crypto research .report

January 2019
Edition V.

"Crypto Winter Edition"

Custody Solutions for Cryptocurrencies

Securitization or Tokenization?

Could a Bitcoin Standard work?

Demelza Kelso Hays
Mark J. Valek

crypto research .report

We would like to express our profound gratitude to our premium partners for supporting the Crypto Research Report:

Vontobel

bitpanda

GENTWO DIGITAL

www.cryptofunds.li

incrementum

Contents

Editorial

Dear Reader,

The end of the year is always a good time to look back and contemplate what lessons we can learn for the New Year. During 2018, the *Crypto Research Report* covered regulation in the US and in Europe and provided insights on various crypto concepts like smart contracts, hard forks, and consensus mechanisms. In terms of market action, we offered a somewhat critical view. In the inaugural edition of December 2017, we dedicated a chapter on ICOs, called "ICOs. Scams and Big Hopes". Obviously, we were quite critical towards the ICO-bonanza. 12 months later we feel very vindicated in our opinion, as many ICOs have failed. In our March edition, we featured an article on technical analysis called "Is a Crypto Winter About to Start?" The author, Florian Grummes, nailed it when he pointed out that there was a good chance that we would see $4,500 to $5,200 by summer.

Figure 1: March Forecast of Bitcoin Downwards

Source: Midas Touch, Incrementum AG

In our October edition, we presented a valuation methodology based on our quantitative network effect. It also suggested that Bitcoin, and several other coins were still overvalued. However, on a critical note to a piece of content, we would like to state the following: In Figure 9 of the June edition of the *Crypto Research Report*, we plotted cryptocurrency consensus mechanisms according to their degree of centralization and external trust anchor. However, recent research by the International Organization for Standardization (ISO) provides a more elegant method for classifying consensus or governance mechanisms. **Simply put, a public blockchain means anyone can read. A permissionless blockchain means anyone can write.** Cryptocurrencies such as Byteball Bytes and XRP have a transparent ledger of transactions that can be viewed publicly; however, validation or witnessing can only be done by authorized nodes. Privacy

coins that have opaque blockchains, such as Monero and ZCash, fall in the opposite category, private and permissionless.

Table 1: Concensus Mechanism Classification

	Permissioned	Permissionless
Public	Ripple/IOTA/Byteball	Bitcoin
Private	Hyperledger	Privacy coins

A formal definition of "blockchain" is also starting to convalesce in the academic literature. **A blockchain is a distributed ledger database that has a consensus mechanism.** Therefore, distributed ledger technologies (DLT) are the broad category of peer-to-peer database structures and DLTs include Hyperledger, Bitcoin's blockchain, and IOTA's directed acyclic graph.

Figure 2: October's Forecast of Bitcoin Downwards

Source: Coinmetrics; Incrementum AG.

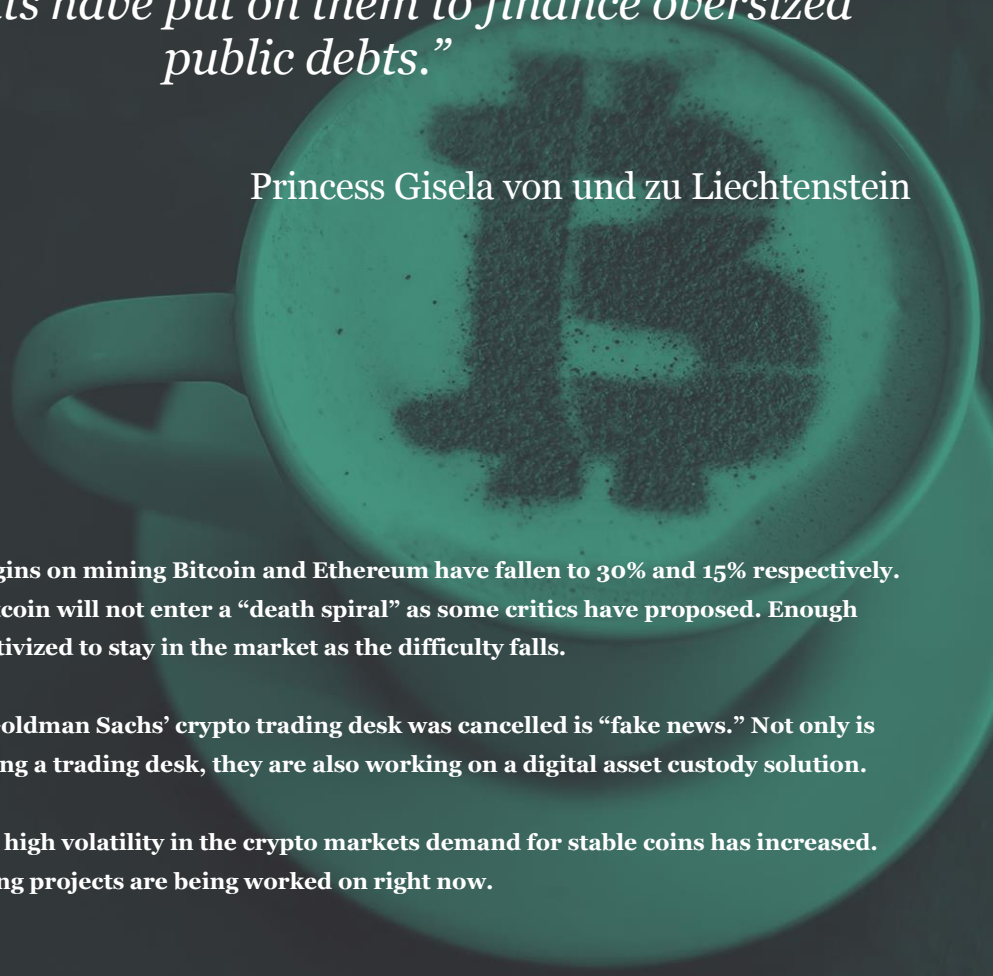
Winter is the perfect season of the year to cuddle up at home and do some research on cryptocurrencies. **This edition of the report covers institutional grade storage solutions, security token offerings, a real cryptocurrency index that considers liquidity and regulations, and an exclusive interview with Saifedean Ammous.** With this, we send you cordial season greetings and hope you enjoy our January Edition of the *Crypto Research Report*.

Demelza Kelso Hays and Mark Valek
Incrementum AG

In Case You Were Sleeping: Crypto Winter Edition

"The idea of having an alternative to traditional fiat money is attractive, especially today, when major currencies' savings value is in jeopardy and the trust they require to work is declining. Central banks are no longer focused on their duty to protect money's value and have instead bowed to the pressure spendthrift governments have put on them to finance oversized public debts."

Princess Gisela von und zu Liechtenstein



Key Takeaways

- **Gross profit margins on mining Bitcoin and Ethereum have fallen to 30% and 15% respectively. Never the less Bitcoin will not enter a "death spiral" as some critics have proposed. Enough miners are incentivized to stay in the market as the difficulty falls.**
- **The rumor that Goldman Sachs' crypto trading desk was cancelled is "fake news." Not only is Goldman launching a trading desk, they are also working on a digital asset custody solution.**
- **Due to the recent high volatility in the crypto markets demand for stable coins has increased. Various interesting projects are being worked on right now.**

Crypto-winter is in full swing. In the background, the major players are working on the infrastructure while the authorities are clearing up the debris of the ICO hype.

Source: David M. Russel/CBS

About ten years after the publication of the famous white paper by Satoshi Nakamoto, almost everything has been said about Bitcoin's anniversary. Therefore, our greetings do not go to the mysterious inventor or inventors of the cryptocurrency, but to Alicia Florrick. The likeable (and fictional) lawyer from the CBS hit series "The Good Wife" had already dealt with a Bitcoin case in 2012. It was probably the very first Bitcoin reference in a mainstream television show. The scriptwriters deserve praise. Not only because they made Bitcoin an issue when the cryptocurrency **was worth just three dollars apiece.** But also, because they could **explain this new innovation within a few minutes.** The viewers were not only entertained, but also well informed when Alicia's teenage children taught her about Bitcoin step by step. Something that others have often failed to replicate when it comes to Bitcoin.

When the Simpsons mentioned Bitcoin a year later, it was – of course – in the way of a joke (S25E07). The protagonist in this case was Krusty the Clown. Lisa Simpson asked Krusty if he was broke, and he answered: "Yeah, all it takes is some bad luck at the ponies, worse luck in the bitcoin market, and heavy investment in a high-end bookmark company." This rather depressive perspective fits in well with Bitcoin's past anniversary year.

As far as prices were concerned, 2018 was virtually the opposite of 2017. After the euphoria came disillusionment. After the boom came the bust. $20,000 was followed by $10,000. Then the $6,000 mark was held for a long time. Until the end of November. Then it went rapidly down – triggered by a dispute in the Bitcoin Cash Community. Bitcoin slipped into the $3,000 area. The media published obituaries. Like so many times before. Explanations of what Bitcoin actually is are no longer necessary. Bitcoin **has actually arrived in the mainstream.** It was a long way. The colleagues from "Breaker Magazine" have compiled a whole list of Bitcoin references in pop culture from the past ten years. They ask, "What does Bitcoin in the mainstream actually mean?" Is it about the price? Is it about using the cryptocurrency in the coffee house? Or is it about fame? We also ask ourselves these questions.[1]

The Crash and the Consequences

Since Bitcoin was first mentioned in "The Good Wife", the price has risen by more than 10,000 percent. The first ten years of the cryptocurrency are actually an incredible success story.

—

[1] https://breakermag.com/a-comprehensive-list-of-crypto-references-in-pop-culture/

But all this does not seem to interest anyone after the depressing year 2018. Bitcoin had to celebrate his birthday with a tear in his eye. Recently, there has even been debate about a death spiral. Some argue that **miners will simply stop their activities if the price falls below the cost of production.**

> *"Once Bitcoin's price falls below its cost of mining, the incentive to mine will deteriorate, thrusting bitcoin into a death spiral. That is, without the mining activities supporting the ledger that maintains the records of who owns what — bitcoin is, after all, a set of encrypted numbers that cannot establish the ownership of anything — bitcoin will become worthless."*[2]
>
> Atulya Sarin

"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

This view of things is not new. The same debate has been going on since 2011. Today, the industry is much bigger, but the answer to the scaremongering remains the same. As then, the prophets of Bitcoin's death overlook the nuances in the game theory behind the cryptocurrency. Satoshi Nakamoto prepared the network very well for a rapid drop in prices. **After 2016 blocks, the difficulty is adjusted.** If the price drops and the number of miners shrinks, the software is designed to make mining easier for the remaining miners. The argument of the death spiral is based on the assumption that the price could fall so quickly that the system does not adjust difficulty in time - and the miners give up. But there are solutions for this problem. Andreas Antonopoulos explains:

> *"If the miners wait until the difficulty retargets and the difficulty becomes less, then each miner who waits makes more profit because in the new scheme they have a greater percentage of the mining power than they did before."*[3]

In addition, one must consider: Mining costs are not the same everywhere, each miner has his or her own calculations. Some might even be able to temporarily mine at a loss. And if all else fails, there is still the option of a hard fork, which would allow the immediate adjustment of the difficulty. That would be the last resort.[4]

Of course, this does not mean that all miners did survive the fall in prices unscathed. The situation is quite dramatic. Bitcoin miners are used to huge gross profit margins of up to 50 percent. Since the fall in prices, the situation has become tougher, as BitMEX has calculated. **Currently, profit margins are only 30 percent for Bitcoin and 15 percent for Ethereum.** There are also a number of mining companies that have misjudged the situation and already went bankrupt. The cleansing of the market during the price decline does not only apply

—

[2] https://www.marketwatch.com/story/bitcoin-is-close-to-becoming-worthless-2018-12-03
[3] https://www.marketwatch.com/story/why-bitcoin-by-design-wont-become-worthless-according-to-this-crypto-heavyweight-2018-12-05?mod=newsviewer_click
[4] https://www.theblockcrypto.com/2018/12/04/the-bitcoin-mining-death-spiral-debate-explained/

to crypto projects, but also to the mining sector.[5] The CIO of BlockTower Capital, Ari Paul, explained on Episode 95 of Laura Shin's Unchained podcast that mining as an industry is not profitable because miners compete with each other in a zero-sum game.[6]

And when it comes to Bitcoin as a currency, things look even grimmer. Around Bitcoin's 10th birthday in October, plenty of experts lampooned Bitcoin's irrelevance as a means of payment.

> *"In 2018, cryptocurrencies in general have sharply limited relevance, if any, to the way that money is moved around the world.* ***Bitcoin is an undoubtedly valuable commodity and is by far the highest-profile and most important of the cryptocurrencies****, but it is not actually a currency in any real sense. It is used for some payments, mostly peer-to-peer, between parties for whom the anonymity of Bitcoin is important, or between the remaining true believers in the global potential of the system."*[7]
>
> Samuel Murrant, GlobalData's payment analyst

"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

But that's a very one-dimensional view of Bitcoin – and Murrant knows it too. He follows up: "Bitcoin is far more like gold than it is like money – it is a store of value, considered precious due to its rarity, and traded among investors to profit from changes in its perceived value over time."

Bitcoin has therefore created its own asset class: crypto. The fact that a bubble burst at the beginning of the year cannot be denied. Air is still escaping. In our very first report in December 2017, we warned of the ICO boom and its consequences. In the March issue of this year we wrote an article entitled "Is there a crypto winter threatening us?" Currently, the northern hemisphere is not only in a meteorological winter, but globally **we are seeing the second deepest crypto-winter after the bear market of 2014 and 2015.** This adjustment may have run its course, although that's too early to call.

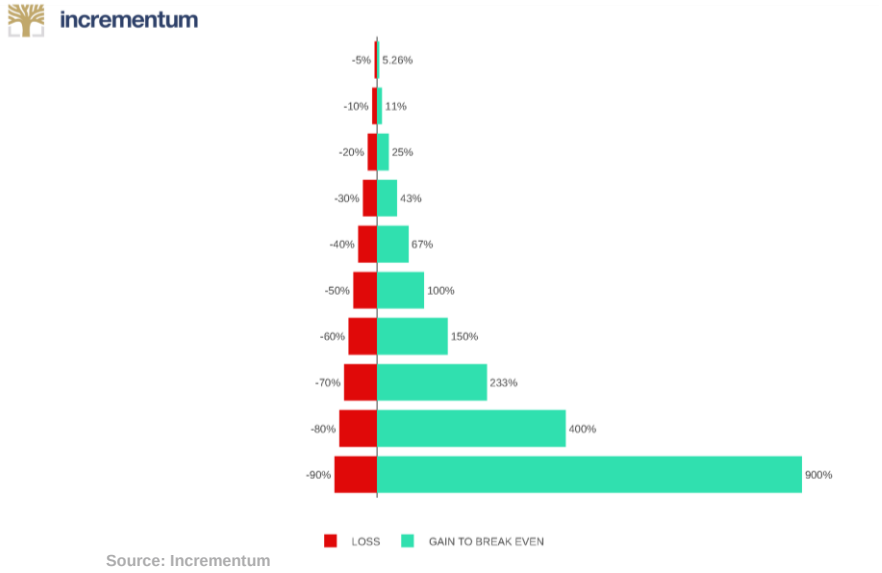
From an economic point of view, this is positive: after a bubble, only a crash can lay the foundation for new, sustainable growth. Unfortunately, however, crypto, which Morgan Stanley now also sees as an "institutional asset class", is so young that we have little experience of how long such an adjustment could take.[8] We can only wait and see how the big players position themselves for the next phase. And, as we have been documenting regularly for more than a year, there is a hell of a lot going on.

—

[5] https://blog.bitmex.com/the-price-crash-the-impact-on-miners/
[6] http://unchained.forbes.libsynpro.com/ari-paul-on-why-bitcoin-is-a-good-value-buy-today-ep95
[7] https://www.globaldata.com/ten-years-bitcoin-now-no-relevance-payments-says-globaldata/
[8] https://www.coindesk.com/morgan-stanley-says-crypto-is-a-new-institutional-asset-class/

The second sector, where Bitcoin and blockchain have undoubtedly innovated, is payment traffic and the area of currencies in general. Not necessarily because Bitcoin has asserted itself as a means of payment. We know that didn't happen. The real breakthrough is mainstream acceptance of digital currencies per se and "private" digital currencies in general. So much is happening here that even the central banks can no longer just idly watch. In a digital world, cryptocurrencies, and privately issued stablecoins in particular, offer an alternative to the Euro, Dollar or Pound.

Figure 3: 2018's Negative Return of 70% Requires Gain of 233%.



Source: Incrementum

"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

Bitcoin has also significantly influenced a third sector: cybercrime. Unfortunately, Bitcoin's second appearance on "The Good Wife" in 2013 was already about a ransomware extortion. The good news: Supervisory authorities are cracking down on fraud in crypto. From our point of view, this is very positive for the sector. 2018 may have been depressing in terms of prices, but this leads to an automatic market cleansing, and it gives the cops time to hunt scammers. The SEC even punished celebrities for advertising scamcoins for the first time. More about that later.

