Decrypt

A deep dive into topics all around the crypto world.

Bitcoin Suisse

Series 2

The Year at a Glance

The Bitcoin Suisse Research Department delivers regular research updates through its Decrypt publication. Launched in July of 2019, Bitcoin Suisse Decrypt provides readers the best combination of focused insights, relevant data and easy-to-understand information. The Decrypt topical articles allow forward-thinking investors, tech enthusiasts and those new to the crypto asset space to get a deeper understanding of the most important concepts and current trends influencing the crypto industry – and help them stay at the leading edge of crypto finance and crypto financial markets.

Written by Dr. Raffael Huber
Head of Research

Impressum
Bitcoin Suisse AG
Grafenauweg 12
6300 Zug Switzerland

Bitcoin Suisse (Liechtenstein)
AG Aeulestrasse 74 9490 Vaduz
Liechtenstein

Calls from within Switzerland
(tollfree):
0800 800 008
Calls from abroad:
+41 41 660 00 00 Contact us:
info@bitcoinsuisse.com

Discover Our Services:
Prime Brokerage • Custody
Collateralized Lending • Payments • Staking • Tokenization

bitcoinsuisse.com

Printing:
Printoset, Zürich
Printed in Switzerland

Episodes

01 Blockchain, not bitcoin? 5

02 A Flight to Safety 9

03 Turn on the Money Printers! 14

04 Block Reward Halvings and the Rational Miner 18

05 Ethereum's Path to Serenity 24

06 Bitcoin SV: Back to Genesis 32

07 Interoperability between Blockchains 37

08 Scaling the Second Layer 43

09 Token Incentives in Decentralized Finance 50

10 Examining Crypto Volatility 56

11 The Evolving Open Finance Ecosystem 62

12 The Aftershock of Governance Tokens 67

13 Shifts in Crypto-currency Markets 73

14 Regulations and Innovations 79

15 Airdrops and Forks – Free Money? 85

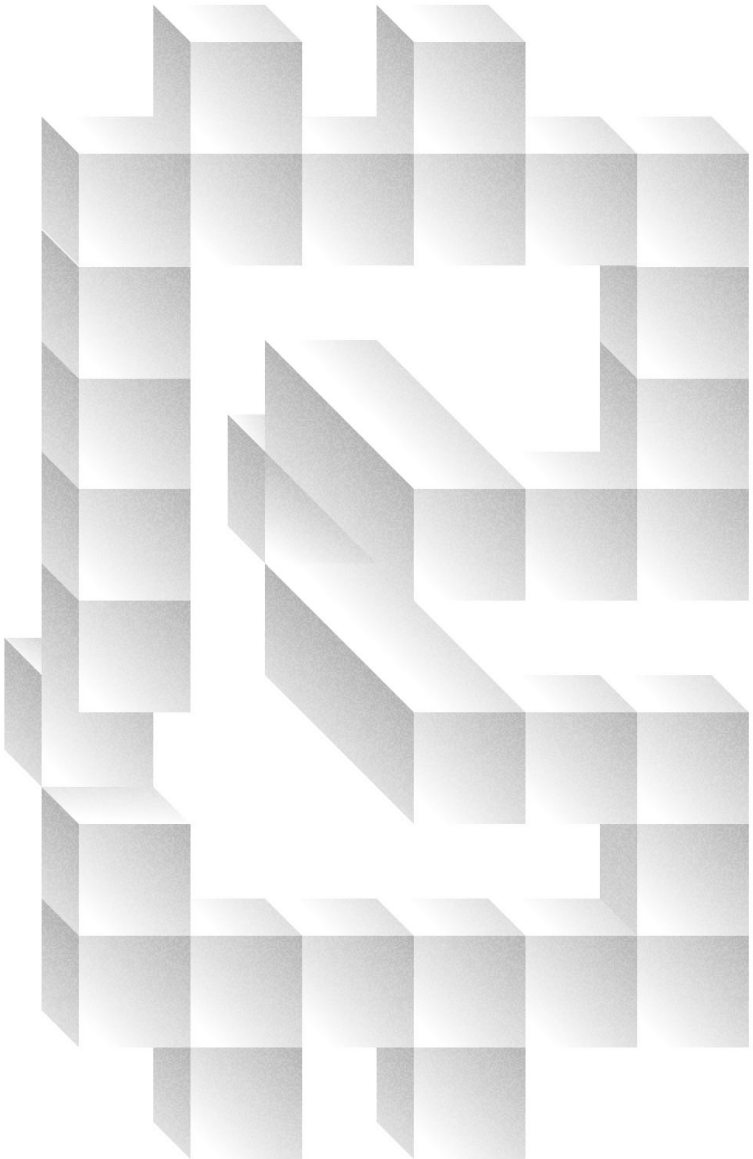
16 Evaluating Smart Contract Security 91

17 Onboarding the Next Wave to Crypto 96

18 Ethereum 2 Is Coming 102

19 Scaling the Decentralized Economy 107

20 The Year 2020 in a Nutshell 112



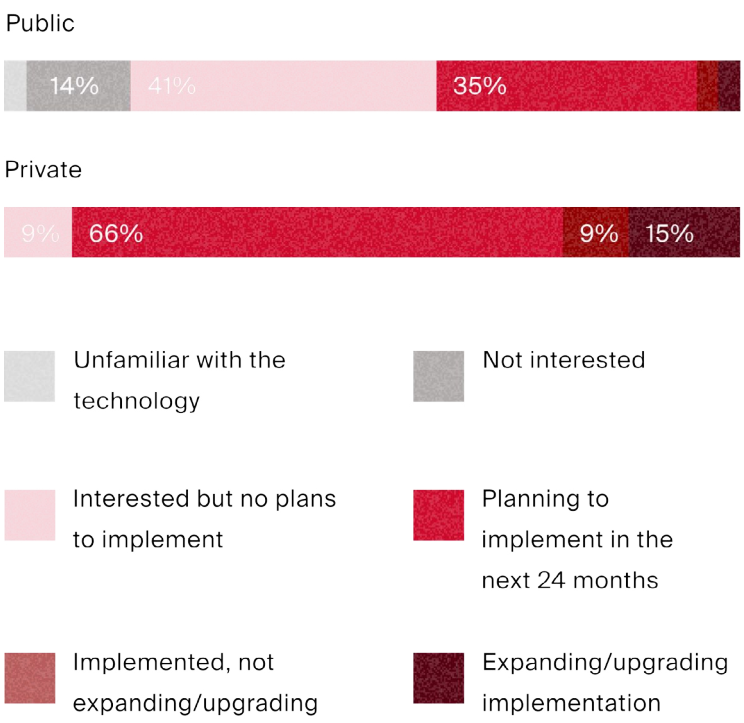
Blockchain, not bitcoin?

An often-heard stance on the digital asset space is: “Blockchain yes, cryptocurrencies no.” However, the value proposition of the two is linked together, and cryptocurrencies are an integral part of decentralized blockchains.

In late 2017, cryptocurrencies experienced their euphoria phase with the total market capitalization reaching almost $1 trillion. The underlying blockchain technology also became a hyped buzzword that was able to quickly attract capital. One example would be the case of “Long Island Iced Tea Corp.”, a beverage producer in the U.S. that rebranded itself to “Long Blockchain Corp.” in December 2017 – a move after which its stock price tripled within a day (and later led to a subpoena by the SEC).[1]

More than two years later, blockchain usage in companies continues to pick up, although it largely remains under the radar. A recent study[2] by Forrester and EY showed that companies still mostly use private blockchains, but public blockchains are on the rise.

Illustration 1: In a recent survey on "What are your organization's plans when it comes to blockchain?", one third of companies indicated that they are planning to implement public blockchains in their businesses over the next two years.



Source: Forrester, ey.com, Bitcoin Suisse Research.

In the Bitcoin Suisse Crypto Outlook 2020,[3] Marco Schurtenberger from the Tezos Foundation gave detailed insights into the opportunities and challenges that come with private and public blockchains. Companies looking to implement blockchain in their daily business typically have two concerns: privacy and regulatory uncertainty.

Both concerns are increasingly being addressed. On the privacy side, advances in zero-knowledge proof technology[4] make it possible to treat transaction data confidentially while still recording it on a public blockchain. On the regulatory side, legal frameworks keep improving through the pioneering work of countries like Switzerland and Liechtenstein. For example, the Federal Council of Switzerland submitted a series of blockchain/DLT related amendments to existing legislation in March 2019[5] and Liechtenstein developed the "Token Container Model"[6] for the tokenization of assets. These steps will help to alleviate regulatory uncertainty.

The main reasons to use public blockchains instead of private ones will come from economic considerations. Public blockchains can save costs compared to private ones,[7] as the infrastructure is already built and accessible in a permission-

less way. The only requirement to use a public blockchain is a certain amount of the blockchain's native cryptocurrency to pay for transactions being recorded in blocks.[8] Interoperability with other network participants that use the same public blockchain is automatically given.

Also, the open source nature of public blockchains allows anyone to innovate. Ultimately, it was this permissionless way of finding solutions with bright minds all over the world that brought the Internet to where it is today – even more powerful than many of its advocates would have thought possible only 25 years ago.[9]

> [Satoshi] treated cryptographic protocols as being economic protocols, where the economics is not just an afterthought – the incentives are a fundamental building-layer of the entire system.
>
> – Vitalik Buterin

Connecting the Dots: Cryptocurrencies

The biggest advantages of blockchain technology are reaped when it is paired with a decentralized structure.[10] At its core, a blockchain is an immutable, tamper-proof ledger of transactions – no more, no less. In centralized systems, these characteristics are hard to achieve and even harder to credibly prove to an outside inspector. They will always possess single points of failures, be it from a technical or a human perspective. Decentralized systems are tolerant towards faulty behavior: Failure of one computer, one node, or one participant in the network does not have an impact. This is illustrated, for example, by the near-100% uptime that both Bitcoin and Ethereum boast.[11]

Decentralized systems come with separate challenges, however. The absence of a central authority means that no single entity pays for operating the blockchain. Thus, the protocol needs a means to transfer value from the users of the network to its operators. A decentralized blockchain protocol cannot print government-issued currencies – this is where cryptocurrencies enter the picture. The protocol can issue more cryptocurrency to pay its operators, such as miners (Proof-of-Work blockchains such as Bitcoin[12]) or validators (Proof-of-Stake blockchains such as Ethereum 2).[13] The rules for this issuance

are hard-coded into the protocol and should follow the mantra “as little as possible, but as much as needed to keep the network secure”. Hence, cryptocurrencies were created as an incentive system that secures the ledger under the game-theoretical assumption that all network participants act in their self-interest.

While this outlines the supply side of cryptocurrencies, where does the demand come from in the long run? As described above, people or companies looking to use public blockchains will need to acquire a certain amount of cryptocurrency to access the public infrastructure. The amount of demand that can be expected here depends largely on the extent of adoption and creates the link between blockchain usage and part of its value.

On the other hand, additional demand might also come from the potential role of cryptocurrencies as stores of value and as part of regular portfolios. The portfolio benefits of incorporating uncorrelated[14] asset classes are widely known, and some go as far as calling it the “Holy Grail of Investing”.[15]

Bitcoin was born out of the subprime mortgage crisis and offers an alternative money whose issuance is controlled by code instead of central banks. This is perhaps not as significant today with inflation rates sitting at levels of around 2%.[16] However, it may become more relevant in the future as governments start to experiment with more aggressive forms of expanding the total monetary supply, such as helicopter money.[17]

In conclusion, cryptocurrencies are a crucial ingredient in a decentralized blockchain protocol and provide a game-theoretically balanced incentive system to run such networks. The degree of decentralization that such blockchains have is tightly linked to their value proposition, as this guarantees some key aspects such as immutability. Many of the older cryptocurrencies, for example Bitcoin or Ether, have proven over the course of the past years that they have found a game-theoretically stable equilibrium and hence have the potential to provide the infrastructure for the “Internet of Value”.

Sources

1 https://www.bloomberg.com/news/articles/2018-08-01/long-blockchain-gets-hit-with-sec-subpoena-after-nasdaq-ouster

2 https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/blockchain/ey-public-blockchain-opportunity-snapshot.pdf

3 https://www.bitcoinsuisse.com/outlook/why-public-blockchains-are-the-future

4 https://www.bitcoinsuisse.com/research/decrypt/the-identity-of-the-future

5 https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-77252.html

6 https://www.bitcoinsuisse.com/outlook-2020

7 https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/$File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf

8 https://www.bitcoinsuisse.com/research/decrypt/transaction-fees-markets-for-block-space

9 https://thenextweb.com/shareables/2010/02/27/newsweek-1995-buy-books-newspapers-straight-intenet-uh/

10 https://www.bitcoinsuisse.com/research/decrypt/the-benefits-of-decentralization

11 http://bitcoinuptime.com/

12 https://www.bitcoinsuisse.com/research/decrypt/the-recipe-for-trustlessness

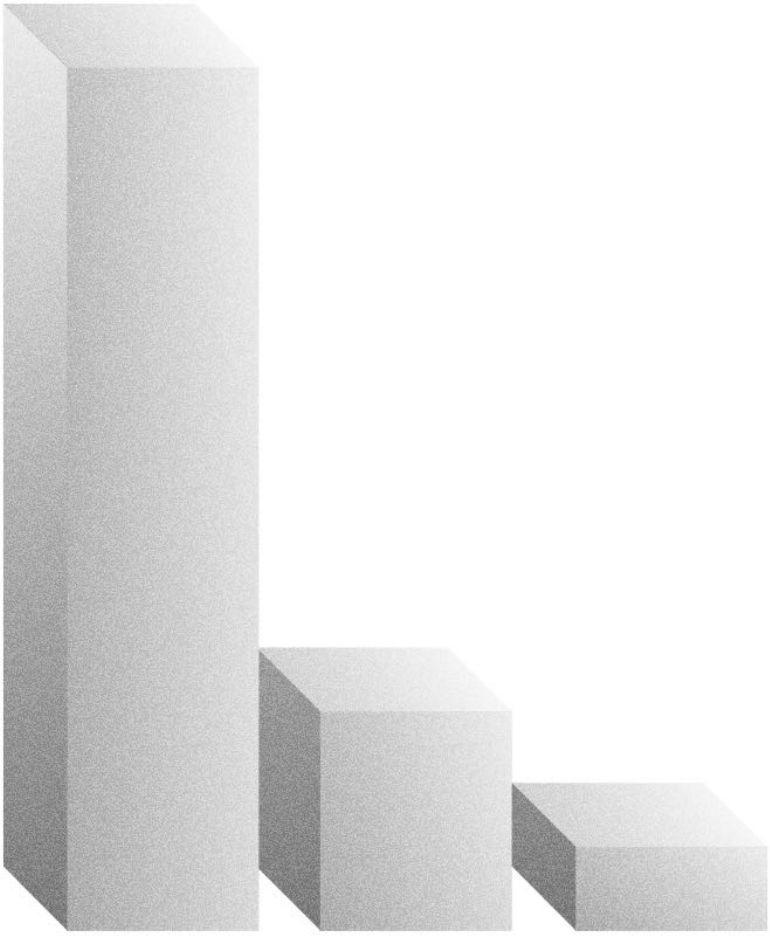
13 https://www.bitcoinsuisse.com/research/decrypt/staking-on-chains

14 https://www.bitcoinsuisse.com/outlook/bitcoin-in-2020-halving-the-block-reward

15 https://www.forbes.com/sites/forbesmarketplace/2019/03/27/holy-grail-of-investing/#9edc993af490

16 https://data.oecd.org/price/inflation-cpi.htm

17 https://ftalphaville.ft.com/2020/02/26/1582705518000/Helicopter-money-is-here/



A Flight to Safety

Cryptocurrencies were not immune to concerns about the global economy and saw a market-wide sell-off last week. What happened? And how did it happen?

Last week marked a historic event in the cryptocurrency markets, with Bitcoin and other cryptocurrencies losing almost 50% of their value – the biggest single-day loss since 2013. This sell-off came amidst global market fears about the impact that the novel coronavirus COVID-2019 will have on economies worldwide. In an attempt to slow down the spread of the virus, multiple countries have elected to impose restrictions on travel and social gatherings.[1] Stock markets globally reacted to the crisis with double-digit declines over the past weeks. On top of that, tensions between Russia and the OPEC dropped oil prices by -24.6% on March 9.[2] These are turbulent times, which was also reflected in the cryptocurrency markets.

Leveraging Derivatives

To understand how and why Bitcoin dropped to this extent, it is crucial to look at what happened on the largest crypto derivatives exchanges during the sell-off. Correlations between cryptocurrencies typically rise strongly during large drops, which is why this Episode will focus on the movements in the Bitcoin markets – most other cryptocurrencies experienced similar sell-offs.

