Idee hinter Bitcoin sowie potenzielle Kursgewinne, die dem Ethereum-Projekt anfänglich Leben einhauchten. Von Juli bis August im Jahr 2014 lancierte die Ethereum-Foundation ein Initial Coin Offering, um mit ihrem Konzept bei Bitcoin-Besitzern zu werben. Nur wer sich von einem Teil seiner Bitcoin trennte, konnte diese für Ether – dem Token des Ethereum-Netzwerkes – hingeben und so in die Vision des heute zweitgrössten Krypto-Assets investieren.

Das Superhirn hinter Ethereum ist Vitalik Buterin. Auf Bitcoin stiess der Russisch-Kanadier im zarten Alter von 17 im Februar 2011, als sein Vater ihn auf die Kryptowährung aufmerksam machte. Bald darauf faszinierte ihn das Bitcoin-Projekt und Buterin begann, sich immer intensiver damit auseinanderzusetzen. Mit der Zeit ging die Faszination auch in das Bestreben hinüber, eine Limitation Bitcoins zu beseitigen, die Buterin ausgemacht zu haben glaubte. So stellte das Wunderkind fest: Obschon Bitcoin ein beeindruckendes Stück Programmiercode ist, entwickelte kaum jemand Applikationen auf Bitcoin. Und dies war absichtlich so. Seit Anbeginn der Bitcoin-Blockchain bestand deren Hauptaufgabe darin, eine möglichst sichere Übertragung von digitalen Werten zu ermöglichen. Um dieses Ziel keinesfalls unnötig zu gefährden, wurde dem Bitcoin eine möglichst rudimentäre, dafür aber umso robustere Skriptsprache zugrunde gelegt. Um Entwicklern, das Programmierern neuer Software auf Bitcoin zu vereinfachen, bräuchte es eine komplexere Skriptsprache, eine sogenannte Turing-vollständige Programmiersprache, ersann das Computergenie. Natürlich würde bei einer solchen programmierbare Blockchain auch die Fehleranfälligkeit steigen, merkten einige Kritiker von Buterins Ansatz an.

Als Vitalik die Bitcoin-Community von seinen Änderungsversuchen nicht zu überzeugen vermochte, setzte er seine Ideen mit einem kleinen Kreis von ihm vertrauen Leuten in die Tat um. Nach dem der Code programmiert war und mittels Initial Coin Offering Bitcoin zu einem Wert

von damals 18 Millionen USD eingenommen wurden, wurde am 30. Juli 2015 der erste Ethereum-Block kreiert.

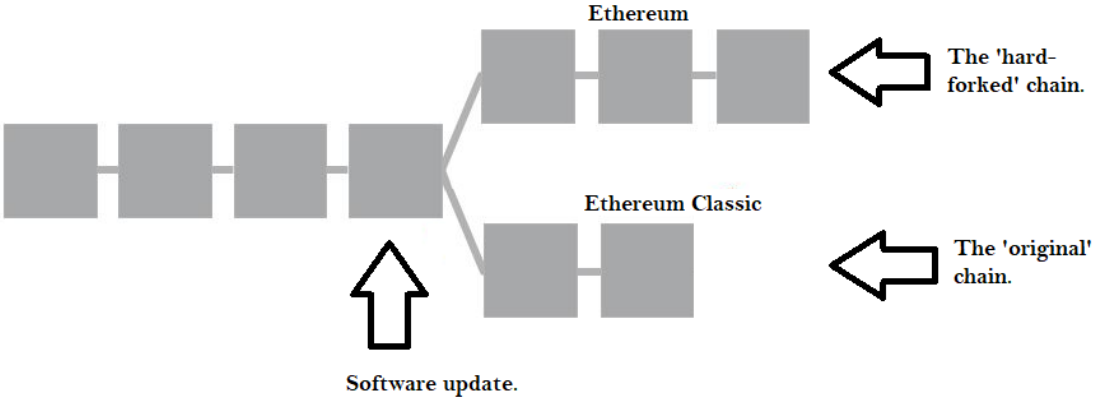
Falsche Dichotomie

Wie schon Bitcoin zuvor, zog auch Ethereum immer mehr Leute in seinen Bann – insbesondere ein grösseres Spektrum an Software-Entwicklern machten nun ihren ersten Schritt in die Krypto-Welt. Aufgrund des steigenden Interessens schoss auch der Ether-Preis regelrecht durch die Decke und die Rivalität zwischen den beiden Camps nahm zu. Einige Bitcoin-Anhänger – vielleicht ein wenig durch den Preisaufschwung bei Ether verunsichert – sahen in diesem neuen Krypto-Asset einen billigen Abklatsch Bitcoins, das den eigentlichen Wert kaum mehr treu sei. Aufseiten Ethereums sprachen einige Proponenten hingegen bereits davon, dass die programmierbare Blockchain dem Bitcoin haushoch überlegen sei und dass erstere die letztere deshalb eher früher als später obsolet machen würde. Noch heute bekämpfen sich die beiden Lager in Internetforen, auf Twitter oder an Konferenzen. Während Ethereum-Maximalisten als Häretiker geschimpft werden, sind Bitcoin-Maximalisten die Fundamentalisten der Krypto-Welt.

Mehr Akzeptanz > Größeres Netzwerk > Höherer Preis von

Die Debatte um den Titel «Einzig wahre Blockchain» ist unser er Meinung nach letztlich nichts als ein clowneskes Scheingefecht. Denn Bitcoin und Ethereum sind überhaupt keine direkten Kontrahenten, verfolgen sie doch andere Ziele. Als unabhängiges Wertaufbewahrungsmittel muss die Bitcoin-Blockchain grösstmögliche Sicherheit bieten.

Grafik 17: Hardfork von Ethereum



Quelle: Hackernoon

Das impliziert, dass Bitcoin notwendigerweise auf einer rudimentäreren Skriptsprache beruhen muss, die weniger Programmierungsmöglichkeit offenlässt, gleichzeitig aber auch die Anfälligkeit für Programmierfehler, sogenannte «Bugs» einschränkt. Der Zweck von Ethereum liegt gewissermassen darin, diesen Trade-Off genau gegenteilig aufzulösen. Einer grösseren Experimentierbarkeit und Flexibilität in der Programmierfähigkeit der Blockchain wegen wird auf der Ebene des Quellcodes auch eine grössere Fehleranfälligkeit in Kauf genommen.

Ereignisse wie der DAO-Hack, der Parity-Bug und anderer Rückschläge, die letztlich auf Programmierfehler zurückzuführen sind, dokumentieren das. Weil der Ethereum-Ansatz programmiertechnisch viel mehr zulässt, erscheint dessen Use-Case einiges breiter, was viele Ethereum-Fans daraus schliessen lässt, in Ethereum das langfristig lukrativere Projekt zu sehen. Ob sich diese Ansicht bewahrheiten wird, wird sich zeigen.

"The network effect of Bitcoin is powerful and all that matters today is securing ownership of the network, the daily price is just noise."

Mark W. Yusko

Ethereum wird heute insbesondere für den ICO-Hype von Ende 2017 verantwortlich gemacht. Dabei ist der Ton nicht selten etwas vorwurfsvoll, zeichnet sich doch für viele mittlerweile ab: Nicht nur haben Investoren in dieser Spekulationshausse viel Geld verloren, sondern wurden sie auch von etlichen ICO-Betrügern und Krypto-Scharlatanen an der Nase herumgeführt.

Vor lauter Kritik am ERC20 Token Standard geht vergessen: Dank dieses Standards kann jeder seinen Token zu geringen Kosten lancieren, ohne sich um den Aufbau einer Blockchain-Infrastruktur kümmern zu müssen. Damit hat Ethereum die Möglichkeit des Crowdfunding auf eine ganz neue, eine globale Ebene gebracht. Eine Finanzierung lässt sich plötzlich effizient, schnell und eigenständig über das Internet durchführen.

Während Bitcoin also die Geldschöpfung durch zentrale Entitäten wie Zentralbanken und Geschäftsbanken infrage stellt, liegt die revolutionäre Kraft Ethereums darin, eine echte Alternative zum eher zentralistisch organisierten Kapitalmarkt bzw. zu den Finanzintermedieren ermöglicht zu haben. Seit jeher fungieren Investmentbanken als Vermittler zwischen Vermögensverwaltern und Unternehmen oder Staaten, die eine Anleiheemissionen machen oder über ein IPO Aktien ausgeben wollen. Vor Ethereum gab es technisch keine Möglichkeit, diese zu umgehen. Heute gibt es sie. Noch spüren Investmentbanken von dieser disruptiven Kraft wenig. Ganz anders die Risikokapitalgeber[47]. Deren Geschäftsfeld wird gerade auf den Kopf gestellt, weshalb es nicht mehr ungewöhnlich ist, Risikokapitalunternehmen wie Andreessen Horowitz oder Union Square Ventures auf Pre-ICO-Investorenlisten zu finden. Die Aushängeschilder des Risikokapitalgebertum haben also bereits auf die «Ethereumisierung» des Investierens reagieren müssen – ein Schicksal das der Wall Street noch blühen dürfte.[48]

Ein dezentraler Weltcomputer

Wie Bitcoin basiert Ethereum ebenfalls auch auf einer öffentlichen Blockchain und ist daher letztlich nichts anders, als ein Netzwerk von zehntausenden geografisch verteilten Computern, die alle über das Ethereum-Protokoll kommunizieren. Da sich auf Ethereum im Gegensatz zu Bitcoin aber eben beliebige Applikationen programmieren lassen, trifft hier die Analogie eines Weltcomputers noch besser zu. Die Ethereum-Blockchain funktioniert also wie ein Computer. Einer Festplatte

—

47 Vgl. "ICOs are Disrupting VC Funding & Ethereum Coopetition is Challenging VC Unicorn Dynamics", *Voices of VR*, August 15th, 2018.

