crypto research .report

Januar 2019
Edition V.
„Krypto-Winter Edition“

Verwahrungslösungen für Kryptowährungen
Securitization oder Tokenization
Ist ein „Bitcoin Standard“ denkbar?

Demelza Kelso Hays
Mark J. Valek

crypto research .report

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

Vontobel

bitpanda

GENTWO DIGITAL

www.cryptofunds.li

incrementum

Inhalt

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: 2019 Incrementum AG. All rights reserved.

Editorial

Geschätzte Leser,

Der Jahreswechsel ist die Zeit für einen Rückblick und um über das Geschehene zu reflektieren. Das Kryptojahr 2018 ist zweifelsfrei sehr ereignisreich verlaufen. Mit dem Crypto Research Report haben wir sowohl aktuelle Themen abgedeckt, als auch grundlegende Kryptothemen konzeptionell erarbeitet. Im Hinblick auf das Marktgeschehen haben wir mehrfach eine kritische Sichtweise eingenommen. In der ersten Ausgabe vom Dezember 2017 haben wir dem Thema ICOs ein Kapitel mit dem Titel "ICOs: Geld, Betrügereien und große Hoffnungen“ gewidmet. Wir waren der ICO-Bonanza gegenüber sehr kritisch eingestellt und fühlen uns zwölf Monate später in unserer Meinung bestätigt. Etliche ICOs haben sich als nicht nachhaltig erwiesen und als Betrugsfälle entpuppt. In unserer März-Ausgabe haben wir einen Artikel über die technische Analyse mit dem Titel "Droht uns ein Krypto-Winter?" veröffentlicht. Dem Autor, Florian Grummes, gelang eine Punktlandung, als er darauf hinwies, dass die Wahrscheinlichkeit hoch sei, dass Bitcoin bis zum Sommer auf 4.500 bis 5.200 USD fallen würde.

Abbildung 1: Prognose vom März 2018 für fallende Bitcoin Preise

Quelle: Midas Touch, Crypto Research Report März 2018

In unserer Oktober-Ausgabe haben wir eine Bewertungsmethode vorgestellt, die auf unserem quantitativen Netzwerkeffekt basiert. Gemäß dieser Bewertung, war (u.a.) Bitcoin im Herbst immer noch überbewertet (siehe Chart nächste Seite). Von dieser Seite sind wir also durchwegs zufrieden mit unserer Berichterstattung im abgelaufenen Jahr. Aber auch selbstkritische Anmerkungen dürfen nicht fehlen.

Zu einem unserer Artikel wollen wir Folgendes nachtragen: In Abbildung 9 der Juni-Ausgabe des Crypto Research Reports haben wir Kryptowährungen nach ihrem Zentralisierungsgrad und den Externalitäten von Konsens-Mechanismen kategorisiert. Die Internationalen Organisation für Normung (ISO) schlägt jedoch seit kurzem eine elegantere Methode zur Klassifizierung von Konsensus- oder

Governance-Mechanismen vor und zwar die Kategorisierung nach Lese- und Schreibrechten. Vereinfacht ausgedrückt ist eine öffentliche Blockchain jene, bei welcher jeder Nutzer Einsicht in alle Transaktionsdaten hat. Eine erlaubnislose („permissionless“) Blockchain bedeutet, dass auch jedermann Transaktionen gemäß dem Konsensusmechanismus validieren kann. Kryptowährungen wie beispielsweise Byteball Bytes oder XRP verfügen über Transparenz hinsichtlich der durchgeführten Transaktionen, die Validierung kann jedoch nur von autorisierten Nodes durchgeführt werden. Privacy Coins mit nicht transparenten Blockchains wie Monero und ZCash fallen in die Kategorie „privat und erlaubnislos".

Tabelle 1: ISO Klassifizierung von Konsensuns Mechanismen

	Permissioned	Permissionless
Öffentlich	Ripple/IOTA/Byteball	Bitcoin
Privat	Hyperledger	Privacy coins

Erwähnenswert ist weiters, dass sich eine formale Definition von „Blockchain“ in der akademischen Literatur durchzusetzen scheint. Eine Blockchain ist demnach eine distributed Ledger-Datenbank mit einem Konsensmechanismus. Daher sind Distributed-Ledger-Technologien (DLT) die oberste Kategorie von Peer-to-Peer-Datenbankstrukturen. Dazu gehören Hyperledgers, die Bitcoin-Blockchain und die bei IOTA verwendete „directed acyclic graph“-Technologie.

Abbildung 2: Bitcoin Überbewertung im Oktober aufgezeigt

Quelle: Coinmetrics; Crypto Research Report Oktober 2018

Der Winter ist die perfekte Jahreszeit, um es sich zu Hause gemütlich zu machen und den Wissensstand in Sachen Kryptowährungen aufzufrischen. Auch erscheint es vermutlich ratsam, sich auf einen bevorstehenden Krypto-Frühling vorzubereiten.

Nun wünschen wir Ihnen viel Vergnügen mit der Januar-Ausgabe des Crypto Research Report und wünschen Ihnen für das Jahr 2019 alles Gute!

Demelza Kelso Hays and Mark Valek
Incrementum AG

In Case You Were Sleeping: Krypto-Winter Edition

“Die Idee, eine Alternative zum traditionellen Papiergeld zu haben, ist attraktiv, besonders heute, da die Kaufkraft der großen Währungen gefährdet ist und das Vertrauen, das sie zur Arbeit benötigen, sinkt. Die Zentralbanken konzentrieren sich nicht mehr auf ihre Pflicht, den Wert des Geldes zu schützen, sondern haben sich dem Druck gebeugt, den die Regierungen auf sie ausgeübt haben, um überdimensionale öffentliche Schulden zu finanzieren.“

Prinzessin Gisela von und zu Liechtenstein

Key Takeaways

- **Die Bruttogewinnmargen beim Mining von Bitcoin und Ethereum sind auf 30% bzw. 15% gesunken. Trotzdem wird es nicht zur von Skeptikern befürchteten „Todesspirale“ kommen, da ausrechend viele Miner weiterhin tätig bleiben aufgrund fallender „Difficulty“.**
- **Das Gerücht, dass Goldman Sachs' Krypto Trading Desk abgesagt wurde, ist „Fake News“. Goldman Sachs baut nicht nur einen Trading Desk auf, sondern arbeitet auch an einer Digital Asset Custody-Lösung.**
- **Aufgrund der hohen Volatilitäten im vergangenen Jahr ist die Nachfrage nach Stable Coins gestiegen. An diverse interessante Projekte wird derzeit gearbeitet.**

Der Krypto-Winter ist im vollen Gange. Im Hintergrund arbeiten die großen Player am Ausbau der Infrastruktur, während Behörden die Trümmer des ICO-Hypes aufräumen.

Quelle: *David M. Russell/CBS*

Rund zehn Jahre nach der Veröffentlichung des berühmten Whitepapers von Satoshi Nakamoto ist zum Thema Bitcoin-Geburtstag fast alles gesagt. Deshalb gehen unsere Grüße nicht an den oder die mysteriösen Erfinder der Kryptowährung, sondern an Alicia Florrick. Die sympathische (und fiktionale) Anwältin aus der Hit-Serie „The Good Wife“ (CBS) hatte schon 2012 in einem Fall mit Bitcoin zu tun. Das war spannend, das war neu und es war wohl die allererste Bitcoin-Referenz in einer Mainstream-Fernsehsendung. Den Drehbuchautoren gebührt Lob. Nicht nur, weil sie Bitcoin zum Thema gemacht haben, als die Kryptowährung gerade **einmal drei US-Dollar wert war**. Sondern auch, **weil sie das neuartige Ding binnen weniger Minuten gut erklären konnten**, in einer simplen Szene, in der Alicias Kinder im Teenager-Alter ihr das Thema Bitcoin Schritt für Schritt beibringen. Die Zuseher wurden nicht nur unterhalten, sondern auch gut informiert. Andere sind beim Thema Bitcoin hingegen oft gescheitert.[1]

Als die Simpsons ein Jahr später Bitcoin erwähnten, geschah das nur nebenbei, im Scherz (S25E07). Protagonist war in diesem Fall Krusty, der Clown. Auf Lisa Simpsons Frage, ob er denn pleite sei, antwortete dieser in der Folge „Yellow Subterfuge“: „Ja. Alles was es braucht ist ein bisschen Pech auf der Rennstrecke, mehr Pech im Bitcoin-Markt und ein großes Investment in einen Anbieter für high-end Lesezeichen.“[2] Diese eher depressive Perspektive passt gut zum vergangenen Jubiläumsjahr für Bitcoin.

Was die Preisentwicklung angeht, war 2018 quasi das Gegenteil von 2017. Nach der Euphorie kam die Ernüchterung. Nach dem Boom der Bust. Auf 20.000 USD folgten 10.000. Dann wurde die Marke von 6.000 USD lange gehalten. Bis Ende November. Da ging es, ausgelöst von einem Streit in der Bitcoin Cash Community, noch einmal rasant nach unten. Bitcoin rutschte in die Gegend von 3.000 USD. Die Medien veröffentlichten Nachrufe auf die Kryptowährung.[3] Wieder einmal.[4]

Erklärungen, was Bitcoin eigentlich ist, waren nicht mehr notwendig. Jahre nach dem Auftritt bei „The Good Wife“ und den „Simpsons“ ist **Bitcoin tatsächlich im Mainstream angekommen**. Es war ein weiter Weg. Die Kollegen vom „Breaker Magazine“ haben eine ganze Liste mit Bitcoin-Referenzen in der Popkultur aus den vergangenen zehn Jahren erarbeitet. Und sich die Frage gestellt, was „Bitcoin im Mainstream“ eigentlich bedeutet. Geht es um den Preis?

—

[1] https://www.youtube.com/watch?v=-fazu1rgr9k
[2] https://www.youtube.com/watch?v=8ovL20iGEac
[3] https://www.marketwatch.com/story/bitcoin-is-pretty-much-dead-says-teenage-crypto-phenom-2018-12-14
[4] https://99bitcoins.com/bitcoinobituaries/

Geht es um die Nutzung der Kryptowährung im Kaffeehaus? Oder geht es um die Bekanntheit? Diese Fragen stellen wir uns auch.[5]

Der Crash und die Folgen

Seit dem Bitcoin-Megaboom ist ein Jahr vergangen. Was den Preis betrifft, so wissen wir immer noch nicht, ob nach einem Jahr Bärenmarkt inzwischen ein Boden erreicht wurde. Auch nicht nach dem jüngsten Abverkauf. Als wir diese Zeilen schreiben, befindet sich der Preis gerade knapp über der Marke von 4.000 USD.

Freilich: Seit der ersten Erwähnung von Bitcoin bei „The Good Wife" hat sich der Preis zuerst auf 30 USD verzehnfacht. Und ist in der Folge –noch einmal um mehr als 10.000 Prozent gestiegen. Die ersten zehn Jahre der Kryotowährung sind eigentlich eine unglaubliche Erfolgsgeschichte. Auch preislich.[6] Aber all das scheint nach dem deprimierenden Jahr 2018 niemanden zu interessieren. Bitcoin musste seinen Geburtstag mit einer Träne im Auge begehen.

Zuletzt wurde sogar über eine Spirale des Todes debattiert. Einige argumentieren, dass die Miner ihre Tätigkeit einfach einstellen werden, wenn der Preis unter die Produktionskosten fällt. Das wäre tatsächlich eine Katastrophe, wie der Skeptiker Atulya Sarin argumentiert:

„Wenn der Bitcoin-Preis unter die Mining-Kosten fällt, verschlechtert sich der Anreiz, Bitcoin zu schürfen. Das stürzt Bitcoin in eine Todesspirale. Ohne die Mining-Aktivitäten, die den Ledger erhalten, der die Aufzeichnungen erfasst, wird Bitcoin wertlos."[7]

"The blockchain is a distributed network that solves all the problems that we have of finance, but more broadly, it's like a philosophy. It's a way of life."

Mike Cernovich

Diese Sicht der Dinge ist nicht neu. Dieselbe Debatte gab es schon 2011. Heute ist die Industrie zwar deutlich größer, die Antwort auf die Angstmache bleibt aber dieselbe. Wie damals übersehen die Propheten des Todes von Bitcoin die Nuancen in der Game-Theorie hinter der Kryptowährung. Satoshi Nakamoto hat das Netzwerk sehr wohl auf einen raschen Preisverfall vorbereitet. **Alle 2016 Blocks wird die Difficulty angepasst**. Fällt der Preis und schrumpft die Zahl der Miner, wird es für die verbliebenen leichter, neue Bitcoins zu erzeugen. Das Argument der Todesspirale fußt auf der Annahme, dass der Preis so schnell fällt und die Miner so schnell aufgeben, dass das System nicht rechtzeitig mit der Anpassung der Mining-Difficulty nachkommt.

Aber auch für dieses Problem gibt es Lösungen. Andras Antonopoulos erklärt:

—

5 https://breakermag.com/a-comprehensive-list-of-crypto-references-in-pop-culture/
6 https://www.bloomberg.com/news/articles/2018-10-30/halloween-birth-of-bitcoin-led-to-unimaginable-gains-in-10-years
7 https://www.marketwatch.com/story/bitcoin-is-close-to-becoming-worthless-2018-12-03

„Wenn die Miner warten bis die Difficulty gesenkt wird, dann macht jeder Miner, der wartet, mehr Profit weil sie jetzt einen größeren Anteil an der Mining-Power haben als zuvor.“[8]

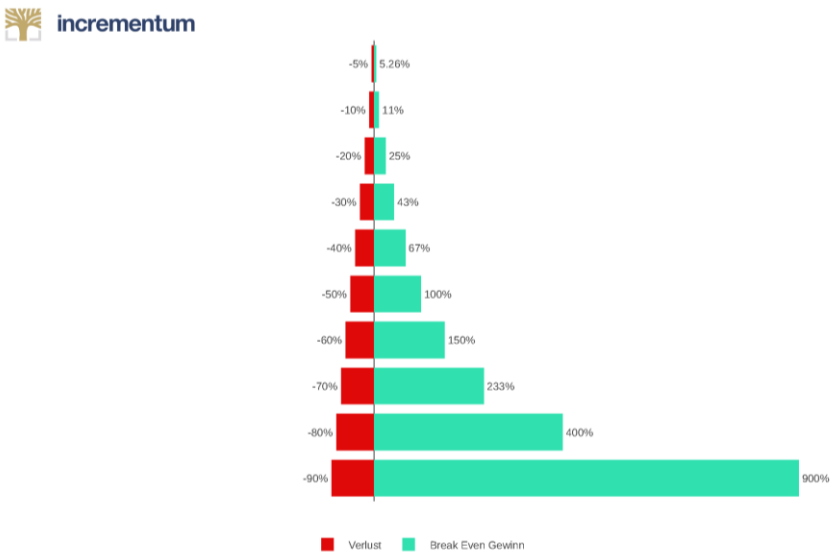
Außerdem muss man bedenken: Miningkosten sind nicht überall gleich, jeder Miner hat seine eigenen Berechnungen. Auch mit Verlust zu Minen, ist manchen eine Zeit lang möglich. Und wenn alle Stricke reißen, gibt es immer noch die Option einer Hard Fork, was die sofortige Anpassung der Difficulty ermöglichen würde. Das wäre der äußerste Schritt.[9]

"To raise equity, an Initial Coin Offering, or ICO, system was developed. This uses the blockchain technology to replace the stock market, and effectively decentralizes its function of supplying capital to the economy."

Princess Gisela von und zu Liechtenstein

Das soll freilich nicht heißen, dass die Miner den Preisverfall unversehrt überstehen. Die Lage ist durchaus dramatisch. Bitcoin-Miner sind an gewaltige Margen von bis zu 50 Prozent gewohnt. Seit dem Preisverfall ist die Lage härter, wie BitMEX ausgerechnet hat. Aktuell liegen sie nur noch bei 30 Prozent für Bitcoin und bei 15 Prozent für Ethereum. Es gibt auch eine Reihe von Miningfirmen, die sich verschätzt haben, und schon aufgeben mussten. Die Bereinigung des Marktes findet während des Preisverfalls also nicht nur bei den Kryptoprojekten statt, sondern auch im Miningsektor.[10]

Abbildung 3: Verluste entsprechende Break Even Gewinn



Quelle: Incrementum AG.

Und wenn es um Bitcoin als Währung geht, sieht es noch düsterer aus. Die Experten überschlugen sich rund um den 10. Geburtstag im Oktober 2018 mit Feststellungen zu Bitcoins Irrelevanz als Zahlungsmittel. Ist eine Kostprobe gefällig? Hier ist Samuel Murrant, Analyst für den Zahlungsverkehr bei GlobalData: „Ende 2018 haben Krytowährungen generell nur eine sehr limitierte Relevanz für die Bewegung von Geld rund um die Welt. Bitcoin ist zweifellos ein —

[8] https://www.marketwatch.com/story/why-bitcoin-by-design-wont-become-worthless-according-to-this-crypto-heavyweight-2018-12-05?mod=newsviewer_click
[9] https://www.theblockcrypto.com/2018/12/04/the-bitcoin-mining-death-spiral-debate-explained/
[10] https://blog.bitmex.com/the-price-crash-the-impact-on-miners/

wertvoller Rohstoff und mit Abstand die bekannteste und wichtigste Kryptowährung. Aber es ist eigentlich keine Währung. Es wird nur für wenige Zahlungen eingesetzt. Zwischen Parteien, denen die Anonymität wichtig ist. Oder zwischen den wahren Jüngern, die immer noch an das globale Potenzial des Systems glauben."[11]

Aber das ist ein sehr eindimensionaler Blick auf Bitcoin und Murrant weiß das auch. In weiterer Folge schreibt er: „Bitcoin ist eher mit Gold zu vergleichen als mit Geld. Es ist ein Wertspeicher und, wegen seiner Seltenheit als wertvoll erachtet und auf der Basis von Annahmen über seinen Wert gehandelt."

Bitcoin hat sich also seine eigene Assetklasse geschaffen: Krypto. Dass hier eine Blase geplatzt ist und noch immer Luft entweicht, ist nicht zu übersehen. Wir haben schon in unserem allerersten Report von Dezember 2017 vor dem ICO-Boom und seinen Folgen gewarnt. In der Märzausgabe dieses Jahres hatten wir einen Artikel geschrieben mit dem Titel „Droht uns ein Krypto-Winter?". Derzeit herrscht auf der nördlichen Hemisphäre der meteorologische Winter, global allerdings tiefster Krypto-Winter. Diese Bereinigung scheint vorerst noch nicht zu Ende zu sein.

Aus ökonomischer Sicht ist das positiv, weil nach einer Bubble nur ein Crash die Basis für neues, nachhaltiges Wachstum legen kann. Aber leider ist Krypto, das inzwischen auch von Morgan Stanley als „institutionelle Anlageklasse" gesehen wird, so jung, dass wir nur geringe Erfahrungswerte damit haben, wie lange so eine Bereinigung dauern könnte.[12] Wir können nur abwarten und beobachten, wie die großen Player sich für die nächste Phase in Stellung bringen. Und da tut sich, wie wir seit mehr als einem Jahr regelmäßig dokumentieren, verdammt viel.

"Trust is established through mass collaboration and clever code rather than by powerful intermediaries like governments and banks."

Don Tapscott,
author of *The Digital Economy*,
Wikinomics

Der zweite Sektor, wo Bitcoin und die Blockchain fraglos für Innovation gesorgt hat, ist der Zahlungsverkehr und das Gebiet der Währungen generell. Nicht unbedingt, weil Bitcoin sich selbst als Zahlungsmittel durchgesetzt hat. Wir wissen, dass das nicht geschehen ist. Der wahre Durchbruch ist die Mainstream-Akzeptanz für digitale Währungen an sich und „private" digitale Währungen generell. Hier tut sich so viel, dass auch die Notenbanken inzwischen nicht mehr zusehen können. Kryptowährungen bieten sich in einer digitalen Welt als Alternative zu Euro, US-Dollar oder Pfund an.

Und auch einen dritten Sektor hat Bitcoin maßgeblich beeinflusst. Die Cyberkriminalität, leider. Schon beim zweiten Auftauchen von Bitcoin bei „The Good Wife" im Jahr 2013 ging es um eine Ransomware-Erpressung. Die gute Nachricht: Branche und Aufsichtsbehörden bekommen das Thema Betrug im Kryptosektor immer besser in Griff. Aus unserer Sicht ist das sehr positiv für den Sektor. Das Jahr mag preislich deprimierend gewesen sein. Aber das sorgt nicht

—

[11] https://www.globaldata.com/ten-years-bitcoin-now-no-relevance-payments-says-globaldata/
[12] https://www.coindesk.com/morgan-stanley-says-crypto-is-a-new-institutional-asset-class/

nur für eine automatische Marktbereinigung. Es gibt auch den Aufsehern Zeit, Betrüger zu jagen. Die SEC hat sogar erstmals Prominente bestraft, weil sie für Scamcoins Werbung gemacht haben. Dazu später mehr.

Assetklasse und Adoption

"The blockchain does one thing: It replaces third-party trust with mathematical proof that something happened."

Adam Draper

Werfen wir zuerst einen Blick auf die Entwicklungen bei der „Assetklasse Krypto". Wir beobachten diesen Bereich, seit es ihn gibt. **Der Preisrückgang hat auch hier das Tempo gedrosselt.** Oder, wie es Michael Novogratz, einer der bekanntesten Krypto-Investoren ausdrückt: „Eine Sache, die man hier lernt, ist: Alles dauert ein bisschen länger als man hoffen würde." Die Marke von 10.000 USD werden wir 2018 nicht mehr sehen, musste der Bitcoin-Bulle neulich eingestehen. Seine Firma, Galaxy Digital Holdings, musste heuer bereits mehr als 150 Millionen USD an Verlusten verbuchen. Aber Novogratz, einer der bekanntesten Bitcoin-Verfechter an der Wall Street, will nicht aufgeben.[13]
Im Gegenteil: Novogratz, selbst ein ehemaliger Partner bei Goldman Sachs, ist gemeinsam mit der Investmentbank zuletzt bei BitGo Holdings eingestiegen. Goldman und Novogratz Galaxy Digital Ventures erhoffen sich von dem Start-Up eine Lösung für das weiter ungelöste Problem der Verwahrung von Kryptoassets. Die US-Regulatoren verlangen von den Geldmanagern nämlich die Lagerung von Assets bei so genannten „qualifie d custodians". Die traditionellen Player in diesem Sektor bleiben dem Kryptomarkt bisher fern. Aus Angst vor Hackern und wegen der immer noch herrschenden Rechtsunsicherheit.[14]

Abbildung 4: Die größten Hacks in den vergangenen Jahren

Quelle: Incrementum AG.

[13] https://www.bloomberg.com/news/articles/2018-10-15/novogratz-says-bitcoin-rally-likely-to-take-place-next-year
[14] https://www.bloomberg.com/news/articles/2018-10-18/goldman-wades-deeper-in-crypto-betting-on-bitgo-with-novogratz

„Wenn man in irgendein anderes Asset investiert, hat man wahrscheinlich nicht die Angst, dass es einfach verschwinden könnte. Aber hier haben einige Leute noch diese Angst“, so Mike Belshe, BitGos Mitbegründer und CEO in einem Interview mit Bloomberg. Seine Firma hat inzwischen rund 70 Millionen USD durch Fundraising eingesammelt. Das in Palo Alto angesiedelte Unternehmen wurde 2013 gegründet und bietet digitale Wallets an, die für Transaktionen multiple Signaturen benötigen. Zudem werden auch Offline-Safes für Bitcoin und andere Währungen angeboten. Aktuell verwaltet man 75 verschiedene Kryptoassets und ein Gesamtvolumen von rund zwei Milliarden USD, so das Unternehmen. Der Einstieg von Novogratz und Goldman Sachs könnte BitGo aber auf ein ganz neues Level befördern.

Goldman Sachs gehört an der Wall Street sicherlich zu den mutigsten Banken, was Bitcoin und Co. betrifft. „Wir glauben, dass die Frage der Aufbewahrung ein logischer Schritt in Richtung der Rolle als Market Maker für digitale Assets ist“, so Goldman Sachs-Sprecher Michael DuVally. Meldungen, denen zufolge Goldman Sachs seine Pläne für einen eigenen Krypto-Tradingdesk angesichts des Preisrückganges wieder gestrichen habe, bezeichnete die Bank zuletzt als „Fake News“. Man hält der neuen Assetklasse also sehr wohl die Stange, sieht sich aber mit ungewöhnlichen Herausforderungen konfrontiert. Angeblich arbeitet Goldman Sachs auch an einer eigenen Lösung für Bitcoin-Custodianship.

“Just as it got easier to use email, it will be easier to use Bitcoin as people invest in it and become more familiar with it.”

Gavin Andresen (Core Developer of Bitcoin)

Fest steht: Solange diese Fragen nicht geklärt sind, bleibt der Kryptomarkt sowohl für den „normalen“ Kleinanleger als auch für alle institutionellen Investoren verschlossen. In dieser Ausgabe widmen wir ein gesamtes Kapitel Lösungsansätzen für die sichere Verwahrung, die bereits bestehen oder gerade live gehen.

