



crypto research
.report

February 2020
Edition IX.

“Plan B Edition”



Is Bitcoin Evolving to Digital Gold?

The “Plan B” Model – Holy Grail of Bitcoin Valuation?

Crypto Custody: What’s new in Germany?

Demelza Hays
Mark J. Valek

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

coinfinity



FALCON

PRIVATE BANK

www.cryptofunds.li

Contents

Editorial.....	4
In Case You Were Sleeping: Iran, Gold, and a Small Bitcoin Boom.....	5
Bitcoin and The Iran Conflict	6
Bitcoin as Safe Haven and Friend of Gold	8
The Halving as a Big Non-Story?	11
Central Banks Are Coming.....	12
Conclusion	14
The “Plan B” - Model: The Holy Grail of Bitcoin Valuation?	16
What is the Stock-to-Flow Ratio?	17
Bitcoin, Gold and Scarcity	17
The Quantitative Valuation of “Plan B”	18
Further Models	20
The Law of Potency	22
Conclusion	22
The Stock to Flow Model: Mark Valek’s Exclusive Interview with “Plan B”	23
Plan B, When Will You Show Yourself?	24
Crypto Custody: What’s new in Germany	29
Storing Digital Assets in a Digital High Security Vault	30
Self Custody vs Serviced Custody	34
Regulatory Developments in DACH	35
Global State of Custody Service Providers	36
Bitcoin vs. Gold – a Fictitious Debate	38
Incrementum Recommended Books	47
New Research in Crypto	48
Official Launch of Incrementum’s Research Cooperation with the University of Liechtenstein	48

Disclaimer:

This publication is for information purposes only and represents neither investment advice, nor an investment analysis or an invitation to buy or sell financial instruments. Specifically, the document does not serve as a substitute for individual investment or other advice. The statements contained in this publication are based on the knowledge as of the time of preparation and are subject to change at any time without further notice. The authors have exercised the greatest possible care in the selection of the information sources employed; however, they do not accept any responsibility (and neither does Incrementum AG) for the correctness, completeness, or timeliness of the information, respectively the information sources made available, as well as any liabilities or damages, irrespective of their nature, that may result there from (including consequential or indirect damages, loss of prospective profits or the accuracy of prepared forecasts).

Editorial

Dear Reader,

This edition of the Crypto Research Report discusses whether Bitcoin's halving is priced in yet or not. We interview the author of the infamous Stock to Flow Ratio Model, Plan B, and we critique this model by reviewing competing models. We are of the opinion that the halving is not priced in fully yet. Due to Bitcoin's young age, investors have ambiguity aversion and correspondingly high discount rates. Due to uncertainty surrounding cryptocurrencies, investors are taking a "wait and see" approach. As the date approaches, more investors will become aware of the forthcoming halving and invest accordingly.

CRR XIV discusses how the tension between the US and Iran is fueling demand for privacy coins like Dash, Monero, and Zcash. This edition also features a guest article by Daniel Wingen, founder of the Valuing Bitcoin Conference in Germany. He discusses how cryptocurrency custody works, and the questions that investors should ask when deciding how to securely store cryptoassets.

In addition to a timely report packed with brand new research on Bitcoin's price development, there is big news for the Crypto Research Report team! Over the past two years, we have published nine editions with over 800,000 impressions in 187 countries. The Crypto Research Report is growing, and we have made the strategic decision to launch a new company dedicated solely to publishing the Crypto Research Report. In addition to the free quarterly report and our custom buy-side research reports, we will begin offering a host of complimentary products including a weekly newsletter, podcast, YouTube video, and data analytics platform. The launch of the new CRR website will include daily news articles that focus on data and research. In addition to daily news, the CRR is launching a weekly newsletter that shows the official CRR cryptocurrency portfolio and weekly trades. To sign up for the CRR's weekly newsletter, visit:

<https://cryptoresearchnewsletter.substack.com/>

The *Crypto Research Report* began as a sister report of Incrementum's *In Gold We Trust* report in 2017. It quickly established itself as an outlet for unbiased and in-depth articles on the cryptocurrency market. Incrementum will stay a strategic partner for the report. Demelza Hays will be in charge of the new company whereas Mark Valek will continue to contribute articles on a regular basis to the Crypto Research Report. We are excited to embark on this journey, and we hope that you will join us.

Last but not least, we especially want to thank our ongoing Premium Partners of the *Crypto Research Report*, [Falcon Private Bank in Zurich](#) and [Coinfinity in Graz](#).

Demelza Kelso Hays and Mark Valek,
Incrementum AG

In Case You Were Sleeping: Iran, Gold, and a Small Bitcoin Boom

“Last night’s U.S. strike, killing Iranian General Soleimani, is the sort of event that gets markets moving. As one might expect, oil jumped and so did gold. Oil is up 3% and gold jumped 2%. In this new world there is a third safe haven asset, bitcoin (BTC). It is up 5%.”

Clem Chambers, Forbes

Key Takeaways

- ◆ The price of Bitcoin rose after the attack on General Soleimani - just like the price of gold. The correlation of the two assets is higher than it has been in a long time. This raises the question again, whether Bitcoin will start the new decade as the one and only digital gold.
- ◆ Three important events and trends for this year can be foreseen: Bitcoin will be talked of as a safe haven and escape route, the next Bitcoin Halving will be in May, and central banks will fill the gap with self-made currencies.
- ◆ According to the Bank of International Settlements, almost three quarters of all international central banks are working on some form of digital currency.



Is Bitcoin currently acquiring a new status as a safe haven asset, as digital gold? There is some evidence for this, the Iran crisis provides interesting clues. The Halving could help too.

Bitcoin and The Iran Conflict

"Luck in the crisis? The Iran-conflict could trigger the next Bull Run (on Bitcoin)."

BTC-ECHO

Suddenly the price of Bitcoin took a leap. And then another one. The reason for the first leap was the targeted killing of Iranian General Qasem Soleimani on January 3, 2020 by the US. The Bitcoin price then took its second leap due to the Iranian counterattack against Western military bases in Iraq. Twice the world held its breath. Twice Bitcoin shot up together with gold. And twice it all looked like a new safe haven was born. But is Bitcoin really the new digital gold?

The correlation between the two assets has rarely been as high as it was in early 2020, and some analysts see a clear connection between the shiny precious metal and the digital coin. Others urge patience. One event does not make a safe haven. But the growing tension between Washington and Tehran is a Bitcoin story – in more ways than one. It was not the first time that the cryptocurrency has reacted sensitively to a political event - and it will not be the last. Comparison with gold is also understandable: For in the daily practice of Iranians (or Venezuelans before them) the two assets play a very similar role. And Bitcoin has not only just arrived with the current worsening of the situation in Iran. Cryptocurrencies have long been part of everyday life there.

Here is what Brian O'Hagan had to say about his experiences in Iran in 2018:

*"People who own savings in rials see their purchasing power diminish every day. They are looking for ways to protect their wealth, and find a refuge for what little cash they have. They are looking for stores of value to survive the economic collapse: dollars (but they can't find any in Iran) or gold. People in Iran are increasingly turning to cryptocurrencies to protect themselves from an economic collapse and to evade the financial repression. And the government is noticing."*¹

¹ <https://hackernoon.com/how-donald-trump-is-helping-bitcoin-grow-in-iran-331ee7445bd8>

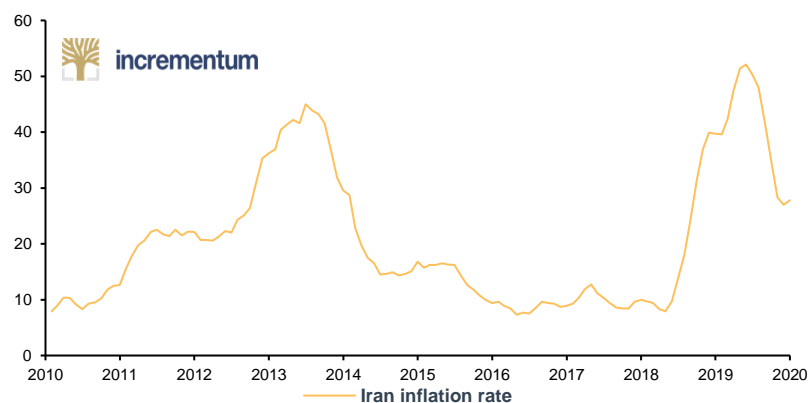
"Iran removes four zeros from the national currency."

Haldelsblatt.com

"Now Iranian President Hassan Rouhani demands a crypto-currency for the entire Muslim world in order to make itself less dependent on the US dollar."

Cryptomonday.de

Figure 1 Inflation rate Iran



Source: Reuters Eikon, tradingeconomics.com, Incrementum AG

The US sanctions have been making it difficult for Iranian companies and private individuals to trade with foreign countries for years. In addition, there is high inflation in the country, which has a negative impact on the purchasing power of Iranians. Perfect conditions for the adoption of Bitcoin, as we have also seen in Venezuela. Another parallel: thanks to extremely low energy costs, mining in these countries is much cheaper than elsewhere.

As far as the official side is concerned, Iran is very ambivalent. That's understandable. On the one hand, Bitcoin can help circumvent US sanctions. On the other hand, it also provides the population with a way to get money out of the country. This then leads to excesses such as a significantly inflated Bitcoin price within Iran. In September 2018, there were reports of an Iranian Bitcoin exchange rate of almost 26,000 dollars.²

Like China and other US antagonists, the Iranian regime has a great fear of capital flight. The country's banks have therefore been forbidden to engage in the crypto business. Mining is handled with a more pragmatic approach. The industry is now recognized by the government and it cannot even be ruled out that the regime itself is active in mining to fill its coffers.³ At the same time, Iran is working on a state cryptocurrency - just like Venezuela and China. More on this later.

And it is not only Tehran that is taking the issue seriously- Washington is too. At the end of 2018, the Iran sanctions were extended for the first time to the Bitcoin wallets of two individuals. Even the "New York Times" has already been to Iran to visit the Bitcoin mines there: "Iran's economy has been hobbled by banking sanctions that effectively stop foreign companies from doing business in the country. But transactions in Bitcoin, difficult to trace, could allow Iranians to make international payments while bypassing the American restrictions on banks."⁴

This brings us to the three megatrends we see for 2020:

² <https://hackernoon.com/why-is-bitcoin-trading-at-a-253-premium-price-in-iran-45f9a2f30017>
³ <https://www.aljazeera.com/ajimpact/iran-government-recognises-cryptocurrency-mining-caveat-190804193912792.html>
⁴ <https://www.nytimes.com/2019/01/29/world/middleeast/bitcoin-iran-sanctions.html>

- ▶ Bitcoin will be talked of as a safe haven and escape route - and will increasingly be compared to gold.
- ▶ The Halving will bring attention - but not necessarily higher prices.
- ▶ While Facebook's Libra project is running into more and more problems, some central banks will launch government cryptocurrencies.

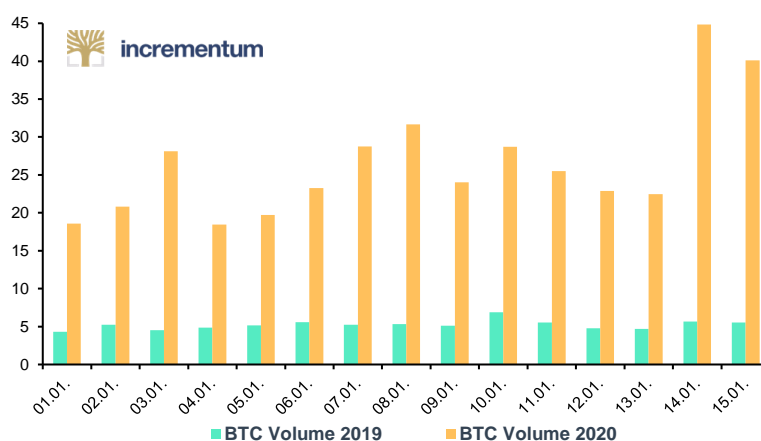
Bitcoin as Safe Haven and Friend of Gold

"Bitcoin is going to be a safe haven."

FinanzundWirtschaft.ch

In the first few days of the year, volumes in Bitcoin markets doubled. In the midst of an ongoing bear market, investors and fans saw a silver lining on the horizon. Around the escalation of tensions between Iran and the USA, Bitcoin was traded as a safe haven asset. The correlation with gold was stronger than it has been for years. The mood on the Bitcoin market has also improved as a result, with sentiment no longer being bad but neutral.⁵

Figure 2 Trading Volume of Bitcoin in the beginning of 2019 and 2020 compared



Source: coinmarketcap.com, Incrementum AG

However, the vast majority of analysts agree that one data point is not enough, that the safe haven story must stand up to further scrutiny - and that the prevailing downward trend has not yet been broken. One analyst doesn't believe the Iran story at all and speaks of a technical rally.⁶

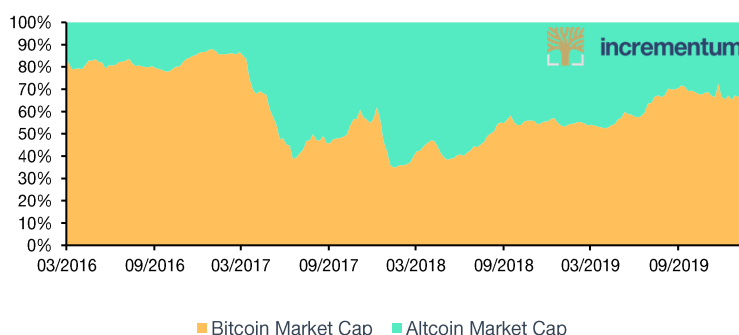
Be that as it may, the comparisons between Bitcoin and gold will now be heard more often. Bloomberg analysts even see gold as a proxy for the Bitcoin price because the assets are so similar. Both are scarce in quantity and are particularly suitable for value storage. Bitcoin has the advantage of simplified transport and dominates in the digital world. Gold has the advantage of a history going back several thousand years - and dominates in the real world. Find out more about the similarities and differences of Gold and Bitcoin in the article "Bitcoin vs. Gold – a Fictitious Debate" in this episode of the CRR.