Asset Class and Adoption

As Michael Novogratz, one of the best-known crypto investors, puts it: "One thing you learn in this process is that everything takes a little longer than you hoped it would." **We won't see the $10,000 mark again this year,** the Bitcoin bull recently said. His company, Galaxy Digital Holdings, has already posted more than $150 million in losses this year. But Novogratz, one of Wall Street's best-known Bitcoin supporters, won't give up.[9] On the contrary: Novogratz, himself a former Goldman Sachs partner, recently invested in BitGo Holdings – together with the investment bank. Goldman and Galaxy Digital Ventures hope that the start-up will provide a solution to the still unsolved problem of custodianship of cryptoassets. US regulators require money managers to store assets in so-called "qualified custodians". The traditional players in this sector have so far stayed away from the crypto market for fear of hackers and the legal uncertainty that still prevails.[10]

Figure 4: Timeline of Famous Hacks.

Source: Incrementum

"If you were investing in any other asset class, you're probably not worried about the asset just disappearing – but this one, people still have that fear," said Mike Belshe, BitGo's co-founder and CEO in an interview with Bloomberg. His company has now collected around $70 million through fundraising. The Palo Alto-based company was founded in 2013 and offers digital wallets that require multiple signatures for transactions. Offline safes for Bitcoin and other currencies are also

—

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

available. **The company currently manages 75 different cryptoassets and a total volume of around $2 billion dollars.** But the entry of Novogratz and Goldman could take BitGo to a whole new level.

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

Adam Draper

Goldman is certainly one of the most courageous banks on Wall Street when it comes to Bitcoin. "We believe that a custody offering is a logical precursor to digital asset market making," said Goldman spokesman Michael DuVally. Reports that Goldman has cancelled its plans for its own crypto trading desk in view of the price drop have led the bank to deny this as **"fake news"**. Allegedly Goldman is also working on their own solution for Bitcoin custodianship. One thing is certain: as long as these questions have not been clarified, **the crypto market will remain closed both to the "normal" retail investor and to almost all institutional investors.** In this issue we dedicate an entire chapter to safe custody solutions that already exist or are going live soon.

Another important player who wants to compete against Goldman in this area is Fidelity Investments. **The company, which manages $7.2 trillion in customer funds in its traditional business, established its own crypto subsidiary in October.** Under the name Fidelity Digital Asset Services, customers will be able to trade Bitcoin on various stock exchanges at the best prices. Cold storage, i.e. safe storage without an internet connection, could be part of the package right from the start.[11]

> *"If you look at the existing market infrastructure, it’s heavily skewed toward the needs of retail investors and early adopters of the space. The time is quite good for this announcement. We’ve seen a real acceleration of demand over the last couple months."*
>
> Tom Jessop of Fidelity

Fidelity has been experimenting with Bitcoin since 2014, and they have even mined hundreds of Bitcoins. In the Fidelity canteen you can now pay with Bitcoin. "The question is, how do we stay ahead of the competition? How do we innovate and bring new products onto the platform?" asks Jessop.

It is by no means the case that all institutional investors are merely sitting on the sidelines and waiting. In fact, institutional investors may have replaced high net worth individuals as the largest buyers of cryptocurrencies. These trades usually take place directly between investors and large miners or people with large Bitcoin fortunes. According to current estimates, **this over-the-counter (OTC) market sees a daily volume of $250 million to $30 billion dollars.**[12] For comparison: According to "coinmarketcap.com", cryptoassets worth around $15

—

[11] http://fortune.com/2018/10/15/fidelity-launches-company-help-hedge-funds-big-investors-trade-crypto/
[12] https://www.bloomberg.com/news/articles/2018-10-01/institutional-investors-are-using-back-door-for-crypto-purchases

billion are traded daily on the exchanges. Some of the stock exchanges listed there are however not considered to be very reputable and their figures should be viewed with skepticism. At the University of Liechtenstein, a comprehensive analysis is currently being carried out on this subject, which deals with the actual market depth of the asset class. The results of the study will certainly be a topic in one of our next issues.

"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

There is no doubt that the OTC market has also suffered from the price decline. Nevertheless, growth can be observed here, says Jeremy Allair, CEO of Circle Internet Financial in Boston: **"We've seen triple-digit growth enrolling in our OTC business. That's a big growth area."** This growth is likely to continue as long as institutional investors enter the market. Because they often need more coins than are offered on the exchanges. Or they are afraid of moving the price too far by buying or selling big amounts. That's why they look for trading partners.

None of this is hidden from the big Wall Street banks. We've heard about Goldman and Fidelity**. But it looks like Fear of Loss (FOL) is quickly transitioning to Fear of Missing Out (FOMO).** Morgan Stanley, Citigroup and Bank of America Merrill Lynch are also reportedly working on their own Bitcoin products to meet customer demand.[13] Russia's Gazprombank is also venturing into the market via a subsidiary in Switzerland.[14]

And then there are the big US universities that manage their income and donations in endowments. **96 percent of university money managers still say they don't want to touch the crypto market.** In a recent interview with Mark Yusko, we discussed university investments in cryptocurrencies because some of the big names like Harvard, Stanford and MIT are already in business.[15] The same goes for Yale. The elite school recently invested in the Paradigm Fund, which was launched by former employees of Coinbase, Sequoia Capital and the Pantera Capital crypto fund. A total of around $400 million is invested in this fund. However, it is not known how much of this comes from Yale's $30-billion-dollar purse. But the step is significant, because Yale's money is managed by David Swensen.[16] Swensen is considered a pioneer among institutional investors and has managed some of the best performing college endowments over the past decades. He focuses on long time horizons and often on markets with low liquidity assets. Many other universities try to imitate him. Under Swensen, Yale has seen a return of almost 12 percent annually - over the past 20 years. In total, more than **$500 billion dollars are invested in the funds of US colleges.**[17]

—

[13] https://bitcoinexchangeguide.com/breaking-bank-of-americas-merrill-lynch-to-launch-bitcoin-trading-product-to-rival-goldman-sachs-and-morgan-stanley/
[14] https://gazprombank.ch/news/gazprombank-switzerland-ltd-prepare
[15] https://www.theinformation.com/articles/harvard-stanford-mit-endowments-invest-in-crypto-funds
[16]: 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/
[17] https://www.bloomberg.com/news/articles/2018-10-05/yale-is-said-to-invest-in-crypto-fund-that-raised-400-million

Two important players have recently underlined their interest in the crypto market but have adjusted their schedule to the new pricing conditions. Bakkt, the crypto platform of Intercontinental Exchange (ICE), has postponed the launch of its own Bitcoin futures until the end of January. "As is often true with product launches, there are new processes, risks and mitigates to test and re-test, and in the case of crypto, a new asset class to which these resources are being applied", said Bakkt CEO Kelly Loeffler. The partnerships between ICE, mother of the New York Stock Exchange, and Starbucks as well as Microsoft are still up to date - but there are no new details.[18] Nasdaq also intends to stick to its plan to enter the market with futures contracts. Starting date is the first quarter of 2019, but talks are still underway with the US regulatory authority CFTC. Nothing is set in stone.[19]

M&As and Europe

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

Fred Ehrsam

Another way to enter crypto is to become active in business yourself or to buy up other companies. We have already mentioned several times that the market crash of the past months can be good for Bitcoin - because dubious projects become unprofitable as a result and perhaps even disappear. At the same time, the sector is being consolidated and the financially strong companies are going on a shopping spree. By October, **the number of mergers and acquisitions (M&As) in the crypto sector had already risen by more than 200 percent** - compared to the previous year. At least 30 deals are still open.[20]

The crypto industry is global and so far, appropriately, without a real financial center. One of the biggest and most interesting deals, therefore, did not take place in the USA, but in Europe. **The Belgian investment company NXMH has just bought the Bitstamp stock exchange - and paid cash for it.** The purchase price was not stated. Two years ago, Bitstamp, the largest cryptocurrency exchange in the European Union, was valued at around **$60 million.** It can be assumed that the valuation for the sale was significantly higher after the 2017 boom. Bitstamp has more **than three million registered users and a daily trading volume of $100 million dollars.** For the two founders, Nejc Kodrič and Damian Merlak, the deal was definitely successful. They founded Bitstamp in Slovenia in August 2011 - in a garage. Their starting capital: A server, a few laptops and a thousand euros in cash. Today, Bitstamp is registered in Luxembourg. It is supposed to stay that way after the deal.[21]

—

[18] https://www.theblockcrypto.com/2018/11/20/bakkt-has-pushed-back-its-bitcoin-futures-launch-to-2019-but-phase-two-is-still-on-track/
[19] https://www.bloomberg.com/news/articles/2018-11-27/nasdaq-is-said-to-pursue-bitcoin-futures-despite-plunging-prices
[20] https://www.cnbc.com/2018/10/18/crypto-deal-makers-see-opportunity-in-bitcoins-price-slump.html
[21] https://www.businessinsider.com/r-european-investment-firm-buys-digital-exchange-bitstamp-in-all-cash-deal-2018-10?IR=T

"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

Two more anecdotes from Europe, this time from the German-speaking area, which is very close to us. We know from past reports that Switzerland is actively trying to attract Blockchain and Bitcoin companies. As we reported in detail in our October issue, the government of Liechtenstein is planning its own law, which is already being praised by many as exemplary. But even the giant Germany is by no means inactive. The hipster capital Berlin has a lively crypto scene. **Now there is an advance from the party of chancellor Angela Merkel. The CDU wants to make Germany the number one ICO country and a "blockchain financial centre".**[22]

Austria has another way of doing things. In Austria, ICOs are supposed to be carried out with legal certainty soon. A working group is to present results by the end of the year - then there will be a new law. But a lot is already happening on a small scale. **The Graz-based company Coinfinity and the privately-owned Austrian state printing company have developed a solution for physical, offline storage of Bitcoin private keys**. This is called "Chainlock" - and is the solution to the custodian problem, so to speak, but more for private individuals than for institutional investors.[23]

And the Viennese law firm Stadler & Völkel has succeeded in getting a capital market prospectus for a Security Token Offering (STO) approved by the supervisory authority for the first time.[24] An STO can be understood as a further development of the ICO. Like share owners, holders of security tokens also have securitized rights and are not solely dependent on the price development of a purchased token - as was the case with ICOs. In return, the security tokens are subject to the same rules as other securities. For this reason, Austria requires approval from the Financial Market Authority (FMA) before such a token can be sold. The security token of Hydrominer, whose prospectus has just been approved, is expected to be available to investors in February 2019.[25]

Central Banks and Stablecoins

After just learning a new abbreviation (STO) we now present another one: CBDC. Central Bank Digital Currency. The subject is getting hotter every day. Although to this day it's not even clear what we're actually talking about. The media likes to pretend that the central banks experimenting with digital money are developing their own "cryptocurrencies" like Bitcoin. But it's not that simple. For them, the blockchain is a vehicle to create a digital equivalent for cash.

—

[22] http://www.faz.net/aktuell/finanzen/digital-bezahlen/cdu-vorschlag-deutschland-soll-mekka-fuer-kryptogeld-werden-15887209.html?printPagedArticle=- sync:ßÇÈâÊâ<font color="#ffff00">-=
[23] https://www.trendingtopics.at/card-wallet-coinfinity-und-staatsdruckerei-bringen-neue-speicherloesung-fuer-bitcoin/
[24] One of the partners of the law firm, Oliver Völkel, is member of the Advisory Boards of the Crypto Research Report.
[25] https://diepresse.com/home/wirtschaft/recht/5541879/Depot-in-der-Hosentasche_FMA-approved-BlockchainEmission

Nouriel Roubini, the notorious Bitcoin hater, is firmly convinced that the CBDC of the future will kill Bitcoin. Because no one would accept anarchy-money if they could have state money, he reasons. However, Roubini overlooks the fact that Bitcoin has something that digital central bank currencies can never have: its deflationary character as discussed in depth in the interview with Saifedean Ammous contained in this edition of the report.[26]

"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

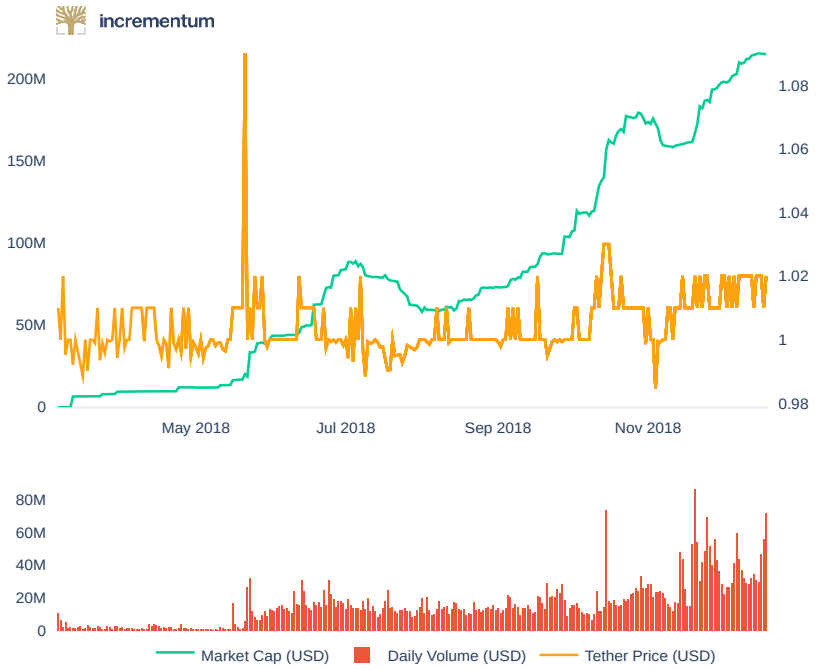
It is extremely unlikely for a central bank to ever issue a currency that tends to appreciate. In the event of over-indebtedness, the expansion of the money supply is often used as a form of concealed state financing. What can no longer be completely ruled out today is the "denationalization of money" as demanded and predicted by Friedrich August Hayek. He envisioned that commercial banks will come into the market as money producers. That is still possible. As far as private money is concerned, we are at the very beginning, but the most important steps have been taken.

Christine Lagarde, the influential head of the International Monetary Fund (IMF), has become aware of the issue. Central banks around the world need to be more open to new technologies, she said recently in Singapore. "I think we should consider issuing a digital currency. There must be a role for the state to provide the digital economy with money."[27] She speaks of a "counterweight" for private currencies and thus shows that even the high priests of money now consider the existence of Bitcoin to be a given. Lagarde, like Hayek, also wants to involve the banks. But them printing their own money is not part of the plan. Lagarde sees CBDC primarily as a substitute for cash: "A digital currency could bring advantages as a last resort for payments. And it could drive competition forward because it offers an efficient alternative at a low price - just like its grandfather, the old, reliable paper money." **But the complete anonymity of cash would then be gone.**

—

[26] https://www.project-syndicate.org/commentary/central-banks-take-over-digital-payments-no-cryptocurrencies-by-nouriel-roubini-2018-11
[27] http://www.faz.net/aktuell/wirtschaft/diginomics/iwf-chefin-fordert-digitale-waehrungen-15889788.html

Figure 5: Tether USD Price and Growing Capitalization



Source: Coinmarketcap, Incrementum AG

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

Princess Gisela von und zu Liechtenstein

Instead, Madame Lagarde proposes to record transactions and **pass on the details to the state only in case of suspicion.** A delicate idea - but not completely crazy, at least in constitutional countries where there is a separation between the state and the central bank. However, Lagarde's own experts from the IMF are quite skeptical about the subject. A recent IMF paper on the subject states:

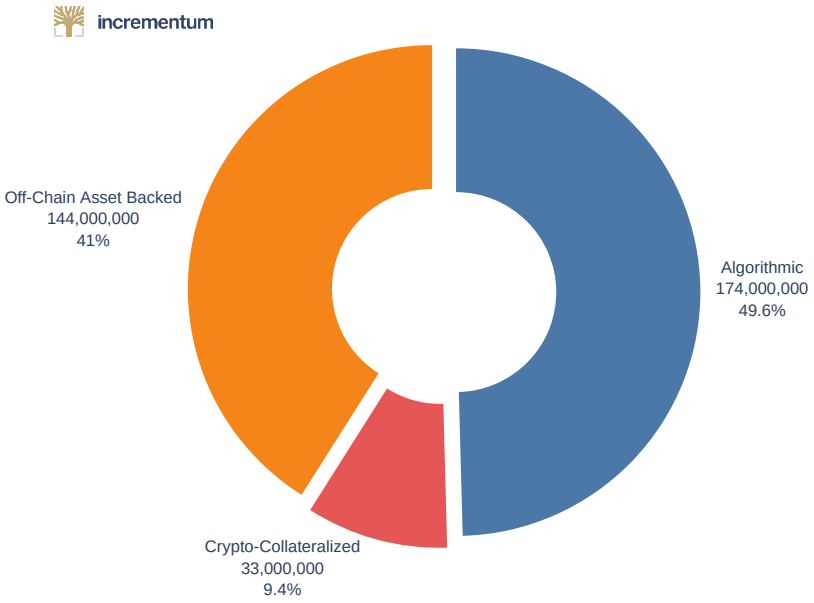
> *"All in all, it is still too early to assess the benefits of CBDC. Central banks should take into account the specific circumstances in their respective countries, pay cautious attention to risks and the benefits of other solutions. It needs further analysis and studies of technical feasibility and costs."*