Ein weiterer wichtiger Player, der in diesem Bereich gegen Goldman Sachs antreten will, ist Fidelity Investments. Die Firma, die im traditionellen Geschäft Kundengelder in der Höhe von 7,2 Billionen USD verwaltet, hat im Oktober eine eigene Krypto-Tochter gegründet. Unter dem Namen Fidelity Digital Asset Services soll ein Service entstehen, der es Kunden ermöglicht, Bitcoin auf verschiedenen Börsen zu den besten Preisen zu handeln. „Cold Storage“, also die vor Hackern sichere Verwahrung ohne Internetanbindung, soll von Anfang an zum Paket gehören.[15]
“Wenn man sich die existierende Infrastruktur ansieht, dann merkt man schnell: Die ist sehr stark auf Retail Investoren und Früheinsteiger ausgerichtet“, sagte Tom Jessop von Fidelity: „Das Timing ist gut, wir haben in den vergangenen Monaten ein Wachstum der Nachfrage beobachten können.“ Fidelity habe bereits seit 2014 mit Bitcoin experimentiert und sogar hunderte Bitcoin selbst geschürft. Selbst in der Kantine kann man inzwischen mit Bitcoin bezahlen. „Die Frage ist, wie bleiben wir vor der Konkurrenz? Welche Innovationen braucht es und wie bekommen wir neue Produkte auf die Plattform“, fragt Jessop.
—

[15] http://fortune.com/2018/10/15/fidelity-launches-company-help-hedge-funds-big-investors-trade-crypto/

Es ist dabei keinesfalls so, dass alle institutionellen Investoren lediglich an der Seitenlinie sitzen und warten. Tatsächlich dürften sie inzwischen sogar die reichen Privatpersonen als die größten Käufer von Kryptowährungen abgelöst haben. Die Trades finden dabei meist direkt zwischen den Investoren und große Minern bzw. Personen mit einem großen Bitcoin-Vermögen statt. Dieser OTC- Markt sieht aktuellen Schätzungen zufolge täglich ein Volumen von 250 Millionen USD bis 30 Milliarden USD.[16]

"This is the missing piece for infrastructure — it's a treacherous environment today. Hedge funds need it, family offices need it, they can't participate in digital currency until they have a place to store it that's regulated [...] This is early stages in an industry that's volatile right now. We're in a down cycle in terms of where we're going, but the institutions see an opportunity. It's going to progress quickly."

Mike Belshe,
co-founder and CEO of BitGo

Zum Vergleich: An den Börsen werden laut „coinmarketcap.com" täglich Kryptoassets im Wert von rund 15 Milliarden USD gehandelt, wobei einige der dort gelisteten Börsen als wenig seriös gelten und man ihre Zahlen mit Skepsis betrachten sollte. An der Universität Liechtenstein wird hierzu zurzeit eine umfangreiche Analyse durchgeführt, die sich mit der tatsächlichen Markttiefe der Kryptoassets auseinandersetzt. Die Ergebnisse der Studie werden wir sicherlich in einer der nächsten Ausgaben behandeln.

Fraglos hat auch der OTC-Markt unter dem Preisrückgang gelitten. Dennoch sei hier Wachstum zu beobachten, sagt Jeremy Allair, CEO von Circle Internet Financial aus Boston: „Wir sehen im OTC-Business derzeit dreistellige Wachstumsraten. Es ist ein wichtiger Wachstumssektor." Dieses Wachstum dürfte anhalten, solange institutionelle Investoren in den Markt eintreten. Denn sie benötigen oft mehr Coins, als an den Börsen überhaupt angeboten werden. Oder sie haben Angst davor, den Preis durch den eigenen Kauf oder Verkauf zu stark zu bewegen. Deswegen suchen sie sich abseits der Börsen Handelspartner für diese großen Deals.

All das bleibt den großen Wall Street Banken nicht verborgen. Von Goldman Sachs und Fidelity haben wir ja schon gehört. Aber niemand will zurückbleiben, wie es aussieht. Auch Morgan Stanley, Citigroup und Bank of America/Merrill Lynch arbeiten Medienberichten zufolge an eigenen Bitcoin-Produkten, um die Nachfrage der Kunden zu befriedigen.[17] Auch Russlands Gazprombank wagt sich über eine Tochter in der Schweiz in den Markt.[18]

Und dann sind da noch die großen US-Universitäten, die ihre Einnahmen und Spenden in Endowments verwalten. 96 Prozent der Uni-Geldmanager geben noch an, vom Kryptomarkt nichts wissen zu wollen. Aber einige klingende Namen wie Harvard, Stanford und das MIT sind schon im Geschäft.[19]

Dasselbe gilt für Yale. Die Eliteschule hat zuletzt in den Paradigm Fonds investiert, den ehemalige Mitarbeiter von Coinbase, Sequoia Capital und dem Kryptofonds —

[16] https://www.bloomberg.com/news/articles/2018-10-01/institutional-investors-are-using-back-door-for-crypto-purchases
[17] https://bitcoinexchangeguide.com/breaking-bank-of-americas-merrill-lynch-to-launch-bitcoin-trading-product-to-rival-goldman-sachs-and-morgan-stanley/
[18] https://gazprombank.ch/news/gazprombank-switzerland-ltd-prepare
[19] https://www.theinformation.com/articles/harvard-stanford-mit-endowments-invest-in-crypto-funds

Pantera Capital gestartet haben. Insgesamt stecken rund 400 Millionen USD an Investorengeldern in diesem Fonds. Wieviel davon aus der 30 Milliarden Dollar USD schweren Geldbörse von Yale stammen, ist aber nicht bekannt. Der Schritt gilt aber als signifikant, denn Yales Geld wird von David Swensen verwaltet.[20]

Swensen gilt als Pionier unter den institutionellen Investoren und hat in den vergangenen Jahrzehnten einige der College Endowments mit der besten Entwicklung verwaltet. Er konzentriert sich auf lange Zeithorizonte und oft auf Märkte mit wenig liquiden Assets. Viele andere Unis versuchen es ihm nachzumachen. Unter Swensen hat Yale eine Rendite von fast 12 Prozent jährlich gesehen – über die vergangenen 20 Jahre. Insgesamt stecken mehr als 500 Milliarden USD in den Fonds der US-Colleges.[21]

"Everything will be tokenized and connected by a blockchain one day."

Fred Ehrsam

Zwei wichtige Player haben zuletzt ihr Interesse am Kryptomarkt zwar unterstrichen, den Zeitplan aber den neuen Preisgegebenheiten angepasst. So hat Bakkt, die Krypto-Plattform von Intercontinental Exchange, den Start der eigenen Bitcoin-Futures auf Ende Jänner verschoben. „Wie so oft bei der Einführung neuer Produkte, gibt es neue Prozesse und Risken, auf die man sich vorbereiten muss. Bei Krypto geht es um eine neue Assetklasse und wir müssen Ressourcen bündeln", sagte Bakkt CEO Kelly Loeffler. Die Partnerschaften zwischen ICE, Mutter der New York Stock Exchange, und Starbucks sowie Microsoft sind weiter aktuell. Neue Details gibt es aber derzeit nicht.[22]

Auch die Technologiebörse Nasdaq will weiter am Plan festhalten, mit Futures-Kontrakten in den Markt einzusteigen. Losgehen soll es im ersten Quartal 2019. Noch befindet man sich aber in Gesprächen mit der US-Aufsichtsbehörde CFTC. Soll heißen: Nichts ist fix.[23]

M&A und Europa

Eine andere Variante, am Kryptokuchen mitzunaschen, ist selbst unternehmerisch tätig zu werden oder andere Firmen aufzukaufen. Wir haben schon mehrmals geschrieben, dass der Marktcrash der vergangenen Monate gut für Bitcoin und Co. sein kann, weil unseriöse Projekte dadurch unrentabel werden oder vielleicht sogar verschwinden. Gleichzeitig wird der Sektor konsolidiert und die zahlungskräftigen Firmen gehen auf Einkaufstour. Schon bis Oktober ist die Zahl der Zusammenführungen und Zukäufe (M&A) im

—

[20] Wir hatten das Vergnügen mit Mark Yusko ein exklusives Interview zu führen. Auch er war früher für die Investments einer Eliteuniversität verantwortlich und investiert nun zunehmend in Krypto Technologie: https://www.incrementum.li/journal/advisory-board-discussion-q4-2018-blockchain-technology-the-biggest-wealth-creation-opportunity-of-our-lifetime-feat-special-guest-mark-yusko/
[21] https://www.bloomberg.com/news/articles/2018-10-05/yale-is-said-to-invest-in-crypto-fund-that-raised-400-million
[22] https://www.theblockcrypto.com/2018/11/20/bakkt-has-pushed-back-its-bitcoin-futures-launch-to-2019-but-phase-two-is-still-on-track/
[23] https://www.bloomberg.com/news/articles/2018-11-27/nasdaq-is-said-to-pursue-bitcoin-futures-despite-plunging-prices

Kryptosektor im Vergleich zum Vorjahr um mehr als 200 Prozent gestiegen. Mindestens 30 waren zu diesem Zeitpunkt noch nicht abgeschlossen.[24]

Der Kryptosektor ist global und bisher – passenderweise – ohne wirkliches Finanzzentrum. Einer der größten und interessantesten Deals hat sich deshalb nicht in den USA abgespielt, sondern in Europa. Da hat die belgische Investmentfirma NXMH gerade die Börse Bitstamp gekauft und dafür bar bezahlt. Der Kaufpreis wurde nicht genannt. Vor zwei Jahren wurde Bitstamp, die größte Börse in der Europäischen Union, mit rund 60 Millionen EUR bewertet. Es ist davon auszugehen, dass die Bewertung für den Verkauf nach dem Boom von 2017 deutlich höher war. Bitstamp hat mehr als drei Millionen registrierte Nutzer und einen täglichen Handelsumsatz von 100 Millionen USD. Für die beiden Gründer Nejc Kodrič und Damian Merlak war der Deal auf jeden Fall erfolgreich. Sie hatten Bitstamp im August 2011 in Slowenien gegründet, in einer Garage. Ihr Startkapital: Ein Server, ein paar Laptops und eintausend Euro in bar. Heute ist Bitstamp in Luxemburg registriert. Das soll auch nach dem Deal so bleiben.[25]

"The interesting thing about blockchain is that it has made it possible for humanity to reach consensus about a piece of data without having any authority to dictate it."

Jaan Tallinn

Zwei weitere Anekdoten aus Europa, diesmal aus dem uns sehr nahestehenden deutschsprachigen Raum. Wir wissen aus den vergangenen Crypto Research Reports, dass die Schweiz sich aktiv um Blockchain- und Bitcoin-Firmen bemüht. Wie wir in unserer Oktober-Ausgabe ausführlich berichteten, plant die Regierung in Liechtenstein ein eigenes Gesetz, das jetzt bereits von vielen als vorbildlich gelobt wird. Aber auch der Riese Deutschland ist keineswegs inaktiv. **Die Hipster-Hauptstadt Berlin hat eine lebhafte Kryptoszene**. Jetzt gibt es einen Vorstoß aus der Partei von Regierungschefin Angela Merkel. Die CDU will aus Deutschland das ICO-Land Nummer eins machen. Inklusive deutscher Ordnung und deutscher Gründlichkeit, versteht sich. Anders als in Liechtenstein gibt es hier aber noch kein neues Gesetz, sondern nur den Traum vom „Blockchainfinanzplatz Deutschland".[26]

Wieder anders geht es Österreich an. Auch hier will man ICOs Rechtssicherheit geben. Eine entsprechende Arbeitsgruppe soll bis Ende des Jahres 2018 Ergebnisse vorlegen, dann wird es ein neues Gesetz geben. Im Kleinen tut sich aber jetzt schon sehr viel. So hat die Staatsdruckerei gemeinsam mit dem Grazer Unternehmen Coinfinity eine Lösung für die physische Offlinespeicherung von Bitcoin-Private-Keys entwickelt, die den Namen Chainlock trägt. Chainlock ist eine Lösung des Custodian-Problems, aber eher für Privatpersonen, nicht für institutionelle Investoren.[27]

—

[24] https://www.cnbc.com/2018/10/18/crypto-deal-makers-see-opportunity-in-bitcoins-price-slump.html
[25] https://www.businessinsider.com/r-european-investment-firm-buys-digital-exchange-bitstamp-in-all-cash-deal-2018-10?IR=T
[26] http://www.faz.net/aktuell/finanzen/digital-bezahlen/cdu-vorschlag-deutschland-soll-mekka-fuer-kryptogeld-werden-15887209.html?printPagedArticle=true#pageIndex_0
[27] https://www.trendingtopics.at/card-wallet-coinfinity-und-staatsdruckerei-bringen-neue-speicherloesung-fuer-bitcoin/

Und der Wiener Anwaltskanzlei Stadler & Völkel[28] ist es gelungen, von der Aufsichtsbehörde erstmals ein Kapitalmarktprospekt für ein STO, ein Security Token Offering, genehmigt zu bekommen. Ein STO kann man als Weiterentwicklung des ICO verstehen. Die Halter von Security Token haben wie etwa Aktienbesitzer auch verbriefte Rechte und sind nicht einzig von der Preisentwicklung eines erworbenen Tokens abhängig, wie es etwa bei ICOs der Fall war. Im Gegenzug sind die Security Token denselben Regeln unterworfen wie andere Wertpapiere auch. Deshalb braucht man in Österreich etwa die Genehmigung durch die Finanzmarktaufsicht FMA, bevor so ein Token verkauft werden kann. Der Security Token der Firma Hydrominer, deren Prospekt gerade genehmigt wurde, soll im Februar 2019 für Anleger zu bekommen sein.[29]

Notenbanken und Stablecoins

"Alternatively, not to act in the face of current developments and completely leave the payment market to private agents, will ultimately leave the general public entirely dependent on private payment solutions, which may make it more difficult for the Riksbank to promote a safe and efficient payment system."

Riksbank

Nachdem wir gerade eine neue Abkürzung gelernt haben (STO) kommt jetzt noch eine: CBDC. Central Bank Digital Currency. Das Thema wird jeden Tag heißer. Wobei bis heute nicht einmal klar ist, wovon wir eigentlich reden. In den Medien wird gerne so getan, als würden Notenbanken, die mit digitalem Geld experimentieren, eigene Kryptowährungen wie Bitcoin entwickeln. Aber so einfach ist das nicht. Tatsächlich gibt es immer mehr Zentralbanken, die sich des Themas annehmen. Aber für sie ist die Blockchain vor allem ein Vehikel, um ein digitales Äquivalent für Cash zu schaffen. Zwar ist der notorische Bitcoin-Kritiker Nouriel Roubini fest davon überzeugt, dass die CBDC der Zukunft Bitcoin verdrängen werden. Weil ja niemand Anarchiegeld akzeptieren würde, wenn er staatliches Geld auch haben könne. Dabei übersieht Roubini aber, dass Bitcoin etwas hat, dass digitale Zentralbankwährungen niemals vorweisen können, nämlich einen deflationären Charakter.[30]

Es ist höchst unwahrscheinlich, dass eine Zentralbank jemals eine Währung begibt, die tendenziell aufwertet. An dieser Stelle ist aber einmal mehr auf den grundlegend unterschiedlichen Charakter dezentraler Kryptowährungen wie z. B. Bitcoin und zentralisierten staatlichen Formen von digitalem Geld hinzuweisen. Staaten haben historisch ein starkes Interesse, über das Geldmonopol zu verfügen, sei es direkt oder indirekt über Zentralbanken, da bei einer Überschuldung die Geldmengenausweitung gerne zur verdeckten Staatsfinanzierung herangezogen wird.

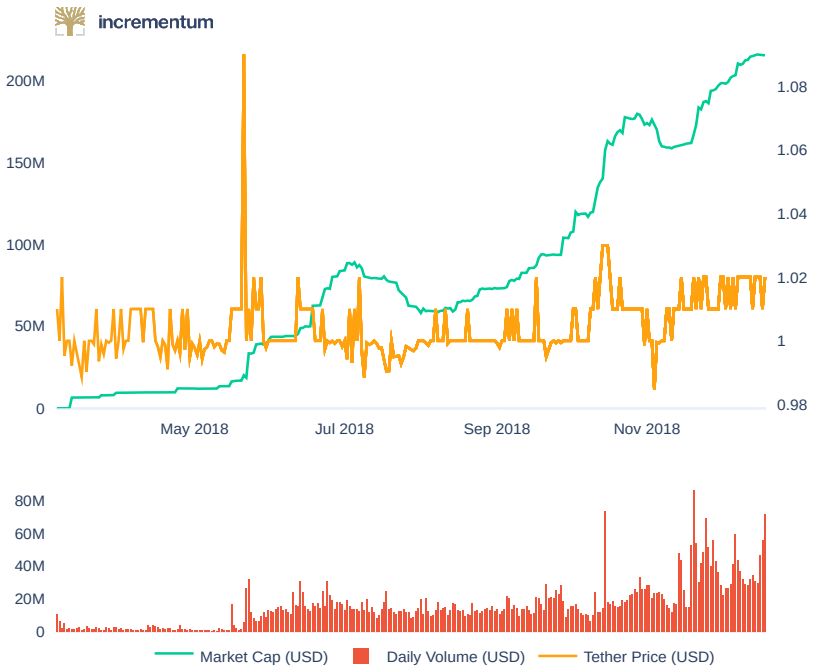
Was heute nicht mehr ganz auszuschließen ist, ist eine „Entnationalisierung des Geldes", wie sie Friedrich August von Hayek gefordert und vorhergesehen hat. Bei Hayek waren es die Geschäftsbanken, die als

—

[28] Einer der Partner der Kanzlei, Oliver Völkel, ist dankenswerterweise Mitglied des Advisory Boards dieser Publikation.
[29] https://diepresse.com/home/wirtschaft/recht/5541879/Depot-in-der-Hosentasche_FMA-bewilligt-BlockchainEmission
[30] https://www.project-syndicate.org/commentary/central-banks-take-over-digital-payments-no-cryptocurrencies-by-nouriel-roubini-2018-11

Gelderzeuger in den Markt eintreten. Auch das ist noch möglich. Was privates Geld betrifft, stehen wir ganz am Anfang. Aber die wichtigsten Schritte sind getan. Bitcoin ist gerade dabei, sich zu etablieren. Und sogar Christine Lagarde, die einflussreiche Chefin des Internationalen Währungsfonds (IWF), ist auf das Thema aufmerksam geworden. Die Notenbanken müssten sich weltweit den neuen Technologien stärker öffnen, sagte sie kürzlich in Singapur. „Ich glaube, wir sollten uns überlegen, eine digitale Währung auszugeben. Es muss eine Rolle für den Staat geben, die digitale Ökonomie mit Geld zu versorgen“, so Lagarde.[31]

Abbildung 5: Tether USD Preis und Marktkapitalisierung



Quelle: Coinmarketcap, Incrementum AG.

“A Blockchain fulfills the ideal conditions for digitizing money, assets and intellectual property.”

Princess Gisela von und zu Liechtenstein

Sie spricht von einem **„Gegengewicht“ für private Währungen** und zeigt damit, dass auch die internationalen Währungsgremien die Existenz von Bitcoin inzwischen als gegeben erachten. Auch will Lagarde, ähnlich wie Hayek, die Banken einbeziehen. Dass diese auch ihr eigenes Geld ausgeben sollen, ist aber nicht Teil des Plans. Lagarde sieht in CBDC vor allem einen Ersatz für das Bargeld: „Eine digitale Währung könnte Vorteile bringen, als letzte Rettung für Zahlungen. Und sie könnte den Wettbewerb vorantreiben, weil sie eine kosteneffiziente Alternative bietet – so wie ihr Großvater, das alte, verlässliche Papiergeld.“ Die vollständige Anonymität von Bargeld sei dann aber dahin, so Lagarde.

Sie schlägt vor, die Transaktionen sehr wohl zu speichern, die Details aber nur im Verdachtsfall an den Staat weiterzugeben. Ein heikler Gedanke – aber nicht vollkommen verrückt – zumindest in Rechtsstaaten, in denen es eine Trennung zwischen Staat und Zentralbank gibt. Lagardes eigene Experten vom IWF sind bei
—

[31] http://www.faz.net/aktuell/wirtschaft/diginomics/iwf-chefin-fordert-digitale-waehrungen-15889788.html

dem Thema übrigens ziemlich skeptisch. So heißt es in einem aktuellen IWF-Artikel zum Thema: „Alles in allem ist es noch zu früh, die Vorteile von CBDCs zu beurteilen. Notenbanken sollten die spezifischen Umstände in ihren jeweiligen Ländern berücksichtigen, den Risiken vorsichtige Aufmerksamkeit widmen und den Vorteilen anderer Lösungen. Es braucht weitere Analysen und Studien der technischen Machbarkeit und Kosten."

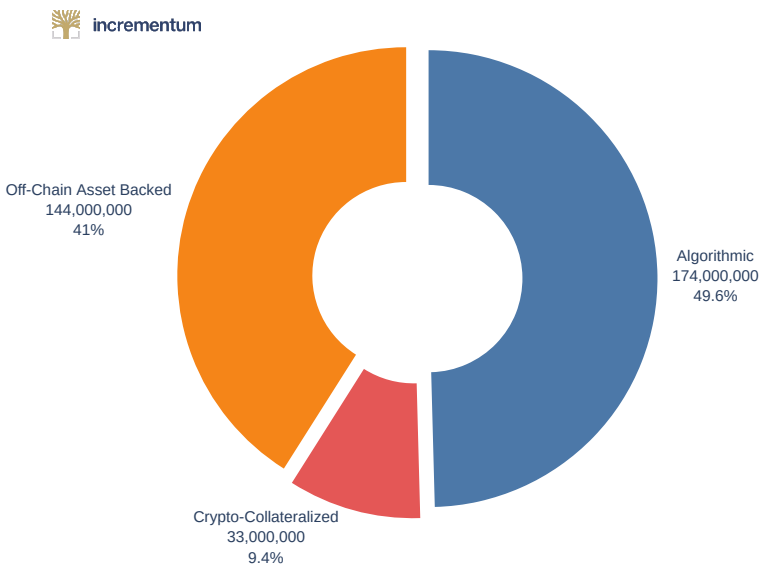
"It is a good alternative to central bank-issued money and through competition could eventually enforce more monetary policy discipline in the current system."

Princess Gisela von und zu Liechtenstein

Man muss an dieser Stelle festhalten, dass Zentralbanken notorisch langsam sind, was technische Neuerungen betrifft. Die Pläne für CBDC sind keineswegs ausgereift. Fest steht nur: Wir reden nicht von digitalem Geld, wie wir es bereits kennen. Ein Kontostand ist am Ende eine Forderung an die Bank. CBDC müssen Währungen sein, bei deren Besitz es kein Gegenparteirisiko gibt – also wie bei Bitcoin oder Gold (in eigener Verwahrung). **Auch wenn die wahre Motivation von Zentralbanken bzw. IWF hinter dem möglichen Einsatz von digitalem staatlichem Geld der Erhalt des Geldmonopols sein mag, legitimieren die Bemühungen nach eigenem digitalem Geld letztendlich indirekt private Alternativen wie Bitcoin konzeptionell.**

Es sollte niemanden überraschen, dass Schweden jenes Land ist, wo die Pläne für eine CBDC am weitesten vorangeschritten sind. Schweden gilt als Versuchslabor einer bargeldlosen Gesellschaft und stößt inzwischen an die Grenzen des Machbaren.

Abbildung 6: Kategorisierung von Stablecoins



Quelle: Incrementum AG

Längst gibt es Proteste von Bürgern gegen die vor allem von den Geschäftsbanken gepushte Abschaffung des Bargelds. Die Notenbank hat auch deshalb das E-Krona Projekt ins Leben gerufen und untersucht gerade die unterschiedlichen technischen Möglichkeiten zur Einführung einer elektronischen

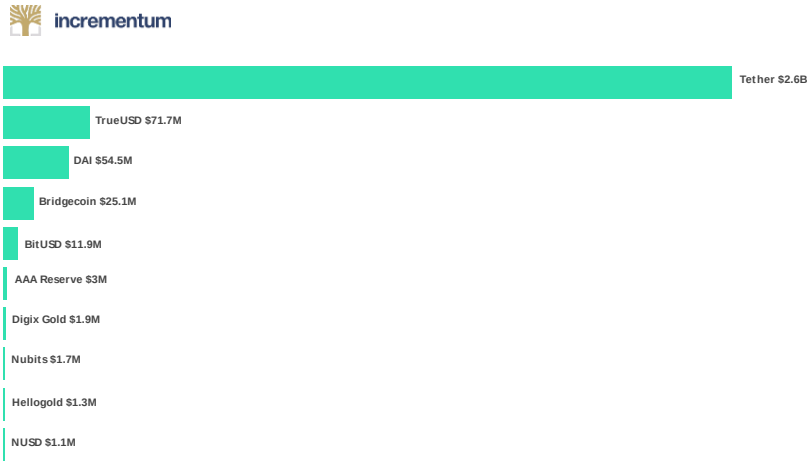
Krona. Die Riksbank, die schwedische Notenbank, hat die Regierung jetzt dazu aufgefordert, die notwendigen rechtlichen Rahmenbedingungen für eine etwaige Einführung der E-Krona zu schaffen. „Wenn die Marginalisierung von Bargeld weitergeht, kann eine digitale Krona (E-Krona) sicherstellen, dass die Öffentlichkeit noch Zugang zu staatlich garantierten Zahlungsmitteln hat“, so die Riksbank, die zudem folgende Befürchtung äußert: „Wenn wir angesichts der aktuellen Entwicklungen nicht handeln und den Zahlungsverkehr den privaten Anbietern überlassen, wird die Öffentlichkeit ultimativ komplett von privaten Lösungen abhängig sein. Das kann es der Riksbank schwer machen, sichere und effiziente Zahlungssysteme anzubieten.“[32]

“The blockchain is a distributed network that solves all the problems that we have of finance, but more broadly, it’s like a philosophy. It’s a way of life”

Mike Cernovich

Die Riksbank ist übrigens selbst schuld, hat sie doch die Bargeldversorgung in den 1990er-Jahren aus Kostengründen an die Geschäftsbanken abgetreten. Jetzt, da diese das Bargeld immer weiter zurückdrängen, suchen die Notenbanker nach Lösungen.[33]

Abbildung 7: Ein Vergleich der größten Stablecoins



Quelle: Coinmarketcap, Incrementum AG

Im Gegensatz zu Roubini glauben wir jedenfalls, dass diese Entwicklungen positiv für Bitcoin sind. Aus dieser Perspektive erst recht. Nicht nur, weil CBDC die Akzeptanz von digitalen Währungen weiter erhöhen würden und Bitcoin sich in diesem Bereich bereits etabliert hat. Auch nicht, weil das Lightning-Network für Bitcoin immer schneller wächst und damit Kryptowährungen auch für den täglichen Zahlungsverkehr wieder interessant werden. Sondern vor allem, weil Bitcoin den von der Notenbank angedachten Dienst bereits seit zehn Jahren anbietet. Und die Riksbank will sich noch mindestens zwei Jahre Zeit lassen.[34]

—

[32] http://fortune.com/2018/10/26/sweden-riksbank-e-krona/
[33] https://diepresse.com/home/wirtschaft/kolumnen/wertsachen/5391098/Der-Kampf-gegen-das-Bargeld-ist-klaeglich-gescheitert
[34] https://www.ccn.com/2-million-lightning-network-hits-major-milestone-despite-bitcoin-price-decline/

In dieser Zeit werden wir auch den dritten Teil des elektronischen Geldsektors weiter wachsen sehen, die so genannten Stablecoins. Das sind Blockchain-Entsprechungen von bestehenden Währungen, also etwa Tether (USD), um das es weiterhin wilde Kontroversen gibt. Inzwischen gibt es auch den Gemini Dollar, TrueUSD und Paxos. Und natürlich USDCoin, hinter der niemand anderer als Circle steckt, in das auch Goldman Sachs investiert ist. USDCoin wird inzwischen sogar vom Bitcoin-Giganten Coinbase eingesetzt und angeboten.[35],[36]

Aktuell gibt es mehr als 50 solche Stablecoins. Manche davon sind gar nicht an eine bestehende staatliche Währung gebunden, die meisten aber schon. Sie erfreuen sich auch wegen der fallenden Preise großer Beliebtheit, weil man seine digitalen Gelder in eine USD-Stablecoin retten kann, um dann zu warten, bis sich der Markt beruhigt hat. Freilich: Die Kontroversen rund um die Ur-Stablecoin Tether reißen nicht ab. Inzwischen untersuchen sogar die US-Behörden Vorwürfe, denen zufolge die Hintermänner von Tether und der Börse Bitfinex den Bitcoin-Preis manipuliert haben sollen.[37]

ICO-Bust und Ausblick

"It's surprising just how easy it is without any tech skill to commit cybercrimes like ransomware."