A dominant player in the derivatives space is BitMEX,[3] which traded volumes of $10 billion and $8.5 billion on March 12 and March 13, respectively. Their most liquid product, a perpetual swap,[4] aims to track a price index comprising various spot markets. This is accomplished through a “Funding Rate”: If the perpetual swap trades below the index price, holders of short positions must pay holders of long positions, and vice versa. Trading this derivative on leverage is also enabled, meaning that a user who owns 1 BTC on the platform can open positions that are multiple times as large (up to 100 BTC worth usually). If losses on a trading position get close to where the trader would become bankrupt, a liquidation engine takes over the position and tries to close it by selling or buying in the open derivatives market. Leverage trading played a major role in the speed at which this recent drop happened.

Illustration 1: Bitcoin's price changed by -55% from peak (March 12) to trough (March 13). XBTUSD perpetual swap prices, UTC times.

Source: BitMEX API, Bitcoin Suisse Research.

Crypto Sell-Off: The Timeline

An hour before noon (UTC) on March 12, Bitcoin took a first plunge from levels of about $7.3k down below $5.6k. This was accompanied and accelerated by a cascade of long position liquidations: Traders holding large positions were liquidated during the drop, the liquidation engine took over their position and sold them, which pushed prices further down. This in turn caused more traders to be liquidated, creating the "cascade".

Over the next two hours (until about 1 p.m.), markets were still processing the shock. An indication of this was the disparity between the pricings of the derivatives and spot markets. The perpetual swap traded far below the index price coming from the spot markets. Over time, markets are usually brought back into equilibrium by arbitrageurs, which buy the perpetual swap and sell Bitcoin on the spot markets, converging the two.

After a consolidation period that lasted until about midnight, the price continued to slip lower, triggering a second wave of liquidations of long positions. It is noteworthy that during this second drop, the liquidation engine had a hard time getting its sell orders filled due to a lack of buy-side liquidity. Liquidation orders remained in the system and were not fully processed (i.e., bought) until hours later at 5 a.m., creating continuous downside pressure on the market and pushing Bitcoin to lows of $3.6k.

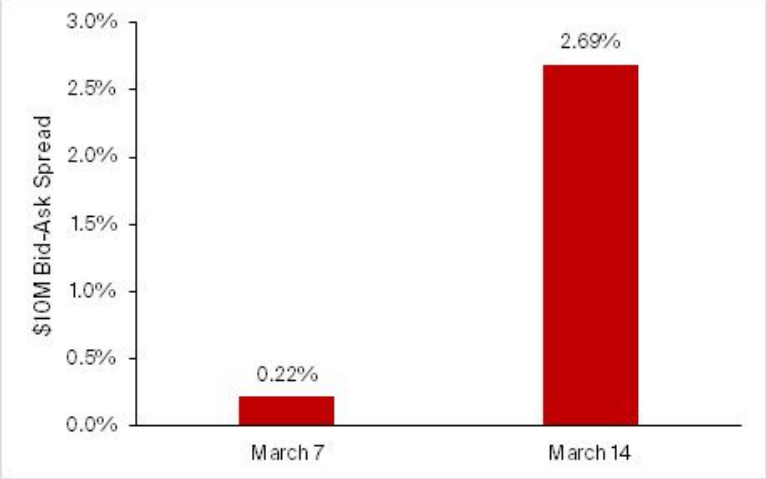
At these lows, BitMEX experienced hardware issues and was briefly taken offline. This meant that much of the selling pressure in the market coming from liquidation orders was taken out. BitMEX's outage acted as a sort of circuit-breaker, which

is common in traditional markets and halts trading after large drops. What followed was a relief rally up to almost $6k, but the market remained in a distressed state, with bid-ask spreads as large as $600-700 and the perpetual swap trading hundreds of dollars below the spot markets. Arbitrageurs slowly stepped back in after being cautious initially, and readjusted the pricings of derivatives and spot markets over the course of the next 36 hours.

State of the Markets: The Aftermath

At the time of writing, liquidity in the markets still remains low.

Illustration 2: Bid-ask spreads for a $10 million order are currently 10 times higher than before the sell-off, illustrating the low liquidity in the markets.



Source: skew.com, Bitcoin Suisse Research.

This indicates that large market makers that typically quote tight spreads for Bitcoin and offer liquidity also for large orders are still exercising caution with respect to a full re-entry to the market. The widespread crypto sell-off has deleveraged the side of the market that was long, with total liquidations during the drop amounting to more than $1.5 billion.

So far, Bitcoin has not acted as a “safe haven” in the current liquidity crisis that is also reflected in the stock markets. Instead, what can be observed in every market right now is a flight to safety – which is mostly cash, especially during the beginning stage of a potential global recession. Correlations briefly move towards 1 during such a sell-off, which can also be seen in traditional asset classes. Even gold, as the traditional safe haven asset, has seen some downside pressure and volatility, losing 7.6% over the past few days. During the financial crisis in 2008, gold dropped by about 30%, but recovered to

levels close to its previous all-time high by the time the S&P 500 reached its bottom.

Bitcoin is still a nascent technology in the grand scheme of things, and the next few months may be the first time that it gets to prove its worth during a global recession. Satoshi Nakamoto's vision for Bitcoin foresaw it as a hedge against improper monetary policies and currency devaluations. The inscription in the first ever Bitcoin block mined in 2009 reads: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."

- Satoshi Nakamoto

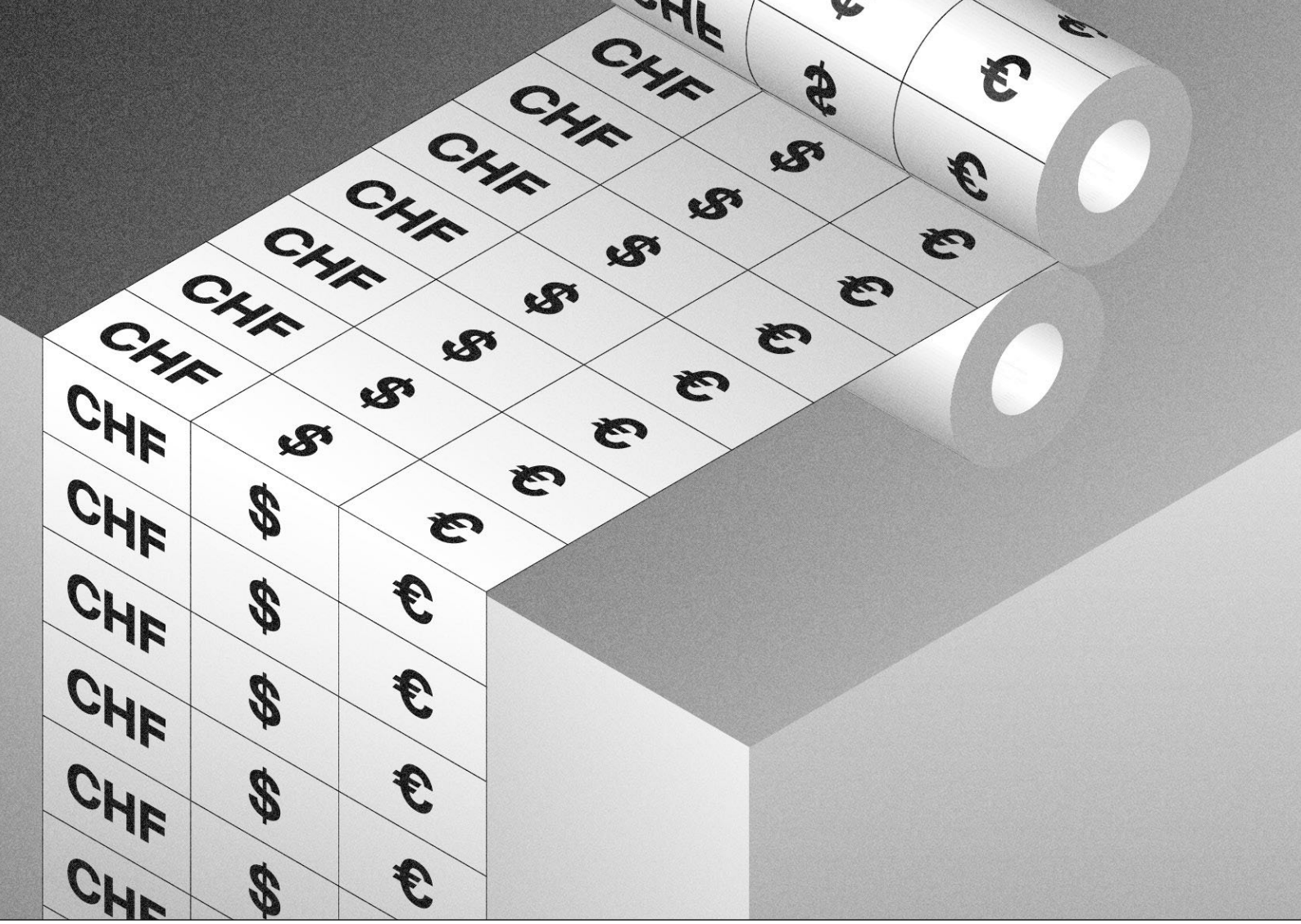
Sources

1 https://www.nytimes.com/2020/03/11/us/politics/anthony-fauci-coronavirus.html

2 https://www.wsj.com/articles/saudi-russia-disclose-dueling-output-plans-amid-intensifying-oil-market-war-11583835347

3 https://www.bitcoinsuisse.com/research/decrypt/on-chain-derivatives-and-insurance

4 https://www.cryptocritics.com/perpetual-swap-futures-contracts-and-leverage-trading-explained/



Turn on the Money Printers!

The current global crisis has led governments and central banks to launch extensive measures in fiscal and monetary policies. This brings up the discussion about a fundamental aspect of cryptocurrencies: their use as a hedge against inflation.

Cryptocurrency markets have recovered strongly from the drop in mid-March that saw a low of around $3.6k for Bitcoin. Bitcoin almost reached $7k and is now consolidating around $6k. On a fundamental level, advances for major blockchains keep continuing. The specifications of Ethereum 2 have passed the audit [1]by security firm LeastAuthority, with few potential vulnerabilities to still address. In addition, the Baseline Protocol – a joint effort by ConsenSys, Microsoft and EY to use the public Ethereum chain for confidential on-chain collaboration between enterprises – has been open-sourced on GitHub.[2] The Bitcoin block reward halving is now less than one and a half months away and is projected to take place on May 13, 2020, with the block reward halvings on Bitcoin Cash (BCH) and Bitcoin Satoshi Vision (BSV) happening even sooner – in approximately 8 and 10 days, respectively.

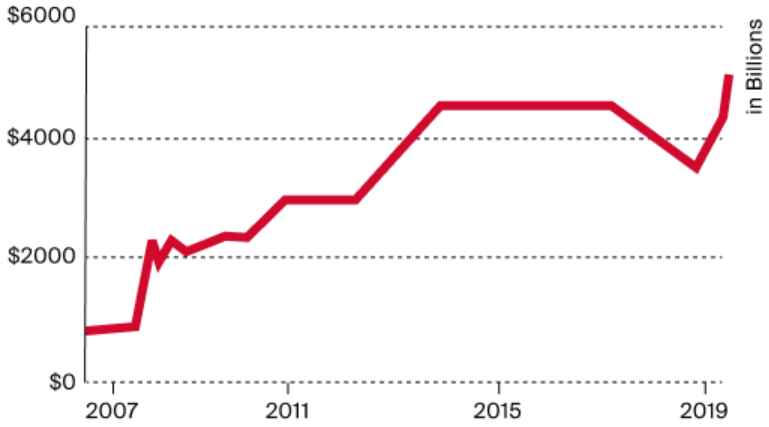
However, during a time like this, it is also important to keep global macroeconomic events on the radar. As mentioned in the last episode of Decrypt,[3] Satoshi Nakamoto's vision for Bitcoin included the idea of it being a way out of currencies that require trust. The trust in conventional fiat currencies may now be put to the test rather sooner than later.

Traditional markets have continued to experience pressure due to the pandemic and global economic crisis. For example, initial jobless claims in the U.S. rose above 3 million, which represents an (unfathomably rare!) 30-sigma event,[4] statistically speaking. Governments and central banks all around the world are unleashing their fiscal and monetary policy firepower to counteract the consequences of the pandemic on the economy, with the goal to ensure liquidity in the financial system and support the flow of credit.

Massive Stimulus Packages

In that regard, a swathe of measures have been put in place globally. The Federal Reserve has dropped interest rates to 0% and announced a first immediate help package to the tune of $700 billion, purchasing $500 billion of Treasury securities as well as $200 billion of mortgage-backed securities. The reserve requirements for banks and other depository institutions have been lowered[5] to zero percent, which allows them to accelerate the expansion of credit. Later, the Fed announced[6] for the first time that it would purchase these securities "in the amounts needed" – equaling the announcement of unlimited quantitative easing (QE). Its balance sheet has since grown[7] from $4.2 trillion to $5.2 trillion over the course of a month (or: by about $400k per second).

Illustration 1: The balance sheet of the Federal Reserve has continuously grown since 2008, and spiked in the past month from $4.2 trillion to $5.2 trillion.



Source: federalreserve.gov, Bitcoin Suisse Research.

On top of that, the U.S. Congress has passed a $2 trillion stimulus bill,[8] which includes a direct payment of $1'200 to each individual and direct support to all parts of the economy. The original version of this bill also included talk of a digital dollar, which has been removed in the final version though. Nonetheless, this has reignited[9] discussions about central bank digital currencies.

> "There is an infinite amount of cash at the Federal Reserve. We will do whatever we need to do to make sure there is enough cash in the banking system."
>
> - Neel Kashkari, Federal Reserve Bank of Minneapolis

Other central banks have taken measures of similar relative magnitude. The Bank of England has launched an initiative[10] to buy unlimited quantities of commercial paper. The European Central Bank has announced a €750 billion "Pandemic Emergency Purchase Programme", and lifted[11] its restriction not to buy more than one-third of a country's eligible bonds. This is in part done to provide ample liquidity to countries that now plan to ramp up their spending, which in turn will come with rising debt levels. These rising debt levels put central banks and governments in a difficult position: They will need to continue to help debtors rather than creditors to keep the house of cards of ballooning debt as stable as possible. As such, interest rates can be expected to remain low, or debt will need to be monetized by central banks – which in turn could shatter the trust in the currency that this debt was issued in.

How Does All This Relate to Cryptocurrencies?

Cryptocurrencies were invented as a form of money that does not require trust in a central authority, such as a government, not to debase it. The issuance of new cryptocurrency is programmatically defined – for Bitcoin, the issuance schedule converges towards 21 million as a hard maximum, and the majority (or 87%) of that has already been mined. The reason for issuing new coins is solely to ensure the security of the network and incentivize miners.

As such, cryptocurrencies are often seen as an inflation hedge – a safe haven not in the short term, but in the long run to protect against currency debasing. Gold as the classic inflation hedge and safe haven money has recovered from its drop two weeks ago. However, gold markets remained in distress, as supply chain disruptions have caused gold futures to decouple[12] from spot prices (which led the CME to launch new futures contracts[13] with more flexible physical delivery options).

Inflation vs. Deflation

Thus, it is crucial to look at both inflationary as well as deflationary pressures that are now present in the markets, especially since previous quantitative easing programs by central banks did not cause a spike in inflation. The consumer price index (CPI), which is one of the most widely watched measures for gauging inflation (alongside the producer price index PPI), has increased steadily by the Fed's desired range around 2% since the first quantitative easing program was started in the post-2008 financial crisis era. However, previous QE programs did help the stock markets go on a near-unprecedented bull run, indicating that much of the money may have ended up in financial assets. The situation at hand now has eliminated a lot of the wealth generated on paper, and the large negative demand shock due to the pandemic adds to the deflationary forces that counteract the printing presses put in motion by central banks. Also adding to deflation is the large drop in oil prices – oil is a major input cost to the economy, and that cost has been slashed by more than 50% in March.

Overall, the course of the pandemic and global economic crisis will define how inflationary and deflationary pressures compete against each other. In the case where inflation picks up or even goes into hyperinflationary overdrive, cryptocurrencies offer one of the few ways out of traditional fiat currencies and into an easily transferrable, hard money that is resistant to debasing.