It should be noted at this point that central banks are notoriously slow when it comes to technical innovations. The plans for CBDC are by no means mature. One thing is certain: we are not talking about digital money as we already know it. An account balance is ultimately a claim to the bank. CBDCs must be currencies with no counterparty risk - as with Bitcoin or gold. **Even if the true motivation of central banks and the IMF is the preservation of the money monopoly, the efforts to obtain their own digital money ultimately indirectly legitimize private alternatives such as Bitcoin conceptually.**

It should come as no surprise to anyone that Sweden is the country where plans for a CBDC are the most advanced. Sweden is regarded as the test tube of a cashless society and is now reaching the limits of what is feasible. There have long been protests by citizens against the abolition of cash, which has been pushed mainly by banks. This is one of the reasons why the central bank launched the E-Krona project and is currently investigating the various technical possibilities for introducing an electronic Krona. The Riksbank, the Swedish central bank, has now

called on the government to create the necessary legal framework for a possible introduction of an E-Krona. "If the marginalisation of cash continues, a digital krona, an e-krona, could ensure that the general public still has access to a state-guaranteed means of payment", the Riksbank said.[28]

Figure 6: Stablecoins Categorized by Funding in Dollars



Source: Incrementum AG

"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

2019 will see the rise and expansion of private stablecoins. Joining Tether is also the Gemini Dollar, TrueUSD and Paxos. And of course, USDCoin, which is backed by no one other than Circle, in which Goldman Sachs is also invested. USDCoin is now even used and offered by the Bitcoin giant Coinbase.[29][30] Currently there are more than 50 such stablecoins. Some of them are not even tied to an existing national currency - but most of them are. During falling Bitcoin prices, investors can save their digital money in a USD stablecoin and wait until the market calms down. Of course, the controversies surrounding the original stablecoin Tether are not over. Even the US authorities are now investigating accusations that the backers of Tether and the Bitfinex stock exchange manipulated the Bitcoin price.[31]

—

[28] http://fortune.com/2018/10/26/sweden-riksbank-e-krona/
[29] https://www.bloomberg.com/news/articles/2018-10-29/stable-coin-backed-by-circle-coinbase-draws-most-early-demand
[30] https://www.bloomberg.com/news/articles/2018-10-23/crypto-exchange-coinbase-to-list-stable-coin-backed-by-circle?srnd=cryptocurrencies
[31] https://www.bloomberg.com/news/articles/2018-11-20/bitcoin-rigging-criminal-probe-is-said-to-focus-on-tie-to-tether

Figure 7: Stablecoins in Comparison

Source: Coinmarketcap, Incrementum AG

ICO-Bust and Outlook

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

Rick McElroy,
Carbon Black security strategist

The SEC has dozens of investigations into crypto matters under way.[32] Two providers of ICOs (Airfox and Paragon Coin) had to pay fines of $250,000 each and compensate investors. They conducted their ICOs after the SEC issued an explicit warning last summer that ICOs were illegal sales of securities.[33] The penalties imposed by the SEC on two celebrities who had advertised dubious crypto currencies are likely to be much more effective. The boxer Floyd Mayweather and the hip-hop star DJ Khaled accepted fines of $300,000 and $100,000 dollars, respectively, as part of a settlement. The celebrities also had to relinquish the proceeds from their promotional activities - amounting to a further $300,000 and $50,000 respectively. According to the SEC, they had advertised ICOs on social media without disclosing that they were being paid.
Both celebrities had advertised Centra, a project that has been in the SEC's sights for quite some time. "Investors should be sceptical about investment advice posted on social media platforms and not make decisions based on recommendations from celebrities", warned Steven Peikin of the SEC. "Social media influencers are often paid promoters."[34]

While we consider it positive that the authorities have intervened here, it must be said that it is a drop in the ocean. Investors should be extremely careful with any form of information they obtain from the crypto-media and crypto-influencer environment. **Three independent studies have shown that the media, so-called rating agencies, and individuals on social media and on YouTube are highly corrupt.** The "Breaker" magazine wrote to 22 different crypto media

—

[32] http://fortune.com/2018/11/02/sec-ico-report-cryptocurrency-scams/
[33] http://fortune.com/2018/11/16/sec-airfox/
[34] https://diepresse.com/home/wirtschaft/5538851/KryptogeldWerbung_High penalties for Boxer Mayweather and DJ Khaled

companies from a fake address of an alleged Russian PR man. **The result: more than half of the websites would have taken money for articles without marking them as "ads" or "sponsored".** Some were even willing to simply adopt ready-made PR texts and pass them off as their own. The smallest websites took less than $300. The largest more than $3000. In any case, this study explains why there are so many miserably written texts on the Internet about relatively obscure coins. **Advertising is subtle.** Among the websites that take money for reports are some of the best-known names in the cryptosector. But to be fair: Around 10 of the websites contacted immediately rejected the offer.[35]

"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

But news sites are just the tip of the iceberg. The covert advertising campaigns are often managed by so-called ICO agencies, which have price lists for various channels at hand. These agencies do not only take care of the marketing of a coin on the relevant websites, but also provide comments and traffic in the Telegram groups and other social networks. **Many people who discuss cryptocoins or ICOs on YouTube are also paid for their service.** Research by Breaker, Techcrunch and Reuters paints a picture of a deeply corrupt industry at the heart of which is the hunt for money by ICOs.[36][37]

If the drop in prices and the SEC's crackdown leads to this swamp being drained, then this should be welcomed. This is part of the development of the sector towards more professionalism. As far as mainstream acceptance is concerned, we no longer need to worry. Years after Bitcoin's first appearance on "The Good Wife", a feature film with Kurt Russel is soon to come. The title is simply "Crypto".[38] And shortly before this report went to press, this news came in: Electronics giant Samsung is supposedly working on a cryptowallet for their smartphones. If there is any truth to this, it would be another big step into the mainstream. And a confirmation of the old thesis: **While prices are falling, true innovations are taking place.**[39]

—

[35] https://breakermag.com/we-asked-crypto-news-outlets-if-theyd-take-money-to-cover-a-project-more-than-half-said-yes/
[36] https://www.reuters.com/article/us-crypto-currencies-promoters-specialre/special-report-little-known-to-many-investors-cryptocurrency-reviews-are-for-sale-idUSKCN1NW17S
[37] https://techcrunch.com/2018/09/18/inside-the-pay-for-post-ico-industry/
[38] https://www.imdb.com/title/tt8563452/
[39] https://www.sammobile.com/2018/12/11/exclusive-samsung-bitcoin-app-cold-wallet-cryptocurrencies/

bitpanda

Home of **Cryptocurrency**

TRADE. SEND. SWAP.

Visit us on **www.bitpanda.com**
and download our app

GET IT ON Google Play

Crypto Concepts: Custody Solutions for Crypto Currencies

"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 of Swiss Crypto Vault AG

Key Takeaways

- **At no point should a crypto custody solution provider have access to a client's unencrypted private key. The industry standard may very well become Hardware Security Modules (HSMs) for the creation of private keys.**
- **Reputation and experience should be considered when evaluating a crypto custody solution for your organization.**
- **Consider that outsourcing your private key storage is similar to outsourcing your gold storage. In case of an emergency, will you be able to access your cryptocurrency if someone else is the gatekeeper?**

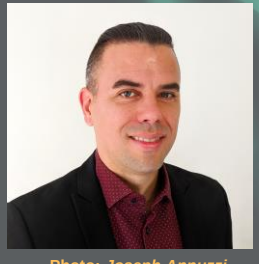


Photo: *Joseph Annuzzi*

Authored by Joseph Annuzzi Jr.

Joseph Annuzzi Jr is the founder and CEO of a stealth cryptocurrency decentralized exchange and the sole inventor of a novel cryptocurrency secret key protection algorithm designed for consumers. He is a software architect and entrepreneur from Silicon Valley and an author of a series of computer science text books published by Pearson Education, Inc. He is also the owner of cryptocustodysolutions.io a resource for crypto custody solutions.

In this article, we explore solutions for institutional cryptocurrency custody. Cryptocurrency custody solutions are needed because improper handling and storage of cryptocurrencies can result in loss or even theft. Self-managed cryptocurrency accounts are not insured against loss or theft, and law enforcement may have difficulty in recovering stolen cryptocurrency such as Bitcoin depending on the different ways thieves attempt to mask their efforts. From a regulatory point of view, professional custody solutions can also be compulsory. As is the case with investment funds. Thus, there is an increased demand for professional solutions.

Not All Institutional Storage Solutions Are Made Equal

"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

Let's begin with a brief overview of some of the components required to use cryptocurrency. One such component is a cryptographic key pair in the form of a public key and private key. The public key is used to derive a public cryptocurrency address that may be made available to the public. A cryptocurrency address is very similar to an email address, meaning, anyone with knowledge of the address can send information to that address, in the form of a balance of coins or tokens. A cryptocurrency address has a record of its balance and is able to receive and send an amount of cryptocurrency, provided the owner of the cryptocurrency address has access to its associated private key. The private key must always remain private and is much like a password for a particular cryptocurrency address. Only the owner of a cryptocurrency address should have access to the private key. Revealing the private key to an unauthorized party puts a cryptocurrency address at risk for theft of its balance. Further, to spend any balance associated with a particular cryptocurrency address, access to the private key of that address is required to authorize the transaction. One wouldn't want to give an unauthorized party access to their email password, so in the same respect, one would not want to give an unauthorized party access to their cryptocurrency private key. The cryptocurrency address or the balance associated with a cryptocurrency address is not the asset that needs protection. A user's private key associated with a cryptocurrency address is the asset that needs protection.

In the last issue of the Crypto Research Report, we explored this topic and titled the entire issue ("Handy Theft Edition"). The private key requires extreme care and consideration with its storage and security and failure to maintain the utmost of care may result in loss or theft of cryptocurrency. Anyone who has been around the cryptocurrency space for some time has probably seen news related to theft of cryptocurrency. Theft of cryptocurrency has been a focus of cyber criminals because **once stolen, it is impossible to reverse a transaction.** The only way to recover any funds would be to gain access to any private key associated with any cryptocurrency address that has taken custody of the stolen funds. Good luck locating extremely sophisticated cyber criminals in this day and age.

Theft is not limited to criminals hacking into computer systems of an organization. Theft could also originate from within the organization if one or more of the wrong personnel are put in charge of the safekeeping of the private keys associated with

any cryptocurrency address holdings. Let's consider how institutions are organized, for example, a corporation or other similarly organized entity. Being that an institution may be made up of more than one individual, comprising personnel that makes up a board of directors, executive management, and other such employees, how should a company decide who should have the rights to access and secure the private key associated with a cryptocurrency address? Should it be the chairman? The board? An executive, such as the CEO or the CFO? A particular employee such as a software developer? What about a combination of one or more of the preceding options? An organization might ultimately decide that a combination of personnel comprised of a board member, an executive, and a software developer is required to transact with any cryptocurrency holdings. With the complexities associated with storing and securing cryptocurrency, we should be able to see that there is an opportunity for businesses to provide cryptocurrency custody solutions for those lacking the sophistication or resources required for securing private keys for cryptocurrency addresses that are associated with large holdings.

"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."

Kyle Samani,
Multicoin Capital hedge fund manager

Via our Twitter Channel @cryptomanagers, we invited institutional custody solutions to provide us with some information about their products. The following five companies which offer custodian services of cryptocurrencies reached out to us. In exclusive interviews with the security officers, we gained knowledge of how these different firms attempt to solve the custody problem for investors. Our research results lead us to the conclusion that not all storage solutions are made equal. Many thanks to all contributing companies for their helpful cooperation. The results presented here are based on the information provided by the providers and are not guaranteed.

Crypto Storage AG

The first crypto custody solution that we investigated was Crypto Storage AG.[40] Crypto Storage AG is a subsidiary company of Crypto Finance AG which was founded in 2017 and is based in Zug, Switzerland. Crypto Storage AG offers services for storing blockchain based assets securely through a compelling infrastructure solution. We had the pleasure of speaking with the CEO, Stijn Vander Straeten, and the Technical Sales Engineer and Implementation Project Manager, Maria Sommerhalder. According to the company's material, they have over 40 internal and 13 external professionals involved with creation and implementation of the solution.

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

Mohsin Jameel

The infrastructure of Crypto Storage AG is made up of a transaction user interface that communicates with a backend server infrastructure that specializes in bookkeeping and relaying of messages between the Hardware Security Modules (HSMs) and the Hardware Approval Terminals (ATs). An HSM is a computer with

—

[40] See "Storage," *Crypto Finance*, 2018.

cryptographic processing capabilities that operates within a tamper-resistant hardware device that is capable of performing encryption and decryption, key generation, and digital signature creation and verification. Some HSM manufacturers allow for customizing the processing capabilities through programmable extensions made possible with software development kits or by special request.

Approval Terminal and Hardware Security Module Increases Security. Source: Crypto Storage AG

"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

The backend server infrastructure and the HSMs are distributed across Switzerland in a georedundant fashion, and one of the locations used to be a military bunker located in the Swiss Alps. Georedundancy provides strong assurances that if one location goes offline there is another location available as a backup. The ATs are installed at the client's facility and are linked cryptographically with the backend servers and HSMs through encrypted communication. The company behind the HSMs and the ATs is called Securosys, which is based in Zürich, Switzerland. The company involved with the operational security aspects and backend software development is AdNovum, which is also based in Zürich, Switzerland. These companies assisted in the development and implementation of Crypto Storage AG's solution.

What is unique about the Crypto Storage AG solution is the combination of HSMs and ATs that are cryptographically paired. This allows for both hot and cold storage capabilities for the client where the private keys are generated on the HSM and never leave the device, thus, being the cold storage aspect. Crypto Storage AG is unable to access the client's private keys stored on the HSM due to its secure tamper-proof construction. In addition, the cryptographically paired ATs provide hot-wallet-like capabilities **where the client may initiate withdrawal transactions out of cold storage while being able to rely on a secure device.** Crypto Storage AG refers to this as "deep cold storage allowing for the flexibility and speed of a hot wallet."

Further, the client is able to design a custom approval framework where the client can mirror their own operational processes for approving crypto transactions. The approval framework allows for the design of rules which are then stored with the

private key inside the HSM. For example, an m-of-n approver scheme might be configured for initiating any transaction, where one or more groups of approvers are required. Time delays may also be configured to ensure that any withdrawal transaction follows the appropriate governance procedure suitable for the client. The ATs have the same security standards as the HSMs and the ATs require a personalized smart card and pin code per approver to initiate any withdrawal transaction. This solution is an extremely powerful yet highly secure means of storing and transacting with crypto.

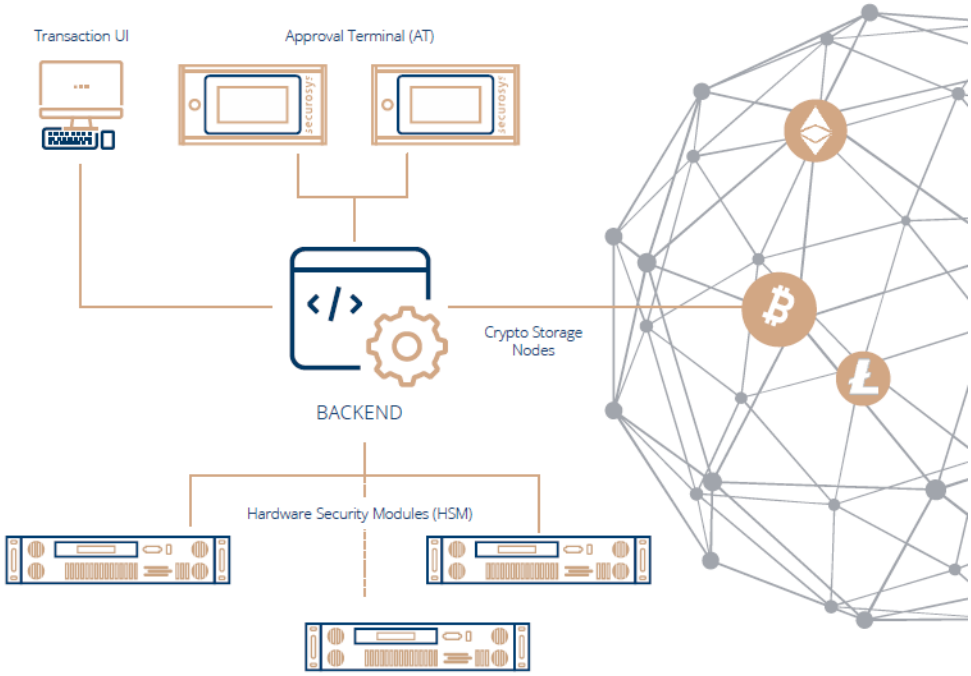
"As to storing coins safely, I'd say a hardware wallet, however a lot of care is required in avoiding compromised hardware. Using multiple hardware wallets from multiple vendors in a multisig configuration would probably be the safest at this point."

Mark Karpelès,
former chief executive of Mt.Gox.

