crypto research .report

June 2018
Edition III.

Demelza Kelso Hays
Mark J. Valek

incrementum

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

Vontobel

incrementum

Cryptofunds.li

Contents

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 therefrom (including consequential or indirect damages, loss of prospective profits or the accuracy of prepared forecasts).

Editorial

Dear Reader,

The main topic of CRR III is consensus. Taking decisions in a firm is faster when there is a vertical hierarchy of owners, managers, and subordinates. Likewise, countries ruled by dictatorships are faster at making decisions than direct democracies. Although, centralized entities are faster, the increased speed is not without costs. Similar parallels can be drawn to how decisions are made in a blockchain. Slow and egalitarian networks such as Bitcoin are criticized by investors that want a fast and global payment network. IOTA and other coins based on the directed acyclic graph structure are rumored to solve the scaling problem associated with the Bitcoin blockchain by paralleling validation of transactions. In contrast, rival Blockchain 3.0 technologies, such as Tezos and Dfinity promise to solve the scaling problem by building governance directly into the protocol. **This edition of the Crypto Research Report covers the trade-off between decentralization and efficiency when it comes to what is called a "consensus mechanism", and importantly, we discuss what this means for investors.**

In the current report, our Coin Corner chapter focuses on how Hashgraph, Iota, and Byteball are competing to become scalable blockchain networks. The Crypto Concept chapter contains an in-depth analysis of what consensus mechanism are, and how the top 100 market capitalization coins use different consensus mechanisms in order to secure their network and settle the chronological order of transactions recorded in the blockchain. Although, competitors are striving to outperform Bitcoin's consensus mechanism called proof-of-work, it is still the undefeated champion because of its proven track record of almost a decade. This edition also features an article on the Nobel Prize winner Friedrich von Hayek's work on denationalizing currency and how theory shapes the minds of some cryptocurrency investors.

Thank you for reading the second edition of the Crypto Research Report that we published in Q1 of 2018. We received wonderful feedback and constructive criticism from many of you. ***As always, the third edition of the report will be available for free in German and English on our homepage, CryptoResearch.Report.*** We are looking for new sponsors to support our research. Interested companies can contact us directly at crypto@incrementum.li.

Demelza Kelso Hays
Research Analyst, Incrementum AG

Demelza Hays

In Case You Were Sleeping

“The total market cap of cryptocurrencies was around USD 400bn, around a quarter of that of gold as store of wealth (gold bars, coins and physical gold ETFs all together amount to USD 1.5tn). And monthly trading volumes of the three largest cryptocurrencies by market capitalization (Bitcoin, Ethereum and Ripple) have increased sharply in recent months, from around USD 5bn in early 2017 to USD 550bn in December. This represents around half of the monthly trading volume of gold futures of USD 1.1tn, as of January 18 aggregate volumes were higher, reaching around USD 680bn.”

J.P. Morgan Perspectives 2018

Key Takeaways

- **Big investment banks are entering the cryptocurrency market with a bang.**
- **SEC is tightening up on regulation around the ICO craze.**
- **Cryptocurrency markets are still largely driven by retail investors sentiment and rife speculation. So called “whales” exert a massive influence on the market due to insufficient liquidity.**

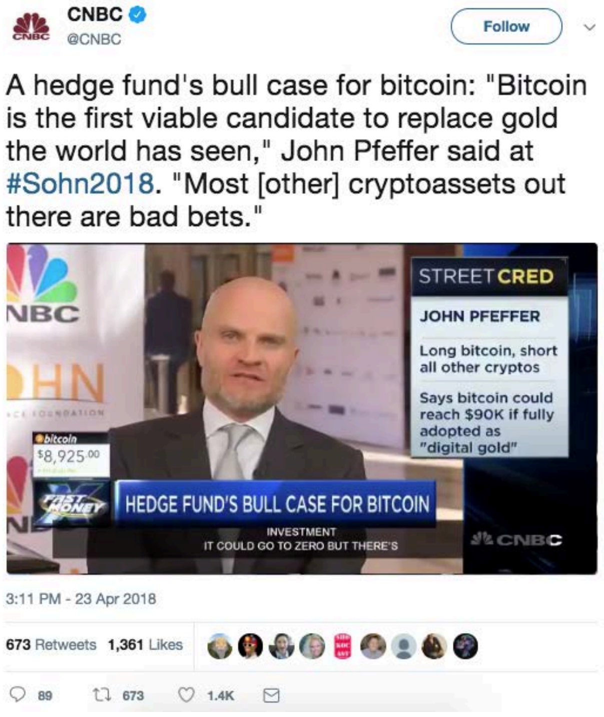
The Bitcoin price is plummeting and looking for a floor. Meanwhile big players on Wall Street are working on their grand entrance. At the forefront of this: Goldman Sachs.

> *"Economists and journalists often get caught up in this question: Why does Bitcoin have value? And the answer is very easy. Because it is useful and scarce."*
>
> Erik Voorhees

What to do if you are stationed in the middle of nowhere surrounded by super computers? Exactly, you mine cryptocurrencies. This happened in a Russian government research center in Sarov, a secluded city 400km east of Moscow, the seat of the Russian nuclear program. The first Soviet atomic bomb was built here in 1949. And now researchers have been caught using the strongest computers the Russian state has to offer to mine cryptocurrencies.

This came to light through a press statement by the authorities in February of this year. Apparently, this is becoming a common occurrence in companies with good IT infrastructure. However, maybe the researchers just took a statement from Vladimir Putin during his visit to Sarov in 2014 a bit more literal than expected. At said meeting with young scientists, President Vladimir Putin praised the Russians' spirit of resourcefulness, saying, "When life sets us certain challenges, we are forced to tackle them one way or another and we do." As a side note, the Russian authorities neither informed us which coins had been mined nor did they shed any light on what had happened to them in the meantime. [1]

It is however not only Russian civil servants or the population of inflation-riddled countries such as Venezuela, who have discovered cryptocurrencies and are using them for their own gain. Recently military investigators uncovered a drug ring at the US-Navy academy in Annapolis, Maryland. Ten officers in training had been supplying their comrades with cocaine, LSD and ketamine. They had apparently bought the drugs on the Dark Net and paid for them with Bitcoin. The management of the academy ordered a spontaneous drug test for all 4500 recruits, the results of which were never made public. [2]



CNBC
@CNBC

Follow

A hedge fund's bull case for bitcoin: "Bitcoin is the first viable candidate to replace gold the world has seen," John Pfeffer said at #Sohn2018. "Most [other] cryptoassets out there are bad bets."

NBC
HN
STREET CRED
JOHN PFEFFER
Long bitcoin, short all other cryptos
Says bitcoin could reach $90K if fully adopted as "digital gold"
bitcoin
$8,925.00
FAST MONEY
HEDGE FUND'S BULL CASE FOR BITCOIN
INVESTMENT
IT COULD GO TO ZERO BUT THERE'S
CNBC

3:11 PM - 23 Apr 2018

673 Retweets 1,361 Likes

89 673 1.4K

The Bitcoin Price is Plummeting

In our first report in 2018, we predicted a spell of crypto winter. Our technical analysis of the crash in January 2018 goes to show that a hard plummet right down to USD 2,500 is very possible. Other (especially pessimistic) analysis corresponds with this evaluation. Many are looking at the charts of the crash after 2013 for some sense of direction in which Bitcoin could go now. Especially bleak outlooks have been published since analysts saw a "Death Cross" in the charts in mid-March.[3] Others, such as the crypto hedge fund "Pantera Capital Management" assume that we have already reached the rock bottom price of Bitcoin at USD 6,500, and we will therefore soon

—

[1] See "Russia Busts Crypto Miners at Secret Nuclear Weapons Lab," Stepan Kravchenko, *Bloomberg*, February 9, 2018.

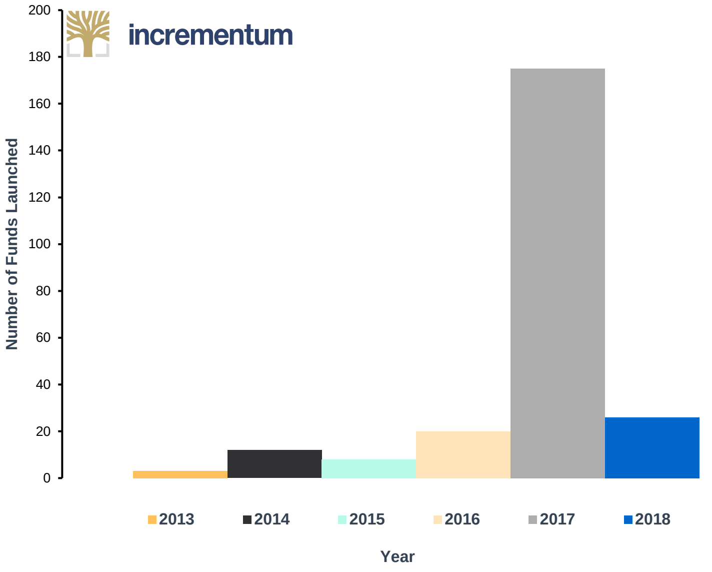
[2] See "Naval Academy Rocked by Drug Scandal; Ring Bought Cocaine With Bitcoin," Tyler Durden, *Zero Hedge*, February.

[3] See "Bitcoin's 'Death Cross' Looms as Strategist Eyes $2,800 Level," Todd White and Eddie van der Walt, *Bloomberg*, March 16, 2018.

witness an upwards trend again.[4] While we are finishing this report, prices are dropping again, then shooting up because of good news, then dropping again. Where do we go next? That is the age-old question - in hindsight we are always smarter. The markets are unpredictable and the crypto market is especially volatile.

> *"You can't stop things like Bitcoin. It will be everywhere, and the world will have to readjust. World governments will have to readjust."*
>
> John McAfee

Figure 1: Number of Hedge Funds Launched from 2013–Q2 2018.



Sources: Autonomus NEXT, Incrementum AG.

Note: 251 funds in total, with $3.5 - 5 billion in assets under management.

A study by the Warwick Business School showed that trades on the crypto market are made on a purely emotional basis instead of being based on fundamental analysis.[5] The survey covered trade data from April 2016 up to September 2017, and the results do make sense.

The crypto market is still dominated by small investors who don't have the knowledge or data for a technical or fundamental analysis. On top of this, Bitcoin and Co. are still so relatively new that there is a real lack of accepted official data for an unbiased assessment. It is however noticeable that over the past few months more and more central bankers have had a closer look at Bitcoin – and in the process, have confirmed Bitcoin's role as a currency[6] as well as the fact that Bitcoin does indeed have value. One central bank economist sees the fundamental price (based on mining costs) at USD 1,800.[7]

The debate is however still ongoing. The author of the Warwick survey, Daniele Bianchi, has a similar view. "It's not like with normal currencies, in which the productivity of a country influences the price. Instead, they have similarities to investments in shares of a high-tech company." This phenomenon can be seen

[4] See "Crypto Hedge Fund Says Bitcoin Has Bottomed Out," Camila Russo, *Bloomberg*, April 12, 2018.
[5] See "The Fundamentals Driving Crypto Trading? There Aren't Any," Julie Segal, *Institutional Investor*, May 24, 2018.
[6] See "A Short Introduction to the World of Cryptocurrencies," Aleksander Berentsen and Fabian Schär, *Federal Reserve Bank of St. Louis Review*, 2018, 100(1), pp. 1-16.
[7] See "Making Sense of Bitcoin Price Levels," Joost van der Burgt, *Federal Reserve Bank of San Francisco*, April 2018.

time and time again and economists are now discovering the new field of crypto economics. The puppet masters behind the various tokens try and create different incentive systems to pull in more investors. These tokens therefore almost turn into shares of the company or project at hand. At least they are traded like shares. An important factor in the price drop over the past few months has been the so-called Tokyo Whale. This is the nickname for the bankruptcy trustee of the now extinct exchange Mt. Gox. The hack and subsequent collapse of which lead to the bear market of 2014 and onwards.[8] It is the Tokyo Whale's job to sell the rest of Mt Gox' Bitcoins as profitably as possible. In total, he will unleash 200,000 Bitcoins to the market.[9] This will obviously not happen in one go, but according to media reports the trustee Nobuaki Kobayashi has trickled Bitcoins into the market worth USD 400 million since September 2017.

> *"The reason Cryptocurrencies are interesting is because it cannot be controlled, it cannot be censored, because it's open."*
>
> Andreas Antonopoulos

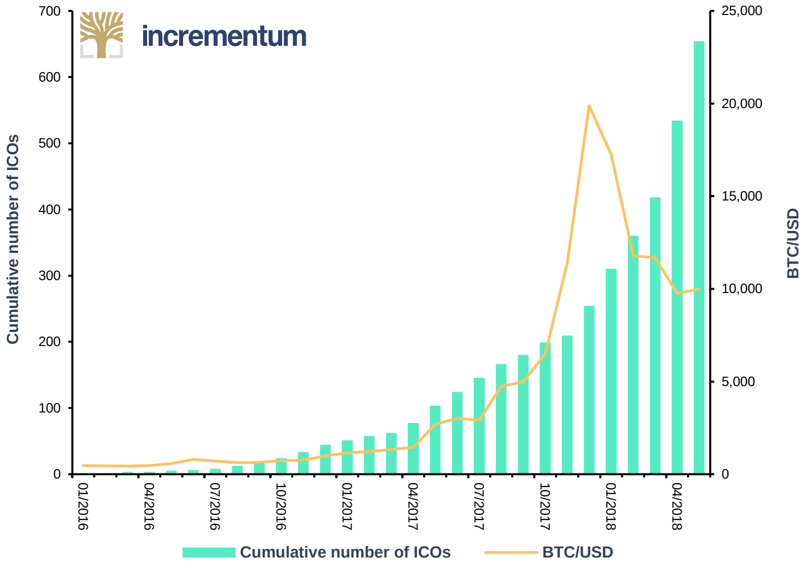
By the beginning of February, he must have sold roughly 40,000 Bitcoins. What followed was a temporary recovery until Kobayashi moved 16,000 Bitcoins onto an exchange ready for the presumable subsequent sale. The community follows his wallets closely, as the game only ends when all 200,000 Bitcoins from Mt. Gox have been turned into "real" money.[10]

Which Altcoins Will Survive?

All these elements together make for an extremely volatile market. **The least volatile cryptocurrency, measured by standard deviation of returns, in this market is Bitcoin.** However, altcoins such as Ethereum and Ripple are also becoming increasingly popular on the market. Market sentiment in June 2018 first showed signs of desperation, maybe even despair – in social media as well as in various forums. We are sure we will only start a new bull market once the weak hands have been swept out of the market. Investors which only joined the game during the ICO Boom of 2017 should be aware that although Bitcoin has survived such a "crypto winter" before, the majority of Altcoins however have not been put through the same test of time.

[8] See "Inside The Bizarre Upside-Down Bankruptcy of Mt. Gox," Adrianne Jeffries, *The Verge*, March 22, 2018.
[9] See "Mt. Gox Trustee Sold Half a Billion Dollars Worth of Bitcoin and Bitcoin Cash," Trustnodes, March 7, 2018.
[10] See "Bitcoin's Tokyo Whale Sold $400 Million and He's Not Done Yet," Go Onomitsu, *Bloomberg*, March 7, 2018.

Figure 2: Cumulative number of ICO´s vs. BTC/USD.



Sources: coinschedule.com, investing.com, Incrementum AG.

"The entire human populace is now taking charge of the means of production and changing the rules of the game. They're making their own freaking currencies, for God's sake!"

Paul Vigna

The analysts from Goldman Sachs categorically warn against holding on to Altcoins in a bear market. In a report dating back to February of this year, Goldman analyst Steve Strongin, suggests that a large percentage of existing Altcoins could completely disappear and could be replaced by a small number of robust cryptocurrencies which lead the way to a new upward turn. "The high correlation between the different cryptocurrencies worries me", Strongin said. "Because of the lack of intrinsic value, the currencies that don't survive will most likely trade to zero."[11]

Like others before him, Strongin draws parallels between the Blockchain market and the Dot Com Bubble. Only a few of the hottest stocks from the late 1990s have survived. Those that did however, became huge. "*Will the cryptocurrencies of today turn into the Amazons or Googles of tomorrow or will they end like the many now non-existent search engines? Just because we are in a speculative bubble doesn't mean the price for the few surviving ones can't rise again. At the same time this means that many won't ever reach their all-time highs ever again.*"

It is true that such gloomy prophecies regarding Bitcoin have turned out to be wrong time and time again.[12] But then again, we have been in good company when we have warned against the ICO Mania. This is why we must say the Goldman analyst could be right. **A handful of projects could survive in the long-term, but many are facing the end before we leave this valley of death.** The Godfather of cryptocurrencies Bitcoin has proven its stability before. **While small investors are at home licking their wounds from the market downturn, the big boys are finally here to step into the ring. This is probably the most important trend of 2018, and we call it the *"Goldman-Effect"*.** The second trend comes as a direct result of the first: the

[11] See "Get Ready to See Most Cryptocurrencies Hit Zero, Goldman Says," Kana Nishizawa, *Bloomberg*, February 7, 2018.
[12] See "Bitcoin Obituaries," *99Bitcoins*, 2018.

regulators are finding themselves under more and more pressure because institutional investors need legal security before they can enter the market.