⁵ Arcane Research Weekly Update 2/2020

⁶ <https://www.ccn.com/bitcoin-price-bounce-has-nothing-to-do-with-iran-situation/>

At the same time, Bloomberg does not speak highly of Altcoins, whose market share continues to shrink: "The fact that a store-of-value asset with fixed supply and increasing adoption is more likely to appreciate in price will keep Bitcoin supported in 2020. We expect movements in gold to remain a proxy for Bitcoin. The broader crypto market is at risk of more mean reversion of the parabolic 2017 rally and depends on advancing Bitcoin for buoyancy. Our takeaway is straightforward: Bitcoin is winning the adoption race, notably as a store-of-value in an environment that favors independent quasi-currencies."⁷

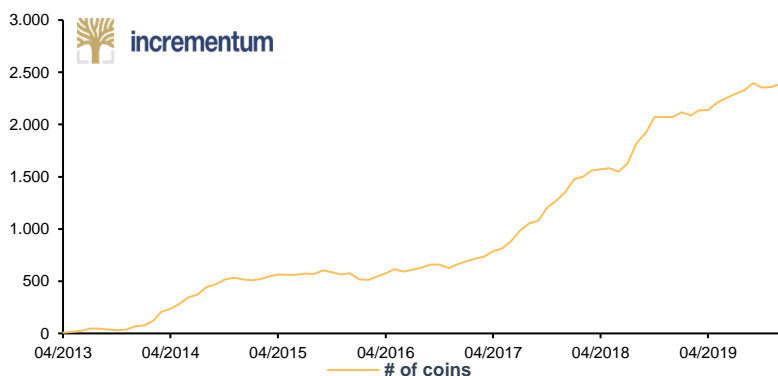
Figure 3 Bitcoin Dominance in comparison to Altcoins



Source: coinmarketcap.com, Incrementum AG

Unlike Bitcoin itself, which benefits from its scarcity, Altcoins suffer from a constantly growing oversupply. We have already examined this process in our previous reports and do not see any change in the trend." Just too many crypto-assets competing for adoption will keep broad market prices biased to the downside, in our view. A future of appreciating prices for cryptocurrencies is unlikely until rapidly increasing supply is curtailed. In 2019, the number of tradable crypto assets listed on Coinmarketcap.com increased by about 3,000 – up to 5,078, the most ever."⁸

Figure 3 Number of Altcoins over time



Source: coinmarketcap.com, Incrementum AG

⁷ Bloomberg Crypto Outlook - January 2020 Edition

⁸ Bloomberg Crypto Outlook - January 2020 Edition

In the first week of the year alone, Bitcoin increased its market share by 1.0 percent, while both ETH and XRP fell by 2.6 percent. Interestingly enough, the tense Iranian situation had **a positive effect on the anonymous cryptocurrencies Dash and Monero, which increased their market share by 15 percent each.** In our eyes, this is proof that the crypto sector also has a meaning in real events and that these coins are not just bought for speculative purposes.⁹

This development, the experience from Iran and the price movements in early 2020 clearly show in the eyes of Bloomberg analysts that Bitcoin is establishing itself on the market as a store of value. Again, the similarity to gold is striking. Unlike many in the crypto-community, analysts do not see gold and Bitcoin as enemies, but as friends: "Gold prices will keep climbing in 2020 and so should Bitcoin, in our view. The digital version of the metal is in the maturing process of consolidating the rapid price appreciation of its youth. Bitcoins' ever-more inverse relationship with the U.S. dollar indicates the maturation process of the new quasi-currency toward a digital version of gold."¹⁰

"The (Peterson) correlation between gold and BTC rose to 0.217, last seen in October 2016."

Coin News Telegraph.com

The correlation between Bitcoin and gold had already been on an upward trend since the beginning of 2019 and, according to the analysts of Arcane Research, reached a peak in January 2020, which was last seen in the summer of 2016.¹¹

But there is another correlation that should make Bitcoin investors less happy. We're talking about Tether. In recent months two studies have come to the conclusion that the price of Bitcoin, at least in the past, has been very strongly dependent on the development of the stablecoins money supply.¹²

The accusations of the US researchers John Griffin (University of Texas) and Amin Shams (Ohio State University) are particularly blatant. They have written a paper to prove that only Tether and the stock exchange Bitfinex alone were behind the huge price increase at the end of 2017. They talk of massive manipulation. Griffin told Bloomberg: "Our results suggest instead of thousands of investors moving the price of Bitcoin, it's just one large one. Years from now, people will be surprised to learn investors handed over billions to people they didn't know and who faced little oversight." Tether and Bitfinex categorically deny the allegations.¹³ Now the controversy around Tether is by no means new. We have reported on this on several occasions, and for the sake of completeness, we list the study and the allegations here. Unfortunately, we cannot judge whether there is something behind it or not.

⁹ Arcane Research Weekly Update 2/2020

¹⁰ Bloomberg Crypto Outlook - January 2020 Edition

¹¹ Arcane Research Weekly Update 2/2020

¹² <https://www.bloomberg.com/news/articles/2019-10-03/bitcoin-gains-correlate-with-tether-issuance-researcher-says?srnd=technology-vp>

¹³ <https://www.bloomberg.com/news/articles/2019-11-04/lone-bitcoin-whale-likely-fueled-2017-price-surge-study-says>

The Halving as a Big Non-Story?

Another factor that accompanies Bitcoin and will become acute this year is the story of the Halving. Bloomberg has collected quotes by industry leaders on the event, which is expected to take place in May 2020. The conclusion: Some hope for price increases, others consider the halving to be priced in, and yet others see it as the best way to educate people about Bitcoin. We are most likely to be found in this third camp. The fact that we even know that the supply of fresh coins will be cut back this year is **a great victory for the transparency of Bitcoin's monetary policy**. It is also the basis of the comparisons to gold that we cited in the previous chapter. Find out more about the Halving in the Article "The Stock to Flow Model Mark Valek held an Exclusive Interview with "Plan B" in this episode.

Taking a look at past halvings, you quickly understand why many enthusiasts are looking forward to 2020: "In a halving, Bitcoin rewards that go to the so-called miners that support the coin's network drop in half in order to prevent inflation from eroding the purchasing power of the coins. In the previous reductions, the price rose about 8,000% in the year after the 2012 decrease and around 2,000% in the 18 months following the 2016 cut, according to data compiled by Bloomberg."¹⁴

What do the pros say?

"Unlike most Bitcoiners, I don't think the halving is particularly bullish. I am of the view that most people with a Bitcoin position understand that it's capped in supply, so the issuance change shouldn't make a difference. Also, the halving is perfectly forecastable, so I have a hard time believing that it constitutes an informational shock. Bitcoin supply has been described and understood from January 2009 and has followed the ordained trajectory ever since."

Nic Carter,
Co-founder of Coin Metrics

"As Bitcoin is often influenced by momentum thinking -- and the halving is magnified by a transformation of the economic structure -- I'd estimate it will have a positive influence on price."

Dave Balter,
Chief Executive Officer of Flipside Crypto

"Many market participants have been asking the question -- is the Bitcoin halving priced in? That's the wrong way to frame it. A small single digit percentage of the world currently owns Bitcoin. For those that currently own Bitcoin, a large portion of them understand that Bitcoin's newly issued supply is cut in half every

¹⁴ <https://www.bloomberg.com/news/articles/2020-01-08/bitcoin-halvening-isn-t-until-may-but-nothing-else-matters-now?srnd=cryptocurrencies>

four years. This is likely a significant reason why they own it -- because of Bitcoin's provable scarcity. For the many billions of people around the world that do not own Bitcoin, few understand this provable scarcity characteristic. So for those billions, it cannot be priced in. To the extent those billions of people discover Bitcoin in the future and decide to buy some, there will be less new available supply to satisfy that increased demand to purchase Bitcoin."

Travis Kling,
Founder of Ikigai Asset Management

We find the perspective of Kling particularly interesting. How can one assume an efficient market if the market has so few participants so far? The halving will in any case give the media the opportunity to point out the positive sides of Bitcoin and to explain the functioning of the original cryptocurrency in detail once again. This could further strengthen the Bitcoin-as-Safe-Haven narrative and further weaken the Altcoins.

But it would also be the perfect time for a state actor to enter the field of cryptocurrencies. Even if that has little to do with Bitcoin per se.

Central Banks Are Coming

Anyone who belittles the efforts of central banks in the crypto area could overlook important points. One thing is true, though: Neither China, nor the Eurozone or Sweden are planning any real competition to Bitcoin. The new digital currencies will be just that: currencies - no digital store of value.

State cryptocurrencies, which also allow state surveillance, could even drive some users into the arms of Bitcoin, Dash and Monero, which at least partially guarantee anonymity. But: "Politicians are looking to destroy this competitive advantage for non-state digital currencies by making them less secure. Governments are investing heavily in a technology that could one day - in theory - crack the public-key cryptography underpinning Bitcoin: Quantum computing. The Trump administration has committed \$1.2 billion to this endeavor. China is active too."¹⁵

China even takes a particularly nefarious approach. In November 2019, President Xi even caused a 30 percent increase in Bitcoin prices, because he had spoken positively about the blockchain and expressed the government's interest in the technology: "The irony is striking, considering Bitcoin's anarchic origins. But there's something broader going on here. The future of digital money is being shaped increasingly by national governments. Politicians are under pressure to make electronic payments more efficient, to neutralize the threat of cryptocurrencies to their sovereignty and to crack down on illicit money flows.

¹⁵ <https://www.bloomberg.com/opinion/articles/2019-11-04/bitcoin-s-government-enemies-will-have-their-sweet-revenge>

"The preparation for the e-Krone (Sweden) is well advanced."

Business Insider.de

None of that is good news for the blockchain's true believers, however much a Beijing stamp of approval boosts the price of a Bitcoin."¹⁶

Meanwhile, Chinese media report that the state cryptocurrency is almost ready. What exactly this digital yuan will look like and when it will be launched is still unclear. According to reports, China has been working on the project since 2014. What we do know: The currency is to be put into circulation via the commercial banks in the same way as the paper currency. Users can then open accounts with these banks and use the crypto-yuan. The first pilot projects are to start in Shenzhen and Suzhou.¹⁷

It is a certain irony that Mark Zuckerberg, of all people, warned of precisely this development. If the West is not open to new blockchain projects like its Libra-Coin, China will take the lead in this area, Zuckerberg told the US Congress: "China is moving quickly to launch a similar idea in the coming months. We can't sit here and assume that because America is today the leader that it will always get to be the leader if we don't innovate."¹⁸

Zuckerberg sees Libra as the western counterpart to China's plans, where cryptocurrency is to be combined with close monitoring of the population. But Libra is severely handicapped in the West. The skepticism is huge in the USA and in Europe. Recently, Switzerland has also bowed to the pressure. Libra will not receive permission to set up the headquarters of its consortium in Switzerland in the foreseeable future, the government said. The status of the project is open, its future remains uncertain.¹⁹ **Recently, some of the most important supporters have backed out: Mastercard, Visa, E-Bay and Stripe.**²⁰

At the same time, however, according to the Bank of International Settlements, almost three quarters of all international central banks are working on some form of digital currency.²¹ But: Only five projects are in the pilot phase. It is highly unlikely that a digital Euro or digital Pound will be introduced the day after tomorrow. It is true that individual countries in Europe, such as Sweden, have already made great strides on the road to a cashless society - and are therefore very interested in a state cryptographic currency. However, the so-called "E-Krona" is still a long way off it seems.

In the EU, the focus so far has been on the further development of existing systems. However, there is a joint crypto project that the ECB is running with the Bank of Japan: "Project Stella". As an individual state, France wants to position itself particularly prominently and wants to "test" a digital currency in 2020. But that's all it will ever be, because France, as a member of the Euro, is not allowed to

¹⁶ <https://www.bloomberg.com/opinion/articles/2019-11-04/bitcoin-s-government-enemies-will-have-their-sweet-revenge>

¹⁷ <https://www.theblockcrypto.com/linked/52616/chinas-central-bank-says-it-has-completed-top-level-design-of-digital-currency>

¹⁸ <https://cointelegraph.com/news/libra-could-serve-as-counter-to-chinese-digital-currency-says-zuckerberg>

¹⁹ <https://www.nzz.ch/schweiz/bundesrat-maurer-libra-hat-derzeit-keine-chance-auf-bewilligung-ld.1530913>

²⁰ <https://www.ft.com/content/a3e952dc-ec5c-11e9-85f4-d00e5018f061>

²¹ <https://www.ledgerinsights.com/bis-70-percent-central-bank-digital-currency-cbdc/>

"Switzerland cannot authorise Libra in its present form."