Rick McElroy,
Carbon Black security strategist

Ob hinter den Vorwürfen gegen Tether etwas steckt, oder ob es sich nur um einen Kampf der Stablecoins handelt, wissen wir nicht. Aber dass der Kryptosektor seit jeher auch fragwürdige Gestalten anlockt, ist bekannt. Insofern ist es sehr positiv, wenn sich die Behörden Krypto-Betrüger vorknöpfen. So geschehen in den USA, wo die Aufsichtsbehörde SEC nach eigenen Angaben dutzende Ermittlungsverfahren in Sachen Krypto am Laufen hat.[38]

Zwei Anbieter von ICOs (Airfox und Paragon Coin) mussten jetzt Strafzahlungen in der Höhe von jeweils 250.000 USD leisten und auch die Investoren kompensieren. Sie führten ihre ICOs durch, obwohl die SEC im Sommer ausdrücklich vor diesem Schritt gewarnt hatte, weil sie ICOs als den illegalen Verkauf von Wertpapieren betrachtet.[39]

Deutlich wirkungsvoller dürften die Strafen der SEC gegen zwei Prominente sein, die Werbung für fragwürdige Kryptowährungen gemacht hatten. Der Boxer Floyd Mayweather und der Hip-Hop-Star DJ Khaled akzeptierten im Rahmen eines Vergleichs Strafen in Höhe von 300.000 USD beziehungsweise 100.000 USD. Auch die Einnahmen aus den Promo-Aktionen in der Höhe von weiteren 300.000 USD beziehungsweise 50.000 USD mussten die Prominenten wieder abgeben.

—

[35] https://www.bloomberg.com/news/articles/2018-10-29/stable-coin-backed-by-circle-coinbase-draws-most-early-demand
[36] https://www.bloomberg.com/news/articles/2018-10-23/crypto-exchange-coinbase-to-list-stable-coin-backed-by-circle?srnd=cryptocurrencies
[37] https://www.bloomberg.com/news/articles/2018-11-20/bitcoin-rigging-criminal-probe-is-said-to-focus-on-tie-to-tether
[38] http://fortune.com/2018/11/02/sec-ico-report-cryptocurrency-scams/
[39] http://fortune.com/2018/11/16/sec-airfox/

Laut SEC hatten sie auf Social Media Werbung für ICOs gemacht ohne offenzulegen, dass sie dafür bezahlt werden.

Beide Prominente hatten Werbung für Centra gemacht, dessen Hintermänner die SEC schon länger im Visier hat. „Anleger sollten skeptisch sein bei Investmentratschlägen, die auf Social-Media-Plattformen gepostet werden, und keine Entscheidungen auf Basis von Empfehlungen von Prominenten treffen", warnte Steven Peikin, Co-Direktor der SEC. „Social Media- Influencer" seien oft bezahlte Promoter.[40]

"For Mises, gold's industrial role is an impediment to performing its monetary role, an impediment with which he is happy to contend compared to the alternative of money whose supply is controlled by governments."

Saifedean Ammous

Während wir es als positiv erachten, dass die Behörden hier eingeschritten sind, so muss man sagen: Es ist wohl ein Tropfen auf den heißen Stein. Anleger sollten extrem vorsichtig mit jeder Form der Information umgehen, die sie aus dem Umfeld der Krypto-Medien und Krypto-Influencer beziehen. Drei voneinander unabhängige Untersuchungen haben gezeigt, dass sowohl die Medien, als auch so genannte Rating-Agenturen und einzelne Persönlichkeiten in den sozialen Medien und auf YouTube hochgradig korrupt sind.

Vielleicht sollte das auch niemanden schockieren, angesichts der Tatsache, dass das Produkt auch als Zahlungsmittel eingesetzt werden kann. Dennoch ist das Ausmaß der Korruption erschreckend, gerade was die ICO-Berichterstattung betrifft. Das „Breaker" Magazin hat 22 verschiedene Krypto-Medien von einer Fake-Adresse eines angeblichen russischen PR-Mannes aus angeschrieben. Das Ergebnis: mehr als die Hälfte der Websites hätte Geld für Artikel genommen, ohne diese als „Anzeige" oder „Sponsored" zu kennzeichnen. Manche waren sogar bereit, vorgefertigte PR-Texte einfach zu übernehmen und als eigenen Text auszugeben. Die kleinsten Websites nahmen weniger als 300 USD. Die größten mehr als 3.000 USD. In jedem Fall erklärt diese Untersuchung, warum es im Internet so viel miserabel geschrieben Texte zu relativ obskuren Coins gibt. Hier wird Werbung gemacht, ohne das publik zu machen. Unter den Websites, die Geld für Berichte nehmen, sind einige der bekanntesten Namen im Kryptosektor. Aber um fair zu bleiben: Rund zehn der angeschrieben Websites haben das Angebot sofort abgelehnt.[41]

Aber News-Websites sind nur die Spitze des Eisbergs. Oft werden die verdeckten Werbekampagnen von so genannten ICO-Agenturen betreut, die Preislisten für verschiedene Kanäle parat haben. Diese Agenturen kümmern sich nicht nur um die Vermarktung einer Coin auf den einschlägigen Websites, sondern sorgen auf Wunsch auch für Kommentare und Traffic in den Telegram-Gruppen und anderen Sozialen Netzwerken. Auch viele Personen, die auf YouTube Cryptocoins oder ICOs besprechen, lassen sich für ihren Service bezahlen. Oft in Ether oder der Coin, die

—

[40] https://diepresse.com/home/wirtschaft/5538851/KryptogeldWerbung_Hohe-Strafen-fuer-Boxer-Mayweather-und-DJ-Khaled
[41] https://breakermag.com/we-asked-crypto-news-outlets-if-theyd-take-money-to-cover-a-project-more-than-half-said-yes/

angepriesen werden soll. Die Recherchen von Breaker, Techcrunch und Reuters zeichnen ein Bild einer zutiefst korrupten Industrie, in deren Zentrum die Jagd nach Geld durch ICOs steht.[42,43]

"Everything will be tokenized and connected by a blockchain one day."

Fred Ehrsam

Wenn der Preisverfall in Kombination mit diesen Recherchen und dem Crack-Down der SEC gegen ICOs und ihre Proponenten dazu führt, dass dieser Sumpf trocken gelegt wird, dann ist das nur zu begrüßen. Auch das ist Teil der Professionalisierung des Sektors, die wir gerade erleben.

Was die Mainstream-Akzeptanz betrifft, so brauchen wir uns keine Sorgen mehr zu machen. Jahre nach dem ersten Auftritt von Bitcoin bei „The Good Wife" soll bald ein Kinofilm mit Kurt Russel in die Kinos kommen. Der Titel lautet schlicht: „Crypto".[44]

Kurz vor Redaktionsschluss dieses Crypto Research Reports ist noch diese Nachricht hereingekommen: Der Elektronikgigant Samsung arbeitet – angeblich – an einer Kryptowallet für seine Smartphones. Sollte an diesem Gerücht etwas dran sein, wäre das ein weiterer großer Schritt in den Mainstream. Und eine Bestätigung der alten These: Während die Preise fallen, finden die wahren Innovationen statt. [45]

—

[42] https://www.reuters.com/article/us-crypto-currencies-promoters-specialre/special-report-little-known-to-many-investors-cryptocurrency-reviews-are-for-sale-idUSKCN1NW17S
[43] https://techcrunch.com/2018/09/18/inside-the-pay-for-post-ico-industry/
[44] https://www.imdb.com/title/tt8563452/
[45] https://www.sammobile.com/2018/12/11/exclusive-samsung-bitcoin-app-cold-wallet-cryptocurrencies/

bitpanda

Home of **Cryptocurrency**

TRADEN. SENDEN. TAUSCHEN.

Besuche uns auf **www.bitpanda.com**
und installiere unsere App

JETZT BEI Google Play

Crypto Concepts: Verwahrungslösungen für Kryptowährungen

“The next level for the crypto community is for additional institutions to enter the space. They will only do so if there is a super secure way of storing the assets or the private key.”

Philipp Vonmoos, CEO, Swiss Crypto Vault AG

Key Takeaways

- **Zu keinem Zeitpunkt sollte ein Anbieter von Krypto-Verwahrungslösungen Zugriff auf die unverschlüsselte Private Key eines Kunden haben. Der Industriestandard für die Schaffung von Private Keys könnten Hardware Security Modules (HSMs) werden.**
- **Bei der Bewertung einer Krypto-Verwahrungslösung für Ihr Unternehmen sollten Reputation und Erfahrung berücksichtigt werden.**
- **Berücksichtigen Sie jene Eigenschaften, die Ihr Unternehmen bei der Bewertung einer Krypto-Custody-Lösung benötigt, wie Geschwindigkeit, Benutzerfreundlichkeit, Versicherung, konfigurierbare Governance und physische/digitale Sicherheit.**

Photo: *Joseph Annuzzi*

Verfasst von Joseph Annuzzi Jr.

Joseph Annuzzi Jr. ist Gründer und CEO einer dezentralen Kryptowährungsbörse und der Entwickler eines neuartigen, für Verbraucher entwickelten Algorithmus zum Schutz von private Keys. Er ist Softwarearchitekt und Unternehmer aus dem Silicon Valley und zudem Autor einer Reihe von computerwissenschaftlichen Lehrbüchern, die von Pearson Education, Inc. veröffentlicht wurden. Weiters betreibt er die Webpage cryptocustodysolutions.io, welche eine renommierte Quelle für den Bereich Verwahrungslösungen für Kryptowährungen ist.

In diesem Artikel untersuchen wir Lösungen für die institutionelle Verwahrung von Kryptowährungen. Kryptowährungs-Custody-Lösungen sind notwendig, da die unsachgemäße Handhabung und Lagerung von Kryptowährungen zum Verlust oder sogar Diebstahl der eigenen Kryptowährungsguthaben führen können. Selbstverwaltete Kryptowährungskonten sind nicht gegen Verlust oder Diebstahl versichert und die Strafverfolgungsbehörden sind selten in der Lage, gestohlene Kryptowährungen aufzuspüren. Auch von regulatorischer Seite können professionelle Verwahrungslösungen obligatorisch sein, wie dies z. B. bei Investmentfonds der Fall ist. Somit besteht ein erhöhter Bedarf nach professionellen Lösungen.

Nicht jede institutionelle Verwahrungslösung ist gleichwertig

"As the crypto-asset class seasons and institutional demand builds, there are a plethora of opportunities for traditional firms to engage in the eco-system. These include the provision of custodial and asset management services as well as traditional brokerage functions like market-making."

CNBC

Beginnen wir mit einem kurzen Überblick über einige der Komponenten, die für die Verwendung von Kryptowährung notwendig sind. An erster Stelle steht ein kryptographisches Schlüsselpaar in Form eines öffentlichen Schlüssels (public key) und eines privaten Schlüssels (private key). Der öffentliche Schlüssel wird verwendet, um eine öffentliche Kryptowährungsadresse bereitzustellen, die der Öffentlichkeit frei zugänglich gemacht werden kann. Eine Kryptowährungsadresse ist einer E-Mail-Adresse sehr ähnlich, d. h. jeder, der die Adresse kennt, kann an diese Adresse Coins oder Token überweisen. Eine Kryptowährungsadresse führt Buch über das Saldo und kann Beträge an Kryptowährung empfangen und senden, vorausgesetzt, der Besitzer der Kryptowährungsadresse hat Zugriff auf den zugehörigen privaten Schlüssel. Der private Schlüssel muss immer privat bleiben und ist wie ein Passwort für eine bestimmte Kryptowährungsadresse. Nur der Besitzer einer Kryptowährungsadresse sollte Zugriff auf den privaten Schlüssel haben. Die Offenlegung des privaten Schlüssels gegenüber einem Unbefugten stellt ein Diebstahlsrisiko für das Guthaben einer Kryptowährungsadresse dar. Um über ein Guthaben auf einer bestimmten Kryptowährungsadresse zu verfügen, beispielsweise durch eine Transaktion, ist der Zugriff auf den privaten Schlüssel dieser Adresse erforderlich. Genauso wie man einem unbefugten Dritten keinen Zugriff auf sein E-Mail-Passwort gewährt, muss auch der Zugriff auf einen privaten Schlüssel geschützt sein. Die Kryptowährungsadresse oder der mit einer Kryptowährungsadresse verbundene Saldo ist nicht der zu schützende Vermögenswert. **Der zu schützende Vermögenswert ist der private Schlüssel eines Benutzers, der den Zugriff zu einer Kryptowährungsadresse verschafft.** Die sichere Lagerung des privaten Schlüssels erfordert demnach äußerste Sorgfalt.

In der vergangenen Ausgabe des Crypto Research Report haben wir uns mit diesem Thema beschäftigt und die gesamte Ausgabe danach betitelt („Handy Theft Edition"). Der Diebstahl von Kryptowährungen ist ein Betätigungsfeld der Cyberkriminellen, **denn einmal gestohlen, ist es unmöglich eine Transaktion rückgängig zu machen**. Die einzige Möglichkeit, Gelder wiederherzustellen, besteht darin, Zugang zu jenem privaten Schlüssel zu erhalten, der das gestohlene Geld vereinnahmt hat.

Doch ein Diebstahl ist nicht auf Kriminelle beschränkt, die sich in die Computersysteme eines Unternehmens hacken. Der Diebstahl könnte genauso gut innerhalb eines Unternehmens begangenen werden, wenn ein oder mehrere ungeeignete Mitarbeiter mit der Verwahrung jener privaten Schlüssel betraut werden, die den Zugang zu den Kryptowährungsguthaben des Unternehmens ermöglichen.

Werfen wir einen Blick darauf, wie Institutionen wie beispielsweise eine Gesellschaft oder eine ähnlich organisierte Einheit organisiert sind. Ein Unternehmen besteht typischerweise aus mehr als einer Person: Mitarbeiter, Verwaltungsrat, Geschäftsleitung und weitere Gruppen bilden eine Gesellschaft. Wer soll nun die Rechte auf den Zugang und die Sicherung des privaten Schlüssels haben, der mit einer Kryptowährungsadresse verbunden ist? Soll es der Vorstand sein? Eine Führungskraft wie der CEO oder der CFO? Ein bestimmter Mitarbeiter wie z.B. ein Softwareentwickler? Oder eine Kombination aus mehreren Parteien?

"There are a lot of investors where custodianship was the final barrier. Over the next year, the market will come to recognize that custodianship is a solved problem. This will unlock a big wave of capital."

Multicoin Capital Hedge Fund Manager, Kyle Samani

Angesichts der Komplexität der Speicherung und Sicherung von Kryptowährungen bietet sich für innovative Unternehmen die Möglichkeit, Verwahrungslösungen für Kryptowährungen für jene anzubieten, denen angesichts der Komplexität die Ressourcen fehlen, die für die Sicherung privater Schlüssel für Kryptowährungsadressen mit großen Beständen erforderlich sind.

Über unseren Twitter-Channel @cryptomanagers haben wir Anbieter von Verwahrungslösungen eingeladen, uns Informationen über ihre Produkte zu geben und an diesem Artikel mitzuwirken. Die folgenden fünf Unternehmen, welche Verwahrungsdienstleistungen von Kryptowährungen anbieten, haben sich an uns gewandt. In exklusiven Interviews mit den Sicherheitsbeauftragten haben wir erfahren, wie diese verschiedenen Unternehmen versuchen, das Custody-Problem für Investoren zu lösen. Herzlichen Dank an alle beitragenden Unternehmen für die auskunftsfreudige Mitarbeit. Die hier dargestellten Ergebnisse basieren auf den von den Anbietern zur Verfügung gestellten Informationen und sind ohne Gewähr.

Crypto Storage AG

Die erste Krypto-Verwahrungslösung, die wir untersucht haben, war jene der Crypto Storage AG.[46] Die Crypto Storage AG ist eine Tochtergesellschaft der 2017 gegründeten Crypto Finance AG mit Sitz in Zug (ZG) in der Schweiz. Sie bietet Dienstleistungen zur sicheren Speicherung von blockchainbasierten Assets über eine bemerkenswerte Infrastrukturlösung an. Mehr als 40 interne und 13 externe Fachleute sind an der Erstellung und Implementierung beteiligt. Mit dem CEO Stijn Vander Straeten und der

—

[46] https://www.cryptofinance.ch/en/storage

technischen Vertriebsingenieurin und Projektleiterin für Implementierung Maria Sommerhalder haben wir ein persönliches Gespräch geführt.

"Blockchain Technology Could Save Banks $12 Billion Per Year."

Mohsin Jameel

Die Infrastruktur der Crypto Storage AG besteht aus einer Transaktionsbenutzeroberfläche, die mit der Backend-Server-Infrastruktur kommuniziert, und sich auf die Buchhaltung wie den Nachrichtenaustausch zwischen den Hardware Security Modulen (HSMs) und den Hardware Approval Terminals (ATs) spezialisiert. Ein HSM ist ein Computer mit kryptographischen Verarbeitungsfunktionen, der innerhalb einer manipulationssicheren Hardwarevorrichtung arbeitet, die in der Lage ist, Ver- und Entschlüsselung, Schlüsselerzeugung sowie die Erstellung und Verifizierung digitaler Signaturen durchzuführen. Einige HSM-Hersteller erlauben die Anpassung der Verarbeitungsmöglichkeiten durch programmierbare Erweiterungen, die als Software Development Kits zur Verfügung stehen oder auf Sonderanfragen hin möglich sind.

Freigabeterminal und Hardware-Sicherheitsmodul erhöhen die Sicherheit; Quelle: Crypto Storage AG

Die Backend-Server-Infrastruktur und die HSMs sind geo-redundant über die Schweiz verteilt. Einer der Standorte war früher ein Militärbunker in den Schweizer Alpen. Ortsunabhängigkeit ist ein starkes Argmuent dafür, dass im Falle eines Ausfalles an einem Standort ein anderer Standort als Backup zur Verfügung steht. Die ATs werden beim Kunden installiert und sind kryptographisch durch verschlüsselte Kommunikation mit den Backend-Servern und HSMs verbunden. Das Unternehmen hinter den HSMs und ATs heißt Securosys mit Sitz in Zürich. Das Unternehmen, das sich mit den operativen Sicherheitsaspekten und der Backend-Softwareentwicklung beschäftigt, ist die ebenfalls in Zürich ansässige AdNovum. Diese Unternehmen haben sowohl bei der Entwicklung als auch der Implementierung der Lösung der Crypto Storage AG mitgewirkt.

Das Besondere an der Lösung der Crypto Storage AG ist die Kombination von HSM und ATs, die kryptographisch gepaart sind. Das ermöglicht sowohl Hot- als auch Coldstorage für den Kunden, bei der die privaten Schlüssel auf dem HSM erzeugt werden und das Gerät nie verlassen. Die Crypto Storage AG kann aufgrund der manipulationssicheren Konstruktion nicht auf jene privaten Schlüssel des

Kunden zugreifen, die auf dem HSM gespeichert sind. Darüber hinaus bieten die kryptographisch gekoppelten ATs Hot-Wallets ähnliche Funktionen, **bei denen der Kunde Auszahlungstransaktionen aus der Cold-Storage initiieren kann, während er sich auf eine sichere Vorrichtung verlassen kann.** Die Crypto Storage AG bezeichnet dies als „Deep cold storage, dass die Flexibilität und Geschwindigkeit eines Hot-Walltes ermöglicht".

"The New York State Limited Purpose Trust charter, which now enables Coinbase Custody to act as a Qualified Custodian for crypto assets, builds on our unparalleled success as a crypto custodian while holding the company to the same exacting fiduciary standards and oversight of other, mature financial institutions operating in New York."

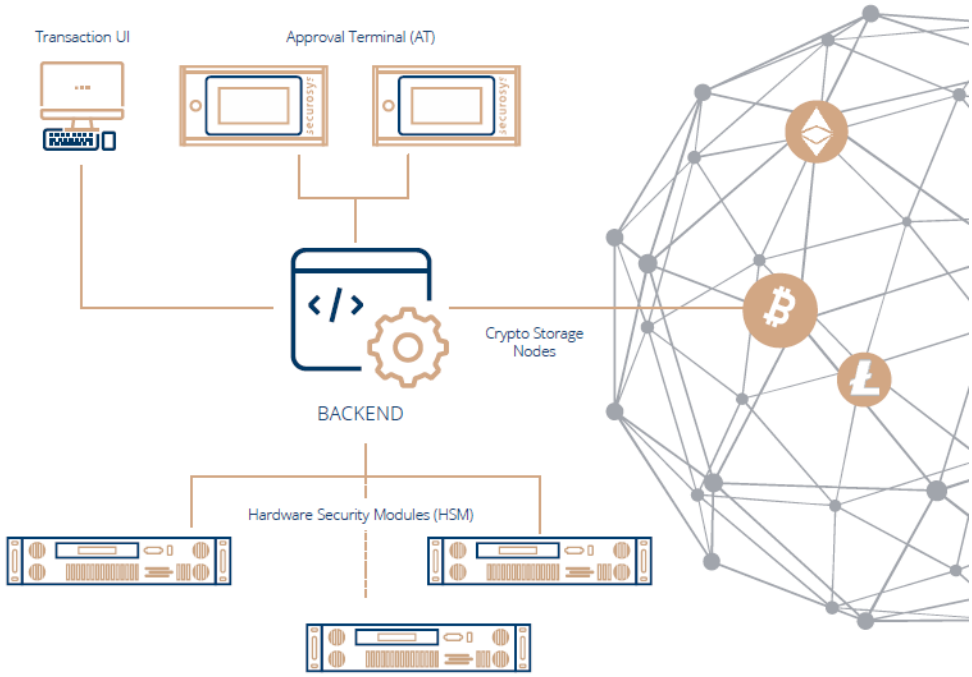
Asiff Hirji,
Coinbase COO and president

Darüber hinaus ist der Kunde in der Lage, ein individuelles Genehmigungsverfahren zu entwerfen, in dem er seine eigenen betrieblichen Prozesse zur Genehmigung von Kryptotransaktionen abbilden kann. Das Genehmigungsverfahren ermöglicht die Erstellung von Regeln, die dann mit dem privaten Schlüssel im HSM gespeichert werden. So kann beispielsweise ein m-of-n-Genehmigungsschema konfiguriert werden, um eine Transaktion einzuleiten, bei der eine oder mehrere Gruppen von Genehmigenden erforderlich sind. Zeitverzögerungen können auch konfiguriert werden, um sicherzustellen, dass jede Auszahlungstransaktion dem für den Kunden geeigneten Governance-Verfahren folgt. Die ATs haben die gleichen Sicherheitsstandards wie HSMs und erfordern zur Einleitung einer Auszahlungstransaktion sowohl eine personalisierte Smartcard als auch einen PIN-Code pro Genehmiger. Diese Lösung ist ein extrem leistungsfähiges und dennoch hochsicheres Mittel zur Speicherung und Transaktion von Kryptowährungen.