48 Vgl. "The Ethereumization Of Wall Street Is Inevitable: Expert Take", Vincent Launay, *Cointelegraph,* February 8th, 2018.

eines Computers gleich, speichert die Blockchain alles, was auf dem Ethereum-Weltcomputer passiert.

Auf einer programmierbaren Blockchain wie jener von Ethereum können Entwickler alles programmieren, was sie auf einem lokalen Computer auch programmieren können. IT-technisch handelt es sich somit um einen Computer. Der Ethereum-Weltcomputer unterscheidet sich von einem gewöhnlichen Computer jedoch insofern, als dass dieser gemäss seines Programmiercodes laufen muss und aufgrund seiner non-zentralen Struktur nur unter Inkaufnahme extremer Kosten manipuliert werden kann. Gleichzeitig liefert ein solcher Weltcomputer auch eine ungemein hohe Robustheit. Da die Ethereum-Blockchain auf zehntausenden von einzelnen Computern läuft, ergibt sich eine Redundanz. Die Ethereum-«Festplatte» existiert eben nicht nur einmal und an einem Ort, sondern ist über die ganze Welt verteilt. Das Downtime-Risiko ist daher schwindend gering.

Wozu eine programmierbare Blockchain?

Im Zusammenhang mit Ethereum fällt immer wieder der Begriff des «Smart Contract». So wird die Ethereum-Blockchain gemeinhin als jenes Blockchain-Projekt angesehen, welches das Potenzial solcher «intelligenten Verträge» als erstes erkannt und die Idee somit popularisiert hat.

"The most encouraging thing about crypto is the amount of sheer opposition."
Alex Otsu

Eine primitive Form von Smart Contracts kennt bereits die Bitcoin-Blockchain. Im Falle von Bitcoin beschränken sich diese auf die simple Übertragung von Bitcoin-Werteinheiten. Da Ethereum – wie wir gesehen haben – eine programmierbare Blockchain ist, lassen sich die Smart-Contract-Funktionen hier in der Theorie nahezu beliebig erweitern. Neben der Abwicklung von Transaktionen digitaler Werteinheiten sollen mittels eines Smart Contracts auch andere Werttitel wie Anleihen, Aktien und andere (bspw. sogar physische) Eigentumstitel transferiert werden können. Letztlich sollen die unterschiedlichsten Verträge, die unser gesellschaftliches Leben heute ausmachen, in Computercode konvertiert, in Form von Smart Contracts auf der Blockchain gespeichert und durch das Ethereum-Netzwerk in non-zentralisierter Manier ausgeführt werden, so die Vision, welche sich mit dem Aufkommen Ethereums in den Köpfen immer mehrerer Menschen festsetzt.

Die Eleganz eines Smart Contract besteht darin, dass es sich dabei um einen digitalen Vertrag handelt, der sich gemäss vordefinierter Parameter selbst exekutiert. Will heissen: Sind die Vertragskonditionen erfüllt, wird der Vertrag entsprechend seines Inhaltes ausgeführt. Hier hilft der Vergleich mit einem Warenautomaten. Man füttert den Warenautomaten mit Geld und erhält im Gegenzug die gewählte Ware. Es bedarf keiner Drittpartei, welche die Ware herausgibt. Die Theorie hinter einem Smart Contract funktioniert ähnlich: Auf Bezahlung mittels eines Smart Contracts erhält man die entsprechende Ware, eine Übertragungsurkunde, einen Führerschein oder sonstiges. Darüber hinaus definiert der Smart Contract nicht nur die Regeln und Sanktionen rund um die Vereinbarung, er setzt diese auch gleich selber durch.

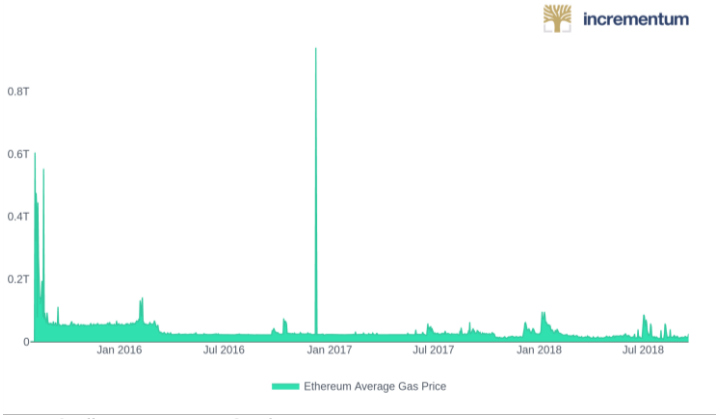
Gas – eine unerlässliche Komponente Ethereums

"The average user should pick up bitcoin to experience the future of money. To gain a glimpse into an exciting technology. To learn about how money could be in the future and also become aware of how limited money and banks are today."

Andreas M. Antonopoulos

Natürlich sind es die einzelnen Computer, welche zusammen das Ethereum-Netzwerk ausmachen, die den in einem Smart Contract definierten Programmiercode ausführen. Diese werden auch Ethereum-Clients genannt. Da Ethereum turing-vollständig ist – ein Begriff aus der Informatik – sind die Computer des Ethereum-Netzwerkes imstande, Code beliebiger Komplexität auszuführen. Gleichzeitig hat die Turing-Vollständigkeit aber auch zur Folge, dass ein Smart Contract, bzw. dessen Programmiercode, durch die ausführenden Ethereum-Clients endlos ausgeführt würde. Eine solche Endlosschleife würde die Ethereum-Blockchain allerdings funktionsunfähig machen, da bereits die Ausführung eines einzelnen Smart Contract die gesamten Ressourcen aller im Ethereum-Netzwerk partizipierenden Computer aufbrauchte.

Grafik 18: Ethereums Durchschnittlicher Gas Price



Quelle: Incrementum AG, Etherscan

Als Lösung integrierte Vitalik Buterin einen Mechanismus in Ethereum, der es den Ethereum-Clients möglich macht, jeweils die Ausführungslänge eines jeden Smart Contracts zu eruieren, um so Endlosschleifen zu verhindern. Das Stichwort hier: Gas. Jede Ausführung eines Smart Contract kostet eine bestimmte Menge Gas. Dabei handelt es sich aber bloss um eine Ausdrucksform. Hinter jedem Gas-Preis, den es für die Ausführung eines Smart Contracts zu bezahlen gilt, steckt eine gewisse Menge Ether, die Kryptowährung der Ethereum-Blockchain. Wie viel Ether es jeweils kostet, bzw. wie hoch der jeweilige Gas-Preis ist, hängt von der aktuellen Auslastung des Ethereum-Netzwerkes ab. Nicht alle Smart Contracts haben einen gleich hohen Gas-Preis. Je nach Komplexität ist die zu bezahlende Menge Ether kleiner oder grösser.

Im Prinzip ist das Gas von Ethereum mit dem Benzin eines Fahrzeuges zu vergleichen. Genauso wie das Benzin ein Fahrzeug zum Laufen bringt, sorgt Gas dafür, dass ein Smart Contract ausgeführt wird. Doch wird der Smart Contract dann eben nicht unendlich ausgeführt, sondern nur so lange bis die zur Ausführung benötigte Gas-Menge aufgebraucht ist. So wie ein Auto zum Stillstand kommt, wenn der Benzintank leer ist, definiert auch das Ethereum-Gas eine Obergrenze für die Ausführung von Smart Contracts und verhindert so Endlosschleifen.

Empfänger der über den Gas-Preis bezahlten Ether sind die Ethereum-Clients, welche für die Ausführung der Smart Contracts verantwortlich sind. Basierend auf seinem Komplexitätslevel kostet jeder Smart Contracts einen Mindestausführungspreis. Bietet man allerdings einen höheren Preis, sind die Chancen auf Verarbeitung und Ausführung grösser, da sich die Ethereum-Clients in der Regel nach dem lukrativsten Angebot richten.

Kann sich Ethereum auf dem Thron behaupten?