Swiss Federal Council
 Ueli Maurer

introduce its own currency.²² In a position paper at the end of October, the German Banking Association also spoke out in favor of a European digital currency. But the ECB only wants to make plans for a digital Euro if the private sector does not manage to make international transfers cheaper and faster.²³

Within the Bank of International Settlements, a Frenchman will be responsible for the digitization of money: Benoît Cœuré, a former member of the ECB's Executive Board, heads a new department which is charged with developing public alternatives to projects such as Libra. "The first task facing Mr Cœuré, who starts in January and will serve a five-year term, will be to co-operate with the Swiss National Bank to create a central bank digital currency for wholesale use between banks, safeguarded by so-called distributed ledger technology (DLT)".²⁴

Conclusion

The efforts of the central banks have made one thing very clear: From an economic perspective, this is not about Bitcoin. It's about the danger posed by Libra. It is about the possibilities of saving on cash logistics. And it is - unfortunately - about the surveillance of citizens.

Against this background, Bitcoin should actually find fertile soil in which a new bull market can flourish. The story of Bitcoin as a store of value, of "digital gold", becomes more credible with each crisis. It's also simpler and better digestible for the masses than the hype about blockchain, from which, apart from Bitcoin itself, not many useful applications have emerged so far.

The combination of these factors should make for a good year for Bitcoin. Even though we do not know when the downward price trend will really end. In the days after the short Iran crisis, when the price of gold was long since on the way down again, the Bitcoin price did actually continue to rise. A sign of life, if you will. From a market that is still in its infancy.

We must not forget that. Just around the last pump to around 8,650 dollars per Bitcoin, public television in Germany even reported with a positive undertone about the introduction of Bitcoin options at the CME stock exchange. "Bitcoin reaches the mainstream," was the headline. We share this opinion. We have stated the same many times.²⁵

"Facebook has 2.4 billion active users. And it's planning its own digital currency called Libra. Politicians in Europe - including Germany's finance minister - fear for their currency power."

Zeit.de

²² <https://www.derstandard.at/story/2000111883615/frankreich-will-ab-2020-digitalwaehrung-testen>

²³ <https://www.bloomberg.com/news/articles/2019-12-04/ecb-says-own-digital-euro-may-be-answer-if-payment-efforts-fail?srnd=premium-europe>

²⁴ <https://www.ft.com/content/c7739de6-03e7-11ea-a984-fbbacad9e7dd?sharetype=blocked>

²⁵ <https://www.tagesschau.de/wirtschaft/boerse/bitcoin-153.html>

Falcon Digital Assets Solutions

First Swiss bank to introduce direct crypto transfers



Regulated. Secure.
Convenient.

falconpb.com


FALCON
PRIVATE BANK

The “Plan B” - Model: The Holy Grail of Bitcoin Valuation?

“The high stock-to-flow ratio, the liquidity of the market, and its unique features as a monetary good set gold apart from all other asset classes and make it an efficient hedge against systemic market risk.”

In Gold We Trust-Report 2011, page 26

Key Takeaways

- ◆ The "Plan B" valuation model for the development of Bitcoin's price quickly gained worldwide attention. In it, the price of Bitcoin is modelled with the "stock-to-flow ratio", a proxy for scarcity.
- ◆ Historically, the stock-to-flow ratio was an almost perfect exogenous regressor for the development of the price of Bitcoin (R² was 95%).
- ◆ According to the model, the price of Bitcoin should rise to USD 55,000 after the next "halving" in May.

What is the Stock-to-Flow Ratio?

Since the article "Modeling Bitcoin's Value with Scarcity" appeared on the online platform Medium in March 2019, it has already been translated into over 25 languages and will soon spread worldwide. But what exactly is it all about and what conclusions can be drawn from it? In the following article, we'll explore these and other questions.

The Stock-to-Flow Ratio

The stock-to-flow ratio is a ratio of two figures corresponding to raw materials, which can ultimately be used for price modelling.

The term "stock" refers to how much of a certain raw material is mined or would potentially be in stock if the entire stock was offered.

In this concept, "flow" stands for the production quantity within a certain period, usually within one year.

If you now compare these two figures, you will see relatively quickly that this can be used as a measure of the constancy of the quantity of raw materials.

$$\frac{\text{Stock}}{\text{Flow}} = \frac{\text{Total Stock (Quantity Issued to Date)}}{\text{Annual Quantity Issued}}$$

An example: While the total amount of gold ever mined is about 190,000 tons (stock), the annual production is about 3,000 tons (flow). If you divide the stock by the flow, you get a stock-to-flow ratio of 63.3, which means that at the current production level, it would take more than 63 years to double the gold stock or rebuild the current stock.

So, the larger the number, the more constant is the raw material that is examined. While the "stock" is a given size and grows yearly exactly around the "flow", the "flow" depends on various factors, such as the rarity, the price and the difficulty of extracting the raw material.

The basis for the entire model is the so-called "Stock-to-Flow Ratio", a concept that interested readers of the Crypto Research Report and its sister report, the "[In Gold We Trust Report](#)", have been familiar with for many years. For those who are not yet familiar with the concept or who would like to refresh their knowledge of it, please refer to the info box on the left.

The author of the article, who blogs under the pseudonym "Plan B", dared to try to model the price of Bitcoin with the "Stock-to-Flow Ratio" (hereinafter SF). The concept, which was originally applied to gold and other precious metals, hit the Bitcoin scene like a bomb. How did it come about that a concept for commodities could be applied to a cryptocurrency?

Bitcoin, Gold and Scarcity

Two main factors contribute to the value of gold— the most important precious metal for investors:

1. The Relative Rarity

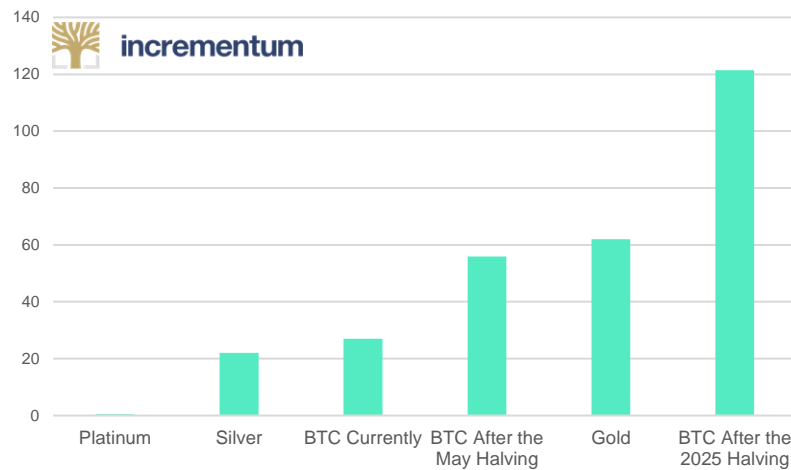
► How much gold is available depends on how much gold has been provided by Mother Nature and how easy or difficult it is to mine. For Bitcoin, the amount does not depend on exogenous factors, but on the computer code defined in the protocol, which limits the maximum amount of Bitcoins to 21 million pieces.

2. The Difficulty of Extraction or The Extraction of the Raw Material.

► Extracting gold is complex, and therefore, expensive. The material wear and tear, energy consumption as well as the labour input of the extraction is high. Mining new Bitcoin is also costly. Hardware, software, specific know-how and above all a lot of electricity is needed to provide the network with computing power and thus to secure and operate it.

Similar to gold, Bitcoin is both scarce and expensive to extract. Therefore, an analysis of the price development of Bitcoin with the SF model, which was originally designed for commodities, seems to be reasonable due to its similarity to gold.

Figure 5: Bitcoin vs. Gold - Stock-to-Flow-Ratio



Source: Medium Original Article, ZPX, Satoshi & Co. Research

The Quantitative Valuation of “Plan B”

A special feature of the Bitcoin protocol is that the code already determines how the Bitcoins offering - and thus the stock to flow ratio - will develop in the future.



By way of comparison, in the case of gold or silver, for example, it cannot be completely ruled out that one day a huge find will be made, and the flow will shoot up, because more can be mined.

The maximum number of Bitcoins is 21 million (maximum stock). The number of newly generated Bitcoins is also fixed (flow). However, the Bitcoin flow is not constant over time. Every 210,000 blocks the so-called "block-reward" is halved. This is the number of Bitcoins that the successful miner receives for its validation services. Miners currently receive 12.5 Bitcoins per block, but the next "halving" will take place in May of this year. From then on, only 6.25 Bitcoins per block will be "mined".



The “Halvings” lead to:

1. Inflation of Bitcoin getting smaller and smaller until it reaches zero.
2. An increasing SF ratio as the flow is halved.



Since Bitcoin is denominated to eight decimal places, the reward per block will arrive at 0 exactly after the 33rd "halving". Based on a halving every four years, the last Bitcoin will therefore be mined in 2140.

Table 1 Development of the "Block Rewards"

Period	Number of New Bitcoins per Block
Genesis Block – November 2012	50
November 2012 – July 2016	25
July 2016 – May 2020	12,5
May 2020 ~ May 2024	6,25
May 2024 ~ May 2028	3,125

Source: Incrementum AG

Plan B examined a total of 111 data points between December 2009 and February 2019 and determined the respective market capitalization of Bitcoin and the corresponding SF ratio.



Because the S2F ratio is constantly increasing, time is already included in the model as an exogenous variable.

Then the author pulled the data and one thing was immediately apparent: The higher the SF ratio, the greater the market capitalization. If one regresses the rising stock to flow ratio with the logarithmic price time series of Bitcoin, one finds a surprisingly high explanatory value. The correlation can also be seen with the naked eye.



The natural logarithm was used. This makes it possible to show the correlation of both quantities linearly and thus opens up possibilities for a solid statistical investigation.

Important Links:

[Live BTC Stock-to-Flow:](#)

DIGITALIK:

<https://digitalik.net/btc>

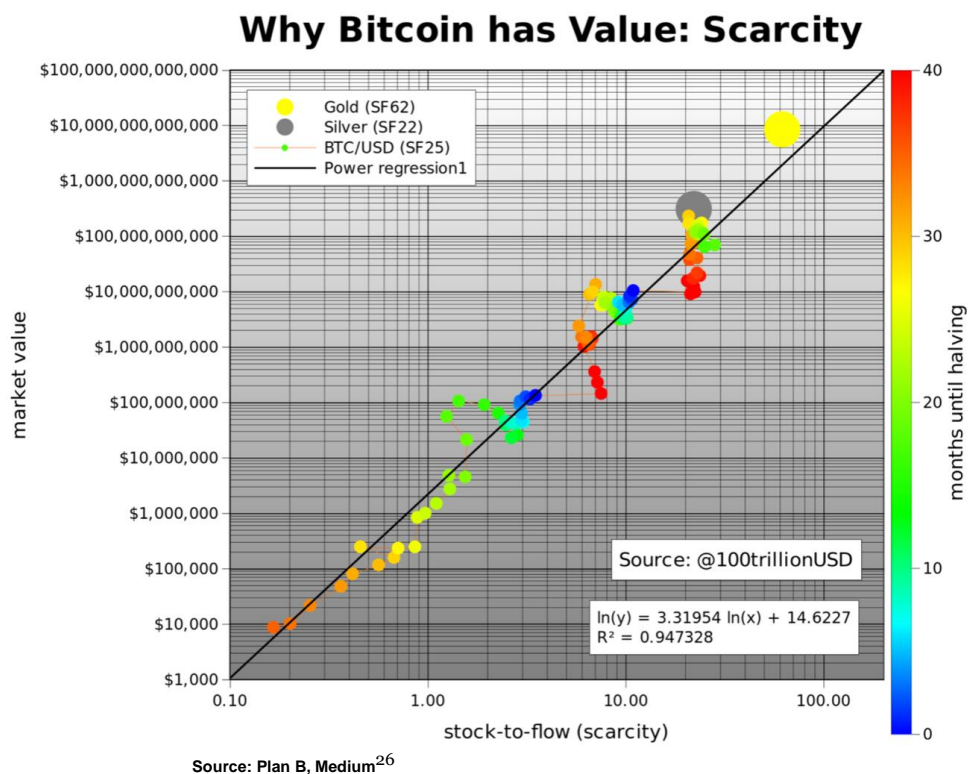
LOOKINTOBitcoin:

<https://www.lookintobitcoin.com/charts/stock-to-flow-model/>

The Original Article:

<https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25>

Figure 6: Plan B's Infamous Graphic



Source: Plan B, Medium²⁶

For the Number Crunchers:

If one models the price of BTC directly by SF and converts the resulting formula

$$\ln(\text{Market Capitalization}) = 3.3 * \ln(SF) + 14.6$$

Then you get the law of potency:

$$\text{Market Capitalization} = \text{Exp}(14.6) * SF^{3.3}$$

In Plan B's infamous stock to flow chart, the small dots represent Bitcoin's historical price data over time. The large grey and yellow dots show the respective market capitalization of silver and gold and their respective stock to flow ratio. The regression suggests what can be seen with the naked eye: a statistically significant relationship between S2F Ratio and the market capitalization of Bitcoin.

For the Number Crunchers:

Test Data of the Regression:

$R^2: 0.95$

$F\text{-Test}: 2.3E-17$

$P\text{-Value}: 2.3E-17$

Plan B argues that the correlation is so strong that the dominant driver for the price must be scarcity, or SF ratio. However, the author also acknowledges that other factors such as regulatory measures, hacks, and other news have an impact on the price; therefore, not all the data points are perfectly in line. The fact that the S2F ratio of gold and silver also fits very well into the picture is a further validation of the model.