Sources

1 https://leastauthority.com/static/publications/LeastAuthority-Ethereum-2.0-Specifications-Audit-Report.pdf

2 https://medium.com/baselineprotocol/baseline-protocol-opens-to-public-77601d1cf39d

3 Bitcoin Suisse Decrypt Series 2, "A Flight to Safety"

4 https://twitter.com/lenkiefer/status/1243166718924554240

5 https://www.federalreserve.gov/newsevents/pressreleases/monetary20200315b.htm

6 https://www.federalreserve.gov/newsevents/pressreleases/monetary20200323b.htm

7 https://www.federalreserve.gov/monetarypolicy/bst_recenttrends.htm

8 https://www.congress.gov/bill/116th-congress/senate-bill/3548/text

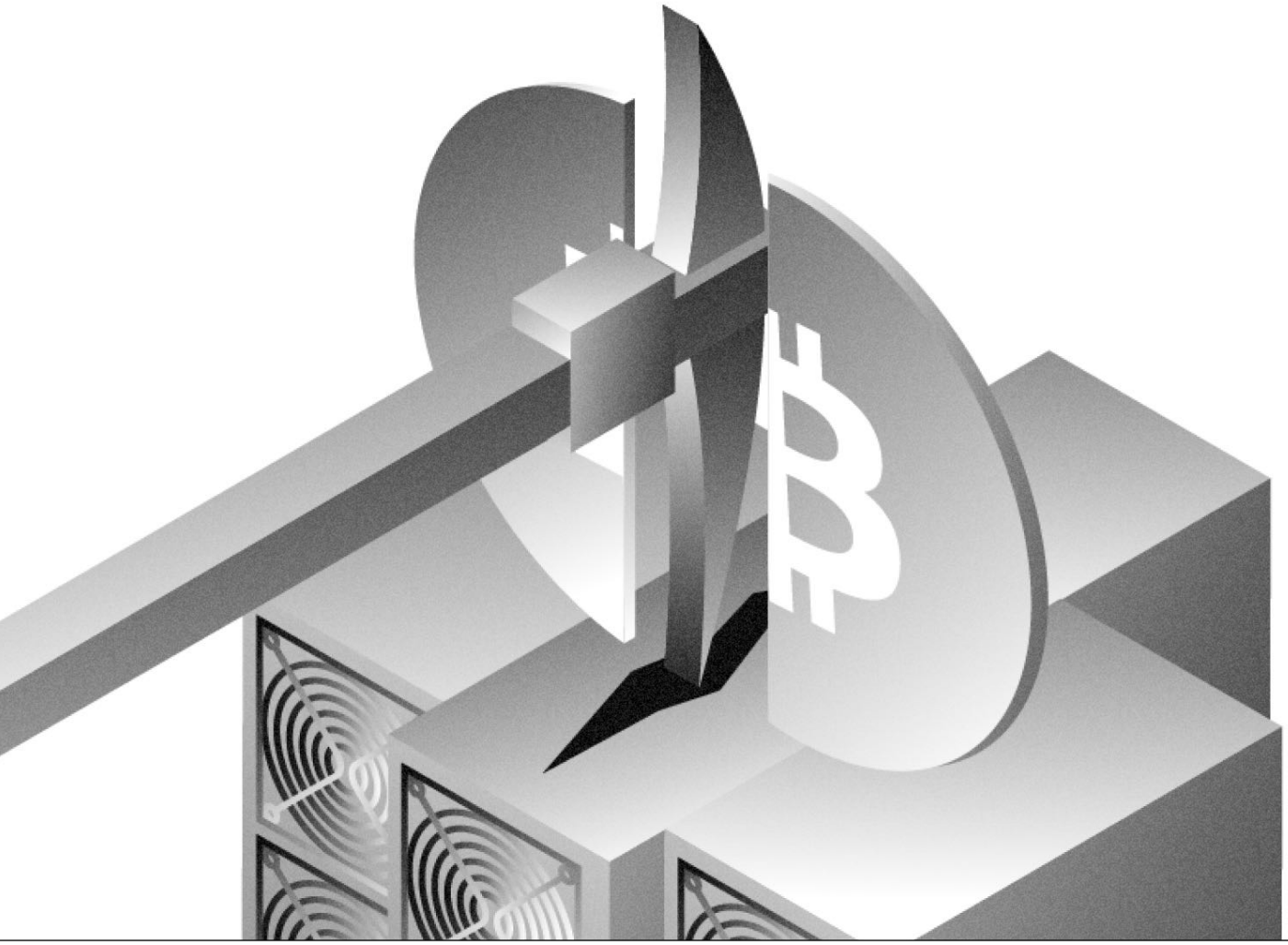
9 https://www.forbes.com/sites/jasonbrett/2020/03/23/new-coronavirus-stimulus-bill-introduces-digital-dollar-and-digital-dollar-wallets/#322fbe154bea

10 https://www.ft.com/content/bfb22e3e-6921-11ea-800d-da70cff6e4d3

11 https://www.ft.com/content/d775a99e-13b2-444e-8de5-fd2ec6caf4bf

12 https://www.zerohedge.com/news/2020-03-26/golds-gone-wild

13 https://www.cmegroup.com/media-room/press-releases/2020/3/24/cme_group_to_launchnewgoldfuturescontractwithexpandedflexibledel.html



Block Reward Halvings and the Rational Miner

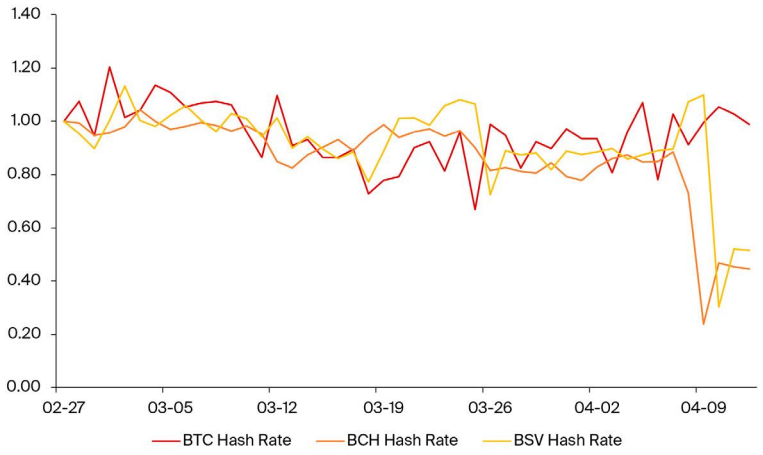
04

Bitcoin's third block reward halving in May will reshape the mining landscape and strongly affect the economics of mining. What will this mean for the supply of BTC coming from miners to the open markets?

Bitcoin's "halvening" event, which reduces the block reward from 12.5 BTC to 6.25 BTC, is coming closer and is projected to take place in about 28 days[1] on May 12. As one of the most anticipated events for Bitcoin in 2020,[2] the block reward halving will also have a major impact on the economics of mining – and since miners that are selling their coins (to cover capital and operational expenditures) are one of the main sources of supply in the open market, it will most likely also have an impact on Bitcoin's price. Currently, around $360 million worth of BTC are produced each month, and a significant portion of this needs to be sold to cover miners' operational expenses.

Bitcoin Cash[3] (BCH, a fork of Bitcoin) and Bitcoin SV[4] (BSV, a fork of Bitcoin Cash) already had their halving events last week, on April 8[5] and April 10,[6] respectively. As halving the reward strongly decreases the size of the cryptoeconomic pie to be distributed among miners, a logical conclusion is that many miners will switch to a coin with the same mining algorithm (in this case SHA-256) that did not have its halving yet. This can be observed for both BCH and BSV post-halvening, but did not influence their price much – both cryptocurrencies are still highly correlated with overall crypto market movements and have not decoupled from them.

Illustration 1: After their reward halvings, the hash rate of BCH (April 8) and BSV (April 10) significantly dropped, with some of the hash rate migrating to BTC. The hash rates for each chain were normalized to 1 for the end of February.



Source: coinmetrics.io, Bitcoin Suisse Research.

The impact on the hash rate of Bitcoin was minor, as the hash rate of BCH and BSV combined only make up about 5% of the total SHA-256 hash rate. The price drop by about -50% on "Black Thursday" (March 12) had a much stronger effect and led to a temporary decrease in Bitcoin's hash rate by about -30%. The hash rate has since largely recovered and sits at about 115 Exahashes per second (or around 86% of its all-time high at 133 EH/s)

A Miner's Breakeven Price

The large price drop on March 12 also meant that some miners are now operating below their breakeven cost to mine Bitcoin. The main factors involved in calculating the breakeven price are a) type of hardware used, and b) electricity price.

Miners using older hardware, e.g. the Antminer S9 (one of the more common mining rigs), were hit especially hard in comparison to users of newer, more expensive Antminer S17 hardware. The difference between the two mining machines is their chip size: While the S9 uses 16nm chips, the S17 has much smaller chips that are 7nm large. This translates to a hash rate output for the mining rig which is about 300% higher for the S17,[7] while the energy consumption is only increased by about 50%.

The other input to the profitability equation for miners, the electricity price, also varies a lot globally. While some miners have access to electricity at prices below $0.025/kWh, the majority is estimated to have access to energy at rates of $0.04-0.05/kWh.[8]

After the halvening, miners will need to excel in at least one of the two categories – either employ the newest hardware that produces more hash rate per kWh, or have access to some of the cheapest energy worldwide. Miners that do neither of the two will likely become unprofitable, meaning their breakeven cost per BTC will be above market prices, and they will be pushed out of business.

Miner Capitulation

While turning mining gear on and off is a frictionless process for hobbyist miners, that is not the case for professional mining businesses. Such setups can have several aspects that delay simply shutting off the mining gear. For example, they rely on low electricity rates that were agreed upon with local energy producers in return for constantly using a certain amount of power. Thus, instead of immediately turning off mining gear, professional miners finance their operation through their Bitcoin treasuries (that were accumulated during profitable periods) to stay in business when Bitcoin trades below their breakeven price.

Thus, lower prices may actually accelerate sell-offs, since the selling pressure from miners – over longer timeframes the main source of selling pressure for Bitcoin – increases, as they need to sell more than usual (and even more than they mine!) to cover operational costs. This continues at most until their Bitcoin treasuries are depleted and the miners are forced to capitulate.

When these miners capitulate, the hash rate drops, and Bitcoin's mining difficulty adjusts. This will make the remaining miners more profitable, since the daily output of BTC is constant (1'800 BTC now, 900 BTC post-halvening), but then gets distributed to a smaller set of more efficient miners with a lower breakeven Bitcoin price.

With this, the next part of the cycle begins: Newly mined BTC now go to the pockets of highly efficient miners that need to sell less to cover their operational expenses, meaning they can in principle retain more BTC and grow their Bitcoin treasury more quickly, which in turn also reduces the selling pressure in the open market. If price reacts to this diminished selling pressure and increases, this will create a positive feedback loop for miners that survived and enable them to sell even less (while still covering expenses), accelerating the upwards price movement. Such feedback loops may have played a significant role in the price rallies after the previous halvenings in 2012 and 2016.

While miner behavior in the markets is certainly not the only variable that influences price, it is important to understand the mechanics behind it: Low market prices or reward halvings initially increase selling pressure, but then strongly reduce it after miners capitulate. As such, one question remains: How can this miner capitulation be identified?

Spotting Miner Capitulation

As outlined above, the halving will lead to another wave of miners that have to capitulate, especially those that use older hardware or have high electricity cost. Indicators based on the hash rate were popularized in 2019 by various[9] researchers;[10] one of these indicators is called hash ribbons. Hash ribbons[11] are a simple 1- and 2-month moving average (SMA) of Bitcoin's hash rate. Historically, buying Bitcoin after the hash rate has started to recover after a miner capitulation (as indicated by the 1-month SMA moving above the 2-month SMA) has yielded great results.

Illustration 2: Hash ribbons indicate miner capitulation (grey circles) as well as recovery (blue and green circles). Previous halvings in 2012 and 2016 are plotted with red bars in the hash ribbon indicator.

Source: tradingview.com.

As was seen already in the hash rate chart above, the most recent drop from $10.5k down to a bottom below $4k has led to some miners capitulating, which is also indicated by the hash ribbons. This will happen again after the halvening in May. Bitcoin's ingenious mechanism of difficulty adjustments ensures, however, that the remaining miners will still be profitable. Thus, the hash rate is expected to recover also after the reduction of the block reward – potentially offering an opportunity for investors looking to enter the market.

Sources

1 https://www.bitcoinblockhalf.com/

2 https://www.bitcoinsuisse.com/outlook/bitcoin-in-2020-halving-the-block-reward

3 https://www.bitcoinsuisse.com/fundamentals/what-is-bitcoin-cash

4 https://www.bitcoinsuisse.com/fundamentals/what-is-bitcoin-sv

5 https://blockchair.com/bitcoin-cash/block/630000

6 https://blockchair.com/bitcoin-sv/block/630000

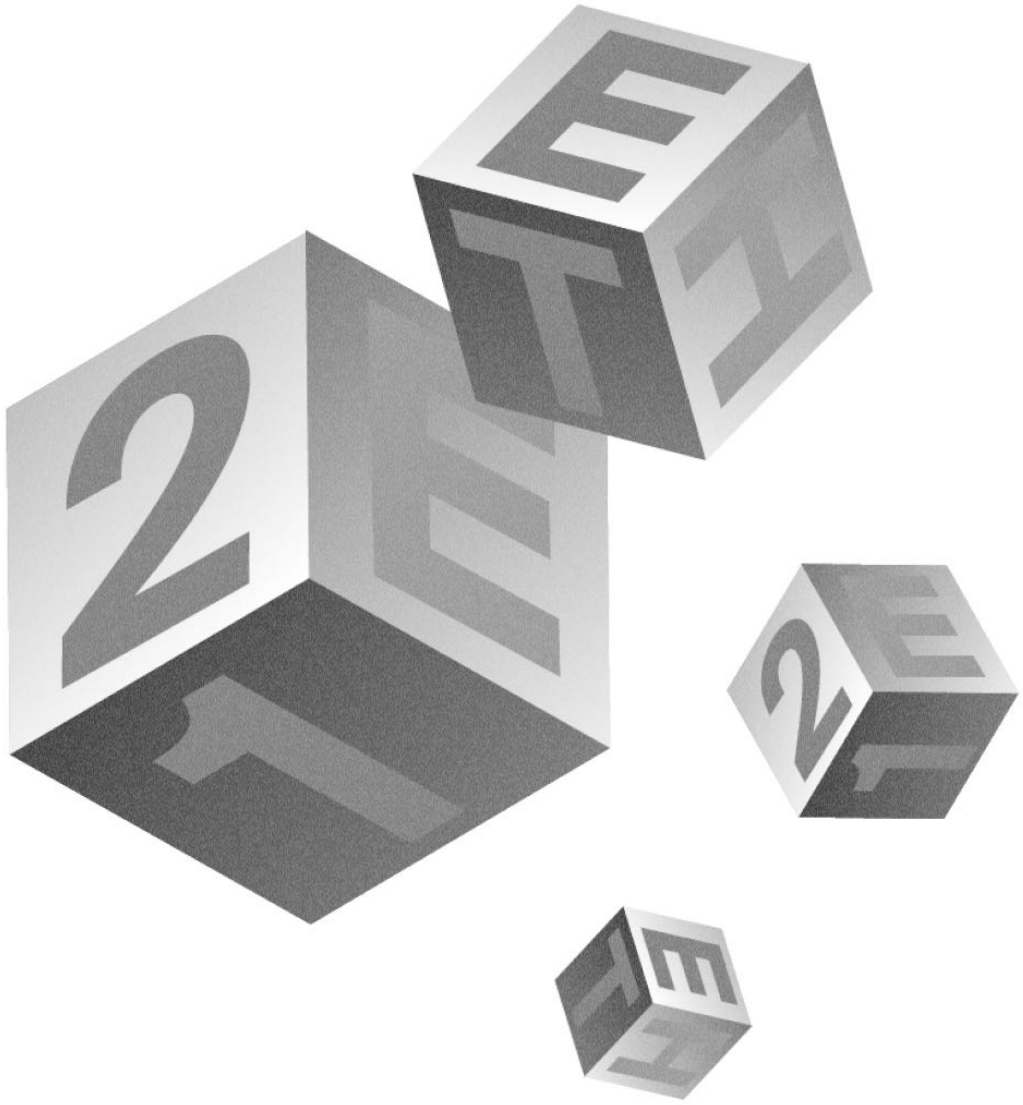
7 https://www.blockwaresolutions.com/research-and-publications/2020-halving-analysis

8 https://coinsharesgroup.com/research/bitcoin-mining-network-december-2019

9 https://medium.com/capriole/bitcoin-bottom-fishing-with-miner-capitulation-ad693b8a6519

10 https://woobull.com/introducing-the-difficulty-ribbon-the-best-times-to-buy-bitcoin/

11 https://medium.com/capriole/hash-ribbons-bitcoin-bottoms-60da13095836


1
2
3

Ethereum's Path to Serenity

Ethereum is inching closer to one of its most anticipated events: the launch of Ethereum 2. The key factor to look out for that could signal an imminent launch is a multi-client testnet that runs smoothly for 2-3 months. Meanwhile, stablecoins are dominating value transfer on the current Ethereum chain.

Ethereum's "Serenity", the last stage outlined in the launch process already in 2015,[1] is getting closer. The proposal, whose major aspect is the change from Proof-of-Work to Proof-of-Stake, has taken on different shapes over the years and Ethereum core developers have been continuously working to improve it. Most commonly, this phase is now known as Ethereum 2 (or Ethereum 2.0).

