crypto research .report

April 2019
Edition VI.

"When the Tide Goes Out…"

Investments: Gold and Bitcoin, Stronger Together

Technical Analysis: Spring Awakening?

Cryptocurrency Mining in Theory and Practice

Demelza Kelso Hays
Mark J. Valek

crypto research .report

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

coinfinity

www.cryptofunds.li

Contents

Editorial

Dear Reader,

"Only when the tide goes out do you discover who's been swimming naked." This quote is attributed to star investor Warren Buffett, who has experienced a multitude of economic cycles. The ebb did indeed set in this crypto winter, and the entire industry is currently going through a period of heavy consolidation. Many enthusiastically started projects were either put on hold or failed completely. The teams behind numerous utility coins have disbanded over the last year, as the promise of easy money turned out to be a pipe dream. The area of crypto-mining also suffered severe setbacks.

Since **mining is a major component of decentralized crypto currencies**, our report also focuses on this issue. To gain an insight into what is happening in the world of mining, we have interviewed mining companies including Unity, Blockbase, and Alpine Mining. We want to understand how their business model works and how they came through the bear market.

Further we look at an **investment strategy that combines gold and crypto currencies**, which could offer interesting risk-return characteristics for institutional investors. We have also updated our **technical analysis** for the 2019 crypto market.

We are proud to announce our two newest Premium Partners in our April issue: Coinfinity and Bitcoin Suisse. Coinfinity is a crypto broker and supporter of the Lightning network from Graz, Austria. Coinfinity has designed a "Card Wallet" in cooperation with the State Printing Office - a simple version of a paper wallet for Bitcoin. Without Bitcoin Suisse, we would hardly have such a vibrant ecosystem in Zug's Crypto Valley. Bitcoin Suisse is mainly a broker, but it also supports the Crypto Franc Stablecoin project, Värdex's ATM network and the Swiss Crypto Vault.

We hope our report can continue to help investors distinguish between who is swimming and who is sinking. After all, surviving the crypto winter will make some players stronger and perfectly positioned for the next crypto spring, when it finally arrives.

Demelza Kelso Hays and Mark Valek,
Incrementum AG

In Case You Were Sleeping: When the Tide Goes Out…

"Only when the tide goes out do you discover who's been swimming naked."

Warren Buffett

Key Takeaways

- **Bitcoin's price recovered 63% from its low of $3,125 in December. JP Morgan, Fidelity, Nasdaq, Goldman Sachs, Swissquote, Vontobel, and Twitter are preparing the drinks and food for guests in preparation of a new bull market.**
- **Investors have historically priced in each Bitcoin halving 458 days prior to the halving. We are currently about 400 days away from the May 2020 halving.**
- **New bull market gains even more momentum if negative interest rates are charged on personal bank accounts held by retail investors as recommended by the International Monetary Fund.**

It's still chilly in cryptoland, but with the Twitter founder and the bosses of Fidelity and Nasdaq, the circle of Bitcoin fans is getting bigger and bigger. Even JP Morgan is doing crypto now.

Back to the Roots

Source: Twitter

What's the purpose of Bitcoin? This question is often answered with far-reaching visions. The word "revolution" is often used. "Blockchain" of course. But sometimes a news item surfaces that makes things much clearer. **Bitcoin's purpose is to give financial sovereignty; not for a state or a company, but for the smallest of all minorities: the individual.**

In February, the International Monetary Fund once again raised the question of how negative interest rates could be implemented in the event of the next recession. **You should know that conventional monetary policy has only one answer to a crisis: cheap(er) money, i.e. lower interest rates.** But since the great financial crisis we have reached a limit. If the interest falls below zero, someone has to pay. Either the banks or their customers, the savers. They can tolerate negative real interest rates. It's not so obvious. But when it comes to actually losing money from their account, they get restless. This has not yet happened for private individuals, but it has happened for companies in Europe. Their reaction: they started stashing cash in vaults.[1][2]

"If they become widely accepted, virtual currencies could have a substitution effect on central bank money."

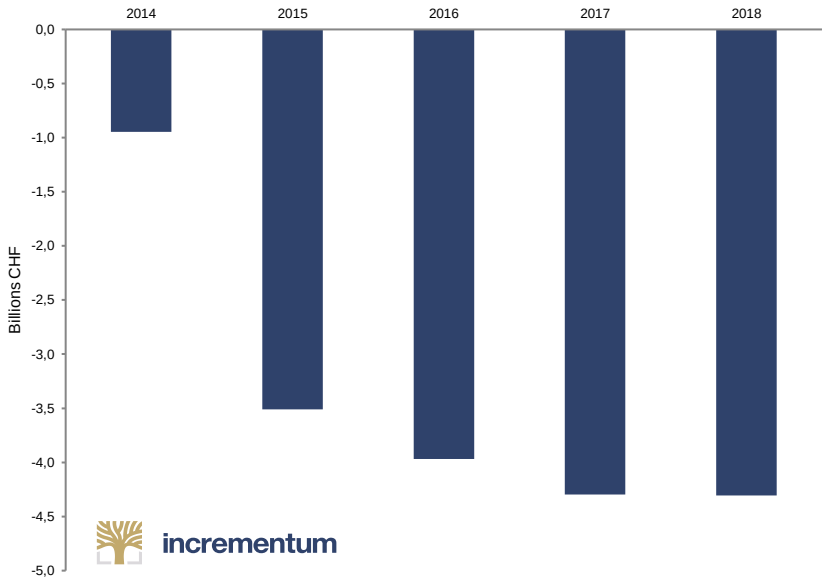
European Central Bank

In the next crisis, when the negative interest rates become even more extreme and also hit private customers, they will react similarly, according to the experts of the Monetary Fund. **Their "solution" is to massively restrict the use of cash in order to make it more difficult to escape expropriation through interest rate policy.** Ironically, they even want to introduce an "electronic currency". With that in place, negative interest rates can be easily implemented according to economists. At the same time, they have in mind a two-tier society. Anyone who wants to pay cash in the supermarket could do so - but with a penalty surcharge. This "nudging" will herd us all into the clutches of the state electronic monetary system that they have in mind.[3]

—

1 See "Bargeld soll in den Tresor statt zur EZB", Handelsblatt, June 8, 2016
2 See "Immer mehr Schweizer Firmen bunken Bargeldberge", Die Presse, September 13, 2016
3 See "Cashing In: How to Make Negative Interest Rates Work", IMFBlog, February 5, 2019

Figure 1: Negative Interest Payments of Banks to Swiss National Bank



Source: SNB, Incrementum AG

"There's something going on here, Millennials trust [Bitcoin] more than fiat currency."

Jeffrey Sprecher,
Chairman of the NYSE

Luckily, nothing is eaten as hot as it is cooked. These ideas are neither economically sound nor politically feasible. But the proposal should serve as a warning to us. By now it should be clear why Bitcoin is here to stay. Why it's needed. It's the antidote to such crazy ideas. Bitcoin makes it possible to get out of a system that is becoming increasingly hostile towards the users.

Of course: Bitcoin is still young. The extreme volatility is a deterrent. The technical difficulties, the hacks, scams and criminal cases as well. All these are growing pains that are to be expected when building a completely new, alternative monetary system. The *Crypto Research Report* has been documenting these developments for almost two years now and our sister report, *In Gold we Trust* has been covering cryptocurrencies since 2014. We offer an alternative explanation to the mainstream media's fixation on Bitcoin's price.

The falling price since January 2018 has curbed Bitcoin's attractiveness and the crypto winter is still underway. The industry is bleeding. More and more companies have to reduce their staff. We are not even talking about the big and small investors who have lost a lot of money - at least on paper. The comparison with the dotcom bubble is certainly fitting. Too many people have invested too much money in ambitious projects that have often failed to deliver on any of their promises. But where there's shade, there's also light. And we can see some big rays shining through. But first we have to talk about the shadow.

How Long Will This Bear Market Last

According to Coindesk, Bitcoin is officially in the longest bear market in its history.[4] However, this is very hard to estimate. Since December 2017, when the

—

4 See "Bitcoin is Now Officially In Its Longest Bear Market Ever", Coindesk, February 2, 2019

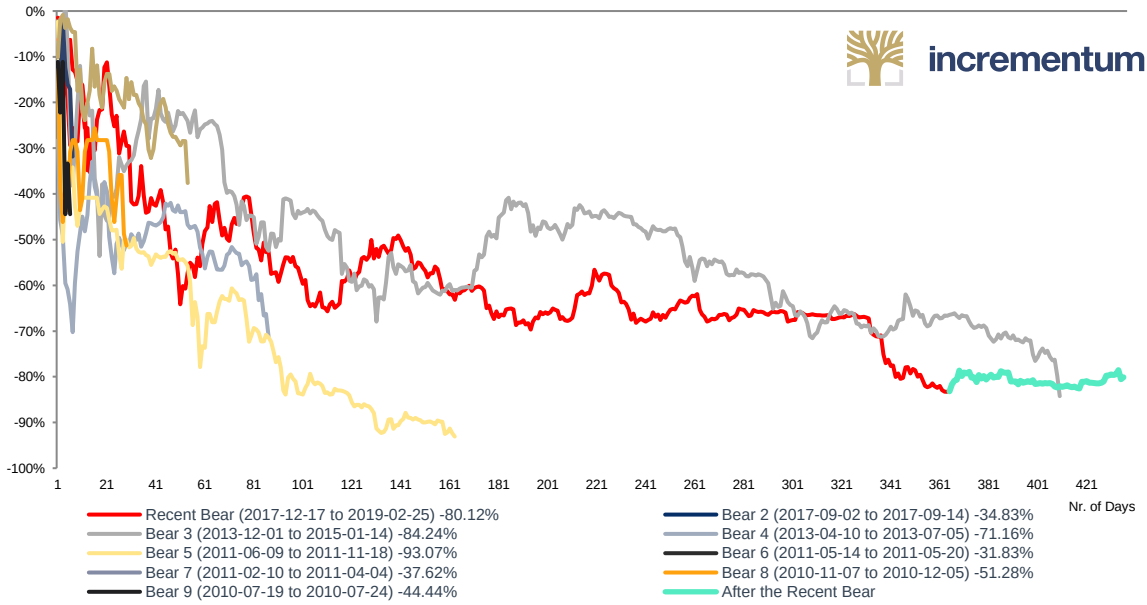
"Cryptocurrency currencies take the concept of money and they take it native into computers, where everything is settled with computers and doesn't require external institutions or trusted third parties to validate things."

Naval Ravikant

price of one Bitcoin briefly rose to $19,764, the price fell for 360 days before reaching its most recent trough at $3,125 in December of 2018. Shortly after, Bitcoin actually surpassed $4,000, realizing a gain of over 29.92%. Although, the price dropped down shortly afterwards. Defining a bear market by a percentage loss or gain in cryptocurrencies is difficult because of the strong volatility associated with the asset class. Talking about stock markets usually the beginning of a bear or bull market is defined by losses or gains of 20%, respectively. Empirically, Bitcoin has only had three downturns that lasted more than three months, and each saw a loss of over 80%. In contrast, Bitcoin has only had several bull markets with returns over 1000%, but only two of them lasted longer than five months. In the *Crypto Research Report*, we define a bear market as a drawdown of over 30%. We define a bull market as a gain of 30%. **Therefore, we have officially begun a new Bitcoin bull market.**

The crypto winter saw a maximum drawdown of 84%. In contrast, the first bear market lasted only 163 days. This was in 2011, when the price fell from $31.50 to $2.01, which equates to a loss of 93%. Between 2013 and 2015, prices fell by 86%. Although we are hopeful that the movement from $3,125 to the current price around $5,000 is the beginning of a new bull market, we will only know in hindsight whether or not the tide has come back in. **However, a hint may lie in the Bitcoin's monetary policy.**

Figure 2: Bitcoin Bear Markets



Source: Yahoo Finance, Incrementum AG

Every 210,000 blocks, the reward the miners receive per block is halved. This roughly corresponds to a four-year cycle. Observers pay very close attention to the schedule, because the so-called "halving" is regarded as an important indicator of price movement. There is only little experience so far, since there have been only two such "halvings". But they show that the price has always risen in the months before the actual event. Specifically, the Bitcoin price found its

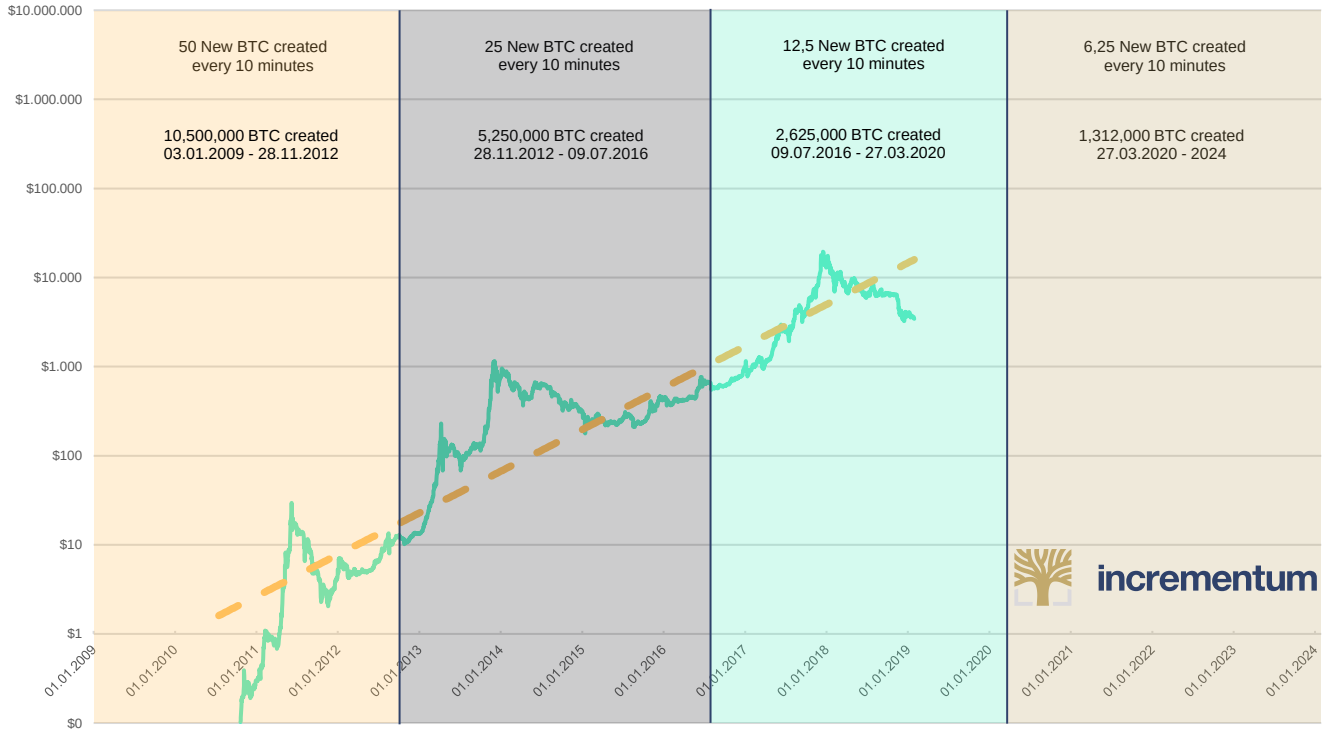
"The last time Bitcoin saw its 50-day moving average cross definitively above the 100-day moving average, a spot on the ledger cost about $300. Since then, bitcoin is up 17x. It just happened again."

Bill Miller IV

bottom in the first bear market exactly 378 days before the first halving. And in the second bear market 539 days before the second halving.