The Goldman-Effect

The boss of Goldman Sachs, Lloyd Blankfein, earned lots of criticism in 2009, when he was quoted saying his bank was doing “God’s work” in an interview with London Times. He added that his bank had a social role: “We help companies grow. Growing companies create standards and jobs. We have a social responsibility.”[13]

Early Bitcoin adopters and purists may note like to hear this, but Goldman is doing a lot for the legitimization and growth of the crypto sector. The investment bank, which has always thought of itself better than the competition, wants to be the first to get in on the new opportunity. The analyst from Goldman took a closer look at Bitcoin back in the summer of 2017. And now this. At the beginning of May, in a carefully choreographed article in the New York Times, it was made public news that “Goldman Sachs will be entering the trading floor of Bitcoin”.[14]

The new trading desk will initially be part of the department for foreign currency. It will be led by the 38-year-old Justin Schmidt. In 2017, he had only left the hedge fund Seven Eight Capital to trade Bitcoin and other crypto assets by himself. The reasoning behind the decision, which are described in the New York Times article, paint a very interesting picture of the growing popularity of Bitcoin on Wall Street. “It resonates with us when a client says, ‘I want to hold Bitcoin or Bitcoin futures because I think it is an alternate store of value”, says Rana Yared, a senior of Schmidt’s at Goldman. “Bitcoin is not a scam”, she goes on “But it is also not a currency. Clients want to hold cryptocurrency as a sort of precious natural resource, similar to gold.”

“Bitcoin will do to banks what email did to the postal industry.”

Rick Falkvinge

It was possible for Goldman to get in on the action through the implementation of futures and other derivates. However, the Goldman bankers aren’t the only ones buying up Bitcoin-Futures. **The daily trading volume of the CME Futures in Chicago have risen by 250% since the initiation in December 2017.**[15] There is still room to grow. According to Reuters one fifth of the big banks want to enter the Bitcoin trade by the end of 2018.[16] As of now, it is still prohibited for institutional investors to buy Bitcoin outside of regulated fund vehicles, trackers, futures, and trusts. They are however getting prepared for when the day comes that this will be possible, and they are putting real thought into how one can directly buy Bitcoin and store them securely for clients.

[13] See “Blankfein Says He’s Just Doing ‘God’s Work’,” Dealbook, *The New York Times*, November 9, 2009.
[14] See “Goldman Sachs to Open a Bitcoin Trading Operation,” Nathanial Popper, *The New York Times*, May 2, 2018.
[15] See “The CME recorded an all time record volume of its 5-lot BTC futures yesterday,” Jon Najarian, *Investitute*, April 26, 2018.
[16] See “One in five financial institutions consider cryptocurrency trading, says survey,” *Reuters*, April 24, 2018.

Et tu, J.P. Morgan?

One of them could be J.P. Morgan. This is highly interesting as J.P. Morgan's CEO Jamie Dimon is a known Bitcoin skeptic. He has after all called Bitcoin a scam.[17] He went as far as to say he would fire any employee who touches the stuff. The comments didn't age well. In May, just a mere few months after Dimon's last outburst, the U-turn was made official: J.P. Morgan is working on its own crypto strategy.[18]

They created a new position for exactly this purpose and found the 29-year-old Oliver Harris to fill it. Up until then he was responsible for J.P. Morgans Fintech-Program. J.P. Morgan seems to be still be a few steps behind the competition as direct trading with cryptocurrencies or even derivatives are as of yet, not on the horizon.[19]

Daniel Pinto, co-president of J.P. Morgan, separately told CNBC on Wednesday that the Wall Street giant was now "looking into that space". "Cryptocurrencies are real, but not in the current form," he said.[20] We are left wanting further explanations by Dimon's potential successor. But when Dimon revised his statement regarding Bitcoin and even noted that there was a viable future for the Blockchain technology, one could have known the bank was about to announce their official move towards the sector.

Dimon is not the only one to change his mind when it comes to Bitcoin. The currency speculator George Soros had claimed just six months ago at the economics forum in Davos that Bitcoin was only interesting for a dictator wanting to keep some money safe on the side. **A very lopsided view of things given that the technology actually allows the small man on the street to keep money away from a dictators as it is happening in Venezuela.** Soros has changed his mind anyway. In April he gave the green light to his fund, which has USD 26 billion in assets under management to invest in Bitcoin.[21]

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

Rock and Coins

And yet another big name from the finance world has arrived: Venrock, the Venture Capital arm of the Rockefeller family (Ven stands for Venture, Rock for Rockefeller). Two of the most successful early investments of the company include Intel and Apple. Now they are heading into the crypto sector. In stark contrast to George Soros, Partner of Venrock David Packman doesn't hold back his enthusiasm regarding the new industry. More specifically, Venrock has a partnership agreement with CoinFund, a company based in Brooklyn.[22]

[17] See "Jamie Dimon Slams Bitcoin as a 'Fraud'," Hugh Son, Hannah Levitt and Brian Louis, *Bloomberg*, September 12, 2017.

[18] See "JPMorgan launches crypto strategy months after Dimon 'fraud' warning," Paul Clarke, *Financial News London*, May 17, 2018.

[19] See "JPMorgan has asked 29-year-old highflier to draw up a cryptocurrency strategy," Oscar Williams-Grut, *Business Insider Deutschland*, May 17, 2018.

[20] See "JPMorgan's Wall Street chief talk China, bitcoin, Amazon, and is preparing for an inevitable big downturn in stocks," Hugh Son, *CNBC*, May 16, 2018.

[21] See "George Soros Prepares to Trade Cryptocurrencies," Alastair Marsh, Saijel Kishan and Katherine Burton, *Bloomberg*, April 6, 2018.

[22] See "It Started With the Rockefellers: Now it's Takin on Crypto," Robert Hackett, *Fortune,* April 6, 2018.

CoinFund supports Start-ups which base their business model on the Blockchain technology. Both companies have invested in YouNow, an app for live video streaming which had planned an ICO last year. Yet another client of CoinFund is the Canadian Chat-app Kik, which already completed its ICO.[23] David Packman from Venrock commented on his company's entrance onto the crypto scene, that they are in it for the long haul: "There are many cryptocurrency traders. There are many cryptocurrency hedge funds. This is different. For us it looks more like Venture Capital."[24]

Venrock is not alone in its mission to infiltrate the market. Despite the consistent popularity of ICOs more and more, Venture Capital firms are looking for a way into the game. In just the first three months of this year Blockchain companies have been able to pull in a combined investment of USD 400 million.[25] It is doubtful though that many of these are actual long-term investments like Venrock's are meant to be. It seems to be the norm that investors buy in the Pre-Sale-Phase of an ICO since the value of their equity already rises through the ICO itself.[26]

The ICO-Bubble Continues

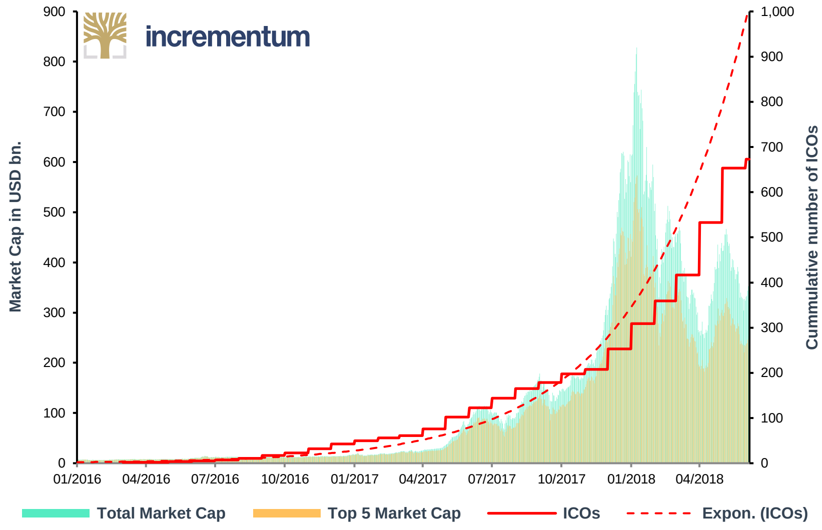
As a comparison: Blockchain companies have had an influx of over USD 3 Billion via ICOs just this year. It comes at little surprise that many of the investors, no matter if they bought in the Pre-Sale-Phase or during the actual ICO, get rid of their shares quite quickly. **Roughly half of all ICO funded projects have already failed.**[27] Many of these companies only exist on paper – the so called White Paper.

> *"Cryptocurrency protocols are like onions."*
>
> Vitalik Buterin

This investment boom is compared time and time again with the Dot Com Bubble. Many big players within the scene, like Ethereum founder Vitalik Buterin, have called out for caution in regard to an ICO Bubble. In our past reports, we have not only given the subject much room but have also warned against a too flippant approach when investing via ICOs. Especially, since regulation bodies are also highly alarmed. The question if a coin which is financed via ICO is in fact a security, and should be regulated as such, puts this process very much in the legal grey zone. The US authorities have already convened on this subject, more specifically looking at the sector's giants Ethereum and Ripple.

[23] See "VC Firm With Rockefeller Roots Turns to Crypto Startup," Olga Kharif, *Bloomberg*, April 25, 2018.
[24] See "Rockefeller's VC Arm Venrock Partners With Coinfund, Exec Highlights Focus On Long Term," Molly J. Zuckerman, *CoinTelegraph*, April 8, 2018.
[25] See "Blochain-Startups haben dieses Jahr bereits mehr Investment bekommen als 2017," Jakob Steinschaden, *Fortune*, April 6, 2018.
[26] See "Venture Capital Surges Into Crypto Startups," Olga Kharif and Camila Russo, *Bloomberg*, March 26, 2018.
[27] See "46% of Last Year's ICOs Have Failed Already," Kai Sedgwick, *Bitcoin.com*, February 23, 2018.

Figure 3: Cumulative Number of ICO´s vs. Market Capitalization.



Sources: coinmarketcap.com, coinschedule.com, Incrementum AG

A story which broke in the Wall Street Journal claiming there had been a meeting of regulatory authorities back in April caused for confusion and panic on the market.[28] It is unclear to this day if said meeting actually ever happened. What we however did find out in the course of the coverage of this story is that Ethereum and similar products have gained a huge fan base in the Tech-sector. Defenders of the crypto world are organizing themselves in Silicon Valley – once again driven mainly by Venture-Capital-investors. This new lobby wants to persuade the regulatory bodies to at least not classify already existing and successful projects such as Ethereum as mere securities. Initially founded via ICO, Ethereum's structure is now completely decentralized, they argue. And their voice seems to be heard. **In a speech on June 15, the SECs point man on crypto, William Hinman, stated, that Bitcoin and Ethereum are in fact not to be treated as securities.** However, he did not comment on Ripple.[29]

A Scam is a Scam – Even on the Blockchain

"Just because you call something a blockchain or an ICO, that doesn't mean you aren't subject to normal laws."

Juan Benet

The US regulatory board SEC has also started to act based on the existing rules.[30] A scam is a scam – even on the Blockchain. The founders of the cryptocurrency Centra were arrested in April. The charge: Their ICO had criminal intent and they relieved their investors of USD 32 million. Centra was supposed to be a crypto credit card and work together with Visa and Mastercard - at least that was what was advertised.

According to SEC, the company Centra never had a business agreement with either of the credit card providers. One of the two apparent imposters was caught just before leaving the country. "We allege that Centra sold investors on the promise of new digital technologies by using a sophisticated marketing campaign to spin a

[28] See "World's Second Most Valuable Cryptocurrency Under Regulatory Scrutiny," Dave Michaels and Paul Vigna, *The Wall Street Journal*, March 1, 2018.
[29] See "Bitcoin and ether are not securities, but some initial coin offerings may be, SEC official says. " Bob Pisani, *CNBC,* June 18, 2018.
[30] See "The SEC Is Finally Cracking Down On ICOS," Tyler Durden, *Zero Hedge*, March 1, 2018.

web of lies about their supposed partnerships with legitimate businesses", Stephanie Avakian, co-director of the SEC's Division of Enforcement, said in a statement Monday. "As the complaint alleges, these and other claims were simply false."[31]

Centra was not the first case to be looked into by the SEC. The AriseBank case, who's ICO was also stopped, involved more than USD 500 million. The Centra case is so juicy marketing wise because the famous boxer Floyd Mayweather had publicly endorsed the ICO.

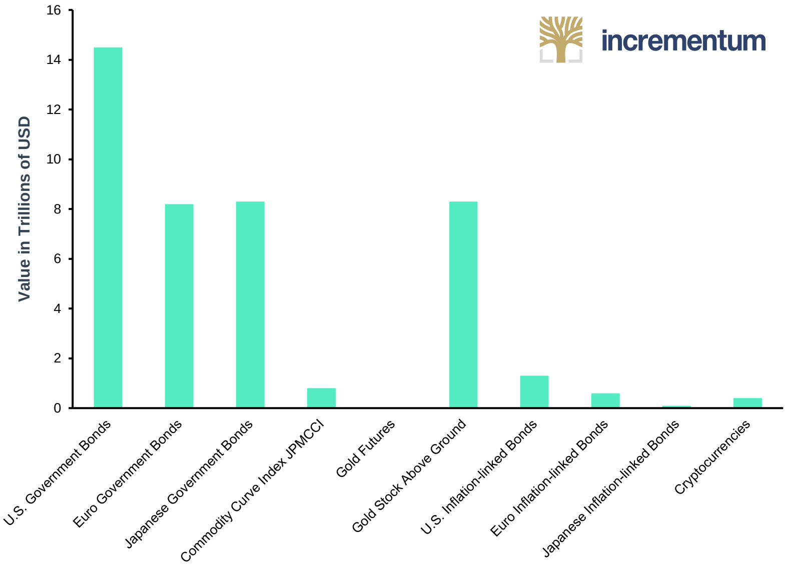
To educate investors, the SEC went as far as to create its own fake ICO as a honeytrap. They even wrote a White Paper full of the specific Blockchain language for the fake project "Howeycoins".[32] "Howeycoins" set out to disrupt the global tourist industry. The website looked like many others of which ICO investors have seen plenty, it even included the famous count down timer to indicate when the bonus phase of the ICO was to kick off.

Whoever clicked on "invest" ended up on the website of the US regulatory authority. This site also included a list of "red flags" to look out for and avoid. **For example, ICOs with celebrity endorsements should rather be avoided instead of gravitated towards.** This whole ploy was largely more successful than any official warning the SEC had issued up until then and shows that even regulators have a sense of humour.

"Early on, there was a strong suspicion that much of CCs were used in the illicit economy, largely because of the way CCs were set up as anonymous and off-the-official-grid. But recent surveys, and the small size of Bitcoin transactions, suggest that the share of illegal transactions had fallen to 20% in 2016 and has continued to fall since. Part of this is due to authorities clamping down on dark web sites and tax authorities starting to demand tax information from companies that support the CC world."

Mika Inkinen
J.P. Morgan

Figure 4: Total Value of Different Asset Classes.



Sources: J.P. Morgan Perspectives 2018, Incrementum AG

[31] See "Founders of cryptocurrency backed by Floyd Mayweather charged with fraud by SEC," Arjun Kharpal, *CNBC*, April 3, 2018.
[32] See "ICO Howeycoins," *Investor.gov*, 2018.

Robby Bradford
@RobbyBradford2

A giant Bitcoin logo has been projected onto the Swiss National Bank in the centre of Zurich. A photograph of

3:05 PM - 30 Apr 2018

903 Retweets 2,601 Likes

Authorities are also looking into potential price manipulation. **The US Department of Justice has opened a new investigation in regard to illegal practices.**[33] **This includes spoofing or strategically placed buy and sell orders used to manipulate the market, which are deleted before being activated**. Also, the act of "wash trading", the manipulation of prices through a participant who completes his own orders. The Billionaires Mike Novogratz and Cameron Winklevoss have both whole heartedly supported the supervisory authorities' attempts in the field of cryptocurrencies. "Weeding out the bad actors is a good thing, not a bad thing for the health of the market," Novogratz, said in a telephone interview. "Plenty of exchanges have these inflated volume numbers to create some sense of excitement around coins," he said, citing his own experience trying to trade.[34]

One thing is for sure: the big players want in on the action. But only in areas where the rules are clear and above board can they actually also play. This has led to a behind-the-scenes race of the big names. It is not about investing now, it is about being the best prepared player when the time has come, the dust has settled and the rules are clear. This creates more pressure on the authorities to come up with rules which give investors and consumers legal security, but also don't jeopardize this new sector.

For this report, we have especially highlighted the role of the US authorities as they have been extremely proactive here. It should be noted that almost all countries are currently asking the same question: How can we regulate without strangling the Bitcoin sector? This means there is not only a race to regulate between states, but also between national governments and the international organizations. At the moment one can say the governments are leading the way.

In some EU countries, such as Austria and Germany, there will be obligatory rules regarding ICOs soon. An overall EU law is currently not on the agenda.[35] Although, the fifth know-your-customer and anti-money laundering directive is expected to include specific provisions for cryptocurrencies. As predicted in the last report, the attempts of the G20 have also been without results so far. However, even the managing director of the IMF, Christine Lagarde, has said that something is needed. Regulating the sector is unavoidable, she said, but a balanced approach would be commendable.[36]

[33] See "U.S. Launches Criminal Probe into Bitcoin Price Manipulation," Matt Robinson and Tom Schoenberg, *Bloomberg*, May 24, 2018.

[34] See "Probe into Bitcoin Price Manipulation Probably 'A Good Thing', Novogratz Says," Camila Russo, *Bloomberg*, May 24, 2018.

[35] See "ICOs: EU-Kommission plant in naher Zukunft keine einheitliche Regulierung," Bastian Kellhofer, *Trending Topics*, March 9, 2018.

[36] See "An Even-handed Approach to Crypto-Assets," Christine Lagarde, *IMF Blog*, April 16, 2018.

You Can Buy an Exchange

"Cryptocurrency is such a powerful concept that it can almost overturn governments"

Charles Lee

Other participants are also preparing for the days with more transparent rules in the land of Bitcoin. The Intercontinental Exchange (ICE), the mother company of the New York stock exchange, publicly announced to be working on a Bitcoin trading tool at the same time the New York Times article about Goldman Sachs broke. The technology exchange Nasdaq also seems to be well underway in this direction. Nasdaq CEO Adena Friedman is quoted saying just in April of this year "There is no doubt that Nasdaq will consider becoming an exchange for digital cryptocurrencies." That same day, Nasdaq announced a cooperation with the American Bitcoin exchange Gemini. According to some sources, the second largest exchange of the US could start trading Bitcoin as early as October 2018.[37]

These plans correspond perfectly with Goldmans and others plans. **The big institutional players obviously need big, regulated exchanges in order to start trading.** Goldman can't just open a Binance account.