Crypto Storage AG supports 59 out of the top 100 cryptocurrencies by market capitalization and new cryptocurrencies are added regularly. Target clients are banks, asset custodians, family offices, brokers, insurance companies, pension funds, exchanges, and foundations. **As for insurance, the technical infrastructure is covered which may include some client assets but not all.** How much of one's assets may be insurable is definitely worth investigating when exploring Crypto Storage AG as a potential custody infrastructure provider.

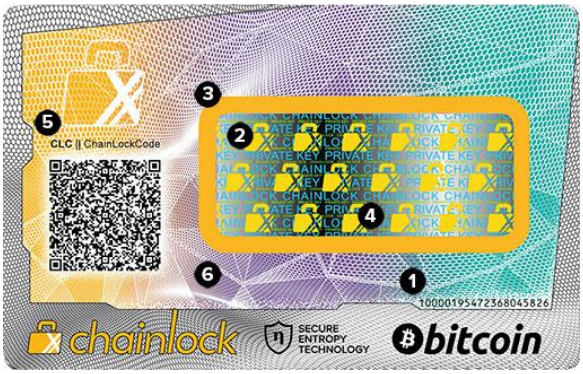
Overall, Crypto Storage AG has a very compelling solution worth exploring for any institution or private individual that desires extremely secure storage with near immediate withdrawal capabilities and a highly configurable governance process if desired.

Figure 8: System Architecture of Crypto Storage AG.



Source: Crypto Storage AG

Card Wallet



Card Wallet by Coinfinity.
Source: Coinfinity GmbH

Card Wallet is another company that we reviewed, which is a co-production between Coinfinity and the Austrian State Printing House. Coinfinity is a Bitcoin broker based in Austria that offers services to both businesses and consumers. Coinfinity also offers consumers the ability to purchase Bitcoin at retail outlets throughout Austria at nearly more than **4,000 locations and is also known for installing the first Bitcoin ATM in Austria**. In addition to retail locations, Coinfinity also provides services that allow merchants to get paid in Bitcoin. The Austrian State Printing House is known for their services in printing identity documents in a highly secure facility and controlled fashion. Together, their services are used for operating Card Wallet.

Managing Director of Coinfinity, Max Tertinegg explained in an exclusive interview that Card Wallet is a **credit-card-sized tamper-proof card that allows customers to store Bitcoin in an offline manner, similar to how one would store Bitcoin using a paper wallet, that is, writing down the private key on a piece of paper.** The difference is that Card Wallet is a polycarbonate plastic card and a Bitcoin private key is laser-etched directly onto the card and then covered and sealed with a tamper-proof sticker. The private key is generated with what Card Wallet defines as Secure Entropy Technology (SET).

According to Max, SET leverages three random number generators for generating the entropy for deriving a Bitcoin private key printed on the card. Entropy is a way to generate an unpredictable output of information that is nearly impossible to reproduce. The random number generators are made up of a hardware device provided by the Austrian State Printing House, a software solution provided by the Austrian State Printing House, and a human-derived random number generator performed by the personnel of Card Wallet by rolling dice and then documenting the results to produce the random number. When these three generated random numbers are combined, they are used as inputs for generating a Bitcoin private key that is then laser-etched onto a physical card.

The printing of cards is performed in a secure room of the Austrian State Printing House and, according to Max, is protected by approximately seven or eight different physical firewalls, so one could imagine how secure the facility may be. No copy of any private key is stored on any permanent storage means, and, assuming the facility maintains its security guarantees, in theory, the personnel at the facility will never gain access to the private keys. The card is reasonably priced at €59 and currently supports Bitcoin. In the future, Ether along with other cryptocurrencies will be supported. Card Wallet is very similar to a pre-paid gift card and seems most appropriate for insignificant amounts of cryptocurrency, maybe for gifting a family member or friend. Given the counterfeiting possibility of card storage solutions, the party who receives this as a gift should be told to only purchase new Card Wallets directly from the manufacturer.

For the institutional or wealthy investor looking to securely store hundreds of thousands, or millions, a different custody option may be more appropriate. In view of the possibility of forgery, Card Wallets should only be purchased directly from the manufacturer.

Attack Vectors of Card Storage Solutions

1) Since the private keys exist on a computer system in temporary memory for a brief moment in time before it is laser-etched onto a card, a bad actor within the facility or who compromised the facility infrastructure could potentially gain access to one or more private keys. This attack scenario is highly unlikely and would require the coordination of many different parties to execute.

2) During the shipment of a card, a postal facility could potentially intercept and swap a counterfeit card in place of a genuine card as it is making its way to a customer. This type of attack would require the coordination of many actors across many different facilities, but it is not impossible. Credit cards passing through postal facilities on their way to unsuspecting customers have been known to go missing while in transit. Registered shipping significantly reduces the risk. Registered shipping significantly reduces the risk.

3) Counterfeit cards listed for sale on an online marketplace, such as eBay or Amazon, could accidentally be purchased. A counterfeit card would mean the unsuspecting customer is purchasing a deposit address under the control of a criminal or a private key that has been intentionally compromised so any deposits of Bitcoin could be stolen by the criminal. Counterfeiting is not impossible, as we have seen occurrences of counterfeit consumer hardware wallets purchased at online marketplaces, such as eBay and Amazon.

Daenerys & Co.

Daenerys & Co. is another crypto custody solution that comes from the Silver Bullion Group. Silver Bullion Group was founded in 2009 by Gregor Gregersen and is based in Singapore. Silver Bullion Group offers secure storage facilities for precious metals, provides insurance, as well as liquidity services. Since 2009, Silver Bullion Group has done over $400 million in sales. As Silver Bullion Group

has done with safeguarding precious metals, Daenerys came from a need to solve custodial and compliance issues as they pertain to digital assets. Gregor Gregersen and Clint Mark Gono are positioning Daenerys to be a leader in the space with a one-of-a-kind business and security protocol called the Gregersen-Gono Physical Crypto Storage (GGPCS) standard.[41] GGPCS is currently being used at Silver Bullion Group's vaulting company called The Safe House.

Encrypted polycarbonate card of Daenerys & Co.
Source: Daenery's & Co.

The process begins in a secure vault on computers that have no Internet connection. These computers generate a Bitcoin private key within the temporary memory of the computer, then encrypt this private key with a first encryption key, and then encrypt it once again with a second encryption key. Each of these encrypted private keys is then laser-etched, in the form of a QR code, onto its own polycarbonate plastic card, a primary card, and a recovery card. Once the encryption process is finished, the private key is then wiped from the computers' temporary memory and is not stored anywhere in the permanent storage of the device. The cards are then analyzed to ensure the etching process performed as expected and that the QR code is readable. The polycarbonate plastic is a material that is capable of **surviving long periods of time, although the material is not fireproof but supposedly readable even if up to 30 % of the card become damaged.** This is why it is useful to have a primary card and a recovery card. If the primary card suffers any sort of damage, the recovery card stored at a different physical location could be used to recover any assets associated with that Bitcoin private key. Once the etching process is complete, the card is then placed in a lockbox that resembles a gold bar, and that lockbox is then stored in the facility in a manner similar to how gold bars are secured.

Secure vault at the Daenerys facility.
Source: Daenery's & Co.

Once the client has access to the deposit address associated with a particular private key, the client is then able to initiate a deposit to that address. On the other hand, withdrawals from this address require a multistep process to ensure the withdrawal request is coming from the actual client initiating such a withdrawal. Prior to a withdrawal, the client is required to configure Authorization Mandate rules. These rules might reflect the client's governance structure within their own organization, where one or more authorized representatives, such as the CEO, the CFO, and/or the compliance officer, are all required to approve such a withdrawal, or possibly two of those three. Daenerys uses a live video conference to authenticate the representative initiating the withdrawal, and any withdrawal may only be made to a preapproved address.

Insuring one's cryptocurrency assets is probably a great idea when someone else maintains custody. **Daenerys also offers an optional insurance policy where an individual card is insurable up to $5 million.** The insurance

—

[41] See "Crypto Currency Physical Storage," Gregor Gregersen and Clint Mark Gono, *Little Bit*, September 21, 2018.

provider has a Standard & Poor's A+ rating, is based in London, and is something worth looking into.

Blockvault

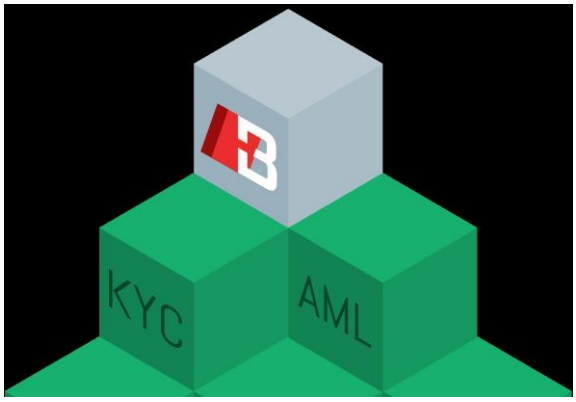
"A lot of people are unaware in this new gold rush, people are using cloud wallets and not securing their money."

Rick McElroy

Another crypto custody solution investigated was Blockvault, which is powered by Goldmoney Inc. We had the pleasure of speaking with Josh Crumb, co-founder and director of Goldmoney, and Will Felsky, director of operations of Blockvault. Goldmoney is a company that provides a way for institutions to invest in precious metals. The company was also founded in 1999 and is **a public company listed on the Toronto Stock Exchange (XAUMF).** Their current customers rely on **Goldmoney to secure $2 billion worth of assets**. Goldmoney is also **a debt-free company with more than $100 million at its disposal.**

Being that Goldmoney is in the precious metal's storage business, they have access to precious metal storage facilities around the world. Goldmoney saw an opportunity to provide similar custody solutions for institutional clients in the crypto space. They are leveraging their network of vault providers around the world for Blockvault.

Blockvault offers its clients an offline private key storage of crypto. The private keys are created by Blockvault, although the method of private key generation was not disclosed during the interview. Regardless, client's cryptoassets may be covered under an insurance policy. The company's auditor is KPMG, and they are used to confirm and verify that the assets under its management are in fact in its respective vault. KPMG is also the auditor for Goldmoney where they perform IASC audits for gold bar custody confirmation. The Blockvault insurance they are offering is made up of a collection of many of the major insurance companies. Blockvault also mentioned that their vault providers, auditors, and insurance partners are all publicly traded businesses. They are currently working with vault providers in Canada, United States, United Kingdom, Switzerland, Dubai, Singapore, and Hong Kong.



Blockvault focuses on Know-Your-Customer and Anti-Money Laundering.
Source: Blockvault

Blockvault described the high-level process of how their offering works. It begins with know-your-customer (KYC) and anti-money-laundering (AML) checks during the client onboarding process. Once through the onboarding process, the client is provided with a trade receipt of a list of addresses that they are able to deposit their crypto funds to. Blockvault's target clients are regulated or registered financial institutions, banks, broker-dealers, registered funds, cryptocurrency miners, and other similar businesses that can pass bank level KYC/AML tests. The target customer is more than likely the institution looking to safeguard $50 million or more in crypto, although they would be willing to accept clients starting with $1 million. They recommend that each address store approximately $50,000 worth of crypto, so if depositing $1 million of crypto, those assets would be safeguarded across 20 different crypto addresses that have a corresponding key pair. Every deposit is issued a trade receipt, and the governance model for how to deposit and withdraw

is customizable by the client, and that is something that is usually agreed-upon through the contractual relationship with Blockvault. As for the maximum amount of cryptocurrency insurable, they prefer to have those conversations directly with the client. Further, withdrawals and trading of cryptocurrency assets are able to be performed within one business day to an address of the clients choosing.

Assets that Blockvault supports safeguarding in their vaults include Bitcoin, Bitcoin Cash, Ether, XRP, Litecoin, as well as all ERC20 tokens. Coming soon, they will be supporting XLM. Blockvault also mentioned the potential for financial institutions to white label the Blockvault service and offer it to their own clients.

Overall Blockvault seems to be in a great position and has a long history and track record of safeguarding precious metals for its clients. Any company looking into their solution should inquire about the private key generation and storage methods employed and should also ask about their insurance policy.

Swiss Crypto Vault AG

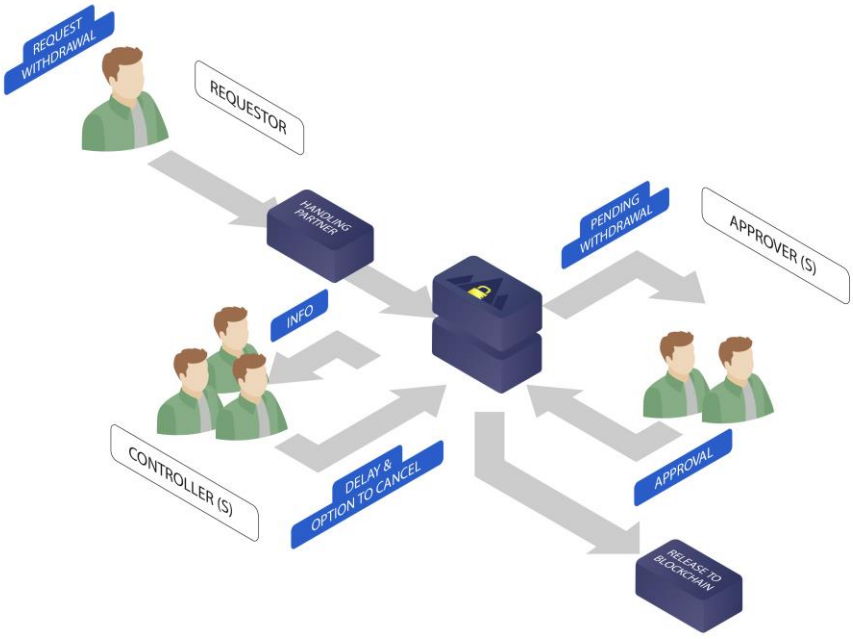
Swiss Crypto Vault AG (SCV) is branded as a hyper-secure crypto storage solution for institutional investors and high-net-worth individuals (HNWI) and is a joint venture between Bitcoin Suisse AG and Swiss Gold Safe AG. For this interview, we had the pleasure of speaking with Philipp Vonmoos, CEO of 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

If you are from the cryptocurrency space, you may have heard of Bitcoin Suisse, who is known for its cryptocurrency-related financial services and storage solutions for institutional and private clients. Established in 2013, Bitcoin Suisse has helped facilitate and raise nearly ₣1 billion for initial coin offerings (ICOs) or token generation events (TGEs) for some of the most well-known cryptocurrency projects. If you are from the precious metals space, you may have heard of Swiss Gold Safe AG, which is known for its precious metals and valuables storage services. Established in 2006, Swiss Gold Safe has helped secure precious metals and valuables for institutions and HNWI. SCV was formed under the laws of Switzerland in 2017 and is based in Zug. The partnership between the two organizations to form SCV was to combine their knowledge of cryptocurrency handling and physical security and storage.

Figure 9: Withdrawal Process of Swiss Crypto Vault.



Source: Swiss Crypto Vault AG.

Attack Vectors of Private Key Generation Without Hardware Security Modules

1) As Daenerys does not use a Hardware Security Module (HSM), there is a small window when the private key remains within the temporary memory of the computer that generates the private key. Being that the computer has no Internet access, it's impossible for hackers outside the facility to penetrate their system, but it might be possible for an insider, such as someone who has physical access to the device that generates the private keys, to compromise the device in some way. Considering how secure the facility must be to store the amount of precious metals Daenerys is safeguarding, executing this attack is highly unlikely.

2) Another attack vector could be during a withdrawal process, where internal personnel swap out a whitelisted client address for their own.

Implementing the key creation process on an HSM would ensure that the private key never has the ability to leave the device and whitelisted addresses could also be preconfigured on the HSM. Therefore, both attack vectors could be ameliorated if implemented.

SCV's solution provides clients with a deposit address that is associated with a **private key that was generated on an HSM so the private key never leaves the device.** The client is able to deposit their cryptocurrency assets as needed into the deposit address. The private keys are redundantly distributed, after being encrypted, ensuring that if one facility were to suffer a catastrophic event there is a backup to your private keys. The governance model is highly customizable by the client, allowing for multi-signature transactions and role designations of requester, controller, and approver. The requester, using the web portal, is able to initiate withdrawals. One or more controllers are able to cancel a withdrawal request and two or more approvers are able to approve a withdrawal request. An optional time delay may also be defined, and withdrawals are only allowed to be delivered to preapproved addresses. Another configuration the client is able to make is the selection of a handling partner. To prevent Swiss Crypto Vault from having complete authority over the withdrawal process in case their personnel or computer systems were to ever become compromised, **a handling partner is a company different from Swiss Crypto Vault, that provides the client with the additional benefit that the authorization of 2 separate organizations with different business operations, personnel, and computer infrastructure are required to authorize the client's withdrawal request.** Requiring 2

organizations to authorize a withdrawal request is in addition to the clients own configurable withdrawal approval process. Currently, the only handling partner is Bitcoin Suisse, with the promise that other handling partners will be available for clients to utilize in the future. This architecture is similar to a multi-signature transaction, in that more than one party is required to authorize a withdrawal. In other words, both Swiss Crypto Vault and the chosen handling partner (currently only Bitcoin Suisse) must both agree to authorize a withdrawal request otherwise a withdrawal request will be denied. This is a worthwhile safety feature which reduces the odds of both organizations being compromised when a client makes a withdrawal request.