This equals an average of 458 days, and we are currently approximately 400 days from the next halving. The next halving will probably take place towards the end of May 2020. **If the pattern observed so far is confirmed, the bottom should occur somewhere between December 2018 and May of 2019.** So far so good, but again: in retrospect, we'll be smarter.[5]

Figure 3: Bitcoin Halving



Source: Incrementum AG

A Tragic Story Traverses the World

Since the megaboom at the end of 2017, no Bitcoin story has been as present in the mainstream media as the one about the mysterious death of Gerry Cotten. The founder and CEO of Canadian crypto exchange Quadriga CX died unexpectedly at the beginning of December on a trip to India. Complications with his chronic bowel disease were given as a cause of death. Quadriga had money problems before, after their bank had frozen nearly $26 million of their funds. But what followed Cotton's death was much worse. His widow told the Canadian authorities that Cotten had used his encrypted laptop to handle all the finances of the exchange. And that, despite the involvement of experts, she has not yet succeeded in cracking the laptop.[6]

—

5 See "Bitcoin is Now Officially In Its Longest Bear Market Ever", Coindesk, February 2, 2019
6 See "QuadrigaCX Shutters, Claiming It Lost Access to Crypto Accounts After CEO's Mysterious Death", BREAKERMAG, February 1, 2019

As a result, almost $140 million in client funds are no longer available. It is understandable that major customers now want to take legal action. There is also wild speculation within the community. After so many cases of frauds and rip-offs that the crypto world has seen in the past months, the distrust is enormous. Is Gerald Cotten still alive? Does his wife pretend she doesn't have access to the money? There are more than 20,000 Bitcoin and a number of Altcoins missing. The Reddit community watches the well-known Quadriga wallets with eagle eyes.[7][8]

Source: Twitter

On a meta-level, the case underlines two things: **crypto exchanges are a damn bad place to store your coins**. If you don't want to take responsibility for your own funds, you should fall back on professional providers of custodianship solutions that are insured by regulated insurance agencies.[9] Or even stay away from cryptoassets altogether. Quadriga was not the first and probably not the last case in which an exchange did not deal professionally with its customers' funds. Many exchanges have experienced rapid and tremendous growth. Their systems did not always grow with them. Scaling problems affect not only the blockchains themselves but also the infrastructure of the market.

When the tide goes out…

"Only when the tide goes out do you discover who's been swimming naked."

Warren Buffett

It was to be expected that scams and half-baked projects would be uncovered and disappear in a bear market. This is what happened in the "normal" market after the great financial crisis in 2009. But now a second wave is also hitting the crypto sector. A phase that was also to be expected: it is shrinking. **Jobs are being cut**

—

7 See "Digital exchange loses $137 million as founder takes passwords to the grave", Arstechnica, February 2, 2019
8 See "Zwei mysteriöse Todesfälle erschüttern die Bitcoin-Welt", Die Presse, February 5, 2019
9 Last *Crypto Research Report* we had a closer look at different custody solutions.

from companies that want to slim down for winter so that they can still exist at the end of the crypto winter.

The most prominent case is probably ConsenSys. This "decentralized company" serves as a kind of umbrella fund for around 50 Ethereum projects, which Ethereum co-founder Joe Lubin himself has selected. Lubin announced in December 2018 that **13 percent of the 1200 employees will leave the company** and that the entire project will be restarted as "ConsenSys 2.0". This also fits in with the plans to rebrand Ethereum as "Ethereum 2.0".

Lubin himself is considered one of the richest men in the scene because he has a large amount of ETH at his disposal. But that is not enough to keep ConsenSys running in the form of 2017 and 2018. According to Forbes, the "decentralized company" consumes about $100 million a year. **And developers report that they never had to present a business model to get money.** All it took was a thumbs up from Uncle Joe.[10]

"In my 43 years as a trader there has never been a move like $BTC. The only other market that achieved a superior parabolic advance was German interest rates in 1920s."

Peter Brandt

Even the Chinese crypto giants **Bitmain and Huobi are not getting off scot-free.** Bitmain is the world's largest manufacturer of mining hardware. The company will experience "some adjustments in the workforce", according to a press release. Followed by a phrase that is often used in bad times. Bitmain says that they want to concentrate again on "their core business". Bitmain denied rumors that **more than half of the employees had to leave.**[11] Bitmain also closed a research center in Israel and fired 20 employees there. Huobi, one of the world's largest exchanges, also announced that it would "optimize" its workforce. The employees with the worst performance would have to leave. Bitmain had almost 2600 employees in its prime, Huobi more than 1000.

Other prominent victims of the bear market were the decentralised social media platform SteemIt and the NEM Foundation, which is behind the cryptocurrency XEM. **SteemIt had to reduce staff.** The **NEM Foundation slipped into a real bankruptcy** - only to ask the community for the equivalent of $8 million in order to be able to continue until February 2020. AKA, in order to make a "restart". That's a very popular word in the scene at this stage: restart. Soon it'll all be "2.0."

"Downsizing is a natural cycle in new, rapidly growing industries and blockchain is unfortunately no exception."

Jehan Chu

Jehan Chu, the co-founder of Kenetic Capital in Hong Kong said in an interview with the South China Morning Post "We have also seen this with the Internet in the early 2000s. But this period has also produced some companies that are today the

—

10 See "Insiders Say ConsenSys Faces a Hurdle to 2019 Rebound: Joe Lubin's Grip", Coindesk, January 9, 2019
11 See "China's Bitmain Technologies and Huobi plan lay-offs as cryptocurrency crunch begins to bite", South China Morning Post, December 26, 2018

largest in this sector. I'm looking forward to a better, more focused version 2.0 of the blockchain industry."

"If the cryptocurrency market overall or a digital asset is solving a problem, it's going to drive some value."

Brad Garlinghouse

Admittedly, this is a dream for the future. At the present time, we must tighten our belts in Europe too. In the famous Crypto Valley in the Swiss city of Zug many cutbacks have already been announced. During the boom, too many start-ups had generously hired people who they can no longer afford or want to pay. Shapeshift, which is based in Switzerland, **let about 37 employees go** - a third of the workforce.[12] Locally, Crypto Finance in Switzerland had to lay off seven staff members mostly coming from their sales team.[13] In Liechtenstein, the Binance-supported exchange LXC is rumored to be having major problems.

Some crypto projects, such as Hosho's Smart-Contract auditors, had to **reduce up to 80 percent of their employees** to get through the cryptowinter.[14] But there are also success stories: Blockdaemon, for example, which hosts nodes for blockchains, had a good year: "This is the most productive phase we have ever been in," said CEO Konstantin Richter. Many start-ups have to step on it to deliver what they promised - and they are turning to service providers such as Blockdaemon: "The projects now have to show what they are made of. The time is up of raising a lot of money and talking a lot of talk." Some investors are even happy about the cryptowinter. Many projects that were previously overvalued can now be entered at more reasonable prices.[15]

A State Cryptocurrency?

"I think the internet is going to be one of the major forces for reducing the role of government."

Milton Friedman
Nobel Prize Nominee in Economics

Bitcoin was originally invented to offer people an alternative to state currencies. Therefore, we are sometimes very surprised when the crypto fans absorb every message of an alleged "state crypto currency" as if it were honey. Especially since the nations in question are often a little questionable. We are not talking about the "electronic currency" that the IMF experts have in mind, but about Venezuela and Iran. The allegedly planned "crypto rial" is currently fascinating the media. In Venezuela, it was the Petro. The motivation is the same for both countries: they want to avoid US sanctions. Neutrally speaking, that is understandable. But the "Petro" of Venezuela can be considered a grandiose by most accounts.

Be that as it may, Iran is allegedly in talks with eight states from Europe and Africa (including Switzerland, Austria and Russia).[16] The content of the talks is whether international transactions could be carried out with cryptocurrencies. At the same time, there are reports of a "crypto rial" that may be linked to gold. Iran has been cut off from the international monetary and banking system for months. Europe, on the other hand, has a strong interest in circumventing the new US sanctions

—

12 See "Schweizer "Crypto Valley": Bitcoinkrise bringt viele Jobverluste", Futurezone, February 1, 2019
13 See "Swiss Crypto Firm Pares Staff", Finews, February 5, 2019
14 See "Smart Contract Auditor Lets Go 80% of Staff in Crypto Winter Cutbacks", Coindesk, February 1, 2019
15 See "Crypto Winter Isn't Fatal For All 'Picks and Shovels' Makers", Bloomberg, January 16, 2019
16 See "Talks with 8 countries over using cryptocurrency in monetary transactions going on", TehranTimes, January 28, 2019

and maintaining trade relations. Even an own agency was founded, the INSTEX. It is intended to facilitate trade between European countries and Iran. At the same time Tehran signals to consider everything that could harm the "great Satan" USA.[17][18]

"The performance of commodities like gold and oil have been far from stellar since November 2013, and in the period up to January 2017, bitcoin actually outperformed oil."

Chris Burniske and Jack Tatar

Against this background we ask ourselves: Why does it need a "crypto rial"? Is this all about propaganda? Misinformation? Which European country, which Russian company should accept such a new coin? If Tehran were really serious about using cryptocurrencies, wouldn't the Iranians immediately resort to Bitcoin? Especially since the First Mover would have enormous advantages in such a scenario. As long as no such plans are known, we will not take the news from Iran too seriously. A "crypto rial" would probably have the same success as the "Petro" from Venezuela. **None at all.**

The Swedish plans for an E-Krona are of course different. They are to be taken quite seriously. Especially since Sweden is a test laboratory for the "cashless society". But here, too, we are still years away from implementation. And if it comes in the end, it will be a kind of cash substitute on a blockchain basis, not a cryptocurrency with its own monetary policy.[19]

Meanwhile in Europe, central banker Ardo Hansson has attracted attention - as a harsh critic of cryptocurrencies: "I think we will come back in a few years from now and say how could we ever have gotten into this situation where we believed this kind of a fairy-tale story", Estonia's central bank chief said in January. Crypto currencies are a "complete nonsense" and will probably disappear, says Hansson.

"Bitcoin is history's first universally honest ledger."

Caitlin Long

We need to point out that there are 19 national central bank governors and one ECB president in the euro zone.[20] These 20 people do not always agree and do not automatically speak for the Eurosystem when they express an opinion. It's also not surprising that a central bank chairman, no matter which country, has nothing good to say about Bitcoin. Let us recall the IMF story we mentioned at the beginning of the report. Bitcoin is not only the enemy of state fiat money, but also hinders the implementation of extreme monetary policy elements. But it is a pity, nevertheless, that an ECB man is so derogatory. For the economists of the ECB were the first of a large central bank to deal with the advantages and disadvantages of Bitcoin in detail as early as 2012. It would be a pity if such a differentiated point of view from a serious source was forgotten, because the bosses prefer to make pithy remarks. That is why we recommend that everyone read the two ECB reports on Bitcoin. These come from a time when the central banks did not yet see the cryptocurrency as a threat, but as an enrichment.[21][22]

—

17 See "Iran's Crypto Experiments Are a Shield Against Trump's Unilateralism", BREAKERMAG, February 1, 2019
18 See "Europa legt sich mit König Dollar an", Die Presse, February 2, 2019
19 See "Difference between e-krona and crypto-assets", Sveriges Riksbank, October 18, 2018
20 See "Virtual Currencies To Go Down as 'Load of Nonsense," Says ECB's Hansson", Bloomberg, January 7, 2019
21 See "Virtual Currency Schemes", European Central Bank, October, 2012
22 See "Virtual currency schemes – a further analysis", European Central Bank, February, 2015

Support is Increasing

Source: Google Keyboard

Economists and central bank leaders who reject Bitcoin are truly no new phenomenon. What is striking, however, despite the ongoing bear market, is that the number of celebrity names that openly support Bitcoin is growing strongly. There's Twitter's CEO Jack Dorsey who said in a podcast,

"I believe the internet will have a native currency and I don't know if it's bitcoin. I think it will be bitcoin given all the tests it has been through and the principles behind it, how it was created. It was something that was born on the internet, was developed on the internet, was tested on the internet, and it is of the internet."[23]

Dorsey even went so far as to say that in the end the world knew only one currency, and that Bitcoin was that currency. The timeframe he has set for this unique revolution is very ambitious: Ten years, maybe faster. Of course, Dorsey is also behind Square and its Cash App, where Bitcoin can be traded. Like all other proponents (and opponents), he therefore has a certain self-interest. Dorsey also recently confirmed that he wants to integrate the Lightning Network into his cash app as soon as possible.[24]

Source: YouTube

Not only the Twitter founder, but also another social media giant is playing with the idea of integrating cryptocurrencies into his apps. We are actually talking about Mark Zuckerberg. He already said at the beginning of 2018 that he wants to deal more closely with cryptocurrencies. It was a New Year's resolution back then. What has come of it now? Less than a year later, reports appear that Facebook is developing its own cryptocurrency to enable money transfers via WhatsApp. This is not about Bitcoin, **but about a stablecoin that is supposed to be pegged to the dollar.** In any case, Zuckerberg is fully in line with the trend. The competition of

—

23 See "Twitter CEO Jack Dorsey Has Made A Bold Prediction About Bitcoin", Forbes, February 4, 2019
24 See "Square CEO Jack Dorsey Says Bitcoin's Lightning Is Coming to Cash App", Coindesk, February 11, 2019

Kik and Telegram is also tinkering with its own currency. And in China, WeChat has long since dominated the market for mobile payment.[25]

We also can report remarkable news from Samsung. It has equipped its new top smartphone, the Galaxy S10, with a crypto wallet.[26] This is a big step towards user-friendliness for Bitcoin. And the South Koreans are also putting massive pressure on Apple. In any case, it seems appropriate, because in South Korea cryptocurrencies are still extremely popular despite the crypto winter.[27]

Preparations are also underway by the major financial institutions. Vontobel and Swissquote from Switzerland have both just introduced custodianship solutions for banks and asset managers. Bank Vontobel says it is the first in the world to meet all the standards of financial institutions and regulators. The product is called Digital Asset Vault and enables other banks and asset managers to offer their customers the purchase and sale of cryptocurrencies. Vontobel positioned itself early on as a Bitcoin-friendly bank and has been offering a Bitcoin certificate for some time, enabling traditional investors to bet on the Bitcoin price.[28]

"Bitcoin is the most compelling alternative asset of the twenty-first century."

Chris Burniske and Jack Tatar

In March, Fidelity Investments wants to follow up and enter the market with its own solution for the storage of Bitcoin and other cryptocurrencies. Fidelity's CEO, Abigail Johnson, is a supporter of Bitcoin and has repeatedly advocated making digital assets available to a wider range of investors. It's convenient that she's in the executive chair of a giant in the financial industry. Fidelity is currently testing the technology with a small group of investors and their own employees. They want to start with Bitcoin, then follow up with Ether. Fidelity is one of the largest fund providers in the US with $7 trillion in assets under management, and they already work with 13,000 financial institutions. If this company gives its customers access to Bitcoin once, you can confidently call it a game changer.[29]

"When I first heard about Bitcoin, I thought it was impossible. How can you have a purely digital currency? Can't just copy your hard drive and have your Bitcoins? I didn't understand how that could be done, and then I looked into it and it was brilliant."

Jeff Garzik
Founder of Dunvegan Space Systems

Nasdaq boss Adena Friedman also outed herself as a Bitcoin fan in early 2019. "Cryptocurrencies can still become the global currency of the future," Friedman wrote in a blog post in the run-up to the World Economic Forum in Davos. Crypto currencies "deserve the chance to take a sustainable future place in our economy." Bitcoin's invention is "great evidence of human resourcefulness and creativity". The ups and downs of Bitcoin's price are due to the classic life cycle of a new invention and are no longer worrying, according to the Nasdaq boss. But the well-known technology exchange has a lot of catching up to do.[30]

—

25 See "Facebook Is Developing a Cryptocurrency for WhatsApp Transfers, Sources Say", Bloomberg, December 21, 2018
26 See "Blockchain Goes Mainstream? Samsung Confirms Digital Wallet Integration for Galaxy", Cryptovest, April 2019
27 See "Cryptocurrency Was Their Way Out of South Korea's Lowest Rungs. They're Still Trying.", The New York Times, February 10, 2019
28 See "Swiss Multi-Billion Dollar Bank Vontobel Launches Regulated Crypto Custody", Cointelegraph, January 14, 2019
29 See "Fidelity Is Said to Plan March Launch of Bitcoin Custody Service", Bloomberg, January 29, 2019
30 See "„Potenzial zur globalen Währung der Zukunft" – Nasdaq-Chefin outet sich als Bitcoin-Fan", Handelsblatt, January 23, 2019

More than a year after the introduction of Bitcoin futures, Nasdaq still has no such product on offer. We already reported in our last report that Nasdaq wanted to introduce such a system soon. Little has happened since then. It almost seems as if players like Nasdaq and the Bakkt project (of ICE, the operator of the New York Stock Exchange) are taking their time because they don't want to risk embarrassment of launching a flop in the middle of the crypto winter. Only when prices recover can they be sure to receive full attention for their new products. After all, the **Nasdaq boss's comments show that the path is clear, it's only a question of timing.**

Source: http://me.me

Speaking of Bakkt, on December 31, 2018, the new digital assets platform raised $180 million in investor funds. Among the donors were the Boston Consulting Group and Microsoft's Venture Capital Arm, M12. A company called Horizons Ventures has also joined. Behind this one is a certain Li Ka-shing. The billionaire is number 23 on the global list of the super-rich. But Ka-shing is no stranger in the Bitcoin scene. He invested in BitPay with Horizon Ventures in 2013 and in Blockstream in 2016.[31]

Most recently, Jeremy Allaire, CEO and co-founder of the crypto company Circle, said in an AMA session on Reddit: "In my view, **crypto is a much more significant and disruptive innovation than the web**, and its impact on society, politics, economics, governance will be far, far greater for humanity over time." Circle was making waves last year when the start-up bought the established crypto exchange Poloniex. The company is also behind the Stablecoin USDC, which is operated jointly with the Bitcoin giant Coinbase. But what makes Circle special: None other than Goldman Sachs is heavily invested in Circle. Rumor has it that Circle is Goldman's crypto experiment.[32]

"I am very intrigued by Bitcoin. It has all the signs. Paradigm shift, hackers love it, yet it's derided as a toy. Just like microcomputers."