However, there is another way. You can simply buy an exchange. The investment bank itself didn't do so, but the start-up Circle which is supported financially by Goldman did. At the end of February, Circle acquired the popular crypto exchange Poloniex.[38] The "NYT" journalist Nathaniel Popper got his hands on internal presentations which explain the motivation behind this takeover: Circle wants to keep Poloniex as an independent exchange, however they are looking to work very closely with the SEC. The goal: Circle wants to make Poloniex the first regulated crypto exchange in the USA.[39]

The slides read as follows: "By becoming the first regulated Crypto Exchange will enable Circle to list and provide a platform for all forms of emerging crypto tokens, including tokens that would be deemed securities. We believe the market for security-like tokens will continue to expand, creating demand for this market infrastructure. Circle (and evidently Goldman) are obviously preparing for a world in which regulated securities can be traded on the Blockchain as a token. The plan goes on: Circle wants to introduce a cryptocurrency which is bound to the Dollar. **A Crypto-Dollar by a company which is covered by Goldman Sachs would be a complete and utter game changer.** The issue of regulation is completely open in this aspect as well.

We assume that the race for the Bitcoin infrastructure has only just begun. That every step is a step into a legal grey zone still discourages many institutional players. Some, such as the huge investment manager Vanguard, are steering clear of the sector all together. In May, CEO Tim Buckley went as far as saying: "You will never see a Bitcoin fund from us. We stay away from assets which don't have a sound basic economic value and don't generate income or cash flow."[40]

[37] See "Nasdaq May Launch Bitcoin Trading in October 2018," Marko Vidrih, *Medium*, April 27, 2018.
[38] See "Circle Acquire Poloniex," Sean Neville and Jeremy Allaire, *Circle*, February 26, 2018.
[39] See tweet by Nathanial Popper on Twitter, February 26, 2018.
[40] See "Vanguard chief: You will never see a bitcoin fund from us," Thomas Franck, *CNBC*, January 22, 2018.

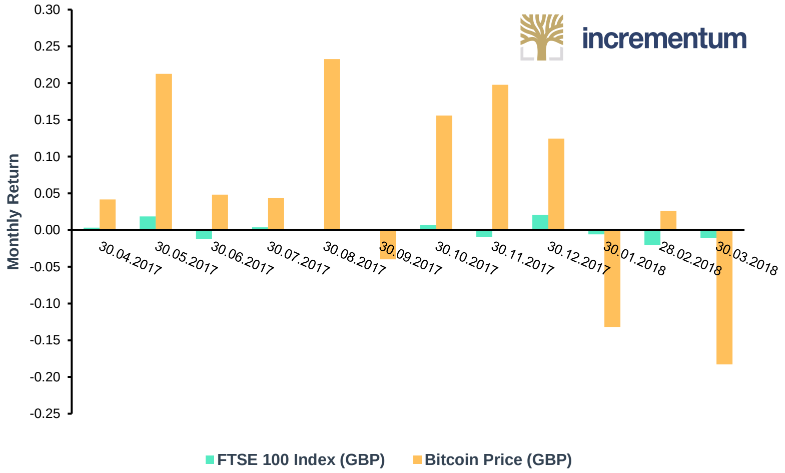
Conflict of Generations

"Bitcoin is a very exciting development, it might lead to a world currency. I think over the next decade it will grow to become one of the most important ways to pay for things and transfer assets."

Kim Dotcom

Similar to Warren Buffett, who misses no opportunity to hate on Bitcoin, companies such as Vanguard have no interest in making Bitcoin sound too interesting as an investment. They want their clients to continue to put their money in traditional investment opportunities. There is more behind this all than the mere discussion and discourse about the Blockchain technology. It is a generation conflict. Millennials, people aged between 18 and 39, are deeply influenced by the last financial crisis. This coincides with the fact that this is the generation which grew up with internet access. A whole row of studies show that Millennials are the most likely to be interested in crypto assets.[41]

Figure 5: Bitcoin and FTSE 100 monthly Returns from Q2 2017 – Q2 2018



Sources: Coindesk, Yahoo Finance, Incrementum AG

The combination of technological trust and wariness towards the financial system is a dangerous one for providers of legacy investment products. It is to be expected that established players such as Buffet and Vanguard will be become more and more outspoken against Bitcoin. Others such as Goldman have already decided to go a more proactive route and be first in line when it comes to institutions embracing the new sector. And others like J.P. Morgan have proven that they can and must change their thinking.

Without a doubt, the economic success of the partially dubious crypto exchanges must have drawn the attention of the big players to the sector itself. The top 10 exchanges generate roughly USD 3 million in fees per day. Just the top two, Binance and OKEx, have a daily trading volume of approximately USD 1.7 billion. "The exchanges and transaction processors are the biggest winners in the space because they're allowing people to transact and participate in this burgeoning sector," said Gil Luria, an equity analyst at D.A. Davidson & Co, who reviewed the methodology for the revenue estimates. "There's a big business there and it would not surprise me if they're making hundreds of millions of dollars in revenue and possibly even billions a year."[42]

[41] See "A bitcoin bubble made in millennial heaven," *Financial Times*, 2018.
[42] See "Crypto Exchanges Are Raking in Billions of Dollars," Camila Russo, *Bloomberg*, March 5, 2018.

"We don't really know how this coin is created. You can't have a functional money without a basic transparency. Unless you are addicted to volatile trading for the sake of trading, stay away from the Bitcoin. Thankfully its plunge will be a salutary caution to most folks."

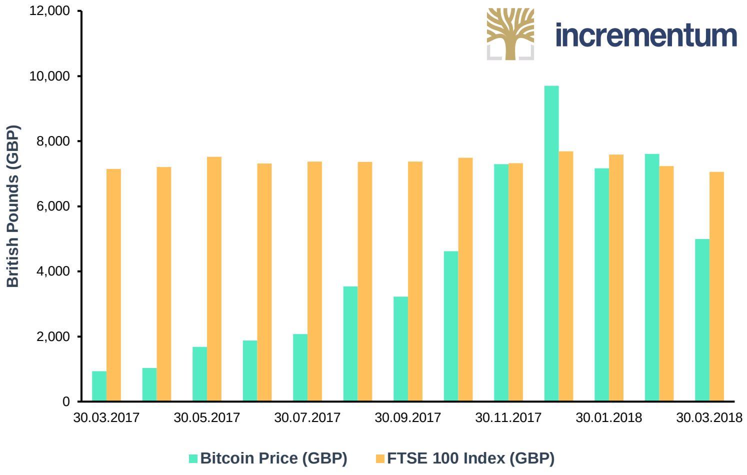
Steve Forbes

Of course, at the moment it is still unclear if the crypto exchanges of today will even be around tomorrow. The current market leader Binance is just over a year old. If established players such as Nasdaq really set their sights on these markets, they will subsequently also be able to pull in a lot of investors. This is however in the distant future. There are still a few battles to be fought – also in the generational conflict of the exchanges.

One player deserves special attention: Coinbase. Subject of many chats within crypto forums is the speculation of which coin will next be released on the Coinbase platform. The "standard" app for Bitcoin newbies has more than 20 million clients - more than the traditional US investment management firm Charles Schwab. The US company is currently expanding in many directions simultaneously. The Coinbase app is available in 32 different countries and has additionally initiated a crypto fund. The fund is currently only available for US investors and only if they decide to invest at least half a million USD. The name of the new venture speaks volumes of where this ride will take us: Coinbase Asset Management.[43]

Coinbase has its own exchange, Gdax, which will soon be relaunched as "Coinbase Pro". Additionally, Coinbase recently purchased Paradex. This "decentralized" exchange not only takes care of the storage of tokens of their customers, but also allows users to directly trade with each other. Speculators say the purchase of Paradex is paving the way for Ethereum based ERC20 tokens to be launched on the Coinbase exchange. Currently the app only offers four cryptocurrencies: Bitcoin, Ethereum, Litecoin and Bitcoin Cash.[44] Ethereum Classic could also be added soon.

Figure 6: Bitcoin and FTSE 100 from Q2 2017 – Q2 2018



Sources: Coindesk, Yahoo Finance, Incrementum AG

Last but not least, Coinbase has also entered the Venture Capital sector and has initiated their own incubator fund for start-ups in the crypto sector. "It could be possible that we start investing in companies that look a lot like competition for

[43] See "The SPY of Crypto? Coinbase Launches Cryptocurrency Index Fund," Tyler Durden, *Zero Hedge*, March 6, 2018.

[44] See "Coinbase acquires cryptocurrency trading platform Paradex," Anna Irrera, *CNBC*, May 23, 2018.

Coinbase. We have a long-term perspective and believe that different approaches are healthy and viable”, Coinbase stated on their blog.

Bitcoin Has Become Mainstream

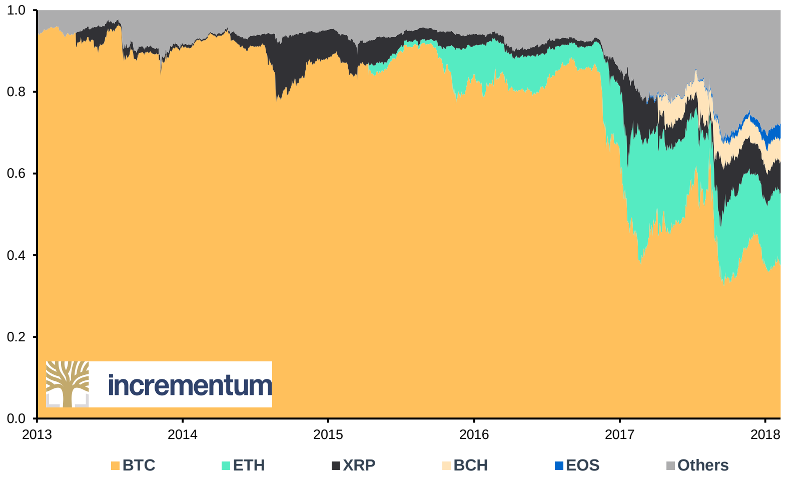
“I think the fact that within the Bitcoin universe an algorithm replaces the functions of the government is actually pretty cool. I am a big fan of Bitcoin.”

Al Gore

Predictions are always tricky. But the abundance of activity within the Bitcoin sector since the crash of January 2018 goes to show that cryptocurrencies are far from dead. It is however still most probable that only a few of the Boom phase projects will survive in the long run. The overall dominance of Bitcoin is not in danger at the moment.

The infrastructure side of things promises to be very active in the coming months. We will stay tuned. New players such as Binance are attacking companies like Coinbase. In addition, there is a continuously growing list of newcomers: from Goldman all the way to start-ups like Revolut or exchanges such as Nasdaq. Within the crypto market itself, there are of course also many promising projects. While the market is still recovering from the ICO Bubble, new coins which aren’t based on the classic Blockchain are gaining traction. One example is the Iota project which is already pretty popular in Europe, and is investigated in length in next chapter of this report.

Figure 7: Top 5 coins in % of total market capitalization.



Sources: coinmarketcap.com, Incrementum AG

Bitcoin and the crypto sector have become mainstream. We won’t find out what this all really means until we have finally come out the other side of this valley of doom. As with most things in life, in hindsight we will be wiser as to where the real bottom of the Bitcoin price in 2018 was and if we have already seen it or not.

Vontobel

Investment Banking

Driven by the power of possibility

vontobel.com

Crypto Concept: Consensus Mechanisms

"Distributed consensus simply means a large pool of people who are geographically segregated agreeing on something. In cryptocurrencies like Bitcoin, 'something' here means agreeing on which transactions or blocks are valid and which are invalid to be added/rejected to the blockchain."

Sudhir Khatwani

Key Takeaways

- **Investors can earn up to 7.5 % in annual return by buying cryptocurrencies and staking the investment in a cryptocurrency wallet. Tokens such as Dash, PIVX, and Stratis all pay interest on account holdings. Minimum investments may apply.**
- **Proof-of-work and proof-of-stake are the two most common consensus mechanisms; however, over 17 different consensus mechanisms exist. Allocating investments across different consensus mechanisms provides diversification.**

"Invest in things that have never happened before, hedge for regression to the mean, and plan for the unimaginable."

John Burbank

In cryptography, there is a theory that states that anything that can be done with a central party, can also be done without a central party. This refers to voting, auctions, banking, etc. For example, OpenBazaar is a decentralized version of eBay, Bisq is a decentralized version of Coinbase, and Bitcoin itself is a decentralized version of fiat currency. In a decentral network there is no ruler to make sure that everyone follows the rules. Instead, decentral networks rely on consensus mechanisms.

A consensus mechanism is the way that a group of people make a decision. For example, Bitcoin users need to constantly update their history of transactions in order to reflect new transactions and wallet balances. Consensus mechanisms enable strangers to come to an agreement by giving financial rewards or financial punishments. A major goal of consensus mechanisms is to stop users from double-spending the same coin. If a user could send the same Bitcoin to two different wallets, then the supply of Bitcoin could be inflated infinitely, which would result in a decrease in the purchasing power of the currency. In order to stop double-spends, every computer that maintains the Bitcoin blockchain needs to have the same information about which wallets hold what amounts of value.

Table 1: Consensus Mechanisms of the Top 100 Cryptocurrencies.

Consensus Mechanism	Cryptocurrencies
Proof of Work	Bitcoin, Ethereum Classic, Syscoin, DigiByte,
Proof of Stake	NXT, PIVX, Reddcoin, Stratis, Ardor, Neblio,
Leased Proof of Stake	Waves
Delegated Proof of Stake	EOS, Lisk, Nano, Steem, BitShares, Ark, GXChain
POW/POS Hybrid	IOTA, Ethereum, Dash, Power Ledger, Enigma, Dragonchain
Federated Byzantine Agreement	Ripple, Stellar
Byzantine Fault Tolerance	Ontology,
Delegated Byzantine Fault Tolerance	NEO, Gas
Practical Byzantine Fault Tolerance	Hyperledger
Proof of Asset	DigixDao
Proof of Storage	Siacoin
Proof of Intelligence	Aion
Proof of Believability	IOStoken
Proof of Devotion	Nebulas
Proof of Retrievability	Storj
Proof of Authority	VeChain

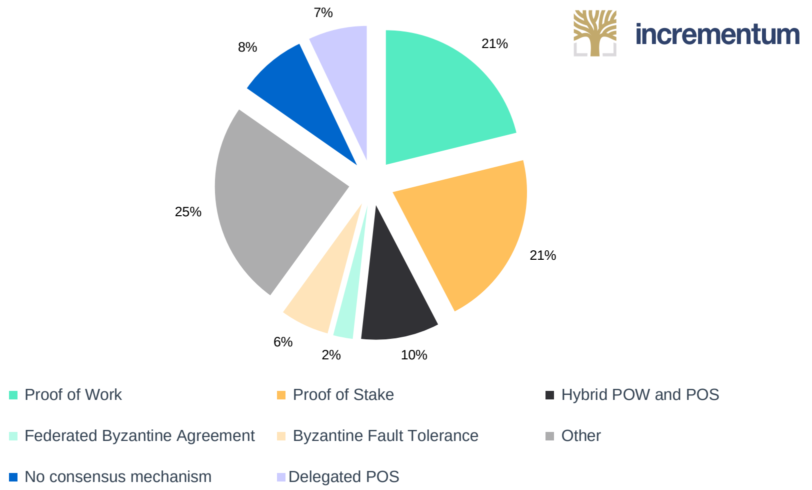
Source: White Papers, Incrementum AG

"Markets are adapting to a new set of rules, while most market participants are still playing by the old."

Bob Farrell

As shown in Table 1, around 17 different consensus mechanisms exist; however, none of them are perfect. So far, the most secure consensus mechanism is still the original one used by Bitcoin: proof of work. However, proof of work relies on miners, which can lead to centralization. Developers are constantly trying to beat proof of work because a coin that removes miners and their electricity consumption would splash big waves in the ICO market.

Figure 8: Consensus Mechanisms of Top 100 Cryptocurrencies.



Source: Incrementum AG.

Companies such as Visa and PayPal do not need to employ a consensus mechanism because they control the entire network. If someone uses their Visa credit card, the information is sent to a centralized database that is maintained by Visa. We trust these companies to protect our sensitive information and settle our transactions. Since Visa controls the network, they can reverse and censor transactions. In the 1970s, computer specialists began to explore other ways to solve this problem because they realized that even a central authority can be hacked by an adversary or corrupted from within. The two most popular methods for taking decentralized decisions in a cryptocurrency network are known as “proof of work” and “proof of stake”. However, dozens of consensus mechanisms exist including proof of authority, proof of space, proof of importance. All of these different methods are proposed solutions to the Byzantine Generals’ Problem.

Byzantine Generals’ Problem

Imagine there is a king in a castle defended by 300 soldiers. The castle is surrounded by five armies of 100 men each. Each army has its own camp in the surrounding hills and its own general. The generals need to communicate with each other in order to agree on an attack strategy. However, the generals cannot easily trust each other because they suspect that some of the generals are traitors. If they send a message on horseback from one camp to another with the time of the attack and strategy, then the disloyal generals could easily change this message and relay false information to the next camp. Sending a simple message is not secure because written text is easy to change. Misinformation could result in the traitors winning the battle because the different camps will attack at the wrong time or not attack at all.[45]

“Whether it be miners, oracles, witnesses, delegates, or stakers, they all have their own flaws and drawbacks.”

JP Buntinx

[45] See “Bitcoin and the Byzantine Generals Problem“, Patricia Estevao, *We Use Coins*, July 13, 2015.