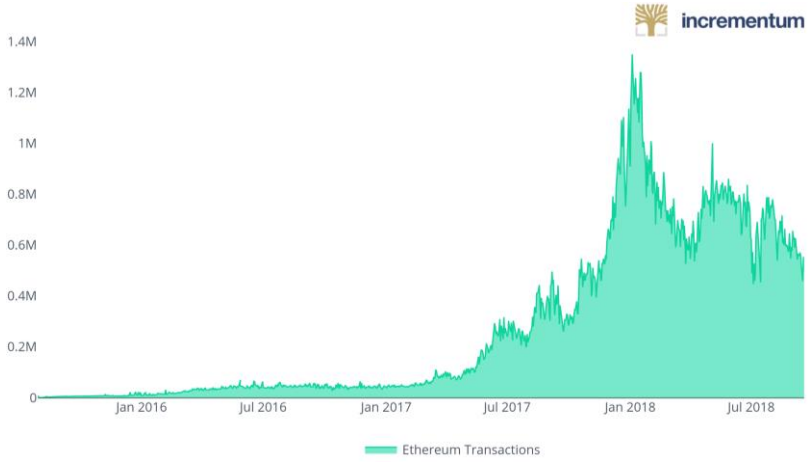
Wer Ether kauft, investiert in den ersten dezentralen „Weltcomputer". Damit will Ethereum das Rückgrat eines zukünftigen dezentralen Internets werden. Sollte das Ethereum-Netzwerk jemals diese wichtige Position erreichen, wird Ether der "Krypto-Kraftstoff" sein, der die gesamte Ethereum-Maschine antreibt. So wie das Ölzeitalter die Rockefeller-Familie und andere reich machte, könnten Ether-Besitzer aufgrund der Krypto-Revolution eines Tages die neuen "Ölbarone" werden.

"We believe that the current situation of Bitcoin is comparable to the early days of the internet. Back in the '90s it required a lot of patience to download a single song, while nowadays we are streaming movies in HD quality."

Lidia Bolla, Vision &

Ethereum ist heute (erst) drei Jahre alt. Seit der erste Ethereum-Block am 30. Juli 2015 geschaffen worden ist, hat sich die Blockchain in Sachen Marktkapitalisierung zum zweitgrössten Krypto-Asset entwickelt und zählt heute bereits über 250'000 Entwickler.[49] Bis heute sind ungefähr 1'800 DApps[50] registriert. Ethereum ist zudem zweifellos die erfolgreichste, blockchain-basierte Crowdfunding-Plattform. Von den Top 100 Token nach Marktkapitalisierung wurden 94 Prozent ursprünglich auf Ethereum aufgebaut – 13 Milliarden USD an Kapital sind auf diese Weise über Ethereum zustande gekommen. Von den Top 700 Token nach Marktkapitalisierung entfallen 87 Prozent auf Ethereum. Das entspricht 15 Milliarden von 19 Milliarden USD, die über die Ethereum-Plattform gesammelt wurden.[51]

Grafik 19: Ethereum Transaktionsvolumen im Zeitablauf



Quelle: Incrementum AG, Etherscan

—
49 Vgl. "The State of the Ethereum Network", ConsenSys, *Medium,* June 1st, 2018.
50 Vgl. "Happy third birthday to Ethereum. What's it done in life so far?", Andrew Munrow, *Finder,* July 30th, 2018.
51 Vgl. "Misconceptions in the Ether(eum) Market", Sam Cassatt, *Hackernoon,* August 22nd, 2018.

Dieses Wachstum und die daraus resultierende Dominanz hat andere Smart-Contract-Plattformprojekte auf den Plan gerufen. Obwohl Ethereum einen kometenhaften Aufstieg erlebte, ist heute klar: Damit Ethereum dezentralisierte Dienste und Applikationen in einem Ausmass handhaben kann, um gegenüber traditionellen zentralisierten Lösungen eine echte Alternative zu sein, bedarf es wirkungsvoller Skalierungsmöglichkeiten. Die Ethereum-Community hat dies erkannt und arbeitet daran – noch hat sie *den* Durchbruch aber nicht geschafft.

Hier sehen viele alternative Smart-Contract-Plattformen ihre Chance, Ethereum zuvorzukommen. Gelingt es ihnen eher und besser zu skalieren, dürfte nicht nur die alte Welt – in der Hoffnung technologische Umbrüche mitgehen zu können – sondern auch die neue Welt ihre Anwendungen in Zukunft auf einer dieser alternativen Smart-Contract-Plattform bauen.

Cardano: Wenn Wissenschafter Blockchains bauen

Die meisten Smart-Contract-Projekte versuchen Ethereum mit Geschwindigkeit den Rang abzulaufen. Nicht so Cardano – in der Krypto-Community auch als japanisches Ethereum beschrieben. Dies aber nicht etwa, weil es sich dabei um ein Projekt japanischen Ursprungs, sondern weil das Projekt in Japan lanciert worden ist und angeblich rund 95 Prozent aller ICO-Investoren im dem Land der aufgehenden Sonne beheimatet waren.[52]

"Bitcoin: a digital currency with limited and known supply, no borders, and no central group controlling it. US Dollar: a digital currency with unlimited and unknown supply, border restrictions, and controlled by a banking cabal."

Erik Voorhees

Bei Cardano wird nicht auf Schnelligkeit gesetzt. Im Gegenteil gilt der Fokus der Genauigkeit und Richtigkeit. Gegründet wurde Cardano von Charles Hoskinson, der ebenfalls bereits bei Ethereum und BitShares mitgewirkt hatte. Dass Hoskinson Mathematiker ist, schimmert bei Cardano ganz klar durch. Wohl kein anderes Smart-Contract-Projekt ist derart akademisch geprägt und auf mathematische Korrektheit aus. Für die Entwickler hinter Cardano steht die fachliche Begutachtung des Codes im Vordergrund. So ist es deren Absicht, die Cardano-Protokolle einem Peer-Review-System zu unterstellen und jeglichen Programmcode, wenn möglich, mit formaler Verifikation[53] zu validieren. Formal verifiziert ist ein Programmcode dann, wenn mathematisch nachgewiesen ist, dass er für alle Inputs korrekt ist. Mittels formaler Überprüfung ist zwar (noch) nicht bewiesen, dass ein Code das tut, was er tun soll, doch ist bewiesen, dass gewisse Fehler ausgeschlossen werden können. Diese Art der formalen Verifikation ist ein neuer Bereich, und obwohl sich auch andere Projekte vermehrt daran orientieren, will Cardano hier führend sein.

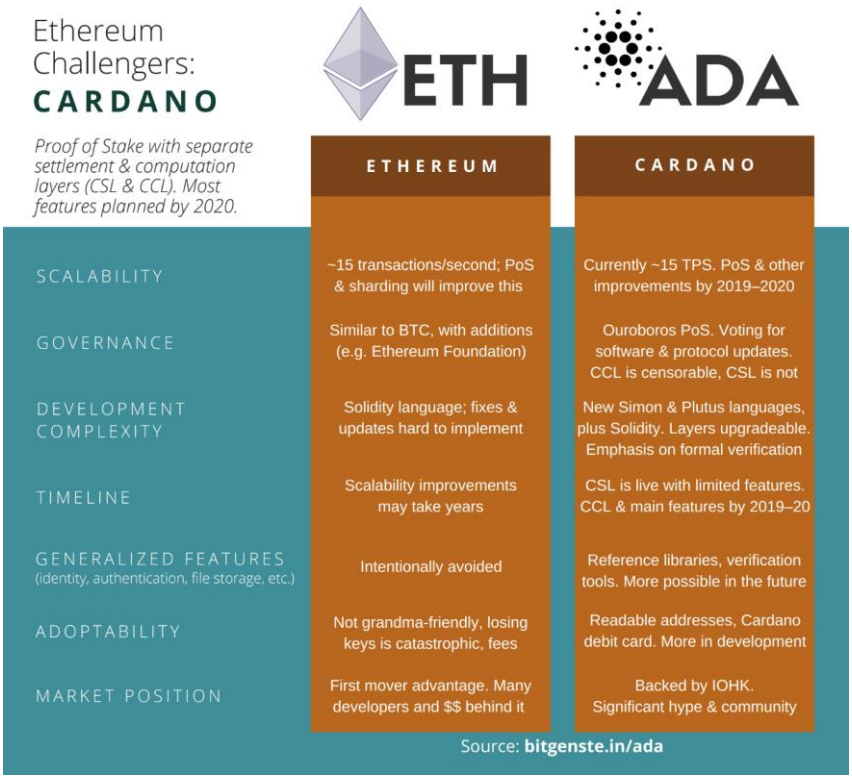
Cardano läuft zwar bereits auf einem eigenen Mainnet, viele der Eigenschaften und Merkmale dieser Smart-Contract-Plattform sind allerdings noch in der Entwicklung. Für einen Aussenstehenden gibt es daher noch wenig gesicherte Informationen. Schon heute scheint klar zu sein: Während bei vielen anderen Projekten die Buchführung von Werttransaktionen sowie das Ausführen von Smart-Contract-Befehlen zusammenfallen, sind diese Prozesse bei Cardano auf zwei unterschiedliche «Layers» getrennt. Da gibt es zum einen den «Settlement

—
[52] Vgl. "Cardano the Japanese Ethereum", Blox_Official, *Reddit,* February 2018.
[53] Vgl. "Why Cardano", Cardano Team, *whycardano.com*

Layer» für den Werttransfer sowie den «Computational Layer» für die Anwendung von Smart Contracts. Von dieser Aufspaltung verspricht man sich bei Cardano vor allem entscheidende Aspekte wie Skalierbarkeit, Privatsphäre sowie regulatorische Fragen und Compliance[54] besser unter einen Hut bringen zu können. Die beiden unterschiedlichen «Layers» basieren zudem auf zwei verschiedenen Programmiersprachen. Die eine Sprache ist spezifisch und begrenzt, damit aber auch weniger anfällig für Bugs und anderen unvorhersehbaren Programmierfehlern, während die andere flexibler ist. Je nach Anwendung kann dann die eine oder die andere Programmiersprache verwendet werden, weshalb Cardano hier eine gewisse Auswahl bietet.