Paul Graham
Creator of Yahoo Store

And then shortly before the editorial deadline of this issue, an almost unbelievable message fluttered in: **JP Morgan is the first large bank to develop its own cryptocurrency.** Even if Jamie Dimon, the boss of JP Morgan, is known as a particularly vocal Bitcoin opponent. Admittedly, JPM Coin is not a competitor to the number one cryptocurrency Bitcoin. Instead, JPM is supposed to be a cheap vehicle for money transfers between banks and companies. **Therefore, JPM Coin is more of a competition for Ripple** than for Bitcoin.

—

31 See "World's 23rd Richest Man Invests in Cryptocurrency Exchange Bakkt's First Funding Round", Cryptoslate, January 8, 2019
32 See "Circle CEO Says Crypto Is a "Much More Significant" Innovation Than the Web", BREAKERMAG, January 10, 2019

The JPM coin is a currency tied to the dollar, i.e. it is a stablecoin. The idea seems to be to make it easier, faster and cheaper for large corporate customers to move dollars around the globe. "Pretty much every big corporation is our client, and most of the major banks in the world are, too," says Umar Farooq, who heads the blockchain projects at JP Morgan. "Even if this was limited to JPM clients at the institutional level, it shouldn't hold us back."[33]

Spring setting in?

"People don't need to understand how blockchain works for it to enrich their lives. People didn't understand how e-mail worked in the 90's ... They were told to copy/paste an address into a box, type a message and hit send. That was it, people still hated it at first... it's the same with cryptocurrency, you copy/paste an address into a box, type in a price and hit send. How did e-mail turn out in the end?"

Brad Marsh
CMO PACcoin

So, there is also a lot of good news from the sector, despite crypto winter, layoffs, and deaths. **We suspect that the recent low of $3,125 is the trough of the last bear market, and that we are actually beginning the next bull market**. However, we will only be able to tell in hindsight if this premonition was correct. The well-known Bitcoin bull Mike Novogratz recently said,

> *"There's 118 elements on the periodic table, and only one gold [...] Bitcoin is going to be digital gold, a place where you have sovereign money, it's not U.S. money, it's not Chinese money, it's sovereign. Sovereignty costs a lot, it should."*[34]

What does that mean for the price? Well, Novogratz, has often been wrong here. But for the sake of completeness: he sees $8,000 dollars as an acceptable value in the medium term, which would make sense if investors price in the 2020 halving. Since bitcoin's inflation rate will half, a doubling of the value is what is required in order to keep miners online.

What we know: Mark Dow, a trader who opened his Bitcoin shorts at an almost perfect time at the height of the last bubble, **closed this short at the end of 2018**. As it looks today that was great timing. However, as we have just seen, there are good reasons to stay with Bitcoin. Not only because a number of institutional investors are thinking about entering positions and more and more prominent names are standing behind crypto currencies but **because the original fundamentals of Bitcoin have not changed.** The original use case for Bitcoin - i.e. its use as an independent, censorship-resistant currency - is still intact, and we don't know how many of the current competitors to Bitcoin really have a future.[35] To see that, we just have to look at Venezuela again. There, Bitcoin transactions have recently reached new all-time highs. People do not trust the already broken Bolivar or the state crypto currency Petro. They want Bitcoin. And they buy Bitcoin.[36]

—

33 See "JP Morgan is rolling out the first US bank-backed cryptocurrency to transform payments business", CNBC, February 14, 2019
34 See "Mike Novogratz: Bitcoin Will Be Digital Gold, "Sovereignty Should Cost A Lot"", February 13, 2019
35 See "The Trader Who Nailed the Bitcoin Top Just Covered His Short", Bloomberg, December 18, 2018
36 See "Bitcoin trading in crisis-stricken Venezuela has just hit an all-time high", CNBC, February 14, 2019

"The reason we're all here is that the current financial system is outdated."

Charlie Shrem
Founder of BitInstant

Bitcoin is needed in a world full of crazy money experiments. We also know that Bitcoin as a currency and digital gold is still at the beginning of its life cycle[37]. That technical innovations such as the Lighting Network will be needed to start the next phase. That the next halving, i.e. the halving for block rewards, is due in less than two years. The charts are already circulating on the web today. Bitcoin cycles slow down over time. In other words: The halving alone does not guarantee a new all-time high. But if Bitcoin continues to evolve as before, some calculations suggest that the price will be between $100,000 and $200,000 per Bitcoin by 2023.[38]

Is that a prognosis on our part? Not at all. A buy recommendation? No! But that is the basis for those who are continuing to work on the infrastructure even in a prolonged bear market and for those who plan to buy now - or at least soon, when the bottom is really reached, somewhere between $2,000 and $3,000 dollars. And it is also the reason why we will continue to document the development of this sector until 2020 and beyond.

—

37 See "The Original Crypto Bull Thesis, Revisited & Reinvigorated", Zerohedge, January 2, 2019
38 See "Bitcoin's journey to the new peak will be longer this time", Tradingview

Gold and Bitcoin: A Crypto Strategy, also for Institutional Investors

"Digital gold and physical gold make a highly interesting combination as a portfolio. Excess volatility is dampened by gold, while you still can participate in much of Bitcoin's optionality."

Mark Valek

Key Takeaways

- **Practical problems and structural hurdles have so far prevented most institutional investors from entering the crypto asset arena. A generally low level of expertise and exorbitant volatilities, among other things, were decisive factors in this wait-and-see attitude.**
- **The two assets Gold and Bitcoin have partly similar characteristics but different patterns of price movement. In combination, volatility can be reduced disproportionately due to the diversification effect.**
- **A rebalancing strategy with broad rebalancing bands and an option overlay can further improve the risk-adjusted return significantly and together this combination of assets represents an uncorrelated portfolio building block for a traditional portfolio.**

Where are the Institutional Crypto-Investors?

The crypto-community has been asking this question for a few years now. Given the last hype of 2016-2017, the interest in the young asset class has naturally increased dramatically even among professional investors. However, not many conventional investment vehicles were available for this class of investors during the boom time. This has changed in the meantime. Certificates, futures and regulated funds are now on the market. With falling prices, however, the appetite for the asset class has somewhat disappeared again. At least for now.

"We are seeing more managed money and, to an extent, institutional money entering the space. Anecdotally speaking, I know many people who are working at hedge funds or other investment managers who are trading cryptocurrency personally, the question is, when do people start doing it with their firms and funds?"

Olaf Carlson Wee

An announcement of the investment manager Morgan Creek Capital recently has attracted some attention[39]: its *Blockchain Venture Capital Funds* is backed by USD 40 million coming from traditional investors. These include two public pension funds, a university endowment fund, a network of hospitals and an insurance company. Nevertheless, investments by traditional institutions still seem to be rare.

In our view, this is due on the one hand to special features of the asset class, which cause **practical problems for institutional investors**. On the other hand, **structural hurdles within the asset management sector** are also responsible for the current reluctance of many institutional investors.

Practical Problems for Institutional Investors

The following **practical issues** can be identified in the context of digital asset classes:

- Legal (un)certainty
- Custody
- Liquidity
- Investable vehicles

These practical problems inherent to the new asset class are not trivial, but in our view, are already largely solved.

"There has never been a global recession since Bitcoin was created. Next time it happens, there is an escape hatch."

Erik Voorhees

Legal certainty regarding crypto-assets is of course crucial for institutional investors. The rise of digital assets meant that a whole range of legal issues had to be identified and regulated. First of all, legislators and regulators – as well as the entire investment industry – had to become familiar with and understand the phenomenon of crypto-assets and where necessary create appropriate legal foundations. For a long time, it was unclear whether cryptocurrencies should be treated as securities, cash or commodities. Meanwhile, many regulators have decided that distinctions must be made. The Swiss authority FINMA, for example, has commented on this topic and has provided an important foundation stone for

—

39 In December, we had the honor of holding an exclusive Advisory Board Meeting with Mark Yusko of Morgan Creek.

the classification of crypto-assets with the FINMA ICO guidelines. For corporate financing Security Token Offerings (STO) have to be used instead of the Initial Coin Offerings (ICO), which were misused in the early years. In the case of STO the rights of investors are better protected. Apart from these rulings, legislators by now have decided on the tax treatment of cryptocurrencies and have thus solved the central elements of previously prevailing legal uncertainty.

"I understand the political ramifications of cryptocurrencies and I think that government should stay out of them and they should be perfectly legal."

Ron Paul
Former U.S. Congressman

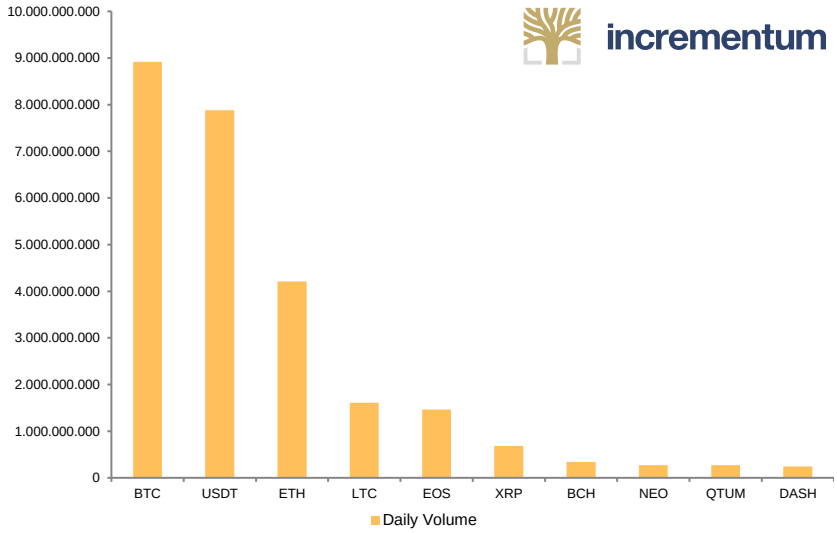
Custody of digital assets is an essential issue. Traditional securities investments have a settled infrastructure that has grown over decades, which has now become a standard procedure for the seamless transfer and safekeeping of assets. The new phenomenon of digital asset management industry is once again facing challenges in terms of safekeeping. In particular, the phenomenon of "cybersecurity" is inherent in this context. In recent years, however, many companies have offered safe and professional solutions for this area. Some of them have already developed so far that they have been approved by the regulators of the European fund industry as safe custody solutions. In our last Crypto Research Report, we dealt with different custody solutions[40].

Cryptocurrency liquidity is also of great importance to institutional investors. They have to make sure that the large volumes they manage can be invested without significant impact on prices (slippage). The measurement of liquidity in this area, however, is problematic. Many large transactions are processed OTC ("over the counter") and not through an exchange. As a result, existing liquidity is underestimated. However, when looking at exchange-traded liquidity, it is probably too high. The background is that crypto-exchanges have an incentive to identify their own market share as high as possible. In any case, apart from the difficulties of accurately measuring liquidity it is remarkable how different the liquidity between the individual cryptocurrencies is. By far the most liquid is Bitcoin. For liquidity reasons Bitcoin is by far the most attractive for an institutional investor, perhaps even the only realistic form of investment within the crypto-universe in the current market environment.

—

40 See January 2019 Crypto Research Report: Crypto Concepts: Cryptocurrency Custody Solutions

Figure 4: Ten Most Liquid Crypto-Assets[41]



Source: Coinmarketcap, Incrementum AG

"We need blockchain technology."

Vladimir Putin

Investment products could not be found in the regulated area until a few years ago. Although in principle, a direct investment in cryptocurrencies would also be an option from the prevailing perspective, from the point of view of institutional investors there is much to be said for investing securitized securities in this asset class. Thus, the custody does not have to be dealt with independently. Furthermore, consolidating crypto-assets with the remaining portfolio values becomes a much easier task.

"For many young people, Bitcoin is the first thing that they are truly responsible for. Everything else has a safety net, a way to undo things should you screw up. It's the antithesis of the "you deserve" BS that they've grown up with and the first real taste of reality."

Jimmy Song

If anything, crypto-investment for institutional investors was originally only possible via moderately regulated offshore hedge fund vehicles, which often do not separate the depositary from the manager. In the meantime, investment in crypto-assets can be done through an increasing number of conventional investment products. For instance, already regulated blockchain and crypto-funds, certificates and ETPs have appeared on the market. Below some examples.

Blockchain & crypto-funds:

- Polychain Capital
- Pantera Bitcoin Fund
- Galaxy Digital Assets

Certificates:

- VONCERT on Bitcoin by Vontobel
- Tracker certificate on Bitcoin by Leonteq
- Bitcoin Tracker One - SEK (COINXBT – ETF type)

ETP:

- Amun Crypto Basket Index
- Amun Bitcoin ETP
- Amun Ethereum ETP

—

41 Average daily trading volume in March 2019

As we can see, many of the practical issues surrounding legal uncertainty, custody and investment products have already been defused or resolved. As far as liquidity is concerned Bitcoin is currently primarily suitable for institutional investors.

Structural Hurdles within the Asset Management Sector

Even more relevant than the initial practical problems today are probably **structural hurdles within the asset management industry**, which slow down the entry of many players. This includes in particular

- The expertise and the decision-making structures within the asset management
- The extraordinary volatility of most cryptocurrencies
- The principal agent dilemma

"Bitcoin is the beginning of something great: a currency without a government, something necessary."

Nassim Taleb

Expertise and decision-making structures within large organizations such as asset managers are highly relevant when it comes to the question of adding a new asset class into the investment universe. In principle, new asset classes do not often emerge during the career of a portfolio manager. The asset management industry's last asset-class "revolution" was probably the spread of hedge funds in the late 1990s and early 2000s. At that time, endowment funds at universities in the US were among the first institutional investors regarding hedge funds as an own asset class. Only gradually institutional investors followed and introduced hedge funds or alternative investments asset classes.

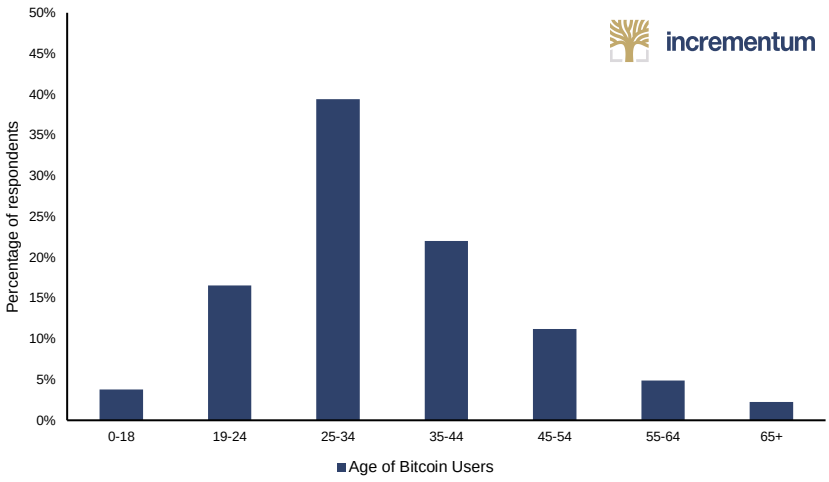
Over the next few years, players in the asset management industry will gradually have to come up with answers to how they handle the phenomenon of digital assets. The majority of institutional investors will for the time being ignore or negate it. However, the longer crypto assets are in the market, the more professional investors will make strategic allocations in this area.

"Digital currency is going to be a very powerful thing."

John Donahoe
CEO of eBay Inc

One of the reasons for the sluggish entry into established institutions is probably that crypto-affine individuals within the organizations tend to be younger while the decision makers tend to be older. Of course, a young person does not automatically have to be comfortable with the crypto-phenomenon, but an affinity may be more likely because younger generations as *"digital natives"* are more likely to be in touch with the developments in the crypto-world and therefore better able to understand it. Even though there are counterexamples, there is one thing that catches your eye: young crypto-savvy employees repeatedly come up with suggestions and ideas about crypto-assets in the executive team of many traditional institutions, as conveyed at any rate by anecdotal accounts of their experiences.