Investor Alert: Proof of Work Mining

Large professional data centers have taken over the cryptocurrency mining business because this industry exhibits economies of scale. Historical mining revenues are easy to compute; however, forecasting future revenues depend on the cryptocurrency's price and transaction fee. For example, the Bitcoin network creates 1,800 new coins per day. With a price of Bitcoin at USD 7,000, this equates to USD 12.6 million in daily revenue from minting new Bitcoin. Currently, the daily amount of transaction fees accrued to miners is approximately USD 300,000. This means that transaction fees are currently a small fraction of the total revenue earned by miners.

Costs of mining depend on several factors including electricity costs and climate. Mining has fixed and variable costs. Fixed overhead costs include renting warehouses to store mining hardware, hiring employees to oversee operations, and building direct access to an affordable electricity source. Variable costs include electricity consumption for mining and cooling, number of mining rigs, and mining pool fees. The CEO of Alpine Mining in Valais, Switzerland, Ludovic Thomas estimates that electricity costs are 70% of their total costs.

For investors who are interested in gaining access to mining without opening a mining operation, the Logos Fund registered with the German BaFin in June of 2016 works with one of the world´s largest mining companies, Genesis.

Nowadays, a conference call could replace the messenger on horseback, but the problem still persists. How can you be sure that the message is authentic and not tampered with? Authenticity refers to the problem that adversaries can fake phone calls or emails by pretending to be someone else. Tampering refers to the content of the message being changed, deleted, or read by an adversary.

To solve the Byzantine generals' problem, consensus algorithms rely on two concepts. First, each of the generals would need to invest resources into the network, i.e. they need to have "skin in the game." For example, imagine two businessmen decided to co-found a venture, and one refused to invest any time or capital into the venture. The invested partner would feel suspicious of his partner's loyalty to the project. The same idea holds in a decentralized network. The second concept is that there must be a ledger of all previous communication that is "tamper-proof". Tamper-proof refers to the ability of the computers to immediately detect when the history of communication has been changed or deleted. The digital version of the ledger is a blockchain that tracks each user's transactions and links them using hash functions that ensure the data's authenticity.[46]

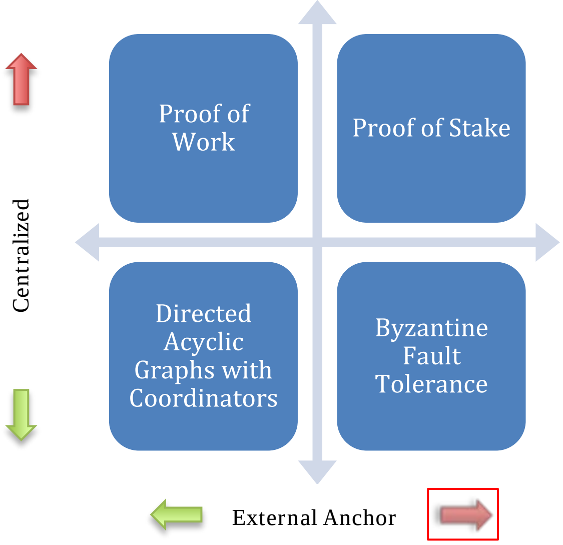
To go back to the Byzantine Generals' problem, one way they could ensure the loyalty of their comrades is to make each general invest a large sum of money in an escrow account that is impenetrable. Before a general sends a message, he must sign his name with a cryptographically secure signature that proves his identity. If any of the generals misbehave, the army will look at the message book and see the traitor's signature. The traitor can still misbehave, but now he will suffer financially because the army will not give him back his deposit. This method of coming to a decentralized consensus is referred to as "proof of stake" because each general, or computer user in modern times, has a stake invested in the success of the network. Another option would be for the network to force each general to solve an extremely complex math problem before they can successfully sign and send a message. To solve the math problem quickly, the general would need to invest large sums of money in expensive mathematicians. This consensus method is called "proof of work" because the general proved that he invested scarce resources such as time and capital into solving the math problem.

[46] IOTA and Byteball use a directed acyclic graph instead of a blockchain to record transactions.

Overview of Consensus Mechanisms

As shown in Figure 9, consensus mechanisms exist along two main axes, degree of centralization and degree of external anchor. The vertical axis ranges from centralized, where you need to trust a person or an organization to settle transactions correctly, to decentralized, where strangers settle transactions. For example, Bitcoin's proof of work consensus mechanism is an example of a permissionless and public blockchain because an untrusted stranger can become a transaction validator and their identity does not need to be disclosed. Another example is Monero.

Figure 9: Centralization and Externality of Consensus-Mechanisms.


Proof of Work
Proof of Stake
Centralized
Directed Acyclic Graphs with Coordinators
Byzantine Fault Tolerance
External Anchor

Source: Incrementum AG.

> *"So, the problem is not so much to see what nobody has yet seen, as to think what nobody has yet thought concerning that which everybody sees."*
>
> Arthur Schopenhauer

The horizontal axis refers to what kind of investment a user needs to pledge in order to gain power within the system. For example, Bitcoin requires users to pledge scarce resources in the real world in order to make decisions in the Bitcoin network. This is referred to as an external anchor. In contrast, consensus mechanisms that fall into the upper right quadrant, such as proof of stake, do not require external resources in order to make decisions within the network. This quadrant includes coins such as NXT and Peercoin. Ethereum is planning to switch from the upper left quadrant to the upper right quadrant over the next year.

On the other side of the spectrum in the bottom right quadrant are permissioned and private consensus mechanisms such as byzantine fault tolerance. IBM's Hyperledger is an example of a data structure that allows the creator to specify who will settle transactions. A company that uses Hyperledger or Microsoft's Blockchain as a service will know the identities of the people that they select to control the network, and the users of the network will need to trust these people. **These systems are centralized, and they do not have external anchors.** In the bottom left quadrant are coins like IOTA, Byteball, and Hashgraph. These coins have witnesses and coordinators that centralize the system; however, they still require the validators to pledge external resources in order to gain power within the network. The most common consensus mechanism is the directed acyclic graph structure combined with proof of work to prevent Sybil attacks.[47]

Proof of Work

In the case of Bitcoin, you can think of the Byzantine Generals as different Bitcoin wallets. Computers that run the Bitcoin software use the proof of work consensus algorithm to come to an agreement on which payments are valid.

According to Hristian Hristov at the BlackSeaChain Conference, proof of work is

> *“a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with a low probability so that a lot of trial and error is required on average before a valid proof of work is generated.”*

If Mark wants to send 5 Bitcoins to Demelza, the entire network must ensure that Mark has the 5 Bitcoins and that the transaction is being signed with Mark’s digital signature. Bitcoin nodes come to an agreement every ten minutes about which transactions are valid in a process known as “mining”. Before confirming a new block of transactions, the miners compute hashes until they find a desirable number that is less than a specific number set by the software protocol called the difficulty target. In the Bitcoin protocol for example, miners must find the right “nonce”, or arbitrary number, that produces a hash lower than the difficulty target set by the software. This is called a hash-puzzle because the miner must add the nonce to the hash of the previous block in the blockchain. The computational output is a number which basically falls into a target space which is comparatively small in relation to the large output space of the entire hash function.[48] This number becomes that block’s identification number, which is used as an input in the next block’s hash puzzle.

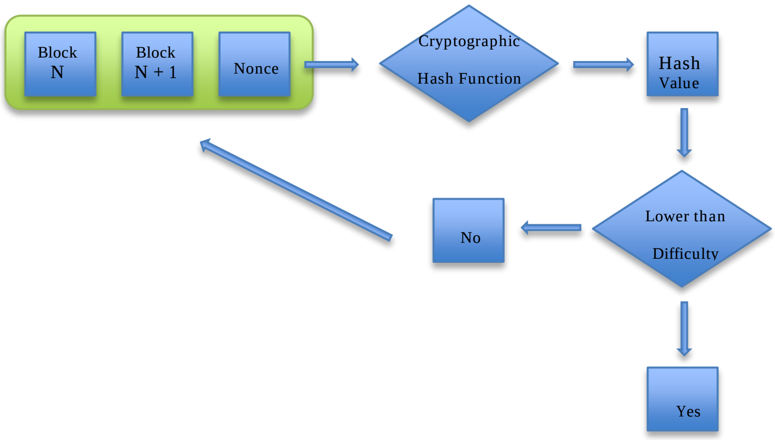
“Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value”.

Eric Schmidt, CEO of Google

[47] Witnesses & coordinators are meant as a temporary measure until the network reaches scale according to developers; however, the path to decentralization is not clearly defined.

[48] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies. New Jersey: Princeton University Press.

Figure 10: Proof of Work Computation.



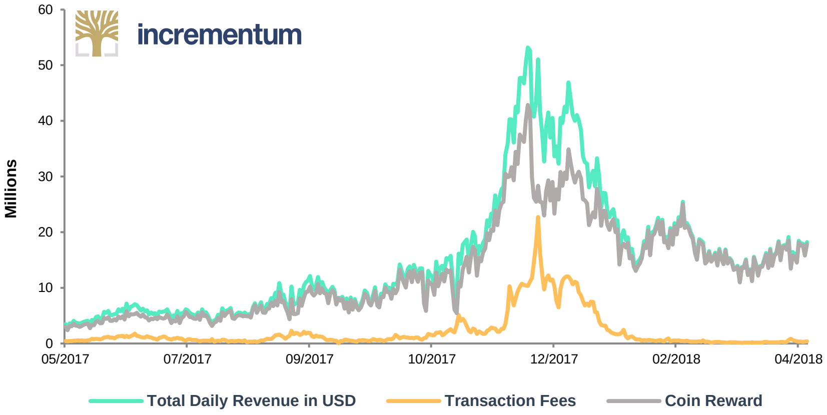
Source: Incrementum AG.

"Every informed person needs to know about Bitcoin because it might be one of the world's most important developments."

Leon Luow
Nobel Peace Prize Nominee

Proof of work uses two main types of financial rewards to incentivize users to maintain the network: **rewards and transaction fees**. The first miner to find a hash that is lower than the given difficulty target will be entitled to "print" new Bitcoins and receive the transaction fees that the senders paid to the network when they broadcasted their payments. The first transaction of every block is a "coin-creation transaction". The coin-creation transaction allows the miner of the block to mint new Bitcoin and to send these new Bitcoin to his or her wallet. In 2016, the value of the block reward was about 25 Bitcoins.[49] However, this rate drops roughly every four years and is currently 12.5 Bitcoins. The block reward incentivizes honest behavior because the coin-creation transaction will only be valuable if it is accepted by the other users maintaining the network. The second reward is the transaction fee. When users send Bitcoin transaction they attach a fee. The higher the fee, the more likely a miner will include the transaction in their candidate block, which means the confirmation time of the transaction will be faster.

Figure 11: Bitcoin Mining and Transaction Revenues



Sources: Blockchain.info, Incrementum AG.

"Virgin Galactic is a bold entrepreneurial technology. It's driving a revolution and Bitcoin is doing just the same when it comes to inventing a new currency."

Sir Richard Branson,
Founder of Virgin Records

[49] Ibid.

Investor Alert: Proof of Stake

Several cryptocurrencies offer investors returns simply for owning the cryptocurrency. Dash, NEO, PIVX, and Stratis are just a few examples.

1.) Although Dash is considered to have a master-node version of proof of work, Dash's consensus mechanism is closer to a hybrid between proof of work and proof of stake. Dash investors can earn more than 7.5% annually just for holding their long positions. To earn new Dash by staking, an investor must purchase 1,000 Dash and leave their coins in an official Dash wallet that is similar to an escrow. With a price of USD 250 per coin, the minimum investment is equal to USD 250,000.

2.) NEO offers 5.5% annual return and no minimum investment required.

3.) PIVX offers 4.8% annual return and has a minimum investment of 10,000 PIVX. With a current price of USD 6, this equates to USD 60,000.

4.) Stratis offers between 0.5% and 1% annually. There is no minimum investment.

While staking the coins, the investor's computer must be constantly on and running the wallet software. The risks are the same as holding normal cryptocurrencies. Losing passwords, getting hacked, and decreasing value in terms of fiat.

However, Bitcoin's proof-of-work algorithm has disadvantages. First, there are several attack vectors that adversaries can exploit including:

- race attack
- Finney attack
- vector 76 attack
- alternative history attack
- majority attack
- denial-of-service-attack
- Sybil attack
- selfish mining

Second, the network uses large quantities of energy and hardware equipment, which have been estimated to cost approximately $400 million per year. Since more and more entrepreneurs are joining the mining industry, the difficulty of finding a Bitcoin block continuously increases. Consequently, the electricity a miner must buy to find a block is constantly increasing. This is why mining has naturally become centralized in countries where electricity is cheap. Table 2 shows the cost of electricity in several counties.

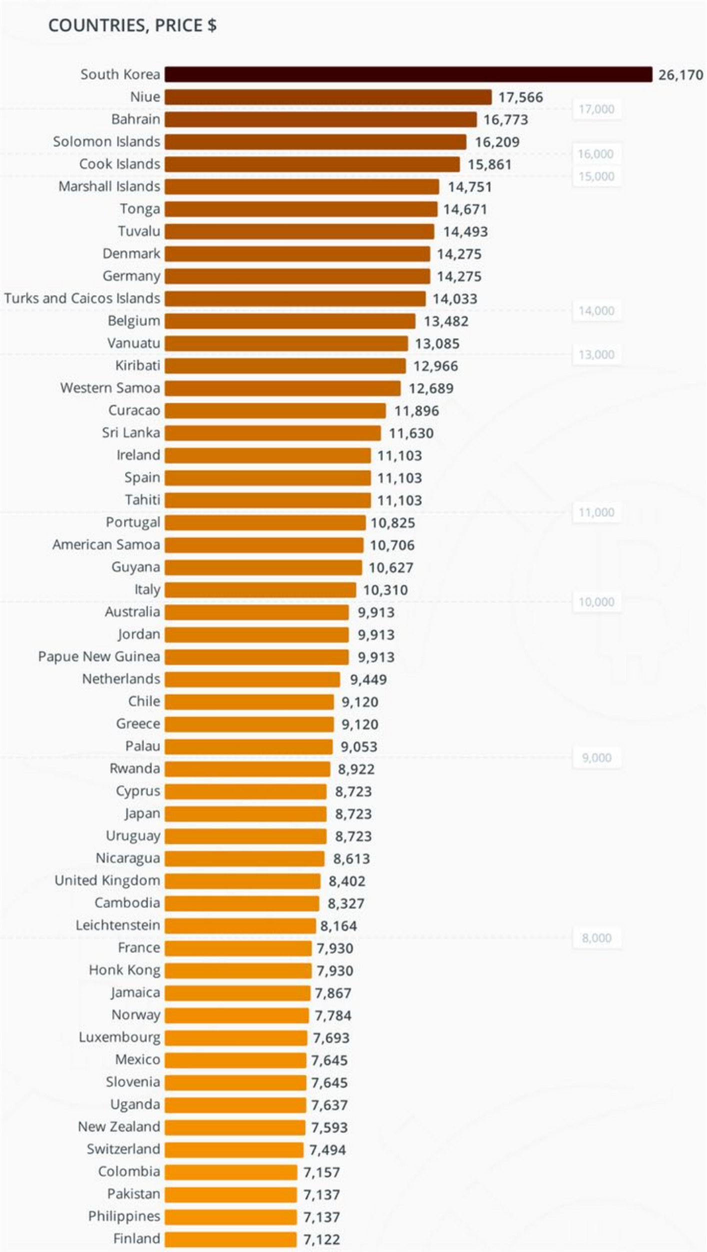
Like gold, Bitcoin uses electricity and capital equipment to mine new coins. The probability of randomly being chosen to create a block and receive a reward is equal to each miner's amount of mining power divided by the total amount of mining power on the network. The more power the mining hardware consumes, the higher the hash rate. This results in a higher profit from mining. The parameters used to calculate include: difficulty factor, hash rate (TH/s), BTC/USD Exchange rate, pool fees in %, hardware cost (USD), power (watts), power cost (USD/kWh).[50]

Table 2: Cost of Electricity by Country in 2018.

Country	Price per KwH in USD
USA	$0.10
Iran	$0.0375
Switzerland	$0.098
Austria	$0.15
China	$0.08
Iceland	$0.043

Source: Incrementum

[50] See "Is Bitcoin Mining Profitable in 2018," Ofir Beigel, *99Bitcoins*, 2018.



Proof of Stake

Unlike Bitcoin or gold, proof of stake allows the users with the largest holdings to create coins out of thin air. In a proof-of-stake system, the probability of receiving a reward is equal to the fraction of coins held by the user divided by the total number of coins in circulation. Several varieties of proof of stake exist including leased proof of stake and delegated proof of stake.

Both systems achieve similar outcomes; however, proof of work incurs a negative externality on the environment. **Then why are people still using proof of work?** The highest market capitalization coins all rely on proof of work but proof of stake is gaining popularity: Ethereum, the second largest market capitalization coin, is expected to switch from proof of work to delegated proof of stake during the next year.

Proof of stake attack vectors:

- nothing-at-stake attack
- short- and long-range attacks
- precomputing attack
- denial of service
- Sybil Attack
- bribe Attack

In addition to attack vectors, proof of stake has not been well tested on the market. Although many supporters of proof of stake claim that it is less centralized than proof of work, this is not necessarily true. Since investors receive interest on their long positions, proof of stake encourages hoarding more than proof of work. As Andreas Antonopoulos explained during the Wisma BeeOn Group in Kuala Lumpur, Malaysia, proof of stake allows **the rich to get richer**. This has a centralizing impact on the holders of the cryptocurrency. In contrast, proof of work miners are forced to release a certain number of coins to the market in order to invest in new mining hardware and to pay electricity bills. This allows a relatively constant amount of newly minted Bitcoins to hit the market every day.