"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 reviewed the storage solution, oversaw the private key generation, and will also compare the amount of stored crypto assets to the balances registered on the associated blockchain. Zuhlke Engineering reviewed the private key generation code. They **don't yet offer insurance**, but this is something that they said they are looking into. As for their clients, they are currently serving those from Europe, USA, Asia, and the Middle East. As for the typical client deposit amount, SCV makes sense for those starting around ₣500,000, up to triple digit millions. A SCV client does not require any physical hardware installed on their end, although they may co-sign a transaction with the private key of their own Trezor or Ledger hardware wallet under their control. They may also leverage multi-factor authentication for accessing the web portal. Many types of cryptocurrencies are supported as of today, such as Bitcoin, Bitcoin Cash, Bitcoin Gold, Ether, Litecoin, and all ERC20 and ERC223 tokens. Others will be added on an ongoing basis.

Swiss Crypto Vault appears to be a highly redundant, highly secure, well thought-out implementation and process that is also easy to use and configure by the client. SCV is backed by a track record of experience and expertise in both cryptocurrency and precious metals. The solution is suitable for both institutions and HNWIs, and definitely a crypto custody solution worth investigating.

HSMs Matter and Outlook

In this article, we covered a few options for crypto custody solutions. Two solutions ensure that a private key never leaves an HSM, two others generate the private key in temporary storage where it remains for a brief moment. The final solution desired to maintain confidentiality and secrecy of their private key generation process. For those where the private key is not generated on a HSM, an insurance policy could make up for any potential vulnerabilities assuming the policy covers theft and is bullet-proof. As for technological innovation, speed, ease of use, customization of governance, physical security, and digital security, the most well-rounded solutions appear to be Swiss Crypto Vault AG and Crypto Storage AG. Of those two, Swiss Crypto

Source: Scott Adams, Dilbert

Vault AG has the longest track record and most experience. Crypto Storage AG appears to be the most innovative solution. If your organization requires insured options, Daenerys & Co. and Blockvault may be right for your organization. Both are capable and in positions for the physical storage of large sums of cryptocurrency. These evaluations are not meant to be recommendations of one company over the other, as they each have their own use case. We should stress the importance of doing your own due diligence when investigating the solution that is right for your organization.

If you have any questions or comments, are looking for a solution for your organization, or if you have your own solution that you are interested in sharing, please head over to this website for participating in a brief survey and be entered for a chance to win a Ledger Nano S sent directly from the manufacturer. Joseph can also be reached at joseph (at) cryptocustodysolutions.io.

A Bitcoin Standard? Saifedean Ammous Musing with the *Crypto Research Report*

"Sound money is money that gains in value slightly over time, meaning that holding onto it is likely to offer an increase in purchasing power"

Saifedean Ammous

Key Takeaways

- **One reason gold has been used as a store of value and medium of account is because of its low annual supply growth. The optimal money would have zero supply growth.**
- **In a free market for money, money would appreciate in value every year. Therefore, banks would no longer pay interest on deposits. Instead, depositors would choose between a deposit contract, a mutuum contract, or a private equity investment.**
- **A debt-based monetary system must be inflationary because interest payments must be made. As investors gradually purchase cryptocurrencies and pay off debt in the fiat system, the fiat money supply will contract over time.**

Source: Saifedean Ammous

We want to Thank Saifedean Ammous for having an exclusive conference call with Demelza Hays and Mark Valek from Incrementum. Saifedean Ammous is a Professor of Economics at the American University in Lebanon, and he is the author of the bestseller *The Bitcoin Standard*.

Bitcoin's Stock-to-Flow Ratio catching up to Gold's

A starting point for Saif's analysis of different monies is the **stock-to-flow ratio.** Readers of our sister report – the *"In Gold we Trust"* Report are well aware of this concept, as we have discussed it at length. Most people fail to understand why gold has been used as a store of value for thousands of years. It is true that Gold is scarce. However, it is definitely not the scarcest metal at all. Rather its above-ground quantity has the most constant quantity of any rare commodity available. The quantity of a good can be expressed in the stock-to-flow ratio. A high stock-to-flow ratio means its quantity is not inflated very much. An ideal unit of account for measuring value obviously needs low fluctuation of the 'yard stick'. The master of the British Mint and inventor of the gold standard, Sir Isaac Newton, said,

"Gentlemen, in applied mathematics, you must describe your unit."

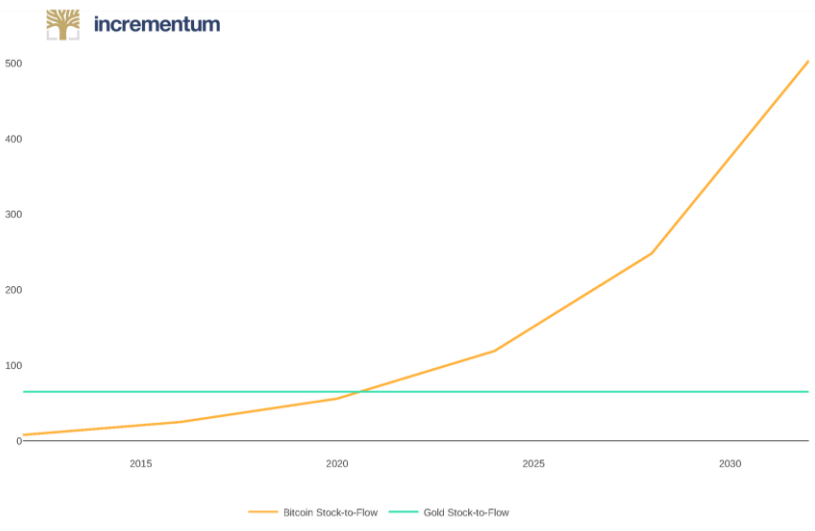
"For Mises, gold's industrial role is an impediment to performing its monetary role, but an impediment with which he is happy to contend compared to the alternative of money whose supply is controlled by governments."

Saifedean Ammous

Even though gold has a very high stock-to-flow ratio, Bitcoin will soon have a higher one. Its capped supply is one reason Saifedean Ammous claims that Bitcoin is even better than gold.

In the figure below, Bitcoin has a stock-to-flow ratio of around 71 currently, but by 2020, because of the halving, the ratio will be going up to 119.

Figure 10: Bitcoin versus Gold Stock to Flow



Source: Incrementum

Taming Bitcoin's Volatility?

In *The Journal of Structured Finance,* Saif wrote a paper, "Can Bitcoin's Volatility Be Tamed", about how the price of gold is affected by the demand from the jewellery market and industry. When people sell gold excessively, the price of gold drops. However, demand from jewelry makers and industrial fabricators absorbs the price drop, which creates a lower bound for the price of gold and has a moderating effect on the volatility of gold's price.

In Paul Krugman's article on why he is a crypto skeptic, he explained that Bitcoin is not "tethered" to the real world like gold.[42] **Since there is no real-world market that has demand for Bitcoin, the price of Bitcoin has no lower bound, and therefore, Bitcoin can never ascend to the role of money.** However, Saif answers Krugman's critique with a quote from *Theory of Money and Credit* by Ludwig von Mises,

> *"The significance of adherence to a metallic-money system lies in the freedom of the value of money from State influence that such a system guarantees. Beyond doubt, considerable disadvantages are involved in the fact that not only fluctuations in the ratio of the supply of money and the demand for it, but also fluctuations in the conditions of production of the metal and variations in the industrial demand for it, exert an influence on the determination of the value of money."*[43]

"A However, loose monetary practices and overly bureaucratic regulation of the financial industry have caused people to look for alternatives. A traditional one for savers is gold, but it is unsuitable for payments. Now, many see an opportunity for cryptocurrencies to meet this need.

Princess Gisela von und zu Liechtenstein

As Saif explains, fluctuations in the demand from industry cause gold's value to fluctuate and prevent it from being a purely monetary asset that reflects monetary demand only. He says that gold is not money because of its industrial activity. Industrial activity is secondary in the determination of the value of gold. For Mises, a money that has only a monetary demand will be a superior form of money because **the value of money will be based purely on time preference**. According to Saif, in a situation where Bitcoin becomes the only money in the world, hypothetically speaking, then the demand for Bitcoin is just the demand for cash balances. **In other words, Bitcoin demand is a reflection of time preferences.**

Mark Valek, author of *The Crypto Research Report* and fund manager at Incrementum, compares Saif's idea with the "reservation demand with gold". **The volatility of gold, due to this reservation demand, will probably always be lower than Bitcoin as long as Bitcoin is only a store of value and only potentially has monetary demand.** However, in the future, if hypothetically a majority of people adopt Bitcoin as unit of account, the volatility would be lower than gold because Bitcoin would be the denominator of goods and services. In fact,

—

[42] See "Transaction Costs and Tethers: Why I'm a Crypto Skeptic," Paul Krugman, *The New York Times*, July 31, 2018.
[43] See "The Theory of Money and Credit", Ludwig von Mises

if one starts using Bitcoin to measure goods and services the volatility would go to zero, like during a gold standard.

Saif explains, "That is the idea of the stock-to-flow because, with gold, and especially silver, yearly mining production does not significantly impact total above ground supply compared to other metals. **You want your money to be purely your money.**"

Mark compares the predetermined stock-to-flow ratio of Bitcoin with other rule-based monetary policies, such as Milton Friedman's automated *k-percent rule*[44] and John Taylor's *Taylor Rule*, that attempt to stabilize the purchasing power of money over time. On the other hand, these attempts do not achieve long-term sustainability because of political tension explained by Gordon Tullock and the Public Choice literature on economics.

However, Saif does not believe that the k-percent rule and Bitcoin's algorithm are equivalent. **"The key thing for me is that the value of money should be determined by the market for money, which is the supply and demand for cash balances."** The supply and demand for money are what determines the price and the interest rate for money. It is very different from the rule-based monetary policies **because they want to calculate the right price, and then they want the market to adjust.**

"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

While discussing the topic of Bitcoin with Larry White, he argued that gold has an advantage over Bitcoin because its supply is elastic in the long run. Gold supply increases by 1–2 % every year and inflation compounds. Within a 40 to 50 years, the supply of gold will double. However, Saif couldn't disagree more. According to him, **what makes gold a good money is the fact that it has the least supply growth.** Larry White is a supporter of fractional reserve banking on top of a gold system because he holds that a fully backed gold standard would have a shortage of money. Therefore, for Larry White, the reason gold became an international money is because of the small 1–2 % in inflation every year. In contrast, Saif says, "Gold wins out because the **demand for money is always a demand for a money that can be inflated the least**. The demand for money is always growing and the value of non-inflationary money always grows in the long run. If we follow Larry's argument, then we have to ask why did silver or copper not become money instead of gold since they have supplies which are more elastic to demand?"

—

44 See *A Monetary History of the United States, 1867–1960.*

Can a Deflationary Monetary System Work?

Mark Valek gets right to the point and asks, "Does the monetary system need inflation at all?" Some gold proponents would argue that the monetary system needs some monetary inflation to keep up with population growth. Saif claims the following: "From a mathematical point as well as from the perspective of a Bitcoin maximalist, I think the argument against inflation is quite strong as outlined by Philipp Bagus' book on deflation[45]: **the hardest form of money is one with constant money supply and zero elasticity.**"

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

Philipp Bagus

Demelza Hays, author of *The Crypto Research Report* and fund manager at Incrementum, mentioned her 2017 Forbes article based on the work of Professor Dr. Antal Fekete. She posited the question to Saif, "For me, it looks like we want to have a currency with a high stock-to-flow ratio, but if we take to the logical conclusion, **why do we need money that has any flow at all?**"

"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."

Saifedean Ammous

The Current Monetary System is Debt-Based

*"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

Mark Valek holds that central banks follow inflationary monetary policies and governments support inflation when the monetary system is debt-based. "If we have debt as the basis of our money, that requires an ever-increasing money supply. Otherwise, I don't know **where the interest for the debt should come from**. Do you agree with that?"

"Yes, I definitely agree on that," answers Saif. "I go even farther than most Austrian economists. **In a free market for banking, depositors would not earn any interest on their deposits because the money would be appreciating in value, which is the real return.** Essentially, lending money to the bank enables depositors to save on the cost of securely storage money. **The second kind of money would be the direct equity and that is the model of Islamic banking**, which is also the model of traditional banking. If you are going in on an investment, I think what it comes down to is what society accepts to be legitimate. If a society accepts that it is ok for the government to impound the

—

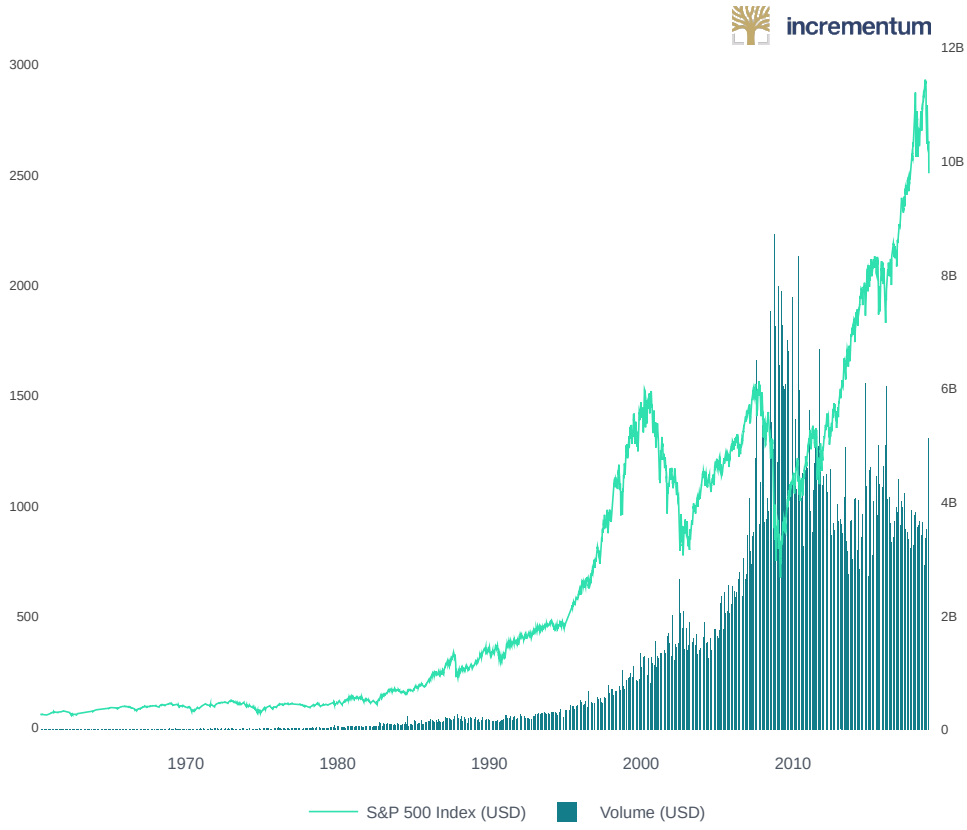
45 Bagus, P. (2015). *In Defense of Deflation.* Springer.

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

Princess Gisela von und zu Liechtenstein

property of the borrower if they can't pay back, then effectively you are monetizing the property of the borrower, which is the collateral. Thus, you are effectively monetizing the collateral. Interest lending carries collateral that can be impounded and repossessed by the bank. Effectively, it makes the certain asset monetized because you have issued a loan backed by that asset which is not money, it is a house or car or a piece of land. That kind of business model is only accepted in places when it is fine for the government to impound that property when the borrower defaults. On the other hand, if the borrower's collateral cannot be impounded, then lenders often reject these kinds of deals and banks do not engage in them.

Figure 11: Are US Equities indicating the next Recession?



Source: Yahoo Finance, Incrementum.

In a world where banks can only lend deposits or invest in direct equity and they cannot repossess collateral, then the bank cannot make guarantees obviously, because there is always a risk in business. Since the bank cannot create money from fractional reserves and must first bring in money deposits from clients, they cannot guarantee the solvency of their depositor accounts. So, the depositors are accepting unlimited downside of complete default of the bank, and the bank is asking them to accept limited upside. **So, the notion of interest without risk of default is untenable in that kind of world**. Nobody would put their money with someone who tells you,

"If we lose, you lose all your money and if we win you only get 3 %. *Consequently, everybody would go into equity investments. Either you put money into a bank as a deposit available for maturity in which case you pay the bank a fee for the storage and for making the money available for you. Or if you have money that you are willing to sit on, you invest it as equity in some other business and it is the job of the bank to match maturities between the borrowers and the lenders."*

Saifedean Ammous

"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

Although, Mark Valek does not agree with Saif 100 %, he thinks that in addition to full deposits and equity investments there will also be demand for debt instruments or deposits. "I think also in a zero-inflation monetary system there would definitely be demand for investments not only in equity but also in debt. A differentiated capital structure of a company enables different payout characteristics for investors. Low returns on bonds or also lending accounts at banks, enable the investor to receive predictable cash flows with higher seniority in case of bankruptcy. It's important to note that these would not be riskless investments."