Ob dieser sorgfältige Weg der Peer-Review-Begutachtung und der formalen Verifikation in der doch ungemein schnelllebigen Krypto-Welt zum Erfolg führen wird, kann nur die Zeit zeigen. Vielleicht schüttet man bei Cardano das Kind aber auch mit dem Bade aus, hat doch die Methode der Peer-Review-Begutachtung auch ihre auserlesenen Kritiker. Deren Argument: Akademische Begutachtungsprozesse liefern bei weitem nicht immer Gewissheit und sind daher den Aufwand oftmals nicht wert. Selbst ein solcher Vorbehalt täuscht jedoch nicht darüber hinweg, dass man bei Cardano philosophisch, mathematisch sowie technisch saubere Arbeit leisten will. Folglich könnte das Projekt der Krypto-Welt in Zukunft noch einige interessante Ansätze bezüglich Smart-Contract-Plattformen liefern.

Grafik 20: ETH VS ADA



Quelle: Bitgenste

54 Vgl. „Regulation", Cardano, *whycardano.com*

China nimmt es mit Ethereum auf

Ein weiteres Projekt, das eine Plattform für das Internet der Zukunft errichten will, stammt aus China. Vormals als Antshares bekannt, wechselte das Projekt im Juni 2017 seinen Namen auf NEO und sorgte dann gleich für Furore unter den Krypto-Investoren. Alsbald kam unter diesen jedoch die Frage auf: Kann ein Blockchain-Projekt aus China überhaupt Erfolg haben, wo doch die Regierung Chinas 2017 dezidiert Stellung gegen Bitcoin und ICOs bezogen hatte?

Natürlich ist das mit China und seinen eisernen Massnahmen immer so eine Sache. Denn wer genau hinschaut, erkennt: China hat sich nicht generell gegen die Blockchain-Technologie gestellt, immerhin hat sich die Zentralbank Chinas in seinem Fünfjahresplan für das Ausloten der Möglichkeiten der Blockchain-Idee stark gemacht. Im Grunde genommen interessiert sich die chinesische Regierung einfach für jene Blockchain-Projekte, die berechenbar und damit steuerbar sind. Und genau hier scheint NEO, wohl aus gutem Grund und in beabsichtigter Weise, anzusetzen.

"Bitcoin is at the same stage as the Internet in 1992-1993. At that time, it took UNIX command-line skills to send email. No way near ready for mainstream adoption."

Andreas M. Antonopoulos

Es ist das erklärte Ziel der Verantwortlichen hinter NEO auf Geschwindigkeit und regulatorische Compliance zu setzen. Bei NEO will man die Blockchain-Technologie dazu nutzen, Vermögenswerte aller Art zu digitalisieren, die Verwaltung und den Handel derselben mittels Smart Contracts zu automatisieren, um so die Strukturen für eine sogenannte Smart Economy ins Leben zu rufen. Hierfür ist die Lösung einer digitalen Identität unverzichtbar, weshalb der NEO Council – das Organ zur Förderung des NEO-Ökosystems – mit PikcioChain eine GDPR-konforme digitale Identitätslösung unterstützt. Baut eine Blockchain-Plattform auf Pseudo- oder gar Anonymität, ist sie für einen Staat – vor allem einer wie China – sowie Unternehmen von geringem Interesse, da regulatorische Erfordernisse so kaum erfüllt werden können.

Gleichzeitig legt NEO seinen Fokus aber auch auf Lösungen zur Entwicklung der Privatsphäre und des Datenschutzes. So will NEO über seine Partnerschaft mit OnChain, ein Unternehmen zur Förderung von Blockchain-Projekten, Unternehmen den Datenschutz ermöglichen. Gegründet von Da HongFei und Erik Zhang, die ebenfalls NEO ins Leben gerufen haben, arbeitet OnChain mit Regierungen und Unternehmen zusammen, um öffentliche und private Blockchains zu schaffen, welche dereinst über die dezentrale Netzwerkarchitektur (DNA) von OnChain mit dem NEO-Ökosystem verbinden sollen.

Wie Ethereum und andere Smart-Contract-Projekte verfügt auch NEO bereits über eine Open-Source-Gemeinschaft für Entwickler und Programmierer mit dem Namen City of Zion. Sie zielt Interoperabilität von NEO mit NEOX ab und hat eine ICO-Plattform, die Zahlungslösungen, dezentralisierte Handelsbörsen und mehr erlauben soll.

Der Konsensus-Mechanismus von NEO nennt sich Delegated Byzantine Fault Tolerance oder dBTF. Hinter diesem Begriff verbirgt sich letztlich ein uns aus der traditionellen Welt bekanntes Governance-Modell: dasjenige einer repräsentativen Demokratie. Die NEO-Token-Inhaber bestimmen Delegierte, sogenannte Buchhalter („Accountants“), die für Konsens sorgen und das Netzwerk so aufrechterhalten. Insgesamt gibt es sieben dieser Buchhalter. Gegenüber Ethereum ist die Anzahl der das Netzwerk validierenden Knoten um einiges geringer. Zudem haben die NEO-Buchhalter erst noch digitale Identitäten und echte Namen – sind also für jedermann ersichtlich, während die Netzwerkknoten bei Ethereum anonym sind. Dass bei NEO die Buchhalter bekannt sind, macht im Hinblick auf die Ziele dieses Projektes gewiss Sinn. Um den regulatorischen Erfordernissen gerecht werden zu können, muss das Blockchain-Projekt über diesen Grad an Transparenz verfügen.

Der ICO-Markt im zweiten Quartal 2018 machte trotz regulatorischer Unsicherheit und Volatilität 45% bzw. 31% des traditionellen IPO-Marktes und des Risikokapitalmarktes aus.

Über das Modell der delegierten Buchhalter kann verhindert werden, dass Transaktionen von allen Knoten im Netzwerk validiert werden müssen. Auf diese Weise vermag NEO eine höhere Anzahl an Transaktionen abzuwickeln als Ethereum. Darüber hinaus sind NEO-Transaktionen final. Das bedeutet: Forks, als Aufspaltungen der Blockchain in mehrere Ketten sind unmöglich. Erreichen die Buchhalter einen Konsens von 66 Prozent, wird die zu validierende Transaktion nicht nur in die Blockchain aufgenommen, sondern endgültig und kann nicht durch einen Fork obsolet gemacht werden.

Ein weiterer Unterschied zwischen Ethereum und NEO betrifft die Programmiersprachen zur Entwicklung von Smart Contracts. Ethereum setzt hier Solidity voraus - eine speziell für Ethereum entwickelte Programmiersprache. NEO hingegen unterstützt eine Vielzahl der bekanntesten Programmiersprachen. Bei NEO sieht man darin vor allem den Vorteil, traditionellen Entwickler das Programmieren auf der NEO-Blockchain zu ermöglichen, ohne dass dazu eine neue Programmiersprache erlernt werden muss.

Die Unterschiede sind nicht zu übersehen

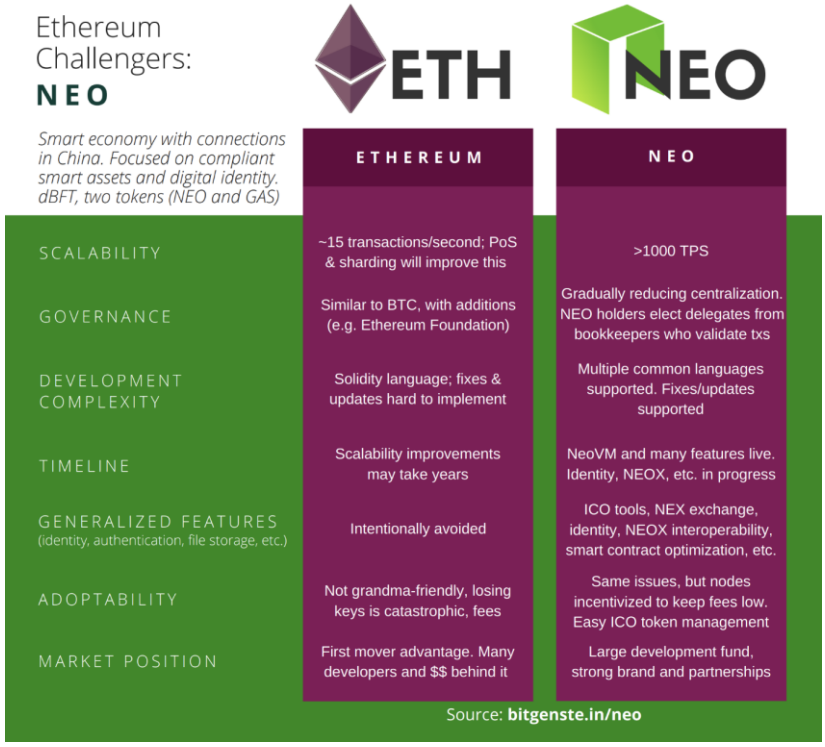
Besonderes interessant ist die Tatsache, wonach NEO ähnlich wie Ethereum das Gas-Prinzip kennt. Während bei Ethereum der Ether-Token allerdings auch als Gas Verwendung findet, verfügt NEO neben dem NEO-Token noch über einen separaten Gas-Token.