Ethereum Casper Proof of Stake

The second largest cryptocurrency Ethereum is planning to switch to proof of stake from proof of work over the next few years. Ethereum will use a special kind of proof of stake called Casper, which was originally proposed in 2014 by Ethereum developers Vlad Zamfir, Vitalik Buterin, and Virgil Griffith. Casper is a form of delegated proof of stake whereby each validator gets to vote on which proposed block should be added to the blockchain. If the validator votes correctly, meaning that the block they chose is successfully added to the Ethereum blockchain, they receive transaction fees. The special feature of proof of stake is that Casper punishes malicious nodes by taking away their staked Ether.

Ethereum has not announced the official minimum investment yet; however, they have discussed 1000 Ethereum online. With a current price of $780, staking Ethereum would cost approximately $780,000. Since Casper has not been fully integrated into Ethereum, the return on this investment is not yet known.

Conclusion

The main trade-off that cryptocurrencies face is between centralization and efficiency. The more centralized the decision-making process is, the faster the decision can be taken and the more scalable the network is. On the other hand, the less centralized a network is, the longer it takes to come to a consensus. This is not unlike the dichotomy between dictatorships and direct democracies. When the hierarchy between shareholders is flat, unanimous decision making is difficult to achieve. Although the introduction of counterparties may not be a problem in every case, the original goal of the blockchain technology was to create consensus without intermediaries. Miners, oracles, witnesses, delegates, or stakers all centralize the system to some degree. **A consensus mechanism that could remove proof of work's electricity use without introducing a directed acyclic graph coordinator would make huge headlines in the cryptospace.** MIT cryptographer, Silvio Micali, reports that his consensus mechanism, Algorand, achieves decentralization and security simultaneously. We plan to keep this algorithm and coins that employ it on our radar. Also, coins such as Tezos and Dfinity promise to embed governance at the protocol level, which may enable decentralized shareholders to come to a consensus faster. While we are optimistic about the ability of developers to overcome the scaling problem in the long run, we recognize that proof of work's proven track record of at least ten years makes it the undefeated champion of consensus mechanisms. However, governments may crack down on the use of electricity to mine cryptocurrencies, therefore, we recommend holding a range of cryptoassets with different consensus mechanisms.

Cryptocurrencies.
The New Asset Class.

Regulated | Diversified | Liquid

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

Competing Currencies and Digital Money: How Hayekian Are Cryptocurrencies?[51]

"The history of government control over money is, with the exception of a few fortunate time periods, a history of unceasing deceit and fraud."

Friedrich A. von Hayek

Key Takeaways

- **Economic crises are often attributable to governments abusing their monopoly on money.**
- **Hayek pleads in favor of private currencies which can evolve in a decentralized discovery procedure and are free to compete with government issued fiat money as well as against each other**
- **Free choice in currencies on the part of money users would give both private suppliers of money and governments an incentive to issue sound money and exercise fiscal discipline.**
- **Cryptocurrencies harbor the potential for the emergence of a competitive monetary order.**
- **"Hayek would prefer gold to Bitcoin": Interview with Dr. Richard Zundritsch, F.A. Hayek's nephew**

[51] Curtesy of the "In Gold we Trust" Report 2018, where this article initially was published.

The Government Monopoly on Money – For a Long Time Unquestioned

“I do not think that it is an exaggeration to say that history is largely a history of inflation, and usually of inflations engineered by governments and for the gain of governments.”

Friedrich August von Hayek

It is a truism that monopolies are detrimental to economies. They are inefficient with respect to quality and cost, their price fixing generates welfare losses, and beyond this, they occasionally waste substantial resources merely on erecting barriers to entry for competitors.[52] In an efficient economic order, monopolies are therefore either prohibited or are at least subject to curbs.

Natural monopolies[53] and government monopolies represent special cases. The latter are based on the notion that the state is able to fulfill certain tasks either more efficiently or in a more “social” manner than private suppliers are. These tasks include security (the monopoly on the legitimate use of physical force), state-run health insurance schemes, and the provision of transport infrastructure.

“The motive of protecting and expanding political power ultimately infuses the entire history of money, which can be read as a history of monetary manipulation.”

Norbert F. Tofall

The monopoly on money is a very powerful tool at the state’s disposal,[54] **and it’s a monopoly that has been abused for about as long as it has existed.**[55] Already in antiquity the funding of wars was accomplished by systematically diluting the precious metal content of coins, which over time pushed the value of their precious metal content ever further below their nominal value.[56] Rulers across history have succumbed to the temptation of increasing their seigniorage income or of generating indirect tax revenues by means of inflation. Such behavior was eventually institutionalized in the form of the two-tiered banking system we know today — with money creation through the interplay between central banks (issuance of central bank money) and commercial banks (deposit money creation through lending of circulation credit) also known as fractional-reserve banking – which drapes a veil over the collection of seigniorage

[52] A special case is temporary monopolies, which generate so-called “pioneer profits”. Companies can, for instance, obtain patents for innovations, which protect them for a limited time from imitations of their products made by competitors. The idea is that the state temporarily restricts competition for a time via the patent system in order to promote competition over the long term, since many companies won’t regard the required R&D spending as economically viable if there is no prospect of making temporary monopoly profits. See “Theory of Economic Development”, Joseph Schumpeter, 1911

[53] Natural monopolies are the result of a cost structure (in most cases involving high fixed and low marginal costs) in which competitors are held to raise the total cost of supplying a good. Examples for this are railways, which have high fixed costs in the form of rail networks, and power and water utilities, which require electrical grids or piping systems for distribution.

[54] We are going **to refer to the “**state (or government) monopoly on money” in this section, even though it is nowadays usually not the central bank itself that produces new money. (Exceptions are QE, repos, and coupon passes, which affect the money supply directly and indirectly over a wide range of time frames.) Most money production results from inflationary lending by fractionally reserved private commercial banks (with central bank support), i.e., it is so to speak the result of a private-public partnership. Regardless, the government ultimately decides what may be used as legal tender.

[55] See “Monetary Regimes and Inflation. History, Economic and Political Relationships”, Peter Bernholz, Cheltenham, 2003.

[56] See “The Monetary Aspect of the Fall of Rome”, *In Gold We Trust* report 2016, pp. 98-103, or “The Frogs”, Aristophanes, pp. 719-737.

profits.[57] Latter-day efforts to stabilize the financial system and save the euro in response to the financial crisis are blending seamlessly into this history of abuse.

Thus, it is hardly surprising that criticism of the monetary and financial system has a long tradition as well. **However, even intellectuals who placed individual liberty at the center of their deliberations hardly ever questioned and question the state monopoly on money as such – despite all the criticism leveled at the monetary system.**[58]

Hayek's Proposal of Introducing Competing Private Currencies

> *"Everything comes down to the question: Which forms of order promote liberty?"*
>
> Walter Eucken

> *"The profit the government makes from diluting coinage is unjust ... every mutation of coinage, apart from a few exceptions, takes money from subjects against their will."*
>
> Nicolas d'Oresme

When Richard Nixon suspended the US dollar's convertibility to gold in 1971, it became obvious that the attempt to establish a monetary system based on a gold-exchange standard had failed due to over issuance of uncovered money substitutes. Upon this event Friedrich August von Hayek felt compelled to reexamine the question of what constituted an expedient monetary order.[59] In Hayek's opinion, not only the abolition of the tie between the US dollar and gold but also the proliferation of Keynesian economic thinking at the time worsened the prospect of a stable, noninflationary money ever emerging under a government-run currency monopoly.[60] In 1975 Hayek eventually gave a lecture entitled "Choice of Currency"[61], in which he articulated for the first time the provocative demand that the state monopoly on money should be repealed. The publication of the monographs *Free Choice in Currency* and *The Denationalization of Money* followed a year later, in which he expanded in greater detail on his ideas on competition between private money issuers.

[57] See The Zero Interest Rate Trap: Sustainable Wealth Accumulation in a Non-Sustainable Monetary System, Ronald-Peter Stöferle and Mark J. Valek, 2018 (to be published shortly)

[58] Hayek noted that the economic literature offered no answer to the question of why a government monopoly for the provision of money was deemed indispensable, nor was there any academic discussion examining the abolition of this monopoly (The Denationalization of Money, Friedrich A. von Hayek, 1976, pp. 26 ff). He attributed the notion that governments had a quasi-natural prerogative to be the exclusive suppliers of money to the historical fact that they had usurped the right to mint coins a very long time ago and then simply retained it as if this were a perfectly natural state of affairs (The Denationalization of Money, Friedrich A. von Hayek, p. 28).

[59] What makes this very interesting is the fact that Hayek previously espoused quite contrary views: "[A] really rational monetary policy could be carried out only by an international monetary authority [...] [S]o long as an effective international monetary authority remains an Utopian dream, any mechanical principle (such as the gold standard) ... is far preferable to numerous independent and independently regulated national currencies" (Monetary Nationalism and International Stability, Friedrich A. von Hayek, 1937, pp.93ff). Later Hayek wrote that a free currency market was "not only politically impracticable today but would probably be undesirable if it were possible" (The Constitution of Liberty, Friedrich A. von Hayek, 1960, pp.324ff). Nevertheless, what unites the different positions Hayek has taken over time is his desire to create a noninflationary monetary order. Moreover, the evolution of his position illustrates his growing skepticism with respect to the state.

[60] See "Toward a Free Market Monetary System", Friedrich A. von Hayek, p.2.

[61] See "Choice of Currency: A Way to Stop Inflation", Friedrich A. von Hayek, The Institute of Economic Affairs, 1976.

"It is impossible to grasp the meaning of the idea of sound money if one does not realize that it was devised as an instrument for the protection of civil liberties against despotic inroads on the part of governments. Ideologically it belongs in the same class with political constitutions and bills of rights."

Ludwig von Mises

Hayek's core thesis was that the entrenched abuse of the state monopoly on money for the purposes of enriching selected private groups, making good on fiscal deficits, or financing wars illustrates that concentrating the power of money issuance in the hands of the state (or any other centralized entity) does not work. Hence government has to be deprived of its monopoly on money creation, which should be replaced by a market-based monetary order that constitutes a system of power-sharing among competing entities.

What shape would an order reflecting these power-sharing principles take, and how could it emerge? Hayek argues that such an order would take shape if the following liberties were granted:

- Private money producers would be free to issue money and enter into currency competition.
- Citizens would be free to choose which currencies they want to use.

Banks would, for instance, issue their own currencies – in any amount they wished. While Hayek regarded money backed by gold or commodities as ideal, he explicitly allowed for the possibility of banks engaging in excessive creation of uncovered deposit money. However, he believed that this practice would fail to survive in a competitive market. In an unhampered market, banks would find that the incentive to boost their asset base over and above the amount of savings deposited with them would be curtailed. The preference of money users for an easy to use money with stable purchasing power would force banks to fulfill these expectations in the best possible way. Money suppliers issuing uncovered money substitutes would eventually face an exit of customers and disappear from the market.

Private Currency Competition as a Discovery Procedure

It is hardly surprising that Hayek was first among representatives of the Austrian School to elaborate systematically on the idea of a competitive monetary order. Like no other economist, he interpreted human action – both on the individual level and in the context of society at large – as a continual discovery procedure. This approach was in the spirit of Carl Menger, the founder of the Austrian School, who regarded money as a "social construct" that was the "result of an unplanned societal evolution" or "the unintentional result of the purposeful individual efforts of members of a society".[1] Men discovered the nature of money in a wide variety of contexts in a sociocultural evolutionary process. It seemed therefore obvious to Hayek that the production of money should be left to such a discovery procedure as well, namely to competition.

[1] Mikl-Horke, Gertraude: Soziologie: Historischer Kontext und soziologische Theorieentwürfe, Oldenbourg Verlag München, 2011, p.94. [own translation]

Competition would – analogous to competition in nonmonetary goods and services – exert discipline. The structure of incentives would be optimal, as general welfare would increase as a result of numerous competing actors pursuing their own interests.[62] Hayek famously concluded:

"Money is the one thing competition would not make cheap, because its attractiveness rests on it preserving its 'dearness'."[63]

What role would a central bank play in such a competitive order? It would become obsolete. This prospect is welcomed by Hayek, as government-run monetary policy is precisely what he regards as the major source of economic instability. According to Hayek, historical economic

[62] See The Denationalization of Money, An Analysis of the Theory and Practice of Concurrent Currencies, Friedrich A. von Hayek, 1977, p. 57.
[63] See The Denationalization of Money, An Analysis of the Theory and Practice of Concurrent Currencies, Friedrich A. von Hayek, 1977, p. 94.

crises were time and again attributable to the distorting effects of monetary policy implemented by governments, rather than to so-called market failures:

> *"The past instability of the market economy is the consequence of the exclusion of the most important regulator of the market mechanism, money, from itself being regulated by the market process."*[64]

However, the central bank would not necessarily have to stop operating right away. It could continue to issue (government) currency. However, it would be in competition with commercial banks and other private money producers and would therefore have a strong incentive to supply citizens with a stable currency.

"The money monopoly is perhaps the most important pillar on which the modern day's state power rests."

Thorsten Polleit

Cryptocurrencies – Free Currency Competition in Practice?

"Cryptocurrencies are a use case of competing private currencies as envisaged by Friedrich August von Hayek."[65]

Norbert F. Tofall

Initially the debate over the idea of competing private currencies was purely theoretical, as the government monopoly on money had been so deeply rooted for such a long time that the public at large never thought of seriously questioning it. When Hayek published his proposal, the voluntary abolition of the money monopoly would have been required to adopt it, which was tantamount to governments relinquishing a great deal of their power – a highly unrealistic prospect.[66]

"It will be extremely hard for CCs to displace and compete with government-issued currencies, as dollars to euros and yuan are virtual natural monopolies in their regions and will not easily give up their seigniorage profits."

J.P. Morgan, The Bitcoin Bible

Since then, conditions have fundamentally changed, though, as a result of the pervasive spread of the Internet. After the near-collapse of the monetary and financial system in the 2008 financial crisis and the erosion of confidence in government currencies and central banks in its wake, the first private digital currency in the form of Bitcoin made its entrance in the realm of Web 2.0. Since then more than 1,500 cryptocurrencies (in their entirety better described as crypto assets) with a market capitalization totaling roughly USD400bn have entered the market. As cryptocurrencies are largely outside of government control – at least until now –, a kind of laboratory for private currency competition could be established. In fact, the ECB suspects (rightly) that Hayek's theoretical work was the *spiritus rector* of today's cryptocurrencies.[67]

[64] See The Denationalization of Money, An Analysis of the Theory and Practice of Concurrent Currencies, Friedrich A. von Hayek, 1977, p. 102.

[65] See "Währungsverfassungsfragen sind Freiheitsfragen: Mit Kryptowährungen zu einer marktwirtschaftlichen Geldordnung?," Norbert F. Tofall, Flossbach von Storch Research Institute, 2018, p. 4 (Currency questions are questions of liberty: Toward a market-based monetary order with cryptocurrencies?).

[66] See "A praxeological analysis reveals that currency competition is simply not in the state's interest." Thorsten Polleit: "Hayek's 'Denationalization of Money' – a Praxeological Reassessment", Journal of Prices and Markets, p. 79.

[67] See "ECB: 'Roots Of Bitcoin Can Be Found In The Austrian School Of Economics,'" Jon Matonis, Forbes, 2012.

Decentralization: The Cryptocurrency Killer App

What makes cryptocurrencies so interesting is that they are so contrary to the mental image many people have of money.[68] The most famous cryptocurrency, Bitcoin, functions as a payment system based on monetary units that consist of themselves and are not redeemable for gold or any other commodity. Bitcoin is accepted as currency, though in line with the definition of Ludwig von Mises it has to be considered as pure fiat money [69], that is not run by the state and is not tied to a commodity. Many monetary theorists were convinced that such a currency could not possibly emerge in a free market. Hayek himself believed that currencies tied to commodities would prevail in a system of free competition. What is the reason, then, for the growing acceptance of cryptocurrencies?

The secret of their success that is at the core of an accepted currency is a result of their decentralized nature. Cryptocurrencies such as Bitcoin, Monero, and Litecoin are not issued by a single private institution; they are based on a source code protocol and maintained through a decentralized network of widely dispersed market participants. Unlike a currency issued by a private money producer, whose paper money represents a promise to pay, Bitcoin is a fiat money that is no one's liability. In this respect, a cryptocurrency like Bitcoin is similar to gold.

An interesting aspect of the currency competition launched by the emergence of cryptocurrencies is also that it differs from Hayek's proposal in one decisive respect. The situation as envisaged by Hayek would always carry the latent risk that a – centralized – money-issuing entity could fail.

"Money is power, and rare the heads that can withstand the possession of great power."

Benjamin Disraeli

In the case of a cryptocurrency such as Bitcoin, no such central entity exists. The smooth operation of a cryptocurrency is safeguarded by geographically dispersed interest groups such as developers, miners, traders, users, and others working within the ecosystem. Trust and risk are distributed across a network of numerous parties pursuing their own interests.[70] Those purchasing a cryptocurrency ultimately place their trust in mathematical and encryption protocols that maintain a system of incentives, which in turn provides all participating entities or groups with a motive to ensure the currency's integrity. Hence the slogan "In Code We Trust"[71]. To this day this system of incentives has worked splendidly, and not one of the numerous attempts to destroy it has been successful.