Figure 5: Age of Bitcoin Users



Source: Statista 2019, Incrementum AG

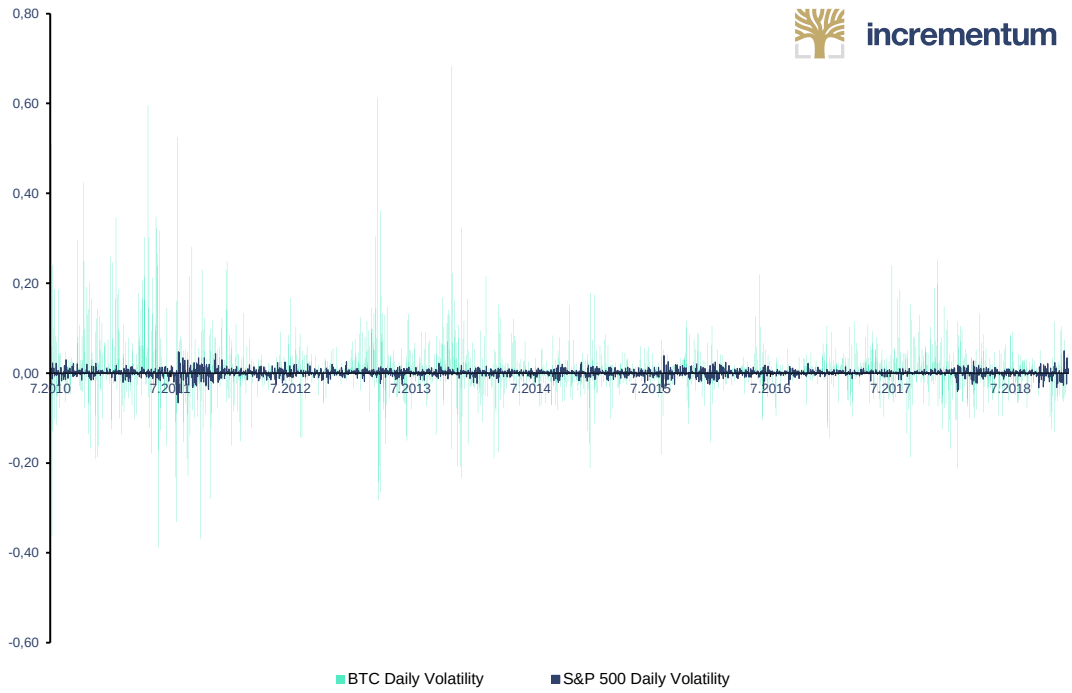
In addition, as everywhere, even among the asset managers the average level of knowledge is still quite low. It takes time for the executive levels of these organizations to allocate resources to educate their staff or set up their own departments that are committed to cryptocurrency. The number of banks and asset managers that are dealing with the issue on a project-related basis is growing. Some entities have recognized cryptocurrency and blockchain technology as a strategic business and openly admit to it. These include banks such as Bank Frick in Liechtenstein, Falcon Private Bank and SEBA Crypto AG in Switzerland, SolarisBank and Fidor Bank in Germany, but also Fidelity Investments in the US.

"Bitcoin is digital gold in the eyes of a growing subset of the population. To some extent this group already operates on a Bitcoin Standard: investments are evaluated on their ability to yield a return in Bitcoin."

Tuur Demester

One of the largest obstacles for institutional investors is the exorbitantly high volatility of most cryptocurrencies. Fluctuations in prices of up to twenty percent within just a few hours have been recurring in Bitcoin over the past few years, while other cryptocurrencies have shown even more excessive volatility. When US stocks dipped by just five percent in February 2018 Wall Street was already in turmoil. Handling such high price fluctuations is also difficult for institutional investors and poses some problems.

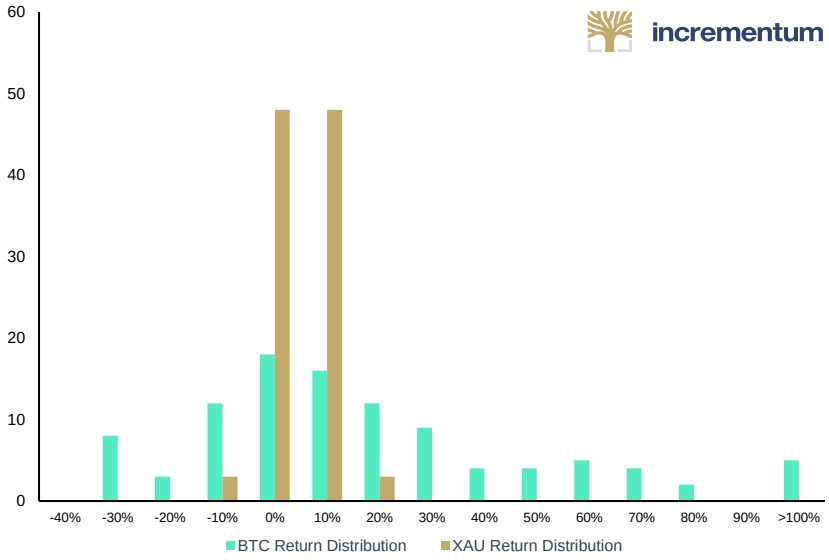
Figure 6: Daily Volatility BTC vs S&P 500



Source: Yahoo Finance, Incrementum AG

The volatility or risk weighting of a single position in the portfolio context can actually be easily managed by adjusting the portfolio weighting accordingly. A position with high volatility should correspondingly have less weight if one wants to control the influence on the overall portfolio. For risk-return reasons, right-skewed asset classes such as Bitcoin should be particularly attractive as an addition since a large impact can be achieved with a small positioning.

Figure 7: Monthly Return Distribution BTC vs XAU



Source: Yahoo Finance, Incrementum AG

From the point of view of the responsible portfolio manager, however, despite all this there is a weighty reason against even a small position in the crypto-sector: the

principal-agent dilemma.[42] If well-paid asset managers do not manage their own capital, they have an incentive not to take higher risks on a single position, even if from a capital theory perspective these are endowed with attractive risk-return ratios despite high volatility. The motto is: even with satellite positions one does not want to justify oneself as "agent" with the "principal" for high losses if they become striking.

Gold and Bitcoin – Stronger Together?

Market timing is difficult for any asset class. With such a volatile asset class as cryptocurrencies, one would like a favorable entry and exit time all the more. In practice, however, it can almost be ruled out that investors choose the ideal deadline to make their investments or to realize the gains.

Here we want to introduce our proprietary investment strategy, which defuses the volatility problem or even converts it to the benefit of the investor. In order to achieve this, our strategy draws on an old wisdom in portfolio management: Rebalancing. More on that later.

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

Tyler Winklevoss

We already discussed in last year's sister report, the *In Gold we Trust* report, that gold and Bitcoin cannot be seen as enemies but rather as complementary friends.[43] At a philosophical level, the investment assets are very similar because:

- Their stock cannot be inflated and devalued by a central bank
- They are nobody else's obligation (no counterparty risk)
- They are easily transferable
- They represent liquid assets outside the fiat system

In addition, both forms of investment are difficult to confiscate and have a good chance of succeeding in an environment of over-indebtedness, impending negative interest rates and financial repression. To a certain degree, this also applies to other "payment tokens" or "store of value tokens". This strategy can be implemented with gold and an index of store of value tokens instead of gold and bitcoin. This would ensure that potential competitors of Bitcoin are on the radar and in the investment strategy in the future. For the sake of simplicity, we will examine the combination of Bitcoin and gold below.

To a certain extent, this also applies to other "payment tokens" or "store of value tokens". This strategy can therefore be implemented with gold and bitcoin or **gold and an index of store of value tokens**. Including other "store of value tokens" would ensure that potential competitors of Bitcoin are on the radar and part of the investment strategy in the future. For the sake of simplicity, we will examine the combination of Bitcoin and gold below.

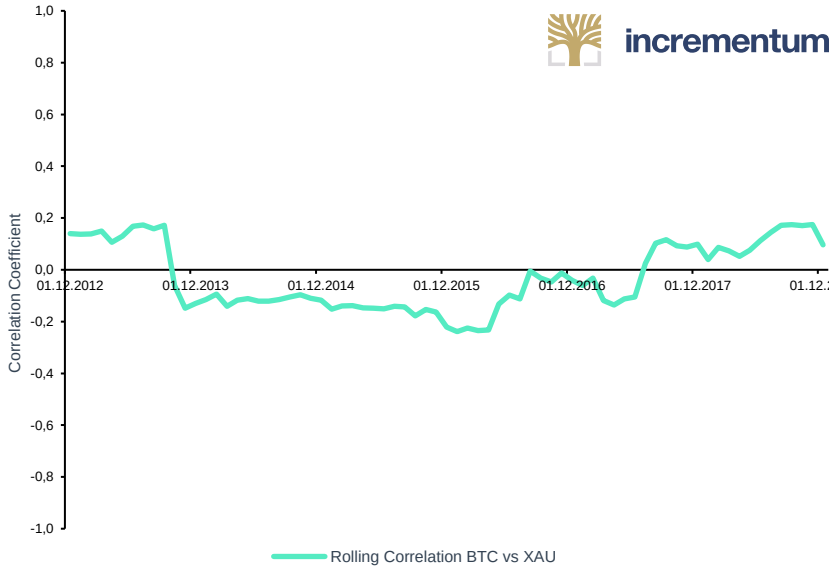
—

42 See https://en.wikipedia.org/wiki/Principal%E2%80%93agent_problem
43 See https://ingoldwetrust.report/download/1373/?lang=en, pages 177 following.

The Diversification Effect

Despite these similarities, the returns of gold and Bitcoin show low and sometimes negative correlation. This situation is welcome for an investor because the fluctuation of a combined strategy is reduced.

Figure 8: Rolling Correlation BTC vs XAU



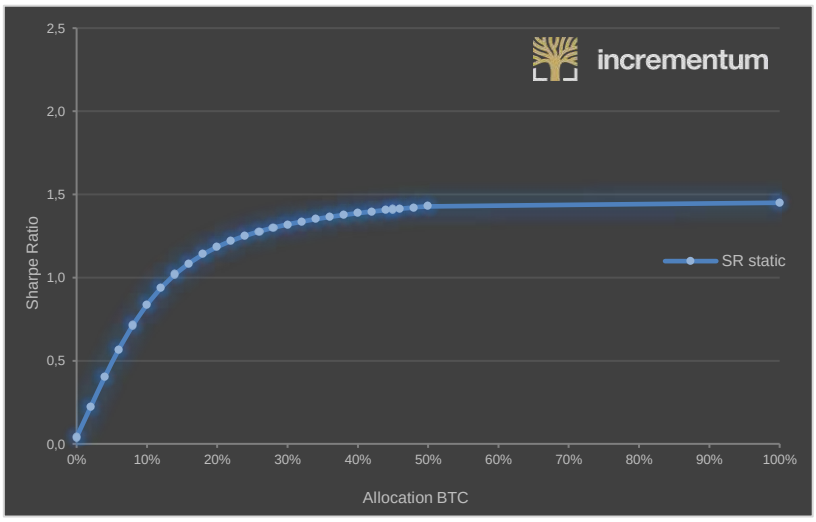
Source: Yahoo Finance, Incrementum AG

"Cryptoassets are the silver bullet of diversification."

Chris Burniske and Jack Tatar

Of course, the volatility and thus the price risk of a crypto strategy will change significantly if gold is added to the investment strategy. Since gold is subject to significantly lower price fluctuations, the overall volatility decreases as the share of gold increases. In addition, the low correlation due to the well-known diversification effect helps to reduce fluctuations disproportionately.

Figure 9: Sharpe Ratios of Various BTC-XAU Portfolios (Static Allocation)



Source: Yahoo Finance, Incrementum AG

The Rebalancing Bonus

In addition to exploiting the diversification characteristics of gold and Bitcoin, this investment strategy allows unlike any other to benefit from the "rebalancing bonus".

Source: Twitter

What exactly is the rebalancing bonus, and what is the best way to receive it? Price fluctuations cause portfolio components to change dynamically over time. Thanks to so-called "rebalancing", shifts in the portfolio are balanced out by resetting the portfolio to the original, strategic asset allocation.

In order to benefit from the rebalancing bonus, a strategic allocation and a rebalancing method must be defined for both assets. For example, an institutional investor may choose to assign 30% to Bitcoin and 70% to gold as a strategic allocation, as this mix creates an overall risk that is familiar to professional investors.

As a rebalancing method, one can either set a fixed time interval or make adjustments only on an ad hoc basis when predefined portfolio shifts are reached (see info box). Our comprehensive quantitative analysis has shown that event-based rebalancing is more useful, especially considering transaction costs. In the strategy presented here, we have provided a wide range of Bitcoin allocations between 15% and 60%. The method therefore calls for the strategic allocation (or the initial allocation) to be restored through corresponding buy and sell transactions as soon as the Bitcoin allocation falls below 15% of the total portfolio or exceeds 60% due to price fluctuations. In case Bitcoin develops better than gold, it has to be sold and replaced by gold and vice versa.

Various studies confirm that the more the asset classes fluctuate in value and the lower their correlation, the stronger the rebalancing bonus.[44][45] This circumstance must be taken into account against the background of the high price fluctuations in Bitcoin.

In a comprehensive quantitative analysis, we tested this investment strategy in several variants. As the graph below shows, rule-based rebalancing can significantly improve the risk-return ratio. Correspondingly, the Sharpe Ratio could be consistently improved with the help of the rebalancing strategy, irrespective of the Bitcoin allocation.[46]

Different Rebalancing Methods

Rebalancing means restoring portfolio weights to an original allocation. In principle, there are two versions of rule-based rebalancing:

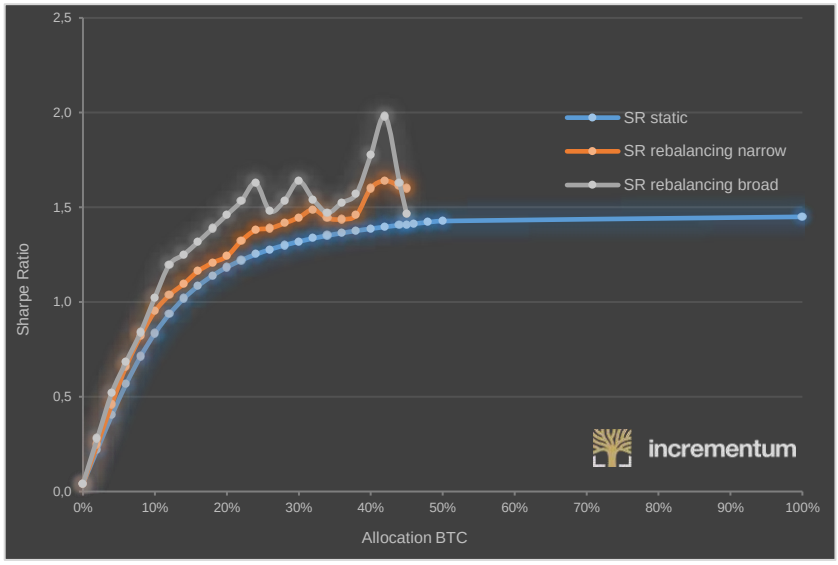
One possibility is to define a period with fixed time intervals, in which rebalancing is performed each time a time window closes. For example, the rule might require rebalancing at the end of each month or quarter.

Another method is event based, i.e. one has to determine portfolio weights, at which the rebalancing is triggered. In case of an overweight the outperforming asset will be sold and the underperforming asset will be purchased and vice versa.

—

44 See "When Does Portfolio Rebalancing Improve Returns?", HodlBot, October 26, 2018
45 See "THE REBALANCING BONUS", www.efficientfrontier.com
46 Obviously past performance is no guarantee for future returns.