Originally, the hope was to have Proof-of-Stake already implemented by now. However, architectural changes on the protocol level and unforeseen research challenges repeatedly delayed the launch. Another reason for the constant delays is that Ethereum has quickly transitioned from a pure experiment that hadn't accrued much value (2015-2016) to a global blockchain infrastructure that stored billions of dollars' worth of cryptocurrencies (mid-2017). Upgrading code that secures this many assets requires utmost care.

These delays may also have been one of the reasons for Ether's relative underperformance compared to Bitcoin over the past two years.

The question is now: How much of the risk that Ethereum 2 does not launch soon is priced into the current price of ETH? While

assessing this exactly is impossible and will only be known after the fact (i.e., after Ethereum 2 has launched), it is reasonable to assume that at least some of ETH's bear market versus Bitcoin can be ascribed to the delays of Ethereum 2.

Ethereum 2 in 2020?

Some developers of Ethereum 2 are "95% confident"[2] that the launch will happen this year. There is one key factor that investors should look out for to get a more accurate grasp of when the launch is actually close: a multi-client testnet that runs smoothly for 2-3 months.

Testnets for Ethereum 2 have been running for quite some time now and have already been integrated to various block explorers.[3] In another milestone, Prysmatic Labs recently introduced their Topaz testnet that features the full Ethereum 2 mainnet configuration.[4] While this was not the multi-client testnet yet, it is capable of forming the base for multi-client experimentations. Topaz has been running with minor client bugs since its launch on April 18. Last but not least, just yesterday evening, a first multi-client testnet called "Schlesi" that is based on a slightly modified mainnet configuration has had its genesis event and successfully hosted both Prysm and Lighthouse validators.[5]

As outlined in the Outlook2020 report, Ethereum 2 will also have an impact on the supply of ETH.[6] Initially, the annual issuance rate of new Ether will increase to around 5-6% – but once Ethereum 2 can be used to secure the current Ethereum 1 chain, issuance will drop dramatically, most likely to below 1%. Given the current ETH issuance rate of around 4.8%, this would equal a "double halving" in terms of new supply coming to the market. The effect of this would most likely differ from halvings in Bitcoin,[7] since the ETH issuance reduction comes with the switch to Proof-of-Stake and hence validators instead of miners. This fundamentally changes the incentive structures of the blockchain.

Higher Volatility and a Liquidity Premium

After the launch of the deposit contract and the beacon chain of Ethereum 2, ETH that have been sent to the deposit contract will not immediately be transferable in the early phases of Ethereum 2. This will have an effect on the markets – how much exactly depends to some extent on how much ETH will be locked up in staking. Generous estimates assume that around 30 million ETH will be staked fairly quickly after the launch.

However, the initial market influence might be smaller than some people expect. Investors willing to stake large amounts at the beginning might not have been active market participants, but rather passive holders. In this case, whether the ETH are held in a cold storage wallet on Ethereum 1 or in validator nodes on Ethereum 2 does not matter. On the other hand, if active market participants decide to move their ETH to staking, this might decrease liquidity in the primary market as well as in the lending markets, driving ETH lending rates up. One consequence of the decreased liquidity could be an increase in volatility.

Due to the initial non-transferability of ETH2, it is also conceivable that an ETH2 futures market will develop. ETH1 and ETH2 do not need to trade at the same price until transferability and full convertibility is established. In fact, in such a futures market it is highly likely that investors demand a liquidity premium for ETH2 – meaning that ETH2 is initially cheaper than ETH1 due to the forced lockup period of ETH2 until the later phases of Ethereum 2. Such liquidity premia are well-known, for example in the yield curves of traditional bond markets or from token sales discounts that are tied to vesting periods.

Rise of Stablecoins on Ethereum 1

Stablecoins had one of their best years so far in 2020, and stablecoin growth is one of the trends to watch in the crypto space during this year.[8] Their total market cap has surpassed $8 billion, and they contributed majorly to total value transfers on Ethereum reaching parity with that of Bitcoin.[9] Today, about 80% of the value transferred on Ethereum involves a stablecoin. This justifies revisiting a key on-chain metric called “Network Value to Transaction volume”, or NVT for short. Often called the “crypto P/E ratio”, NVT is a ratio between the market capitalization of a cryptocurrency and the transaction volume of that cryptocurrency.[10] The idea behind NVT is to make sense of a cryptocurrency’s valuation in light of how much value is actually transferred through the network.

Its most used form today involves an adapted form that smooths transaction volumes with a 90-day moving average[11] to eliminate spikes that are related to temporary price spikes, since such price spikes often coincide with increased transaction activity to and from exchanges.

Illustration 2: Ethereum's NVT ratio is below Bitcoin's, and even more pronouncedly so if value transferred in the largest ERC-20 stablecoin USDT is also considered.

Source: cryptodatadownload.com, Bitcoin Suisse Research.

The question is now: How much of the risk that Ethereum 2 does not launch soon is priced into the current price of ETH? While assessing this exactly is impossible and will only be known after the fact (i.e., after Ethereum 2 has launched), it is reasonable to assume that at least some of ETH's bear market versus Bitcoin can be ascribed to the delays of Ethereum 2.

Ethereum 2 in 2020?

Some developers of Ethereum 2 are "95% confident" that the launch will happen this year. There is one key factor that investors should look out for to get a more accurate grasp of when the launch is actually close: a multi-client testnet that runs smoothly for 2-3 months.

Testnets for Ethereum 2 have been running for quite some time now and have already been integrated to various block explorers. In another milestone, Prysmatic Labs recently introduced their Topaz testnet that features the full Ethereum 2 mainnet configuration. While this was not the multi-client testnet yet, it is capable of forming the base for multi-client experimentations. Topaz has been running with minor client bugs since its launch on April 18. Last but not least, just yesterday evening, a first multi-client testnet called "Schlesi" that is based on a slightly modified mainnet configuration has had its genesis event and successfully hosted both Prysm and Lighthouse validators.

As outlined in the Outlook2020 report, Ethereum 2 will also have an impact on the supply of ETH. Initially, the annual issuance rate of new Ether will increase to around 5-6% – but once Ethereum 2 can be used to secure the current Ethereum 1 chain, issuance will drop dramatically, most likely to below 1%.

Given the current ETH issuance rate of around 4.8%, this would equal a “double halving” in terms of new supply coming to the market. The effect of this would most likely differ from halvings in Bitcoin, since the ETH issuance reduction comes with the switch to Proof-of-Stake and hence validators instead of miners. This fundamentally changes the incentive structures of the blockchain.

Higher Volatility and a Liquidity Premium

After the launch of the deposit contract and the beacon chain of Ethereum 2, ETH that have been sent to the deposit contract will not immediately be transferable in the early phases of Ethereum 2. This will have an effect on the markets – how much exactly depends to some extent on how much ETH will be locked up in staking. Generous estimates assume that around 30 million ETH will be staked fairly quickly after the launch.

However, the initial market influence might be smaller than some people expect. Investors willing to stake large amounts at the beginning might not have been active market participants, but rather passive holders. In this case, whether the ETH are held in a cold storage wallet on Ethereum 1 or in validator nodes on Ethereum 2 does not matter. On the other hand, if active market participants decide to move their ETH to staking, this might decrease liquidity in the primary market as well as in the lending markets, driving ETH lending rates up. One consequence of the decreased liquidity could be an increase in volatility.

Due to the initial non-transferability of ETH2, it is also conceivable that an ETH2 futures market will develop. ETH1 and ETH2 do not need to trade at the same price until transferability and full convertibility is established. In fact, in such a futures market it is highly likely that investors demand a liquidity premium for ETH2 – meaning that ETH2 is initially cheaper than ETH1 due to the forced lockup period of ETH2 until the later phases of Ethereum 2. Such liquidity premia are well-known, for example in the yield curves of traditional bond markets or from token sales discounts that are tied to vesting periods.

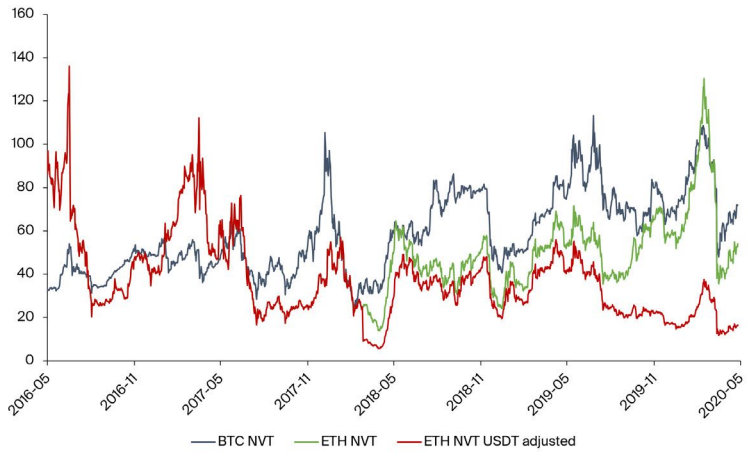
Rise of Stablecoins on Ethereum 1

Stablecoins had one of their best years so far in 2020, and stablecoin growth is one of the trends to watch in the crypto space during this year. Their total market cap has surpassed $8 billion, and they contributed majorly to total value transfers on Ethereum reaching parity with that of Bitcoin. Today, about 80% of the value transferred on Ethereum involves a stablecoin. This

justifies revisiting a key on-chain metric called “Network Value to Transaction volume”, or NVT for short. Often called the “crypto P/E ratio”, NVT is a ratio between the market capitalization of a cryptocurrency and the transaction volume of that cryptocurrency.The idea behind NVT is to make sense of a cryptocurrency’s valuation in light of how much value is actually transferred through the network.

Its most used form today involves an adapted form that smooths transaction volumes with a 90-day moving average to eliminate spikes that are related to temporary price spikes, since such price spikes often coincide with increased transaction activity to and from exchanges.

Illustration 2: Ethereum’s NVT ratio is below Bitcoin’s, and even more pronouncedly so if value transferred in the largest ERC-20 stablecoin USDT is also considered.



Source: coinmetrics.io, aleth.io, Bitcoin Suisse Research.

Typical NVT calculations do not take token transfers into account,[12] but given their recent significance, it makes sense to add at least the largest ERC-20 based stablecoin USDT into account. While USDT was originally launched on Bitcoin’s Omni Layer, Tether has migrated most of it to Ethereum, a process which started in early 2018.[13] The NVT adjusted for USDT (red line in Illustration 2) shows that based on this metric, Ethereum is attractively valued in comparison to Bitcoin.

The rise in stablecoin activity also brings up the topic of whether a “cryptodollar” could have a macroeconomic importance.[14] The current global crisis has shown that US dollars are in high demand. This is because much of the world’s debt is denominated in USD ever since it emerged as the dominant reserve currency after WW2.

The USD infrastructure on Ethereum fostered by stablecoins thrives, and one potentially large use case of Ethereum today

and in the future could be to facilitate access to dollars as well as cheap cross-border payments. For this to reach a massive scale though, the increased throughput of Ethereum 2 of multiple thousand transactions per second is needed.

Sources

1 https://blog.ethereum.org/2015/03/03/ethereum-launch-process/

2 https://www.reddit.com/r/ethereum/comments/ez972u/ama_we_are_the_eth_20_research_team_pt_3/

3 https://beacon.etherscan.io/

4 https://medium.com/prysmatic-labs/introducing-topaz-testnet-8e8a4e00a700

5 https://twitter.com/a4fri/status/1254770386186584196

6 https://www.bitcoinsuisse.com/outlook/ethereum-and-its-transition-to-ethereum-2

7 Bitcoin Suisse Decrypt Series 2, "Block Reward Halvings and the Rational Miner"

8 https://www.bitcoinsuisse.com/outlook/trends-to-watch-in-2020

9 https://twitter.com/RyanWatkins_/status/1250427795483684867

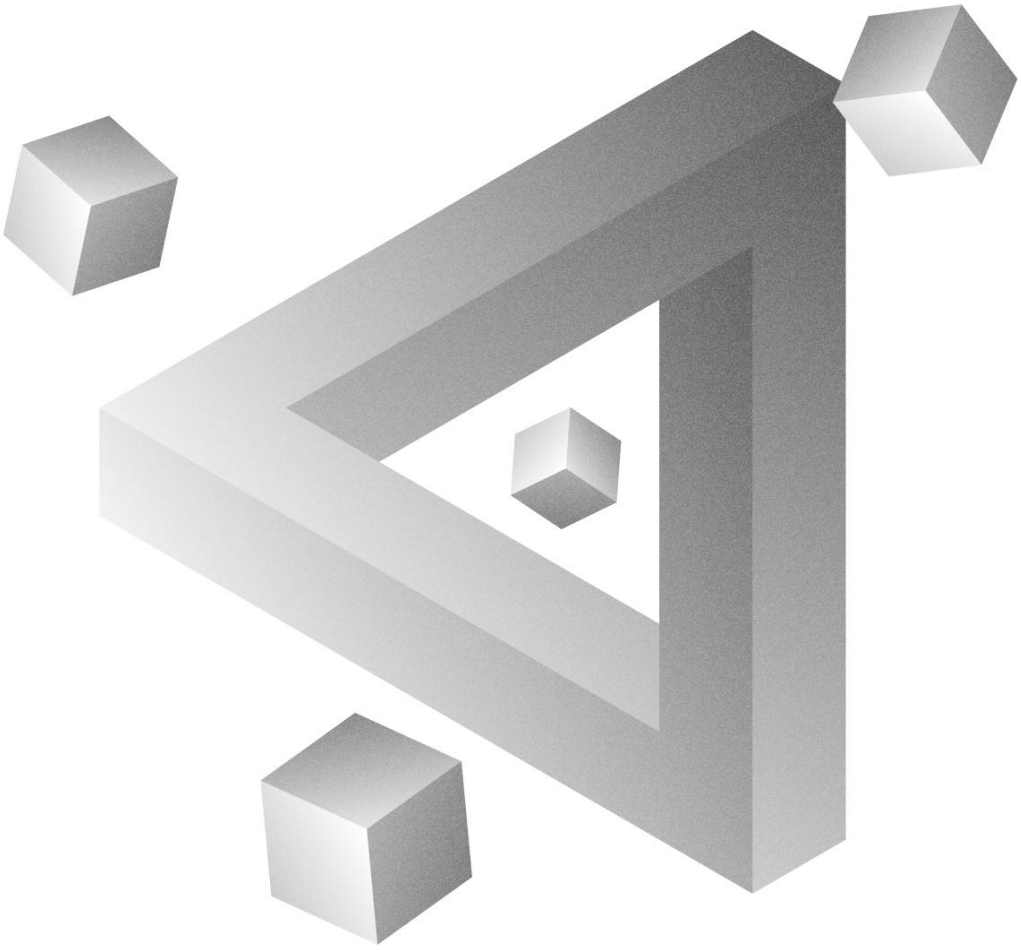
10 https://twitter.com/RyanWatkins_/status/1250427801225711625

11 https://medium.com/cryptolab/https-medium-com-kalichkin-rethinking-nvt-ratio-2cf810df0ab0

12 https://consensys.net/blog/blockchain-explained/types-of-ethereum-data-series-ethereum-network-data/

13 https://wallet.tether.to/transparency

14 https://unexpected-values.com/crypto-dollars/



Bitcoin SV: Back to Genesis

Since Bitcoin Satoshi Vision came into existence in November 2018, a lot has happened on the chain, from the establishment of decentralized social media to simplified payment solutions. Miners – or transaction processors – will play a key role moving forward.

Bitcoin Satoshi Vision, the fifth largest cryptocurrency by market capitalization (excluding Tether), was created as a fork of Bitcoin Cash (which is a fork of BTC) on November 15, 2018 at block number 556766. It came into existence due to disagreements in the Bitcoin Cash community on, for example, how to handle scalability in the future, namely what the block size limit should be. While Bitcoin Cash kept a 32 MB limit, Bitcoin SV supporters opted to increase the limit to 128 MB and more.

The BSV Mindset

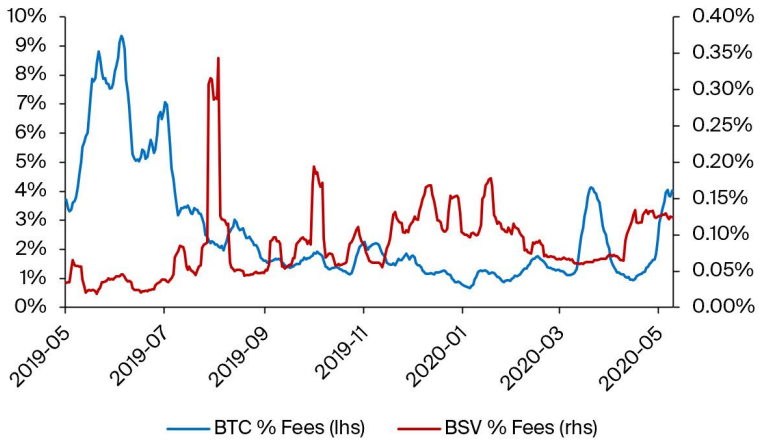
In accordance with the name of the cryptocurrency, one of the main goals of BSV is to remain as close to the protocol specification as outlined in the original Bitcoin whitepaper as possible. The protocol is not supposed to do something special, but instead provide a stable, consistent base protocol to build on – similar to how IPv4, deployed in 1983, still routes most of today's internet traffic. Such a base protocol was reinstated with the Genesis hard fork that occurred in February of this year. The Genesis hard fork, among other changes, restored the functionality of OP_RETURN in the Bitcoin scripting language, which allows to terminate scripts early. Additionally, pay-to-script-hash (P2SH), which is often used in BTC for multi-signature wallets, is no longer available as an option for new outputs. BSV's

last hard fork will be called Chronicle and mark the move back to Bitcoin's original difficulty adjustment algorithm (every 2016 blocks) instead of the one inherited from BCH, which adjusts the difficulty for each block based on a moving average of block times in the last 144 blocks.