However, in this monetary system, investors would not necessarily need to risk their Bitcoin in a security investment, such as stocks or bonds, but they would still experience an appreciation of the currency in form of a real increase in the purchasing power of money. If investors do lend out Bitcoin to a bank or financial intermediary who pools the risk of their borrowers, then the bank should pay a fee to the depositor for accepting counterparty risk." So, there may be a case for such a thing as a low-risk interest rate investment but probably the tendency would be much lower to take this kind of risk. This is just a minor disagreement," Mark adds.

Table 2: Bank Account Options Under a Global Bitcoin Standard.

Bank Account Options for Depositors	Saifedean Ammous	Mark Valek
Full reserves available on demand – depositor pays bank/depositor for storage and optionally insures deposit. Investor earns from appreciation of currency over time.	✓	✓
Depositors invest directly in equity. Investor earns positive or negative return and owns equity shares.	✓	✓
Depositors deposit money in bank in a certificate deposit or bond. Bank pools borrower risk and lends matched maturity loans. Bank pays yield to depositor.	✗	✓

Source: Saifedean Ammous Interview, Incrementum AG.

Mark responded to the full reserve argument with the common critique posited by mainstream economists, **"Will a deflationary monetary system hamper growth like the Keynesians claim?"** Mark holds that a debt-based monetary system needs inflation in order to stimulate research, development, expansion, and intervention. However, under the classical gold standard, capital markets still existed. Even though there was some kind of gold flow or inflation, the productivity was higher than the inflation rate of gold.

"Yes absolutely," Saif believes. "In order to create interest in a debt-based system, the bank monetizes the collateral, and in order to run fractional reserve banking, it allows a central bank to create money and **a fractional reserve system would be unstable without a central bank.** The central bank can become more inflationary by manipulating interest rates downwards, which enables the government to borrow and spend more. There are different layers of inflation, and the key is to create parts of the economy that are dependent on this credit money. They end up with all these industries and all these people employed because of that money; they are politically connected, and they need to keep that money going. This is a bug, not a feature, you would want to get rid of that, you would want to make it that there is no money creation going on so that investments have to come from real saving. In this case, you would have an actual functioning capital market. Maturity matched."

Saif on Investing in Bitcoin

Question: What do you think about smart contracts and utility tokens that can facilitate decentralized capital markets?

Answer: Bitcoin is all we get, we have to learn to accept it.

Question: If you were to create a cryptocurrency fund, would you allocate 100 % of the portfolio to Bitcoin?

Answer: I would not create a cryptocurrency fund, because the only cryptocurrency investment you need is to just hold the Bitcoin.

Question: What are your thoughts on how to make an initial investment in Bitcoin? Would you buy with cost-averaging over time or would you put your entire investment in the market at once?

Answer: Bitcoin is a highly risky asset. I would not advise putting a lot of money into it. I always have to keep telling people, this could still blow up. It has only been around for 10 years. Bitcoin might not work, or it might go through a bear market for another 10 to 20 years. Even in the best-case scenario, Bitcoin will be highly volatile, and it is going to have some massive drops. Among cryptocurrencies, I think that Bitcoin is the only one that might stay as a long-term hedge against monetary inflation.

A Free Market for Money

Transitioning to the future outlook for the money market, Demelza asked, "If all the central banks around the world respond to Bitcoin by decreasing the flow of their currencies and making their currencies harder, **do you think that Bitcoin and central bank-issued fiat currencies will compete alongside each other** like Uber and taxies or Airbnb and hotels? Or do you think one is going to completely substitute the other?"

Saif's answer: "For the first time, people have an alternative; they can opt out of central banking. This was not possible before Bitcoin, but it is possible now. Bitcoin will limit the ability all these government from inflating. You can imagine Bitcoin developing a so-called **monetary Batman that is hanging in the shadows of every central bank and is waiting for that central bank to begin inflating the money supply, and then people in that country would jump into Bitcoin.** When they jump to Bitcoin, its value will significantly appreciate.

Saif thinks it is good to think of Bitcoin as a small side bank account that you have for a rainy day. He said, "The important thing is that you may be stuck in a country one day where you got robbed, you don't have access to your bank account, and you do not have money. If you have Bitcoin, you can get out of

trouble by buying an airline ticket with it. **I think it is important to understand the value proposition.**"

Mark echoed Saif. "We are very much on the same page because, even though we are optimistic, I think that from a portfolio point of view **investors do not have to allocate a huge amount to have an impact.** Investors can allocate a low-digit percentage, **even as low as 1 percent of their entire net wealth, and it will have a huge impact if Bitcoin monetizes**. Mark explains that Bitcoin is a binary investment. Either Bitcoin becomes some kind of monetary asset and store of value, or Bitcoin will be succeeded by something else and the price will go to zero.

Bitcoin: Two Paths to Monetization

If we muse about the future, how will the transition from being a store of value to a unit of account look for Bitcoin? Mark Valek considers two scenarios:

- **Positive scenario:** Bitcoin becomes a reserve asset for central banks. A domino effect could prompt more nations to buy Bitcoin to protect against speculative attacks and to ensure that public debt can be paid off with investments in Bitcoin. The Marshallian Islands already have investment in Bitcoin, and the Central Bank of Barbados wrote a paper on the topic in 2015.
- **Negative scenario.** Loss of confidence in the fiat system, and there will be a huge rush into the new safe haven being 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

On the other hand, Saif sees a scenario in which Bitcoin ascends into monetary supremacy by each person slowly transitioning to Bitcoin. "Just a monetary upgrade. Install healthy software on a crappy windows PC, and it starts functioning better. **The monetary system that we have creates money when debt is created**. The flipside of that is that it destroys money when debt is paid off. We have had this sort of system for the past 40 to 50 years, and now we have another alternative, and everybody will jump into this new system (Bitcoin). Eventually, people can use Bitcoin to pay off their fiat debt. If we just keep paying off our debt, an orderly unwinding of the global monetary fiat system will ensue. Basically, **everyone pays off all of their debt and the money supply contracts until it drops to zero**, and then a new monetary system that is functional takes over the world. It might be slow or quick, but it doesn't have to be messy and ugly."

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

Institutional Requirements for an Investible Crypto Index

"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

- Indices that act as benchmarks must be investable and replicable.
- In order for institutional investors to be able to invest, crypto currencies must be able to be held in custody by professional custodians.
- The LY Incrementum Krypto Index takes into account the requirements of institutional clients with regard to investability and replicability.

Authored by LIMEYARD

LIMEYARD is a Swiss index provider with offices in Zurich, New York, and Vienna. LIMEYARD focuses on both proprietary and nonproprietary indices and combines cutting-edge index innovation with a state-of-the-art cloud-based technology. Its fast-growing family of global equity and cryptographic assets indices is rules-based, compliant, traditional, and provides smart-beta investable solutions for institutions on the sell side and on the buy side. LIMEYARD entered into a joint venture with Wiener Börse AG in February 2018.

Creating a Benchmark for a Premature Market

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

Ben Bernanke,
14th chairman of the Federal Reserve

The complex cryptoasset market environment inspired a joint innovation between LIMEYARD and Decentriq, two Swiss-based companies. They combined their expertise to develop a comprehensive cryptoasset index aimed at capturing the dynamics of the overall cryptographic assets market whilst dealing with unique regulatory and economic challenges embedded in this premature market. For investors, an index must be tradable, meaning that liquidity and rebalancing are feasible. Furthermore, the cryptographic assets market presents specific challenges regarding regulatory requirements, such as the **exclusion of investments in privacy coins or coins that are only traded on one exchange.**

- **Active asset managers typically use a benchmark to measure the performance of their portfolio in relative terms.** They assess market efficiency and price systemic risks using benchmarks. Prior to setting up a fund strategy, asset managers apply various risk models and compare the past performance of the strategy against the underlying benchmark, long-term outperformance being their aspired goal. The benchmark itself is performance-agnostic.
- **Passive asset managers (e. g., ETF providers), on the other hand, invest into a portfolio which tracks an index.** Their underlying question is: what new strategy, theme, region, sector, etc. could be a great investment opportunity for investors? The ETF provider simply tracks a factor/risk model-based index, e. g., a low volatility index, a momentum index, a quality index, etc.

For active and passive managers, "tracking the market" has the same meaning; however, for the latter, the index concept reflects an investment strategy. In other words, active managers use the benchmark to track the market as a whole, and is **therefore performance-agnostic**, as long as the performance is in line with the overall performance of the market. On the other hand, for passive investors **the index represents an investment strategy** with the clear ambition to achieve long-term positive performance. **In both cases, the index is rules-based, meaning it's not subject to discretionary decisions.**

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**.

- **Reflecting market dynamics:** This requires compliance with data sufficiency, as data are the main ingredient of every benchmark. Insufficient availability of data bears the risk of not adequately representing a market.
- **Maintaining/government rules:** To be fully rules-based and transparent, the methodology of an index has to be applicable under all market circumstances avoiding the necessity for a discretionary interference.

- **Manipulation prevention:** Internal operational processes have to be designed to prevent index manipulation (last experienced with the LIBOR scandal in 2011). IOSCO, the international body of the world's security regulators, defined the IOSCO Principles for Financial Benchmarks, consisting of 19 principles for index providers to adhere to, all of which are implemented in LIMEYARD's governance structure and audited on an annual basis.

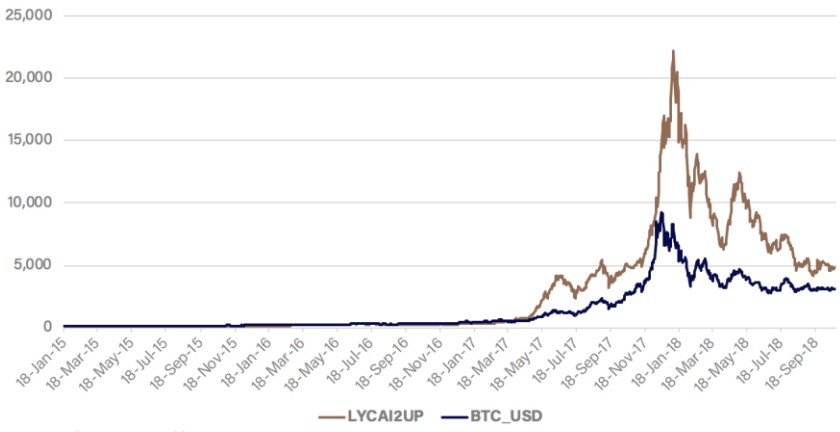
The Creation of the LIMEYARD Cryptoasset Index (LYCAI)

"There are three eras of currency: commodity based, politically based, and now, math based."

Chris Dixon

LIMEYARD and Decentriq faced two main challenges when creating a comprehensive cryptographic market index: How to handle (1) a highly dynamic market with numerous, partly unknown factors influencing its overall development and (2) practical requirements of a benchmark that make the index rules-based, transparent, and compliant. The result of this challenging endeavour is the **LIMEYARD Crypto Assets index (LYCAI), consisting of the largest 20 cryptoassets that are publicly tradable.**

Figure 12: Index Performance LYCAI vs. Bitcoin.



Source: LIMEYARD.

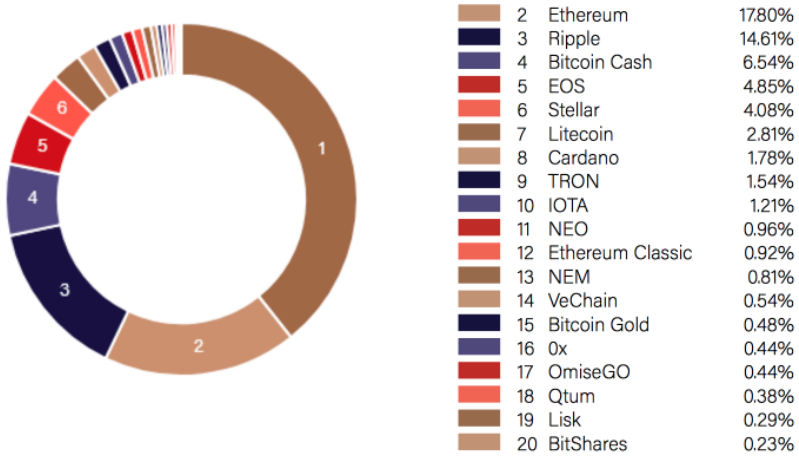
To be part of the LYCAI, an asset has to fulfil several parameters to ensure sufficient robustness, liquidity, and tradability. **The index is calculated in real-time 24/7, using trading data from eight different exchanges**. The aggregation over several trusted exchanges improves robustness against exchange-level failures and price manipulations, providing an adequate representation of the underlying market. The selected exchanges have, among other things, a comparably high monthly liquidity. LIMEYARD is only considering assets that are traded on at least two trusted exchanges. This ensures that, if one exchange experiences any technical issue, the index can continue to pull price data on the full predefined set of assets. The price data aggregation algorithm factors in both volumes and outliers, reducing undesired spikes in the index level which could happen in a young and fragmented market. Additionally, only the assets that are in the top 60 % in terms of trading volume are eligible for inclusion in the index.

"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

The index considers only those assets whose protocols are not designed to enable anonymity, avoiding the risk of being associated with illegal transactions and maintain a certain degree of transparency for taxation purposes. With this criterion, LIMEYARD and Decentriq anticipated concerns by regulators and aimed to limit the infringement of KYC/AML standards when using the LYCAI as an underlying for financial instruments. To provide diversification and compensate the high skewness of the market through Bitcoin, the index smoothes each constituent's market capitalisation by an exponential moving average over the month prior to the relevant review date. The weights are then derived from a sigmoid function which penalises high values without imposing a hard cap.
As a result of the weighting methodology, an allocation of large assets is well-balanced compared to other indices. For instance, Bitcoin and Ethereum's weight as of the end of October 2018 corresponds respectively to 39.30 % and 17.80 % compared to more than 60 % and 13 % for the Crypto Market Index 10 and 30 % (cap) and 23.46 % for the Bloomberg Galaxy Crypto Index.

Figure 13: LYCAI Asset Allocation November 2018.



Source: LIMEYARD.

The LYCAI index is the true benchmark for measuring fund performance by cryptographic asset managers. The index meets all IOSCO requirements and the regulators' current concerns that they have explicitly stated regarding cryptoassets.

Incrementum Investible Cryptoasset Index

Different clients have different requirements. For this reason, we tailored the LY Incrementum index to Incrementum's requirements.
The LIMEYARD Crypto Asset Index is the basis concept for the LY Incrementum Index, with the following deviations:

- Coins in the index must be able to be stored in cold storage using hardware in order to be insured by Swiss insurance companies.
- Coins must have market capitalisation of more than $500 million.
- The number of assets is fixed at ten in order to reduce rebalancing transaction costs.

Figure 14: Index Performance LYCAI vs. Incrementum Index

Source: LIMEYARD.

This slightly revised index concept proves to be very solid resulting in a one-year return of 16.10 % compared to LYCAI's 0.58 % one-year return. The one-year annualised volatility is 96.49 % compared to LYCAI's 97.06 %. The one-year volatility is, of course, mainly driven by Bitcoin, the largest asset in both indices. The lower number of assets in the LY Incrementum Index makes the index more tradable compared to the 20 assets in the LYCAI, which is designed to primarily represent the overall crypto market.

Final Remarks

"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

The Bitcoin market is entering a more mature state. Relevant markets are regulated (e. g., CBOE) with rules designed to prevent potential manipulation. There is a steady growth of Bitcoin futures traded on the CME platform to currently more than $162 million average daily volume (ADV). Various leading investment banks and traditional exchanges run internal projects to further evolve the maturity not only of Bitcoin, but also of other large cap digital assets. Many projects have already been announced, others are expected to be announced very soon. That's why LIMEYARD continues to invest into strategic partnerships and the development of a broader crypto index family, also covering investment strategies for the passive asset management segment, derived from its leading LIMEYARD Crypto Asset Index methodology.

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 tokens enable companies to raise equity using blockchain technology without locking up investors.**
- **Issuers of securities tokens are seeking to access the large pool of institutional money that has not yet penetrated the crypto currency market. Institutional investors expect KYC/AML, data protection and see a hurdle in one of the core elements of the blockchain, namely its immutability.**
- **In 2019 there will be a race between stock exchanges, which can offer the first regulated market for securities tokens.**

"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

The Austrian Financial Market Authority **approved the first financial prospectus for a fully regulated tokenized security in the European Union in late November.** The Financial Market Authority in Liechtenstein already approved Liechtenstein's first security token in August. Mt. Pelerin, Tokenestate, and Securosys are also purportedly offering security tokens in Switzerland. This means that a cryptocurrency can represent legal ownership in a company or can represent other securities, such as certificates and bonds, if they also register as a security. Unfortunately, there are no cryptocurrency exchanges that are licensed to trade security tokens. However, equity tokens are not for the standard cryptocurrency investor. **Instead, equity tokens are trying to access the large pool of institutional money that has not entered the cryptocurrency market yet.**

Institutional Money-Steering Innovation

The public blockchain technology reduces the cost of raising capital, and this matters for small firms. One of the main benefits of trading digital assets on the public blockchain infrastructure is that **anyone can issue a digital asset, and anyone can invest in a digital asset.** This saves immense amounts of time and money for issuers who no longer need licenses, underwriters, or lawyers. The large cost of listing a company on a stock exchange erects barriers to entry for small and medium-sized enterprises (SMEs). The blockchain also removes the barriers to entry posed by **regulations that limit investment possibilities for retail investors** like grandma.