Der NEO-Token verleiht Mitbestimmungsrechte an der NEO-Plattform. Wie bereits erwähnt, sind NEO-Token-Inhaber dazu berechtigt, „Buchhalter“ zu bestimmen. Der Anteilscharakter des NEO-Token spiegelt sich auch darin wider, dass dieser nicht teilbar ist.

Der GAS-Token hingegen dient der Bezahlung aller Operationen wie Transaktionen im NEO-Netzwerk und fungiert so ebenfalls als Krypto-Fuel. Die Bezahlung in Form der Gas-Token geht zum einen an die Buchhalter, zum anderen aber auch an alle NEO-Token-Inhaber. Zur Einforderung der Gas-Token ist ein persönliches NEO-Wallet von Nöten - wie beispielsweise NEON.

Diese Entkopplung von NEO und GAS besticht vor allem durch die Tendenz der Buchhalter, die Transaktionsgebühren niedrig zu halten. Der Grund ist der folgende: Hohe Transaktionsgebühren, die nur den Buchhaltern zu Gute kommen, verhindern, dass Operationen auf der NEO-Blockchain durchgeführt werden. Je weniger Operationen, desto weniger Belohnung erhalten NEO-Token-Inhaber. Das bewegt diese dazu, für Buchhalter zu stimmen, die wiederum die Transaktionsgebühren niedrig halten.

Grafik 21: ETH vs NEO

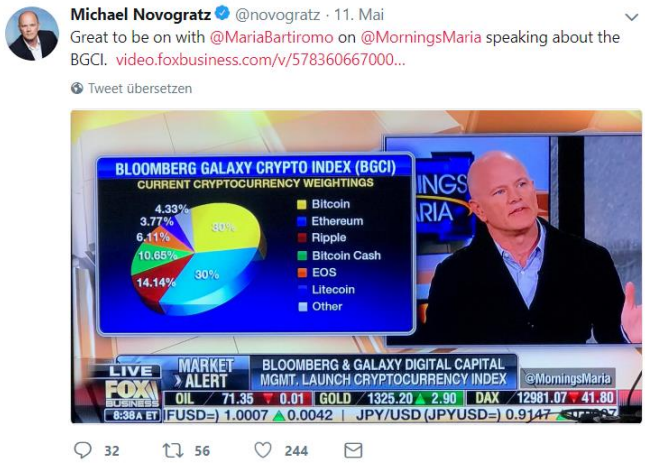


Quelle: Bitgenste

"Money is one of the greatest instruments of freedom ever invented by man. It is money which in existing society opens an astounding range of choice to the poor man, a range greater than that which not many generations ago was open only to the wealthy."

F.A. Hayek

Es sind solche Eigenschaften, welche NEO zu einer interessanten Smart-Contract-Plattform machen. Aus einer Makrosicht unterscheidet sich diese Plattform allerdings von Ethereum in einem grundlegenden Aspekt: Allem Anschein hat sich NEO in die Dienste des chinesischen Staats gestellt, weil man sich davon einiges verspricht. Folglich ist NEO seinem Wesen nach ein geplantes und von oben nach unten orchestriertes Unterfangen, das vor allem durch den NEO Council im Interesse des chinesischen Staates vorangetrieben scheint. Aus Sicht von NEO hat diese Strategie denn auch intakte Erfolgschancen. Wer sich auch nur in China selbst durchsetzt, und einen Markt von 1,4 Milliarden Menschen bedient, kann sein Vorhaben bereits als Erfolg verbuchen.



Novogratz prognostizierte, dass der niedrigste Preis von Bitcoin in dieser Baisse am 13. September 2018 bei 6,350 $ lag. Leider konnte Bitcoin nicht über dieser Grenze bleiben und fiel am 19. September 2018 unter seine Prognose von 6,200 $.

Und falls sich im Westen eine oder mehrere andere Smart-Contract-Plattform etablieren sollten, würde dies nicht das Ende NEOs bedeuten. Techgiganten aus den USA wie Facebook oder Amazon liefern hierfür ein gutes Beispiel. Obschon ihre Dominanz in der Welt ausserhalb Ostasiens immer grösser wird, haben sie im Land der Mitte gegen die heimischen Plattformen so gut wie keine Chance. Weshalb sollte das im Bereich der Smart-Contract-Plattformen anders sein?

Anders Ethereum, auf das zwar auch Interessensgruppen wie Consensys oder die Ethereum Enterprise Allianz Einfluss nehmen, dessen Ökosystem nichtdestotrotz die Philosophie organischen Wachstums hochzuhalten scheint. In diesem Sinne erweckt die Ethereum-Plattform vielmehr den Eindruck, sich gewissermassen als spontane Ordnung zu gebärden. Aufgrund dieser unterschiedlichen Ausrichtungen sind die beiden Projekte nur schlecht miteinander zu vergleichen. Während NEO eine fortgeschrittene Zukunft anstrebt, die auf die bestehenden Akteure und Gegebenheiten angepasst ist, arbeitet man bei Ethereum an einer neuen Zukunft, an der sich die gegenwärtigen Unternehmen und Staaten dereinst werden ausrichten müssen.

EOS - Ethereum's grösster Konkurrent?

Dem Drama der Krypto-Welt gerecht werdend, tragen einige dieser Smart-Contract-Kontrahenten daher auch den Namen «Ethereum-Killer». Das wohl prominenteste dieser Projekte ist EOS, von einigen auch «Ethereum on Steroids» genannt. Während Ethereum ein etabliertes Blockchain-Projekt mit einer voll funktionsfähigen Plattform ist, steckt EOS noch in den Kinderschuhen. Im Anschluss an das grösste je auf Ethereum durchgeführte ICO, bei dem eine Rekordsumme von ungefähr vier Milliarden USD zusammengekommen ist, führte EOS im Juni dieses Jahres seinen Mainnet-Launch durch und wechselte so von einem ERC-20-Token basierend auf Ethereum auf eine eigene Blockchain, die EOS-Blockchain.

Obschon EOS letztlich auch das Programmieren von Smart Contracts ermöglicht, gibt es doch einige gewichtige Unterschiede. So werden Ethereum-Smart-Contracts beispielsweise mit JavaScript / Solidity entwickelt. Smart Contracts auf der EOS-Blockchain hingegen müssen in C++ geschrieben werden. Da diese Programmiersprache nicht ganz so gebräuchlich und benutzerfreundlich ist, sehen einige Programmierer hier eine Eintrittsschwelle, die EOS gegenüber anderen Smart-Contract-Plattformen benachteiligen könnte. Gleichzeitig soll EOS künftig die Implementierung von C/C++ Bibliotheken aufweisen, was die Möglichkeiten von Entwicklern erheblich erweitern würde.

Anders als Ethereum basiert der Konsens-Mechanismus von EOS auf dem sogenannten "Delegated Proof of Stake" oder kurz DPoS. Diese Art der Konsensus-

Findung wurde von EOS-Gründer Dan Larimer erfunden. Wie schon bei NEO berechtigt DPoS jeden EOS-Token-Inhaber dazu, Validatoren in einer Abstimmung zu wählen. Analog zur Devise «ein Mensch, eine Stimme gilt hier: Ein Token, eine Stimme. Das heisst auch: Wer über mehr EOS-Token verfügt, hat grösseren Einfluss auf das Abstimmungsergebnis[55].

Die Validatoren werden bei EOS Block-Produzenten genannt, da sie in gegenseitiger Übereinstimmung die EOS-Blöcke produzieren und auf ihre Richtigkeit prüfen, um so die Funktionalität der Blockchain aufrechtzuerhalten. Insgesamt haben die EOS-Token-Inhaber 21 Block-Produzenten zu bestimmen, die effektiv dazu befähigt sind, die Blockchain zu verwalten und damit das Netzwerk sicher und funktionsfähig zu halten. Für ihre Arbeit werden sie mit neuen EOS-Token belohnt. Leistet ein Block-Produzent keine gute Arbeit und validiert beispielsweise ungültige Transaktionen, kann ihm der Status als Block-Produzent entzogen werden. Die Abstimmungen werden ungefähr alle zwei Minuten durchgeführt. Grundsätzlich ist es somit möglich, Validatoren alle paar Minuten auszuwechseln.[56] Denn neben den 21 tätigen Block-Produzenten gibt es ungefähr hundert weitere Block-Produzenten im Standby-Modus. Wird ein Block-Produzent aus welchen Gründen auch immer abgewählt, rückt einer aus der Reserve nach.

In einer szenariogewichteten Analyse, wenn 8% der weltweit getätigten Investitionen in Wertsachen in Bitcoin investiert würden, würde der Preis von Bitcoin in den nächsten acht Jahren 65.000 US-Dollar pro Münze betragen.