For BSV supporters, accountability is a key functionality and one of the arguments against employing second-layer solutions such as the Lightning Network. By storing a full record of all transactions directly on-chain, the blockchain aims to enable regulatory compliance. Storing everything on-chain will require enough block space, which is why scalability through large blocks is so important for BSV. The largest block[1] mined so far on BSV was 256 MB large and added to the chain in July 2019 during a mainnet stress test. In the long run, the goal is to produce terabyte-sized blocks and overcome potential propagation issues that might arise. The idea is that such an abundant amount of block space would impose no limits on users and strengthen the peer-to-peer model outlined in the Bitcoin whitepaper. Instead of governing how the chain should be used, the free market would decide.

This scalability approach also has the longer-term goal to shift miner revenues from block rewards to transaction fees. While in BTC, individual transactions are supposed to become more valuable to the user, e.g. opening a channel in the Lightning Network that could then be used many times, BSV is instead focusing on growing the overall transaction volume to increase revenues from fees.

Illustration 1: The percentage of miner revenue coming from fees is currently low for both BTC and BSV. Data smoothed with a 7-day moving average.



Source: bitinfocharts.com, Bitcoin Suisse Research.

Overall, fees have so far only accounted for small percentages of the overall miner revenue. BSV's goal is to change that through a new mining model.

Transaction Processors

To compensate for the block subsidy, miners would – after this year's reward halving – need to make up for 6.25 BTC or BSV per day. With BSV's plan of terabyte blocks, this could be achieved by having around 1 billion transactions per day, at low per-transaction fees of <1 satoshi/byte.

The new model of viewing miners as transaction processors[2] means that miners have predefined volume based contracts with parties that are interested in conducting a lot of transactions each day. The miner promises certain settlement times for transactions, i.e. inclusion in a block for example within 1 hour, 4 hours or by end of day. This is an improvement over current settlement processes in the financial system, which typically takes two days ("t+2 settlement"). Such an offering would also open up the possibility for businesses to pay transaction processors in traditional fiat currencies, removing the need to take on price volatility risk.

"The current system where every user is a network node is not the intended configuration for large scale. That would be like every Usenet user runs their own NNTP server. The design supports letting users just be users. The more burden it is to run a node, the fewer nodes there will be. Those few nodes will be big server farms. The rest will be client nodes that only do transactions and don't generate."

- Satoshi Nakamoto

Miners, or transaction processors, would need to operate large data centers under the new model to handle the large blocks and amount of transactions. The idea is that these data centers could also be rented out and serve as a new form of cloud com-

puting – the monetary incentive for carrying out the calculations could directly be settled on-chain.

The miners would also play a major role in providing the infrastructure to support new applications powered by the BSV blockchain.

Developments on Bitcoin Satoshi Vision

While much of the public discussions around BSV are focused on "crypto-political" issues, there is a lot of development going on under the hood.

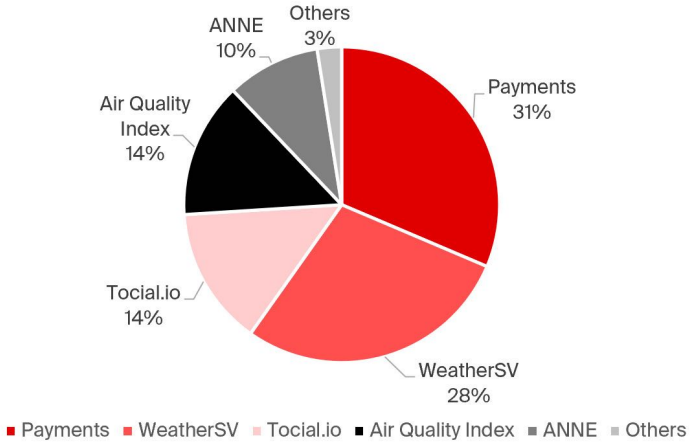


Illustration 2: The largest amount of transactions on BSV are related to payments and WeatherSV, a weather data collection service. Snapshot on May 11, 2020.

Source: bitcoinblocks.live, Bitcoin Suisse Research.

While most transactions are related to payments (31%), WeatherSV[3] comes in as a close second (28%), and Air Quality Index (AQI)[4] as well as Tocial.io[5] share the third place (14% each). WeatherSV and AQI are recording environmental data on BSV, whereas Tocial is a decentralized social network launched in March of this year with a focus on image sharing. The last application that generates significant transaction volume is ANNE[6] (10%), which is a decentralized data storage protocol. In the future, data storage services could pick up even more in volume, e.g. due to collaborations such as the one with EHR Data[7] to digitize healthcare data.

The data structure protocol that underlies such new services and businesses is the Metanet. In simple terms, the Metanet aims to be the "Internet of Value". Information is openly available but linked to a monetary premium – tackling some of the obstacles the internet faces today, such as spam and bots in social media platforms or the need for intermediaries to transfer value.

The concept of linking attention to content with value is implemented in social media platform Twetch.[8] Although the general feeling is similar to Twitter, the connection to a value transfer system offers some benefits. Simple actions such as following someone, creating a new post, liking a post etc. each come at a small price tag (in the range of $0.01-$0.10), and a tipping system for variable amounts is included through Moneybutton,[9] a user-friendly API service to the BSV blockchain. These payments go directly to the content creator, with Twetch taking a small cut for providing the infrastructure. This setup has the goal to increase accountability and incentivize the creation of content that is perceived as valuable by many, and hence to reduce spam.

As a last ingredient to the "Internet of Value", Pixel Wallet[10] is working on a BSV-based digital identity system and KYC solution called VOAM – which stands for "verify once, authenticate many". The system hides encrypted identity data inside images, and only the user has the key to decrypt the data and knows which image the data is stored in. In the future, this should enable more selective and only authorized access to user data instead of the data silos that large corporations possess nowadays.

Conclusion

Overall, the direction that BSV takes for its base layer – e.g. aiming to serve as a regulatory compliant infrastructure provider for big corporations – compared to BTC strongly reflects the different mindset between the two communities. In spite of the ongoing, at times heated and unconstructive discussion of which approach is "better", it is worth to take a look through the social media-driven smokescreen and pay attention to the diverse developments happening right now. In the end, the free market will be the judge on how to value each concept.

Sources

1 https://blockchair.com/bitcoin-sv/block/593161

2 https://www.taal.com/blog/2020/what-is-the-transactional-processing-business-model-for-bitcoin/

3 https://weathersv.app/

4 https://twitter.com/dailyzhou/status/1186689277893074944

5 https://tocial.io/

6 https://medium.com/@bsmith12251960/a-n-n-e-the-alpha-testing-begins-545f809c6129

7 https://coingeek.com/ehr-data-to-migrate-41-years-of-healthcare-data-to-bitcoin-sv/

8 https://twetch.app/

9 https://www.moneybutton.com/

10 https://pixelwallet.io/

07

Interoperability between Blockchains

The future of blockchains is interconnected. Just like the Internet, blockchains will not be isolated systems operating on their own, but instead form a global network. What is needed to achieve this? And which approaches are being tried today?

Interoperability is one of the trends to watch[1] of this year. In principle, interoperability means nothing more than the ability to communicate between different computer systems and exchange data or information. This may sound like a simple task, but in practice, there are many obstacles to overcome, such as varying standards for code, or – more specific to the blockchain world – different consensus algorithms.
However, interoperability is crucial to avoid a segmented digital infrastructure. The blockchain infrastructure of today is mostly siloed, and even something as seemingly simple as a trustless value transfer between the two largest crypto-ecosystems (Bitcoin and Ethereum) is still impossible,[2] although efforts such as REN[3] or tBTC[4] are working towards this.

Interoperable Means Frictionless

In the future, end users such as businesses that employ blockchains for their internal tracking, payments or various other systems will demand interoperable solutions – just how today, it is seen as self-evident that merchants and ATMs are capable of accepting different brands of credit card standards. Interoperable solutions are cheaper: A specific integration that only works with one particular blockchain will lead to friction and costs once multiple companies try to implement their shared business logic (such as automated ordering and payment of parts between a manufacturer and its supplier).
Interoperability is also important to ensure the freedom of platform choice, without too many restrictions that need to be considered. Certain blockchains may be optimized for certain use cases, and those chains will need to be able to communicate with each other.

Creation of Standards

Standards have always been a crucial ingredient to achieving interoperability. The Internet relies on them – be it through the TCP/IP (Transmission Control Protocol / Internet Protocol) base layer or through unified API (Application Programming Interface) endpoints with standards such as FIX or REST. These ensure a coherent layering of applications within the internet.

Blockchains will need similar standards to guide developers and users. Efforts in this direction are already underway, for example through consortia like the Enterprise Ethereum Alliance.[5] Examples of already existing standards in blockchain technology would be the various token standards (such as the widely known ERC-20 standard for fungible tokens).

Types of Interoperability

There are three major types of interoperability. The first is the interoperability between private and public blockchains. The blockchain infrastructure of a near-term future may involve both private and public blockchains, which serve different needs. Still, it is likely that these will need to communicate – and this needs to be carefully addressed even if the private and public blockchains share much of the underlying code base (such as the private Quorum implementation of Ethereum and the public mainnet). In this case, standards for developers are of paramount importance. The second type is interoperability between different public blockchains. These may be built on entirely different fundamentals, all the way down to the cryptographic core of a chain (such as signature algorithms). As mentioned above, today's blockchains infrastructure is siloed.

However, there are blockchains that aim to solve this by functioning as bridges between other blockchains, such as Polkadot[6] or Cosmos[7] (see below). Both feature some kind of a central chain that will connect to many others. This architecture is likely to emerge more prominently in the future for one simple reason: If there are 100 different, specialized blockchains that need to communicate with each other and they all establish individual connections to all other blockchains, the number of connections would quickly grow very large. In this example, it would take about 10'000 connections if each needed to be linked individually. Therefore, a hub-like structure makes sense.

The third aspect of interoperability is the one with legacy systems, such as the traditional financial infrastructure or current supply chain management systems. In this case, being interoperable is mostly an oracle problem – meaning the transfer of data from legacy systems to the new blockchain-based system. Chainlink[8] presents a potential solution to this, and is working together[9] with SWIFT on developing an optimal integration. Additionally, the Baseline Protocol (supported by Microsoft, EY and ConsenSys) recently showcased[10] the interaction of ERP systems with blockchain technology.

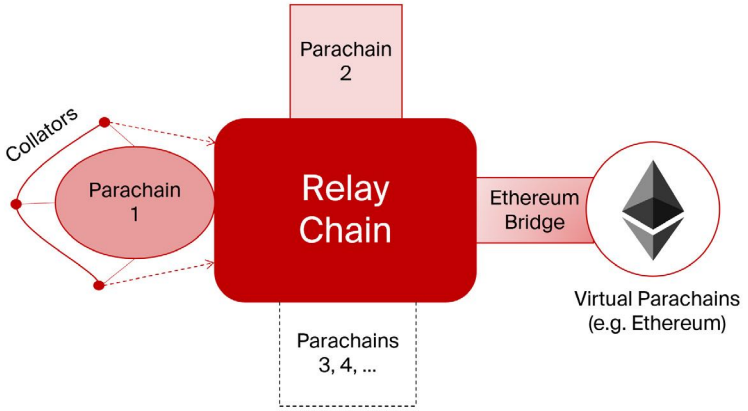
Blockchains Focused on Interoperability: Polkadot and Cosmos

There are currently two main contenders in the game of "blockchain for blockchains" – Polkadot and Cosmos.

Polkadot

The basic structure of Polkadot involves a relay chain and parachains.[11] The relay chain is the main chain of Polkadot. It provides a pooled security guarantee parachains and has a game-theoretical setup that encourages maximal DOT (the native token of Polkadot) decentralization.[12] Additionally, the relay chain handles the overall network governance.

Illustration 1: Simplified structure of Polkadot. Besides the native parachains, other blockchains can be connected through a bridge.



Source: Polkadot Whitepaper, Bitcoin Suisse Research.

Parachains conduct most of the actual computations on Polkadot. They construct and propose blocks to validators on the relay chain – or more precisely, collators which collect information about the state of the parachain do. Parachains are largely unrestricted in terms of design and only need to be verifiable by the relay chain. They can be specialized, such as for high transaction throughput or for strong privacy guarantees. The number of slots for parachains on top of the relay chains is limited, though, and chains that would like to become a parachain need to bid on the slot.[13]

Other chains can be integrated through bridges, which are adapted to a type of chain (e.g. Bitcoin or Ethereum). These bridges have the goal to make them compatible to the code architecture of Polkadot. Through such bridges, any chain can become a “virtual” parachain of Polkadot.

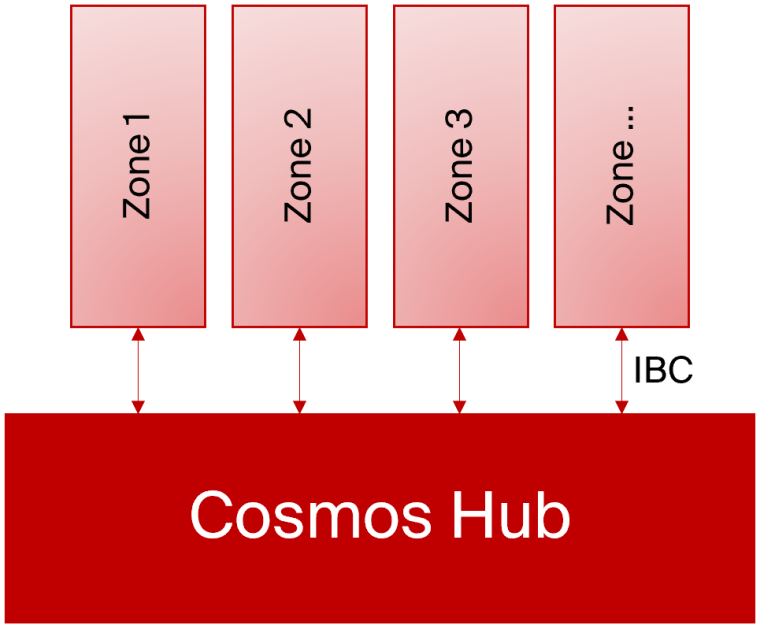
Interoperability between parachains is addressed through a Cross-Chain Messaging Protocol (XCMP). This allows parachains to communicate, and the protocol will handle transfers of data or assets (such as tokens).

Illustration 2: Simplified structure of Cosmos hubs and zones. They communicate with each other through the IBC protocol.

Cosmos

Cosmos' way to address interoperability is the Inter-Blockchain Communication (IBC) protocol, which allows two chains to have light clients of the other chain.

A simplified illustration of a use case would be the transfer of ETH to Tezos. A smart contract on each chain allows submitting block headers from the other chain, which in turn allows to prove that ETH or a token has been locked up on Ethereum and can be issued on Tezos (or vice versa), ensuring that a 1:1 backing and peg remains at all times. This is different from an atomic swap, because value actually crosses from one chain to the other.



Source: Polkadot Whitepaper, Bitcoin Suisse Research.

A key component of Cosmos are hubs (such as the Cosmos Hub) and zones.[14] These communicate with each other through the IBC protocol. The Cosmos Hub connects to many zones (or chains) and in principle allows connecting chains to outsource their security guarantees – although in contrast to Polkadot, this is not mandatory. This can be done for a fee and using ATOMs, the native token of Cosmos. In the future, the Cosmos Hub does not need to be at the center of the Cosmos network, and other hubs may emerge. In fact, there already are other hubs such as the Iris hub, [15]which focuses on services and enterprises.

In addition, the concept of peg zones[16] allows to connect to blockchains with fundamentally different architecture (e.g. consensus model) than Cosmos, such as Bitcoin. Validators of a

peg zone translate between the architectures of the two blockchains and make the chain attached through the zone compatible with the Cosmos IBC protocol.

Interoperability – a Solved Problem?

This year has shown considerable progress towards a more connected blockchain world. With the highly anticipated launch of Polkadot,[17] as well as an incentivized testnet[18] for Cosmos' IBC protocol (called "Game of Zones"), it is expected that interoperability will remain a hot topic for 2020.