Since the "halvings" have such a great influence on the SF ratio, Plan B has color-coded the months until the next "halving" in the chart. Dark blue are the halving months and red are the points shortly after the "halving". The current S2F ratio of ~25 will thus double to ~50 in May 2020, which is already close to the S2F value of gold. Based on this model, the forecast market value for Bitcoin after halving in May 2020 is \$1 trillion, which would correspond to a Bitcoin price of \$55,000.

Further Models

We dug a little deeper and found out that there were already several variants of the model that Plan B calculated:

²⁶ <https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25>

Points of Criticism with the “Plan B” Model

- The model is based purely on the supply side (maximum number, Bitcoins per block, etc.) and does not take into account the demand for Bitcoins.
- Regulatory measures, possible hacks, etc., i.e. (largely non-quantifiable) control variables, are not included or built into the model.
- Historical data is not a source of forecasts.
- The statistical correlation between the SF ratio and the price of Bitcoin is not a causality, only a correlation.
- If the model is correct, this should already be reflected in the prices.
- At some point Bitcoin will become truly deflationary (the loss of BTC per year would exceed the annual mining production), resulting in a negative SF ratio. What happens to the price then cannot be predicted by the model.
- Lack of stationarity of the data.
- The high R2- value could be a consequence of the missing stationarity of the data.
- The empirical work of Plan B is not precisely documented, which makes it difficult to find methodological weaknesses.

► Due to the fact that the original model was based on figures up to December 2018, additional monthly data could be included in the model. In addition, historical data research made it possible to incorporate figures back to September 2009 into the model. These data extensions resulted in new price estimates for Bitcoin after the halving. These vary between 60,000 and 90,000 and are therefore higher than the value predicted by the original model.

► Another variant of the model is based purely on the data before November 2012, i.e. no halving has taken place before that date. This model would have anticipated a tenfold increase in the Bitcoin price for both halvings (2012 and 2016). Using this "out-of-sample" variant of the model, one gets a price estimate of USD 100,000 after the next halving.²⁷

Another interesting model is the so-called "time-based model", as it explains the increase in the value of Bitcoin over time with a different underlying causality. The model states that Bitcoin increases in value as more and more market participants know about Bitcoin, deal with it and take the step to buy it. The narrative for the increase in value is thus the adoption, but not the scarcity (S2F). The estimates of this model are more conservative, and it is assumed that the price of Bitcoin will not break the \$100,000 barrier until

2021-2028.

Table 2: Bitcoin Price Development Model Overview

Model	<i>Original Model (Until Dec 2018)</i>	<i>“Additional Data Model”</i>	<i>“Out of Sample” Model</i>	<i>“Time-Based” Model</i>
Value After the 2020- Halving	55,000 USD	60,000 to 9,000 USD	100,000 USD	Between 2021 & 2028: 100,000 USD
Special Feature	The first rapidly spreading model for price evaluation of Bitcoin with scarcity as proxy.	Supplements "The Original" with additional data (older and younger).	Uses only data prior to November 2012, so no halving has occurred in the data set yet.	The reason for the price growth in this model is the progressive adoption of Bitcoin.

Source: Incrementum AG, Plan B

²⁷ See Stephan Livera and Plan B, Nov 4, 2019
<https://stephanlivera.com/episode/122/>

"S2F and price are proportional and react and change proportionally."

Plan B,
Stephan Livera Podcast
November 2019

The Law of Potency

Definition: "A power law is a relation in which a relative change of one quantity leads to a proportional relative change of the other quantity - independent of the initial quantity of these quantities".

Exactly such a law of potency emerges when one examines the regression of the "original model": At each halving, the SF ratio doubles, and market capitalization increases tenfold - this is a constant factor. Plan B therefore suggests:

"The possibility of a power law with a 95% R2 over eight orders of magnitude makes me confident that the main driver of the Bitcoin value is correctly captured by the SF ratio".

Conclusion

The stock-to-flow model has shaped the crypto year 2019 like no other development. The accuracy with which the model traces price developments of the past is outstanding. It was also possible to observe how the model drove additional researchers and critics to take a closer look at the price development of Bitcoin. In the medium and long term, this invested human capital will contribute to a better understanding of the crypto world and its adoption to a broader population. The partly heavily criticized Model from "Plan B" will have the opportunity to prove itself as a forward-looking achievement starting this May - and it deserves exactly this opportunity.

The Stock to Flow Model: Mark Valek's Exclusive Interview with "Plan B"

"I read the whitepaper regarding Bitcoin, was hooked and went down the rabbit hole."

Plan B

Key Takeaways

- ◆ When asked if the Bitcoin Halving is Already Priced In, Plan B Says "No."
- ◆ Plan B says that Bitcoin has done a 10x increase during the last halvings, and his model forecasts this trend to continue.
- ◆ The largest critique of Plan B's Stock to Flow Ratio Model is that it does not consider demand. Plan B answers this critique by saying that many famous financial pricing models including Capital Asset Pricing Model and the Black & Scholes Model do not consider demand.



Plan B is blogging under a pseudonym. Who exactly is behind this baseball cap remains unknown. We also asked him some personal questions in this interview. His signature looks like this: His Twitter handle is: @100trillion USD.

Plan B, When Will You Show Yourself?

As explained in the previous chapter, we arranged an interview with the father of the "Stock-to-Flow Model". Plan B says that Bitcoin is here to stay. He also expects the price explosion of Bitcoin to be foreseen by his model. Why he is so sure about this? How does he deal with critics? Will he ever take off his cap and show his face?

Mark: Plan B, almost a year ago the publication of your model really shook up the entire crypto community. How do you deal with all this attention you and your model have received? What have you experienced this past year?

- ▶ **Plan B:** It has been a very interesting year since the publication of the article March 22nd 2019. The paper was well received and I gained valuable feedback from econometricians and math/stats people all over the world. I love the interaction with the community and the open source vision of sharing knowledge. I really enjoyed doing the podcasts. With 60k followers and a full-time job, I do have to make choices. It is almost impossible to read all the comments, DM's (Direct Messages), Telegram messages, WhatsApp messages, emails, and I hope everybody understands. I want to keep focused on analysis, investing, and writing more articles.

Mark: Can you tell us, what you do for a living and why do you use a pseudonym?

- ▶ **Plan B:** I am both an analyst & investor at an investment office of a large institutional investor in the Netherlands. As a team we invest \$50+ Billion AUM. My main focus is on mortgages, loans, and structured finance. I do not want my employer to have any negative consequences from my Bitcoin "hobby". Also, I consider it good operational security to remain anonymous.

Mark: Where did your interest in Bitcoin come from?

- ▶ **Plan B:** If you have seen the movie The Big Short (2015), that was my life from 2007-2008: CDO's (Collateralized Debt Obligations), ABS (Asset Backed Securities), and RMBS (Residential Mortgage Backed Securities) etc. The craziness of negative interest rates and QE (Quantitative Easing) forced me to rethink everything I knew about finance. So, I was actively looking for QE hedges in 2013 and found an article about Bitcoin on the website Zerotohedge. I read the whitepaper, was hooked and went down the rabbit hole.

Mark: Why did you start to model the value of Bitcoin?

- ▶ **Plan B:** I started modeling because I wanted to know what drives Bitcoin's price. I noticed that there was a lot of technical analysis, but not much statistics / econometrics modeling. So, I tried to make a more fundamental model, based on Bitcoin value: it's scarcity.

Mark: In our “In Gold We Trust Reports” we have been writing about the S2F ratio of Gold and Silver for many years. It's great, that through your model, this concept of scarcity has been introduced to an even greater community. In terms of terminology, however, we prefer to talk about constancy, rather than scarcity when talking about SF (Stock to Flow). A higher SF ratio indicates a more constant quantity rather than a scarcer quantity of the good (as a higher scarcity indicates that the quantity actually goes down). Even though this is just a minor differentiation in terminology, we think that this could be helpful for a more intuitive understanding of the S2F concept. What are your thoughts in this respect?

- ▶ **Plan B:** Unforgeable scarcity (Nick Szabo) is a well know concept in the Bitcoin community, so I see SF as a nice quantification of that concept. Frankly I think some people in the “commodity community” don't have a very good definition of scarcity. For example, I talked to a lot of commodities investors that think platinum is scarcer than gold because there is less platinum in the world than gold. I prefer the definition of scarcity that relates production (flow) to stock. You could also interpret this as inability of producers to influence stock (and thus price): with oil producers have much influence, and with gold less. Maybe your definition of “constancy” is the same? This is something we should discuss further.

“The Drunk & His Dog” Analogy

The drunken sailor goes out with his dog on a leash, wanders around in a random fashion and the dog has to stay with him, but sometimes he is on the right, sometimes on the left, but he cannot go any further as he is on a leash

You don't know where the drunken sailor and the dog are going, but you do know they stay together.

Mark: Could you please explain to us the analogy regarding “the drunk and his dog” again and tell us the meaning for our readership?

- ▶ **Plan B:** The drunk and his dog story is a popular story to explain cointegration. Correlation is about how two series move together. Cointegration is about two series staying together. So, the drunk walks a random unpredictable path, and his dog too, but the distance between the drunk and the dog is predictable, it is never larger than the leash. So, without knowing where the drunk or dog are going, we can predict they stay together. With stock-to-flow and Bitcoin it is special case of course, because we know where one of the two is going: SF. Cointegration is used to test if correlation is spurious or real: no cointegration = spurious. SF and BTC are cointegrated, so they are likely (no guarantee) not spurious.

Mark: Your model has occasionally been criticized – that it only explains the Bitcoin price in reference to Bitcoin supply. If this is even possible, how do you incorporate demand?

Why Current Prices of BTC Do Not Reflect the Predictions of the SF-Model

A. Are people too dumb to get it?

- ▶ **Plan B:** No, it is enough if some people get it. Like with insider information, if only 10-100 get it, they will move the price. Dumb money is formally “noise” according to the EMH (Efficient Market Hypothesis), it is irrelevant.

B. Is it bad model?

- ▶ **Plan B:** I think the cointegration is real, so the model is good. So far, I have not seen anything better.

C. Are the ones that “get it” already invested?

- ▶ **Plan B:** Most will be invested, but I think that many who “get it”, also see the big risks such as government bans, a software bug, “the next Bitcoin”, death spiral, etc. These risks prevent them from going all in. Actually, this is true for myself as well: I am invested, but not 100%; if I knew 100% certain Bitcoin would go to \$100k USD in 2021, I would go all in and even lend money.

D. Are the markets inefficient?

- ▶ **Plan B:** No, the markets are efficient. Also, the \$150 Billion Bitcoin market is efficient, as I have shown in the FX (Foreign Exchange) example in my article. Easy arbitrage between BTC/USD, BTC/EUR, and BTC/JPY markets is not possible.

E. Do people know about the model?

- ▶ **Plan B:** Enough people know about it. I have 60k followers on Twitter and many of them are investment bankers, quants, miners, venture capitalists, hedge-fund CEO’s, and CIO’s, etc. The SF model was featured in MSNBC and in Forbes.

- ▶ **Plan B:** People that use the demand argument probably don’t have a statistics or investing background. The argument is theoretically right (price is a function of supply and demand) but there are a lot of famous pricing models that do not use demand (or supply) as input and still give good predictions. Some examples of this are the CAPM (Capital Asset Pricing Model) and Black & Scholes model, as both price with only risk / volatility (standard deviation, etc). The demand argument is really based on ignorance.

Mark: Let’s now throw a new thought into the equation: The model tries to explain the price of Bitcoin in USD. We know, that measuring value in fiat money over time is difficult, as fiat currencies are designed to be permanently inflated. In our mind, the model implicitly does not take into account fiat money inflation. If say, – at least for the sake of a thought experiment – the USD would hyperinflate within the next years, we would expect the model to vastly underestimate the USD value of Bitcoins. What are your thoughts regarding the dollar-inflation in regard to SF model?

- ▶ **Plan B:** It is true that the SF model doesn’t correct for inflation. If we would do that, we probably see not much difference anyway because from 2009-2019 inflation was low. And indeed, in my opinion the SF model predicts USD hyperinflation because Bitcoin USD does this 10x every 4 years. Many people have problems with this thought, but for me it is not an improbable scenario, given negative interest rates and what central banks are doing with QE: they are going full Zimbabwe in my opinion.

Mark: What is the deal with the artist you commissioned? (The artist is going to make an artwork out of the charts).

Plan B: The artist Petek was intrigued by the charts and she asked permission to paint it. It will be a unique painting with some special elements that are yet to be revealed. It is exciting to see that a lot of other people are inspired as well and are commissioning a similar SF painting. Her idea is that she will make a series of paintings using different colors and materials based on SF. I think Bitcoin is not only about programming and money but also about a movement and a revolution. Art and science are two sides of the same thing, they belong together.

Mark: What other projects are you currently working on?

Plan B: I am cooperating with other Bitcoiners on research and writing more articles. I am working together with some investment funds, also traditional institutes, finding ways to include an exotic investment like Bitcoin in the existing asset mix. Also, I am doing chain-analytics, crunching the 300GB blockchain to find more patterns that can give insights and be used for proprietary trading, that is really uncharted territory.

Mark: (When) can we expect an outing of Plan B?