Die Crypto Storage AG unterstützt 59 der an ihrer Marktkapitalisierung gemessenen Top 100 Kryptowährungen und neue Kryptowährungen werden regelmäßig hinzugefügt. Zielkunden sind Banken, Vermögensverwalter, Family Offices, Broker, Versicherungen, Pensionskassen, Börsen und Stiftungen. **Versichert ist die technische Infrastruktur, die einige aber nicht alle Kundenvermögen umfassen kann.** Wie viel vom jeweiligen Kundenvermögen versicherbar ist, sollte auf jeden Fall berücksichtigt werden, wenn man die Crypto Storage AG als potenziellen Verwahrungs-Infrastrukturanbieter in Betracht zieht.

Insgesamt verfügt die Crypto Storage AG über eine sehr überzeugende Lösung, die bei der Wahl einer extrem sicheren Speicherung mit nahezu sofortigen Auszahlungsmöglichkeiten und einem auf Wunsch hochkonfigurierbaren Governance-Prozess definitiv berücksichtigt werden sollte.

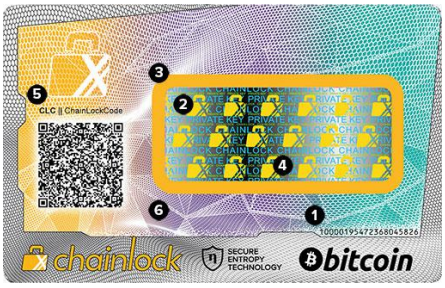
Abbildung 8: System Architektur der Crypto Storage AG



Quelle: Crypto Storage AG

Card Wallet

Card Wallet ist das nächste von uns geprüfte Verwahrungsprodukt, das eine Koproduktion von Coinfinity und der Österreichischen Staatsdruckerei ist. **Coinfinity ist ein Bitcoin-Broker mit Sitz in Österreich**, der Krypto-bezogene Dienstleistungen für Unternehmen und Endkunden anbietet. Coinfinity bietet Konsumenten unter anderem die Möglichkeit, Bitcoin an fast 4000 Standorten in ganz Österreich im Einzelhandel zu kaufen und ist auch für die Installation des ersten Bitcoin-Automaten in Österreich bekannt.



Card Wallet von Coinfinity; Quelle: Coinfinity GmbH

Die Österreichische Staatsdruckerei hat sich mit ihren Dienstleistungen im Bereich des hochsicheren und kontrollierten Drucks von Ausweispapieren einen Namen gemacht. Gemeinsam nutzen die beiden Unternehmen ihr Know-how für den Betrieb vom sogenannten Card Wallets. Ein persönliches Gespräch konnten wir mit Max Tertinegg, dem Geschäftsführer von Coinfinity, führen.

Card Wallet ist **eine manipulationssichere Karte im Scheckkartenformat, die Kunden die Möglichkeit bietet, Bitcoin Private Keys offline zu speichern.** Konzeptionell ist die Lösung ähnlich einem Paper-Wallet, d. h. wenn man den privaten Schlüssel auf einem Blatt Papier notiert. Der Unterschied besteht darin, dass das Card Wallet eine Polycarbonat-Kunststoffkarte ist und ein privater Bitcoin-Schlüssel direkt auf die Karte gelasert und dann mit einem manipulationssicheren Aufkleber abgedeckt und versiegelt wird. **Der private Schlüssel wird jedoch bei Card Wallet im**

Rahmen eines speziellen Verfahrens generiert, das Card Wallet als „Secure Entropy Technology“ (SET) bezeichnet.

Laut Max Tertinegg nutzt SET drei Zufallszahlengeneratoren zur Hervorbringung der Entropie, die den privaten Bitcoin-Schlüssel auf der Karte erzeugt. Entropie ist eine Möglichkeit, eine unvorhersehbare Ausgabe von Informationen zu erzeugen, die praktisch unmöglich zu reproduzieren ist. Die Zufallszahlengeneration besteht aus einer Hardwarevorrichtung, einer Softwarelösung und einer von Menschen generierten Zufallszahl. Letztere wird vom Personal bei Card Wallet durch manuelles Würfeln gebildet. Die Kombination dieser drei erzeugten Zufallszahlen wird als Eingabe für die Generierung eines privaten Bitcoin-Schlüssel verwendet, der dann auf eine physische Karte gelasert wird.

Der Kartendruck erfolgt in einem gesicherten Raum der Österreichischen Staatsdruckerei und wird laut Max Tertinegg durch etwa sieben oder acht verschiedene physische Firewalls geschützt. Keine Kopie eines private Keys wird jemals auf einem permanenten Speichermedium gespeichert und – sofern die Einrichtung ihre Sicherheitsgarantien einhält – erhält das Personal nie Einblick in die private Keys.
Die Karte kostet 59 EUR und unterstützt derzeit ausschließlich Bitcoin. In Zukunft sollen Ether und weitere Kryptowährungen unterstützt werden. Card Wallet ähnelt einer Prepaid-Geschenkkarte und scheint am besten geeignet für geringe Kryptowährungsbeträge zu sein, beispielsweise um ein Familienmitglied oder einen Bekannten zu beschenken. In Anbetracht der Fälschungsmöglichkeit von Scheckkarten sollten Card Wallets nur direkt vom Hersteller bezogen werden.

Potenzielle Schwachstellen von Kartenspeicherlösungen

1.) Da die privaten Schlüssel für einen kurzen Moment auf einem Computersystem im temporären Speicher vorhanden sind, bevor sie auf eine Karte geätzt werden, könnte ein Dieb in oder außerhalb des Unternehmens, möglicherweise Zugang zu einem oder mehreren privaten Schlüsseln erhalten. Dieses Angriffsszenario ist höchst unwahrscheinlich und würde die Koordination vieler verschiedenen Personen erfordern.

2.) Während des Versands einer Karte könnte jemand möglicherweise eine echte Karte auf dem Weg zu einem Kunden abfangen und gegen eine gefälschte Karte austauschen. Eingeschriebener Versand verringert das Risiko deutlich.

3.) Es könnte auch passieren, dass man eine gefälschte Karte auf einem Online-Marktplatz wie eBay oder Amazon erwirbt. Eine gefälschte Karte würde bedeuten, dass der ahnungslose Kunde eine Einzahlungsadresse erhält, die allerdings von einem Kriminellen kontrolliert wird, sodass alle Bitcoins von einem Hacker gestohlen werden könnten. Fälschungen sind nicht ausgeschlossen, da es bereits Fälle von gefälschten Hardware-Wallets für Verbraucher gab, die auf Online-Marktplätzen wie eBay und Amazon zum Verkauf angeboten wurden.

Daenerys & Co.

Daenerys & Co ist eine Krypto-Verwahrungslösung, die von der Silver Bullion Group entwickelt worden ist. Die Silver Bullion Group wurde 2009 von Gregor Gregersen gegründet und hat ihren Sitz in Singapur. Die Silver Bullion Group bietet die sichere Verwahrung von Edelmetallen, Versicherungsdienstleistungen sowie Edelmetallhandel und Edelmetallfinanzierungen an. Seit 2009 hat die Silver Bullion Group über 400 Millionen USD Umsatz erzielt. Genau wie die Silver Bullion Group entsprang Daenerys & Co aus der Notwendigkeit, Verwahrungs- und Compliance-Probleme im Zusammenhang mit digitalen Vermögenswerten zu lösen. Gregor Gregersen und Clint Mark Gono positionieren Daenerys als eine führende

Kraft in diesem Bereich mit einem einzigartigen Geschäfts- und Sicherheitsprotokoll namens Gregersen-Gono Physical Crypto Storage Standard (GGPCS).[47] GGPCS wird derzeit beim Tresorunternehmen der Silver Bullion Group The Safe House eingesetzt.

Der Prozess beginnt in einem sicheren Tresor auf Computern, die keine Internetverbindung haben. Diese Computer erzeugen einen privaten Bitcoin-Schlüssel im temporären Speicher des Computers, verschlüsseln dann diesen privaten Schlüssel mit einem ersten Schlüssel und verschlüsseln ihn dann ein weiteres Mal mit einem zweiten Schlüssel. Jeder dieser verschlüsselten privaten Schlüssel wird dann als QR-Code auf eine eigene Polycarbonat-Kunststoffkarte – eine Primärkarte und eine Wiederherstellungskarte – lasergraviert. Sobald der Verschlüsselungsprozess abgeschlossen ist, wird der private Schlüssel aus dem temporären Speicher des Computers gelöscht. Anschließend werden die Karten analysiert, um sicherzustellen, dass der Ätzprozess ordnungsgemäß abgelaufen ist und der QR-Code lesbar ist. Polycarbonat-Kunststoff ist ein Material, das in der Lage ist, **lange Zeiträume unbeschadet zu überdauern, und stets lesbar bleibt, selbst wenn die Karte bis zu maximal 30% beschädigt sein sollte.** Nach Abschluss des Ätzprozesses wird die Karte in ein Schließfach gelegt und ist dadurch sicher wie physisches Gold gelagert. Aus Sicherheitsgründen ist es sinnvoll, eine Primärkarte und eine Wiederherstellungskarte zu haben. Sollte die Hauptkarte Schäden erleiden, kann die an einem anderen physischen Ort aufbewahrte Wiederherstellungskarte verwendet werden, um alle mit diesem privaten Bitcoin-Schlüssel verbundenen Vermögenswerte wiederherzustellen.

Verschlüsselte Polycarbonat-Karte von Daenerys & Co., Photo: Daenerys & Co.

Tresorraum im von Daenerys & Co. Photo: Deanerys & Co

Sobald der Kunde Zugang zu der mit einem bestimmten privaten Schlüssel verbundenen Einzahlungsadresse hat, kann er eine Einzahlung auf diese Adresse veranlassen. Auszahlungen von dieser Adresse erfordern dagegen einen mehrstufigen Prozess, um sicherzustellen, dass die Auszahlungsanfrage tatsächlich von dem Kunden kommt, der die Auszahlung veranlasst. Vor einer Auszahlung ist der Kunde verpflichtet, die Regeln für das Autorisierungsmandat zu konfigurieren. Diese Regeln können die Führungsstruktur des Unternehmens des Kundens widerspiegeln, wenn z. B. ein oder mehrere bevollmächtigte Vertreter wie der CEO, der CFO oder der Compliance Officer verpflichtet sind, eine solche Transaktion zu genehmigen. Daenerys verwendet eine Live-Videokonferenz, um den Vertreter zu authentifizieren, der die Auszahlung veranlasst, und jede Auszahlung kann nur an eine zuvor genehmigte Adresse erfolgen.

—

47 https://www.daenerys.co/physical-cryptocurrency-storage-white-paper

Daenerys bietet auch eine optionale Versicherungspolizze an, bei der eine individuelle Karte auf bis zu 5 Millionen USD versichert werden kann. Der Versicherungsanbieter mit Sitz in London hat ein Rating von A+ von Standard & Poor's.

Blockvault

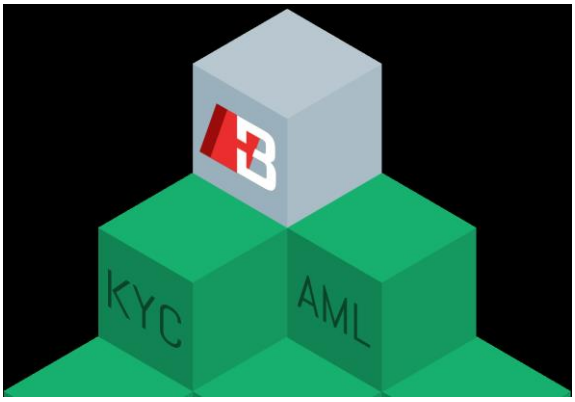
"A lot of people are unaware in this new gold rush, people are using cloud wallets and not securing their money."

Rick McElroy

Eine weitere, von uns untersuchte Verwahrungslösung für Kryptowährungen ist Blockvault, ein Unternehmen das von Goldmoney Inc. betrieben wird. Das Gespräch konnten wir mit Josh Crumb, Mitbegründer und Vorstand von Goldmoney sowie Will Felsky, Direktor für Operations von Blockvault, führen. Goldmoney ist ein Unternehmen, das institutionellen Anlegern die Möglichkeit bietet, in Edelmetalle zu investieren. Das Unternehmen wurde 1999 gegründet **und ist eine an der Toronto Stock Exchange (XAUMF) notierte Aktiengesellschaft**. Das von Goldmoney verwaltete Kundenvermögen beläuft sich aktuell auf rund **2 Milliarden USD.** Goldmoney ist darüber hinaus **ein schuldenfreies Unternehmen mit Barreserven von mehr als 100 Millionen USD.**

Da Goldmoney im Verwahrungsgeschäft von Edelmetallen tätig ist, hat das Unternehmen Zugang zu Edelmetall-Lagerstätten auf der ganzen Welt. Goldmoney hat die Notwendigkeit erkannt, ähnliche Custody-Lösungen für institutionelle Kunden im Krypto-Bereich anzubieten. Sie nutzen ihr Netzwerk von Tresoranbietern auf der ganzen Welt für Blockvault.

Blockvault offeriert seinen Kunden eine Offlinespeicherung von Krypto-Schlüsseln. Die privaten Schlüssel werden von Blockvault erstellt, wobei die Methode zur Generierung privater Schlüssel nicht offengelegt wird. Unabhängig davon können die Kryptoanlagen des Kunden durch eine Versicherungspolizze abgedeckt sein. Der Wirtschaftsprüfer der Gesellschaft ist KPMG, der mit der Überprüfung beauftragt wurde, ob sich die von Blockvault verwalteten Vermögenswerte tatsächlich den Tresoren befinden. KPMG ist auch der Auditor von Goldmoney, für die sie IASC-Audits zur Bestätigung der Verwahrung von Goldbarren durchführen. Blockvault bietet auch Versicherung durch unterschiedliche Versicherungsgesellschaften an. Blockvault merkte zudem an, dass ihre Tresoranbieter, Wirtschaftsprüfer und Versicherungspartner allesamt börsennotierte Unternehmen sind. Sie arbeiten derzeit mit Tresoranbietern in Kanada, den Vereinigten Staaten, Großbritannien, der Schweiz, Dubai, Singapur und Hongkong zusammen.



Blockvault konzentriert sich auf Know-Your-Customer und Anti-Geldwäsche.; Photo: Blockvault

Blockvault hat uns eine Übersicht über die einzelnen Schritte von der Eröffnung eines Kontos bis zur Durchführung einer Überweisung gegeben. Der Prozess beginnt mit der Überprüfung des Kunden (KYC) und Kontrollen zur Einhaltung der einschlägigen Vorschriften zur Geldwäsche (AML) während des Onboarding-Prozesses des Kunden. Nach Abschluss des Onboarding-Prozesses erhält der Kunde eine Handelsquittung mit einer Liste von Adressen, bei denen er seine Krypto-Gelder einzahlen kann. Die Zielkunden von Blockvault sind regulierte oder qualifizierte Finanzinstitute, Banken, Broker-Dealer,

registrierte Fonds, Kryptominer und weitere ähnliche Unternehmen, die KYC/AML-Tests auf Bankenebene bestehen können. Zielkunden sind jene Unternehmen, die 50 Millionen USD oder mehr in Kryptowährungen sicher verwahren wollen, auch wenn sie bereits Kunden ab einem Wert von 1 Million USD akzeptieren. **Blockvault empfiehlt, dass jede Adresse Kryptowährungen im Gegenwert von ca. 50.000 USD speichert, sodass bei einer Einzahlung von 1 Million USD dieser Vermögenswert auf 20 verschiedenen Kryptoadressen aufgeteilt werden kann und mit jeweils einem entsprechenden Schlüsselpaar geschützt wird.** Jede Einzahlung wird mit einem Handelsbeleg versehen und das Governance-Modell für die Ein- und Auszahlung ist vom Kunden individuell gestaltbar. Üblicherweise wird dieses im Rahmen des Vertragsverhältnisses mit Blockvault festgelegt. Die Höchstversicherungssumme ist Gegenstand einer individuellen Vereinbarung zwischen dem Kunden und Blockvault. Auszahlungen und der Handel mit Kryptowährungswerten werden innerhalb eines Werktages durchgeführt.

"As to storing coins safely, I'd say a hardware wallet, however a lot of care is required in avoiding compromised hardware. Using multiple hardware wallets from multiple vendors in a multisig configuration would probably be the safest at this point."

Mark Karpelès, Former Chief Eecutive of Mt.Gox.

Zu den Vermögenswerten, die Blockvault in seinen Tresoren schützt, gehören Bitcoin, Bitcoin Cash, Ether, XRP, Litecoin sowie alle ERC20-Token. In Kürze wird auch XLM unterstützt werden. Blockvault erwähnte auch die Möglichkeit das Finanzinstitute, das Blockvault-Service mit einem White Label versehen und es ihren eigenen Kunden anbieten.

Insgesamt scheint Blockvault gut positioniert zu sein. Jedes Unternehmen, das diese Lösung in Betracht zieht, sollte sich nach den Methoden zur Generierung und Speicherung von privaten Schlüsseln erkundigen und auch nach den Bedingungen für eine Versicherung fragen.

Swiss Crypto Vault AG

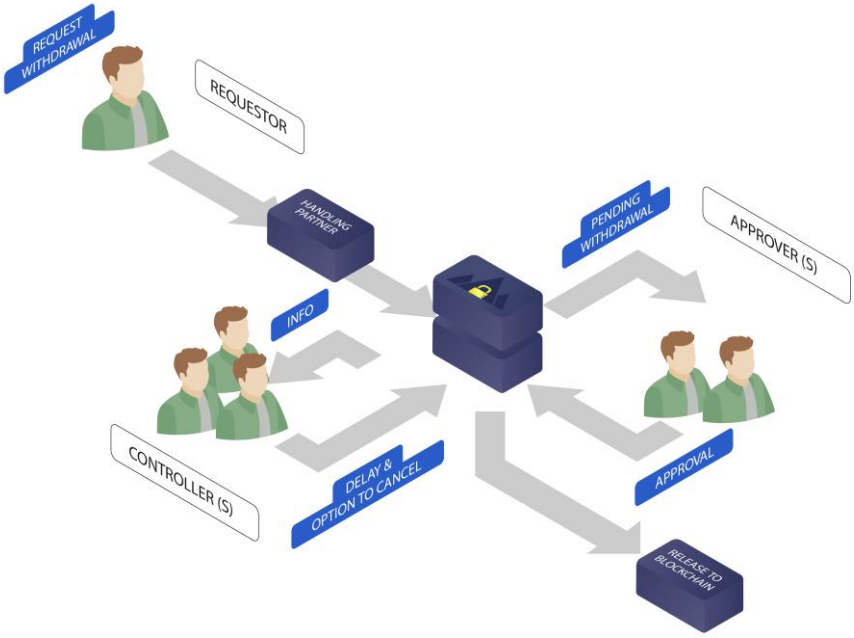
Swiss Crypto Vault AG (SCV) ist eine hochsichere Krypto-Verwahrungslösung für institutionelle Investoren und vermögende Privatpersonen (HNWI). Es ist ein Joint-Venture zwischen der Bitcoin Suisse AG und der Swiss Gold Safe AG. Das Interview führten wir mit Philipp Vonmoos, CEO von SCV.

"Theft of cryptocurrencies through hacking of exchanges and trading platforms soared to $927 million in the first nine months of the year, up nearly 250 percent from the level seen in 2017."

CipherTrace, US Cyber Security Firm

Bitcoin Suisse ist für ihre Finanzdienstleistungen und Speicherlösungen im Kryptobereich für institutionelle und private Kunden bekannt. Die Bitcoin Suisse AG wurde 2013 gegründet und hat dazu beigetragen, einige der bekanntesten Kryptowährungsprojekte mit einem Volumen von beinahe 1 Mrd. CHF im Rahmen von Initial Coin Offerings (ICOs) oder Token Generation Events (TGEs) ins Leben zu rufen. **Im Edelmetallbereich bekannt ist die Swiss Gold Safe AG,** die sich auf Dienstleistungen zur Lagerung von Edelmetallen und Wertgegenständen spezialisiert hat. Swiss Gold Safe wurde 2006 gegründet. Das Joint-Venture der beiden Unternehmen SCV wurde 2017 nach schweizerischem Recht gegründet und hat seinen Sitz in Zug (ZG). Die Partnerschaft zwischen den beiden Unternehmen zur Gründung von SCV ermöglicht es , das Wissen über die Handhabung von Kryptowährungen mit dem über die sichere Lagerung von physischen Assets zu kombinieren.

Abbildung 9: Auszahlungsprozess des Schweizer Krypto-Tresors



Quelle: Swiss Crypto Vault AG

Potenzielle Schwachstellen bei der Generierung von private Keys ohne Hardware-Sicherheitsmodul

1.) Da Daenerys kein Hardware-Sicherheitsmodul (HSM) verwendet, gibt es ein kurzes Zeitfenster, in dem sich der private Schlüssel im temporären Speicher des Computers, der den privaten Schlüssel erzeugt hat, befindet. Da der Computer keinen Internetzugang hat, ist es für externe Hacker unmöglich, in das System einzudringen. Für einen Insider könnte es jedoch möglich sein, das Gerät in irgendeiner Weise zu gefährden. In Anbetracht der Hochsicherheitsmaßnahmen, mit der die Anlage ausgestattet ist, ist es höchst unwahrscheinlich, dass dieser Angriff gelingt.
2.) Ein weiterer Angriffsvektor könnte während eines Auszahlungsprozesses auftreten, bei dem ein beim Unternehmen Beschäftigter eine Kundenadresse auf der Whitelist gegen seine eigene austauscht.

Die Implementierung des Schlüsselerstellungsprozesses auf einem HSM würde sicherstellen, dass nie die Möglichkeit besteht, dass der private Schlüssel das Gerät verlässt, und auch auf dem HSM können Adressen auf der Whitelist vorkonfiguriert werden. Daher könnten beide Angriffsvektoren verbessert werden, wenn sie durch HSMs implementiert werden würden.

Die Lösung von SCV bietet Kunden eine Einzahlungsadresse, **die mit einem privaten Schlüssel versehen ist, der wiederum auf einem HSM generiert wurde, sodass der private Schlüssel das Gerät nie verlässt**. Der Kunde ist in der Lage, seine Kryptowährungsbestände nach Bedarf in die Depotadresse einzuzahlen. Die privaten Schlüssel werden nach der Verschlüsselung redundant an mehreren Orten sicher verwahrt, sodass im Falle eines katastrophalen Ereignisses in einer Anlage ein Backup der privaten Schlüssel vorhanden ist. Das Governance-Modell ist durch den Kunden weitgehend anpassbar und ermöglicht sowohl Multisignatur-Transaktionen als auch die Rollenzuweisung von Antragsteller, Controller und Genehmiger. Der Antragsteller kann über das Webportal Auszahlungen veranlassen. Ein oder mehrere Controller sind in der Lage, eine Auszahlungsanforderung zu stornieren, während zwei oder mehrere Bevollmächtigte eine Auszahlungsanforderung genehmigen. Optional kann auch eine Zeitverzögerung eingeführt werden. Auszahlungen dürfen zudem nur an zuvor genehmigte Adressen geliefert werden. Eine weitere Konfiguration, die der Kunde vornehmen kann, ist die Auswahl des Handling-Partners. Um zu verhindern, dass Swiss Crypto Vault die volle Autorität über den Auszahlungsprozess hat, ist ein Handling-Partner ein anderes Unternehmen als Swiss Crypto Vault. Dies bietet dem Kunden den zusätzlichen Vorteil, dass die Autorisierung von 2 separaten Organisationen mit unterschiedlichen Geschäftsabläufen, Personal und Computerinfrastrukturen erforderlich ist, um den Auszahlungsantrag des Kunden zu autorisieren. Die Anforderung, dass 2 Organisationen eine Auszahlungsanfrage autorisieren müssen, ist zusätzlich zum

konfigurierbaren Auszahlungsgenehmigungsprozess des Kunden. Derzeit ist der einzige Handling-Partner Bitcoin Suisse. Weitere Handling-Partner sollen in Zukunft für die Kunden zur Verfügung stehen. Die Architektur ähnelt einer Multisignatur-Transaktion, da mehr als eine Partei erforderlich ist, um eine Auszahlung zu autorisieren. Mit anderen Worten, sowohl Swiss Crypto Vault als auch der gewählte Handling-Partner (derzeit nur Bitcoin Suisse) müssen sich damit einverstanden erklären, einen Auszahlungsantrag zu genehmigen, da sonst ein Auszahlungsantrag abgelehnt wird. Dies kann eine lohnende Sicherheitsfunktion sein, welche die Wahrscheinlichkeit verringern soll, dass ein Betrugsfall stattfinden kann.

"The New York State Limited Purpose Trust charter, which now enables Coinbase Custody to act as a Qualified Custodian for crypto assets, builds on our unparalleled success as a crypto custodian while holding the company to the same exacting fiduciary standards and oversight of other, mature financial institutions operating in New York."

Asiff Hirji,
Coinbase COO and president

PriceWaterhouseCoopers hat die Speicherlösung überprüft, die Generierung des privaten Schlüssels überwacht und wird auch die Menge der gespeicherten Krypto-Assets mit den in der zugehörigen Blockkette registrierten Salden vergleichen. Zuhlke Engineering überprüfte den Code zur Generierung privater Schlüssel. **Swiss Crypto Vault bietet derzeit noch keine Versicherung an, dies wird aber unternehmensintern derzeit geprüft.** Der Kundenkreis kommt derzeit aus Europa, den USA, Asien und dem Nahen Osten. Was den typischen Kundeneinzahlungsbetrag betrifft, so ist SCV für Beträge ab rund 500'000 CHF sinnvoll. Ein SCV-Kunde benötigt keine physische Hardware, obwohl er eine Transaktion mit dem privaten Schlüssel seines eigenen Tresor- oder Ledger-Hardware-Wallets unter seiner Kontrolle mitunterzeichnen kann. Kunden können auch die Multi-Faktor-Authentifizierung für den Zugriff auf das Webportal nutzen. Viele verschiedene Kryptowährungen wie Bitcoin, Bitcoin Cash, Bitcoin Gold, Ether, Litecoin und alle ERC20- und ERC223-Token werden unterstützt. Weitere werden laufend hinzugefügt.