Figure 10: Sharpe Ratios of Various BTC-XAU Portfolios (Static Allocation & Portfolio with Rebalancing)



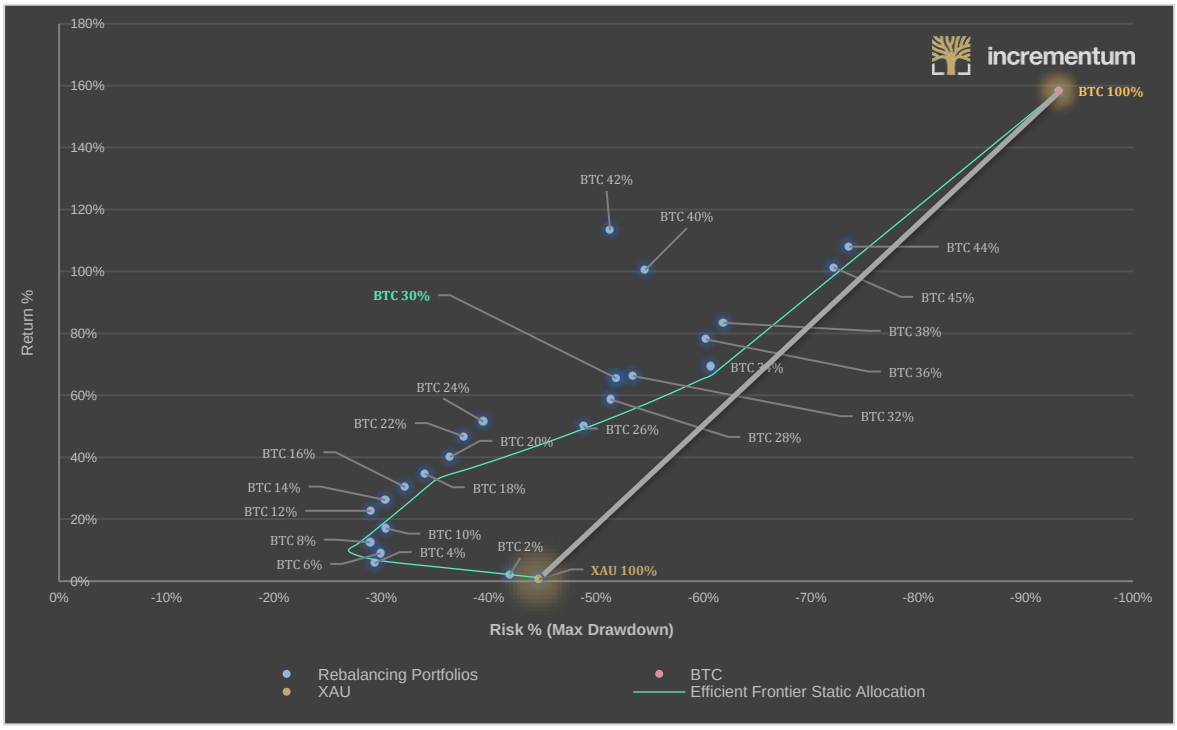
Source: Yahoo Finance, Incrementum AG

"You can't stop things like Bitcoin. It's like trying to stop gunpowder."

John McAfee

The fact that the risk-return ratio can be significantly improved with this strategy becomes particularly evident when considering the maximum drawdown as a risk indicator.

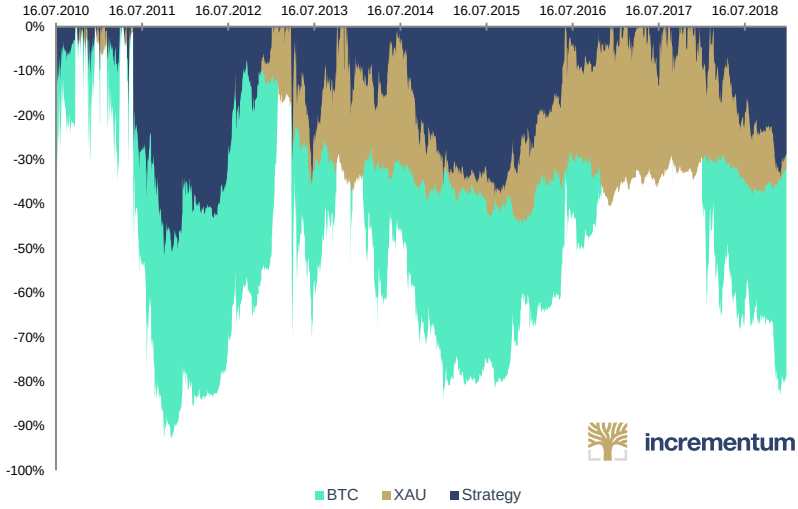
Figure 11: Max Drawdown Return Tradeoff Strategy



Source: Yahoo Finance, Incrementum AG

A drawdown in financial literature refers to the price loss that lies between a high and a subsequent low in a given period. The maximum drawdown is the total loss that an investor has to accept for a period after investing at the time of peak.

Figure 12: Max Drawdown



Source: Yahoo Finance, Incrementum AG

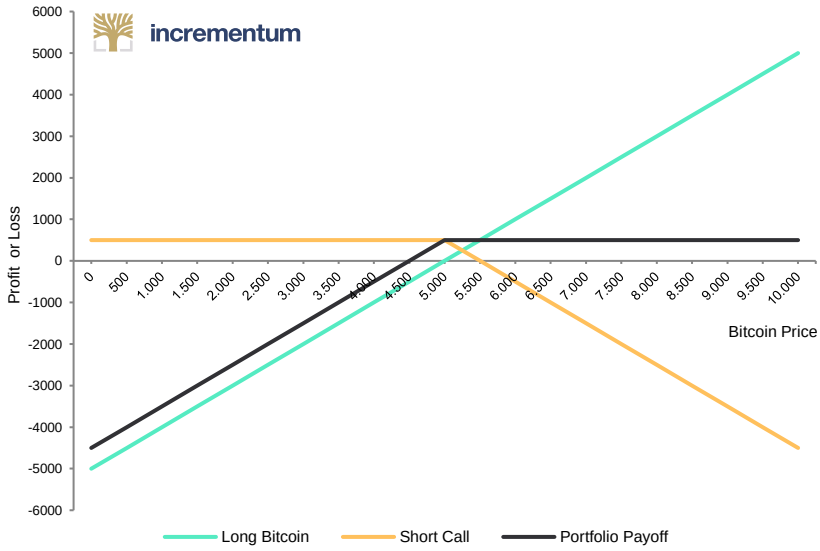
Additional Income through "Covered Call Writing" and "Put Writing"

"The existing banking system extracts enormous value from society and it is parasitic in nature."

Andreas Antonopoulos

In addition to the **diversification effect** and the **rebalancing bonus**, a third element allows the investor to profit from high volatilities and thereby further improve the strategy. To achieve this, one uses the options market, which already exists for Bitcoin. On exchanges such as Ledger X or deribit one can trade options for over a year. Options can be used as a speculative element, for hedging or generating yield. The decisive factor is whether you write options without holding the underlying ("naked") or in combination with the underlying.

Figure 13: Covered Call Writing



Source: Incrementum AG

Covered call writing is a well-known strategy that can be used to exchange the upside potential of a position (or part of a position) for a premium. If you have a position in the portfolio that you want to hold or even sell, you can write a call option on it and thus generate the option premium. In the worst case, you no longer benefit from the full upside of the underlying, but at least you still generate the premium.

"Bitcoin is the currency of resistance."

Max Keiser

Conversely, selling puts is a good way to build a position. In this case, a contract obliges you to buy an underlying at a certain point in time at a given price. In this case, you also receive the option premium for it. If you execute, you will receive a net purchase price (taking into account the generated option premium) that is more favorable than the one that you would have been able to obtain by purchasing the underlying in the normal way. If the option is not exercised due to the price movement, then you will collect the entire option premium and the contract expires. The risk of this strategy is that the option will not be exercised and the price later explodes.

Figure 14: Naked Put Writing

Source: Incrementum AG

"By holding dollars you are ultimately trusting politicians. By holding Bitcoin you are ultimately trusting open source code. Trust in politicians tends to fall over time. Trust in open source code tends to rise over time. And so, with time, which system likely advances?"

Erik Voorhees

The prices of the option premiums are based on the expected fluctuations of the underlying and the volatilities implied in the option prices. As the price of Bitcoin has an exorbitantly high volatility, the option premiums are correspondingly high. According to our calculations, assigning a 10% share of the portfolio to at-the-money options would produce an annualized additional return of 10 to 15%.

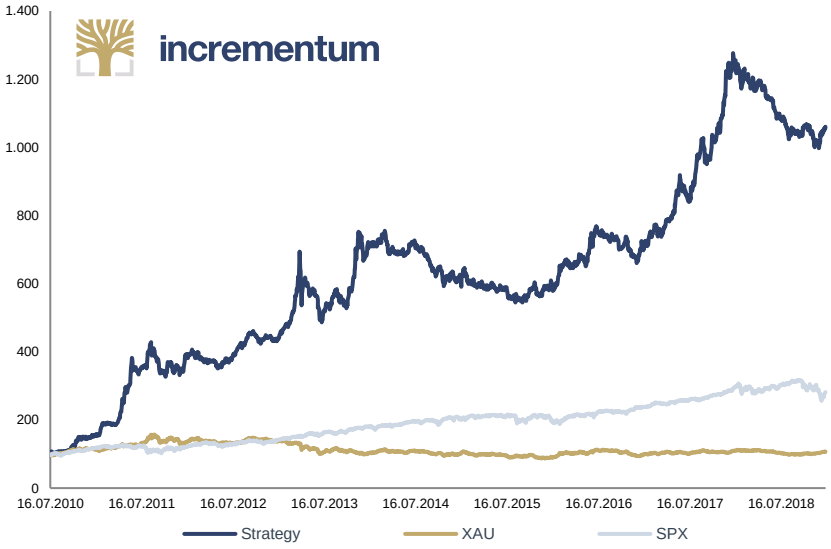
"As a portfolio manager, when do you start advising to your clients that they have some cryptocurrency exposure? When will there be an index, a mutual fund of cryptocurrencies? It will happen."

Melanie Swan

Conclusion

Bitcoin and gold are similar in certain characteristics and can be an attractive investment strategy as a portfolio. By combining both assets, investors benefit on the one hand from the low correlation of both assets. On the other hand, they can use the volatility of Bitcoin to their advantage through a rule-based rebalancing and thus reap the rebalancing bonus. In addition, option strategies generate an interesting return by collecting option premiums. Overall, this approach allows for a strategy that, in view of its volatility, seems to be better suited for institutional investors than highly volatile pure crypto strategies.

Figure 15: Rebalancing Strategy in comparison with XAU and SPX



Source: Yahoo Finance, Incrementum AG

Assumptions underlying the calculation:
3% total expense ratio (including trading costs).
Historical performance is no guarantee of future earnings and performance.

Technical Analysis: Spring Awakening?

"Technical analysis is not the holy grail but the best approach to grasp the hypercomplex markets at a glance."

Florian Grummes

Key Takeaways

- **Technically, Bitcoin and thus the entire crypto sector was definitely in a bear market until the end of March 2019. Since the sharp outbreak of over $4,150 and the rise to $5,330, however, the situation is no longer quite so clear.**
- **At the moment, the Fear & Greed Index is increasingly providing warning signals and indicates that market participants are too optimistic or greedy. At any rate, the ideal time to buy based on sentiment analysis is now clearly behind us.**
- **As long as Bitcoin cannot regain the psychological $6,000 mark, any price recovery remains only a bear market rally below the decisive resistance zone.**

Photo: Florian Grummes

Florian Grummes

We want to sincerely thank Florian Grummes for contributing this chapter. Florian is the founder and CEO of Midas Touch Consulting (www.midastouch-consulting.com). Our readers can sign up for his updates and free newsletter with this link: http://bit.ly/1EUdt2K

Winter has had a firm grip on the crypto sector for over a year. However, we were able to see who was swimming naked when the tide went out. The last two months saw a bottoming out and respectable recovery. The price has already increased $2,200 from the low of $3,125. This is an increase of almost 70%. This recovery may merely be a temporary thaw. However, it could also be the beginning of spring.

Review

"Technical analysis works precisely because people look at it. And if people care, I care."

John Bollinger

Last year, in the March 2018 edition of the *Crypto Research Report*, we suggested a further correction could occur and warned about a potential crypto winter, when Bitcoin was still trading at over 11,500 US dollars.[47] Since then, prices have ultimately only gone further south despite sharp and profitable counter-movements. With the failure of the round psychological mark of $10,000 at the end of April 2018, a series of even lower highs could no longer be stopped. Nevertheless, Bitcoin prices were able to remain above $6,000 during the summer. It was not until autumn that this extremely important support became fragile.

Figure 16: The Big Four Bitcoin Bubbles

Source: Midas Touch

"We believe Bitcoin is in the last stage of this bear market: the accumulation phase. The current sentiment has recovered from capitulation and the blockchain shows us that Bitcoin HODLers are committing for the long term again."

Tuur Demeester and Michiel Lescrauwaet

Technically speaking, Bitcoin has had a descending triangle/ bearish wedge[48] during the first 10.5 months of 2018. After bouncing off the support zone around $6,000 six times and at the same time establishing a series of lower highs, it was just a question of time before the support around $6,000 would break. Breaking such a strong support makes any market crash. A similar formation in the gold-market occurred in 2013, when gold was priced around $1,520. The same is true in an uptrend as well. The more often a market runs against a resistance zone the less strong the resistance line becomes. This is similar to Bitcoin's resistance around $1.000-$1.200. It took a few attempts before Bitcoin finally broke through that number to the upside. After that, the massive rally in 2017 really started to gain steam.

—

47 Technical Analysis: Is a Crypto Winter About to Start? Grummes (2018). *Crypto Research Report*, pg. 51
48 See "Descending Triangle", www.stockcharts.com

Further falling prices were also suggested by us in the October edition of the *Crypto Research Report*.[49] Consequently, after the $6,000 support was broken, Bitcoin's price halved again. **However, a non-laughable recovery of 70% has been observed since mid-December when Bitcoin hit its low of $3,125. Meanwhile, Bitcoin is trading around $5,000, and has completed its first bottom formation.** However, Bitcoin will experience numerous resistances levels going forward!

Figure 17: Support at USD 6000 turned to Resistance?

Source: Midas Touch

"I never use valuation to time the market. I use liquidity considerations and technical analysis for timing. Valuation only tells me how far the market can go once a catalyst enters the picture to change the market direction. The catalyst is liquidity, and hopefully my technical analysis will pick it up."

Stanley Druckenmiller

Parallel to the bleak price development of Bitcoin, most Altcoins had lost between 80% and 100% of their peaks. Many projects have now been buried. Fraud, mismanagement, and lack of a good business model were widespread. Rightly so, utility coins garnered a shady reputation for the entire blockchain industry.

However, we are still convinced that the public blockchain technology has fundamental value as a non-confiscatable asset for wealth preservations. Highly motivated and specialized tech teams worldwide are still working in the background on the further development of numerous blockchain and crypto projects such as Blockstream's Liquid, the Lightning Network, and Plasma. Therefore, the epic popping of the 2017 bubble could actually offer an enormous opportunity. Generally, small investors lack knowledge and discipline, and trade and invest very emotionally. They usually don't have deep pockets and give up at the lows and buy at tops. Smart money, which is not necessarily institutional money, does the opposite: buying when prices are low and nobody is interested, while selling once everybody wants to buy. Strong hands have a plan and are patient. Right now, crypto markets are quiet, and investors can slowly accumulate during this depressed environment. To handle the volatility of the cryptocurrency market, a radically countercyclical approach is needed.

—

49 The Network Effect As a Valuation Methodology. Hays and Zapke (2018). *Crypto Research Report*, pg. 42

Is Bitcoin Dead?

Of course Bitcoin isn't dead. Even though the first crypto currency has only existed for a decade, the Bitcoin has been declared dead countless times. During this period, however, the value of a Bitcoin rose from 0.003 US dollars to almost 20,000 US dollars in the meantime. Basically an incredible success story! And even at current exchange rates of around 5,000 US dollars, you still have to pay almost four times as much for a Bitcoin as for an ounce of gold.

"The market is now clearly rejecting hard forks of Bitcoin. Next we will see competing soft forks followed by their rejection. Only thereafter will Bitcoin ossify and become the ultimate store of value for the world."

Tamás Blummer

The collapse of the crypto sector is weeding out the bad business models. A similar situation occurred after the bursting of the dotcom bubble at the beginning of 2000/2001. **More than 75% of the tech companies founded during the Internet boom in the late 1990s went bankrupt.** But some of the biggest and most powerful companies of all time emerged from the ashes: Amazon, Google and eBay, for example, not only survived the crash, but are now an integral part of our everyday lives. The share prices of these companies have increased more than a hundredfold in the last 15 years. The same can be expected for the cryptocurrency market over the next ten year.

Of course, the market capitalization of the entire sector, currently around $160 billion, is negligibly low compared to other sectors and is far removed from the almost $850 billion in January 2018. The daily trading volume, at just under $30 to 40 billion, is also 60% below its highs of December 2017. Many small investors either sold their crypto investments at high losses or are blindly holding onto their underwater positions. At any rate, speculative money has left the sector at the moment. This lack of speculative money can also be observed by the decline in blockchain conference participants throughout Switzerland. Conference organizers have to give free tickets away in order to fill the hall.