Plan B: I think the chances of me going dark are higher than an outing. I have no desire to become a public figure. Especially when the model works, which I hope and expect of course. People that want to meet me know where to find me, through my network, and everybody can verify it is me by my cryptographic signature (like on the articles).

Storing Bitcoin the safe and easy way



With the Card Wallet by Coinfinity and
the Austrian State Printing House

www.cardwallet.com

Image: Renaissance cassette, courtesy of Schell Collection

You constantly hear it on the news: Bitcoin wallets get hacked, people forget their passwords, and lose their data.

**Storing Bitcoin in the long run is complicated.
The Card Wallet makes it easy.**

All you have to do is keep the card in a safe place - we take care of the rest. The Card Wallet is a co-production of **Coinfinity** and the **Austrian State Printing House**, and provides

- The ability to store Bitcoin as a physical good like gold
- Protection against hacking attacks through offline storage
- Easy handling, even without technical knowledge
- A simple way to gift, transfer, or pass on Bitcoin

Combine the Card Wallet with the Bitcoin savings plan, a recurring purchase via standing order without any binding contract.

Get more information at www.cardwallet.com

coinfinity

BRINGING BITCOIN TO THE PEOPLE

For years, our company has stood for trustworthiness, individual support, and professional brokerage of Bitcoin and other digital assets.

A comprehensive customer service is very important to us. Feel free to contact us, we look forward to hearing from you.

+43 316 711 744 | office@coinfinity.co

For purchases over € 100,000 please directly contact our compliance department via compliance@coinfinity.co

www.coinfinity.co

Crypto Custody: What's new in Germany

“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
Hedge Fund Manager at Multicoïn Capital*

Key Takeaways

- ◆ Storage of digital assets is quite different compared to storing gold since digital assets only exist virtually. Cryptographically secured digital assets are accessed and controlled by a private key which is a sequence of numbers and letters. This private key must be stored securely in an analogic way.
- ◆ Self-custody requires a basic understanding of the technology behind public private key cryptography. The mechanics of private keys must be understood in order to store digital assets safely and prevent loss or theft.
- ◆ The 5th AML directive by the EU gives a guideline on the further regulation of digital assets. Member states are executing the directive differently, with Germany pioneering in the issuance of a crypto custody license.



Daniel Wingen

We want to sincerely thank Daniel Wingen and The Value of Bitcoin Conference for contributing this chapter. Daniel is a Bitcoin Researcher for The Value of Bitcoin Conference. Our readers can register online for their next upcoming conference this June 2020 in Munich, Germany (<https://www.vob-conference.com/>).

In the January 2019 edition of the [Crypto Research Report](#), we extensively covered institutional grade cryptocurrency custody. We interviewed three firms in the space including Crypto Vault AG, Crypto Storage AG, and Coinfinity. This article explains custody from the perspective of a user, including information on how to store keys privately, and what questions to ask when considering using a storage company.

Storing Digital Assets in a Digital High Security Vault

“Custodians are necessary as the next step towards crypto-assets being seen as a safe and attractive financial asset option for large FIs and perhaps for market confidence in general... Major institutional custodians providing a secure place to store large amounts of crypto-assets could provide the protection necessary to reduce the risk of hacks and increase the trust of the investing public in crypto-assets.”

Attorneys at Perkins Coie

Storing your gold or other physical assets comes with two options: either at a facility you completely control in all aspects (self-custody) or at a service provider, who holds the assets in your name secured in a facility you have no access to (service custody). The same principle applies for storing your digital assets like bitcoin. However, digital assets require a digital vault to provide the highest security standards. But what exactly needs to be stored safely in case of digital assets? It is the so called “private key” which provides access and control over the digital asset and thus the right to transfer it to someone else. In the case of Bitcoin, the private key is a 256-bit number represented in hexadecimal form. Storing these keys is basically a physical issue as they could be simply written on a piece of paper or engraved in metal and put into a safe deposit box to limit physical access and digital exposure to the internet where they could potentially be accessed and copied by a hacker. As a private key is needed to sign a transaction (prove ownership), software is required to execute the signature generating process and the key needs to be revealed to this software. In order to facilitate this procedure, specific hardware wallets were introduced which enable not only a hardware secured environment for generating the necessary signatures without exposing the key to the internet, but also can handle an infinite amount of keys deriving from a master private key following a standardized process. This standardization of key derivation enables users to backup just the master private key and recover all necessary keys on a new device in case of malfunction or loss.

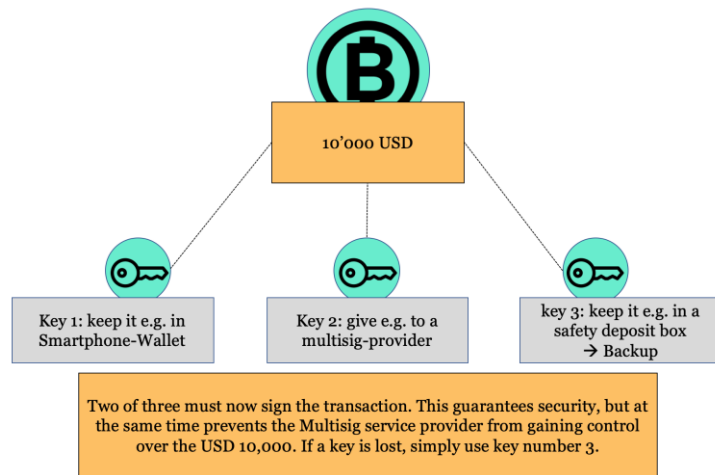


Using only N of M private keys makes it possible to store e.g. another key somewhere as a backup. Should one of the keys be stolen or lost, the secured Mth key can be retrieved.

The next step to attain an even higher level of security would require one to build something which could be described as a digital vault. A digital vault typically involves the creation of multiple master private keys and storage of them on special hardware wallets with secure elements at different geographic locations. The transaction then needs to be signed by N out of M private keys depending on the spending rules implemented when originally receiving the funds. This concept is called multisig - short for “multi signature scheme”.

In order to deal with malfunction of key storage hardware, a proper backup plan is crucial. The most common practice is to either perform a so-called key rotation or to securely store encrypted backups to be able to recover the master private keys. Both methods come with advantages and drawbacks.

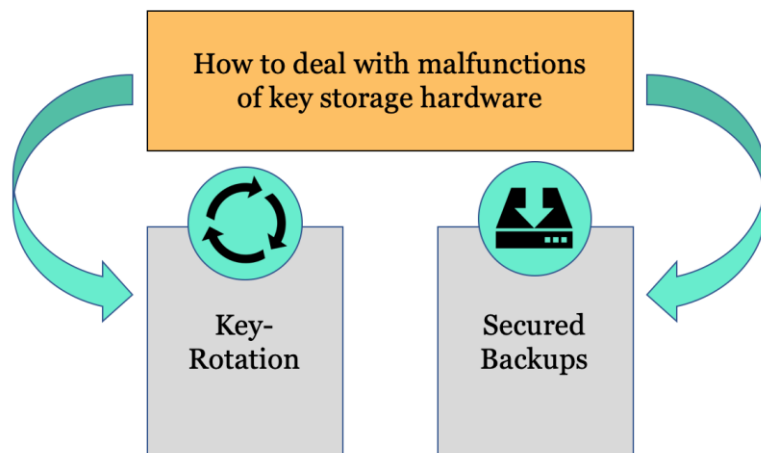
Figure 7: Example of a "Multisig-Scheme"



Source: Incrementum AG, Daniel Wingen

The execution of a key rotation becomes necessary if one decides that the master private key should never leave the secure element of the hardware wallet, which makes backups impossible. This is great for reducing attack vectors as long no

Figure 8: Two major ways of protection against hardware-malfuntions



Source: Incrementum AG, Daniel Wingen



A key rotation scheme means that you have to replace the entire set of keys. This is because if you lose one of three and you need two out of three keys to sign a transaction, you have to act quickly. The coins need to be moved to a new address where you again own all three keys, because if one additional key would be lost, all the coins are lost forever.

device malfunctions, but if there is an incident, all funds need to be moved to a setup of completely new generated master private keys. Moving millions or even billions worth in digital assets is a very critical and expensive endeavor which takes time and introduces a lot of attack vectors if not planned and executed accurately. Backing up the master private keys on the other side also opens a new attack vector for collusion or social engineering to extract the private keys.



Social engineering can be described as a psychological strategy in which attempts are made to gain access to digital safes through targeted manipulation.

Attempts in this context means that company employees come together internally to gain access to digital safes.

This means a well-functioning digital vault for digital assets requires an elaborate technical solution for:

- ▶ key generation
- ▶ signing procedure
- ▶ the storage of private keys (and backups) at different geographic locations.

Social engineering can be imagined as a psychological strategy in which attempts are made to gain access to digital safes through targeted manipulation.

But apart from that, a well-designed digital vault should have further features to make it more secure. First, we have a closer look on how the private key is stored ideally before we go into more details on the signing of transactions.

“From the perspective of IT security, the aspects of recognition performance and security are of particular importance when considering biometrics.”

Federal Office for Information
Security, Germany

In general, it is very common to secure devices which hold the private keys in a physically secured bank vault which is similar to gold storage, however, there are some important differences. To begin, the devices on which the private keys are stored should be protected with additional digital security measures. Only specific predetermined persons may access the device with identification through biometric data such as fingerprint. In addition, entry is only allowed at specific predefined times or else if specifically authorized by the board of directors of the company operating the digital vault. This reduces the probability of unwanted signature generating events virtually to zero.

Most importantly, only transactions authorized by a predefined quorum of decision makers may be signed with the corresponding private keys. In order to achieve that, typically an additional cryptographically secured authorization layer is put in place. This layer is an addition to the cryptography securing the digital

asset itself. Each digital vault operator defines its own authorization processes which can be adapted to different internal processes or client needs. For example, one could agree that the authorization process of a transaction must involve at least three people on the client side signing a transaction approval with their individual authorization keys stored on personal security devices. The authorization process should involve biometric data or other second factors like chip and pin. In order to prevent theft by colluding employees within a custodian, it is reasonable to include a business logic that *technically* requires the authorization by

Cold vs. Hot Storage Custody of Cryptocurrencies

If the wallet is connected to the Internet, this private key is exposed to potential hacker attacks. Because of the online connection to internet, this type of storage is called hot storage.

A cold wallet, in contrast, is a storage space that is not connected to the Internet. The keys with which you can manage your digital money are stored offline. This of course reduces the risk of DDoS attacks and hacker attacks considerably.

the client. However, the board of directors could mutually change the business logic of the authorization layer to access the digital assets without authorization by



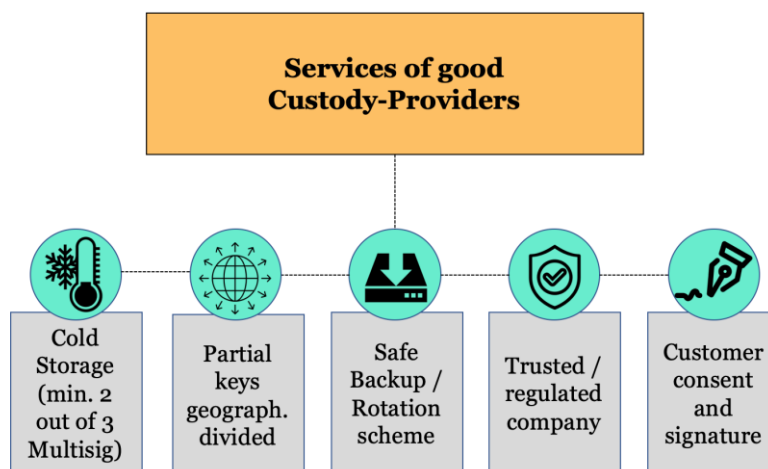
An example of such a BCM rule could be this: Nobody can access the safe deposit box which stores the backups without having registered with the safe company a week in advance. Upon this “one-week in advance registration”, everyone in the company would receive an email/SMS message announcing the registration. Then, only one person with biometric data and/or two-factor authentication can access it on that day at that specific time. In addition, in order to change this rule with the vault company, a quorum of management approvals through formal request and verification would be required. A similar approach could be established for hardware wallets to access them for firmware updates. This could be in the form of a certain quorum of signatures from managers that would be required to overwrite the bootloader and allow firmware updates etc.

the client. They could even just access the master key backups directly if not properly secured through profound business continuity management (BCM). This is why it is important to rely on a custody provider with trustworthy management that is audited by regulatory authorities. Also, the custody provider must show a thoughtfully implemented segregation of duties since human interaction is the most critical point of failure.

If you plan to store your digital assets at a custody service provider, it is of utmost importance to check their technical solution on whether it is designed according to industry standards which reduces risk for loss, theft and fraud of private keys to the lowest possible. **A good custody provider should provide the following:**

- ▶ A digital vault (cold storage) with at least 2 out of 3 multisig.
- ▶ Distribution of partial keys on different geographic locations in countries which are considered to have a stable system in regard to respecting proprietary rights (USA, Singapore, Switzerland, Germany, etc).
- ▶ Safe backup of the private key which should again be distributed geographically, or alternatively, a sophisticated key rotation scheme.
- ▶ Trustworthy management audited by regulatory authorities.
- ▶ Authorization layer that requires customers’ consent to sign transactions.

Figure 9: Services of a good custody provider



Source: Incrementum AG, Daniel Wingen

Self Custody vs Serviced Custody

“James Howells is a multi-millionaire - and somehow not. Thousands of Bitcoins are slumbering on his hard drive, which is now worth 75 million euros. The catch: The hard disk is buried in a dump.”