How well the issue has been addressed so far, and how ready the blockchain industry is for adopting to an unwalled infrastructure where information and value can be transmitted seamlessly not only on single chains, but also across chains, will slowly come to light as overall blockchain adoption progresses.

In the long run, interoperable solutions are not a luxury, but a necessity. The blockchain landscape will evolve towards this, just like the Internet is no longer a small set of poorly connected servers – but a global and tightly intertwined network.

Sources

1 https://www.bitcoinsuisse.com/outlook/trends-to-watch-in-2020

2 https://twitter.com/VitalikButerin/status/1242553658195271681

3 https://medium.com/renproject/how-ren-vm-actually-works-c2f76a2630c4

4 https://tbtc.network/

5 https://entethalliance.org/

6 https://polkadot.network/

7 https://cosmos.network/

8 https://chain.link/

9 https://www.twitter.com/TheMaxZab/status/1230012953002487808

10 https://oasis-open-projects.org/open-source-proof-of-concept-ethereum-mainnet/

11 https://polkadot.network/PolkaDotPaper.pdf

12 https://www.bitcoinsuisse.com/research/specials/game-at-stake-game-theory-analyze-staking

13 https://research.web3.foundation/en/latest/polkadot/Parachain-Allocation.html

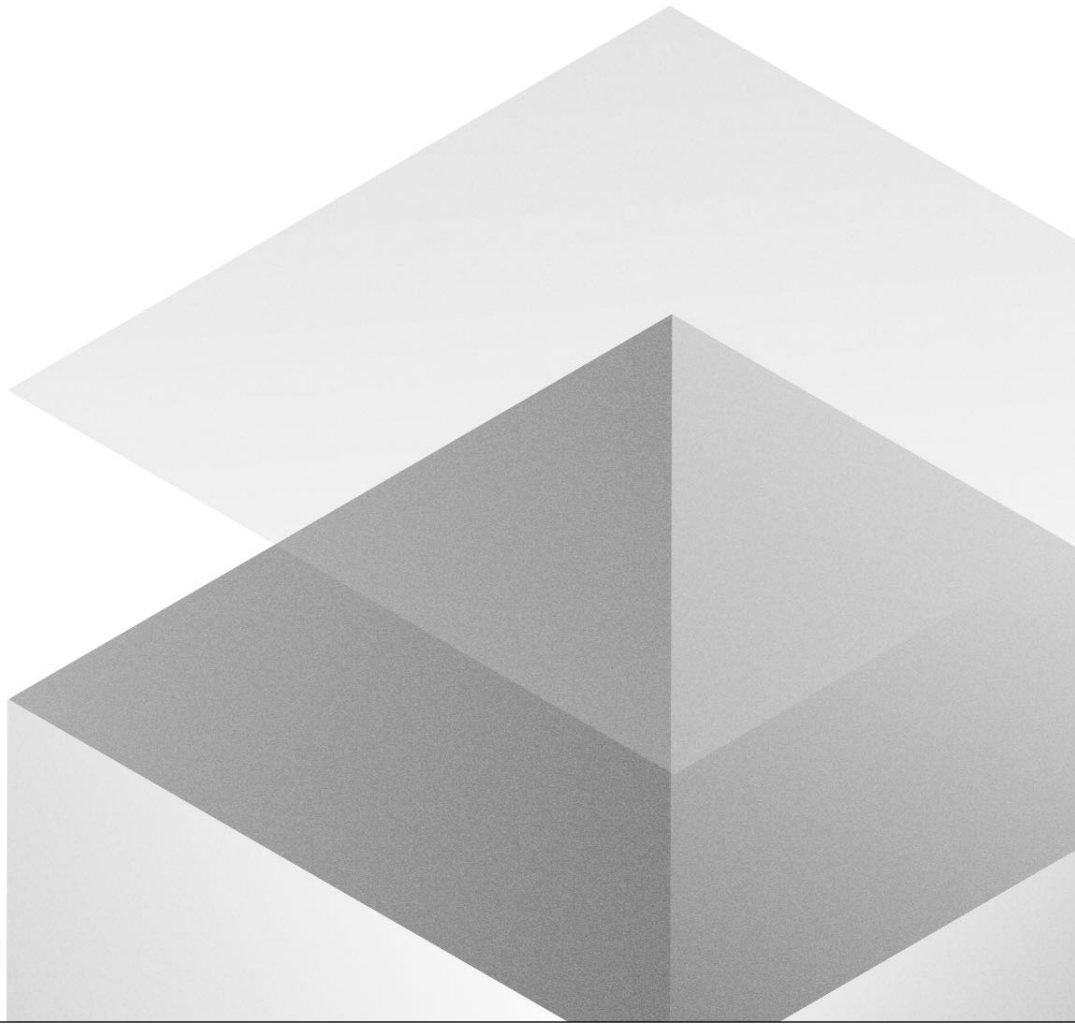
14 https://cosmos.network/cosmos-whitepaper.pdf

15 https://www.irisnet.org/

16 https://blog.cosmos.network/the-internet-of-blockchains-how-cosmos-does-interoperability-starting-with-the-ethereum-peg-zone-8744d4d2bc3f

17 https://polkadot.network/explaining-the-polkadot-launch-process/

18 https://cosmos.network/goz



Scaling the Second Layer

For mainstream adoption, scaling blockchains is a key challenge. Over the past six months, significant improvements to transaction speed and cost have been achieved using second layer technologies.

Scalability is an ongoing field of research[1] and a challenge in blockchain technology. Without scaling the speed of many blockchains today – Bitcoin achieves around 3-4 transactions per second, Ethereum about 15 transactions per second – widespread adoption of the technology by businesses and private individuals all around the world cannot happen. One often quoted reference for ideal throughput in payments is the capacity of the VisaNet, which handles about 1'700 transactions per second, but can process an order of magnitude more during peak times.

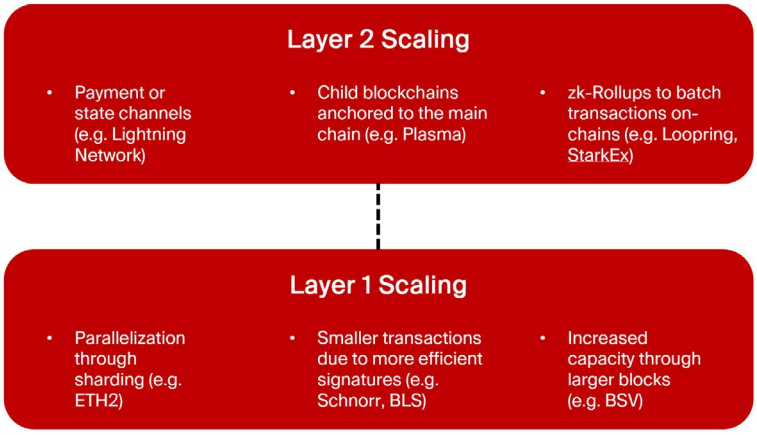
Blockchain Layers to Scale

There are two approaches to blockchain scaling – scaling the protocol layer (layer 1 scaling) or scaling using solutions on top of the protocol that do not require changes to the core code of the blockchain (layer 2, or L2 scaling). Scaling one of these layers offers multiplicative benefits when combined with the other one, meaning a 10x improvement in the first layer (or base layer) and a 100x improvement in the second layer could easily compound to an overall 1000x throughput enhancement.

Second layer scaling is different from sidechains that are linked to the main chain. The advantage is that for well-designed L2 solutions, the main chain has some information about what happens in the second layer and acts as the judge to resolve disputes that might occur on the second layer (e.g. relating to whether funds have been spent or not). Often, they also offer privacy features, which may or may not be desired.

One of the key questions for the design of L2 solutions is data availability: Is the data related to transfers on L2 available on the main chain? Some of the methods presented below store data on transfers off-chain (such as Plasma), which creates friction if users need to collect the data while they are online or download it after a period of offline time. However, there also exist methods in which the data is available on-chain (such as zk-rollups).

Illustration 1: Scaling solutions are available both for the first layer as well as the second layer, and advances in one area also benefit the other.



Source: Cosmos Whitepaper, Bitcoin Suisse Research.

First Layer Scaling Approaches

While this article focuses on L2 solutions, some of the main approaches to scaling the base layer will also be recapped here. One attempt at scaling the first layer is through sharding, most famously planned for the upcoming Ethereum 2.[2] Essentially, sharding means a "parallelization" of the blockchain and if successful, is expected to raise Ethereum's throughput to about 10'000 transactions per second.

Another approach for incremental scalability gains is through optimization of the transactions themselves, mainly through more efficient signature algorithms. Ethereum 2 will use BLS signatures,[3] and for Bitcoin, Schnorr signatures[4] are in development, which would significantly reduce the requirements for block space coming from a subset of transactions.

Last, but not least, one straightforward solution to layer 1 scalability is to increase the block size limit. This is the approach chosen by Bitcoin SV,[5] in which a single 370MB block[6] that was recently mined contained about 1.3 million transactions. This corresponds to around 2'200 transactions per second.

Second Layer Scaling Approaches

Research efforts in the areas of various L2 scaling solutions have come more and more to fruition during this year and specifically the last two months. There are three main L2 scaling techniques which will be outlined below; one of them, zk-rollups, is sometimes also referred to as a "semi-L2" solution due to its strong data availability and validation guarantees on the main chain.

Payment and State Channels

One of the older concepts are payment channels, or their generalized form of state channels that allow not just transfer of value through the channel, but updates to the state of the blockchain in general. Examples of such projects include the Lightning Network[7] for Bitcoin, Raiden[8] and FunFair's fate channels[9] for Ethereum, and Aeternity[10] with built-in protocol support for state channels.

At their core, channels allow two parties to exchange transactions only with each other instead of writing every transaction directly on the chain, which leads to a massive scalability gain and near-instant transaction settlement. Only the result is written onto the main blockchain – making this type of scaling ideal when it is known that two parties will need to transact between themselves a lot in the future. Protection against malicious attempts by either party need to be considered in channel design; usually, it is possible for either party to withdraw their funds from the channel back to the main blockchain. Despite their long history, these channel-based technologies have not been broadly adopted yet, perhaps due to high requirements for keeping channels open and payment routing challenges when more than two parties are involved.

Child Blockchains (Plasma)

Another proposal is to generate child blockchains that are attached to the main chain, and these child chains occasionally write a fingerprint of their state to the root chain (e.g. the current Ethereum blockchain). Users can enter the child (or Plasma)[11] chain through a smart contract. The Plasma chain can operate at a different speed and under a different consensus mechanism than the main chain – in other words, it can be tuned to specific requirements of, for example, a payments network or of a decentralized application. If a user wishes to exit the chain again, this requires a certain "challenge period", in which any potential attempts at fraud can be prevented.

This is also one of the problems of Plasma chains – in the case of congestion of the root chain accompanied by a mass exit from the Plasma chain, this challenge period might not be long enough for challenging all malicious behaviors that might occur. On the other hand, if the challenge period is made too long, this creates friction and opportunity costs for the users due to unavailability of their funds.

A Plasma chain was recently launched[12] after years of development by the OMG Network (formerly OmiseGo). It allows for

>1'000 transactions per second at one third of the cost per transaction, and has already been integrated with Tether,[13] one of the main gas users[14] on Ethereum.

zk-Rollups

zk-Rollups are perhaps one of the most promising scaling approaches yet. They are a form of transaction batching, where SNARKs or STARKs (succinct non-interactive/transparent argument of knowledge)[15] are being used to achieve compression of multiple transactions (for example, a simple value transfer from address A to B) into one on-chain transaction. SNARKs are a cryptographic technique that has been used by Zcash[16] for their privacy guarantees, but zk-rollups showcase the benefits that they may have for scalability purposes.

Users again enter the system through a smart contract, and incentivized relayers take care of bundling transactions and generating SNARK proofs, which is computation intensive and often the bottleneck of such systems.

The first deployment of such a system to the Ethereum mainnet was done by Loopring, a decentralized exchange. They achieved optimizations of the proof generation that allowed to bring down costs per trade to $0.000124. While originally, this system was designed to smoothen the operation of the decentralized exchange, it is also possible to use it for simple transfers of ETH or ERC-20 tokens between users. This feature was launched in June through Loopring Pay,[17] scaling Ethereum capacity for transactions by 1000x – a remarkable achievement. Their token, LRC, reacted positively to this and rose by about 75% (at the time of writing) over the course of last week.

Additionally, StarkWare's StarkEx demonstrated how large communities could be onboarded to the Ethereum mainnet without causing congestions using their zk-rollup technology based on STARKs. They managed to set up 1.3M accounts[18] and seed them with an initial balance using just 2.5% of Ethereum's capacity over 12 hours, at an average cost per transaction of $0.003. Without the zk-rollup, that process would have consumed the entire capacity of Ethereum for 4.5 days.

Conclusion

Second layer scaling is very close to succeeding,[19] and significant achievements of scaling factors of up to 1000x have been achieved. Onboarding users to these systems is the next step for network effects to establish, but given the large savings on

transaction costs, the economic incentives for users to do so are certainly given.

In the future, such L2 solutions could contribute strongly to blockchain adoption overall, since they lower cost, enhance speed and therefore improve usability of the chain. The last pieces of the puzzle are broad deployment of these solutions and user-friendly interfaces that do not require thorough blockchain knowledge – all that the end user will notice is that speed has increased, and costs have decreased.

Sources

1 https://www.bitcoinsuisse.com/research/decrypt/scalability-the-missing-piece

2 https://www.bitcoinsuisse.com/outlook/ethereum-and-its-transition-to-ethereum-2

3 https://ethresear.ch/t/pragmatic-signature-aggregation-with-bls/2105

4 https://www.bitcoinsuisse.com/outlook/bitcoin-in-2020-halving-the-block-reward

5 Bitcoin Suisse Decrypt Series 2, "Bitcoin SV: Back to Genesis"

6 https://blockchair.com/bitcoin-sv/block/635141

7 https://lightning.network/

8 https://raiden.network/

9 https://media.consensys.net/scaling-shoutout-funfair-technologies-c0b0281ce137

10 https://aeternity.com/

11 https://plasma.io/plasma.pdf

12 https://omg.network/omg-network-scales-ethereum/

13 https://www.theblockcrypto.com/linked/66980/tether-stablecoin-launches-on-omg-network-as-ethereum-is-vulnerable-to-severe-network-congestion

14 https://ethgasstation.info/

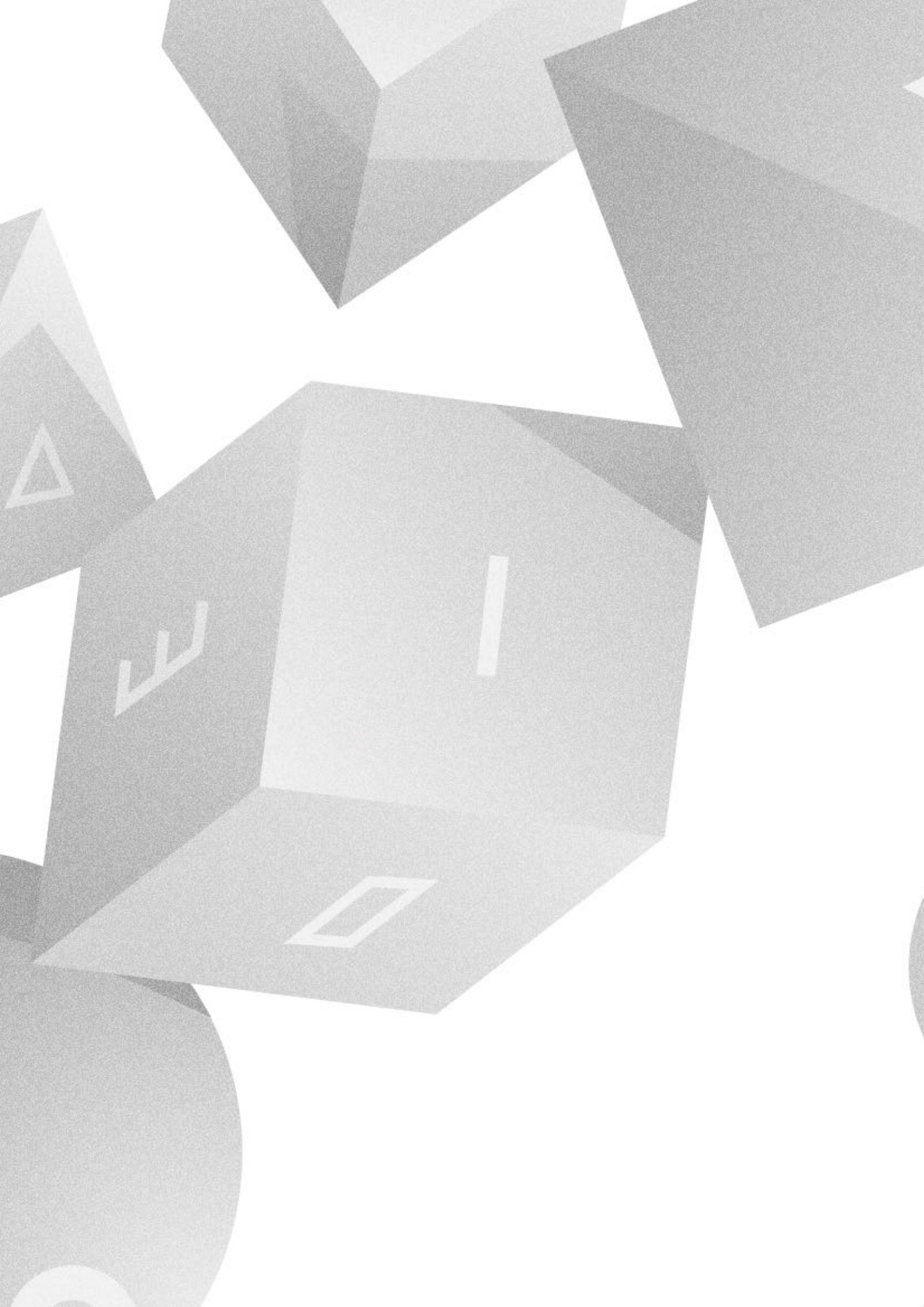
15 https://applicature.com/blog/blockchain-technology/can-zk-snarks-and-zk-starks-solve-privacy-issues