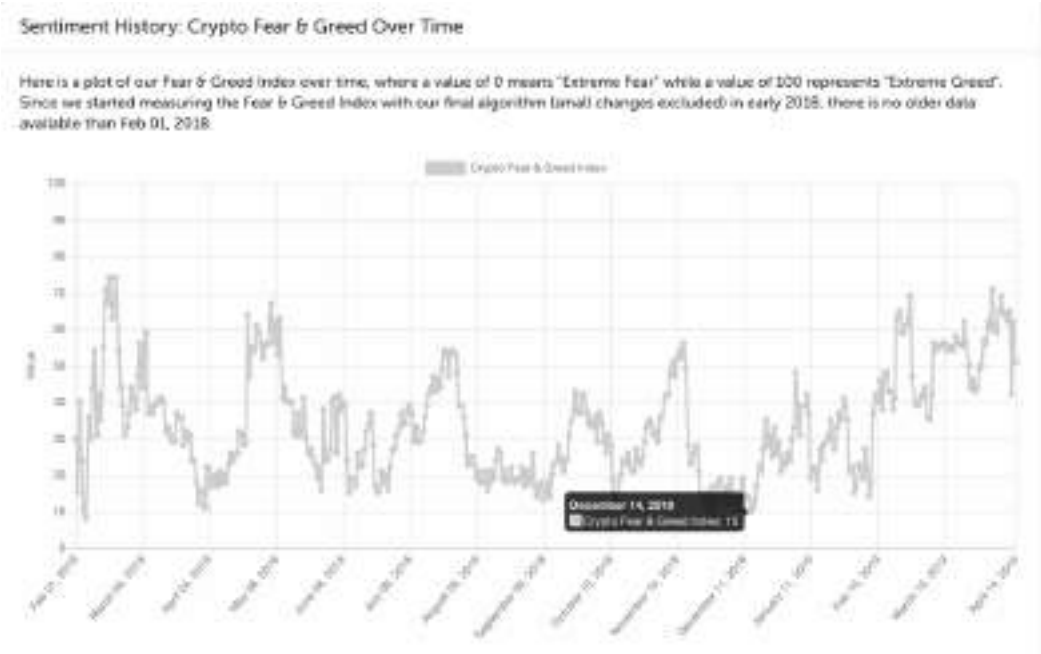
Market Sentiment in the Short and Medium Terms

"Bitcoin is going to change the world from a money transactional standpoint not just for Africa, but for everywhere."

Akon
Recording Artist and Producer

The mood in the crypto sector reached an absolute low in mid-December. One tool for determining the exact trend reversal point is the Fear & Greed Index. **The index reached a low of 10 in mid-December**, which lasted several months. As in all asset classes, returns are based on the individual behavior of countless market participants. The vast majority of buying and selling decisions are made very emotionally. Medium-term turning points often observe extreme fear or blind greed. Mass psychology is an underlying factor drives prices in any market. At market tops like the one in December 2017/January 2018, everybody is bullish and invested. Exactly at this stage you can observe blind greed. At bottoms the contrary is true, everybody is afraid, depressed and has lost his beliefs plus sold his positions in blind panic.

Figure 18: Sentiment History



Source: alternative.me

"Blockchain technology has such a wide range of transformational use cases, from recreating the plumbing of Wall Street to creating financial sovereignty in the farthest regions of the world."

Perianne Boring

Generally, sentiment analysis makes the following assumptions: extreme fear can be a sign that investors are worried. That could be a buying opportunity. When investors are getting too greedy, that means the market is due for a correction. The Fear & Greed Index consists of five different data sources and is calculated automatically on a daily basis. Values of 0 mean extreme fear, while the maximum value of 100 stands for extreme greed and exuberant optimism. The index is comprised of several variables. Bitcoin volatility makes up 25% of the index. **An unusually high volatility is a sign of an anxious market, similar to the stock market.** The market momentum or trading volume contributes a further 25% to the index calculation. Market sentiment on social media including keywords on Twitter, are weighted 15% in the calculation. Weekly surveys among crypto investors and the Bitcoin dominance compared to the more speculative Altcoins make up 15% and 10% of the index respectively. The index is rounded off with various Bitcoin search queries (Google Trends data), which provide the last 10% for index calculation. An example of this is the query "Bitcoin price manipulation", which is clearly a sign of increased fear in the market.

Figure 19: Fear & Greed Index Then (2018) and Now (2019)

Source: alternative.me

"The cryptocurrency community hasn't decided whether they want to be anarchist rebels or to replace the establishment."

Adi Shamir

At the moment, the Fear & Greed Index reads high optimism values, which could be a cause for concern. According to market sentiment analysis using the Fear and Greed index, the ideal time to buy based on sentiment analysis is already behind us. It should also be noted that an extreme euphoria can rarely be observed in a bear market. Should it arise, it must be interpreted as a good sell signal. If a market is in a bear-market, which we are, then any rally/recovery will create too much optimism, which cannot be fully supported while the overall trend is still down. The most extreme number for this sentiment index was around 75, therefore, 51 is not extreme optimism but rather this is moderately too optimistic.

Figure 20: Bitcoin Optix

Source: Bitcoin Optix

The Bitcoin Optimism Index (Optix) published by Sentimenttrader currently comes to a similar conclusion. Sentimentrader.com do not share their formulas; however, each measure is ranked against its historical norms to determine whether or not the current level is at an extreme. The Optix can go from 0 (maximum pessimism) to

100 (maximum optimism), though it generally stays above 20 and below 80. As with most contrary indicators, when sentiment gets extremely pessimistic, below 30, we would become alert to a possible reversal to the upside as expectations improve from very low levels. When sentiment is very high, above 70, then we would become concerned about a correction as expectations may have gotten too optimistic.

"Bitcoin, and the ideas behind it, will be a disruptor to the traditional notions of currency. In the end, currency will be better for it."

Edmund C. Moy

For bitcoin, the Optimism Index has worked best when using a moving average, such as 10 days. "There is currently a neutral optimism indicator. The psychological low of the last mass panic was measured on December 14, 2018. The calculation is based on future volatility expectations, the average discount of an unspecified Bitcoin fund against its net asset value and general price behavior. **Overall, the sentiment analysis recommends a wait-and-see approach in the short term.**

Technical Analysis: Possible Price Targets and Accumulation Zone

Technically, Bitcoin and thus the entire crypto sector was definitely in a bear market until the end of March 2019. Since the sharp outbreak of over $4,150 and the rise to $5,330, however, the situation is no longer quite so clear. On the one hand, the downward trend line of the last sixteen months was clearly broken and since the low of December, the share price has already risen by over 70%. **On the other hand, the price continues to move clearly below the former support zone by $6,000 - 6,200**, while the stochastic oscillator on the weekly and daily charts is completely overbought. As long as the Bitcoin cannot regain the psychological level of $6,000, any price recovery remains only a bear market rally below the decisive resistance zone.

Figure 21: Bitcoin Daily Chart

Source: Midas Touch, Trading View

At the end of March, the Bitcoin was able to free itself from its three-and-a-half months of soil formation on the daily chart. The rise above 4,150 US dollars resulted in massive short covers, which drove prices up almost vertically. The price target from the ascending triangle was in principle worked off at 5,330 US dollars.

As a further rising triangle is emerging in the very short term, the Bitcoin exchange rates could also rise to 5,700 - 5,800 US dollars in the coming days and weeks. However, the resistance around 6,000 US dollars is extremely strong and should by no means be underestimated.

Of course, the newly established series of higher lows is positive. The strongly overbought Stochastic Oscillator, on the other hand, is negative. In any case, the air is now getting thinner and thinner with every further rise.

The imminent setback should lead at least to the still falling 200-day line (4,575 US dollars). It is also possible that only the rising 50th day line will catch the reset. In any case, the constellation of the two moving averages indicates that there is still some need for consolidation overall.

The large picture therefore still lacks a clear trend reversal. In the months to come, an irritating sideways phase is more likely to be planned. Similar to the closing of the last bear market in late summer 2015, a final slip of less than 3,000 US dollars might even be 1,500 US dollars. Only then would the sector be ready for a new bull market. 2019 should therefore be a year of transition.

Figure 22: Bitcoin Weekly Chart

Source: Midas Touch, TradingView

However, as soon as the Bitcoin manages a weekly closing price above 6,200 US dollars, all bearish doubts will be dispelled. Then we have to assume that the correction has already reached its final low in December and that the Bitcon is already in a new upward wave. In this case we have to buy every backstop (Buy The Dip).

Crypto Concepts: Cryptocurrency Mining in Theory and Practice

"The purpose of mining is not the creation of new bitcoin. That's the incentive system. Mining is the mechanism by which bitcoin's security is decentralized."

Andreas M. Antonopoulos

Key Takeaways

- **Cryptocurrency Mining can be seen as global arbitrage on electricity prices. Mining firms can strike lucrative deals with energy providers in Switzerland, the U.S., and Scandinavia. To stabilize the capacity of networks, some energy providers are actually willing to pay miners to use electricity during off-peak hours of the day.**

- **All three of the mining companies interviewed use 100% renewable energy for mining cryptocurrencies. Alpine Tech SA and Blockbase DWC-LLC have minimum investment amounts that are bar most retail investors. Unity Investment AG has a minimum investment of $100.**

- **Before investing in a mining company, due diligence includes checking whether the mining pool software is secure with no backdoors and that the pool is actually capable of delivering the reward for allocating your computation resources to their pool. With cloud mining services, due diligence includes verifying that the data center exists, that the computer or computers that you are renting exist, and are solely dedicated to your exclusive use, and that their software is secure with no trap doors.**

Introduction to Cryptocurrency Mining

As discussed in the chapter on consensus mechanisms in the June edition of the *Crypto Research Report,* decentralized networks need a strategy or algorithm for stopping double spends of digital information. Normally, people state that the two main consensus mechanisms employed by cryptocurrencies are proof of work and proof of stake; **however, this is wrong.**

Source: Twitter

Recently pointed out to us by Ed Thompson of Web3 in Zug, Proof of Work is not Bitcoin's consensus mechanism per say. Agreement on the latest state of Bitcoin's transaction history is based on the longest chain policy. Despite that subtle difference, mining is one of the most important aspects of Bitcoin as well as many other blockchains, because mining serves the purpose of creating a new block in a blockchain. A block is very similar to a page in a financial ledger that documents the order of any debits and credits to its accounts, along with a third entry performed by an auditor, a miner, that commits these debits and credits to each address account. **This is known as triple entry accounting, a significant innovation in accounting.** Therefore, the entire blockchain (a chain of blocks), is like all the pages of a financial ledger.

In Bitcoin, a new block is created approximately every 10 minutes. This block contains the most recent set of transactions among Bitcoin addresses, that have been verified among the network of computers. The act of mining is performed by computers configured for mining. In Bitcoin, these miners perform a computation that is known as a Proof of Work function. This Proof of Work function is computationally difficult and requires many attempts by the computers in the network to discover the solution. The computers in the network compete to find the solution to this Proof of Work before the others. The computer that finds the solution before the others is rewarded with a reward of coins from the blockchain. This is how new coins are created and enter the ecosystem.

Mining Business Costs and Risks

With that said, there are real-world costs associated with running a computer that performs these computations. These costs are in the form of depreciating hardware assets, electric bills, maintenance costs, labor, as well as many other costs. When the price of the cryptocurrency goes up, these costs can be manageable for sophisticated miners. When the price of a cryptocurrency goes down or flatlines, or if a serious mismanagement of expenses has been overlooked, **there is risk in spending more in electricity and hardware than the amount you earn**

from the rewards of mining. Mining is a very risky business unless you have an enormous number of mines and can out compete others because of cost savings stemming from economies of scale. **Even then, many miners suggest that buying cryptocurrency is more profitable and less risky than mining for cryptocurrency.** The advantage to mining and earning a reward is that you know where the coins came from because they are being issued directly from the Blockchain itself. When you buy the coins, you might not know where the coins have been along their path before they got to you.

Source: Twitter

Bitcoin Block Reward Emission Schedule

Proof of work uses two main types of financial rewards to incentivize users to maintain the network: **rewards and transaction fees**. 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.[50] This number becomes that block's identification number, which is used as an input in the next block's hash puzzle. 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. However, this rate drops roughly every four years and is currently 12.5 Bitcoins.

"But bitcoin mining is like a sports competition: there is only one trophy to be handed out, and even if more people compete, more trophies aren't made; winning the trophy just becomes harder. This effectively ensures that the cost invested in producing a bitcoin is roughly equal to the value of a bitcoin, which is what ensures bitcoin is hard money."

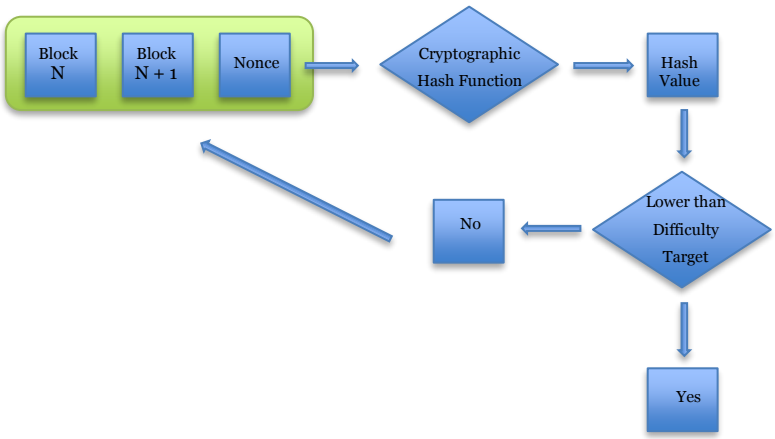
Saifedean Ammous

There are other variables that must be taken into account to determine the true emission schedule, for example, the number of computers and their total computation capacity. This determines how quickly a block is discovered but that rate is estimated to be every 10 minutes. The network self-adjusts the block creation rate every 2016 blocks in order to account for increases or decreases in the amount of computation capacity among the entire network of computers competing to mine the next block.

—

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

Figure 23: Proof of Work Computation



Source: Incrementum AG

Updating the Network

In Bitcoin, mining is how all new coins are created. Once the solution to the Proof of Work function is discovered, the computer that found that solution broadcasts their discovery to the network of miners. Once this broadcast is received, the other miners are tasked with crosschecking that solution for verification purposes. Once there has been enough verifications by other miners in the network, a transaction is said to be verified and becomes a permanent record within a block stored in the blockchain.

Security Layers and Known Attack Vectors

"Various estimates put the range of energy consumption between 1 and 10 GW. Translated over a year, this would be around 8.76 TWh/year to 87.6 TWh/year, or between 0.005% or 0.05% of total global energy consumption.

In other words… Bitcoin currently consumes as much as an average 350,000 to 3.5 million individual humans consume per year."

Saifedean Ammous

Another purpose of a miner is to act as a security layer for the network. There are many known attack vectors for Blockchain and other cryptocurrencies. In Bitcoin's case, the 51% Attack is where an attacker or group of colluders gain control of 51% or more of the computation power performing the Proof of Work function. With this much computation power, an attacker could potentially begin unraveling the transactions that have been previously verified within a block. However, the attacker must start by attacking or unraveling the most recent block. Once the most recent block has been successfully attacked, each subsequent block which came before, would need to be attacked, and this attack only gets harder and more expensive for the attacker as they attack more and more blocks in the blockchain's history.

Different Ways to Mine

In the early days of Bitcoin, miners would use regular computers, such as a laptop or desktop, and the calculations would be performed using code processed by the central processing units (CPUs) of that computer. When more sophisticated participants started mining, they saw opportunities to improve on how fast they could perform calculations by looking at solvers other than CPUs. This led miners to perform those same Proof of Work calculations using the graphical processing units (GPUs) of their computers. GPU's are typically capable of performing this Proof of Work calculation orders of magnitude faster as well as being capable of

performing multiple calculations simultaneously far beyond a CPUs capability. This eventually led to even more sophisticated technologists entering the space, and miners began using field programmable gate arrays (FPGAs) which are devices that are even faster than GPU's. Finally, the market evolved into using application specific integrated circuits (ASICs) which are chips designed for the sole purpose of performing a single calculation, and in Bitcoin's case, the Bitcoin Proof of Work function.

Mining Pools

"Anybody with familiarity with the mining business knows that over the last few months, only the mining businesses operating with the lowest electricity costs have managed to maintain profitability. Miners who invested in infrastructure connected to grids with prices above 10c/kWh, likely stopped being profitable months ago. At this point it is not clear whether even miners at 5c/kWh are profitable at current prices and difficulties.

This became evident as the difficulty started to fall in October, meaning that many miners were shutting down their miners, which signified not only that the miner is not profitable, but that it cannot even cover its operating expense."

Saifedean Ammous

The cryptocurrency mining industry started with hobbyists who thought mining Bitcoin was a novelty, as no one really knew what the future would hold for Bitcoin. From there, as the block rewards got harder and harder to earn, and hobbyists had a more difficult time earning a reward, we saw the introduction of a concept known as mining pools. **A mining pool is where individual miners could contribute their resources to a pool of miners and if one of the pool members achieves the reward, that reward gets split amongst the members of the mining pool.** As the stakes increased, we saw the market evolve yet again, where computer manufacturers, graphics card manufacturers, FPGA manufacturers, and ASIC Manufacturers, entered the space by building specialty products for performing cryptocurrency mining. We even saw cloud mining companies develop. Rather than building or buying your own cryptocurrency mining machine, or joining a cryptocurrency mining pool, one could just rent computing power from a company that purchases and maintains the mining machines on behalf of their customers.