"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

In addition to enabling financial inclusion in the market, the public blockchain technology allows investors to **trade "shares" of companies for much lower fees with instant settlement times.** This means significant savings for retail investors and smaller profits for stock brokers.

However, some investors, especially institutional investors, want features of the traditional capital market to be incorporated into the token market. **Enter "Security Token".** Over the past few months, the term "Security Token Offering" (STO) has been growing in importance compared to initial coin offerings. There are three main problems institutional investors have with the Wild West of blockchain:

- Not all cryptocurrencies follow the laws such as know-your-customer, anti-money laundering, sanctions, etc.
- Large investors want privacy. They do not want transparent blockchains that allow outsiders to see their transaction amounts and destinations.
- Immutability. Public blockchain cryptocurrencies are impossible to retrieve if a private key is hacked or lost. Large investors will not want their shares of Visa stock being controlled by a private key. Instead, cancel and reissue features will be required before the security token market can gain adoption.

In order to manage these concerns, several companies are working on private blockchains that will allow equity tokens to be stored and traded. The Swiss stock market's Swiss Digital Exchange (SDX) near Sihlcity is working on a pilot project that wants to tokenize four main groups of assets.

- First, native tokens for SMEs that only exist on SDX will be issued, stored, and traded.
- Second, tokenize existing securities on the SIX Swiss Exchange.
- Third, tokenize non-bankable assets.
- Fourth, tokenize cryptocurrencies, such as Bitcoin and 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

In addition to SDX, Daura, a partnership between MME and Swisscom, is also working on a private blockchain. Blockchains specifically designed for trading securities will have KYC/AML integration, privacy, and cancel and reissue features that allow the stock exchange owner or broker to reissue shares to companies that lost their private keys or were hacked. Blockstream's LIQUID and Polymath are also both examples of blockchains targeting the security market. However, important legal issues, such as whether or not tokenizing a fund violates fund distribution rights, still need to be answered.

Figure 15: Public Security Token Platforms Performance.

Source: Incrementum

Define Token and Security

A token is a digital representation of value on a particular distributed ledger. Tokens can represent voting rights, ownership shares, bonds, and much more. ERC 20 smart contracts on the Ethereum Blockchain and NEP5 smart contracts on the NEO blockchain are currently being used to pay out company dividends and vote on managerial decisions. On the other hand, the definition of a security differs from jurisdiction to jurisdiction. In the US, a financial product is legally classified as a security if the four following criteria are met:

- Investment of value
- With an expectation of profit
- In a common enterprise
- With the profit to be generated by a third party

As mentioned in the next chapter, these criteria came from the 1946 Supreme Court case between a Florida citrus grower named Howey and the Securities Exchange Commission. In response, US cryptocurrency issuers are applying for Reg D. and Reg S. exemptions from security law. They are also exploring how Airdrops can circumvent security law.

"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

However, Europe does not have any concept of the Howey test. This is because the US has common law where court cases set precedents for future judgements. In contrast, mainland Europe has civil law, which is a principle-based approach to law. According to Article 2 let. b FMIA in Switzerland, a security is defined as, "standardized certificated and uncertificated securities, derivatives and intermediated securities, which are suitable for mass trading." **Subsequently, FINMA has already reported that many cryptocurrencies are securities.**[46]

Should I Tokenize or Securitize or Both?

Tokenization of assets existed before cryptocurrencies were created. They are called certificates. However, certificates cost money to set up and maintain. Unlike issuing an ERC token on Ethereum, certificate issuers must have a business structure that can legally issue structured products, and often certificates are limited to qualified investors. According to the Swiss Collective Investment Schemes Act (CISA) of 2006, a qualified investor is one of the following[47]:

- Supervised financial intermediaries (such as banks, securities dealers and investment fund managers)
- Supervised insurance companies
- Public law institutions and pension funds with professional investment operations
- Business enterprises with professional investment operations
- **Wealthy private persons (German: *vermögende Privatpersonen*) with CHF 2 million worth of financial assets, and direct real estate investments do not count!**

—

[46] See *Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings*, FINMA, February 16, 2018.
[47] See "Qualified Investors," Swiss Fund Data AG, 2018.

- Investors who have a written asset management agreement with a supervised bank, securities dealer or investment fund manager

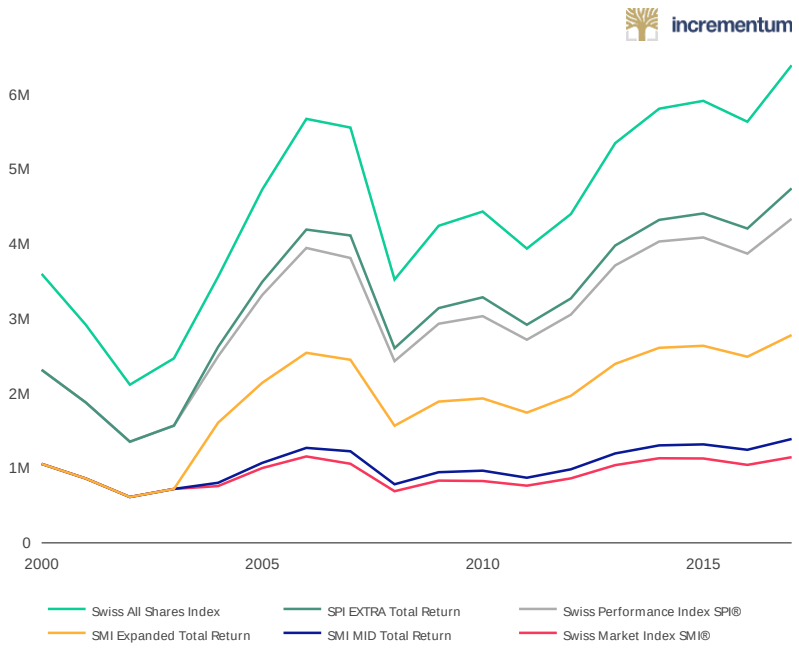
One type of structured product is a certificate. **A certificate can be a tracker certificate that tracks the value of an asset, or a certificate can be actively managed.** The asset could be an IBM share or a cryptocurrency index, or a physical plane, for example. Bank Vontobel, for example, creates many certificates. A certificate is similar to a bond because it represents a predetermined payoff promise that the issuer gives to the investor. This means that the investors can read in the terms of conditions what they will get from the certificate when the certificate expires. For example, the promise could be that "In two years you get the performance of IBM shares." However, certificates can be actively managed as well. Actively managed certificates (AMCs) can contain any type of cryptocurrency, including privacy coins, pre-ICO coins, and ICO coins. Investment managers can also employ riskier strategies than UCITS or AIF can such as shorting and taking leverage.

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

Tim Draper

Certificates are like tokens in the sense that they can be used to securitize anything. The only difference is that certificates contain normal investor protections and they can be easily purchased through security brokers. Since they adhere to existing regulations, they have certain costs. Therefore, securitization of an asset using a certificate only begins to make sense for assets worth over ₣ 10,000. Unlike UCITS and AIF regulated cryptocurrency funds, such as Incrementum's, structured products are exempt from the collective investment scheme regulations.

Figure 16: SIX Assets Growth in Millions of Swiss Francs.



Source: SIX, Incrementum

Advantages and Disadvantages of Certificates vs. Funds for Cryptocurrency Asset Managers

Advantages

- **First.** Unlike Alternative Investment Funds, Guernsey special purpose vehicles do not need to have external custodians that have a bank license. Therefore, investment managers can outsource cryptocurrency storage to third party custodians like the companies mentioned in "**Crypto Concepts: Custody**" in the December 2018 edition of *The Crypto Research Report*.
- **Second.** Lower fees. Since managers of Actively Managed Certificates can execute trades with the counterparties of their choosing and outsource cryptocurrency custodianship, fees can be less than with UCITS or AIF cryptocurrency vehicles that need to work with banks and administrators.
- **Third.** Time. **SPVs take 10 business days to setup and certificates take 3 business days.**

Disadvantages

- **First.** Cryptocurrency securities are not always invested in the underlying cryptocurrency. They can just be trackers. Investors should verify if the security is actually invested in the underlying.
- **Second.** Unless the cryptocurrency security uses a licensed bank or third-party custodian that offers insurance, most cryptocurrency holdings are uninsured. Unlike alterative investment funds that have liable custodians, structured products and managed accounts can have a range of options from completely uninsured to fully insured.
- **Third.** Swiss Certificates are not always passportable to the European Union.

GenTwo Digital, a joint venture of GenTwo AG and Inacta, is a Swiss consultancy firm based in Zug. GenTwo Digital was founded by Patrick Loepfe, a previous Vontobel Deritrade specialist, and the Vice President of the Board or/and Managing Partner of Forstmann, Philippe A. Naegeli. In an exclusive interview with Patrick Loepfe from GenTwo, we discussed the innerworkings of how securitizing a cryptocurrency works. The company helps financial intermediaries, high net worth individuals, and family offices turn bankable assets, such as actively managed accounts and structured products, and non-bankable assets, such as art and cryptocurrencies, into tradable certificates with Swiss International Securities Identification Number (ISIN) numbers. An ISIN number is code that uniquely identifies a specific securities issue. In Switzerland, obtaining an ISIN code for a security requires a prospectus, term sheet, and offering memorandum. In traditional finance, ISINs are used for stocks, bonds, funds, hedge funds, mutual funds, and other securities, whether for a private offering or going public with an IPO (initial public offering).

What GenTwo does is build a financial company for each investment manager, and then the investment managers can issue multiple certificates within the company. GenTwo's issuing structure is a unique dedicated issuance vehicle in Guernsey. Once GenTwo sets up the special purpose vehicle company, investment managers can build structured products as they wish. The advantage of setting up a dedicated issuance vehicle is that issuers can have balance sheet control where liabilities are stored off the balance sheet. Normally, issuers risk balance sheet risk from holding assets on the active side and liabilities that can be impacted from operational issues. Instead, an SPV structure leaves only the assets on the active side of the balance sheet and the certificates on the passive side. **Since the certificate tracks the value of the assets that are held on the active side, there is almost no risk of a default.** For example, Bank Vontobel has an SPV in Dubai from which they issue their certificates. Julias Bär has a SPV in Guernsey, EFG has a SPV in Guernsey.

"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*

Certificates are not really competitors for tokens. Tokens can be issued by retail investors and anyone in the world can invest in them. At Incrementum, we suspect that one will not completely replace the other for the time being. Instead, some market participants will choose to invest in the regulated world and other market participants will choose to invest in the unregulated world. Many companies will raise capital in both markets. As Oliver Völkel said during the Crypto Christmas Market Outlook, the main problem with equity tokens is that a licensed exchanged where investors can trade these assets does not exist. **2019 will be a race for the first legal platform that can trade cryptocurrencies that represent securities.**

Vontobel

Investment Banking

Driven by the power of possibility

vontobel.com

Legal Challenges for Blockchain-Based Capital Markets

"Blockchain technology can achieve what governments wanted to achieve for a long time: a fair, secure and attractive capital market for start-ups, SMEs and investors."

Christian Meisser, LEXR AG

Key Takeaways

- **Tokenization seems to be interesting for small and medium-sized enterprises, as the cost of raising capital via tokens is sometimes lower than on the traditional capital market.**
- **The regulatory classification of whether an issued token represents a security has far-reaching implications and is of the utmost legal relevance. The assessment of whether a token is to be treated like a security under supervisory law is fundamentally different in various jurisdictions.**

Photo: *Christian Meisser*

Authored by Christian Meisser, lic. iur., MBA, CEO of LEXR AG

Christian Meisser is an entrepreneur and lawyer with a focus on the intersection between technology and law. He regularly speaks, publishes, and advises on blockchain-related topics and is specialized in financial market regulation. After working for some of the world's top law firms, he founded the LegalTech company LEXR AG with the vision of providing like-minded entrepreneurs with price-predictable legal services that are tailored to the way companies operate and innovate today.

Capital Flows to the US

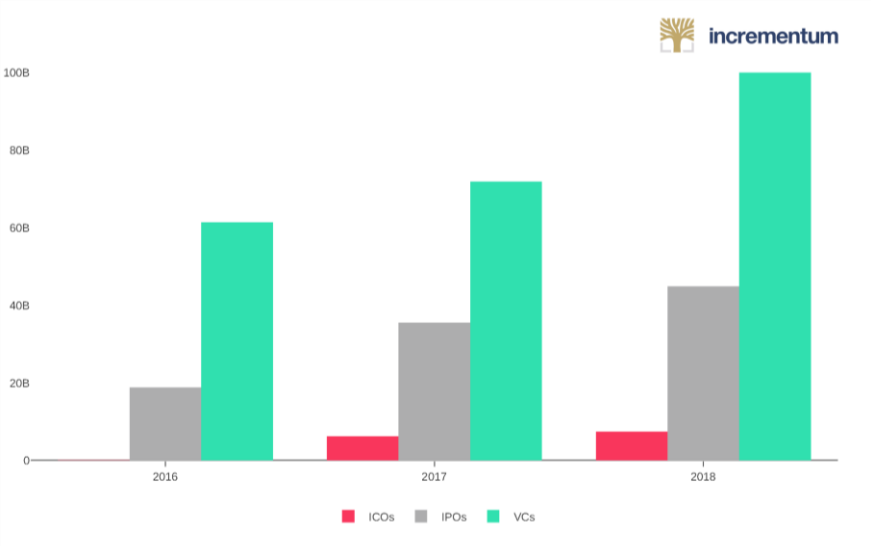
Start-ups as well as small and medium-sized enterprises (SMEs) are praised for being a driving force of economic growth. In principle, Europe offers excellent conditions for growth, with a mobile and well-educated talent pool, a huge domestic market, and modern infrastructure. Nevertheless, risk capital for start-ups is scarce and promising start-ups move abroad. According to a press release of the European Commission,[48] in 2016 **venture capital providers invested only € 6.5 billion in the entire EU, just about one sixth of the € 39.4 billion invested in the US.** According to the same release, **only 26 European companies were regarded as "unicorns" at the end of 2017** (unlisted companies with a theoretical market capitalization in excess of $ 1 billion), **while 109 such companies existed in the US and 59 in China.**

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

Blythe Masters

Not only start-up funding but also financial market support for SMEs appears to be lacking. One reason why start-ups are left wanting is widely considered to be the lack of "exit" opportunities in the form of listings: in 2017, the number of European IPOs of SMEs was still down 50 percent from the time prior to the financial crisis.[49]

Figure 17: ICOs vs IPOs vs VC Funds raised (US).



Source: ICOdata.io, CBInsights, Incrementum

—

[48] See "EU: €2.1 billion to boost venture capital investment in Europe's innovative start-ups" [press release], European Commission, April 10, 2018.

[49] See *Building a proportionate regulatory environment to support SME listing* [public consultation], European Commission, 2017.

"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

With public markets for SMEs weak, venture capital firms hesitate to invest in SMEs at all. While the EU tries to improve the situation with **subsidies**, **harmonization of capital markets** and **mild deregulation**, the world of start-up funding is fundamentally changing because of the blockchain technology. The possibility of transferring assets directly between two parties without intermediaries enables an enormous simplification of issuance and trading of capital market instruments. Thus, start-ups raised $ 5.5 billion worldwide in 2017 by issuing tokens in the framework of ICOs – and this year the total amount has already **swelled to $ 14.3 billion.**[50]

But not only primary markets (i.e., the initial issuance of ICOs) are thriving. **Daily trading volume in tokens in secondary markets amounts to several billion USD.**[51] Thus, blockchain technology has already furnished impressive proof of its application potential in capital markets. From the perspective of investors, it was evidently worth the risk – according to one study, the **average return on investment on ICOs stands at 82 %.**[52] However, the legal design of such tokens as this new technology emerges has received little attention so far and **investors rarely enjoy enforceable rights.** The trend is clearly moving toward issuance of so-called ***security token offerings***: more and more ICO teams want to **tie tokens to enforceable rights, which provide token owners with a legal position akin to that of shareholders.** Thus, the vision of a capital market in which start-ups and SMEs are able to access needed growth capital without having to move offshore and which offers investors safe and simple access to diversification opportunities is coming within grasping distance.