16 https://z.cash/technology/zksnarks/

17 https://medium.com/loopring-protocol/loopring-pay-is-live-zkrollup-transfers-on-ethereum-770d35213408

18 https://medium.com/starkware/with-starkex-ethereum-is-ready-for-reddit-3b2966d5203b

19 https://twitter.com/VitalikButerin/status/1267464298919534593

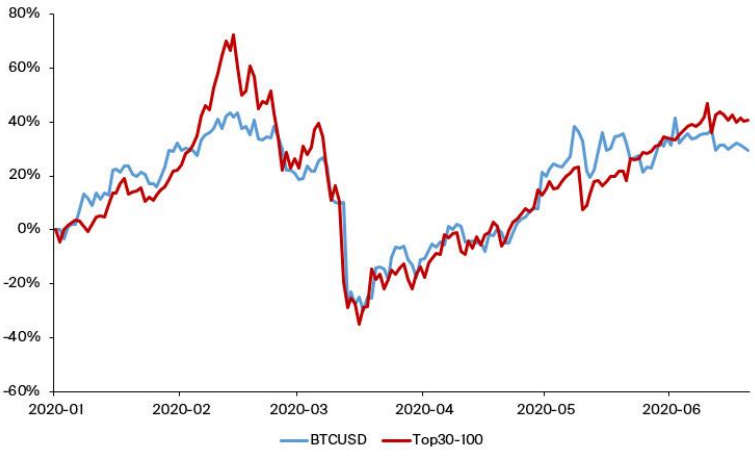


Token Incentives in Decentralized Finance

Altcoins, and especially the ones with smaller market caps, have performed well this year. One particular group of tokens stood out: those related to decentralized finance. What is the current hype all about?

So far in this year and especially since the large price drop on March 12th-13th, many small caps have outperformed Bitcoin. An index of the top 30-100 cryptocurrencies (Bitwise 70) achieved a return of 40% since March 12, whereas Bitcoin yielded 30%.

Illustration 1: Small cap altcoins have outperformed Bitcoin both year-to-date and since March 12/13.

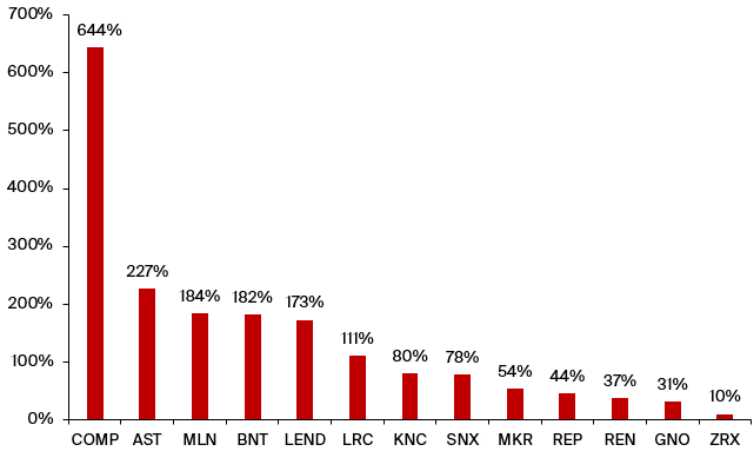


Source: bitwiseinvestments.com, Bitcoin Suisse Research.

This suggests that investors are comfortable again taking on more risk and speculating on the less liquid small cap coins. Particularly from May to June, when Bitcoin entered a consolidation period in a large price range of about $8.5k to $10k, the attention shifted towards altcoins.

Contrary to the state of the market in 2017, though, price increases in smaller altcoins appear to be more selective – indicating that the market is potentially in the process of separating the wheat from the chaff. Among some of the best performers over the last month have been tokens that are related to decentralized finance (DeFi).[1]

Illustration 2: DeFi tokens have provided outsized returns over the past 30 days (or since initial trading launch in the case of COMP).



Source: coingecko.com, Bitcoin Suisse Research.

The benefits of holding these tokens vary, and the jury is still out on how to properly value them. Typical advantages include the right to participate in the governance[2] of the protocol that underlies the token (such as MKR or COMP), fee-based token burn mechanisms[3] as an attempt to correlate long-term platform growth with the token value (e.g. KNC or MKR), and other incentives such as the ability to stake the tokens (e.g. ZRX or SNX).

As outlined in the last episode of Bitcoin Suisse Decrypt,[4] the scalability of Ethereum's second layer has vastly improved during this year, using solutions such as zk-rollups. This enables more efficient decentralized exchanges, whose speed can now even rival some of their centralized counterparts. However, one issue of decentralized exchanges remains liquidity.

To address this issue, new concepts of liquidity mining and "yield farming" have been introduced and led to a wave of new participants in DeFi. The demand for block space[5] was high enough to encourage Ethereum miners to raise the block limit from 10 million to 12 million gas.

Liquidity Mining

Liquidity mining is a concept that was first mentioned in a white-paper[6] by the Hummingbot team, outlining how decentralizing the market making industry could lead to higher efficiency and cost savings both for liquidity buyers (such as exchanges and token issuers) as well as liquidity sellers (the market makers). The goal is to create an incentive structure for decentralized liquidity provision, and reward a large number of market makers through direct subsidies based on their performance, as evaluated through liquidity measures such as average bid-offer spread and order book depth.

However, since each interaction – such as submitting or cancelling an order – with a decentralized exchange has so far required an on-chain transaction, the limited scalability and speed of popular blockchains has hampered the development of a liquid market. Market makers want to be rewarded for the risk they take on, and long delays to order cancellation increase their risk, making spreads (their "reward") larger. With the increased scalability and short settlement times provided by layer 2 solutions, these decentralized markets are set to become more liquid. Additionally, incentive structures such as liquidity mining competitions (as recently announced[7] by zk-rollups pioneer Loopring) may help to accelerate the process.

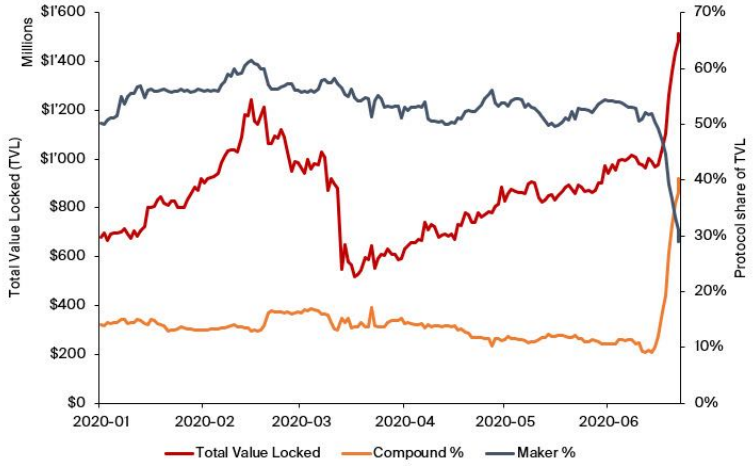
Orderbooks vs. Liquidity Pools

While orderbooks are commonly known from traditional and centralized finance, the DeFi space has brought about another innovation: pooled liquidity and automated market making. For example, on Uniswap,[8] investors looking to exchange one token for another trade against a pool of tokens. The price is not defined by a bid-offer spread, but instead by the composition of the pool (called the "constant product market maker model").[9] Similarly, money markets such as Compound allow lending to and borrowing from a pool of tokens, and the interest rates are set algorithmically depending on the degree of pool utilization.

In June, providing liquidity on Compound was further incentivized[10] through the distribution of their governance token, COMP. About 4.2 million COMP tokens (ca. 2880 per day) will be handed out to borrowers and lenders on the platform. COMP has seen considerable interest on the secondary markets: It started to trade on Uniswap on June 15 just above $30 and has since risen to a high of $369 over the past week, more than a tenfold increase. This also had the effect that both borrowing and lending became profitable, since COMP rewards are more

Illustration 3: Compound has overtaken Maker in terms of total value locked on the platform. Overall, the USD value locked up in DeFi protocols has increased strongly over the past two weeks.

valuable than the interest paid. The total value locked (TVL) in Compound has gone parabolic since then, and the platform dethroned Maker as the largest DeFi project (by TVL).



Source: defipulse.com, Bitcoin Suisse Research.

Along the success of Compound's token, other parts of the DeFi ecosystem have also started to incentivize liquidity through platform governance tokens. Balancer,[11] a decentralized index fund creation protocol with automated index rebalancing, started handing out BAL tokens[12] to platform participants. Similarly, pools of various forms of tokenized Bitcoin on Ethereum, such as WBTC, sBTC and renBTC can earn various governance tokens[13] associated with the involved protocols.

“Yield Farming”

The various ways to earn yield by participating in DeFi protocols has led to a wave of speculators that attempt to maximize their yield by combining various DeFi protocols. One way to do so that was very popular over the last week goes as follows:

1. Obtain a certain amount of stablecoin, such as DAI or USDC, either by buying in the open market or by collateralizing cryptocurrency (e.g. ETH or WBTC) and borrowing against it, for example with a Maker Vault, taking advantage of the currently low stability fees.

2. Deposit to Compound and borrow another stablecoin against it, such as USDT.

3. Swap the borrowed stablecoin for the original one, for example using Curve, a pool-based decentralized stablecoin exchange.

4. Redeposit this stablecoin back to Compound and repeat the procedure.

Essentially, this is leveraging up stablecoin exposure in order to maximize both the interest paid on Compound and in return the share of newly distributed COMP tokens. Other ways to participate were through spillover effects to protocols involved in the procedure, such as providing liquidity to Curve stablecoin pools – which has seen record volumes of >$40M over the past days. Through such methods, annualized returns of >200% were achievable. Such returns never come without risk, though.

No Free Lunch: Risks

Achieving these yields is only possible through a combination of various protocols and smart contracts. Thus, the exposure to smart contract bugs or exploits is magnified. On top of this, the yields are highly unpredictable – it is unlikely that the high current yields persist over a longer period of time, and for example on Curve, yields have already come down to more reasonable levels of 6 to 25% annually. COMP, as a key factor in determining the yield from liquidity mining on Compound, has also retraced from its highs and currently trades around $270.

A collapse of the leveraged stablecoin lending and borrowing cycle may also put the peg of some stablecoins against USD under pressure. In the example above, if USDT were to appre-

ciate in value, some highly leveraged “yield farming” positions may get liquidated and disrupt trading on the secondary markets – in the worst case, leading to a cascade of liquidations. However, Compound has a token reserve (between 10-20% of interest paid by borrowers) that functions as a safety mechanism in the case of liquidations.

Conclusion

Distribution of tokens to platform users appear to be a powerful incentivization mechanism that can help to kickstart a platform or DeFi protocol. As a new user and even for seasoned veterans, cutting through the jungle of protocols and understanding all the ways to earn yield is a complex process. DeFi aggregator platforms like InstaDapp[14] make it simpler for the end user, but the danger is that the investor does not fully understand the protocol interactions happening in the background and hence is unaware of the risks.

The parabolic growth that is seen at the moment in the DeFi space is likely unsustainable – however, the initial hype may well lead to a wave of new DeFi users, and it will be interesting to see at what activity levels the space settles over the next months.

Sources

1 https://www.bitcoinsuisse.com/research/decrypt/leveraging-blockchain-for-decentralizing-finance

2 https://www.bitcoinsuisse.com/research/decrypt/governance-of-distributed-networks

3 https://www.bitcoinsuisse.com/research/decrypt/token-burning-mechanisms

4 Bitcoin Suisse Decrypt Series 2, “Scaling the second layer”

5 https://www.bitcoinsuisse.com/research/decrypt/transaction-fees-markets-for-block-space

6 https://hummingbot.io/blog/2019-11-liquidity-mining/

7 https://medium.com/loopring-protocol/loopring-exchange-liquidity-mining-competition-748917b277e6

8 https://uniswap.exchange/swap

9 https://github.com/runtimeverification/verified-smart-contracts/blob/uniswap/uniswap/x-y-k.pdf

10 https://medium.com/compound-finance/expanding-compound-governance-ce13f-cd4fe36

11 https://balancer.finance/

12 https://medium.com/balancer-protocol/balancer-liquidity-mining-begins-6e65932eaea9

13 https://medium.com/renproject/introducing-an-incentivized-btc-liquidity-pool-by-ren-synthetix-and-curve-213d21691d9a

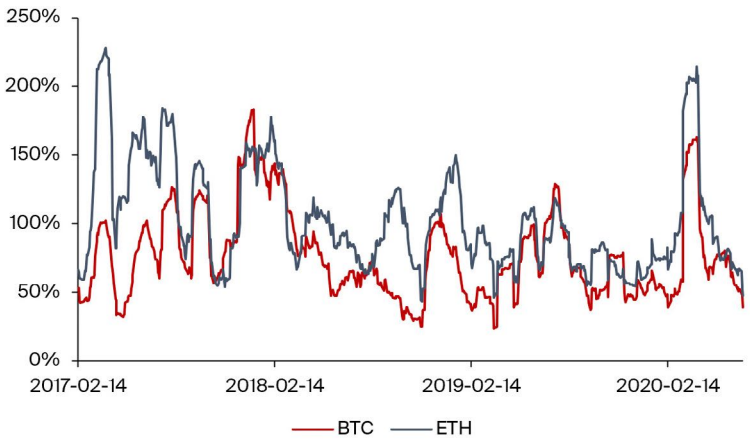
14 https://instadapp.io/

Examining Crypto Volatility

While crypto investors and traders are used to large price swings, volatility has dropped down to historically low levels over the past weeks. What is the current market environment? And how do “the other BTC charts”, valued against non-USD currencies, look like?

Crypto markets have been showing their calmer side over the past weeks. Both Bitcoin and Ether have recently shown low realized volatility in comparison to historical values. At the peak of the bull market in 2017 or during the large drop in March of this year, annualized volatilities of 150-200% (equating to 7-10% daily moves) were seen. Current 30-day volatility values of 39% for Bitcoin and 47% for Ether (annualized) reflect daily moves of 2-2.5%.

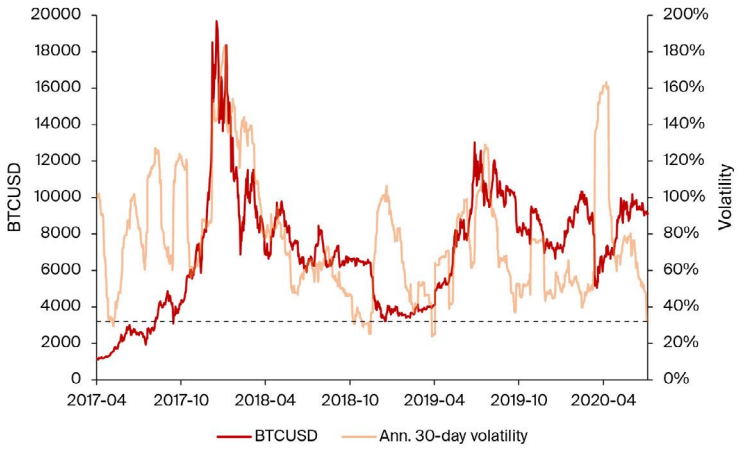
Illustration 1: Bitcoin and Ether 30-day volatility (annualized) is currently low in comparison to historical values.



Source: defipulse.com, Bitcoin Suisse Research.

Periods of low volatility are preceded by periods of high volatility, and vice versa (by definition). Illustration 2 shows occurrences of similarly low volatility since 2017, for example in May 2017, October-November 2018, as well as April 2019. In each case, a large directional move (either bullish or bearish in nature) followed.