The Quest for Stability

A problem plaguing many cryptocurrencies – and, as a proxy for them, Bitcoin – is their excessive price volatility. Bitcoin's inelastic supply, coupled with a demand shock triggered by the rapid diffusion of "crypto-ideology" and the associated

[68] The success of cryptocurrencies does not only irritate a number of laypersons. For instance, the well-versed monetary theoretician (and Austrian School representative) Guido Hülsmann stated in 2007 that a money "that is defined entirely in terms of bits and bytes is unlikely ever to be produced spontaneously on a free market." ("The Ethics of Money Production", Ludwig von Mises Institute, 2008, p. 33).
[69] See The Theory of Money and Credit, Ludwig von Mises, Yale University Press, 1953
[70] See "Trustless is a Misnomer", Nick Tomaino, Medium, July 21, 2016.
[71] See "The Bitcoin Boom: In Code We Trust", Tim Wu, The New York Times, December 18, 2017. (Coincidentally a play on words on the title of this report, which was first published well before Bitcoin was born.)

speculative hype,[72] has temporarily led to an enormous increase in the purchasing power. Leaving aside the recent correction, the history of Bitcoin is a history of hyper-deflation[73] – and in a time of strong deflation it makes more sense to hoard a currency than to use it as a means of payment. As a result Bitcoin and other new cryptocurrencies are barely fulfilling the function of media of exchange at the moment.[74]

“Bitcoin is the beginning of something great: a currency without a government, something necessary and imperative.”

Nassim Taleb

The same feature that underpins the currency’s store of value function hampers its use as a unit of account. As the supply of Bitcoin and other cryptocurrencies is as a rule limited, with no central entity able to balance excess demand by boosting supply, cryptocurrencies are occasionally highly volatile.[75] Contrary to Mises’ belief that an inelastic supply would go hand in hand with comparatively small fluctuations in demand and price, cryptocurrencies have not proved suitable for fulfilling unit of account functions such as drawing up corporate balance sheets – at least so far.[76]

In line with Hayek, one could counter that a cryptocurrency that is undergoing a process of monetization has to be regarded as an object of speculation in the early stages of the process, which will inevitably involve volatility. It seems logical that speculative demand and reservation demand will be strong at an early stage. However, the importance of speculative demand should diminish over time, as ownership of the cryptocurrency in question broadens. **If they are successful, emerging cryptocurrencies should eventually manage the transition from speculative assets to currencies that function reliably as media of exchange.**[77]

“I do not think that it is an exaggeration to say that history is largely a history of inflation, and usually of inflations engineered by governments and for the gain of governments.”

Friedrich August von Hayek

A number of cryptocurrency enthusiasts who don’t want to simply wait and see whether this will happen are working on creating cryptocurrencies with stable

—

[72] Thus, many people believe that cryptocurrencies, which are still at the beginning of more widespread adoption, will continue to gain in value in coming years and are buying them as speculative buy-and-hold investments.

[73] See “Bubble or Hyperdeflation“, Incrementum AG, Crypto Research Report.

[74] Several people in the crypto community argue that Bitcoin is not at all predestined to become a widely adopted medium of exchange for day-to-day use. Rather, they say, Bitcoin represents a decentralized and therefore intervention-resistant store of value. The original source code of Bitcoin, which can be altered only if the extremely disparate Bitcoin community arrives at a consensus, provides the best possible conditions for the currency’s store-of-value function: The total amount of Bitcoin that can be mined is restricted to 21 million units (some of which have already been lost forever – e.g. a famous hard disk drive containing 70,000 BTC is known to be peacefully collecting rust in a UK landfill). It takes around 10 minutes for a new bitcoin to be created. Since the emergence of Bitcoin in 2008, the quantity of newly created bitcoins has been declining by half every four years. According to estimates, by 2140 all bitcoins that will ever exist will have been mined. This continually strengthening deflationary tendency strongly underpins the store-of-value function of BTC.

[75] Cryptocurrencies are affected to a greater extent by this volatility than, for example, gold, as gold is subject to countercyclical buffers through jewellery and fabrication demand (declining demand when prices rise and vice versa) as well as through fluctuations in the gold supply (growth in mine supply and rising sales from existing stocks when prices increase and vice versa).

[76] See Human Action: A Treatise in Economics, Ludwig von Mises, Auburn, Alabama: Ludwig von Mises Institute, 1998, pp. 225ff.

[77] As discussed in this section, relatively supply-inelastic gold is not immune against periodic high speculative demand, either: If in the course of an emerging currency competition currencies backed by gold were to turn out to be preferred by most users, surging demand for gold would rapidly boost its price – and presumably also its volatility – which would at least temporarily suspend suitability of the precious metal as a means of payment and unit of account. (See The Denationalization of Money, An Analysis of the Theory and Practice of Concurrent Currencies, Friedrich A. von Hayek, 1977, pp. 102/127.)

values, so-called “stablecoins”.[78] These currencies have a flexible supply, which is adjusted to fluctuations in demand with the aim of achieving purchasing power stability. But – and here is the problem – how is it possible to guarantee “price stability” without being forced to restrict or abandon the decentralized and therefore intervention-resistant structure of a cryptocurrency? Simply decreeing an “inflation target” from on high is precisely what central banks are doing and is contradictory to the spirit of cryptocurrencies.[79]

The solution to this problem may be DAO, which stands for “decentralized autonomous organization”. Members of such a DAO organize independently. With respect to managing a stable-coin, members of a DAO would be tasked with ensuring the stability of its purchasing power. Stability would be promoted through a structure of incentives embedded in the coin’s programming code. The recently launched Maker DAO project[80] appears to hold promise in this regard. Maker’s stablecoin, called Dai, is still very young, but has already become popular with many users.[81]

Conclusion

> *“Humanity’s progress always involved a small minority deviating from the ideas and customs of the majority, until its example finally persuaded others to adopt its innovations as well.”*
>
> Ludwig von Mises

> *“If politics is the art of the possible, then political philosophy is the art of making the seemingly impossible politically possible.”*
>
> Friedrich August von Hayek

In our opinion Hayek has bequeathed us a vital body of preliminary theoretical work for a future, more crisis-resistant monetary order. In order to create full freedom of choice for money producers and users, the money monopoly of the state has to be repealed and replaced by an environment in which private currencies can be developed and can compete in a decentralized discovery procedure. As money users would punish producers of unsound (i.e., inflationary) money by abandoning it, both government and private currency suppliers would be motivated to keep their seigniorage income low and to issue sound money.

As governments would no longer be able to mitigate their debt burdens through inflation, such a monetary order would be highly effective in enforcing fiscal discipline. **The chronic debt-crisis of our times, namely the overindebtedness of governments, could never emerge in such a system – thus currency competition would be the most powerful debt brake imaginable.**[82]

—

[78] See the chapter Crypto: *Friend or Foe?*

[79] See “The Search for a Stable Cryptocurrency”, Vitalik Buterin, Ethereum Blog, November 11, 2014

[80]: See “Maker for Dummies: A Plain English Explanation of the Dai Stablecoin“, Gregory DiPrisco, Medium, November 20, 2017

[81]: See “Stablecoins: A Holy Grail in Digital Currency“, Nick Tomaino, The Control, April 3, 2017

[82]: See “Währungsverfassungsfragen sind Freiheitsfragen: Mit Kryptowährungen zu einer marktwirtschaftlichen Geldordnung?“, Norbert F. Tofall, Flossbach von Storch Research Institute, 2018, p. 5 (“Currency questions are questions of liberty: Toward a market-based monetary order with cryptocurrencies?”)

For a long time, such competing currencies were unthinkable, as governments have not been inclined to voluntarily abandon their monopoly on money. With cryptocurrencies, which could emerge only due to the spread of the internet and which cannot be effectively suppressed or prohibited due to their decentralized structure, currency competition in the spirit of Hayek has become possible even in the absence of self-limitation by governments.

Friedrich August von Hayek and his nephew Richard Zundritsch in the 80s in Obergurgl

Exclusive Interview with Dr. Richard Zundritsch: “Hayek Would Prefer Gold to Bitcoin”

Dr. Richard Zundritsch studied at the University of Vienna, where he earned a doctorate in law. He is an independent financial advisor based in Switzerland who specializes in capital markets, asset management, succession planning, and venture capital. Dr. Zundritsch is Friedrich A. Hayek's nephew and knew him personally. He is widely acknowledged as an expert on Hayek and his work.

Dear Dr. Zundritsch! You are the nephew of the great F.A. Hayek and are a world-renowned Hayek expert. Hayek is seen as a pioneer on the topic of currency competition. Why Hayek in particular?

When Hayek wrote the monograph *The Denationalization of Money* in 1976, which was published in German one year later, competing national currencies as we know them today did not exist yet due to capital controls. It was customary that one had to obtain a permit for trading foreign currencies. Hayek therefore first of all demanded the adoption of general freedom of contract, so as to make it possible for individuals to freely choose the currencies in which they preferred to conclude contractual agreements.

Hayek succeeded with this.

Indeed – today this freedom of contract exists. One has to mention this at the outset if one wants to discuss Hayek’s ideas in his work on the denationalization of money. Hayek was primarily focused on currency competition and not on the abolition of state-issued money as such. He eventually regretted not having found the time to pursue the topic further.

In short, Hayek demanded more freedom. Many Bitcoin and cryptocurrency supporters demand the same.

That is correct. However, one of the major issues motivating Hayek was inflation. Hayek had experienced the scourge of inflation throughout his life, which is why he fervently wished for monetary stability. This desire underlies Bitcoin as well – but ironically, the value of Bitcoin and other cryptocurrencies is anything but stable.

Would Hayek approve of the freedom-related aspects of cryptocurrencies?

Cryptocurrencies don't bestow quite as much freedom as people seem to think. Trading of cryptocurrencies almost always involves centralized exchanges and state-issued currencies. It may not be possible to impose regulations on Bitcoin itself, but it can be done to the interfaces on its periphery. Hayek would probably be skeptical with respect to this.

And what about Bitcoin's volatility?

I'm quite certain that Hayek would not appreciate it. Achieving stability of the purchasing power of money was clearly his declared goal. He attached great importance to this. He was a fiercely opposed to both inflation and deflation. In Hayek's model private currencies would have been issued by specific issuers – governments, banks, or other companies. Cryptocurrencies lack such issuing entities; instead they are based on a technology, the blockchain. While their supply is limited, and it is impossible to inflate them at will, fluctuations in their value can be substantial.

Wouldn't Hayek, as an opponent of inflation, welcome their limited supply?

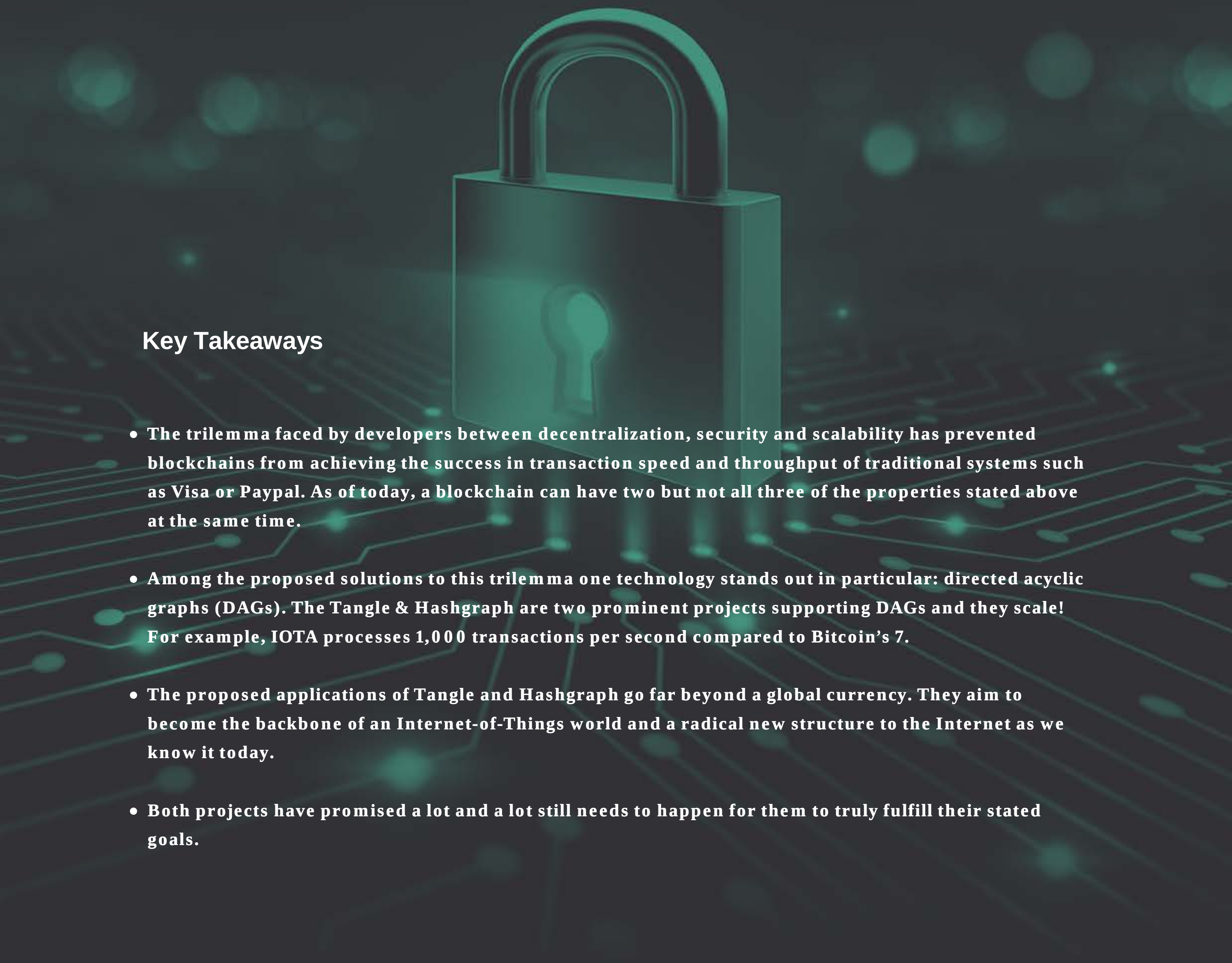
No. Hayek's idea was that currency issuers would be interested in keeping the value of their currencies stable. By contrast, cryptocurrencies have only inventors. Once a blockchain is launched, it so to speak acquires a life of its own. No one is interested in keeping a cryptocurrency under control. On the blockchain it is not possible to manage a currency's purchasing power by altering its supply, such as private money producers as envisaged by Hayek would be able to do.

Do you believe Hayek wouldn't like cryptocurrencies at all?

No, he would. Hayek would undoubtedly welcome the emergence of currency competition. Particularly in international payment transactions, which can sometimes can still take several days and cost an arm and a leg, cryptocurrencies are providing much-needed competition. I think, though, that rather than being a fan, Hayek would be an interested observer of cryptocurrencies. **I believe it is fair to assume that he would still prefer gold to cryptocurrencies.**

Coin Corner – Blockchain 3.0 The Future of DLT?

> *“I think the internet is going to be one of the major forces for reducing the role of government. The one thing that’s missing but that will soon be developed, is a reliable e-cash.”*
>
> Milton Friedman



Key Takeaways

- **The trilemma faced by developers between decentralization, security and scalability has prevented blockchains from achieving the success in transaction speed and throughput of traditional systems such as Visa or Paypal. As of today, a blockchain can have two but not all three of the properties stated above at the same time.**
- **Among the proposed solutions to this trilemma one technology stands out in particular: directed acyclic graphs (DAGs). The Tangle & Hashgraph are two prominent projects supporting DAGs and they scale! For example, IOTA processes 1,000 transactions per second compared to Bitcoin’s 7.**
- **The proposed applications of Tangle and Hashgraph go far beyond a global currency. They aim to become the backbone of an Internet-of-Things world and a radical new structure to the Internet as we know it today.**
- **Both projects have promised a lot and a lot still needs to happen for them to truly fulfill their stated goals.**

Coin Corner – Blockchain 3.0 – The Future of DLT?

"I do think Bitcoin is the first encrypted money that has the potential to do something like change the world."

Peter Thiel

"Cryptography is the essential building block of independence for organisations on the Internet, just like armies are the essential building blocks of states, because otherwise one state just takes over another."

Julian Assange

The Bitcoin blockchain is generally regarded as the original blockchain, since it is the first implementation of a new technology that is commonly described today as distributed ledger technology (DLT). The birth of the Bitcoin blockchain 1.0 was followed by the programmable Ethereum version as the blockchain 2.0 and soon the third generation, the blockchain 3.0 in form of IOTA, Nano, or Hashgraph. Splitting the development into these individual stages is a simplification, because the latest generation of the blockchain technology is not even properly characterized as being a blockchain. Rather, the keyword here is DAG or directed acyclic graph. Projects based on this technology aren't really blockchains. Instead, IOTA, Nano, and Byteball are described as post-blockchain concepts. But why are investors and blockchain users to replace the original blockchain technology with a new "DLT variant"?

The Apparent Weakness of Current Blockchains

In theory, first- and second-generation blockchain technology has already turned the world upside down. There seem to be hardly any fields that could not be fundamentally changed by the blockchain. In practice, however, the situation has been somewhat different.

Currently blockchains such as those of Bitcoin and Ethereum are subject to an unresolved restriction: to date, they have not yet achieved substantial scaling success. This means that all these blockchain protocols are limited in terms of transaction throughput and speed. While legacy systems such as PayPal can process about 200 transactions per second (tps) and Visa even 56,000 tps, Ethereum currently only manages a maximum of 20 tps, while Bitcoin only reaches a capacity of 7 transactions per second. This is why Bitcoin and Co. are currently no match for the incumbent payment systems of our time.[83]

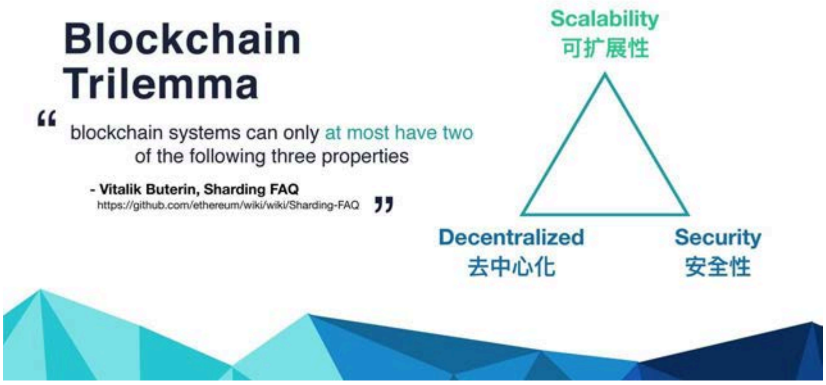
But why does this technical limitation exist at all? The answer is simple: The blockchain protocols are not slow because of some inherent scalability barrier. The restriction is rather the result of a "conscious" decision - to build a decentralized blockchain network.[84] One of the core elements of public blockchains like Bitcoin and Ethereum is to give everyone the possibility to operate a network node. Each node processes every single transaction and therefore has to store the entire transaction history of the blockchain on his computer. Public blockchains are only as strong as their weakest link. Scalability and therefore transaction throughput

[83] See "Why blockchains don't scale," Piers Ridyard, *Radix,* Febrary 8, 2018.