Swiss Crypto Vault scheint hochredundante, hochsichere und gut durchdachte Prozesse zu haben, die auch vom Kunden einfach zu implementieren und zu konfigurieren sind. SCV kann auf eine langjährige Erfahrung und Expertise sowohl in Kryptowährungen als auch in Edelmetallen zurückgreifen. Die Lösung ist sowohl für Institutionen als auch für HNWIs geeignet und definitiv eine Krypto-Verwahrungslösung, die es wert ist, in Betracht gezogen zu werden.

Fazit

Quelle: Scott Adams, Dilbert

In diesem Artikel haben wir einige Optionen für Krypto-Verwahrungslösungen vorgestellt. Zwei Lösungen stellen sicher, dass ein privater Schlüssel niemals ein HSM verlässt, zwei weitere generieren den privaten Schlüssel in einem Zwischenspeicher, wo er für einen kurzen Moment verbleibt. Das fünfte von uns untersuchte Unternehmen bestand darauf, den Prozess zur Generierung privater Schlüssel geheim zu halten. Für diejenigen Lösungsansätze, bei denen der private Schlüssel nicht auf einem HSM generiert wird, könnte eine Versicherungspolizze das Risiko eines Diebstahls decken. Was technologische Innovation, Geschwindigkeit, Benutzerfreundlichkeit, Anpassung der Governance, physische Sicherheit und digitale Sicherheit betrifft, so scheinen die umfangreichsten Lösungen für institutionelle Investoren Swiss Crypto Vault AG und Crypto Storage AG zu sein. Von diesen beiden hat die Swiss Crypto Vault AG die längste Erfolgsgeschichte und die meiste Erfahrung. Die Crypto Storage AG scheint die innovativste Lösung zu sein. Wenn Verwahrstellen mit Versicherung benötigt werden, sind Daenerys & Co. und Blockvault möglicherweise die richtige Wahl. Beide sind in der Lage, größere Summen von Kryptowährungen physisch zu speichern.

"This is the missing piece for infrastructure — it's a treacherous environment today. Hedge funds need it, family offices need it, they can't participate in digital currency until they have a place to store it that's regulated [...] This is early stages in an industry that's volatile right now. We're in a down cycle in terms of where we're going, but the institutions see an opportunity. It's going to progress quickly."

Co-founder and CEO of BitGo
Mike Belshe

Diese Auswertung ist nicht als generelle Empfehlung eines Unternehmens zu verstehen, da sie jeweils einen eigenen Use Case haben. Wir möchten betonen, dass es unumgänglich ist, bei der Suche nach einer geeigneten Lösung für die Verwahrung der Kryptowährungsbestände die gebotene Sorgfalt walten zu lassen.

Wenn Sie Fragen oder Anmerkungen haben, nach einer Lösung für Ihr Unternehmen suchen oder wenn Sie eine eigene Lösung haben, die Sie gerne mit anderen teilen möchten, besuchen Sie bitte http://www.cryptocustodysolutions.io. Wir wären sehr erfreut, wenn Sie an der kurzen Umfrage teilnehmen. Unter allen Teilnehmern verlosen wir ein Ledger Nano S. Joseph ist auch unter joseph (at) cryptocustodysolutions.io. erreichbar.

Disclaimer: Coinfinity und Silver Bullion sind Premium Partner des *Crypto Research Reports* bzw. des *In Gold we Trust Reports*. Die hier angeführten Informationen sind keine Anlage- oder Produktempfehlungen. Der Crypto Research Report gibt im Rahmen von Beiträgen grundsätzlich keine Empfehlungen für Produkte oder Dienstleistungen ab. Sorgfältige eigene Recherche ist unerlässlich.

Ist ein Bitcoin Standard denkbar? Saifedean Ammous im Austausch mit dem Crypto-Research-Report

“I like to call this the easy money trap: anything used as a store of value will have its supply increased, and anything whose supply can be easily increased will destroy the wealth of those who used it as a store of value.”

Saifedean Ammous

Key Takeaways

- **Ein Grund, warum Gold als Wertaufbewahrungsmittel und Rechnungseinheit verwendet wurde, ist das konstant geringe Angebotswachstum. In wenigen Jahren wird das jährliche Wachstum von Bitcoin geringer ausfallen als jenes von Gold. Eine optimale Recheneinheit hat eine konstante Quantität.**
- **Gäbe es einen fairen Wettbewerb für Geld, würde sich jenes Geld durchsetzen, das jedes Jahr an Wert gewinnt. Dann müssten Banken keine Zinsen mehr auf Einlagen zahlen. Stattdessen könnten Sparer zwischen einem Verwahrungsvertrag, einem Darlehens-Vertrag oder einer Beteiligungsinvestition wählen.**

Photo: *Saifedean Ammous*

Wir möchten uns herzlich bei Saifedean Ammous bedanken, dass er sich die Zeit genommen hat, Demelza Hays und Mark Valek von der Incrementum AG ein Exklusivinterview zu geben. Saifedean Ammous ist Professor für Wirtschaftswissenschaften an der American University im Libanon und Autor des Bestsellers „The Bitcoin Standard".

Bitcoins Stock-to-Flow-Ratio ist höher als jenes von Gold

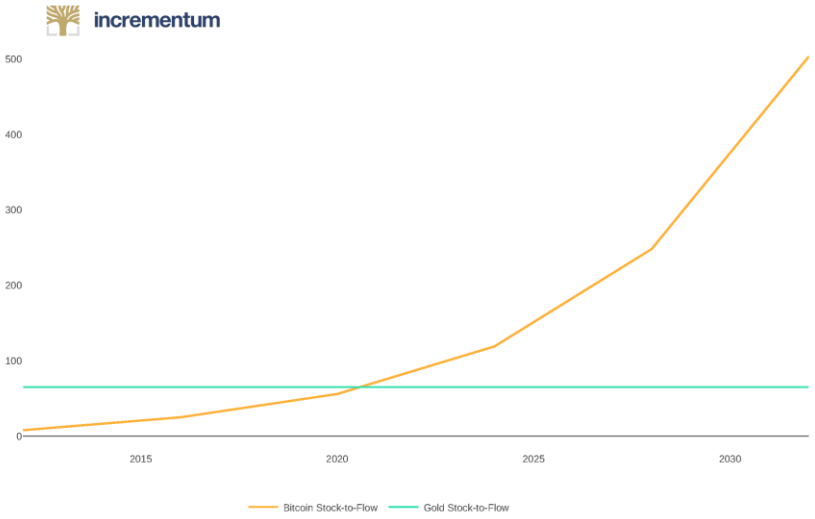
Als Ausgangspunkt seiner Analyse verschiedenartiger Gelder wählt Saifedean **das Stock-to-Flow-Ratio.** Leser des Schwesterberichtes dieser Publikation, der jährlich im Mai erscheinende *In Gold we Trust*-Report, kennen dieses Konzept seit langem, haben wir es doch bereits mehrfach ausführlich diskutiert. Vielen ist dennoch nicht bewusst, warum Gold seit Jahrtausenden als Wertaufbewahrungsmittel verwendet wird. Es stimmt zwar: Gold ist knapp, doch handelt es sich definitiv nicht um das knappste aller Metalle. Entscheidender ist: kein anderer Rohstoff verfügt über eine konstantere vorhandene Menge. Die Menge eines Gutes kann über das Verhältnis seines Bestandes (stock) zu seinem neuen Angebot (flow) ausgedrückt werden. Ein hohes Stock-to-Flow-Ratio bedeutet, dass die Menge des Gutes nicht sonderlich stark wächst. Damit ein Maßstab als verlässliche Rechnungseinheit verwendet werden kann, darf die Maßeinheit keinen hohen Schwankungen ausgesetzt sein. Der damalige Meister der britischen Münze und Erfinder des Goldstandards, Sir Isaac Newton, sagte:

> *„Meine Herren, in der angewandten Mathematik müssen Sie Ihre Einheit definieren".*

Obwohl Gold ein sehr hohes Stock-to-Flow-Ratio aufweist, wird Bitcoin bald ein noch höheres haben. Es ist dieser Umstand, der Saifedean zur Behauptung verleitet, dass Bitcoin in dieser Hinsicht Gold sogar überflügeln wird.

In der folgenden Abbildung hat Bitcoin ein Stock-to-Flow-Ratio von derzeit rund 71, aber 2024 wird das Verhältnis aufgrund des im Algorithmus festgelegten Halbierungsmechanismus auf 119 steigen. Je weniger Bitcoins gefördert werden, umso höher steigt das Verhältnis an. Langfristig werden gar keine neuen Bitcoins mehr gefördert und es herrscht absolute Konstanz der insgesamt existierenden Bitcoins.

Abbildung 10: Bitcoin versus Gold-Stock-to-Flow



Quelle: Incrementum AG.

Ist die Volatilität Bitcoins jemals zu bändigen?

Im „Journal of Structured Finance“ publizierte Saifedean einen Beitrag zum Thema “Can Bitcoin's Volatility Be Tamed”. Darin beschreibt er, wie die Schmucknachfrage und die Nachfrage der Industrie den Goldpreis beeinflussen. Wird Gold durch die Menschen in grossen Mengen verkauft, sinkt der Preis. Dank der dann steigenden Nachfrage von Schmuckherstellern und industriellen Gold-Verarbeitern wird der Preisverfall jedoch aufgefangen und schafft so einen stabilisierenden Boden, weshalb die Volatilität des Goldpreises stets schwach ausgeprägt ist.

“For Mises, gold’s industrial role is an impediment to performing its monetary role, but an impediment with which he is happy to contend compared to the alternative of money whose supply is controlled by governments.”

Saifedean Ammous

In einem seiner Artikel erklärt Paul Krugman, warum er ein Krypto-Skeptiker ist. Seine These lautet, dass im Gegensatz zu Gold Bitcoin keinen Anker in der realen Welt habe. [48] **Und weil es nur eine spekulative und keine reale Nachfrage nach Bitcoin gibt, würde bei Bitcoin auch kein Boden existieren, weshalb Bitcoin niemals die Rolle von Geld übernehmen könne.** Auf diese Kritik antwortet Saifedean mit einem Zitat aus „Theorie des Geldes und der Umlaufmittel“ von Ludwig von Mises:

> *„Die Bedeutung des Festhaltens an einem System des Sachgeldes liegt in der dadurch gewährleisteten Unabhängigkeit des Geldwertes von staatlichen Einflüssen. Es ist zweifellos mit beträchtlichen Nachteilen verbunden, daß*

—

[48] https://www.nytimes.com/2018/07/31/opinion/transaction-costs-and-tethers-why-im-a-crypto-skeptic.html

nicht nur die Schwankungen im Verhältnis von Geldangebot und Geldnachfrage, sondern auch die in den Produktionsverhältnissen des Geldstoffes und die Veränderungen in seiner industriellen Nachfrage auf die Gestaltung des Geldwertes zurückwirken."[49]

Wie Saifedean erklärt, führen Nachfrageschwankungen aus der Industrie dazu, dass der Wert von Gold schwankt, weshalb Gold eben nicht ein rein monetäres Gut sei, das nur eine monetäre Nachfrage widerspiegelt. Gold sei nicht wegen seiner industriellen Verwendung Geld geworden. Die industrielle Verwendung sei bei der Bestimmung des Goldwertes sekundär. Für Mises, so Saifedean, würde ein Geld, das nur von einer monetären Nachfrage getrieben sei, eine überlegene Form von Geld darstellen. In einer Welt, in der Bitcoin zum einzig verwendeten Geld würde, wäre die Nachfrage nach Bitcoin lediglich die Nachfrage nach Barguthaben. **Mit anderen Worten, unter einem Bitcoin-Standard wäre die Bitcoin-Nachfrage letztlich ein Spiegel der Zeitpräferenzen der verschiedenen Menschen,** so Saifedean.

Mark Valek, Autor des *Crypto Research Report* und Fondsmanager bei Incrementum AG merkt an, dass **solange Bitcoin „nur" ein Wertspeicher aber keine Recheneinheit sei, würde die Volatilität von Gold aufgrund der realwirtschaftlichen Nachfrage voraussichtlich immer niedriger sein als jene von Bitcoin.** Würde in Zukunft die Mehrheit der Menschen Bitcoin jedoch als Rechnungseinheit akzeptieren, wäre die Bitcoin-Volatilität geringer als jene von Gold, da Bitcoin die Maßheit zur Bepreisung von Waren und Dienstleistungen wäre. Sollte man dereinst Bitcoin tatsächlich zur Bepreisung von Waren und Dienstleistungen verwenden, würde die Volatilität von Bitcoin auf null sinken, da Bitcoin dann als allgemeine Messlatte fungiert.

"The virtues of the blockchain is that it would be that it's peer-to-peer settlement – no centralized settlement, no manipulation... And most importantly, there's nothing to capture. It's consensus based. It's stateless."

Patrick M. Byrne

Saifedean erklärt: „Hierin drückt sich das hohe Stock-to-Flow-Ratio von Gold und auch Silber aus, dass sich die jährliche Rohstoffgewinnung im Vergleich zu anderen Metallen eben nicht wesentlich auf das gesamte jemals geförderte Angebot auswirkt. **Doch genau das würde man bei einem Geld wollen: Geld soll eben nur Geld sein.**"

Mark Valek vergleicht das algorithmisch definierte Stock-to-Flow-Ratio von Bitcoin mit regelbasierten Geldpolitikansätzen wie Milton Friedmans automatisierter k-Prozent-Regel [50] und der Taylor-Regel von John Taylor. Diese würden ebenfalls versuchen, die Kaufkraft von Geld über die Zeit zu stabilisieren bzw. die das Geldmengenwachstum regelbasiert festzulegen, wenngleich sie „regalbasiert" das Geldangbot zusehns ausweiten wollen. Doch wie sich gezeigt hat, erreichen diese Ansätze ihr Ziel langfristig nicht, wie Gordon Tullock und die Public Choice Literatur einleuchtend erklären. [51]

—

[49] Theorie des Geldes und der Umlaufmittel, S 223;
[50] *A Monetary History of the United States, 1867–1960*
[51]

Diesen Vergleichen kann Saifedean jedoch nichts abgewinnen: **„Das wichtigste Kriterium, so glaube ich, ist, dass der Wert des Geldes durch den Markt bestimmt wird, d. h. durch Angebot und Nachfrage."** Denn letztlich sind es das Angebot und die Nachfrage nach Geld, die die Kaufkraftund den Zinssatz für Geld bestimmen sollten. „Das unterscheidet sich sehr von regelbasierten Ansätzen in der Geldpolitik. **Diese wollen den richtigen Preis berechnen, der dann durch den Markt übernommen werden soll."**

"The hardest form of money is one with constant money supply and zero elasticity."

Philipp Bagus

In seiner Auseinandersetzung mit Bitcoin hat Larry White argumentiert, dass Gold gegenüber Bitcoin folgenden Vorteil habe, in der langen Frist angebotsseitig gerade elastisch genug zu sein. Das Goldangebot steigt jedes Jahr um ein bis zwei Prozent. Innerhalb von 40 bis 50 Jahren verdoppelt sich das Gold-Angebot. Saifedean jedoch widerspricht diesem Argument vehement. Seiner Meinung nach mache die Tatsache, dass **Gold von allen bisher bekannten Gütern das geringste Angebotswachstum hat, das Edelmetall zu einem guten Geld.** Anders als Saifedean ist Larry White ein Verfechter eines auf einem Goldstandard basierenden Teilreserve-Bankensystem, da ihm zu folge, ein Vollreserve-Goldstand einen Geldmangel zur Folge hätte. Für Larry White wurde Gold deshalb zu einem international akzeptierten Geld, weil es eben die optimale Inflationsrate von ein bis zwei Prozent pro Jahr aufweisen würde. Im Gegensatz dazu vertritt Saifedean die Meinung: „Gold hat sich zum international anerkannten Geld entwickelt, weil **die Geldnachfrage immer eine Forderung nach einem Geld ist, das am wenigsten inflationiert werden kann.** Denn die Nachfrage nach Geld wachst ständig und der Wert von nichtinflationärem Geld wächst langfristig immer stärker. Wenn wir Larrys Argument folgen, dann müssen wir uns fragen, warum Silber oder Kupfer anstelle von Gold Geld geworden sind? Immerhin haben sie ein Angebot, bei dem auf eine Nachfrage elastischer reagiert werden kann als dies bei Gold der Fall ist."

Kann ein deflationäres Geldsystem funktionieren?

Genäß Mark Valek ist eine grundsätzliche Frage in diesem Kontext: „Braucht ein Währungssystem überhaupt Inflation?" Auch einige Goldbefürworter argumentieren, dass ein Währungssystem eine gewisse monetäre Inflation benötigt, um mit dem Bevölkerungswachstum Schritt zu halten, so Valek. Darauf entgegnet Saifedean: „Sowohl aus mathematischer Sicht als auch aus der Perspektive eines Bitcoin-Maximalisten denke ich, dass das Argument gegen Inflation, wie es Philipp Bagus in seinem Buch über Deflation ausformuliert, ziemlich einleuchtend ist: **Geld in seiner härtesten Form besitzt nun einmal eine konstante Geldmenge, die vollends unelastisch ist.**"

Demelza Hays, Autorin des *Crypto Research Report* und Fondsmanagerin bei Incrementum, verweist auf ihren Forbes-Artikel, „Bitcoin or Gold“[52] von 2017, der auf der Arbeit von Professor Dr. Antal Fekete basiert. In diesem Zusammenhang stellte sie Saifedean die Frage: „Für mich sieht es ganz danach aus, als würden wir eine Währung mit einem hohen Stock-to-Flow-Ratio haben wollen. Denken wir diesen Wunsch logisch zu Ende, könnten wir zum Schluss kommen, dass **Geld doch überhaupt keine Flussgrösse braucht, das heisst im Angebot überhaupt nicht wachsen muss?**“

*“Some of the most important technological, medical, economic, and artistic human achievements were invented during the era of the gold standard, which partly explains why it was known as **la Belle Epoque**, or the beautiful era, across Europe.”*

Saifedean Ammous

“We don’t need any flow! But we also don’t know any other economic good that is more reliable at limiting flow other than Bitcoin, which has a small annual inflation rate still. The government will make more fiat money flow, the miners of gold will make more gold flow, the miners of silver will make more silver flow. If you could find a way to make a money that doesn’t have any flow, then go for it! That is what Bitcoin will be doing in about 100 years from now.”

Das gegenwärtige Währungssystem basiert auf Schulden

Ist ein Geldsystem schuldenbasiert, so die Ansicht Mark Valeks, hieße das in erster Linie, dass Zentralbanken eine inflationäre Geldpolitik systemimmanent verfolgen muss: „Sind verzinste Schuldpapiere die Basis für unser Geld, erfordert das eine ständig wachsende Geld- und somit auch eine ständig wachsende Schuldenmenge. Andernfalls gibt es an einem Punkt keine Geldeinheiten mehr, um laufende Zinszahlungen für bereits ausstehende Schulden zu bedienen.”

Dieser Ansicht stimm Saifedean zu und führt weitergehend aus: „Ich gehe sogar noch weiter als die meisten Vertreter der österreichischen Schule der Nationalökonomie. **In einem freien Markt für Banken würden die Einleger keine Zinsen auf ihre Einlagen verdienen müssen, weil das Geld an Wert gewinnen würde, was der eigentlichen Rendite entspricht.** Das Verleihen von Geld an die Bank ermöglicht es den Einlegern, die Kosten für die sichere Aufbewahrung ihres Geldes zu sparen. **Die alternative, deflationäre Art von Geld entspräche der direkten Beteiligung, so wie es das Modell des islamischen Bankings vorsieht.“** Dies ist eigentlich auch das Modell des traditionellen Bankings.

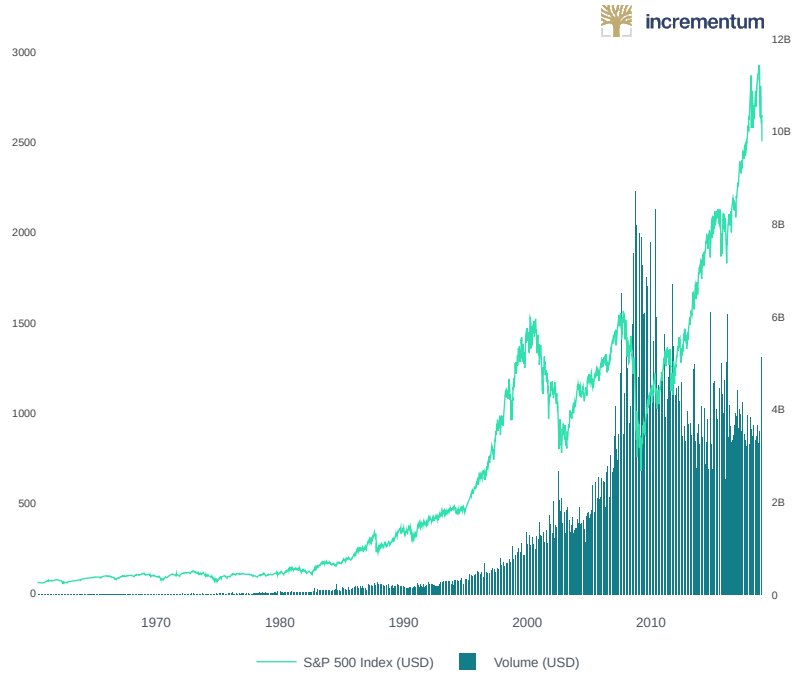
„Wenn Sie eine Investition tätigen, kommt es darauf an, was die Gesellschaft als legitim akzeptiert. Solange eine Gesellschaft akzeptiert, dass der Kreditgeber das Eigentum des Kreditnehmers beschlagnahmt, wenn er nicht zurückzahlen kann, dann monetarisieren Sie effektiv das Eigentum des Kreditnehmers, mit dem der Kredit besichert ist. Schließlich haben Sie ein Darlehen ausgegeben, das durch

—

[52] https://www.forbes.at/artikel/bitcoin-or-gold-why-not-invest-in-both.html

diesen Vermögenswert gesichert ist, der kein Geld ist, sondern ein Haus oder Auto oder ein Grundstück. Diese Art von Geschäftsmodell wird nur an Orten akzeptiert, an denen es rechtlich in Ordnung ist, dieses Eigentum zu beschlagnahmen, wenn der Kreditnehmer in Verzug gerät. Auf der anderen Seite, wenn die Sicherheiten des Kreditnehmers nicht beschlagnahmt werden können, dann lehnen die Kreditgeber diese Art von Geschäften oft ab und die Banken beteiligen sich nicht daran."

Abbildung 11: Steht die nächste Rezession bevor?



Quelle: Yahoo Finance, Incrementum AG.

"It is often in a country's long-term interest to give up political control over its currency."

Princess Gisela von und zu Liechtenstein

In einer Welt, in der Banken nur die Einlagen verleihen oder direkt ihr Eigenkapital investieren können und Sicherheiten nicht in ihren Besitz nehmen können, kann die Bank keine garantierten Zinsen versprechen, da es im Geschäftsleben immer Risiken geben wird. Da die Bank dann auch nicht über eine Teilreserve Geld schöpfen kann und zuerst Geldeinlagen von Kunden entgegennehmen muss, kann sie die Solvenz ihrer Einlagenkonten nicht garantieren. Somit Tragen Einleger das Risiko eines vollständigen Ausfalls Ihrer Einlage. „**In einer solchen Welt gibt es keinen risikolosen Zins.** Nach Saifedean würde niemand Geld bei jemandem anlegen, der sagt:

> ***„Wenn wir als Bank Pleite gehen, verlieren Sie Ihr ganzes Geld. Falls wir jedoch Erfolg haben, bekommen Sie nur drei Prozent.*** *Folglich würde jeder in Aktien investieren. Entweder Sie legen bei einer Bank Geld an, so dass es jederzeit fällig und verfügbar ist. In diesem Fall zahlen Sie eine Gebühr für die Lagerung und die Bereitstellung des Geldes. Haben Sie jedoch Geld, auf das Sie eine Weile verzichten können, investieren Sie es als Eigenkapital in ein anderes Geschäft. Letztlich ist es die Aufgabe der Bank, die Fälligkeiten zwischen den Kreditnehmern und den Kreditgebern stets abzugleichen."*

"For something to assume a monetary role, it has to be costly to produce, otherwise the temptation to make money on the cheap will destroy the wealth of the savers and destroy the incentive anyone has to save in this medium."

Saifedean Ammous

Mark Valek ist in diesem Aspekt nicht vollständig mit Saifedean einverstanden. So ist er der Überzeugung, dass es neben Depositen und Beteiligungen auch eine Nachfrage nach Schuldtiteln geben würde.: „Selbst in einem deflationären Währungssystem würde es eine Nachfrage nach Investitionen in Form von Fremdkapital und nicht nur nach Eigenkapital geben. **Denn letztlich ermöglicht eine differenzierte Kapitalstruktur eines Unternehmens unterschiedliche Auszahlungsprofile für Anleger.** Niedrige Renditen auf Anleihen oder auch Kreditkonten bei Banken ermöglichen es dem Investor vorhersehbare Cashflows zu erhalten, welche höherer Seniorität im Konkursfall gegenüber Aktionären haben. Klarerweise handelt es sich hierbei aber nicht um risikolose Zinserträge."