N-TV.de

The above chapter showed that the process of setting up and maintaining a digital vault to secure a significant amount of digital assets does require a lot of specialized knowledge and well thought through security procedures. Such a complex setup is currently hardly feasible for a private person or small company without investing a significant amount of resources in research and development. This will very likely change in the future, but currently self-custody always comes with reduced security if proper knowledge and secure technical implementation is absent. To achieve a certain level of security, one has to know the technology quite well and understand the digital assets specific mechanics of the public private key methods used. Then, one needs to store the private key safely in a way that it cannot easily be stolen or lost. If the private key is lost, then the digital assets cannot be accessed by anyone anymore which equals a total loss of the assets. Understanding the technical mechanisms of accessing digital assets with a private key requires time and can be very difficult to grasp for the less tech savvy people. In addition, one needs to make sure that one's heirs may obtain access but only when the time has come. This problem can be easily solved with serviced custody, but it is rather difficult to solve in self custody. Self-custody for corporations is even more complex since access to the private keys must be split and distributed to several people to ensure that no single person has access to all funds. If only one person had access and this person gets involved in a deadly accident, then all funds of the corporation would be gone - a situation which shall never occur. Depending on the jurisdiction, financial service providers are even obliged by regulation to store their assets under management in custody. In Germany, however, the separation between financial service companies and custody was eliminated by law.



The obligation to hold the assets under management means no more than that the funds must be placed externally within a depositary.

The idea behind Bitcoin, however, is decentralization and censorship resistance. Bitcoin technology hands people back their financial self-sovereignty and creates a

level playing field where every individual, company or bank has the same entry barriers to transfer the asset globally with near instant settlement - but only if one controls the private keys. In line with this, there is a common perception of “not your keys not your bitcoin” which encourages self-custody.²⁸ We see it as reasonable to have a balanced perspective on self-custody and serviced custody by looking at the pros and cons of both. Deciding on the custody solution for your digital assets should include:

- ▶ your knowledge on the technical solution,
- ▶ the general pros and cons of the options as well as
- ▶ the amount of funds to be stored
- ▶ and the specific use case.

Private individuals can simply store smaller amounts of digital assets with consumer grade hardware wallets which are easy to use and provide reasonable security if handled with care and a basic knowledge of the mechanics involved.

Regulatory Developments in DACH

“New obligated parties (of the 5th AML Directive) are platforms for exchanging virtual currencies and providers of electronic purses (wallets) for virtual currencies (e.g. Bitcoin) etc.”

Paytechlaw.com

The 5th Anti-Money Laundering (AML) Directive is the most important regulation for digital assets in the European Union so far. The directive lays out the anti-money laundering obligations imposed on cryptocurrency businesses which includes the requirement for Know Your Customer (KYC) processes to identify customers. This legislation provides more clarity for national states and businesses on how digital assets are regulated.

Germany pioneered the issuance of crypto custody licenses that came into effect on the 1.1.2020. Crypto custodians now have to apply for a “Kryptoverwahrer” license to provide custody services for digital assets, however, existing custodians are allowed to keep up their business until a decision on the license application is made by the BaFin, the German financial market authority.

Austria made amendments to their Austrian Financial Markets Anti-Money Laundering Act (“FM-AMLA”) and the Beneficial Owners Register Act (“BORA”). Crypto Custodians need to be registered with the Financial Market Authority since 10.1.2020. In Austria, no license is needed to provide crypto custody service. The AML amendments merely require enhanced due diligence measures if a high-risk third country is involved in a transaction.²⁹

The 5th AML directive does not apply to Switzerland since the directive is EU law. According to the Swiss Financial Market Supervisory Authority FINMA, “Switzerland has always applied the Anti-Money Laundering Act to blockchain service providers”.³⁰ In 2019, FINMA granted SEBA Crypto AG and Sygnum Bank AG a full banking and securities dealer license.³¹

²⁸ A detailed report on self-custody can be found here for free: <https://www.smartcustody.com>

²⁹ https://www.schoenherr.eu/publications/publication-detail/the-impact-of-the-5th-anti-money-laundering-directive/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original

³⁰ FINMA Guidance 02/2019 <https://www.finma.ch/finma-aufsichtsmittelungen>

³¹ <https://www.cplaw.ch/2019/finma-grants-banking-licenses-to-new-swiss-crypto-banks-introduces-new-strict-aml-rules-regarding-payments-on-blockchain/>

“[Custody] 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.”

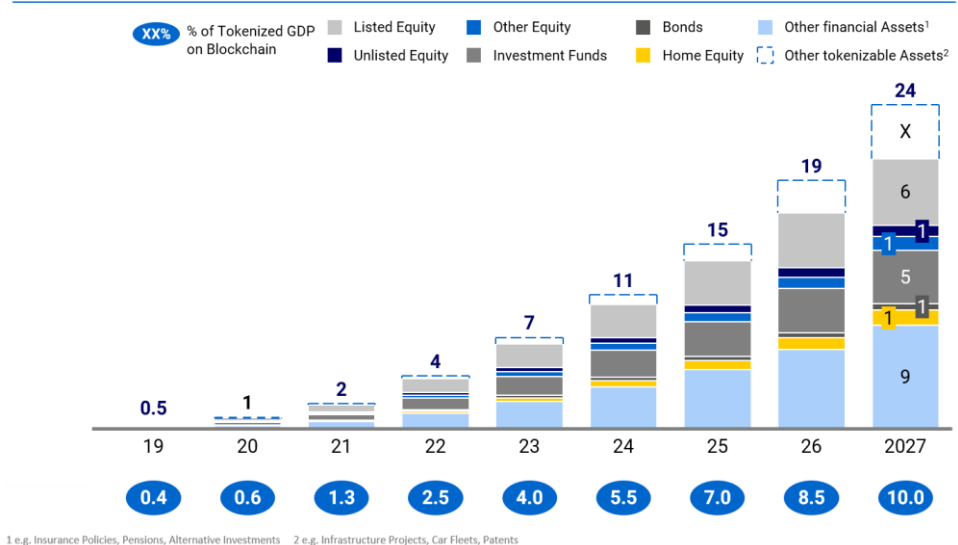
Mike Belshe,
Co-Gründer & CEO von BitGo

Global State of Custody Service Providers

We have identified more than 20 custody providers operating at the end of 2019 with Coinbase, BitGo and Bakkt being the largest. Coinbase has become famous with its exchange services. The company is managing assets with a value of USD 7bn in 2019.³² Bakkt is created by CE the company behind NYSE and known for introducing Bitcoin futures that are fully backed with “physical Bitcoins” - in line with the company’s name. This means that the bitcoin to fulfill a buy position that is scheduled for the future is already available by Bakkt. BitGo provides clearing and settlement services that are connected to several exchanges, OTCs, hedge funds and more. The customer may decide which party to choose and to settle a trade with while the funds are locked during settlement which minimizes counterparty risk.

Figure 10: Projected Tokenized Market Volume until 2027

Projected Tokenized Market Volume until 2027, in \$trn by asset class



Source: Finoa AG, finoa.io³³

In Germany, ING Diba, the most famous direct bank, announced to apply for the crypto custody license³⁴ as well as Solaris Bank, the banking as a service provider for startups³⁵. According to Finoa, a Germany based custody provider, the amount of tokenized assets under custody will reach 1 trillion by 2020 and 24 trillion by 2027. However, these statistics mostly focuses on equity, debt and tokenized real estate, neglecting the expected increase of Bitcoin market capitalization according to the Stock-to-Flow model.³⁶

³² <https://blog.coinbase.com/coinbase-custody-acquires-xapos-institutional-business-becoming-the-world-s-largest-crypto-2c1b46fc94c4>

³³ <https://hackernoon.com/market-outlook-on-tokenized-assets-a-usd24trn-opportunity-9bac0c4dfeff>

³⁴ <https://www.reuters.com/article/us-crypto-currencies-ing-exclusive/exclusive-ing-working-on-digital-assets-custody-technology-sources-idUSKBN1YF2GN>

³⁵ <https://solarisbank.pr.co/184220-solarisbank-launches-subsidiary-solaris-digital-assets-to-drive-adoption-of-crypto-and-further-digital-assets>

³⁶ <https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25>



Value of Bitcoin
Conference 2020

Bitcoin: the money of the future?

VoB is a dialogue platform for professionals bringing together researchers, investors, bankers, regulators and journalists to debate the most fundamental questions around the value of Bitcoin.

JUNE 2-3, 2020 | MUNICH, GERMANY

Alte Kongresshalle, Am Bavariapark 14, 80339 Munich

vob-conference.com

20% Discount Voucher: CRR20

Bitcoin vs. Gold – a Fictitious Debate

Since we have been quite involved with the topics of Gold and Bitcoin for several years, we have already held several discussions on the subject of investing in Gold and Bitcoin. In the form of a (fictitious) debate between a proponent of gold investments (XAU) and a proponent of the cryptocurrency Bitcoin (BTC), we want to dialogue some frequently discussed points such as the similarities, differences and opportunities of these two forms of investment.



Gold has fascinated humanity for thousands of years.

Source: Unsplash.com



Bitcoin is a relatively new technology. Is it becoming the gold of the digital world?

Source: Unsplash.com

BTC: Dear GOLDBUG, I am pleased that we have met here today. I am quite curious if I can convince you that there are some parallels between gold and Bitcoin, and that Bitcoin definitely has a place in the market or will become much more important.

XAU: Thanks for the invitation! As you know, as a rather conservative investor I am very critical of the crypto world, but I am always open to a good argument.

BTC: This is a good basis on which we can build our conversation. Let us start by discussing the differences and similarities between Bitcoin and gold. What are your thoughts?

XAU: That's a great idea! While I did notice that there is a huge trend towards digitalization these days, it stops with me when it comes to the investment of value. This is because gold is a precious metal. You can touch it and it has always imposed an almost mystical fascination on people— especially my wife.

BTC: Sure, but there is a fundamental difference. gold is a chemical element, it exists physically, it can be touched as you say, and admittedly it does have rather interesting properties. But Bitcoin on the other hand, is an open protocol that only exists digitally as bits and bytes. Bitcoin is ultimately a groundbreaking innovation and has managed to successfully give digital information scarcity for the first time!

XAU: What does that mean?

BTC: For example, if you send someone an email, you are not actually transferring your own data. You send a copy of your data. Ultimately the data will be available to both you and the recipient afterwards. Until the invention of Bitcoin and the associated blockchain technology, it was not possible to make digital information definitively transferable, i.e. that it "goes from me to you and is no longer with me afterwards".

XAU: Okay, I'm following so far. I can even concede that this is indeed a groundbreaking invention. But how do I know this transmission will work safely? Everything on the Internet is hackable!

BTC: The inventor of Bitcoin created a very intelligent reward system for the people involved in securing the network. These so-called "miners" fulfill the task of verifying that each transaction is valid and is only actually executed once. The same Bitcoin can never be spent twice simultaneously. With the computing power provided by the miners, they ultimately make the network secure. In return, for compensation they receive newly mined Bitcoins. The more Miners are involved, the more difficult it becomes for Miners to conspire to validate a fraudulent transaction.

XAU: Okay, I can imagine that Bitcoins can be transmitted relatively safely over the Bitcoin network. I have never transferred a Bitcoin, but surely someone by now would have noticed if a secure transmission was compromised?

“Bitcoin is considered to be hack-proof because the Bitcoin blockchain is constantly being monitored by the entire network. Therefore, attacks on the blockchain itself are highly improbable.”

BitPanda.com

BTC: Exactly! Since the network was established, every single transaction has been transferred securely.

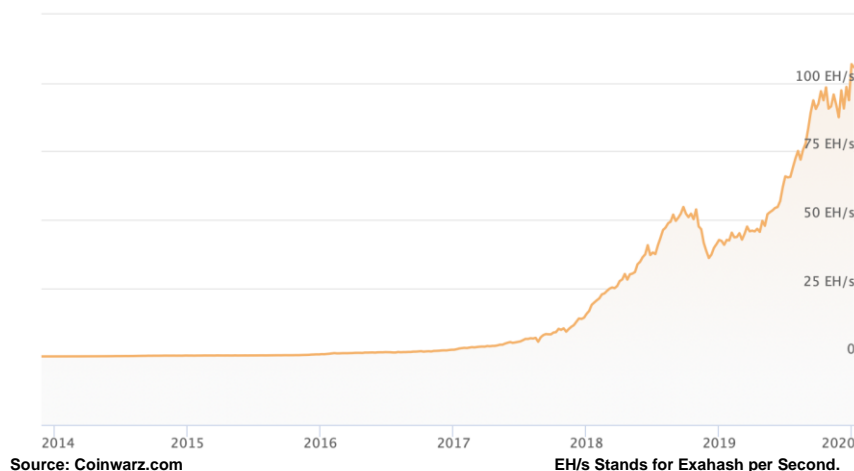
XAU: Still, why exactly would Bitcoin prevail? There are supposedly thousands of such cryptocurrencies in existence today! Whereas the element gold only exists once, guaranteed!

BTC: Well, I have to admit, 100% I can't rule out the possibility that there won't be another crypto currency at some point.

XAU: You see!