[84] Here the term "non-centricity is deliberately used. The frequently mentioned concept of de-centrality implies that there is a central entity, albeit a weak one. However, this does not apply to Bitcoin and some other blockchain projects, which is why "non-central" seems to be better suited.

and speed depend on the capacity of the weakest node. Of course, weak nodes could be discarded, but then the crucial property of censorship resistance would be damaged, as certain network members would be deliberately excluded.[85] Therefore, it is this trilemma between decentralization, security, and scalability that prevents blockchains from achieving the transaction speed and throughput of traditional systems such as Visa or PayPal.

Figure 12: The Blockchain Trilemma Between Decentralization, Security, and Scalability.


Blockchain Trilemma
"blockchain systems can only at most have two of the following three properties
- Vitalik Buterin, Sharding FAQ
https://github.com/ethereum/wiki/wiki/Sharding-FAQ"
Scalability
可扩展性
Decentralized
去中心化
Security
安全性

Note: According to theory, but two not all three of these properties are possible at the same time.
Source: Steemit[86]

The Blockchain Solution That is Not a Blockchain

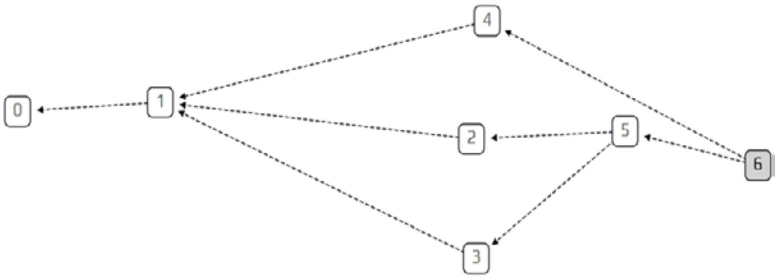
"Bitcoin is evil."

Paul Krugman

Research in the Bitcoin and Ethereum communities is continuously revolving. In each ecosystem, scaling solutions are being developed. On the Bitcoin side, the Lightning Network[87] and RootStock[88] are two of the best-known approaches. In Ethereum, solutions such as Sharding[89], Plasma[90], or Caspar[91] are at the top of the list. **Attempts such as the Lightning Network or Sharding suggest that the answer to the scaling question is that not all participants - or network nodes - need to know all the information at all times to keep the network in sync. This approach is something the DAG or directed acyclic graph is based on as well.**

[85] See "Hate Bitcoin? This May Change Your Mind," Peter Shin, *Medium*, March 10, 2018.
[86] See "Scalability solutions – Part 2," bit-news, *steemit*, January, 2018.
[87] See Crypto Research Report II
[88] See RSK.
[89] See "How to Scale Ethereum: Sharding Explained," Raul Jordan, *Medium*, January 20, 2018.
[90] See "Ethereum Plasma Explained," Lukas Schor of Argon Group, *Medium,* May 28, 2018.
[91] See "What is Ethereum Casper Protocol?," *Blockgeeks*, December, 2018.

Figure 13: A Simple Schematic Representation of DAG.



Note: It is called “acyclic” because transaction “0” cannot cycle back to a previous transaction. The flow of transaction only goes in one direction.

Source: IOTA blog.[92]

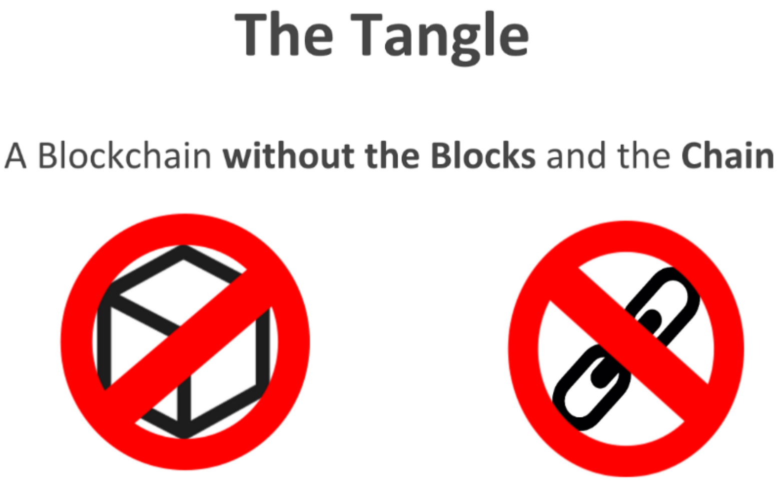
“DAGs don't solve any fundamental scalability problems. They solve latency problems at best, and in general I think DAG tech is overhyped.”

Vitalik Buterin

A DAG works according to a “horizontal” scheme, while a blockchain is based on a “vertical” architecture. With the blockchain, miners create new blocks that are added to the blockchain. The “horizontal” structure of DAGs, on the other hand, enables transactions to be linked directly to other transactions without putting them in a block first. **This way there is no need to wait for a confirmation of the next block.** At the same time, not all network participants have to confirm the block update. Since the DAG concept has neither blocks nor miners, there is no chain of blocks full of transactions and therefore no “blockchain”. The structure of a DAG is much more like a “mazy” network of numerous transactions. This is why it is often referred to as a Tangle - a term that appears again and again, especially in connection with the IOTA project. At its core, however, the Tangle has the same properties as a blockchain: it is still a distributed database based on a peer-to-peer network. Thus, the Tangle is also a validation mechanism for distributed decision making.

How Does the Tangle Work?

Figure 14: The Tangle – a “Blockchain” Without Blocks or a Chain.



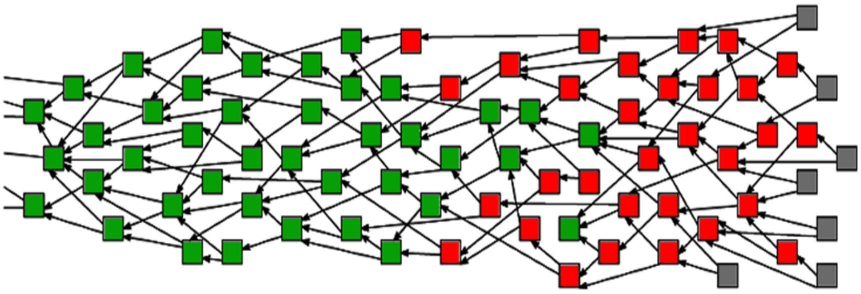
Source: IOTA blog.[93]

[92] See “The Tangle: an Illustrated Introduction,”Alon Gal, *IOTA Blog*, January 31, 2018.
[93] See “A Primer on IOTA (with presentation),” Dominik Schiener, *IOTA Blog*, May 21, 2017.

The Tangle is created by linking individual transactions in the network. The linking is a consequence of the fact that each unconfirmed new transaction must confirm one or two additional transactions before the unconfirmed transaction can be processed and confirmed itself. In contrast to the blockchain of Bitcoin or Ethereum, it is not only the miners who are responsible for the confirmation of transactions. In the case of the Tangle, this task of processing and approving new transactions is the responsibility of all active Tangle or network participants. This way not only newly added transactions are confirmed, but the entire transaction history is also indirectly confirmed with it. **The "transaction issuer" does not pay a direct fee for processing its own transactions – he/she only indirectly pays (with computer hashing power) by confirming other transactions.**

Transactions in the network that have not yet been confirmed are commonly referred to as "tips". In order to obtain confirmation, these "tips" themselves have to confirm other transactions. An algorithm called Markov chain Monte Carlo[94] ensures that network participants do not just confirm their own transactions.

Figure 15: Green-Block, Red-Block, and Grey-Block Transactions.



Note: Green Blocks are transactions on which consensus has been reached (i.e. the transaction is confirmed in the network with security guarantee); red blocks are transactions whose full acceptance is still uncertain, and gray blocks are unconfirmed transactions called tips.

Source: IOTA blog.[95]

"The future of money is digital currency."

Bill Gates

The reason why transactions have to be confirmed is obvious: the problem of double-spending must be avoided. As with a regular blockchain, the cryptocurrency units - in the case of IOTA the IOTA token – must be stopped from double-spend attempts. For example, if Alice sends ten IOTA tokens to Bob, Charlie checks Alice's IOTA token balance before this transaction. If Alice only had five IOTA tokens, then her balance would be too low for the transaction to be valid. Charlie will not want to confirm this transaction because he has an interest in having his own transaction confirmed and this will most likely only happen if he himself does not validate any invalid transactions.[96]

As the name suggests, the Tangle ultimately is a Tangle of transactions. The Tangle has a concept called "confirmation confidence"[97] so that no two separate branches form in this "mazy" cluster of transactions in which Alice has issued the same IOTA token twice. Because this is the level of trust and acceptance that the rest of the Tangle gives to a transaction. Each transaction therefore has a

[94] See "A Primer on IOTA (with presentation)," Dominik Schiener, *IOTA Blog*, May 21, 2017.
[95] See "A Primer on IOTA (with presentation)," Dominik Schiener, *IOTA Blog*, May 21, 2017.
[96] See "The Tangle: an Illustrated Introduction,"Alon Gal, *IOTA Blog*, January 31, 2018.
[97] See "The Tangle: an Illustrated Introduction,"Alon Gal, *IOTA Blog*, January 31, 2018.

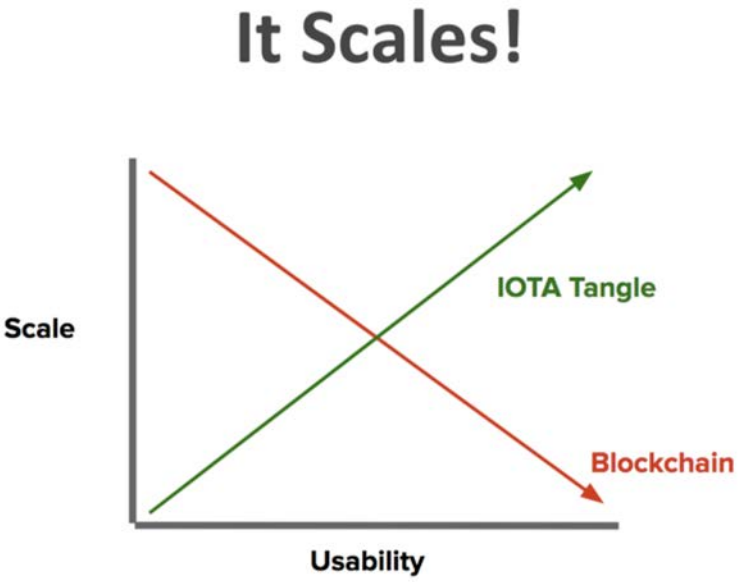
certain percentage, depending on the number of tips (unconfirmed transactions) accepting it. This is intended to ensure that only one branch prevails, namely the one with the larger confirmation confidence.

"We have elected to put our money and faith in a mathematical framework that is free of politics and human error."

Tyler Winklevoss

It is this concept that should enable a better scaling of any DAG project. **What causes a traffic jam in a blockchain and slows down the network should make a Tangle even safer and faster:** The more participants in the network and the more transactions are processed, the better the processing of outstanding transactions - that is what the theory says. As of yet, the IOTA network is still rather small, which is why the claim cannot be validated for sure. However, the largest Tangle projects, IOTA and Nano, indicate that they can currently process ~1,000 and 7,000 tps respectively.[98]

Figure 16: Scalability of IOTA.



Note: The more users that use IOTA network needs, the more reliable and faster it should become.

Source: IOTA blog.[99]

IOTA – The Backbone for an Internet of Things?

The IOTA project emerged from a hardware startup working on a new trinary microprocessor called "Jinn"[100]. In the future, this hardware component should make it possible for every vehicle, every microwave, and every refrigerator to communicate via the IOTA network without functioning as a normal computer.[101] Since the beginning of its development, the IOTA project, due to its inherent scalability, has seen itself as the predestined solution for the obvious problem of efficient transaction processing in a future machine economy.

[98] See "What it means to have 7,000tps!," *Reddit*, January, 2018.
[99] See "A Primer on IOTA (with presentation)," Dominik Schiener, *IOTA Blog*, May 21, 2017.
[100] See "Jinn," *CoinMarketCap,* 2018.
[101] See "IOTA: The hardware part," Chris Mueller, *Medium,* January 6, 2018.

Experts today hardly seem to question the fact that our world will develop into one big Internet of Things.[102] Estimates claim that by 2025, there should be over 100 billion interconnected devices and machines worldwide, all of which will have a dozen or more sensors. Already today our smartphone produces huge amounts of data. Imagine how much greater the amounts of data will be when our car becomes a smartcar, our house a smarthome and our city a smartcity. In our times, where data is the digital oil and thus a new treasure, the revenues generated by the data business will be enormous. Of course, these values should not simply be reaped by large tech companies. As a universal agnostic protocol, IOTA could function as a public, decentralized and self-regulating “machine-to-machine network” via which the respective machines can communicate independently without an intermediary and thus transfer values.

The Internet Strikes Back Against IOTA

Although there is a lot of hype around IOTA and DAGs, various voices within the Internet are lashing out against IOTA. Reddit, YouTube, and Medium posts argue that IOTA has promised too much. The main attack is that IOTA will not be able to successfully remove the coordinator from the network. The coordinator is a centrally-run server controlled by the IOTA Foundation that ensures that double-spend attacks and spam attacks are thwarted. The centrally-run server, or node, validates every single transaction on the IOTA network. This creates what is referred to as a Single Point of Failure (CRR I, pg. 9).

The IOTA Foundation claims in their white paper that, once the network grows to a certain number of nodes, the Foundation will remove the centralized coordinator. However, many investors have asked for specific blueprints explaining how IOTA plans to remove the coordinator. So far, IOTA has failed to provide a specific number of nodes that will be required before they can remove the network. Investors have pointed out that there is no financial incentive for someone to run a node because the network generates no transaction fees, and because all of the IOTA coins were issued at the beginning of IOTA.

This means that IOTA nodes cannot receive transaction fees or coin rewards. Since there is no financial incentive to run a node, the probability that IOTA can develop a decentralized network of nodes is low. Although the Internet has not issued a final verdict on the topic, investors should be weary. A possible solution is to create a similar cryptocurrency to IOTA but to allow nodes to earn coin rewards for validating transactions. This would enable free transactions and a financial incentive for a decentralized network of nodes to protect the network.

A futuristic but often mentioned example is that of a smart car. This intelligent vehicle could have an identity and an "e-wallet" one day. With this equipment, the smart car would be able to pay for various services such as fuel (in the future probably electricity instead of petrol), insurance, washing or road tolls. Even the payment of a parking ticket should be possible, especially because the IOTA network does not have any actual transaction fees and therefore seems to be predestined for "micro-payments", i.e. very small payments.

The vehicle of the future should therefore not only be a self-driving car - it should also be autonomously paying for services used and also be able to offer its own services. The concept of “mobility as a service” could become more attractive in such a machine economy driven by the IOTA network. Whenever one of the vehicle owners does not need his vehicle, his/her car could offer its driving services to paying passengers. By giving customers a ride and collecting the fee through the e-wallet, the car generates a kind of passive income for the owner instead of simply sitting in a parking lot. As an autonomous economic agent, the possibilities for such a vehicle of the future seem to be limitless. Ultimately, we humans benefit because our time can be optimized in more efficient ways. For example, if a passenger is in an extreme hurry, he/she could also instruct the vehicle to make other vehicles that are in less of a hurry go out of its way - obviously, a fee would be

[102] Watch “Jeremy Rifkin on the Fall of Capitalism and the Internet of Things,” *Big Think,* April 22, 2018.

paid directly to other vehicles via the IOTA network using IOTA tokens for clearing the way.[103]

The founders of the IOTA network are pretty confident: While mankind is already creating the Internet of Things by digitizing things and equipping them with sensors, IOTA should have the potential to make a further step possible: An economy of things in which data and IoT devices are able to share their digital assets autonomously via marketplaces in the new machine economy.

With regard to IOTA, one of the most impressive facts is that the project has succeeded in setting up a foundation in Germany. This is astonishing because Germany is regarded as one of the most difficult countries to establish a foundation. In addition, the IOTA foundation has influential advisors on the board of their foundation. For example, the "Chief Digital Officer" Johann Jungwirth of Volkswagen is a member of the Board of Trustees. Robert Bosch Ventures is also a member of the advisory board and its fund has already made substantial investments in IOTA.[104]

> *“The Qubic platform will be the most significant contribution to the IOTA stack, it will enable unlimited new use cases and turn the IOTA Project into a full solution. Information and details are beginning to be unveiled right now at http://qubic.iota.org.”*
>
> IOTA

In mid-April, the world's first charging station for electric vehicles was launched in the Netherlands, where charging and payment can be carried out with IOTA. The charger was installed by ElaadNL, a research institute for innovation.[105] For the IOTA team, this is one of the first steps towards real-world adoption.