In einem derartigen Währungssystem müssten die Anleger ihren Bitcoin jedoch nicht zwingend über eine Wertpapieranlage in Eigen- oder Fremdkapital riskieren, um Kaufkraft zu gewinnen (oder zu erhalten). Denn die Bitcoins würden aufgrund ihres deflationären Charakters eine Aufwertung in Form einer realen Erhöhung der Kaufkraft erleben. „Den Fall einer risikoarmen Zinsanlage dürfte es aber neben dem reinen Horten auch geben, doch wäre die Neigung, ein solches Risiko einzugehen, wohl weitaus geringer als heute. Letztlich handelt es sich hier allerdings nur um eine kleine Meinungsverschiedenheit", fügt Mark Valek hinzu.

Tabelle 2: Anlageoptionen unter einem globalen Bitcoin-Standard:

	Saifedean Ammous	Mark Valek
Anleger horten über 100% gedeckte Einlagen, die nicht verborgt werden. Der Anleger zahlt der Bank/dem Verwahrer für die Verwahrung seiner Einlagen und lässt Bitcoin ggfs Versichern. Der Anleger profitiert von der Aufwertung der Währung im Laufe der Zeit.	✓	✓
Die Anleger investieren in Eigenkapital. Der Investor erzielt eine positive oder negative Rendite und besitzt Aktienanteile.	✓	✓
Anleger investieren Ersparnisse in Fremdkapital. Direkt über eine Anleihe, oder gebündelt via Fonds oder eine Bank. Kreditrisiken werden gebündelt und entsprechende Zinszahlungen lukriert.	✗	✓

Quelle: Saifedean Ammous Interview, Incrementum AG.

Mark Valek greift noch jene Kritik auf, die gemeinhin von Mainstream-Ökonomen geäußert wird: **„Ein Preisdeflation behindert das Wachstum"** Mark Valek ist der Meinung, dass ein stabiles oder fallendes Preisniveau nicht zwangsweise im Widerspruch zu Innovation, Entwicklung und Expansion ist. Der Präzedenzfall eines Goldstandards ist in dem Zusammenhang spannend. Obwohl es eine Art Goldfluss bzw. monetäre Inflation gab, waren die Produktivitätssteigerungen höher als die Inflationsrate von Gold und die Preise sind tendenziell gefallen.

„Ja, absolut", versichert Saifedean, „um Zinsen für ein schuldenbasiertes System zu schaffen, muss eine Bank ihre Sicherheiten monetarisieren. Um ein Teilreserve-Banking zu betreiben, muss eine Zentralbank existieren, die Geld schöpft. **Andernfalls wäre das auf Teilreservehaltung basierende Bankensystem instabil.** Indem eine Zentralbank die Zinsen nach unten manipuliert, kann sie das Geldangebot ausweiten, was es Regierungen ermöglicht, mehr Geld zu leihen und

auszugeben. Es gibt verschiedene Ebenen der Inflation. Heute sind Teile der Wirtschaft von diesem Kreditgeld abhängig. Es gibt verschiedene Industrien, die nur dank des billigen Geldes Menschen zu beschäftigen vermögen. Sie sind politisch gut vernetzt, und Empfänger vom billigen Geld, welches Ihre Unternehmen oftmals am Leben halten. Das ist jedoch eine Schwäche im System und nicht eine Stärke. Wer eine ehrliche Wirtschaft haben möchte, sollte die Geldschöpfung loswerden wollen, damit Investitionen über echte Ersparnisse finanziert werden. Erst dann hätte man einen tatsächlich funktionierenden Kapitalmarkt, bei dem die Fälligkeiten übereinstimmen."

Saifedean über das Investieren in Bitcoin

Frage: Was hältst Du von Smart Contracts und Utility-Token, die dezentrale Kapitalmärkte ermöglichen können?

Antwort: Bitcoin ist die einzige Krypto-Applikation, die wirklich Sinn macht. Damit müssen wir zu leben lernen.

Frage: Wenn Du einen Kryptowährungsfonds gründen würdest, wäre dieser zu 100 Prozent in Bitcoin investiert?

Antwort: Ich würde keinen Kryptowährungsfonds lancieren, denn die einzige Kryptowährung, die man halten muss, ist Bitcoin.

Frage: Wie sollte man seine ersten Bitcoin-Investition tätigen Alles auf einmal kaufen oder über die Zeit, um vom „Cost-Average-Effekt" zu profitieren?

Antwort: Bitcoin ist noch immer eine hochriskante Sache. Ich würde nicht raten, viel Geld zu investieren. Ich muss den Leuten immer wieder sagen, dass dieses Ding noch immer explodieren kann, existiert es nun einmal erst seit zehn Jahren. Bitcoin könnte irgendwann scheitern oder es könnte für die nächsten zehn bis zwanzig Jahre einen Bärenmarkt durchlaufen. Selbst im besten Fall wird Bitcoin sehr volatil sein und einige massive Rückschläge aufweisen. Unter den Kryptowährungen jedoch denke ich, dass Bitcoin die einzige ist, die langfristig eine Absicherung gegen unsere gegenwärtige monetäre Inflation sein wird.

Ein freier Markt für Geld

Hinsichtlich der Zukunft fragt Demelza: „Wenn alle Zentralbanken auf der ganzen Welt auf Bitcoin reagieren, indem sie die Inflationierung ihrer Währungen verringern und ihre Währungen dadurch härter machen, **könnte so ein tatsächlicher Wettbewerb zwischen Bitcoin und den von den Zentralbanken herausgegebenen Fiat-Währungen entstehen,** so wie Uber und Taxis oder Airbnb und Hotels heute im Wettbewerb stehen? Oder wird das eine das andere vollständig ersetzen"?

Darauf antwortet Saifedean: „Die Menschen haben zum ersten Mal eine echte Alternative und können Zentralbanken den Rücken kehren. Vor Bitcoin war das ausgeschlossen, doch mit Bitcoin ist das jetzt möglich. Bitcoin wird die Gefahr stark expansiv wirkender Zentralbanken verringern. Man muss sich das bildlich so vorstellen: **Bitcoin ist eine Art monetärer Batman, der gewissermaßen jeder Zentralbank im Nacken lauert und darauf wartet, dass diese beginnt, die Geldmenge zu inflationieren. Passiert das, werden die Menschen in diesem Land in Bitcoin Zuflucht suchen** und der Wert der Kryptowährung wird deutlich ansteigen".

Saifedean sieht in Bitcoin auch eine Art Nebenbankkonto, das man für schlechte Tage als Schutz haben sollte: „Man stelle sich vor, man sitzt eines Tages in einem Land fest, in dem man ausgeraubt wurde und man keinen Zugang zu seinem Bankkonto hat. Geld hat man also keines. Wenn man in einer solchen Situation Bitcoin hat, kann man sich aus diesen Schwierigkeiten herausmanövrieren, indem man beispielsweise ein Flugticket kauft. **Es ist dieser Nutzen, den es nachzuvollziehen gilt."**

Mark Valek stimmt Saifedean in dieser Hinsicht zu: „Wir denken hier sehr ähnlich. Obwohl wir beide sehr optimistisch sind, denke ich auch, dass **Anleger aus**

Portfoliogesichtspunkten nicht viel investieren müssen, um von Bitcoin zu profitieren. Wer nur schon wenige Prozentpunkte seines Gesamtvermögens in Bitcoin investiert, kann große Gewinne erzielen, sollte Bitcoin tatsächlich zu einem allgemein akzeptierten Tauschmittel werden." So sieht Mark Valek Bitcoin letztendlich als binäre Anlage: „Entweder wird Bitcoin zu einer Art monetärem Vermögenswert und Wertaufbewahrungsmittel oder Bitcoin wird von etwas anderem abgelöst und der Preis fällt auf Null zurück."

Bitcoin: mögliche Wege der Geldwerdung

Wenn wir über die Zukunft nachdenken, wie könnte der Übergang von Bitcoin von einem Wertaufbewahrungsmittel zu einer allgemein verwendeten Rechnungseinheit aussehen? Mark Valek nennt hier zwei Szenarien:

1.) Positives Szenario: Bitcoin wird zu einem Reserve-Asset für Zentralbanken. Ein Dominoeffekt könnte dazu führen, dass immer mehr Zentralbanken Bitcoin kaufen, um sich vor Spekulationsangriffen zu schützen und sicherzustellen, dass die Staatsverschuldung durch Investitionen in Bitcoin getilgt werden kann. Die Marschallinseln haben bereits in Bitcoin investiert und auch die Zentralbank von Barbados hat 2015 einen Artikel zu diesem Thema veröffentlicht.
2.) Negatives Szenario: Das konventionelle Fiat-System verspielt sein Vertrauen ganz und es kommt zu einem großen Überlaufen in den neuen sicheren Hafen Bitcoin.

"Government money is similar to primitive forms of money and commodities other than gold, in that it is liable to having its supply increased quickly compared to its stock, leading to a quick loss of salability, destruction of purchasing power, and impoverishment of its holders."

Saifedean Ammous

Darüber hinaus sieht Saifedean das Szenario, wonach Bitcoin zur monetären Vorherrschaft aufsteigen könnte, weil immer mehr Personen den Nutzen hinter der Kryptowährung entdecken und verstehen lernen: „Das wäre dann bloss als finanzielles Upgrade zu sehen, so als würde man eine gut funktionierende Software auf einem miserablen Windows-PC installieren, worauf dieser dann besser funktioniert. **Das Währungssystem, das wir heute haben, schafft Geld, indem Schulden gemacht werden.** Die Kehrseite davon ist, dass Geld zerstört wird, wenn Schulden abgezahlt werden. Seit 40 bis 50 Jahren haben wir dieses System und jetzt verfügen wir über eine neue Alternative und jeder wird einmal in dieses neue Bitcoin-System einsteigen. Schließlich können Menschen Bitcoin verwenden, um ihre Fiat-Schulden zu begleichen. Sollten wir alle unsere Schulden abbezahlen, wird es zu einer Auflösung des globalen Fiat-Systems kommen. **Im Grunde genommen zahlt jeder seine gesamten Schulden und ab, bis sie auf Null fallen.** Dann übernimmt ein neues, funktionierendes Währungssystem die Welt. Dieser Vorgang mag nur langsam vor sich gehen oder aber schnell. Zu einem verheerenden Kollaps muss es jedoch nicht zwingend kommen, wenn wir zu Bitcoin überlaufen."

Im Falle von Bitcoin könnte es ähnlich ablaufen wie bei der **Dollarisierung in Ecuador, als das Land von der eigenen Landeswährung auf den US-Dollar wechselte.** Normalerweise ist eine Hyperinflation der Auslöser. Was wir jedoch in den letzten 10 Jahren mit Bitcoin gesehen haben, ist, dass die Menschen langsam zu hartem Geld migrieren.

GENTWO DIGITAL

Making Crypto Assets Bankable

We make any token, ICO, STO, crypto asset or crypto portfolio investable, fully bankable and transferable in a Swiss Security (Swiss ISIN)

Securitization of all crypto assets.

The crypto asset industry set out to challenge the traditional finance sector. Talent, ideas, and capital flocked to crypto assets yet for many investors, access remains a challenge.

Seed capital was earmarked for these new opportunities but the majority of funds remains trapped in the old system.
Banks, large scale/ institutional investors are missing out.

We are the bridge between these two worlds.

We are leaders of change in the finance industry. It is our vision to make crypto assets as accessible as the stock market and facilitate exciting new crypto ventures.

+41 44 512 7507

GENTWO Digital AG | Crypto Valley Labs
Dammstrasse 16 | CH-6300 Zug

contact@g2d.io

www.g2d.io

Anforderungen an einen investierbaren Krypto-Index von institutionellen Investoren

“Creating an index that accurately tracks the market requires consideration of three main factors: reflecting market dynamics, maintaining/governing the respective rules, and preventing manipulation.”

Patrick Valovic

Key Takeaways

- **Indizes, die als Benchmark fungieren müssen investierbar und replizierbar sein.**
- **Um für institutionelle Investoren investierbar zu sein, müssen Kryptowährungen von professionellen Verwahrstellen in Verwahrung genommen werden können.**
- **Der LY Incrementum Krypto Index berücksichtigt die Anforderungen von institutionellen Kunden hinsichtlich Investierbarkeit, Verwahrbarkeit und Replizierbarkeit.**

Verfasst von LIMEYARD

LIMEYARD ist ein Schweizer Indexanbieter mit Büros in Zürich, New York und Wien. LIMEYARD konzentriert sich sowohl auf proprietäre als auch auf nicht-proprietäre Indizes und kombiniert modernste Indexinnovationen mit einer hochmodernen Cloud-basierten Technologie. Die schnell wachsende Familie der globalen Aktien- und kryptographischen Vermögensindizes ist regelbasiert, konform, traditionell und bietet intelligente, investierbare Lösungen für Institutionen auf der Verkaufs- und der Käuferseite. LIMEYARD hat im Februar 2018 ein Joint Venture mit der Wiener Börse AG geschlossen.

Die Schaffung einer Benchmark für den Krypto-Markt im Frühstadium

"Virtual Currencies may hold long-term promise, particularly if the innovations promote a faster, more secure and more efficient payment system."

Ben Bernanke

Das zurzeit komplexe Marktumfeld für Krypto-Assets inspirierte mit LIMEYARD und Decentriq zwei in der Schweiz ansässige Unternehmen zu einer gemeinsamen Innovation: Sie haben einen umfassenden **Krypto-Asset-Index entwickelt, der die Dynamik des gesamten Marktes erfassen und gleichzeitig die regulatorischen und wirtschaftlichen Herausforderungen** bewältigen soll. Denn für Investoren muss ein Index handelbar sein, d. h. die Liquidität vorhanden und das Rebalancing machbar sein. Zudem werden an den Markt für Krypto-Assets besondere regulatorischen Anforderungen gestellt. So dürfen beispielsweise sogenannte Privacy Coins nicht Teil eines Investments sein oder aber es dürfen nur Coins in ein Portfolio aufgenommen werden, die an einer Börse gehandelt werden. In der Vermögensverwaltung können grundsätzlich zwei Ansätze verfolgt werden, eine aktive und eine passive Vermögensverwaltung:

- **Aktive Vermögensverwalter** verwenden in der Regel eine Benchmark, um die Performance ihres Portfolios zu vergleichen. Markteffizienz und preissystematische Risiken bewerten sie anhand der von ihnen gewählten Benchmark. Um eine optimale Anlagestrategie zusammenzustellen, wenden Vermögensverwalter verschiedene Risikomodelle an und vergleichen die bisherige Performance der Strategie mit der zugrunde liegenden Benchmark. Eine langfristige Outperformance, also ein Mehrertrag, ist dabei das angestrebte Ziel. Die Benchmark selber ist performance-unabhängig.
- **Passive Vermögensverwalter** (z.B. ETF-Anbieter) hingegen investieren in ein Portfolio, das einem Index folgt. Deren grundlegende Frage ist: Welche Strategie, welches Thema, welche Region, welcher Sektor könnte eine günstige Investitionsmöglichkeit für Investoren sein? Der ETF-Anbieter bildet einen Faktor/Risikomodell-basierten Index ab, z.B. einen Low-Volatility-Index, einen Momentum-Index oder einen Qualitätsindex.

Sowohl für den aktiven als auch den passiven Vermögensverwalter hat „das Abbilden des Marktes" die gleiche Bedeutung. Für letzteren spiegelt das Indexkonzept jedoch eine Anlagestrategie wider. Mit anderen Worten: Aktive Manager nutzen die Benchmark, um den Gesamtmarkt zu verfolgen. Sie agieren daher performance-unabhängig, solange die Performance mit der Gesamtperformance des Marktes übereinstimmt. Für passive Investoren hingegen stellt der Index eine Anlagestrategie mit dem Ziel dar, eine langfristig positive Performance zu erzielen. In beiden Fällen ist der Index regelbasiert, d. h. er unterliegt keinen diskretionären Ermessensentscheidungen.

Die Zusammenstellung eines Index, der den Markt genau abbildet, erfordert die Berücksichtigung von drei Hauptfaktoren: 1.) eine Reflexion über die Marktdynamik; 2.) die Einhaltung der jeweiligen Regeln; 3.) die Verhinderung von Manipulationen.

1. Reflexion über die Marktdynamik: Diese erfordert, dass genügend Daten berücksichtigt werden, da Daten der Hauptbestandteil jeder Benchmark sind. Werden zu wenig Daten berücksichtigt, birgt dies das Risiko, dass ein Markt nicht ausgewogen dargestellt wird.
2. Einhaltung entsprechender Regeln: Um vollständig regelbasiert und transparent zu sein, muss die Methodik eines Index unter allen Marktbedingungen anwendbar sein.
3. Verhinderung von Manipulationen: Interne betriebliche Prozesse müssen so gestaltet sein, dass eine Manipulation des Index unmöglich ist. Das war zuletzt ein Problem im Zusammenhang mit dem LIBOR-Skandal im Jahr 2011. IOSCO, die Internationale Organisation der Wertpapieraufsichtsbehörden, hat die „IOSCO Principles for Financial Benchmarks“ definiert. Diese bestehen aus insgesamt 19 Prinzipien, an die sich Indexanbieter halten müssen. LIMEYARD hat diese allesamt umgesetzt und lässt die Einhaltung jährlich überprüfen.

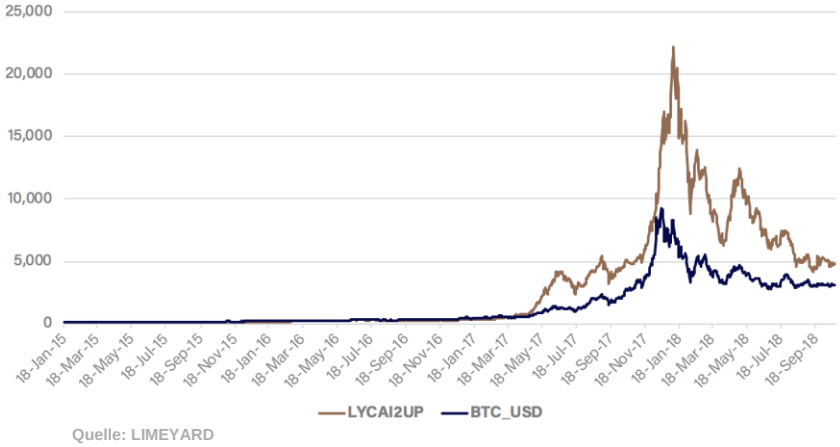
Die Schaffung des LIMEYARD Crypto Asset Index (LYCAI)

“There are three eras of currency: Commodity based, politically based, and now, math based.”

Chris Dixon

LIMEYARD und Decentriq standen bei der Schaffung eines umfassenden Krypto-Marktindex vor zwei grossen Herausforderungen: Wie geht man mit (1) einem hochdynamischen Markt um, der in seiner Gesamtentwicklung durch zahlreiche, teilweise unbekannte Faktoren, beeinflusst ist. Wie handhabt man (2) zudem die praktischen Anforderungen, um den Index regel-basiert, transparent und konform zu machen. Aus dieser anspruchsvollen Aufgabe resultierte schließlich der **LIMEYARD Crypto Assets Index (LYCAI), der die 20 größten öffentlich handelbaren Krypto-Assets umfasst.**

Abbildung 12: Index Performance LYCAI vs. Bitcoin



Quelle: LIMEYARD

Um Bestandteil des LYCAI zu sein, muss ein Krypto-Vermögenswert mehrere Parameter erfüllen. So sollte er eine ausreichende Robustheit, Liquidität und Handelbarkeit gewährleisten. **Der Index wird rund um die Uhr in Echtzeit berechnet, wobei die Handelsdaten von acht verschiedenen Börsen verwendet werden.** Dass die Daten von mehreren vertrauenswürdigen Börsen kommen, erhöht die Robustheit des Index gegenüber Ausfällen auf Börsenebene

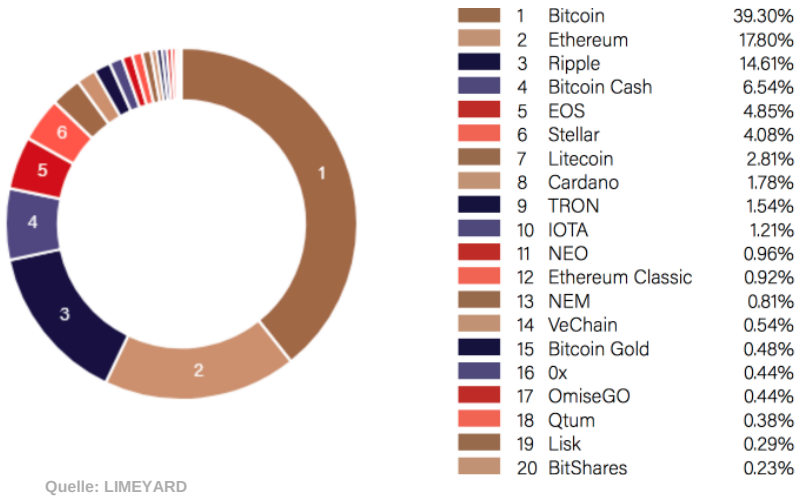
und Preismanipulationen, was eine angemessene Darstellung des zugrundeliegenden Marktes ermöglicht. Die ausgewählten Börsen verfügen über eine vergleichsweise hohe Liquidität. Darüber hinaus berücksichtigt LIMEYARD nur Vermögenswerte, die an mindestens zwei vertrauenswürdigen Börsen gehandelt werden. Dadurch wird sichergestellt, dass, falls eine Handelsbörse technische Probleme haben sollte, der Index weiterhin mit Preisdaten über den gesamten vordefinierten Anlagensatz versorgt wird. Der Algorithmus zur Aggregation der Preisdaten berücksichtigt sowohl das Volumen als auch Ausreißer und reduziert unerwünschte Ausschläge auf das Indexniveau, die in einem jungen und fragmentierten Markt wie dem Krypto-Markt eben auftreten können. Darüber hinaus kommen nur Vermögenswerte in Frage, die beim Handelsvolumen unter den ersten 60 Prozent liegen.

"Well, I think it is working. There may be other currencies like it that may be even better. But in the meantime, there's a big industry around Bitcoin. — People have made fortunes off Bitcoin, some have lost money. It is volatile, but people make money off of volatility too."

Richard Branson

Zudem berücksichtigt der Index nur solche Vermögenswerte, deren Protokolle nicht darauf ausgelegt sind, Anonymität zu gewährleisten. Auf diese Weise soll vermieden werden, dass der Index mit illegalen Transaktionen in Verbindung gebracht wird und dass ein gewisses Mass an Transparenz für Steuerzwecke gewahrt wird. Mit diesem Kriterium haben LIMEYARD und Decentriq die Bedenken der Regulierungsbehörden aufgegriffen und versucht, den Verstoss gegen die KYC/AML-Standards bei der Verwendung des LYCAI als Basiswert für Finanzinstrumente zu begrenzen. Um eine echte Diversifikation zu ermöglichen und die Bitcoin-Dominanz innerhalb des Marktes auszugleichen, glättet der Index die Marktkapitalisierung der einzelnen Indexwerte durch einen exponentiellen gleitenden Kursdurchschnitt über den Monat vor dem jeweiligen Stichtag. Die Gewichtungen werden von einer Sigmoid-Funktion abgeleitet, die hohe Werte bestraft, ohne ein striktes Limit festzulegen. Durch die Gewichtungsmethode ist die Allokation grosser Vermögenswerte im Vergleich zu anderen Indizes ausgewogen. So betrug beispielsweise die Gewichtung von Bitcoin und Ethereum per Ende Oktober 2018 39,30 Prozent bzw. 17,80 Prozent. Im Vergleich dazu liegen die Gewichtungen beim Crypto Markt Index bei mehr als 60 Prozent bzw. 13 Prozent und 30 Prozent (Cap) bzw. 23,46 Prozent für den Bloomberg Galaxy Crypto Index.

Abbildung 13: LYCAI Asset Allocation November 2018



Quelle: LIMEYARD

Der LYCAI-Index ist also als echte Benchmark für die Bemessung von Krypto-Fondsperformance anzusehen. Der Index erfüllt alle IOSCO-Anforderungen sowie die aktuellen Bedenken der Regulierungsbehörden, welche diese in Bezug auf Krypto-Assets ausdrücklich geäußert haben.

Ein Krypto Index für Insitiutionelle Investoren

"PayPal had these goals of creating a new currency. We failed at that, and we just created a new payment system. I think Bitcoin has succeeded on the level of a new currency."

Peter Thiel

Unterschiedliche Kunden haben allerdings unterschiedliche Anforderungen. Aus diesem Grund haben wir den LY Incrementum-Index an die Erfordernisse von Incrementum angepasst. Um in der Praxis vollständing replizierbar zu sein, bedarf es im Bereich von Krypto Investments noch ein paar Nebenbedingungen. Auf dem LIMEYARD Crypto Asset-Index aufbauend zeichnet sich der LY Incrementum-Index durch folgende Abweichungen aus:

- Krypto-Assets im Index müssen mittels Cold-Storage-Hardware-Einrichtungen aufbewahrt werden können, um so von Schweizer Versicherungsgesellschaften versichert zu werden.
- Krypto-Assets müssen eine Marktkapitalisierung von mehr als 500 Millionen Dollar haben.
- Die Anzahl der Krypto-Vermögenswerte wird auf zehn beschränkt, um die Transaktionskosten für das Rebalancing zu reduzieren.

Abbildung 14: Index Performance LYCAI vs. LY Incrementum

Quelle: LIMEYARD

Dieses leicht überarbeitete Indexkonzept erweist sich als sehr solide. So liegt die Einjahresrendite bei 16,10 Prozent, während der LYCAI eine Einjahresrendite von 0,58 zu verzeichnen hat. Die einjährige annualisierte Volatilität beträgt 96,49 Prozent, verglichen mit 97,06 Prozent bei LYCAI. Die einjährige Volatilität wird hauptsächlich von Bitcoin getrieben, dem grössten Vermögenswert in beiden Indizes. Zudem macht die geringere Anzahl von Assets im LY Incrementum Index den Index handelbarer als das Gegenstück des LYCAI, der in erster Linie den gesamten Krypto-Markt repräsentieren soll.