BTC: Regardless of this, since the launch of Bitcoin, the likelihood of another cryptocurrency becoming established as a store of value has already decreased significantly. This is primarily due to the enormous spread of its network and thus the high level of Bitcoin security. The computing power that secures the Bitcoin network is now gigantic. No other cryptocurrency has even come close to achieving similar computing power. This can be observed by looking at Bitcoin's hashrate.

Figure 11: The Development of Bitcoin's Hashrate



XAU: Okay, so you're claiming I can transmit Bitcoins safely and securely on the blockchain because the most processing power is behind the Bitcoin network. But this security method is extremely power consuming! Isn't that a disaster in these times of global climate change?

BTC: I'm sure we could spend a very long time debating this specific topic, but I think the most important point is that the electricity used to produce Bitcoin is often excess electricity that would otherwise be wasted.

XAU: What do you mean? The power used to operate the Bitcoin network must be taken from someone else!

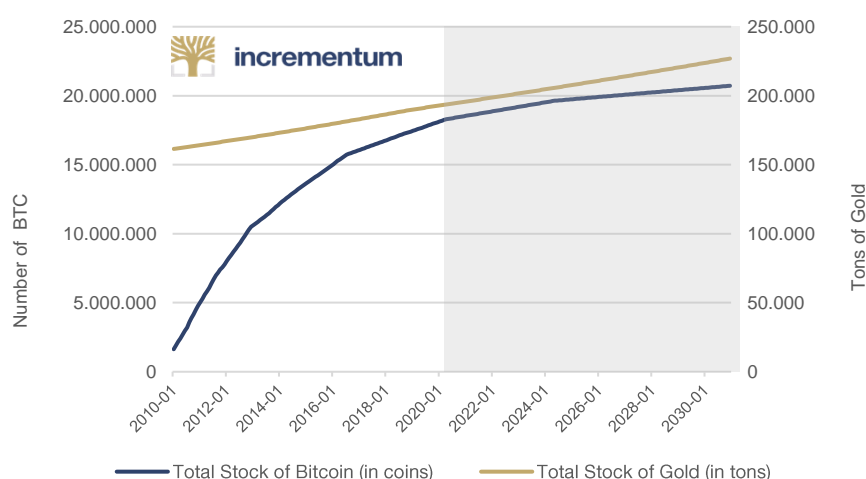
“If the Bitcoin system were a country, its electricity consumption would put it in 43rd place in the world - between Switzerland and the Czech Republic, and the trend is growing.”

Zeit.de

BTC: It is well known that electricity is very difficult to store and can only be transported over long distances with huge losses in power. To mine Bitcoin economically, it is essential to use the cheapest sources of electricity. These are usually remote hydroelectric power plants, as there is often no way to store the electricity. Therefore, many of the Bitcoin farms are located in Scandinavia and Iceland, for example. In both of these places there is large surplus of electricity and it is cheap to use hydroelectric power. Various electricity suppliers have already recognized this and are using Bitcoin mining in some cases to deal with the surplus of electricity. In places with electricity shortages you couldn't even consider mining, because the electricity prices are too high making mining not cost effective. Even at an average electricity price point it is still not possible to mine economically!

XAU: Wow, I really didn't know that. Still, why invest in Bitcoin now? With gold, I know there's a finite amount on earth. So, gold will always be worth something. But Bitcoin is so speculative. And it pays no interest, either.

Figure 12: Stocks of Bitcoin and Gold Compared with Future Outlook - An Indicator of Inflation



Source: Incrementum AG

BTC: Okay, let's get this straight. Both gold and Bitcoin are two investments that yield no interest. Both are "unproductive" assets whose value originates in the investment itself. Shares are invested in order to participate in the success of the company. Or, via government bonds, one participates to a certain extent in the development of the entire economy.

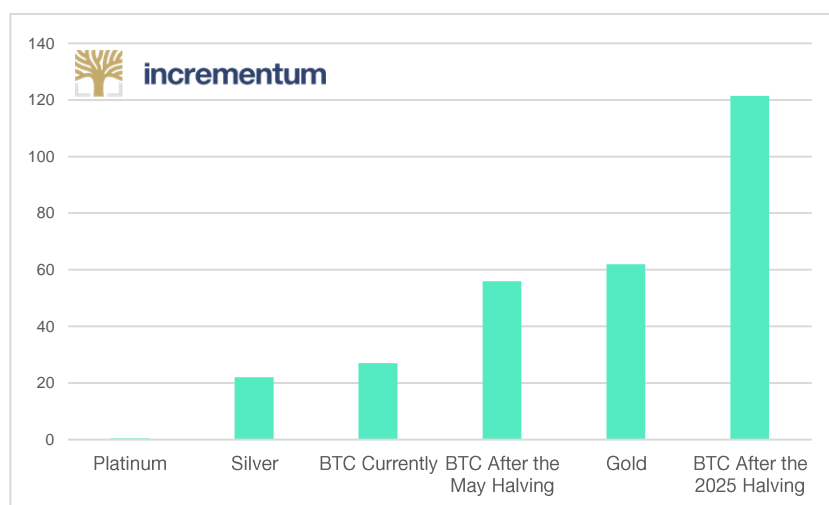
XAU: I understand your argument, but I would still not consider gold and Bitcoin to be equivalent. This is because gold is strong and stable. Gold is only available in limited quantities and is therefore valuable. Every year the amount of gold mined grows very steadily by about 1.5 percent. Even after large price increases, mining companies have not been able to expand their production significantly. Central banks, on the other hand, have been siphoning off vast amounts of money since the financial crisis, amounts that I can no longer even imagine because of the many zeros. Surely, they will go bankrupt at some point!

BTC: On that point we are in complete agreement. The number of Bitcoin cannot be increased arbitrarily at will! Gold and Bitcoin could therefore be two ways of protecting against the dangers of the central banking system.

XAU: But with digital currencies, you could also add the numbers zero and one to somewhere in the code and thus create new "currency".

BTC: [Laughs] I'm so glad you brought that up. You're kind enough to play into my hands. In fact, Bitcoin will become even "stronger" than gold over time, because the maximum number of Bitcoins available is exactly 21 million. That's all there is, and that's all there will ever be, the Bitcoin protocol stipulates this. Every four years the inflation rate of Bitcoin is therefore halved. In May of this year, Bitcoin's inflation rate will fall roughly to that of gold and in the future Bitcoin will be even "stronger", even less inflationary than gold. See also the different stock-to-flow ratios in comparison [chart on the next page, Figure 5]. Simply changing a few numbers in the code is absolutely impossible. There would have to be a 95 percent approval of the miners to do this. But Bitcoin thrives on the fact that it is a scarce commodity, so broad approval for such a change is almost impossible.

Figure 13: Various Stock-to-Flow Ratios in Comparison



Source: Incrementum AG

XAU: But what about the opportunity then to just create a new cryptocurrency? I've heard that one could basically just copy Bitcoin, and everyone could create

their own version. Isn't that called hard fork? Wouldn't that just double the maximum number of Bitcoins in seconds?

What is a Hard Fork?

Simply put: a fork is the further development of a software. A hard-fork, i.e. a backward-compatible change to the rules on the blockchain, results in a blockchain becoming two blockchains. At the time the hard fork is published, the blockchain users have to decide whether they want to stay with the old blockchain or whether they want to switch to the new one. This decision must be made actively. A hard fork always leads to a split, but the blocks remain the same until the split.

A detailed explanation can be found on the Crypto Research Report's website under the following [Link](#).

BTC: Technically, while this sounds quite simple in theory, it is extremely unlikely that a copy of Bitcoin would be widely adopted: First of all, the survival of a new cryptocurrency depends on whether there is any interest in it at all. Why would Bitcoin investors, who probably also trust Bitcoin because the system has limited inflation, want to switch to a new cryptocurrency system? There has to be added value here. If there is not, the hard fork will be very difficult. This has been seen with all Bitcoin hard forks so far. Secondly, the Miners who secure the system would have to go along with it and make their computing power available to the new Bitcoin version in the future. But the Miners don't do that, because they have a far greater incentive to mine the most valuable asset. Without high computing power this "new version" of Bitcoin would be very insecure and thus is not an attractive investment.

XAU: Okay. You know, I keep hearing that Bitcoin has a scaling problem. If you want to use it as a widespread currency it's way too expensive, right?

The "Scalability" Problem of Bitcoin

Bitcoin's current version allows for a maximum of seven transactions per second. If Bitcoin really wants to be used as a means of payment in the long term, at some point that rate will be too little.

BTC: You are correct, there is currently a scaling problem that is caused by the size and decentralization of the Bitcoin network. There is a trade-off between the security of the network and the speed of transactions. One perspective is that Bitcoin does not have to become a mass payment medium to be valuable. This is true for gold as well. The smaller the quantity of gold, the higher the transaction costs in terms of the price difference between buying and selling. It is questionable whether one should really invest in

gold if one only wants to buy 1 gram of gold. With larger quantities of gold, the transaction costs are hardly significant. From a cost perspective, gold is therefore well suited as a store of value for larger investment amounts. Bitcoin can be viewed in the exact same way. From a cost point of view Bitcoin is store of value for larger amounts, i.e. digital gold, but it admittedly can be a volatile one.

XAU: Interesting. But Bitcoin's ultimate claim was to be the advanced electronic payment system. Is that now unfulfilled because of this scaling problem?

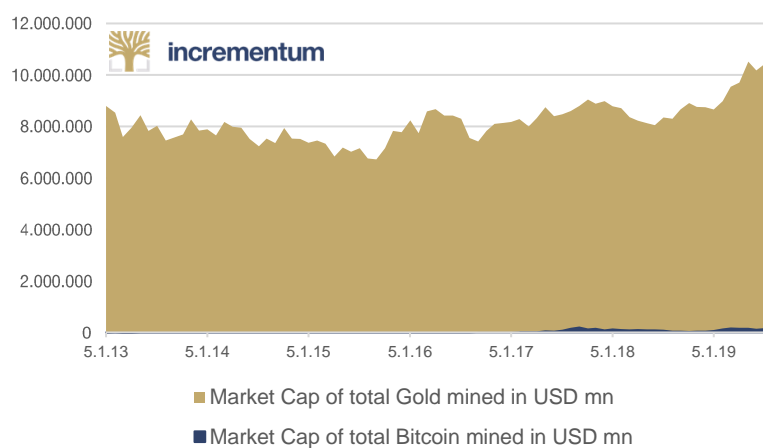
BTC: Quite correct. The title of the so-called white paper was even "Bitcoin: A Peer-to-Peer Electronic Cash System". And there are intensive efforts to fulfill this claim. There are various approaches to enabling more transactions per second. Hard forks are just one approach, which we have already seen with Bitcoin Cash, for example. Other possibilities exist in the areas of off-chain transactions, such as the Lightning-Network. There, transactions outside the blockchain are processed quickly and securely. In any case, thousands of programmers worldwide are working on the solution to this issue. There is an incredible amount of human capital behind this, which is also responsible for the fact that the hurdles that have

been overcome so far have been handled quite effectively. If the scaling problem is actually still being resolved, it would not only be digital gold, but also a strong digital currency! So, another difference between gold and Bitcoin is that Bitcoin can be used as a means of payment and a store of value at the same time. This is a huge advantage of Bitcoin over gold, because gold is hardly suitable as a means of payment.

XAU: Well, I must strongly object here. In the days of the classic gold standard, gold was indeed used as a means of payment! Today's central banks tend to overlook the period from 1870-1914, when there was slight deflation and very high growth rates. But I think that is a different debate. In any case, I don't understand why you, as a Bitcoin fan, keep talking about Bitcoin being a store of value like gold, considering the high level of volatility?

BTC: I think I have already been able to give you some solid arguments, such as limited inflation or the security of the system through the hashrate. I would also like to highlight the fact that Bitcoin is still in its early stages. The market capitalization as of January 9, 2020, at \$ 144 billion, is only a fraction of that of gold. The significant price fluctuations are therefore also offset by an exorbitantly high potential profit. In fact, Bitcoin is an extremely asymmetric asset class, as Bitcoin either succeeds in the medium term and asserts itself as a global digital store of value or - for whatever reason - fails and becomes worthless.

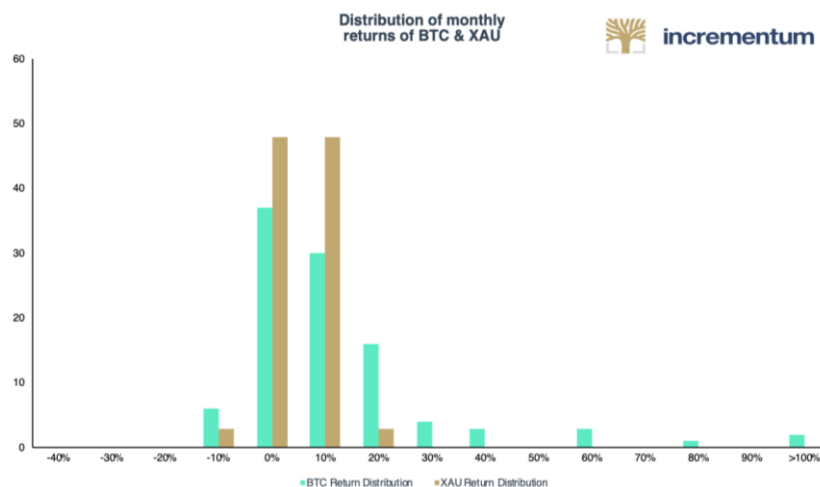
Figure 14: Comparison of Market Capitalization Gold vs. Bitcoin 2013 - 2020



Source: Incrementum AG

XAU: Hmmm, I never thought of it that way. Bitcoin has a different payout profile than gold. I mean, gold really can't drop to zero, or do you disagree with me on this point?