Three Interviewed Mining Companies

To bring the theory of mining into practice, we interviewed three cloud mining companies, Alpine Mining SA, Unity Investment AG, and Blockbase Group DWC-LLC. With that said, we rely on the companies and people that we interview to give us the facts from their perspectives. As writers of the *Crypto Research Report*, we must let our readers know that we began this article naively. We held the erroneous notion that not all mining companies were bad actors, and that every company was doing the best they could. **Unfortunately, we uncovered very suspicious and concerning information regarding two out of the three mining companies interviewed.** We are still presenting this article to you for your information; however, we want to clearly state that we do not endorse these companies, and we hope that each investor does an **extremely thorough** investigation if they are considering investing in mining companies.

Investigating cloud mining companies to invest in requires proper due diligence, which involves many factors and is not easy to perform or get right. If you lack the sophistication for performing due diligence, seek out those who are capable as well as trustworthy to perform the due diligence for you. Or choose a company that performs this due diligence in a public fashion using cryptocurrency industry best practices. This might include **inspections of computer manufacturers to see their manufacturing processes, inspections of cloud mining facilities,**

inspections of any software code, database accounting to ensure the number of users matches up with the number of machines available, performing financial audits of the company bank accounts, verifying the reserves of the company's cryptocurrency holdings, among many other things. Due diligence is not something to be taken lightly when evaluating making an investment. If you are considering an investment, never risk more than what you're willing to lose. Now let's move onto the first interview.

Source: Alpine Tech SA

Alpine Mining Tech SA

Introduction

Another company we interviewed was Alpine Mining SA.[51] We spoke with Ludovic Thomas[52], who is CEO and cofounder of Alpine Mining. In the interview, we discussed how Alpine Mining came to be, what services they offer, and how they fit into the cryptocurrency market. According to Thomas, Alpine Mining is dedicated to their activities and is a team of young, ambitious people, and they strive to have the utmost in ethics and desire to maintain a solid reputation. Thomas and his business partner Christophe Lillo[53], who is CTO and cofounder at Alpine Mining, bootstrapped the company with their own capital and efforts. They started mining cryptocurrency for themselves and have been mining Ethereum since it was $0.30. They started their first cryptocurrency mining data center at a location in Gondo[54], Switzerland. Gondo is a very small municipality on the Swiss Italian border with only 40 residents. For years, the municipality of Gondo, was trying to attract companies to the area by offering extremely low electricity costs but this small municipality was unable to attract people to the area. Thomas mentioned that this municipality offered the lowest electricity prices in all of Switzerland and that's what made them decide to set up their first data center in Gondo. **They were able to power their cryptocurrency mining data center using the hydroelectricity produced from the local river in Gondo.**

"This is why Bitcoin mining will only be profitable at prices lower than the average global electricity rates. These rates would be expected to converge more and more over the coming future thanks to Bitcoin putting a bid under their prices, and thanks to Bitcoin investment in cheap energy allowing the accumulation of capital and the reduction in the cost of energy production."

Saifedean Ammous

They soon realized that they would be unable to scale their operation further because the municipality only had one transformer and there was a limited amount of land for them to expand to. According to Thomas, the transformer provided a total of 1.2 megawatts and half of that was being used by the municipality.

When they first started out mining cryptocurrency, they focused their efforts on coins that were mineable with GPU's. According to Thomas, Lillo used his technical skills to figure out how to optimize the GPU's to perform above and beyond their default configuration. **This is referred to as "overclocking".** They started out mining for themselves, but eventually opened up their mining operation to others, mainly Swiss customers. Because they chose Gondo as the

—

51 See https://alpinemining.ch/en/
52 See https://ch.linkedin.com/in/thomasludovic1991
53 See https://www.linkedin.com/in/christophe-lillo-a0a90711a/
54 See "Cryptocurrency mining to restore Alpine village's goldrush fever", swissinfo.ch, January 10, 2018

location for their first data center, they received a lot of exposure in the news and ended up going viral within the French part of Switzerland.

What Services Alpine Mining Offers

2018 was a difficult year for many companies in the mining space. Many companies ended up shutting their doors and declaring bankruptcy. Luckily, for Alpine Mining, Thomas says they avoided such a tragic outcome with their business flexibility. In 2018, they transitioned into being a service provider offering to build cryptocurrency mining data centers for other companies. They signed their first contract with a Hong Kong based company called Diginex and were tasked with building out a first data center in Sweden for Diginex.

Photo: Demelza Hays, Gondo Switzerland Dec. 2017

According to a press release[55] found on the Alpine Mining website dated May 2018 this partnership was projected to cost around $30 million.

Alpine Mining was tasked with sourcing all the hardware, finding the right locations for the data center, to build out the location for the customer, and to manage the location for the customer. In addition, they needed to assemble all the mining systems, set up and configure the data center with the appropriate monetary tools, and software to increase network efficiency. This marked the beginning of their cryptocurrency mining data center development as service. According to Thomas, they are also extremely focused on hiring skillful people as they continue to develop their company. Thomas stated that at one point, **they were managing 40,000 graphics cards mining various cryptocurrency's such as Ethereum and Monero.**

Conclusion

Alpine Mining is currently going through a transition phase and will most likely be renamed Alpine Tech. Thomas stated that they are still mining cryptocurrencies, but they are now working on creating blockchain solutions for other companies. Thomas mentioned that they will soon be working in collaboration with the university where many of their team members have graduated from. According to Thomas, that project is focused on Blockchain Artificial Intelligence, but the project is currently in stealth mode and Alpine Mining is not publicly announcing details about that project at this time. If you or

—

55 See https://alpinemining.ch/2018/05/14/communique-de-presse-mai-2018/

your company is in the market for building out a cryptocurrency mining data center, you might want to consider reaching out to Alpine Mining to see if they are able to assist you with your needs.

Photo: Unity Investments AG

Unity Investment AG

Unity Investment is a Swiss company developing a cryptocurrency mining solution[56]. For this interview, we spoke with Richard Kobler[57], Senior Program Manager of Unity. Richard is very knowledgeable about the mining industry. During our interview, Richard walked us through what Unity Investment AG is, opportunities they see in the space and how you can learn more about them.

Beginnings of Unity Investment AG

Photo: Incrementum AG, Jona Switzerland, April 2019

The founder and CEO of Unity Investment AG is Sean Prescott[58]. The Unity Investment office is based in Schindellegi, Switzerland, which is a 40-minute drive to Zürich city. Their mining facility is based in Jona, Switzerland.

When they first got started offering cryptocurrency mining services to their clients, the cryptocurrency markets were experiencing their all-time high prices. In December 2017, Unity Investment was offering their clients the ability to invest in units of mining machines. Richard described a unit to be a bundle of 10 cryptocurrency mining machines. So, when you became a client and you purchased a unit, you would have 10 cryptocurrency mining machines mining for you. In January and February of 2018, the market started to experience a selloff from the all-time highs and Unity Investments quickly realized that the cost of cryptocurrency mining machines started to drop and with that, their own prices had to drop. This put earlier purchasers of the units at a disadvantage to new purchasers of units at a lower price. This is when they began to think of ways to restructure their offering to clients so that it would be fairer to all purchasers, no matter when you decided to get started mining with Unity.

Mining Pool

This is how they came up with the notion of mining participation in a pool with other participants rather than the notion of a unit. For example, if a pool of participants comprised a total of 1 million CHF and each participant purchased 100,000 CHF worth of the pool, then each participant's share would be 10% of the pool, and therefore, would receive 10% of the eligible mining reward that

—

56 See https://unityinvestment.ch/
57 See https://www.linkedin.com/in/richard-kobler-0310252/
58 See https://www.linkedin.com/in/seanprescott/

particular pool of participants earned. 30% of the total mining reward of the pool is allocated by Unity to reinvest into new machines, labor, infrastructure, and other costs, and the remaining 70% of the pool gets distributed to that pools participants as the eligible mining reward.

Concerns Regarding Unity Investment AG

Investors should be aware that:

- The CEO of Unity Investment has already engaged in 6 previous ICOs.
- The Unicrypt platform offers custody service of cryptocurrencies, but the method for creating public-private key pairs for the wallets is not open-source. The entropy or randomness used for creating keys should be further investigated.
- Since Unity is not licensed to store fiat currency on the behalf of their clients, the Unicrypt wallet has tokenized fiat currencies that are designed to be stablecoins pegged to fiat currency stored in Unity bank accounts. Whether Unity Investment AG keeps full reserves or fractional reserves of the assets that their stablecoins are pegged to can only be known by Unity Investment making their bank statements publicly available on a regular basis.
- Only 1 out of 3 transformers are currently installed and functional in their warehouse in Switzerland, and the installation of the rest of the transformers depend on government services, which is outside of the control of Unity Investment.

Being that Unity is based in Switzerland, they have figured out how to keep costs under control, mainly electricity, rent, and labor, and are able to operate as lean as possible. They run on renewable energy: 85% of that being hydroelectricity, 10% wind turbines, and 5% solar electricity. Switzerland is also known for having a stable regulatory environment as well as known for providing a very secure physical location close to the Swiss Alps. They have been able to negotiate fairly good terms with the power company, for example, and if they are able to increase their efficiency, they are able to claw back 30% of the costs of electricity that they use, and with very low taxes on the cost of electricity already, Unity appears to be in a great position to compete in this competitive market. According to Richard, there are also no taxes in Switzerland on mining cryptocurrency.

Unity only invests in ASIC powered cryptocurrency miners. They have a partnership with Bitmain and currently have around 1000 ASIC miners. The mining facility is 3000 M^2 and the machine inventory includes the Bitmain S9, L3, and A3. They have also placed orders for the S15. Having a range of machines allows them to mine various cryptocurrencies, including Bitcoin, Bitcoin Cash, and Litecoin – basically any cryptocurrency that is mined using the SHA-256 or Scrypt hashing function. In addition, Unity has engaged BDO AG as their auditor so that potential investors have more confidence in their operation. They also encourage all potential investors to come to their offices as well as visit there mining facility to see the operation.

The Unicrypt Platform

Unicrypt[59] is a product developed by Unity Investments that is an online portal that provides access for clients to their account as pool participants. Unicrypt also introduces a proprietary algorithm known as Proactive Mining[60]. Proactive mining has been developed by Unity and is unique because every minute, the algorithm scans various blockchain's and checks the prices of each blockchain that they support for mining, and based on a proprietary risk to reward ratio, the algorithm determines which cryptocurrency to mine at any given point in time. Once the

—

59 See https://unicrypt.com/
60 See https://unityinvestment.ch/#proactivemining

algorithm has determined which cryptocurrency to mine, it sends instructions to each of the machines to mine that cryptocurrency.

Additional Businesses Outside of Mining

The Unicrypt platform has two other cryptocurrencies created by Unity. The first is the Unity Aurix Coin, and the second is the Unity ExaCoin. Aurix is purportedly backed by physical gold and all deposits are verified through auditors and stored securely in vaults; however, the amount of gold actually tokenized in these coins is unknown to us, and Unity Investment has not released any public documents regarding the quantity of physical gold stored in their vaults or the quantity of tokens that are backed the gold. ExaCoin is backed by Fiat, either CHF, USD, GBP, or EUR. These coins are ERC 20 tokens and investors are able to convert their cryptocurrency into either Aurix, ExaCoin, or both.

"As long as government restrictions over money and banking persist, demand for bitcoin will likely persist, and those who use it will likely continue to find a way to use it. Should governments really want to kill bitcoin, they need to attack that economic incentive for using it. In other words, they need to provide their citizens with a free market monetary system that can compete with bitcoin. Their best bet would be a return to the gold standard."

Saifedean Ammous

Conclusion

As with all things crypto, always do your own due diligence before participating in any project. We highly recommend for anyone interested to visit their mining facility, office building, and to meet Mr. Prescott and the rest of the team in order to begin proper due diligence on Unity Investment[61]. Visits are by appointment only.

Blockbase Group DWC-LLC

Introduction

Source: Blockbase DWC-LLC

For the final interview, we spoke with Vlado Stanic[62], the Founder and CEO of Blockbase Group DWC-LLC[63], which is headquartered in the United Arab Emirates, with mining facilities based in Sweden.[64] In the interview, we learned how Stanic got his start in cryptocurrency mining, the history that led to the creation of Blockbase Group, and also received insight into how their business operates.

—

61 See https://unicrypt.com/contact

62 See https://zw.linkedin.com/in/techdisplay
63 See https://blockbasegroup.com/
64 See https://blockbasemining.com/

Scrappy Startup to Large Operation

Stanic first learned about Bitcoin in 2013 and was turned on to the technology after reading the Bitcoin whitepaper. He started his first cryptocurrency mining company in 2015 based in Austria, by raising money from friends and family. Soon thereafter he partnered with his now Chief Technology Officer, Alexander Dietrich[65], who also provided startup capital. Together, they setup their first cryptocurrency mining company, named Techdisplay, which was based in Austria. Techdisplay's first data center was setup near a hydroelectric power plant inside of a shipping container.

Source: Blockbase DWC-LLC

They got their start by filling the shipping container with custom built GPU cryptocurrency miners and began mining Ethereum. During this time, they also started onboarding their first cryptocurrency mining clients which allowed them to grow. They helped their customers figure out which GPU's made the most economical sense and **began buying GPU's in bulk, anywhere from a few hundred, to 1000 to 2000 at a time, from hardware suppliers in both Hong Kong and Europe.** They eventually ran into issues with keeping these rigs cool because running GPUs all hours of the day at its highest level of performance creates a tremendous amount of heat. According to Stanic, some of the GPUs caught fire because the heat was so great.

Source: Blockbase DWC-LLC

Techdisplay eventually grew from one shipping container to three shipping containers, and suddenly faced scalability limitations. Three shipping containers full of mining machines was the maximum number of containers the hydroelectric power plant was able to support with its energy production. These limitations were partly due to the winter months when the flow of water slowed due to freezing, causing the production of energy to drop. **Stanic described that when the snow is melting there is a large flow of water which produces a lot of energy,**

—

65 See https://at.linkedin.com/in/alexander-dietrich-b90681154

and that the opposite occurs when everything is frozen. In order to keep growing they decided to explore their options.

In the quest for finding a more scalable solution, Stanic learned of Sweden, where the energy tax laws were beneficial compared to other parts of the world. Initially, Techdisplay had planned to move their shipping containers to Sweden. Stanic traveled to Sweden in February 2017 to investigate, then in March 2017, they set up Blockbase in Sweden, and by May 2017 they started their new mining operations. They eventually sold the shipping containers based in Austria, and the cryptocurrency mining infrastructure to another Austrian-based cryptocurrency mining company because moving everything to Sweden would have taken a great deal of effort.

Blockbase Mining-As-A-Service

For those who are familiar with KNC Miner, one of the original ASIC Bitcoin manufacturers, they had a mining facility based in Sweden. KNC Miner met the unfortunate fate of going out of business, but this unfortunate outcome became an opportunity for Stanic and Blockbase, as they were able to move into the facility of previously occupied by KNC Miner[66]. One of the benefits of the Swedish mining facility of Blockbase, is that it also makes uses of hydroelectricity to power the data centers. **According to Stanic, this energy is 100% clean and green energy.**


HYDROELECTRIC POWER

ENVIRONMENTAL PRODUCT DECLARATION (EPD)

This is to certify that

Blockbase

during the period 2017-05-19 – 2019-12-31
purchases hydroelectric power with EPD from Vattenfall AB.

EPD- Environmental Product Declaration – is a certified environmental product declaration registered by IVL Swedish Environmental Research Institute with quality assured information on resource consumption, emissions, wastes, recycling etc.

Stockholm 2017-11-17
VATTENFALL AB

Branislav Slavic
Vattenfall Business Sales Nordic

VATTENFALL

Source: Blockbase AG

The website describes Blockbase to be mining-as-a-service and lists that they offer three purchase options for potential customers interested in mining: "Order Miners in Bulk", "Buy Hosted Miners", and "Send us Your Machines". For the first two purchase options, they source, setup, and configure all of the desired mining hardware for the client, and all of the equipment is owned by the actual client, not by Blockbase. If a client has their own mining machines, the client could send them to Blockbase for hosting, but the website lists a minimum quantity of 1000 machines.