Abschliessendes Fazit

Das auf der CME-Plattform gehandelte Volumen von Bitcoin-Futures wächst stetig und das durchschnittliche Tagesvolumen liegt derzeit bei mehr als 162 Millionen USD. Verschiedene führende Investmentbanken und traditionelle Börsen führen interne Projekte durch, um nicht nur die Handelbarkeit von Bitcoin, sondern auch die von anderen Krypto-Assets weiter voranzutreiben. Viele Projekte wurden bereits angekündigt, andere werden voraussichtlich in Kürze bekannt gegeben werden. Aus diesem Grund investiert LIMEYARD weiterhin in strategische Partnerschaften und in die Entwicklung einer breiteren Krypto-Indexfamilie. Schließlich sollen auch Anlagestrategien für das Segment der passiven Vermögensverwaltung abdeckt werden.

Equity Tokens

"Fractional ownership is not unique to blockchain, in fact, it's not even unique to this century. Joint ownership dates back to the Roman Republic, or the Dutch East India Company in more modern times. However, some assets classes such as commercial real estate and fine art continue to be characterized by high unit costs.

A typical retail investor cannot harness the resources required to buy a Manhattan high rise. The investor is left with two options: (1) Forego exposure to Manhattan commercial real estate in their investment portfolio, or (2) gain exposure through an intermediary, for example a publicly traded Real Estate Investment Trust (REIT), where it is often bundled with a portfolio of other buildings of varying quality and characteristics. Security tokens offer an efficient path to fractionalize a single high value asset."

Stephen McKeon, Professor University of Oregon

Key Takeaways

- **Equity-Token ermöglichen es Unternehmen, Eigenkapital mittels der Blockchain-Technologie aufzunehmen, ohne dabei Investoren zu binden.**
- **Emittenten von Wertpapier-Token versuchen, auf den großen Pool an institutionellem Geld zuzugreifen, der noch nicht in den Kryptowährungsmarkt eingedrungen ist. Institutionelle Investoren erwarten KYC/AML, Datenschutz und sehen in einem der Kernstücke der Blockchain, nämlich ihrer Unveränderlichkeit eine Hürde.**
- **2019 wird ein Wettlauf zwischen Börsen stattfinden, welche den ersten geregelten Markt für Wertpapier-Token anbieten kann.**

Die österreichische Finanzmarktaufsicht hat **Ende November den ersten Finanzmarktprospekt für ein vollständig reguliertes tokenisiertes Wertpapier in der Europäischen Union gebilligt.** Die Finanzmarktaufsicht in Liechtenstein hat bereits im August den ersten Security Token Liechtensteins genehmigt. Mt Pelerin, Tokenestate und Securosys wollen in der Schweiz Security-Token anbgeboten werden. Das bedeutet, dass eine Kryptowährung das Eigentumsrecht an einem Unternehmen oder andere Wertpapiere wie Zertifikate und Anleihen darstellen kann, solange sie sich als solches eintragen. Leider gibt es noch keine Kryptowährungsbörsen, die für den Handel mit Security-Token lizenziert sind. Security-Token sind jedoch nicht für den Standard-Kryptowährungsinvestor bestimmt. **Stattdessen haben es Security-Token auf den großen Pool an institutionellen Investoren, die noch nicht in den Kryptowährungsmarkt gedrungen sind, abgesehen.**

Institutionelle Investoren als Anreiz für Innovation

"Blockchain with improved scalability will increase efficiency in many areas: logistics and supply-chain control, healthcare, public administration (for land, car and company registries), smart contracts and more. In the financial industry, it might replace some banking functions, such as payments, custody and accounts – even independent of cryptocurrencies."

Princess Gisela von und zu Leichtenstein

Die Blockchain-Technologie reduziert die Kosten der Kapitalbeschaffung, und das ist vor allem für kleine Unternehmen von Bedeutung. Einer der Hauptvorteile des Handels mit digitalen Assets über die öffentliche Blockchain-Infrastruktur besteht darin, dass **grundsätzlich jeder ein digitales Asset ausgeben kann und jeder in ein solches auch investieren kann.** Das führt bei Emittenten zu enormen Zeit- und Kostenersparnissen, da nun weder Lizenzen, noch Underwriter oder Anwälte benötigt werden. Die hohen Kosten für die Börsennotierung eines Unternehmens stellen eine hohe Eintrittsbarriere für mittelständige Unternehmen (KMU) dar. Auch beseitigt die Blockchain so manche Eintrittsbarriere, welche **Kleinanleger von solchen Investitionsmöglichkeiten ausschließen.**

Die Blockchain-Technologie ermöglicht nicht nur einen demokratischeren Zugang zu Märkten, sondern lässt auch **einen Handel von „Aktien" zu deutlich niedrigeren Transaktionskosten mit sehr kurzen Abwicklungszeiten zu.** Dies bedeutet erhebliche Einsparungen für Kleinanleger und geringere Gewinne für Börsenmakler.

Einige Anleger, insbesondere institutionelle Anleger, wünschen sich jedoch, dass Merkmale des traditionellen Kapitalmarktes in den Token-Markt integriert werden. Willkommen in der Welt von „**Security Token".** Der Begriff "Security Token Offering" (STO) hat in den letzten Monaten im Vergleich zu ICOs deutlich an Bedeutung gewonnen. Es gibt drei Hauptprobleme, die institutionelle Investoren mit der Blockchain haben:

- Nicht alle Kryptowährungen entsprechen den Regulierungsvorschriften wie Know-Your-Customer, Anti-Geldwäsche, Sanktionen, etc.
- Großanleger legen oftmals Wert auf Diskretion. Sie haben kein Interesse an transparenten Blockchains, die es Außenstehenden ermöglichen, ihre Transaktionsbeträge und -ziele zu sehen.
- Unwiderruflichkeit: Öffentliche Blockchain-Kryptowährungen werden unzugänglich, sobald ein privater Schlüssel gehackt oder verloren geht.

Großanleger werden ein Problem damit haben, wenn ihre Vermögenswerte einzig durch einen privaten Schlüssel kontrolliert werden. Das bedeutet Stornierungs- und Neuausstellungsmerkmale werden erforderlich sind, bevor der Markt für Security-Tokens an Bedeutung gewinnen kann.

Um diesen Mangeln entgegenzuwirken, arbeiten mehrere Unternehmen an privaten Blockchains, die es ermöglichen, Security -Token sicher zu verwahren und zu handeln. Die Swiss Digital Exchange (SDX) der Schweizer Börse bei Sihlcity arbeitet an einem Pilotprojekt, das vier Hauptgruppen von Vermögenswerten tokenisieren soll.

- Zunächst sollen native Token für KMU, die bis jetzt nur auf SDX existieren, dort ausgegeben, verwahrt und gehandelt werden können.
- Zweitens, die Tokenisierung bestehender Wertpapiere an der SIX Swiss Exchange.
- Drittens, die Tokenisierung von nicht bankfähigen Vermögenswerten.
- Viertens, die Tokenisierung von Kryptowährungen wie Bitcoin und Ethereum.

"Liechtenstein is likely to be a pioneer, advancing pragmatic, innovative regulation and supervision for cryptocurrency transactions and ICOs."

Princess Gisela von und zu Liechtenstein

Neben SDX arbeitet auch Daura, eine Partnerschaft von MME und Swisscom, an einer privaten Blockchain. Blockchains, die speziell für den Handel mit Wertpapieren entwickelt wurden, verfügen über KYC/AML-Integrations-, Datenschutz-, Storno- und Reissue-Funktionen, die es dem Börseninhaber oder Broker ermöglichen, Aktien an Unternehmen auszugeben, dessen private Schlüssel verloren oder gehackt wurden. Blockstreams LIQUID und Polymath sind auch Beispiele für Blockchains, die sich an den Markt für Security-Token richten. Wichtige rechtliche Fragen, wie z.B. die Verletzung von Fondsvertriebsrechten durch die Tokenisierung eines Fonds, müssen jedoch noch gelöst werden.

Abbildung 15: Performance von Security-Token Plattformen.

Quelle: Incrementum AG

Definition von Token und Wertpapier

Ein Token ist eine digitale Darstellung eines Vermögenswerts auf einem bestimmten verteilten Ledger. Token können Stimmrechte, Eigentumsanteile, Anleihen und vieles mehr repräsentieren. ERC 20 Smart Contracts auf der Ethereum Blockchain und NEP5 Smart Contracts auf der NEO-Blockchain werden derzeit bereits zur Auszahlung von Unternehmensdividenden und zur Abstimmung von Managemententscheidungen eingesetzt. Wohlgemerkt unterscheidet sich die Definition eines Wertpapiers von Land zu Land. In den USA wird ein Finanzprodukt rechtlich als Wertpapier eingestuft, wenn die vier folgenden Kriterien erfüllt sind:

- Es muss sich um eine Geldanlage handeln
- Es besteht eine Gewinnerzielungsabsicht
- Es exisitert eine Gesellschaft
- Der angestrebte Profti wird von einem Dritten generierten

"There will be many types of assets codified into the blockchain, and they are all not just going to be on the Bitcoin blockchain – it's going to be a number of different assets here. And the best way to invest in that is a diversified portfolio."

Olaf Carlson-Wee

Wie auch im Folgeartikel von Christian Messiers über die rechtlichen Aspekte von Wertpapieren erwähnt, hat diese Kriterien der Supreme Court der USA von 1946 aufgestellt, als er in einem Fall zwischen einem Zitruszüchter aus Florida namens Howey und der Securities Exchange Commission zu eintscheiden hatte. Als Reaktion darauf beantragen Kryptowährungsemittenten in den USA Ausnahmen vom Wertpapierrecht die als Reg D. und Reg S bekannt sind. Ein weiteres Thema ist auch, wie Airdrops möglicherweise das Wertpapierrecht umgehen.

Europa hat jedoch kein Konzept Kriterienkatalog wie den Howey-Test. Dies liegt daran, dass das in den USA gepflegte Common Law Präzedenzfälle für zukünftige Urteile setzt. Im Gegensatz dazu gibt es auf dem europäischen Festland das Zivilrecht, das ein prinzipienbasierter Rechtsansatz ist. Gemäß Artikel 2, Bst. b FinfraG ist ein Wertpapier in der Schweiz definiert als „standardisierte verbriefte und unverbriefte Wertpapiere, Derivate und Bucheffekten, die für den Massenhandel geeignet sind." **Es ist daher nicht überraschend, dass die FINMA bereits viele Kryptowährungen als Wertpapiere eingestuft hat.**[53]

—

53 https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=de

"One of the most powerful use cases of blockchain technology was to inscribe immutable and transparent information that could never be wiped from the face of digital history and that was free for all to see. Satoshi's choice first to employ this functionality by inscribing a note about bank bailouts made it clear he was keen on never letting us forget the failings of the 2008 financial crisis."

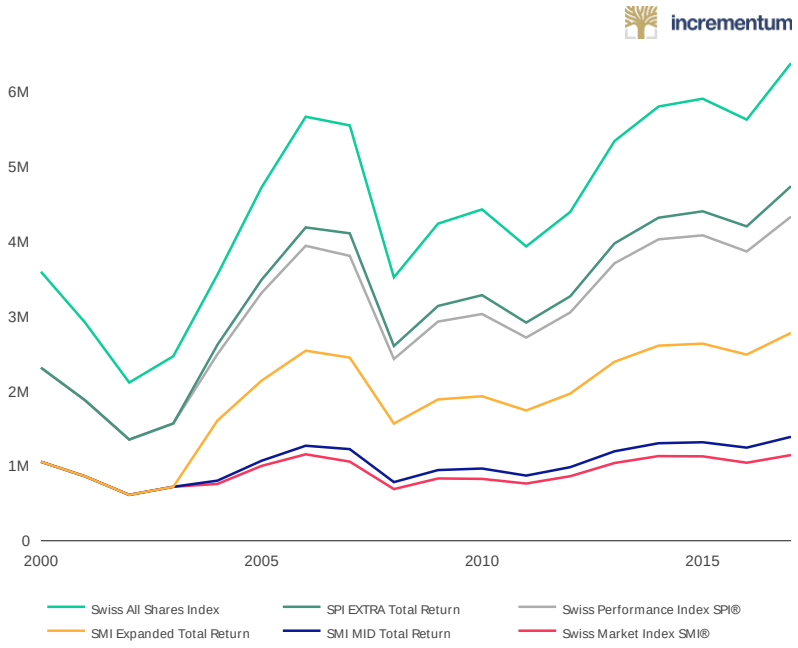
Chris Burniske (Author of Cryptoassets)

Token, Wertpapier, oder beides?

Die Tokenisierung von Assets existierte auch schon bevor Kryptowährungen ins Leben gerufen wurden. Sie sind unter dem Namen Zertifikate bekannt. Zertifikate kosten jedoch Geld bei der Emission und Erhaltung. Im Gegensatz zur Ausgabe eines ERC-Tokens auf Ethereum müssen die Emittenten von Zertifikaten über eine Unternehmensstruktur verfügen, die strukturierte Produkte rechtlich ausgeben darf, und nur qualifizierte Anleger in der Schweiz und professionelle Anleger in Europa können investieren. Gemäß dem schweizerischen Kollektivanlagengesetz (KAG) von 2006 ist ein qualifizierter Anleger einer der folgenden Anleger[54]:

- beaufsichtigte Finanzintermediäre (z.B. Banken, Effektenhändler und Fondsmanager)
- beaufsichtigte Versicherungsgesellschaften
- öffentlich-rechtliche Institutionen und Pensionsfonds mit professionellem Anlagegeschäft
- Unternehmen mit professioneller Investitionstätigkeit,
- vermögende Privatpersonen mit einem Finanzvermögen von 2 Mio. CHF (excl Immobilienvermögen)
- Anleger, die über einen schriftlichen Vermögensverwaltungsvertrag mit einer beaufsichtigten Bank, einem Effektenhändler oder einem Fondsmanager verfügen.

Abbildung 16: SIX Wachstum.



Quelle: SIX, Incrementum AG.

54 https://www.swissfunddata.ch/sfdpub/en/group/info

Vor- und Nachteile von Zertifikaten gegenüber Fonds für Kryptowährungs-Asset Manager

Vorteile

1.) Im Gegensatz zu alternativen Investmentfonds müssen Guernsey-Zweckgesellschaften keine externe Depotbank als verwahrstelle verwenden. Daher können Investmentmanager die Sicherung von Kryptowährungen an Drittverwahrer wie die in dieser Ausgabe des Crypto Research Report im Beitrag „Crypto Concepts“ genannten Unternehmen auslagern.
2.) Niedrigere Gebühren. Da Manager von aktiv verwalteten Zertifikaten Geschäfte mit den Gegenparteien ihrer Wahl tätigen und die Verwahrung von Kryptowährungen auslagern können, können die Gebühren geringer sein als bei UCITS- oder AIF-Kryptowährungsvehikeln, die mit Banken und Administratoren zusammenarbeiten müssen.
3.) Schnelle Implimentierung. **SPVs benötigen 10 Werktage für die Einrichtung, Zertifikate 3 Werktage.**

Nachteile

1.) Kryptowährungzertifikate investieren nicht immer in die zugrundeliegenden Kryptowährungen. Sie können auch nur Tracker sein. Anleger sollten überprüfen, ob das Wertpapier tatsächlich in den Basiswert investiert ist.
2.) Sofern das Kryptowährungspapier nicht von einer lizenzierten Bank oder Drittverwahrstelle, die eine Versicherung anbietet, Gebrauch macht, sind die Kryptowährungsbestände nicht versichert. Im Gegensatz zu alternativen Investmentfonds, die über haftende Depotbanken verfügen, können strukturierte Produkte und Managed Accounts eine Reihe von Optionen haben, die von völlig unversichert bis vollständig versichert reichen.
3.) Schweizer Zertifikate sind nicht immer problemlos in der Europäische Union vermarktbar.

Ein Zertifikat ist eine Art strukturiertes Produkt. **Ein Zertifikat kann ein Tracker-Zertifikat sein, das den Wert eines Assets nachahmt, oder aber auch aktiv verwaltet werden.** Das Asset kann z. B. eine IBM-Aktie oder ein Kryptowährungsindex oder ein physisches Gut sein. Die Vontobel Bank emittiert zum Beispiel viele Zertifikate. Ein Zertifikat ähnelt einer Anleihe, da es ein vorgegebenes Auszahlungsversprechen darstellt, das der Emittent dem Anleger gibt. Das bedeutet, dass die Anleger im Prospekt nachlesen können, was sie nach Fälligkeit des Zertifikats aus dem Zertifikat erhalten. Zum Beispiel könnte das Versprechen lauten: „In zwei Jahren erhalten Sie die Performance von IBM-Aktien.“ Aber Zertifikate können auch aktiv verwaltet werden. Aktiv verwaltete Zertifikate (AMCs) können jede Art von Kryptowährung enthalten, einschließlich Privacy Coins, Pre-ICO-Coins und ICO-Coins. Investmentmanager können auch riskantere Strategien im Rahmen von Fondsstrukturen gemäß OGAW oder AIF anwenden, wie z. B. Short-selling und Leverage.

Zertifikate sind wie Token in dem Sinne, dass sie zur Verbriefung von Vermögenswerten verwendet werden können. Der einzige Unterschied besteht darin, dass Zertifikate normalen Anlegerschutz enthalten und leicht über Wertpapierbroker erworben werden können. Da sie bestehenden Regulierungsvorschriften entsprechen, fallen bestimmte Kosten an. Aus diesem Grund macht die Verbriefung eines Vermögenswertes mit einem Zertifikat erst bei Vermögenswerten über 10.000 CHF Sinn. Im Unterschied zu UCITS- und AIF-regulierten Kryptowährungsfonds wie jener von Incrementum unterliegen strukturierte Produkte nicht den Vorschriften für kollektive Kapitalanlagen.

GenTwo Digital, eine gemeinsame Unternehmung der GenTwo AG und Inacta, ist eine Schweizer Beratungsfirma mit Sitz in Zug. GenTwo Digital wurde von Patrick Loepfe, einem ehemaligen Vontobel Deritrade-Spezialisten, sowie dem Vizepräsidenten des Verwaltungsrates und geschäftsführenden Gesellschafter von Forstmann, Philippe A. Naegeli, gegründet. In einem Exklusivinterview mit Patrick Loepfe von GenTwo haben wir über die Verbriefung

von Kryptowährungen gesprochen. Das Unternehmen unterstützt Finanzintermediäre, vermögende Privatpersonen und Family Offices dabei, bankfähige Vermögenswerte wie aktiv verwaltete Konten und strukturierte Produkte sowie nicht bankfähige Vermögenswerte wie Kunst und Kryptowährungen in handelbare Zertifikate mit ISIN-Nummern (International Securities Identification Number) zu verwandeln. Eine ISIN-Nummer ist ein Code, der eine bestimmte Wertpapieremission eindeutig identifiziert. In der Schweiz erfordert die Erlangung eines ISIN-Codes für ein Wertpapier einen Prospekt, ein Term Sheet und ein Offering-Memorandum. In der herkömmlichen Finanzwelt werden ISINs für Aktien, Anleihen, Fonds, Hedgefonds, Investmentfonds und andere Wertpapiere verwendet, sei es für ein privates Angebot oder für einen Börsengang mittels IPO (Initial Public Offering).

"It's bigger than the Iron Age, the Renaissance. It's bigger than the Industrial Revolution."

Tim Draper

GenTwo inkorperiert Finanzgesellschaften für ihrer Kunden, um anschließend eines oder auch mehrere Zertifikate im Namen dieser Gesellschaft begeben zu können. Die Emissionsstruktur von GenTwo ist ein einzigartiges Vehikel in Guernsey. Sobald das „Special Purpuse Vehicle" ins Leben gerufen wurde, können Kunden strukturierte Produkte nach Belieben emittieren. Der Vorteil ein solch maßgeschneidertes Emissionsvehikel aufzusetzen ist, dass die Bilanz transparent und nachvollziehbar ist. Anleger einer Schuldverschreibung unterliegen dem Ausfallsrisikos des Emmittenten. Im Falle der SPV-Struktur gibt es nur die Vermögenswerte auf der aktiven Seite der Bilanz und die Zertifikate auf der passiven Seite. **Da das Zertifikat den Wert der auf der aktiven Seite gehaltenen Vermögenswerte abbildet, ist das Gegenparteienrisiko überschaubar.** So verfügt die Bank Vontobel beispielsweise über ein SPV in Dubai, von der aus sie ihre Zertifikate ausstellt. Julius Bär hat ein SPV in Guernsey, EFG hat ein SPV in Guernsey.

Zertifikate sind keine tatsächliche Konkurrenz für Token. Token können von Kleinanlegern ausgegeben werden und jeder auf der Welt kann in sie investieren. Wir gehen davon aus, dass das eine das anderen in absehbarer Zeit nicht vollständig ersetzen wird. Stattdessen werden sich einige Marktteilnehmer für Investitionen in der regulierten Welt und andere Marktteilnehmer für Investitionen in der unregulierten Welt entscheiden. Viele Unternehmen werden in beiden Vehicle verwenden, um Kapital aufzunehmen. Wie Oliver Völkel im Rahmen des Crypto Christmas Market Outlook bereits anmerkte, besteht das Hauptproblem bei Security-Token darin, dass es keinen lizenzierten Tausch gibt, an dem Investoren diese Vermögenswerte handeln können. In 2019 wird ein Wettlauf um die erste gesetzlich regulierte Plattform stattfinden, die Kryptowährungen handeln kann, die gleichzeitig Wertpapiere darstellen.

Disclaimer: GenTwo ist ein premium partner des *Crypto Research Report*. Die hier angeführten Informationen sind keine Anlage- oder Produktempfehlungen. Der *Crypto Research Report* gibt im Rahmen von Beiträgen grundsätzlich keine Empfehlungen für Produkte oder Dienstleistungen ab. Sorgfältige eigene Recherche ist unerlässlich.

Vontobel

Investment Banking

Driven by the power of possibility

vontobel.com

Rechtliche Herausforderungen für Kapitalbeschaffung über die Blockchain

„Mit der Blockchain-Technologie kann erreicht werden, was Regierungen sich schon lange wünschen: Ein fairer, sicherer und attraktiver Kapitalmarkt für Startups, KMU und Anleger.“

Christian Meisser, LEXR AG

Key Takeaways

- **Die** Tokenezierung **scheint für Klein- und Mittelbetriebe interessant zu sein, da die Kapitalbeschaffungskosten über Tokens mitunter geringer als am traditionellen Kapitalmarkt sind.**

- **Die** aufsichtsrechtliche **Einstufung ob ein ausgegebener Token eine Unternehmensfinanzierung bzw.** Beteiligung **darstellt hat weitreichende Implikationen und ist rechtlich höchst relevant. Die Beurteilung ob ein Token aufsichtsrechtlich wie ein Wertpapier zu behandeln ist verläuft in verschiedenen Jurisdiktionen fundamental unterschiedlich ab.**

Photo: *Christian Meisser*

Verfasst von Christian Meisser, lic. iur., MBA, CEO der LEXR AG

Christian Meisser ist Unternehmer und Rechtsanwalt mit Schwerpunkt auf der Schnittstelle zwischen Technologie und Recht. Er veröffentlicht, berät und trägt regelmäßig zu Blockchain-bezogenen Themen vor und ist spezialisiert auf die Regulierung von Finanzmärkten. Nach seiner Tätigkeit für einige der weltweit führenden Anwaltskanzleien gründete er das LegalTech-Unternehmen LEXR AG mit der Vision, gleichgesinnten Unternehmern preiswerte Rechtsdienstleistungen anzubieten, die auf die Art und Weise zugeschnitten sind, wie Unternehmen heute arbeiten und innovieren.

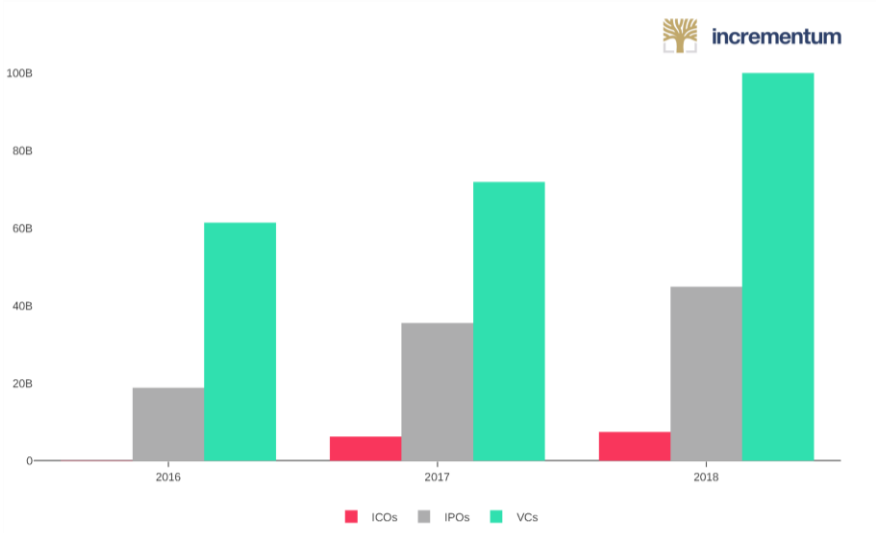
Kapitalflüsse in die USA

"The blockchain is the financial challenge of our time. It is going to change the way that our financial world operates."