This article presents legal challenges for effective blockchain-based capital markets in different countries by way of examples and in particular discusses the following subjects:

- **Challenges posed by the classification of tokens in financial market regulations**
- **Legal preconditions for the issuance of security tokens**
- **Legal framework conditions for trading in security tokens**

Classification of Tokens as Securities

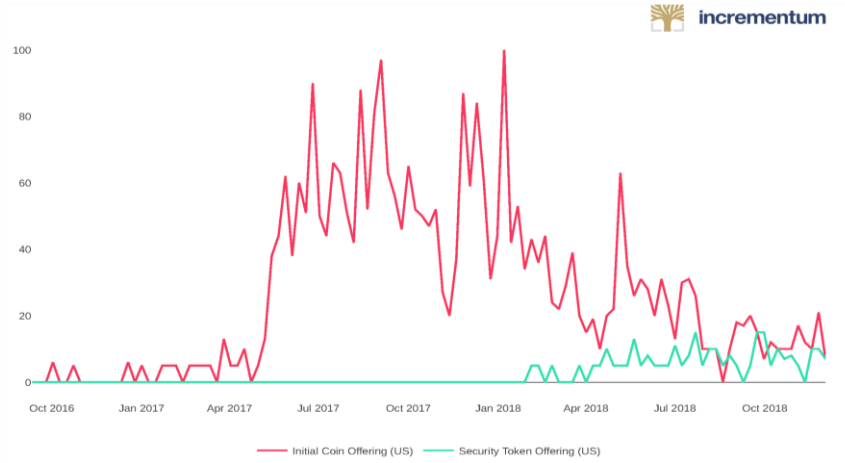
Classification of tokens within the existing framework of civil law is already quite difficult and the opinions of legal scholars differ widely: for instance, in Switzerland it is debated whether tokens are **digital assets**, **contractual rights**,

—

50 Figures according to Coindesk ICO Tracker, accessed September 19, 2018.
51 Figures according to CoinMarketCap, accessed September 19, 2018.
52 See "Digital Tulips? Returns to Investors in Initial Coin Offerings," Hugo Benedetti and Leonard Kostovetsky, *SSRN*, May 20, 2018.

or **a special form of assets in their own right**.[53] This represents a difficult task for regulators with respect to a legal assessment in terms of financial legislation. Obligations under financial market regulations with respect to the issuance and trading of tokens directly depend on their legal classification. For example, if tokens are classified as securities[54] under a specific legal order, **public offerings of such tokens without an appropriate prospectus may make issuers liable to criminal prosecution**. Accordingly, correct classification is quite important, but it is anything but trivial: not unlike a blank sheet of paper, tokens can be configured with any combination of rights and obligations, or in the framework of smart contracts even with complex, automated processes. Various countries are trying to meet this challenge in very different ways:

Figure 18: Google Trends - Security Token Offerings are Gaining Interest



Source: Incrementum

"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

The approach that has been historically established in US case law is based on flexible rather than static principles, which makes it possible to adapt regulations to the countless different possible designs.[55] This is primarily based on the ***Howey Test*** and the term security is tied to whether *"an investment in a common venture is premised on a* ***reasonable expectation of profits*** *to be derived from the entrepreneurial or managerial efforts of others."* Whether there is indeed "*a reasonable expectation of profit"* is sometimes questionable, particularly in ICO projects which refrain from according any rights to investors. Supervisory authorities can strengthen legal certainty by regularly publicizing relevant rulings.

—

53 See "Verfügungsmacht und Verfügungsrecht an Bitcoins im Konkurs" ("Authority to dispose of and right to dispose of Bitcoins in insolvency proceedings"), Christian Meisser, Luzius Meisser, and Ronald Kogens, *Jusletter IT: online*, May 24, 2018.

54 The term *security* is used as an overarching term herein for all designations of a similar type used in different jurisdictions, such as stocks/bonds or financial instruments.

55 See ***Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO***, Securities and Exchange Commission, Release No. 81207, July 25, 2017

The legal situation in the EU is more formal. The EU directive on markets for financial instruments (better known as MiFID, or MiFID II) has largely harmonized financial markets in the single European market; the term "financial instrument" was defined in Annex I, section C. Unfortunately, **it remains essentially unclear under what circumstances a security token is actually classified as a financial instrument**. The definitions in the directive refer to "old world" terms (i. e. before blockchain technology), which simply cannot accommodate the plethora of possible designs associated with tokens. The *Malta Financial Services Authority* has at least attempted to provide some clarity in the form **of a *financial instrument test*.**[56] Without practical examples, the definitions nevertheless exhibit a degree of abstraction that leaves market participants unsure if tokens are deemed to represent financial instruments in view of the multitude of possible configurations.

The Swiss financial market supervisory authority Finma has decided on a compromise in its ICO guidelines.[57] Similar to the method adopted in the US, a functional approach is used with respect to investment purposes. At the same time, formal criteria are taken into account as well, and essentially **every token that represents an asset is considered a security token**. Due to these comparatively clear criteria and the possibility of asking Finma to provide regulatory information on specific cases in advance, the legal situation pertaining to various token configurations can be easily assessed in Switzerland.

"Bitcoin can be best understood as distributed software that allows for transfer of value using a currency protected from unexpected inflation without relying on trusted third parties"

Saifedean Ammous

The tokenization of traditional securities, such as stocks or bonds, is the easiest to assess: The laws were written for these types of securities and issuers are unlikely to face surprises with respect to tax consequences either. In order to prevent the erection of inappropriate barriers to innovation in virtual worlds and the tokenization of real assets, a restrictive application of the various terms designating securities would be welcome. For example, if one were to tokenize tickets to an event, such tokens may already be regarded as securities in several countries: for one thing, a real asset is underlying the token, for another thing one may well purchase event tickets for investment purposes, i. e. in the hope of being able to sell them at a higher price at a later date. At the same time, it seems hardly appropriate to having to issue a prospectus or to trade such tokens on a regulated exchange.

Primary Market: Issuance of Security Tokens

From a technical perspective, the internet makes it easy to market token offerings globally, and cryptocurrencies allow investors to buy tokens globally. Expensive

—

[56] See *Guidance Note To The Financial Instrument Test*, Malta Financial Services Authority, July 24, 2018.
[57] See *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, Finma, February 16, 2018.

intermediaries such as investment banks are barely needed anymore. The rapid growth of ICOs demonstrates that such a global capital market offers highly attractive funding opportunities for companies. However, upon issuing security tokens one is faced with a patchwork of national regulations. **The most important aspect in this context: potential prospectus obligations.**

A prospectus is intended to provide investors with the information required to make an investment decision. What information precisely has to be included varies from country to country and ranges from (for the time being) a few pages in Switzerland to almost book-sized tomes in the US. **Prospectus requirements in the EU are so demanding that small funding rounds are barely worth the investment of time and money needed to draw up and publish a company's financial statements.** As an illustration of the costs involved: according to the Official Journal of the EU, the cost of drawing up an EU prospectus for offers of securities to the public with a total consideration of less than € 1,000,000 is likely to be disproportionate to the proceeds.[58] And that is just the prospectus for the EU. For every additional country in which tokens are to be offered, one has to verify whether a prospectus needs to be published and/or has to be reviewed by the local authorities.

"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

Prospectus obligations may be limited or waived entirely below a certain threshold and plans by a number of countries to raise such thresholds for prospectus publication obligations have to be welcomed in this context (in the EU to around EUR 8 million or in Switzerland to CHF 2.5 million). Further relief is to be provided by various exemptions, such as thresholds on the number of investors or the focus on professional or accredited investors. While prospectus obligations and restrictions on distribution represent barriers to security token offerings, there already exist numerous projects which are able to implement such offerings successfully and with legal certainty. Along with growing interest, the required know-how will spread in the marketplace and costs will be lowered further, not least through the use of legal-tech software for drawing up documentation in various countries.

Secondary Markets: Trading in Security Tokens

The most impressive efficiency gains are possible in trading. Thanks to smart contracts, so-called decentralized trading platforms can be built, which enable trading between two parties **without any intermediaries or counterparty risks**. The assets to be traded are safely stored via the smart contract, and once the required conditions are fulfilled, clearing and settlement takes place automatically

—

[58] See "REGULATION (EU) 2017/1129 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market (prospectus directive 3)," European Union, *Official Journal of the European Union*, June 30, 2017.

on the blockchain. Infrastructure costs, such as centralized security depositories, security settlement systems, or banks, and counterparty risks disappear. It is simply not possible in such a system to be affected by a default such as that of Lehman Brothers.

"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

A sensible function that remains in place consists of match-making platforms similar to those operated by stock exchanges or other trading platforms, which are in particular aimed at efficient price formation and the prevention of market abuse. From a regulatory perspective, risks, such as insider trading and market manipulation, remain extant in the blockchain world as well, and modern-day regulations are in essence applicable to trading platforms for security tokens. In the meantime, both established exchanges such Switzerland's SIX[59] and blockchain enterprises in a number of countries have made public announcements regarding the development of security token trading platforms. As "old-world" regulations remain applicable, a license is necessary, which has so far not been granted in any (developed) country. Moreover, the focus of proposed or already implemented blockchain-related legislation in various countries is on cryptocurrency trading and on utility tokens – which has largely no effect on the regulation of security token trading venues. Nevertheless, advisory practices and press releases by numerous enterprises in the industry give cause for confidence **that trading venues for security tokens will be established shortly.** After all, for ICO teams the tradability of a token is an important criterion affecting its design.

Final Remarks

The consummate ease with which tokens can be issued, transferred, and equipped with automated payment functions could be the basis for an **"internet of finance"** – a new generation of financial markets in which even the smallest projects can quickly and safely obtain external funding without intermediaries. Imagine for example a small bakery in a village which can get funding for a new oven from its loyal customers by issuing a tokenized micro-bond with automated interest payment features, or a movie project which automatically pays out a share of its revenue to the community of fans that funded it with every download. The indirect interaction between capital seekers and capital suppliers makes not only large, global funding rounds possible but also promotes stronger relationships between small investors and their local economy.

Moreover, a blockchain-based, decentralized trading system provides greater stability and safety, as the absence of intermediaries removes potential points of failure and middlemen whose incentives are not necessarily aligned with those of investors. In order for this technology to achieve its full potential for creating an

—

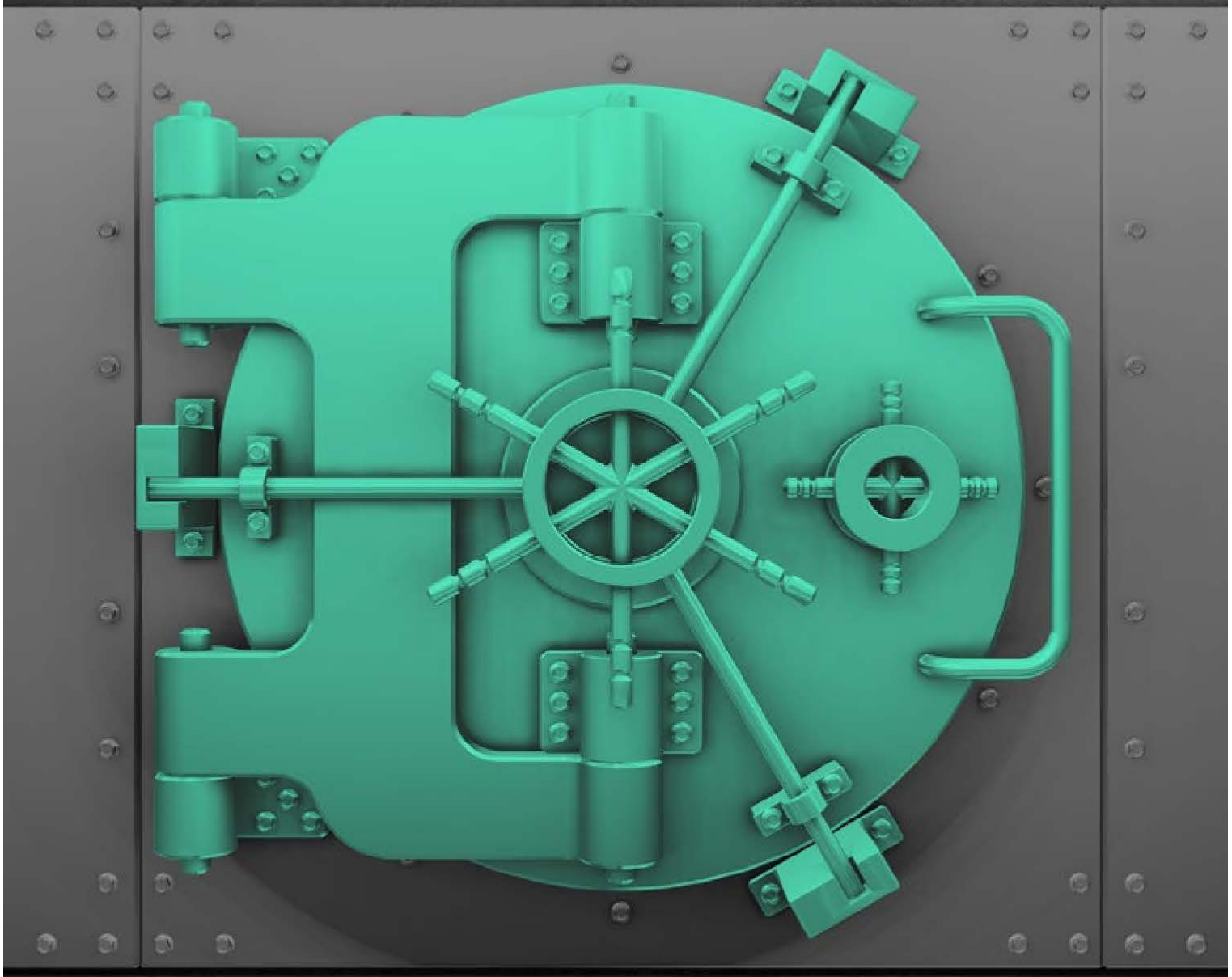
59 See "SIX to launch full end-to-end and fully integrated digital asset trading, settlements and custody training" [press release], *SIX Group AG*, July 6, 2018.

attractive capital market for companies and investors, existing regulations have to be applied with sound judgment and a sense of proportion. Luckily the legislative pendulum is currently swinging toward deregulation again, and more and more regulatory exemptions are planned, particularly for start-up companies and small and medium-sized enterprises.[60] However, in order to make it possible for unicorns and already successful companies to obtain adequate funding in their home markets, more than exemptions for small projects will be needed. **In a global financial market characterized by mobile talent, courage on the part of regulators to open up and liberalize markets stands to be rewarded.**

—

[60] See "Fact Sheet Frequently asked questions: Easier access to financing for smaller businesses through capital markets" [press release], *European Commission*, May 24, 2018.

Cryptocurrencies.
The New Asset Class.



Regulated | Diversified | Liquid

Information about the fund strategy for professional investors (according to MiFID) only.

www.cryptofunds.li

About Us

The Team

Mark Valek

Portfolio Management & Research

Demelza Hays

Research & Portfolio Management

Cristian Ababii

Research

Friederich Zapke

Research

The Report

As a sister report to the internationally acclaimed In Gold We Trust report, the Crypto Research Report brings the same quality and rigor to understanding the cryptocurrency market. The Crypto Research Report is a report produced by Incrementum AG.

The Company

Incrementum AG is an owner-managed and fully licensed asset manager & wealth manager based in the Principality of Liechtenstein.

What makes us stand out in the asset management space? We evaluate all our investments not only from a global economic perspective but also by taking into account global monetary dynamics. This analysis produces what we consider a truly holistic view of the state of financial markets. We believe our profound understanding of monetary history, out-of-the-box reasoning and prudent research allows our clients to prosper in this challenging market environment.

Advisors

In order to provide accurate information on the most important and recent updates in the crypto space, a diverse team of thought-leaders, academics, and finance experts form our board of advisors. The mission of our board is to stimulate discussion on the most pressing risks and opportunities in the cryptocurrency market. Our advisors come from different countries, different education paths, and different careers. However, they all have one trait in common: their avid interest in the blockchain technology and cryptocurrencies. To stay up-to-date, the advisory board meets on a regular basis to discuss current affairs and the next quarter's outlook. All meeting minutes are posted as a transcript and released for free on our website at www.CryptoResearch.Report. Our board members include:

Max Tertinegg

Max Tertinegg is the CEO and co-founder of Coinfinity in Graz. Since 2014, Mr. Tertinegg has worked with merchants, investors, and regulators in Austria to build a cryptocurrency community. Currently, he is working on cryptocurrency storage solutions that are affordable and easy to use.

Oliver Völkel

Based in Vienna, Oliver Völkel is a partner at StadlerVölkel Attorneys at Law. He assists corporations and banks in all stages of capital market issuings and private placements (national and international). His focus is on new means of financing vehicles (initial coin offerings, initial token offerings) and drafting and negotiation of cross-border facility agreements and security-documentation, also in connection with cryptocurrencies and tokens. Mr. Völkel also advises on other cryptocurrency related banking matters, regulatory matters, capital markets regulation, general corporate, and corporate criminal matters.

Joseph Annuzzi Jr.

Joseph Annuzzi Jr is the founder and CEO of a stealth cryptocurrency decentralized exchange and the sole inventor of a cryptocurrency secret key protection algorithm designed for consumers. He is a software architect and entrepreneur from Silicon Valley and an author of a series of computer science text books published by Pearson Education, Inc. He also works with crypto custody solutions.

We sincerely want to thank the following friends for their outstanding support:
Our knowledgeable advisors including Max Tertinegg, Oliver Völkel, and Joseph Annuzzi Jr., the generous authors who contributed to this report including Nikolaus Jilch, Christian Meisser, and Patrick Valovic. We are also grateful to our wonderful research analysts Friedrich Zapke and Cristian Ababii.

Contact:

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