Die Idee der EOS-Gründer hinter dieser Struktur ist folgende: Weil die Aufgabe der tatsächlichen Verarbeitung und Validierung der Transaktionen an nur 21 Block-Produzenten[57] abdelegiert wird, soll das Grundprotokoll und damit die eigentliche Blockchain selber skaliert werden können, um so Millionen von Transaktionen pro Sekunde zu ermöglichen. In der Realität vermochte das EOS-Projekt bis heute ein Maximum von 3'097 Transaktionen pro Sekunde erfolgreich abzuwickeln[58]. Im objektiven Vergleich schneidet EOS bis lang also deutlich besser ab als Ethereum, obschon das eigentliche Ziel von Millionen von Transaktionen kaum erreicht ist. EOS ist aber nicht nur in der Lage, eine grössere Menge an Transaktionen pro Sekunde abzuwickeln – auch die Transaktionsgeschwindigkeit ist höher. Schon nach nur einer Sekunde erreicht die Blockchain Endgültigkeit über einen eben neu hinzugefügten Block.

Inflationierung als Belohnung

Interessanterweise sind bei EOS keine Transaktionsgebühren vorgesehen. Diese werden von den EOS-Gründern eher als hinderlich angesehen. So liest man in diesem Zusammenhang oft von Facebook: Über 50'000 Likes verarbeiten die Facebook-Server pro Sekunde und letztlich stellt jeder dieser Likes eine Transaktion dar. Hätte man auf einer blockchain-basierten Social-Media-Plattform jedes Mal eine Transaktionsgebühr zu bezahlen, dürfte dies dem Kundenerlebnis

—
55 Vgl. "EOS Block Producer FAQ", Ben Sigman, *Medium*, May 8th, 2018.
56 Vgl. https://medium.com/@bensig/eos-block-producer-faq-8ba0299c2896
57 Vgl. "Everything they don't want you to know about EOS.", Thijs Maas, *Hackernoon*, June 9th, 2018.
58 Vgl. „EOS Releases New Version, Transaction Speed May Be Exaggerated", Christine Masters, *Cryptovest*, July 20th, 2018.

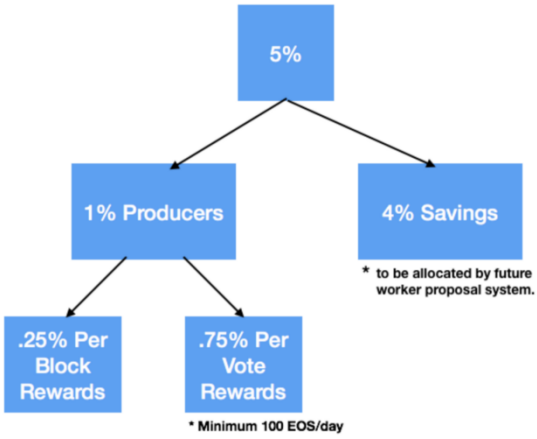
abträglich sein. Während bei Ethereum die Miner, welche Transaktionen validieren und an die Blockchain anfügen, für diese Leistung mittels Transaktionsgebühren entlohnt werden, werden die Validatoren innerhalb des EOS-Systems für ihre Überprüfungsarbeit deshalb nicht mit Transaktionsgebühren entlohnt. Fairerweise muss gesagt werden: Bei Ethereum arbeitet man ebenfalls an Second- oder Third-Layer-Skalierungslösungen, welche die eben beschriebene Problematik entschärfen sollen.

"30 years from now, Bitcoin will be the structure to power organizations without leaders."

Mike Hearn

Wie aber werden die EOS-Block-Produzenten stattdessen entlohnt? Sie erhalten durch das EOS-Protokoll neu geschaffene EOS-Tokens. Jedes Jahr werden fünf Prozent zusätzliche EOS-Token produziert. Konkret heisst das: Der EOS-Token-Bestand wird pro Jahr um fünf Prozent inflationiert. Von diesen fünf Prozent erhalten die Block-Produzenten jeweils ein Prozent als Belohnung für die Validierung der Transaktionen. Die restlichen vier Prozent kommen in einen separaten Pool, von dem Vorschläge zur Verbesserung und Weiterentwicklung der EOS-Blockchain finanziert werden[59]. Bei EOS soll zudem sichergestellt werden, dass Block-Produzenten ihren Verdienst nicht mit jenen teilen können, von denen sie auch ihre Stimmen erhalten. Das «Kaufen von Stimmen» soll also unterbunden werden.

Grafik 22: Verteilung der "EOS Inflation"



Quelle: Medium @bensig

Krypto-ökonomisch betrachtet, dienen Transaktionsgebühren nicht nur um Anreize zu setzten, sondern halten sie bösartige Akteure auch davon ab, das Blockchain-Netzwerk mittels unnötig vielen Transaktionen zu überlasten. EOS hingegen verhindert derartige Spam-Attacken damit, dass die Blockchain-Bandbreitennutzung von der Anzahl EOS-Token abhängig ist. Wer ein Prozent aller Token besitzt, hat Anspruch auf ein Prozent der gesamten Bandbreite des Netzwerkes[60]. Um die Chancen auf eine gezielte Netzwerküberlastung zu erhöhen,

—
59 Vgl. „How EOS Block Producers are Paid", Steve Floyd, *Medium,* May 21st, 2018.
60 Vgl. „The Cryptoeconomics of EOS vs Ethereum", Ian Macalinao, *Medium,* May 24th, 2018.

muss der Angreifer seinen Besitz an EOS-Token steigern, was immer grössere Kosten verursacht. Spam-Attacken sind daher nicht ausgeschlossen, wohl aber ökonomisch kostspielig.

Wer auf Ethereum eine DApp (dezentralisierte Applikation) entwickeln will, nimmt hierfür gewissermassen die Rechenleistung der Ethereum-Miner in Anspruch und bezahlt diese mit dem bereits genannten Ether-Gas. EOS hingegen basiert auf einem Besitzmodell: Hält man ein Tausendstel des EOS-Netzwerkes, verfügt man auch über einen Tausendstel der auf EOS-Blockchain vereinigten Rechenleistung. Wer für das Hosten einer DApp beispielsweise zehn Prozent der gesamten EOS-Rechenleistung beansprucht, muss folglich auch zehn Prozent der gesamten EOS-Tokenanzahl besitzen. Dieses Besitzmodell ermöglicht es DApp-Entwicklern beispielsweise, ihre Hosting-Kosten jederzeit realistisch einzuschätzen.

Angriff auf Ethereums derzeitige Raison d' être

"Bitcoin, having no counterparty risk and no reliance on any third-party, is uniquely suited to play the same role that gold played in the gold standard. It is a neutral money for an international system that does not give anyone country the "exorbitant privilege" of issuing the global reserve currency."

Saifedeam Ammous

EOS tritt auch dafür an, das Konzept des Crowdfunding abermals zu revolutionieren. Dabei sollen vor allem die Mängel von Initial Coin Offerings (ICO) ausgemerzt werden. Über die Ethereum-Plattform lassen sich heute via ICO – auch Token Sale genannt – finanzielle Mittel direkt sammeln. Man gibt einen Token aus und erhält dafür im Gegenzug Ether, Bitcoin oder auch andere Kryptowährungen. Nicht zu vermeiden ist, dass auch Hochstapler, Betrüger und Scharlatane auf diese Weise finanzielle Mittel einnehmen. Es ist die Hoffnung von EOS-Sympathisanten, dass Krypto-Projekte längerfristig von Ethereum wegmigrieren und stattdessen für das Crowdfunding zu EOS wechseln. So geschah es beispielsweise mit Everipedia, einem for-profit Konkurrenten von Wikipedia[61].

Das EOS-Ökosystem kennt keine ICOs oder Token Sales, sondern nur den Airdrop. Will sich ein Projekt über die EOS-Blockchain finanzieren, gibt es seine auf EOS-basierenden Token via Airdrop umsonst an die EOS-Community weiter. Nachdem die Token des Projekts mittels Airdrop verteilt worden sind, soll der Markt den Wert der Token nach dem Gesetz von Angebot und Nachfrage bestimmen. Das Team hinter dem Projekt kann dann einen Prozentsatz an eigenen Token verkaufen, um so Geld für das Projekt zu sammeln. Wie aber ein über einen Airdrop verteilter Token ohne Kapital überhaupt erst an Wert gewinnen und somit durch den Markt akzeptiert werden soll, scheint etwas unklar.

Hier dürfte allenfalls der innerhalb des EOS-Ökosystems geschaffene Risikokapitalfonds zum Zug kommen. Hinter diesem Fonds steht das Unternehmen Block.one, das 2017 das ICO für den EOS-Token gemacht hat. Der Risikokapitalfonds soll dazu dienen, strategische Investitionen in unterschiedliche Projekte zu tätigen, die auf der EOS-Blockchain bauen. Es liegt nahe, dass über diesen Risikokapitalfonds in vielversprechende Projekte investiert wird, die auch einen Airdrop über die EOS-Blockchain durchführen wollen. Natürlich drängt sich dann die Frage auf, wie stark Block.one das Crowdfunding über EOS beeinflusst.