For those who don't have their own machines, one of the other packages available seem more appropriate. The website does mention on the pricing page[67] **a minimum purchase of 30,000 EUR worth of mining machines and the "Standard" plan is priced monthly, with 58 EUR per kilowatt per month.** If you pay by the half year, there is a 6% discount applied, with a rate of 55 EUR per kilowatt per month. If you pay by the year, there is a 13% discount applied, with a rate of 51 EUR per kilowatt per month.

—

66 See https://blockbasemining.com/mining-farm-sweden/
67 See https://blockbasemining.com/pricing/

As for their inventory, Blockbase offers a Canaan AvalonMiner 841[68], which is an ASIC machine produced by the company Canaan[69], and this is used to mine Bitcoin. The website lists these machines as currently in stock. As for the power consumption of these ASICs, they consume 1290 watts, and produce a hashrate of approximately 13.6 TH/s. The other mining machine options available is a GPU Miner P 102-100[70], used for mining cryptocurrencies such as Ethereum, Monero, and Zcash. These machines are listed to be on backorder and require a 50% deposit per machine. As for the power consumption of the GPU miners, they consume 1582 watts, and produce a hashrate of approximately 380 MH/s.

99% Uptime

"Contrary to what many believe, a miner with 51% of the hashrate cannot overturn consensus rules, change the monetary policy, or even confiscate any bitcoiner's coins."

Saifedean Ammous

Stanic described how Blockbase is different from other mining services in the space, **in that they offer a 99% uptime guarantee.** Mining machines do experience failure due to continuous and rigorous operation, and when a failure happens to a client's machine, that client is exposed to downtime until the machine is fixed. Sometimes this could take weeks for a manufacturer to repair the machine if it is under warranty, and by this time, the client will most likely lose money on their investment because when the network difficulty increases and more mining machines come online competing for the block reward, the window for achieving profitability with a mining machine gets smaller and smaller. To fix this exposure to risk, and **to guarantee a 99% uptime, Stanic described, for example, that they could purchase an additional 20% of machines,** so that in case a machine goes down, they are able to replace the failed machines with a new machine quickly, so their clients are back online mining right away and experience very little downtime. Further, Blockbase has implemented an online portal that allows clients to connect their own cryptocurrency addresses for receiving their rewards, and the **rewards are paid out daily.**

Conclusion

Overall, Stanic seems very knowledgeable about mining cryptocurrency and Blockbase appears to have a great location in Sweden with a long mining history. For the most part, **the pricing of the service seems out of reach for the hobby miners and seems more like a service for well-funded companies who are serious about getting into the mining space.** Stanic and Blockbase welcomes all their potential clients to visit their facilities in Sweden to check out their operations, and anyone interested in doing so, should reach out to them through their website. Always do your own due diligence[71] before making any investment decision.

—

68 See https://blockbasemining.com/hardware-servers/asic-miners/
69 See https://canaan.io/
70 See https://blockbasemining.com/hardware-servers/gpu-miners/
71 See "The Blockbase Mining Connections", The Financial Telegram, June 30, 2018

No Room for Trust in A Trustless World

One of the greatest innovations of Bitcoin is being able to transfer digital money in a peer to peer fashion without having to trust a centralized intermediary. Many refer to Bitcoin as trustless, there is no need to trust person or entity, all that is required is to trust the computer source code, the math, and the cryptography behind the system. Being that the computer code is open source, this allows anyone in the world with a computer and internet access to perform an audit.

"Every informed person needs to know about Bitcoin because it might be one of the world's most important developments...Bitcoin might revolutionize more than money or economics. It could transform the role and nature of government."

Leon Louw
Nobel Peace Prize Nominee

The moment a centralized intermediary comes into play in the cryptocurrency ecosystem, trust is required. Purchasing specialty cryptocurrency mining equipment, using a mining pool, or renting computation power from a cloud mining service requires extreme trust. With cryptocurrency mining equipment manufacturers, you must trust that the supply chains for sourcing the materials are in place, that the materials arrive on time and on budget, that the machines actually get assembled and delivered, that the software on those machines is secure with no backdoors, and that those machines actually perform as their supposed to, among many other factors. With a mining pool, you must trust that the mining pool software is secure with no backdoors and that they are actually capable of delivering the reward for allocating your computation resources to their pool. With cloud mining services, you must trust that the data center exists, that the computer or computers that you are renting exist and are solely dedicated to your exclusive use, and that their software is secure with no backdoors.

With that said there have been many companies who have been leading examples by following industry best practices that security conscious consumers would expect. There have also been many poorly managed cryptocurrency mining operations, bad actors, and outright scams. In the early days of Bitcoin, companies began popping up claiming they were going to manufacturer specialty computers or chips for mining Bitcoin or other cryptocurrencies and they would offer "presales" of their equipment on fancy looking websites with incredible statistics. After the "presale", the company would suddenly disappear, leaving unsuspecting purchasers at a loss of their hard-earned Bitcoin or fiat currency. In addition, there were incidents with mining pools that were compromised, whether from insiders or from external hackers, and the miners who contributed their precious computation resources had to suffer the consequences and loses. There have also been cloud mining operations that claimed to have data centers full of specialty mining computers without actually having the number of computers, or even any at all at their disposal for their customers.

"The most significant impact that bitcoin can have on the market for energy is that it is a technological solution that makes energy production far more fungible and liquid."

Saifedean Ammous

We would like to point out important information to those who are new to the cryptocurrency space. It is unwise to give someone access to your private keys. In the same thought pattern, unless you are in direct possession of or control over the cryptocurrency mining machine, and that machine has open-source software that has been audited or reviewed by the community passing a community credibility check, you are essentially giving someone else access to your private keys. **Make sure you trust the service provider who manages your cryptocurrency mining machines for you.**

Cryptocurrencies.
The New Asset Class.

Regulated | Diversified | Liquid

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

www.cryptofunds.li

John Tromp: Making Computer Science Great Again

"PoW (Proof-of-Work) makes for a fairer coin distribution as everyone has to compete on equal terms. A constant reward, resulting in linear emission, extends this fair competition across all times."

John Tromp

Key Takeaways

- **Cuckoo Cycle is memory-bound Proof of Work mining algorithm that tries to find a cycle within a particular type of graph, a bipartite graph.**
- **There are a few projects that are implementing Tromp's Cuckoo Cycle mining algorithm. MimbleWimble, the privacy preserving Blockchain protocol also makes use of Cuckoo Cycle. Aeternity, the unicorn Blockchain project based in Liechtenstein is using Cuckoo Cycle, and the hot privacy coins Grim and Beam, are implementing the MimbleWimble protocol and therefore also implementing Cuckoo Cycle**
- **MimbleWimble is a privacy preserving blockchain protocol implementation and gets its name from the Harry Potter fictional book series.**

**

John Tromp from Cuckoo Cycle

John Tromp[72] is the inventor of the Cuckoo Cycle[73] mining algorithm, and its variants (Cuckatoo Cycle and Cuckaroo Cycle). He is also a core developer of the privacy focused blockchain Grin[74], which makes use of the MimbleWimble[75] protocol, a privacy preserving blockchain protocol. MimbleWimble implements his Cuckoo Cycle[76] mining algorithm. In addition, Tromp is known for having created a mining software implementation, or solver, of the Equihash[77] mining algorithm for Zcash[78]**.** Tromp is one of the most intelligent computer scientists in the crypto space. Tromp has a PhD from the University of Amsterdam in Theoretical Computer Science and has an exceptional knack for bringing that theory into reality with practical algorithm implementations and computer code. Not only is he one of the brightest minds, he is also one of the humblest.

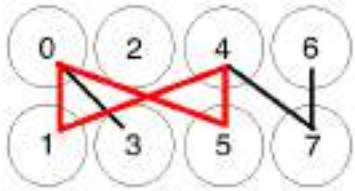
What is Cuckoo Cycle?

"I'm a big fan of Bitcoin... Regulation of money supply needs to be depoliticized."

Al Gore

According to Tromp, Cuckoo Cycle is memory-bound Proof of Work mining algorithm that tries to find a cycle within a particular type of graph, a bipartite graph. In the case of Cuckoo Cycle, **memory-bound means that the rate of solutions a miner can achieve depends on the memory bandwidth of the miner, as opposed to the amount of memory, or the amount of processing power of a miner.** A graph, in simple terms, is a set of points connected with lines. A bipartite graph is two sets of points, where there are no lines between points within that particular set, only lines connecting points across the two different sets. When the lines across sets form a cycle, or in other words a loop, that cycle is known as a bipartite graph.

Figure 26: Bipartite Graph



Source: https://tinyurl.com/y23jy23j

Tromp compared Cuckoo Cycle to Bitcoin's Hashcash[79] mining algorithm and described Cuckoo Cycle as more of a stronger "Proof of Work" than Bitcoin's Hashcash, which claims to be "Proof of Work" because of the tremendous amount of work that must be computed in order to find a solution. **Instead Tromp described Hashcash as more of a "proof of luck" than a Proof of Work.** For a miner to solve the Cuckoo Cycle Proof of Work, the machine must find a

—

72 See https://tromp.github.io/
73 See https://github.com/tromp/cuckoo
74 See https://grin-tech.org/
75 See https://github.com/mimblewimble/grin
76 See https://github.com/mimblewimble/grin/blob/master/doc/pow/pow.md
77 See https://en.wikipedia.org/wiki/Equihash
78 See https://z.cash/
79 See https://en.wikipedia.org/wiki/Hashcash

cycle of length 42. Once a cycle is found, an additional filter of the Hashcash algorithm is applied to the result from the found cycle. According to Tromp, Cuckoo Cycle miners calculate the speed of a machine by its measured graph rate, as opposed to the hashrate measurement used for calculating the mining speed of hardware for Blockchain's such as Bitcoin and Ethereum. Hashrate is simply, how many hashes per second a miner is able to compute. The graph rate is, how many graphs that are able to be computed per second. Tromp further described fidelity, which is the probability that a miner will find a cycle of length 42, so Cuckoo Cycle miners measure the speed of their hardware using a combination of graph rate and fidelity to determine their mining speed.

Cuckoo Cycle Variants

The original whitepaper[80] for Cuckoo Cycle was written in 2014. Since then, there have been many new developments made with Cuckoo Cycle. Tromp originally thought Cuckoo Cycle was "ASIC resistant" Proof of Work. **ASIC resistant simply means that an ASIC programmed for calculating Cuckoo Cycle would not necessarily give a miner a competitive advantage against other forms of mining, for example, compared against a GPU miner.** However, Tromp created has now created two different variants: one variant of Cuckoo Cycle, called Cuckaroo Cycle, is ASIC resistant, another, known as Cuckatoo[81] Cycle, is ASIC friendly. There are at least two cryptocurrency mining machine manufacturers creating ASICs for Cuckoo Cycle Blockchains, in particular, for a blockchain known as **Grin**. Those two companies are Obelisk[82] and InnoSilicon[83].

Source: https://grin-tech.org/

What Coins Use Cuckoo Cycle?

There are a few projects that are implementing Tromp's Cuckoo Cycle mining algorithm. MimbleWimble, the privacy preserving Blockchain protocol also makes use of Cuckoo Cycle. Aeternity[84], the unicorn Blockchain project based in Liechtenstein is using Cuckoo Cycle, and the hot privacy coins Grim and Beam[85], are implementing the MimbleWimble protocol and therefore also implementing Cuckoo Cycle. There is even a research proposal named cuckoo-http[86] that is experimenting with Cuckoo Cycle to limit denial-of-service attacks against web servers.[87]

—

80 See http://hashcash.org/papers/cuckoo.pdf
81 See https://www.grin-forum.org/t/cuckoo-cycle-weakness-and-possible-fix-cuckatoo-cycle/738
82 See https://obelisk.tech/products/grn1.html
83 See https://www.innosilicon.com/html/a9-miner/index.html
84 See https://aeternity.com/
85 See https://www.beam.mw/
86 See https://css.csail.mit.edu/6.858/2019/projects/kaza.pdf
87 See https://github.com/AnimatedRNG/cuckoo-http

MimbleWimble

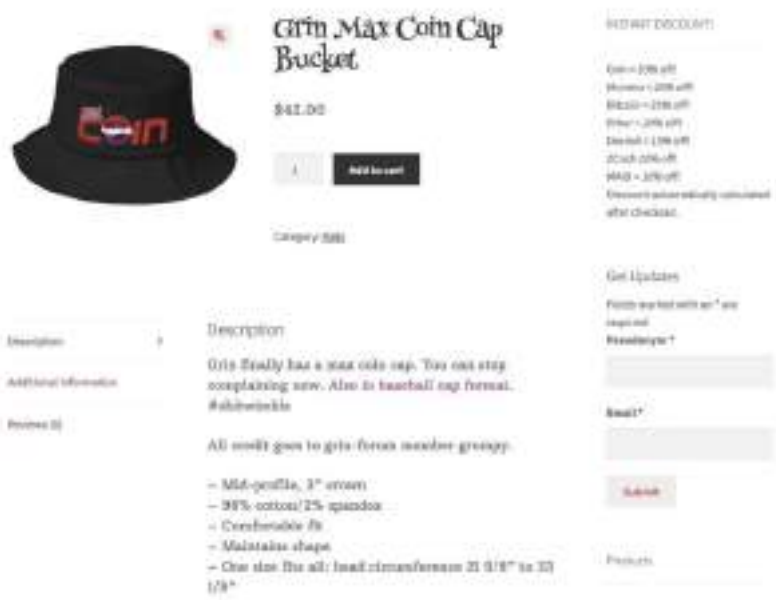
"Inarguably, someone who wants to use a currency for illegal activity is better off using cash than bitcoin."

Chris Burniske and Jack Tatar

MimbleWimble is a privacy preserving blockchain protocol implementation and gets its name from the Harry Potter fictional book series. According to the official MimbleWimble documentation[88], "MimbleWimble as an idea was released anonymously. It's a blockchain with Proof of Work but almost nothing else". The first implementation of MimbleWimble was proposed by an anonymous online persona known as Ignotus Peverell, which is also the name of a fictional character from the Harry Potter series, thus following a similar anonymous origin to Bitcoin as being created by the anonymous Satoshi Nakamoto.

Grim

This first implementation of MimbleWimble eventually became known as Grin. Tromp was particularly excited about MimbleWimble and Grin and their decision to use Cuckoo Cycle as the mining algorithm. Tromp eventually became a core developer and contributor to Grin. Tromp described the coin emission model of Grin[89] to be of particular interest to him as he felt it had many advantages over other Blockchain's coin emission models. However, we have a slightly different view. Grim has no hard cap on the coin supply, which makes it not scarce, and therefore, no different from other infinitely inflationary fiat currencies.



Source: https://tmgox.com/product/grin-max-coin-cap-bucket/

John Tromp, Making Computer Science Great Again

"If we remember, 15 years ago if you were doing anything on the internet you were going to make millions. I think it could be the same with Bitcoin."

Jared Kenna
Founder of Tradehill

We asked Tromp how he felt to have such an influence of spawning an entire ecosystem within the mining industry. He humbly downplayed the significance he has actually had within the blockchain community but from where we're viewing from, he has been very influential and is well respected Computer Scientist by many in the crypto space. When we asked Tromp about his perspective of the cryptocurrency mining industry, he described mining as a very tricky business and noted that many people have regretted getting into mining rather than just outright buying coins, and that novices should take note of this information before considering getting into the mining business. He also suggested that in order to

—

88 See https://github.com/mimblewimble/docs
89 See https://github.com/mimblewimble/docs/wiki/Monetary-Policy

succeed, one must understand the risks with running a mining operation as well as understand the need for having access to cheap long-term power contracts. With that said, we look forward to learning about future developments with Cuckoo Cycle, it's variants, and the many up-and-coming blockchain projects such as Grin that are making use of Cuckoo Cycle.

About Us

The Team

Mark Valek
Portfolio Management & Research

Demelza Hays
Research & Portfolio Management

Cristian Ababii
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. In cooperation with the State Printing House of Austria, Coinfinity has designed a "Card Wallet" that is a bearer paper wallet for Bitcoin.

Oliver Völkel

Based in Vienna, Oliver Völkel is a partner at 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.

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

Crypto Research Report – December 2017 Edition

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

Crypto Research Report - March 2018 Edition

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

Crypto Research Report - June 2018 Edition

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

Crypto Research Report - October 2018 Edition

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

**

crypto research .report

Crypto Research Report - January 2019 Edition

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

We sincerely want to thank the following friends for their outstanding support:
Our knowledgeable advisors including Max Tertinegg and Oliver Völkel, the generous authors who contributed to this report including Nikolaus Jilch, Florian Grummes and Pascal Hügli. We are also grateful to our wonderful research analyst Cristian Ababii, our translator Georg Bühler, our editors Bianca Sayers and Gregor Hochreiter, and our reviewers.

Contact:

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

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