Blythe Masters

Startups sowie kleine und mittlere Unternehmen (KMU) werden rundum als Innovationsmotor, treibende Kraft der Wirtschaft oder gar als Welpen des Kapitalismus gelobt. Europa bietet grundsätzlich hervorragende Bedingungen für Wachstum, mit einem mobilen und hochausgebildeten Talente-Pool, einem riesigen Binnenmarkt und einer modernen Infrastruktur. Und trotzdem: Risikokapital für Startups ist rar, vielversprechende Startups wandern ab. Gemäss einer Pressemitteilung der Europäischen Kommission[55] wurde 2016 **in der gesamten EU nur rund 6,5 Mrd. EUR von Risikokapitalgebern investiert, gerade mal ein Sechstel der 39,4 Mrd. EUR in den USA.** Nach demselben Bericht **waren Ende 2017 in der EU nur 26 Unternehmen als „Einhorn"** (nicht kotierte Unternehmen mit Marktbewertung von mehr als einer Milliarde USD) **eingestuft, während es in den USA 109 und in China 59 solcher Unternehmen gab.**

Abbildung 17: ICOs vs IPOs vs VC Finanzierungen (USA)



Source: ICOdata.io, CBInsights, Incrementum AG.

Doch nicht nur um die Startupfinanzierung, auch um den Finanzmarkt für KMU scheint es nicht gut bestellt. Ein Grund für die darbenden Startups wird denn auch in den mangelnden Möglichkeiten eines späteren "Exits" im Rahmen eines Börsengangs verortet: Die Zahl der Börseneinführungen von KMU in Europa war 2017 nur halb so hoch wie noch vor der Finanzkrise.[56] **Da die öffentlichen Märkte für KMU schwach sind, schrecken Risikokapitalfonds davor zurück, überhaupt in KMU zu investieren.** Währenddem sich die EU mit **Förderprogrammen, Harmonisierung der Kapitalmarktunion und**

—

55 Europäische Kommission - Pressemitteilung vom 10. April 2018: VentureEU: 2,1 Milliarden Euro zur Förderung von Risikokapitalinvestitionen in innovativen Start-up-Unternehmen in Europa. Aufgerufen am 19. September 2018 unter http://europa.eu/rapid/press-release_IP-18-2763_de.htm

56 Europäische Kommission - Öffentliche Konsultation über die Schaffung eines verhältnismäßigen Regulierungsrahmens zur Erleichterung von KMU-Notierungen, Aufgerufen am 19. September 2018 unter https://ec.europa.eu/info/sites/info/files/2017-barriers-listing-smes-consultation-document_de.pdf

sanfter Deregulierung bemüht, die Situation zu verbessern, wird die Welt der Startupfinanzierung gerade durch die Blockchain-Technologie grundlegend verändert. Die Möglichkeit, Vermögenswerte direkt zwischen zwei Parteien ohne Mittelsmann zu übertragen, erlaubt eine enorme Vereinfachung der Ausgabe sowie des Handels von Vermögenswerten.

"Blockchain technology isn't just a more efficient way to settle securities. It will fundamentally change market structures, and maybe even the architecture of the Internet itself."

Abigail Johnson

So wurden mittels Ausgabe von Token im Rahmen von ICO im Jahre 2017 weltweit 5,5 Mrd. USD von Startups aufgenommen – in diesem Jahr sind es bis heute bereits **14,3 Mrd. USD**[57]. Aber nicht nur der Primärmarkt, d.h. die Erstausgabe von Token, floriert. Auch **der Handel mit Token auf dem Sekundärmarkt verzeichnet tägliche Handelsvolumina in Milliardenhöhe.**[58] Die Blockchain-Technologie hat somit ihr technisches Anwendungspotential im Kapitalmarkt bereits eindrücklich unter Beweis gestellt. Auch aus Investorensicht scheint sich das Risiko ausbezahlt zu haben – zumindest gemäss einer Studie sei der **durchschnittliche *return on investment* bei einem ICO 82%.**[59] Der rechtlichen Ausgestaltung solcher Token ist in der Aufbruchsphase dieser neuen Technologie indes noch wenig Beachtung geschenkt worden und **die Investoren werden selten mit durchsetzbaren Rechten ausgestattet.** Der Trend scheint jedoch klar in die Richtung von sogenannten ***Security Token Offerings*** zu gehen: Immer mehr ICO-Teams **möchten Token mit durchsetzbaren Rechten verknüpfen, die dem Tokeninhaber eine aktionärsähnliche Stellung einräumen.** Die Vision eines Kapitalmarkts, auf dem sich Startups und KMUs ohne abzuwandern zum nötigen Wachstumskapital verhelfen können, und auf dem Anleger sicheren und einfachen Zugang zu Diversifikationsmöglichkeiten haben, kommt damit in greifbare Nähe.
Im folgenden Beitrag werden beispielhaft die rechtlichen Herausforderungen in verschiedenen Ländern für einen effektiven blockchainbasierten Kapitalmarkt aufgegriffen und insbesondere die folgenden Themen diskutiert:

(i) **Herausforderungen der Einordnung von Token im Finanzmarktrecht**
(ii) **Rechtliche Voraussetzungen für die Ausgabe von Security Token**
(iii) **Rahmenbedingungen zum Handel von Security Token**

—

57 Zahlen gemäss coindesk, Aufgerufen am 19. September 2018 unter https://www.coindesk.com/ico-tracker/
58 Zahlen gemäss coinmarketcap, Aufgerufen am 19. September 2018 unter https://coinmarketcap.com/exchanges/volume/24-hour/
59 Hugo Benedetti und Leonard Kostovetsky: Digital Tulips? Returns to Investors in Initial Coin Offerings vom 20. Mai 2018, Aufgerufen am 19. September 2018 unter https://ssrn.com/abstract=3182169

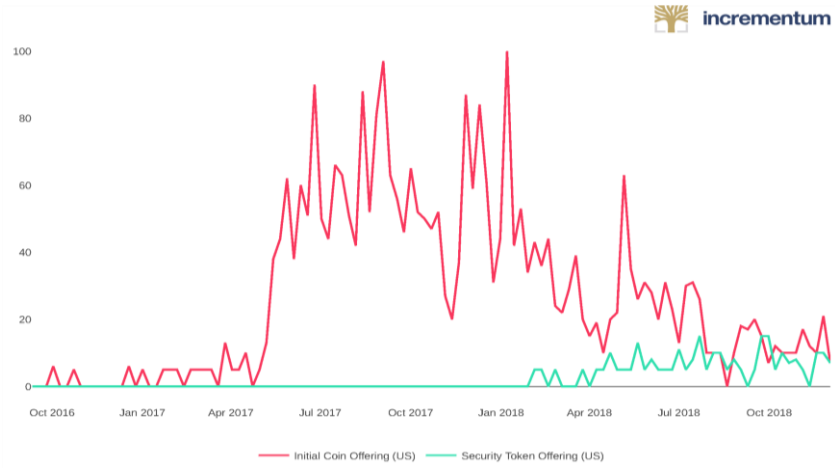
Qualifikation von Token als Security

"The regulators are still a couple of years behind because there are only a few countries that have really applied strong anti-money laundering laws."

Dave Jevans, Chief Executive Officer of CipherTrace

Bereits die zivilrechtliche Einordnung von Token in das Korsett bestehender rechtlicher Gefässe bereitet Mühe und die Meinungen der Juristen gehen weit auseinander. In der Schweiz wird beispielsweise debattiert, ob Token nun als **Daten, digitale Sachen, vertragliche Anerkennungsansprüche oder etwa *Vermögenswerte eigener Art*[60] qualifizieren.** Auch die hier interessierende finanzmarktrechtliche Beurteilung stellt Aufsichtsbehörden vor eine schwierige Aufgabe. Finanzmarktrechtliche Pflichten bei Ausgabe und Handel knüpfen an der rechtlichen Qualifikation von Token an. Gelten Token als *Security*[61] gemäss der entsprechenden Rechtsordnung, kann beispielsweise **das öffentliche Angebot solcher Token ohne entsprechenden Prospekt strafbar sein.** Die korrekte Einordnung ist entsprechend wichtig, ist jedoch alles andere als trivial. Token können, ähnlich einem weissen Blatt Papier, mit jeder erdenklichen Kombination von Rechten, Pflichten oder im Rahmen von Smart Contracts gar mit komplexen, automatisiert ausgeführten Abläufen ausgestattet werden. Verschiedene Länder versuchen diese Herausforderung auf sehr unterschiedliche Art zu lösen:

Abbildung 18: Google Trends – Wachsendes Interesse für Security Token Offerings



Quelle: Incrementum AG

In den USA hat sich historisch in der Rechtsprechung ein Ansatz etabliert, der auf flexiblen anstatt statischen Prinzipien basiert, und der an die zahllosen und unterschiedlichen Möglichkeiten adaptiert werden kann.[62] Dafür dient insbesondere der ***Howey-Test*** als Grundlage und der Begriff der *Security* knüpft daran an, ob *„an investment in a common venture premised on a* ***reasonable***

—

60 Christian Meisser / Luzius Meisser / Ronald Kogens, Verfügungsmacht und Verfügungsrecht an Bitcoins im Konkurs, in: Jusletter IT 24. Mai 2018

61 Der englische Terminus *Security* wird hier als Sammelbegriff verwendet für die sinnähnlichen Bezeichnungen in verschiedenen Rechtsordnungen wie beispielsweise Effekten oder Finanzinstrumente.

62 Securities and Exchange Commission, Release No. 81207 / July 25, 2017: Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO; Aufgerufen am 19. September 2018 unter https://www.sec.gov/litigation/investreport/34-81207.pdf

expectation of profits *to be derived from the entrepreneurial or managerial efforts of others.*" vorliegt. Ob eine „*reasonable expectation of profit*" vorliegt, ist gerade in ICO-Projekten, die den Investoren keine Rechte zusprechen, fraglich. Die Aufsichtsbehörden erhöhen die Rechtssicherheit durch regelmässige Publikation von entsprechenden Entscheiden.

Formeller ist die Rechtslage in der EU. Mit den Richtlinien über Märkte für Finanzinstrumente (besser bekannt unter MiFID bzw. MiFID II) wurden die Finanzmärkte im europäischen Binnenmarkt weitgehend harmonisiert und der Begriff des „Finanzinstruments" in Anhang I, Abschnitt C der Richtlinie definiert. **Wann ein Security Token als Finanzinstrument gilt, bleibt indes weitestgehend unklar.** Die Definitionen beziehen sich auf Begriffe der alten Welt, in die sich die diversen Ausgestaltungsmöglichkeiten von Token nicht einfach pressen lassen. Die *Malta Financial Services Authority* hat immerhin versucht, mit einem ***Financial Instrument Test*** etwas Klarheit zu schaffen.[63] Ohne Praxisbeispiele bleiben die Definitionen indes derart abstrakt, dass es bei vielen Ausgestaltungsarten von Token unklar bleibt, ob diese nun als Finanzinstrumente gelten.

"Over the next decade, there will be disruption as significant as the Internet was for publishing, where blockchain is going to disrupt dozens of industries, one being capital markets and Wall Street."

Patrick M. Byrne

Für einen Schweizerischen Kompromiss hat sich die Eidgenössische Finanzmarktaufsicht Finma (Finma) in ihrer ICO-Wegleitung[64] entschieden. Ähnlich dem US-amerikanischen Ansatz wird mit dem Investitionszweck ein funktionaler Ansatz verfolgt. Gleichzeitig werden auch formelle Kriterien berücksichtigt und es gilt grundsätzlich **jeder Token, der einen Vermögenswert repräsentiert, als Security Token.** Durch die vergleichsweise klaren Kriterien und der Möglichkeit, ein konkretes Fallbeispiel durch die Finma vorab beurteilen zu lassen, ist die Rechtslage in der Schweiz für die Ausgestaltung von Tokens gut abschätzbar.

Am einfachsten fällt die Beurteilung bei der Tokenisierung von klassischen Securities wie Aktien oder Anleihen. Für diese Art Security wurden die Gesetze geschrieben und auch in Bezug auf die Steuerfolgen sind für den Emittenten kaum Überraschungen zu erwarten. Um aber der Innovation in virtuellen Welten und der Tokenisierung von realen Vermögenswerten keine unsachgemässen Grenzen zu setzen, wäre eine restriktive Anwendung der verschiedenen Security Begriffe begrüssenswert. Würde man beispielsweise Eventtickets tokenisieren, könnte dies bereits unter den Security-Begriff in verschiedenen Ländern fallen. Einerseits liegt dem Token ein reeller Vermögenswert zu Grunde, andererseits können Eventtickets auch mit Investitionszweck, d. h. in der Hoffnung auf künftig höheren

—

63 Guidance Note To The Financial Instrument Test, Aufgerufen am 19. September 2018 unter https://www.mfsa.com.mt/pages/readfile.aspx?f=/Files/LegislationRegulation/regulation/VF%20Framework/20180724_GuidanceFITest.pdf

64 Finma, Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs), Ausgabe vom 16. Februar 2018, Aufgerufen am 19. September 2018 unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=de

Wiederverkaufswert, gekauft werden. Eine Prospektpflicht oder der Handel auf einer regulierten Börse sind hierfür indes kaum angebracht.

Primärmarkt: Ausgabe von Security Token

Aus technischer Sicht erlaubt das Internet eine einfache globale Vermarktung von Token-Offerings und mittels Kryptowährungen ist auch die Kaufabwicklung in allen Herren Länder problemlos möglich. Teure Intermediäre wie Investmentbanken sind kaum noch notwendig. Dass ein solcher globaler Kapitalmarkt sehr attraktive Finanzierungsmöglichkeiten für Unternehmen bietet, zeigt das schnelle Wachstum von ICOs. Für die Ausgabe von Security Token sieht man sich indes mit einem Flickenteppich von nationaler Regulierungen konfrontiert, wobei **insbesondere eines wichtig ist: die Prüfung von Prospektpflichten.**

"People didn't know where they could trade. When everybody owes each other IOUs that can be in multiple places at once, that's how the system couldn't tell any more who owned what and who owed what to whom. Blockchain could have prevented 2008."

Patrick M. Byrne

Ein Prospekt soll Investoren die notwendigen Informationen für einen Anlageentscheid liefern. Welche Informationen dies genau umfasst, ist von Land zu Land unterschiedlich und reicht von (noch) wenigen Seiten in der Schweiz bis zu halben Büchern in den USA. **Die Anforderungen an einen Prospekt in der EU sind dergestalt, dass sich für kleine Finanzierungsrunden die Zeit- und Geldinvestition in die Erstellung und Offenlegung von Geschäftszahlen kaum lohnt.** Um sich ein Bild von den Kosten zu machen: Gemäss Amtsblatt der EU dürften die Kosten für die Erstellung eines EU-Prospekts bei einer Ausgabe von weniger als 1 Million EUR in keinem Verhältnis zum Erlös stehen.[65] Und dies ist erst der Prospekt für die EU. Für jedes weitere Land, in dem der Token angeboten werden soll, gilt es zu prüfen, ob ein Prospekt zu erstellen und allenfalls von den lokalen Behörden zu prüfen ist.

Zu begrüssen sind insofern die Bestrebungen in verschiedenen Ländern, die Schwellenwerte für die Prospektpflicht anzuheben (in der EU etwa auf 8 Millionen EUR oder in der Schweiz auf 2,5 Millionen CHF). Mögliche Erleichterungen bieten auch diverse Ausnahmeregelungen, bspw. Schwellenwerte bei der Anzahl Investoren oder der Fokus auf professionelle Investoren. Die Prospektpflicht und beschränkte Vertriebsmöglichkeiten sind zwar ein Hemmnis für Security Token Offerings, es gibt jedoch bereits diverse Projekte, die solche Offerings erfolgreich und rechtssicher umsetzen konnten. Mit wachsendem Interesse wird sich das Know-How im Markt verbreiten und die Kosten, auch dank dem Einsatz von LegalTech-Software, für die Erstellung der Dokumentation in diversen Ländern, werden gesenkt können.

—

65 VERORDNUNG (EU) 2017/1129 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Juni 2017 (Prospektverordnung 3), Aufgerufen am 19. September 2018 unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017R1129&from=DE

Sekundärmarkt: Handel von Security Token

Am Eindrücklichsten sind die möglichen Effizienzgewinne beim Handel. Dank Smart Contracts sind sogenannte dezentrale Handelsplattformen möglich, bei denen der Handel zwischen zwei Händlern ohne jeglichen Intermediär und ohne Gegenparteirisiko für beide Händler möglich ist. Die zu handelnden Vermögenswerte werden vom Smart Contract sicher verwahrt und bei Erfüllung der vorgegebenen Bedingungen erfolgt *clearing* und *settlement* automatisch auf der Blockchain. Zusammen mit den Kosten für Intermediären und Infrastrukturen wie zentralen Effektenverwahrungsstellen, Effektenabwicklungssystemen oder Banken fallen damit auch die zentralen Gegenparteirisiken weg. Ein Ausfall à la Lehman Brothers ist in einem solchen System gar nicht erst möglich.

"2016 has proven to be the year where the most forward-thinking financial institutions are actually using blockchain technologies for payments and settlement rather than as an experiment"

Chris Larsen

Was sinnvollerweise noch bestehen bleibt, sind die Match-Making Plattformen, wie sie von Börsen bzw. Handelsplattformen betrieben werden, insbesondere für die effiziente Preisbildung und der Vermeidung von Marktmissbrauch. Aus Regulierungssicht bleiben denn Risiken wie Insiderhandel und Marktmanipulation auch in der Blockchain-Welt bestehen und die heutigen Bestimmungen hierzu sind grundsätzlich auch auf Handelsplattformen für Security Tokens anwendbar. In der Zwischenzeit werden sowohl von etablierten Börsen wie der Schweizerischen SIX[66] als auch von Blockchain-Unternehmen in diversen Ländern die Arbeit an Security Token Handelsplattformen öffentlich bekanntgegeben. Da die Regulierungen der alten Welt jedoch anwendbar bleiben, ist auch eine entsprechende Lizenz notwendig, die bisher noch in keinem (Industrie-)Land erteilt wurde. Zudem ist der Fokus von vorgeschlagenen oder umgesetzten Blockchain-Gesetzen in verschiedenen Ländern der Handel von Kryptowährungen und Utility Token - die Regulierung von Security Token Handelsplätzen bleibt davon weitgehend unberührt. Die Beratungspraxis und die Pressemitteilungen von diversen Unternehmen stimmen jedoch zuversichtlich, dass es **bald auch Handelsplätze für Security Token geben wird.** Für ICO-Teams ist gerade auch die Handelbarkeit ihres Tokens ein wichtiges Kriterium bei dessen Ausgestaltung.

Ausblick

Die Einfachheit, mit der Token ausgegeben, übertragen und mit automatischen Zahlfunktionen ausgestattet werden können, könnte die Grundlage sein für ein „**Internet of Finance**“ - einer neuen Generation von Finanzmärkten, in denen selbst kleinste Projekte von Geldgebern rasch und sicher ganz ohne Mittelsmann finanziert werden können. Man denke an die Dorfbäckerei, die sich mittels einer Kleinstanleihe mit automatischer Zinszahlung von treuen Kunden einen neuen Ofen leisten kann, oder das Filmprojekt, dessen Einnahmen bei jedem Download automatisch an die geldgebende Fangemeinde ausbezahlt würde. Die direkte Interaktion zwischen die Kapitalnehmer und -geber ermöglicht somit nicht nur
—

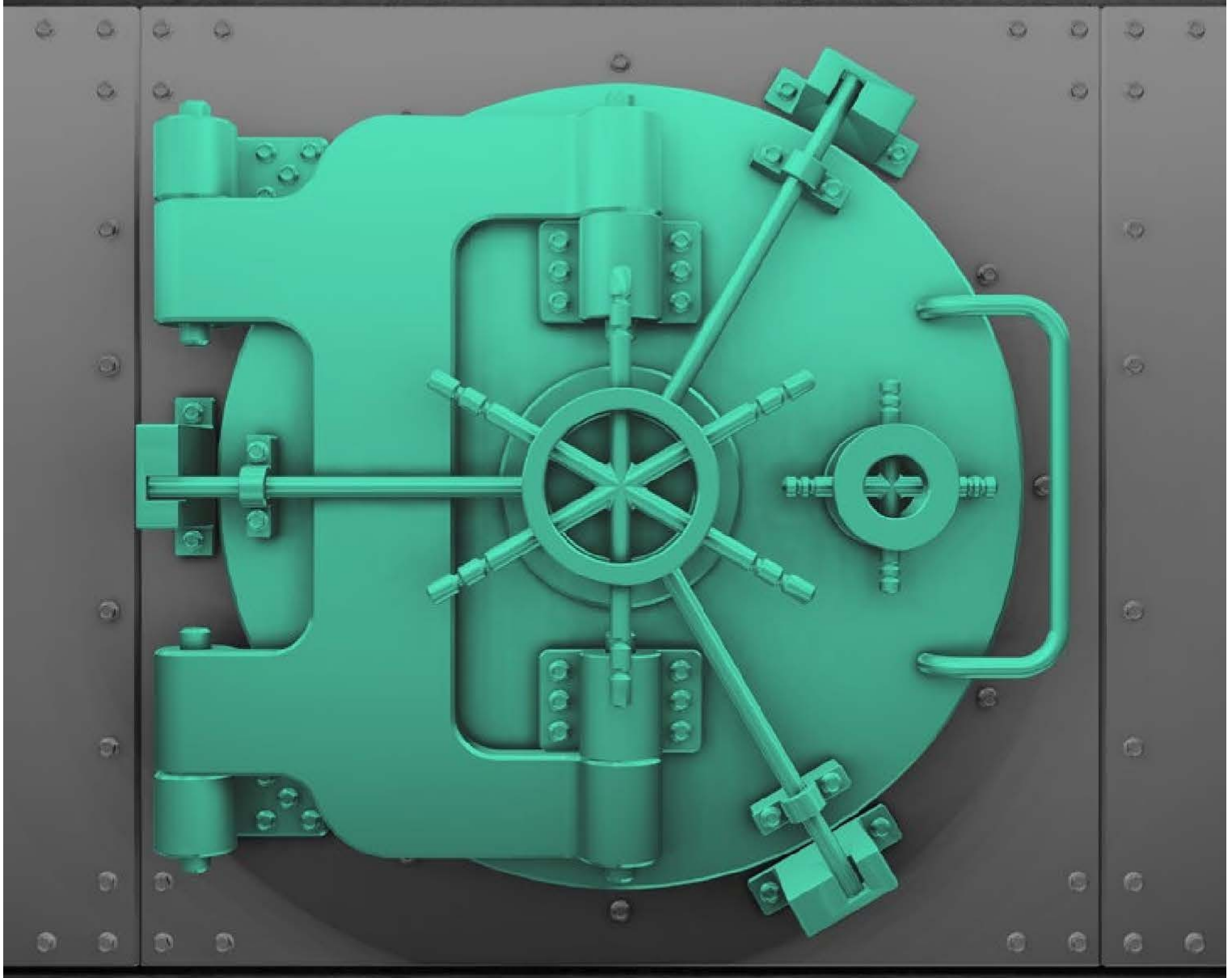
66 SIX Group AG, Medienmitteilung vom 6. Juli 2018, Aufgerufen am 19. September 2018 unter https://www.six-group.com/de/home/media/releases/2018/20180706-six-digitalexchange.html

grosse globale Finanzierungsrunden, sondern auch eine stärkere Einbindung von Kleinanlegern in die lokale Wirtschaft. Zudem ist ein blockchain-basiertes, dezentrales Handelssystem stabiler und sicherer, da mit dem Wegfall von jedem Intermediär auch ein *point of failure* und ein Mittelsmann, dessen Anreize sich nicht immer mit denjenigen der Anleger deckt, entfällt. Damit diese Technologie ihr volles Potential für einen attraktiven Kapitalmarkt für Unternehmen und Anleger voll entfalten kann, ist indes eine Anwendung des bestehenden Regelwerks mit Augenmass notwendig. Glücklicherweise schwingt das Pendel der Gesetzgeber wieder in Richtung Deregulierung, und gerade für Jungunternehmen und kleine und mittlere Unternehmen sind mehr und mehr Ausnahmen vorgesehen.[67] Damit jedoch auch die Einhörner und erfolgreichen Unternehmen sich im Heimmarkt angemessen kapitalisieren können, sind mehr als nur Ausnahmen für Kleinprojekte notwendig. In einem globalen Finanzmarkt mit mobilen Talenten wird der Mut von Regulatoren zu Offenheit belohnt.

—

67 Europäische Kommission – Factsheet zur Erleichterung der Kapitalmarktfinanzierung für kleinere Unternehmen vom 24. Mai 2018, aufgerufen am 19. September 2018 unter http://europa.eu/rapid/press-release_MEMO-18-3728_de.htm

Kryptowährungen.
Die neue Asset-Klasse.



Reguliert | Diversifiziert | Liquide

Informationen zur Fondsstrategie ausschließlich für professionelle Investoren gemäß MiFID.

www.cryptofunds.li

Über Uns

Das Team

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. Zum Advisory Board gehören:

Max Tertinegg

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

Joseph Annuzzi Jr.

Joseph Annuzzi Jr. ist Gründer und CEO einer dezentralen Kryptowährungsbörse und der Entwickler eines neuartigen Algorithmus zum Schutz von private Keys. Er ist Softwarearchitekt und Unternehmer aus dem Silicon Valley als auch Autor einer Reihe von computerwissenschaftlichen Lehrbüchern, die von Pearson Education, Inc. veröffentlicht wurden.

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 Cristian Ababii , dem jüngsten Mitglied des Incrementum Teams, für seine tatkräftige Unterstützung dankbar.

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: 2019 Incrementum AG. Alle Rechte vorbehalten.