—
[61] Vgl. „Decentralized Wikipedia rival ditches Ethereum to launch on the EOS blockchain", *The Next Web,* August 9th, 2018.

Immerhin findet durch den Risikokapitalfonds eine gewisse Vorselektion statt, die es bei Ethereum so nicht gibt.

Hierin zeigt sich sodann das Dilemma: Entweder man nimmt keinen Einfluss auf das Crowdfunding. So wird man dem Image einer uneingeschränkten Blockchain gerecht, auf die Gefahr hin, Betrügereien in Kauf nehmen zu müssen. Oder man trifft eine Vorselektion, um eben diese Betrügereien zu unterbinden, im Wissen eine gewisse Kontrolle und Zensur über die Blockchain auszuüben.

Wie hast du's mit der Dezentralisierung?

"So in many ways, virtual currencies might just give existing currencies and monetary policy a run for their money. The best response by central bankers is to continue running effective monetary policy, while being open to fresh ideas and new demands, as economies evolve."

Christine Lagarde, IMF

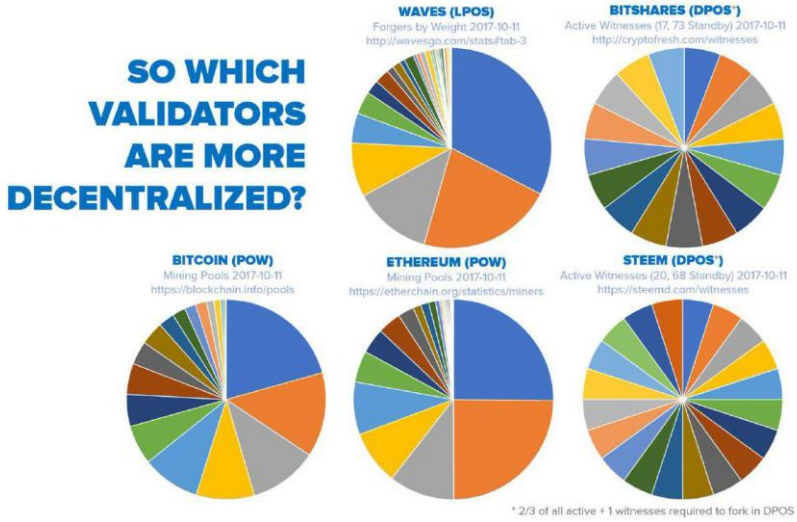
Die entscheidende Frage, die sich Krypto-Investoren heute stellen: Wer setzt sich langfristig durch? Ethereum oder EOS? Um heute schon eine Antwort zu finden, wird überall nach möglichen Anhaltspunkten gesucht. So fokussieren sich die Anleger beispielsweise auch auf die jeweils prominentesten Köpfe hinter den beiden Projekten: Der Kampf zwischen Ethereum und EOS wird auf diese Weise auch zu einem Kampf zwischen Vitalik Buterin und Dan Larimer gemacht. Dabei berufen sich einige Ethereum-Anhänger auf den angeblich astronomisch hohen Intelligenzquotienten Buterins, den ihn zu einem noch grösseren Genie als Larimer machen würde. Die Gegenseite verweist derweil auf die Krypto-Projekte BitShares und Steem, die beide der Feder Larimers entsprungen sind und ihn deshalb zum Triumph führen würden. Letztlich sind diese Vergleiche zwar interessant, doch haben sie wenig Aussagekraft in Bezug auf die Zukunft der beiden Smart-Contract-Projekte.

Etwas aufschlussreicher sind projekt-spezifische Debatten, die unter anderem durch Vitalik Buterin und Dan Larimer angestossen worden sind. In der theoretischen Auseinandersetzung rangiert an oberster Stelle die Frage der Dezentralisierung. Bei der EOS-Blockchain ist es letztlich eine vergleichsweise kleine Anzahl an Knoten, welche das Netzwerk Instand halten. In einer Welt wie jener von Krypto, die sich die Dezentralisierung gesellschaftlicher Strukturen auf die Fahne geschrieben hat, weckt ein Blockchain-Konzept mit nur 21 Block-Produzenten natürlich Argwohn. Ist EOS dezentralisiert genug oder erinnern die 21 Block-Produzenten nicht eher an ein Kartell oder eine Oligarchie? Noch immer halten es viele ehrliche Krypto-Kenner für eine technische Unmöglichkeit, dem Blockchain-Trilemma, wonach es inhärente Trade-offs zwischen Sicherheit, Skalierbarkeit und Dezentralität gibt, auf der Ebene des Basis-Protokolls zu entkommen.

Aufseiten EOS gibt es einige Stimmen, für die Dezentralisierung kein absoluter Wert ist. Da Dezentralisierung immer mit rechnerischen sowie ökonomischen Kosten verbunden sei, müssten diesbezüglich Kompromisse eingegangen werden, um gleichwohl das Ziel der Massenskalierung von DApps erreichen zu können. EOS sei letztlich gerade so stark dezentralisiert, wie es die Skalierungsabsicht bedürfe. Dass es gerade 21-Blockproduzenten sind, sei auf die bisherigen Erfahrungen zurückzuführen, die Larimer mit seinen anderen DPoS-System «BitShares» und «Steem» gemacht hat. In Stein gemeisselt - oder besser im Code festgeschrieben - sei diese Zahl deshalb nicht. Im Lichte neuer Erkenntnisse könne diese auch abgeändert werden, so deren Argumente.

Andere Verfechter von EOS halten die EOS-Blockchain überhaupt nicht für weniger dezentralisiert als Ethereum. So weisen sie darauf hin, dass bei Ethereum drei Parteien mehr als 50 Prozent der gesamten Hashing Power[62] auf sich vereinigten. Würden diese drei Akteure also zusammenspielen, könnten die Ethereum-Blockchain erfolgreich angegriffen und Transaktionen doppelt ausgegeben werden. Darüber hinaus hätten Larimers frühere Projekte «BitShares» und «Steem» gezeigt, dass DPoS-Systeme dezentralisierter seien, da die Miner bei Ethereum oder Bitcoin aufgrund skalenökonomischer Tatsachen eine inhärente Zentralisierungstendenz aufweisen würden.

Grafik 23: Dezentralisierungsgrad mehrerer Validatoren



Quelle: Steemit @adamantine

"Bitcoin has come down below its 200-day moving average, and that is important because the currency has been going up at 170% percent per annum for six years...It's come off 65 percent since its highs, and if you put 100 bucks in each of the four times it's touched its 200-day moving average, you'd have a 285 percent return...it's a screaming buy right now."

Dan Morehead, CEO Pantera Capital

Letztlich lässt sich die Dezentralisierungsdebatte wohl kaum jemals abschliessend beantworten. Es gibt schlichtweg zu viele Parameter innerhalb verteilter Konsens-Systeme, als dass sich die Krypto-Gemeinschaft jemals auf eine einheitliche Definition von optimaler Dezentralisierung einigen könnte. Der offensichtlichste Parameter – die Anzahl der Netzwerk-Knoten – ist nur eine Möglichkeit, den Grad an Dezentralität zu quantifizieren. Doch selbst dieser hat seine Tücken, bedeutet Quantität eben nicht immer Qualität: 1'000 Netzwerk-Knoten, die sich alle in einem Land befinden, sind kaum dezentraler als 21 Validatoren, die sich in den verschiedensten Jurisdiktionen auf der ganzen Welt befinden.

Neben dem Dezentralisierungsgrad wird bei öffentlichen Blockchains wie Ethereum oder EOS auch die Frage der Immutability oder Unveränderlichkeit heiss diskutiert. Unter dem Namen von «Code is Law» argumentieren einige: Eine öffentliche, nicht manipulierbare Blockchain dürfe niemals rückwirkend geändert werden, da eine solche Blockchain eben gerade nicht unveränderbar und daher als manipulierbar anzusehen sei. Würde eine öffentliche Blockchain einmal geändert, öffne das der Willkür Tür und Tor und würde somit den Charakter einer unveränderbaren Blockchain schliesslich ad absurdum führen.

—
[62] Hash Rate, auch Hash Power, meint die Menge an Arbeit (eigentlich Strom), welche die Miner aufwenden, um das Ethereum-Netzwerk aufrechtzuerhalten.

Bei Ethereum wurden diese Fragen im Rahmen des DAO-Hacks bereits gründlich debattiert. Man entschied sich dafür, die Blockchain via Hard-Fork in Ethereum und Ethereum Classic aufzuspalten. Letztere ist jene Blockchain, bei welcher der DAO-Hack nicht rückgängig gemacht wurde, um so das Prinzip von «Code is Law» einzuhalten. Aufgrund dieses Vorfalls bekunden einige Krypto-Enthusiasten noch immer Mühe mit der breiten Ethereum-Community und halten Ethereum für eines jener Projekte, das sich selber untreu geworden ist.

"The better the money is at holding its value, the more it incentivizes people to delay consumption and instead dedicate resources for production in the future, leading to capital accumulation and improvement of living standards."