Figure 15: Number of Months of Different Returns of Bitcoin and Gold



BTC: No, we are in agreement on this! Gold cannot become worthless. But the appreciation potential of gold is of course limited, since gold is known to everyone. Bitcoin is still extremely small and very young. The Internet has only been around for 30 years and Bitcoin for only 10 years. The vision is that Bitcoin will become the universal and digital value standard in an increasingly digitalized world. Very little of this has been taken into account so far. Why shouldn't the central banks hold digital assets in 10 years? They are already thinking about digital currencies today, why shouldn't they invest in "digital gold" at that point in time? When Bitcoin becomes established as the strongest digital currency, the central banks will hold Bitcoin as a currency reserve in addition to gold. I don't think that's so far-fetched. The world is changing!

XAU: Okay. Assuming you have piqued my interest, what would your investment advice be? I'll tell you one thing right off the bat. I certainly won't sell my gold, at least not all of it!

BTC: There are indeed crypto enthusiasts who swear by cryptocurrencies and have invested all their savings. This is of course extremely risky! On top of that, things usually turn out the way they're supposed to! They buy in euphoria and sell in panic. But it is precisely the asymmetric payout profile that makes a small addition of Bitcoin interesting. And the high volatility can be used to your advantage through rule-based rebalancing!



XAU: Well, it seems that Gold and Bitcoin are more alike than one might think, don't they? Together the two asset classes form a thoroughly dynamic duo. In fact, this is the innovative investment strategy that Incrementum makes use of. Learn more at: <https://cryptofunds.li>.

Introducing...

Crypto Research Newsletter

Professional Financial Analysis of Cryptocurrencies

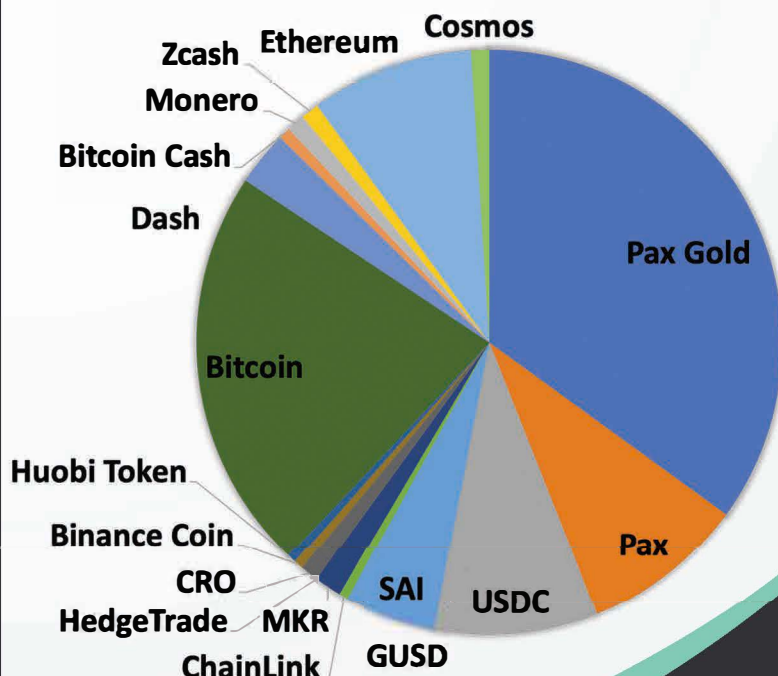


See what our portfolio holds and follow our weekly trades for the price of a coffee!



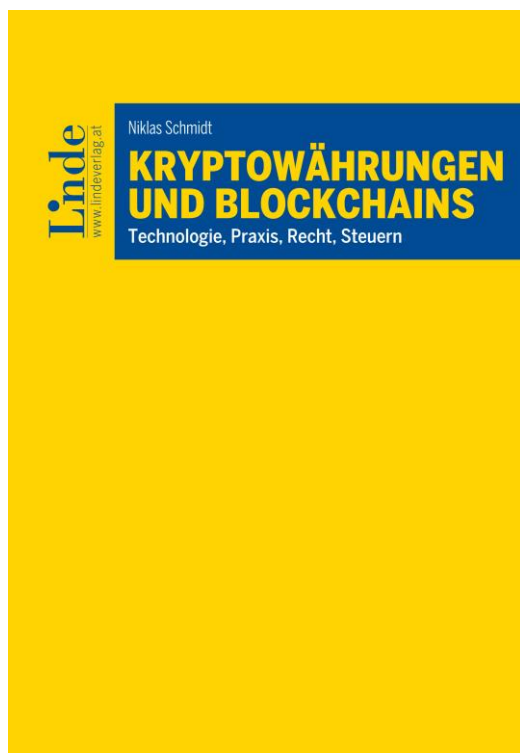
Sign up for
our newsletter!

CRR Portfolio Jan 31st 2020





Incrementum Recommended Books



Today, thousands of cryptocurrencies exist and even more books on the topic of cryptocurrencies exist. Determining which books are worth the read is almost as difficult as determining which cryptocurrencies to invest in. A book that we recently read called *Kryptowährungen und Blockchains* was published last year in March 2019 by Dr. Niklas Schmidt. This book has already had to be reprinted several times due to popular demand and the English version, *Crypto Currencies and Blockchain* is set to be translated and release by the end of this year 2020.

The book closes the gap by covering detailed insights about cryptocurrencies and blockchains for the German-speaking readership. It is comprised of three main characteristics: First and foremost, it contains about 400 Frequently Asked Questions (FAQs) that provide an easily digestible introduction to the subject without having to read the entire book – although we highly encourage the full read.

Secondly, the book covers a wide spectrum of topics in great detail from technological functionality & characteristics of the blockchain to its economic aspects & implications. Some examples of this include: Bitcoin's price development, the disruptive effects blockchain has on various industries, and a legal overview covering civil, tax, accounting, corporate, labour, commercial, data protection, supervisory, money laundering and criminal law.

Thirdly, the content is practical in that it contains many real-life examples and anecdotes so the reader can have better context. Some chapters also offer helpful lists of the industry's current wallets, exchanges, blogs, newsletters, and apps.

Overall, this book we recommend without restriction and a great resource for both beginner readers and those who want to acquire a deeper knowledge of Bitcoin and beyond.

A Physical and Digital copy of *Kryptowährungen und Blockchains* (German) can be purchased on the publisher [Linde Verlag's Website](https://www.lindeverlag.at).

The English version will be released this year (late 2020).



Dr. Niklas Schmidt



New Research in Crypto

Official Launch of Incrementum's Research Cooperation with the
University of Liechtenstein



University of Liechtenstein teams up with Incrementum AG to form a research cooperation

The development of blockchains and cryptocurrencies will permanently change the way of investing and asset management as a whole. Moreover, these technologies themselves represent a promising form of investment. With these developments, it is important to always have your finger on the pulse of time in order not to run the risk of being surprised and overwhelmed by new unknown developments.

The fact that Liechtenstein is keeping pace with the times is clearly demonstrated by the recently adopted "Block Chain Act". But there is also a lot going on at the University of Liechtenstein as well as in the private sector. A great success for the local crypto industry was celebrated on Tuesday, 26th of November 2019 at the University of Liechtenstein, as a special research grant was handed over.

The award, worth CHF 360,000, is a multi-year grant to the Institute of Finance at the University of Liechtenstein, which is clearly linked to the goal of researching the opportunities and risks of blockchain technology in more detail with and for a practical partner. The Schaan based Asset Management Boutique Incrementum AG has been chosen as the practice partner.



"The University of Liechtenstein has been active for several years in researching block-chain technology and cryptocurrencies and has earned a reputation as a neutral and critical voice", project manager Martin Angerer is quoted in a broadcast. Together with his colleagues Michael Hanke and Lars Kaiser, the project focuses on research into the investment management of cryptocurrencies, including data-driven investment strategies and risk management. During the event Frank Heeb from Liechtenstein's Office of Economics gave a speech in which he underlined the importance of such projects for the country. Martin Angerer explained the cooperation strategy and showed how a symbiotic relationship can be created by combining research and practice. Afterwards Mark Valek, Partner at Incrementum AG, spoke about how volatile cryptocurrencies can be used as an asset class and how they could be "tamed". The keynote lecture by Rahim Taghizadegan, who gave fascinating insights into the development of the monetary system, and the subsequent aperitif completed a great evening.



incrementum



UNIVERSITÄT
LIECHTENSTEIN



About Us

Authors



Mark Valek
Portfolio Management



Demelza Hays
Research

The Team



Nikolaus Jilch
Contributor



Pascal Hügli
Token Economist



Stefan Thume
Web Design and Media



Riley Corbett
Research & Business
Development



Florian Grummes
Technical Analyst



Richard Knirsch
Chart Guru

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 was established as a quarterly publication in 2017 and published by Incrementum AG until February 2020. The main editors were Demelza Hays and Mark Valek. From March 2020 onwards the publication is published and edited by CryptoResearch.Report. CryptoResearch.Report is responsible for the content of the editions post February 2020.

The Company

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



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. In cooperation with the State Printing House of Austria, Coinfinity has designed a "[Card Wallet](#)" that is a bearer paper wallet for Bitcoin.



Oliver Völkel

Based in Vienna, Oliver Völkel is a partner at [Stadler Völkel 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.



In case you have missed our last Crypto Research Report and you would like to have a pleasant reading, please follow the links below.



Crypto Research Report – December 2017 Edition

- Introduction to the Blockchain Technology and Cryptocurrencies
- U.S. Regulated Bitcoin Derivatives: Blessing or Curse?
- Constructing a Cryptocurrency Index
- Taxation of Cryptocurrencies in Europe
- Farewell 2017: Year of ICOs, Hard Forks, and Upward Trends



Crypto Research Report – March 2018 Edition

- In Case You Were Sleeping: Ikarus Edition
- Bubble or Hyperdeflation?
- Coin Corner: War Within Bitcoin
- Technical Analysis: Is a Crypto Winter About to Start?
- Crypto Concept: Fork
- 10 Facts About Max Tertinegg, the CEO of Coinfinity
- Incrementum Insights: How Will Cryptocurrencies Change Finance



Crypto Research Report – June 2018 Edition

- In Case You Were Sleeping: Wall Street Is Getting Ready
- Crypto Concept: Consensus Mechanisms
- Competing Currencies and Digital Money: How Hayekian are Cryptocurrencies?
- Coin Corner – Blockchain 3.0 The Future of DLT?



Crypto Research Report – October 2018 Edition

- In Case You Were Sleeping: Cell Phone Theft Edition
- Crypto Concept: Smart Contracts
- Liechtenstein's Blockchain Strategy
- Coin Corner: ETH, NEO, ADA, & EOS
- The Network Effect as a Valuation Methodology



Crypto Research Report – January 2019 Edition

- In Case You Were Sleeping: Crypto Winter Edition
- Crypto Concepts: Custody Solutions for Crypto Currencies
- A Bitcoin Standard? Saifedean Ammous Musing with the Crypto Research Report
- Institutional Requirements for an Investible Crypto Index
- Equity Tokens
- Legal Challenges for Blockchain-Based Capital Markets



Crypto Research Report – April 2019 Edition

- In Case You Were Sleeping: When the Tide Goes Out...
- Gold & Bitcoin: A Crypto Strategy, also for Institutional Investors
- Technical Analysis: Spring Awakening?
- Crypto Concepts: Cryptocurrency Mining in Theory and Practice
- John Tromp: Making Computer Science Great Again



Crypto Research Report – July 2019 Edition

- In Case You Were Sleeping: Facebook Edition
- Libra: The End of the State Money Monopoly
- Coin Corner: XRP and Ripple
- Gold Stablecoins
- Partner Insights: Lucas Erath on Transforming Finance
- Fireside with Nick Szabo on Scaling Bitcoin



Crypto Research Report – October 2019 Edition

- In Case You Were Sleeping: Banking on the Blockchain
- How Crypto Brokers and Funds Source Liquidity
- A Primer on Regulation and Trading in Switzerland
- Tokenizing the Swiss Franc with Armin Schmid of Swiss Crypto Tokens
- Incrementum Recommended Books
- Upcoming Conferences

We sincerely want to thank the following friends for their outstanding support:

Our knowledgeable advisors including Max Tertinegg and Oliver Völkel, the generous authors who contributed to this report including Plan B, Daniel Wingen and Nikolaus Jilch. We are also grateful to our wonderful research analysts, Leonard Wachter and Riley Corbett, and our editors Bianca Sayers and Gregor Hochreiter.

Contact:

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



Disclaimer:

This publication is for information purposes only, and represents neither investment advice, nor an investment analysis or an invitation to buy or sell financial instruments. Specifically, the document does not serve as a substitute for individual investment or other advice. The statements contained in this publication are based on the knowledge as of the time of preparation and are subject to change at any time without further notice. The authors have exercised the greatest possible care in the selection of the information sources employed, however, they do not accept any responsibility (and neither does Incrementum AG) for the correctness, completeness, or timeliness of the information, respectively the information sources, made available, as well as any liabilities or damages, irrespective of their nature, that may result there from (including consequential or indirect damages, loss of prospective profits or the accuracy of prepared forecasts).

Copyright: 2020 Incrementum AG. All rights reserved.