Recently, the IOTA team unveiled the long-awaited secret about the so-called Project Q. With Qubic, the IOTA protocol will not only support smart contracts[106] and oracles[107], but also a form of distributed computing. This makes the IOTA Tangle programmable. At the same time, the free micro-transactions should ensure that external and distributed computing power can be used for the IOTA Tangle. Qubic is intended to make unused computing power available for the IOTA Tangle on a global scale in order to further enhance the performance of the IOTA network. According to the founders of IOTA, the Qubic project is one of the most important milestones of the IOTA project.[108]

Hashgraph – The Latest Excitement Among DLTs

In addition to the Tangle, the term “Hashgraph” is also causing quite a stir on the market. This newly developed technology also falls into the category of distributed ledger technologies (DLT). The idea for Hashgraph was developed by Leemon Baird in mid-2016 and was originally intended for the private corporate sector. The intellectual property in Hashgraph is held by Swirlds, a company founded by Baird.[109] Swirlds distributes a software development program that allows anyone to experiment with the “Hashgraph Consensus Library”. With CULedger, a consortium of 6,000 cooperative banks in North America, Hashgraph has already

—

[103] Watch “IOTA – 100 Billion Reasons Why,” *The bIOTAsphere*, April 11, 2018.

[104] See “Blockchains vs DAG: Behind the Battle for the Backbone of the Internet of Things And the Future of Cryptocurrency – A History,” Wasim Of Nazareth, *Medium*, February 16, 2018.

[105] See “World’s first IOTA Smart Charging Station,” Harm van den Brink, *ITA Blog,* April 19, 2018.

[106] See “Smart Contracts: The Blockchain Technology That Will Replace Lawyers,” *Blockgeeks,* 2016.

[107] See “Types of oracles,” *BlockchainHub*, 2018.

[108] See “IOTA and Qubic – The Start of New Era (And The Fulfillment Of A Long Time Dream),” *IOTA News*, June 42018.

[109] See Swirlds’ website for more information.

found a potent customer who uses their private Hashgraph software and has even preferred it to other alternatives such as Hyperledger.[110]

Due to this success in the corporate sector, Swirlds has now launched the "Hedera Hashgraph Platform" with aims to drive forward Swirlds' patented Hashgraph technology for the development of a public Hashgraph network.[111] While the source code of the Hedera Hashgraph is publicly available and anyone can become part of the Hedera Hashgraph ecosystem as a network node, the project will still have a governance model similar to that of Visa. This means that there will be 39 organizations that will form a kind of leadership council. The exact terms are currently being finalized and the 39 members will be announced.[112] **Due to this structure with a management body, splitting the source code to create an alternative project using a hard-fork will not be possible.**

How Does the Hashgraph Work?

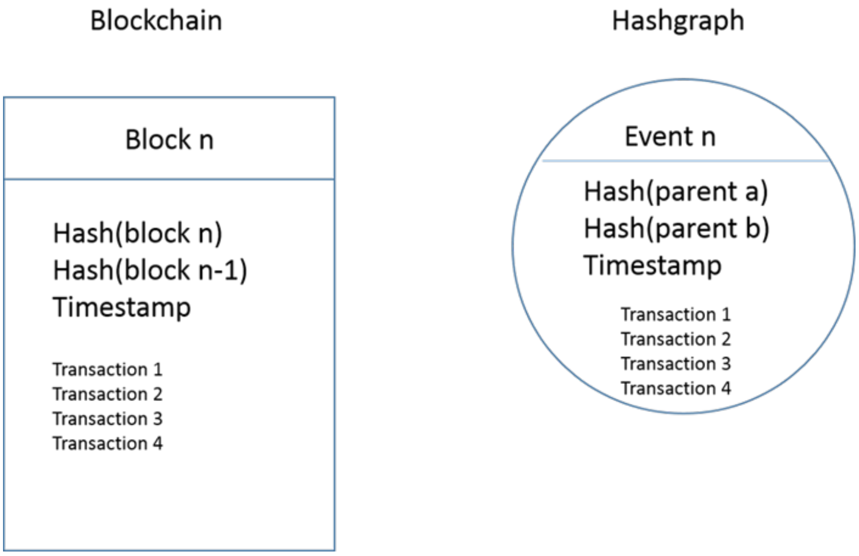
As with the Tangle, the Hashgraph concept is no longer based on blocks that are chronologically put together to form a chain. Instead so-called events, which are hashed to each other - hence the name "Hashgraph". The following information is contained in these "events": a timestamp, two different parent hashes and one or more transactions.

While in a blockchain the winning node has the possibility to add the new block with transactions to the existing chain, in the Hashgraph all nodes within the entire network inform each other about the latest status and "exchange" their information with each other. Similar to a Tangle, a connection diagram of "events" or transactions is created, and transactions are arranged according to a chronological time sequence. This transaction history allows a consensus on the sequence of individual transactions.

> *"It's the same situation as gold and gold mining. The marginal cost of gold mining tends to stay near the price of gold. Gold mining is a waste, but that waste is far less than the utility of having gold available as a medium of exchange. I think the case will be the same for Bitcoin. The utility of the exchanges made possible by Bitcoin will far exceed the cost of electricity used. Therefore, not having Bitcoin would be the net waste."*
>
> Satoshi Nakamoto

[110] See "Swirlds and CULedger Collaborate to Deliver High Performance, Secure, Distributed Applications to Credt Unions," *Swirlds,* October 27, 2017.
[111] See "The Future Of Distributed Ledger Technology: Hashgraph Launches Hedera Platform," Jorn van Zwanenburg, *Invest in Blockchain*, March 26, 2018.
[112] See "The Next-Generation Internet: Mance Harmon and Hedera Hashgraph," *Bitsonline*, May 3, 2018.

Figure 17: Difference Between a Blockchain and the Hashgraph at the Block Level.

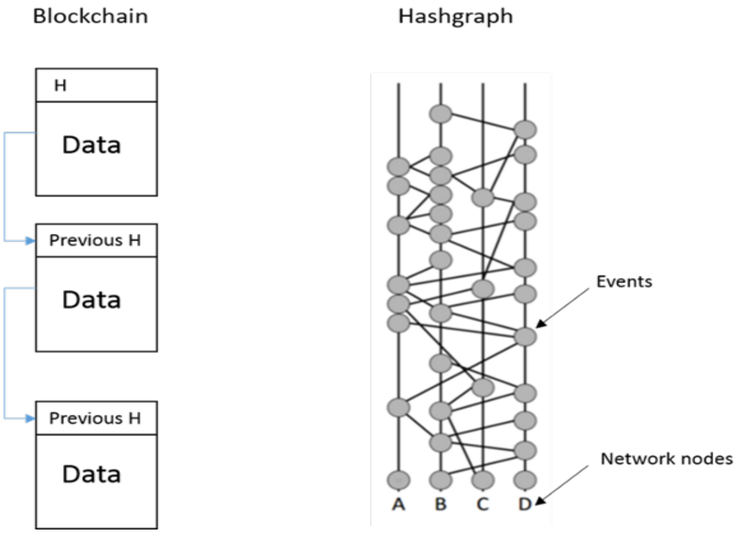


Source: The Hindu.[113]

> *"There are 100 different blockchains out there with 100 different ways that they are going to fix this scaling issue. Part of my thesis is the assumption that they are going to fix it."*
>
> Mike Novogratz

With the Hashgraph concept, the necessary information within the network is also transferred via the so-called Gossip protocol, a communication protocol. To disseminate information within a network, the Gossip protocol is considered the fastest and most efficient method of communicating between different computers. Each computer passes the received information to a randomly selected computer. This leads to an exponential dissemination of information throughout the network.

Figure 18: The Structure of a Blockchain and the Hashgraph in Comparison.



Source: The Hindu[114]

[113] See "Can Hashgraph succeed blockchain as the technology of choice for cryptocurrencies?," Rohan Abraham, *The Hindu*, March 25, 2018.

[114] See "Can Hashgraph succeed blockchain as the technology of choice for cryptocurrencies?," Rohan Abraham, *The Hindu*, March 25, 2018.

However, the mere dissemination of information within the network is not sufficient to achieve a consensus on the shared information. For this purpose, each network participant must know the exact transaction history and thus the exact sequence of individual transactions, which is ensured by the timestamps already mentioned. Therefore, the Hashgraph consensus algorithm makes use of the "Gossip-about-Gossip" approach. Every computer within the network shares all its knowledge about which network accounts spoke to what, to whom and when. Or more technically speaking: Each computer shares all its knowledge about the Hashgraph, which is the exact order of all transactions ever occurring on the network. Because each network participant always has the current Hashgraph, each computer knows the entire transaction history. All participants know that every other participant within the network has all the relevant information about transactions and their order. This circumstance enables what is called "virtual voting" because all nodes in the network have a copy of the transaction history and information about who received the information at which point in time, each participant can calculate how each other network participant will behave. Therefore, each node knows the decision of the other, without an effective decision, i.e. a "vote", having been made. On the basis of this "voting without voting", there is thus a consensus among the network participants, although they do not have to carry out a resource-intensive coordination procedure among themselves.

"The revolutionary stuff are these utility tokens or the token economics"

Mike Novogratz

Interestingly, the voting algorithms used for Hashgraph are already over 35 years old and are used in a slightly modified form. These are so useful because they have a mathematically proven level of security that, to this point in time, cannot be outsmarted. The experts behind Hashgraph therefore claim - and refer to mathematical evidence - that Hashgraph is the only DLT technology to be A-BFT (asynchronous Byzantine fault tolerance). According to them, this means: As long as less than 1/3 of network participants have no intention to defraud the network, a consensus can always be found among the computers about the state of the network and the transaction history.

The Future Vision for Hashgraph

As a form of DLT technology, the Hashgraph is also intended to radically change the structure and organization of today's Internet and with it the world. It is becoming increasingly obvious that the Internet in its current form has serious shortcomings, some of which are due to original birth defects. Today, large centralized server facilities are the cornerstones of our global Internet. Due to these neuralgic points of attack, things like hacks, spam, BotNet or DDoS attacks[115] are part of everyday online life. Again and again we are reminded of this fact in reality.

[115] See "What is a DDOS Attack?," *Digital Attack Map,* 2018.

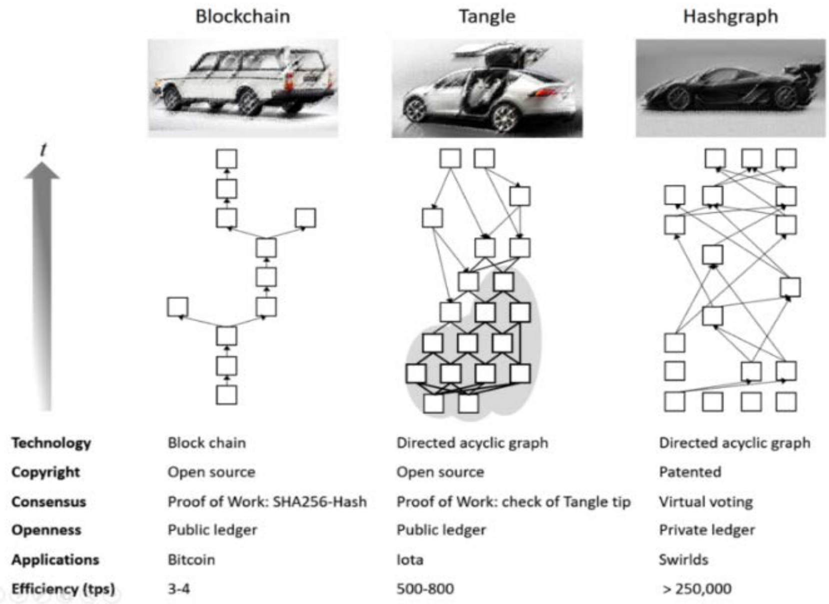
“Very funny. How can a crypto community be toxic? Wasn’t it you @ArminVanBitcoin, who was starting this thread? Maybe you should concentrate first on the problems around Bitcoin, before you start critism on other currencies like IOTA.”

Udo Pasch

In addition to inadequate security, the Internet also suffers from isolation. What this means is that the Internet as a whole consists of mass isolated systems that are not connected to each other by default, which makes smooth communication between these separated silos tedious and complex. Although the Internet appears to be a perfectly interlinked network on the surface, it still consists of countless separate worlds whose bridging is very resource-intensive.

Hashgraph sees itself as a potential solution for these problems. With Hashgraph, it should be possible to create an “Internet of Shared Worlds” that minimizes numerous security risks that exist today and at the same time eliminates isolation. Moreover, this new Internet powered by Hashgraph should in the future enable everyone to create their own world, their own community.

Figure 19: A Simple Overview of the Most Important Key Points of the Various Distributed Ledger Technologies.



	Blockchain	Tangle	Hashgraph
Technology	Block chain	Directed acyclic graph	Directed acyclic graph
Copyright	Open source	Open source	Patented
Consensus	Proof of Work: SHA256-Hash	Proof of Work: check of Tangle tip	Virtual voting
Openness	Public ledger	Public ledger	Private ledger
Applications	Bitcoin	Iota	Swirlds
Efficiency (tps)	3-4	500-800	> 250,000

Source: Fintech News[116]

The hash graph protocol, which in contrast to conventional blockchain protocols already allows scaling on its basic protocol, is designed to fundamentally change the model of Internet data storage also. According to experts, data storage is to be vastly distributed across and within networks. For the provision of their data storage capacity, corresponding network participants would be remunerated on the spot by means of micropayments. The financing of large centralized server units for data storage would no longer be necessary, say advocates believing in the vision of Hashgraph. At the heart of this new Internet would be DLT technologies such as the hash graph, which transparently capture all important information about the community. If Internet applications were based on Hashgraph technology, participants could be sure that the rules defined by the protocol would be enforced in a fair way for all, as they are secured and enforced by cryptography and mathematics. In this way, the individual communities could communicate

[116] See “10 Years Blockchain. The Race is on: Blockchain vs. Tangle vs. Hashgraph,” Prof. Patrick Schueffel, *FinTechNews*, February 19, 2018.

smoothly with each other via DLT technologies and reach a consensus in this new world of digitally shared worlds.

Hashgraph connoisseurs also insist on another important point: This technology can also make the Internet faster. Today's leadership-based Internet, which is based on central servers that have to route all data traffic through the entire system, appears to us to be fast. However, if the Internet were based on a DLT technology such as the Hashgraph, even higher speeds would be possible. With its private Hashgraph network, Swirlds has achieved a higher transaction speed in test attempts than the Visa network currently has. Here too, the visionaries of Hashgraph see another reason why their protocol could possibly improve the existing Internet.

Tangle & Hashgraph - Can They Keep Their Promises?

As described at the beginning of this chapter, innovative approaches such as the Tangle or Hashgraph are seen as the next generation in the still young history of DLT technology. Free market competition is further fueling innovative. The speed with which innovation progresses is astonishing - but the mutual rivalry between the projects often turns into real animosity. The debates degenerate into childish mud battles, which do little to advance the crypto, blockchain and DLT world as a whole. It is difficult for investors to keep track of all the cheap, emotionally charged and often personal accusations and criticisms and to arrive at a reasonable assessment of each cryptocurrency’s potential capital gains.

“Is IOTA just hype or is there real value in Tangle? I've only heard bad things like centralized with coordinators and that they rolled their own crypto and had a huge vulnerability. I'm open to be convinced...”

Charlie Lee

Nevertheless, one of the more meaningful objections should be briefly described: In the case of a DAG, there is no global network state, since a DAG (Tangle and Hashgraph) has no blocks and is based to some extent on the principle of regional consensus. This means that network participants no longer store all transactions, but only “local” data of their “neighbors” and rely on “other regions” to do the same carefully. The ultimate question here is whether this concept of regionalism can actually prevent double-spend-attacks. To be fair, it has to be said that the same question arises in Ethereum's scaling companies that want to take advantage of the sharding solution.

There are also fears that the Tangle and Hashgraph will assume a huge data size due to their scalability and that this will lead to centralization among those network nodes who keep the network running. IOTA and Hedera Hashgraph seem to have a solution for this problem: they announced to regularly shorten the Tangle or Hashgraph. Of course, this would mean though that the networks would potentially introduce certain neural centralized points of attack again. Those responsible for either project argue that the coordinators of the Tangle and the leadership council of the Hashgraph only have a supporting function. Once the two projects had reached a certain size and relevance, these “support wheels” would no longer be needed, on which the IOTA coordinators and the Hashgraph Leadership Council would lose influence. By then the problem of too big data pools might have been solved as well. Until then, however, a lot has to happen, and the projects must first achieve the promised scaling. Although both the Tangle and Hashgraph appear promising, they have yet to provide the final and practical proof for what the claim.

About Us

The Team

Mark Valek

Portfolio Management & Research

Demelza Hays

Research & Portfolio Management

Andres Coronado

Research

Friederich Zapke

Research

The Report

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

The Company

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

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

Advisors

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

Max Tertinegg

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

Oliver Völkel

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

Stefan Wieler

Stefan Wieler, CFA, CAIA, is the vice president of research and corporate sales at Goldmoney. For the past two years, Mr. Wieler has been the head of research at BBL commodities, which is an energy-focused hedge fund that trades WTI, Brent, RBOB, HO, Gasoil, and Natural Gas. Previously, he was a senior oil analyst for Goldman Sachs.

We sincerely want to thank the following friends for their outstanding support:
Our knowledgeable advisors including Max Tertinegg, Oliver Völkel, and Stefan Wieler, the generous authors who contributed to this report including Nikolaus Jilch, and Pascal Hügli. We are also grateful to the newest members of the Incrementum team, Andrés Coronado and Alban Zapke.

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 oran invitation to buy or sell financial instruments. Specifically, the document does not serve as a substitute for individualinvestment or other advice. The statements contained in this publication are based on the knowledge as of the time ofpreparation 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 donot accept any responsibility (and neither does Incrementum AG) for the correctness, completeness or timeliness of theinformation, respectively the information sources, made available, as well as any liabilities or damages, irrespective of theirnature, that may result there from (including consequential or indirect damages, loss of prospective profits or the accuracy of prepared forecasts.