Saifedeam Ammous

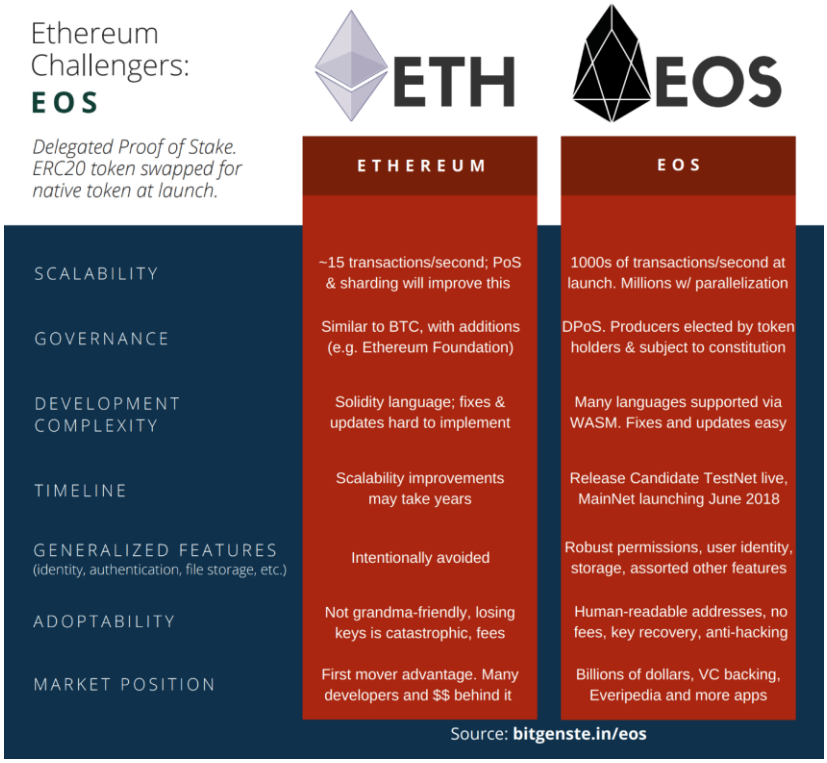
Um es überhaupt nicht zu derartigen Auseinandersetzungen und potenziell bedrohlichen Hard-Forks kommen zu lassen, hat sich das EOS-Projekt dafür entschieden, den Code als nicht unantastbar anzusehen. Im EOS-Whitepaper stehen daher folgende Zeilen:

"Manchmal verhält sich ein Smart Contract auf eine anormale oder unvorhersehbare Weise und funktioniert daher nicht wie beabsichtigt; manchmal kann eine Anwendung oder ein Konto einen Programmierfehler entdecken, der den Verbrauch einer unangemessenen Menge an Ressourcen möglich macht. Da solche Probleme nicht zu vermeiden sind, haben die Block-Produzenten die Möglichkeit, solche Situationen zu korrigieren."[63]

Bei den Gründern von EOS argumentiert man, dass die Block-Produzenten nur bei Fehlern intervenieren. Skeptiker halten dagegen, dass die Beurteilung von Fehlern letztlich stets subjektiv sei. Solche Bestimmungen würden bei EOS eine stets vorhandene Hintertür offenlassen, die Missbrauch nicht ausschliessen würde. Deshalb sei EOS prinzipiell manipulierbar und eben keine unveränderbare Smart-Contract-Plattform, so das Urteil der Kritiker.

63 Vgl. „EOS concept: Code is not law.", Emmanuel, *Medium*, April 12th, 2018.

Grafik 24: ETH vs EOS



Quelle: Bitgenste

Ein Kampf, der eigentlich keiner ist?

"2018 is also proving to be a record breaking year for ICO funding, with total funding raised in the last 6 months already surpassing the total of 2017."

Smith and Crown

Interessanterweise haben viele EOS-Sympathisanten mit diesem Verdikt überhaupt kein Problem. Diesen Schluss vermitteln zumindest zahlreiche YouTube-Beiträge und Blogposts von EOS-Verfechtern. Es scheint so, als bestünde die EOS-Community generell eher aus Leuten, die ein gewisser Spielraum zur Einflussnahme einer völligen Aufsichtsunfähigkeit vorziehen. Immer wieder ist das Argument zu lesen, wonach es grundsätzlich als sinnvoll erachtet werden kann, wenn «demokratisch» gewählte Block-Produzenten in Notfällen wie einem Hack oder Bug im Sinne der EOS-Gemeinschaft intervenieren können.

Ethereum, EOS oder eine andere Smart-Contract-Plattform? Die Diskussionen darum, wer das Rennen machen wird, dürfte noch eine Weile anhalten. Ethereum hat mit Abstand die meisten Entwickler, weist dank der Enterprise Ethereum Alliance zahlreiche einflussreiche Firmen auf und ist noch immer die weitaus am meisten verwendete Crowdfunding-Plattform. EOS hat sich an seine eigene Blockchain gewöhnt und vereint vor allem mit Mike Novogratz, Peter Thiel und Jihan Wu drei der wohl namhaftesten Krypto-Investoren[64] hinter sich.

Vor lauter Konkurrenzkampf geht jedoch vergessen, dass sich nicht zwingend nur eine Smart-Contract-Plattform durchsetzen muss. Sehr wahrscheinlich gibt es genügend Platz für mehr als nur einen Gewinner. So erinnert der Kampf um die Vorherrschaft unter diesen Plattformenauch an das

—
64 Vgl. „Peter Thiel, Bitmain Co-Founder Invest in EOS Developer Block.one", Christine Kim, *Coindesk*, July 16th, 2018.

Tauziehen der verschiedenen Betriebssysteme in den frühen Jahren des Computer- und Internetzeitalters.

Genauso wie heute mit Mac, Windows und Linux mehrere Betriebssysteme existieren, dürfte sich auch dieses Mal kein alleiniger Sieger herausentwickeln. Viel wahrscheinlicher ist: Verschiedene Smart-Contract-Plattformen werden sich durchsetzen, die alle unterschiedliche Tradeoffs eingegangen sind, deshalb über unterschiedliche Stärken und Besonderheiten verfügen und somit koexistieren werden. DApps können sogar auf mehreren Smart-Contract-Plattformen gleichzeitig laufen. Bancor, ein Blockchain-Protokoll für die Schöpfung von Smart Tokens, beispielsweise hat bereits angekündigt, neben Ethereum auch EOS als Fundament zu verwenden[65].

[65] Vgl. „EOS.IO Blockchain To Implement The Bancor Protocol", Bancor, *PR Newswire,* February 22nd, 2018.

Über Uns

DasTeam

Mark Valek

Portfolio Management & Research

Demelza Hays

Research & Portfolio Management

Cristian Ababii

Research

Friederich Zapke

Research

Der Report

Als Schwesterbericht zum international anerkannten In Gold We Trust Report hat sich der Crypto Research Report zum Ziel gesetzt, den Markt der Kryptowährungen in seiner ganzen Tiefe zu verstehen und zu erklären. Qualitätsarbeit steht dabei ganz klar im Vordergrund. Der Crypto Currency Research Report ist ein Bericht der Incrementum AG.

Das Unternehmen

Die Incrementum AG ist ein inhabergeführter und voll lizenzierter Vermögensverwalter & Asset Manager mit Sitz im Fürstentum Liechtenstein.

Was zeichnet uns im Bereich des Asset Management aus? Wir bewerten alle unsere Investitionsentscheide nicht nur aus einer globalen ökonomischen Perspektive, sondern auch unter Berücksichtigung der globalen monetären Dynamiken. Auf dieser Grundlage resultiert eine holistische Sicht auf die Lage der Finanzmärkte. Wir sind davon überzeugt, dass unser profundes Verständnis der Geldgeschichte, die unkonventionelle Argumentation und die umsichtige Forschung unsere Kunden dazu befähigt, in diesem herausfordernden Marktumfeld erfolgreich zu sein.

Advisor des Crypto Research Reports

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. Zu unseren Vorstandsmitgliedern 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. Derzeit arbeitet er an Speicherungslösungen für Kryptowährung, die erschwinglich und einfach zu bedienen sind.

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.

Stefan Wieler

Stefan Wieler, CFA, CAIA, ist Vice President of Research and Corporate Sales bei Goldmoney. In den letzten zwei Jahren war Herr Wieler Forschungsleiter bei BBL Commodities, einem Hedge-Fonds, der WTI, Brent, RBOB, HO, Gasöl und Erdgas handelt. Zuvor war er leitender Analyst für Öl-Themen bei Goldman Sachs.

Wir möchten uns bei folgenden Personen für die Mitarbeit bei der Erstellung des CRR bedanken:
Bei unseren kompetenten Beratern, darunter Max Tertinegg, Oliver Völkel, und Stefan Wieler, den großzügigen Autoren, die zu diesem Bericht beigetragen haben, Nikolaus Jilch, und Pascal Hügli. Wir sind auch dem jüngsten Mitglied des Incrementum Teams dankbar, Christian Ababii.

Kontakt:

Incrementum AG
Im alten Riet 102
9494 – Schaan/Liechtenstein
www.incrementum.li
http://www.cryptoresearch.report
Email: crypto@incrementum.li

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 (wie auch die Incrementum AG) 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: 2018 Incrementum AG. Alle Rechte vorbehalten.