Illustration 2: Periods of low volatility have historically preceded strong moves, such as in November 2018 and April 2019. Current volatility level indicated by the black dashed line.

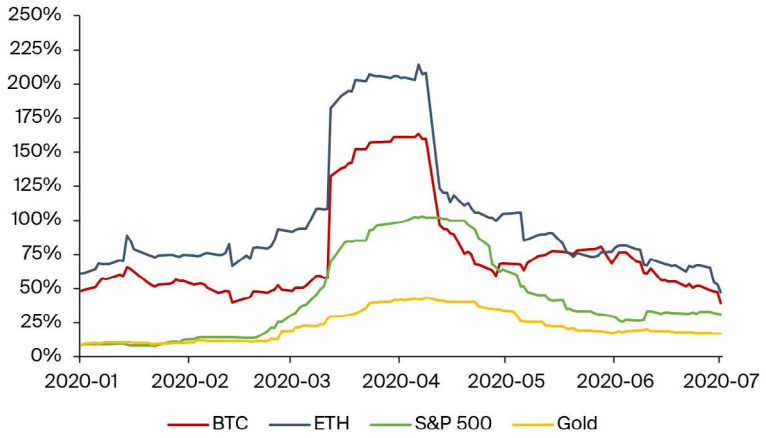


Source: coingecko.com, Bitcoin Suisse Research.

During times where Bitcoin price consolidates in a tight range, attention of traders often turns to altcoins. This is again highlighted during the current period, where much of the action is happening in the DeFi space and its related tokens.[1]

Zooming in on volatility for the period since the beginning of this year, the behavior of the two largest cryptocurrencies Bitcoin and Ether resembles that which can be seen in the stock markets, such as the S&P 500. At current levels, crypto markets are only slightly more volatile than equities. Gold, as the traditional safe haven asset, remained the least volatile throughout the year (currently standing at 16.7% annualized or daily moves of about 1%).

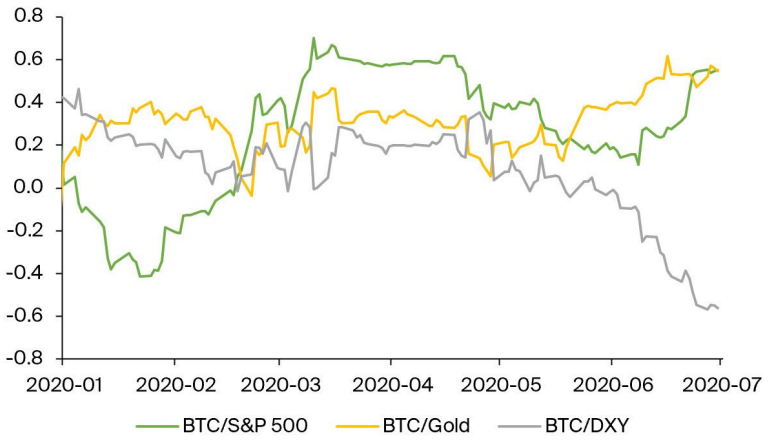
Illustration 3: The current 30-day volatility (annualized) of Bitcoin (39%) and Ether (47%) is close to readings on the S&P 500 (31%).



Source: coingecko.com, Yahoo Finance, Bitcoin Suisse Research.

Short-term 30-day rolling correlations of daily returns between Bitcoin and both the S&P 500 and gold started increasing again after reaching record highs during the market wide sell-off in March.[2] Perhaps even more interestingly, a negative correlation to the dollar index (DXY) started to emerge since May. The dollar index is a measure of the value of the U.S. dollar in comparison to other currencies, specifically against the euro (57.6% index basket weight), the Japanese yen (13.6%), the British pound sterling (11.9%), the Canadian dollar (9.1%), the Swedish krona (4.2%) and the Swiss franc (3.6%).

Illustration 4: The 30-day rolling correlation of daily returns of Bitcoin and the dollar index (DXY) has started to drift into negative territory since May.



Source: coingecko.com, Yahoo Finance, Bitcoin Suisse Research.

A negative correlation means that when the dollar strengthens (DXY rises), Bitcoin drops in value and when the dollar weakens, Bitcoin increases in value as measured in USD. While this intuitively makes sense, historically Bitcoin and the dollar index have been largely uncorrelated. The emergence of a short-term correlation may indicate that recent market movements have been driven by dollar strength and weakness. This might also be an interesting metric to watch in the future, as central banks around the world still continue printing money in large amounts[3] in an attempt to offset economic consequences of the coronavirus lockdowns and to stabilize the flow of credit within the economy through liquidity injections.

A Hedge Against Inflation?

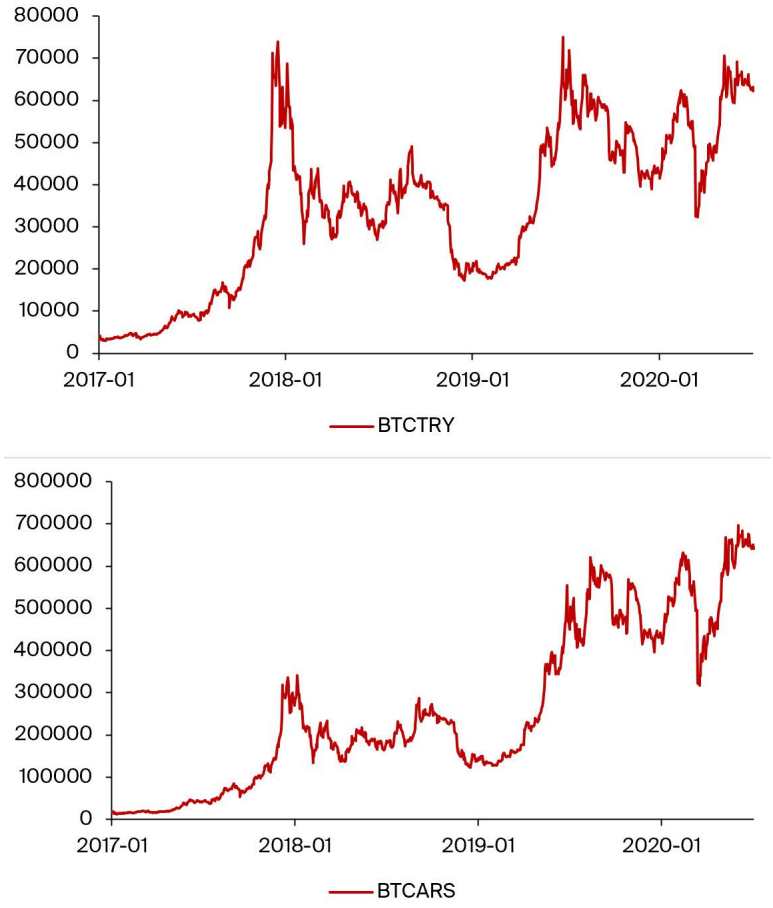
Bitcoin was created in the aftermath of the Great Financial Crisis of 2008, and its creator Satoshi Nakamoto envisioned it to act as an "insurance policy" against mismanagement of government-issued currencies. The first block ever mined references a headline in the Times: "Chancellor on Brink of Second Bailout for Banks".

The recent economic crisis and associated fiscal and monetary policy measures bring up similar topics as in 2008 for example the risk of inflation and currency devaluations due to money printing presses going into overdrive. As such, an emotional moment for many Bitcoin advocates happened during this year's block reward halving. An inscription in block no. 629'999[4], mined by F2Pool, read: "NYTimes 09/Apr/2020 With $2.3T Injection, Fed's Plan Far Exceeds 2008 Rescue".

But whether Bitcoin can truly serve as a hedge against inflation is still unproven. Most major developed economies experienced mild to no inflation over the past years. This is not the case, however, for some emerging economies and their currencies. For example, Turkey experienced an inflation of 15.2%[5] in 2019, and Argentina even more at 53.6%.

While usually, Bitcoin is charted against the USD or EUR, the occasional glance at other currencies can reveal vastly different patterns. As shown in Illustration 5, BTC valued in the Turkish Lira is close to its 2017 all-time high, and it has long breached the 2017 peaks when valued against the Argentine Peso.

Illustration 5: BTC valued in Turkish Lira (TRY) is close to its all-time high, while BTC versus the Argentine Peso (ARS) has surpassed its 2017 high by more than 2x.



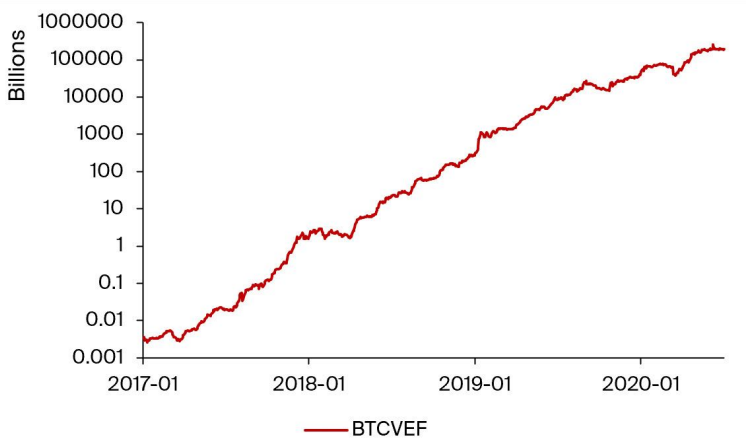
Source: coingecko.com, Yahoo Finance, Bitcoin Suisse Research.

Arguably, using the USD as a store of value in these countries would have offered similar benefits to protect against inflation. Ultimately, accessibility is a deciding factor for the choice of store of value in such cases. Capital controls often restrict the ability to obtain USD – therefore, it may be easier to purchase Bitcoin. Localbitcoins (a peer-to-peer trading platform) vol-

umes in high-inflation countries soared at the end of last year.[6] Once a buyer has entered the crypto markets, access to USD is often easier than through traditional capital markets. Demand for USD-denominated stablecoins has risen rapidly in this year, and the largest one, Tether, is closing in on a $10 billion[7] market capitalization. This may contribute to a (covert) dollarization of such countries.

However, when push comes to shove, any potential store of value is better than a hyperinflationary currency. Bitcoin's "volatility" is barely noticeable when quoted against the Venezuelan bolivar, and one BTC costs around 191'000'000'000'000 VEF (or 1'910'000'000 VES) at the time of writing, give or take a few thousand billion. Under such extreme circumstances, Bitcoin can indeed provide an excellent hedge against inflation.

Illustration 6: BTC versus the hyperinflationary Venezuelan bolivar (VEF).



Source: dolartoday.com, Bitcoin Suisse Research.

Sources

1 Bitcoin Suisse Decrypt Series 2, "Token Incentives in Decentralized Finance"

2 Bitcoin Suisse Decrypt Series 2, "A Flight to Safety"

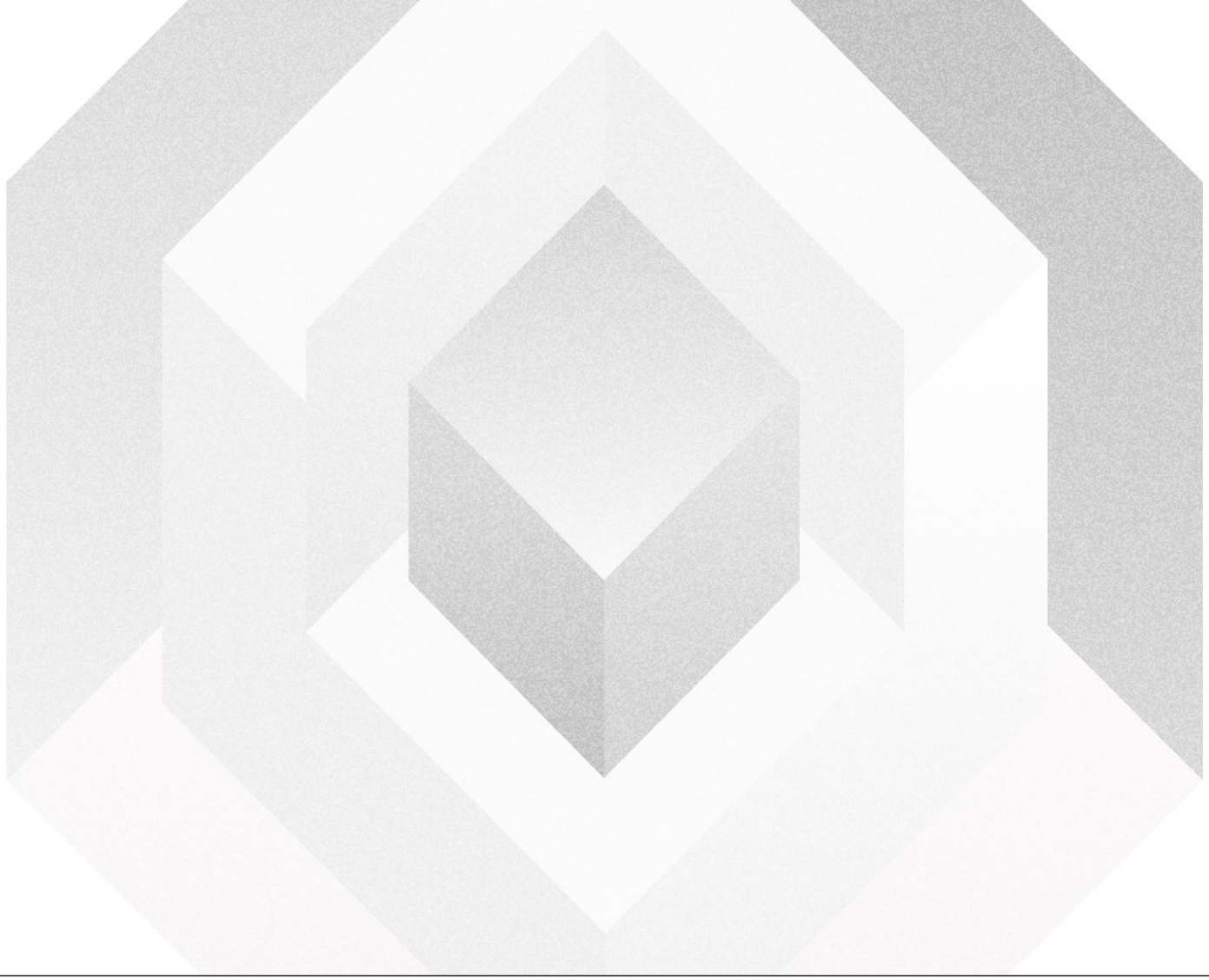
3 Bitcoin Suisse Decrypt Series 2, "Turn on the Money Printers!"

4 https://blockchair.com/bitcoin/block/629999

5 https://www.statista.com/statistics/268225/countries-with-the-highest-inflation-rate/

6 https://www.bitcoinsuisse.com/outlook/bitcoin-in-2020-halving-the-block-reward

7 https://www.coingecko.com/en/coins/tether

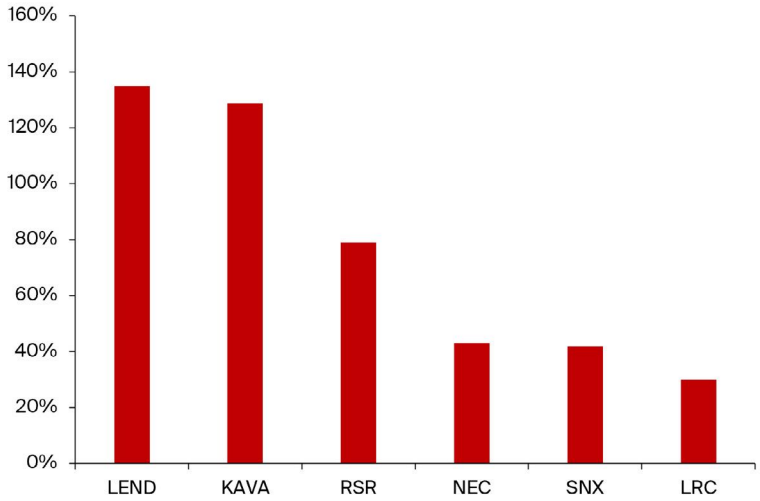


The Evolving Open Finance Ecosystem

During this period of low Bitcoin volatility, decentralized (or open) finance has turned into a hype that is reminiscent of the 2017 ICO mania. Why has it attracted so much attention in a short timespan?

The decentralized finance (DeFi) craze continues, and the total value locked in DeFi protocols is now closing in on $3 billion. The success of Compound's COMP token in attracting users has enticed other protocols to also issue their own tokens. Recently launched examples include YFI, the token of yearn.finance[1] (a DeFi gateway and liquidity aggregator), and MTA, the governance token of the mStable[2] protocol (which attempts to de-fragmentize the ecosystem and yields of "same-peg" assets, such as DAI, USDC, and TUSD, which are all pegged to the U.S. dollar).

Illustration 1: 14-day returns of top performing coins of DeFi-related areas. Aave's LEND token takes the number one spot with a return of 135% over the past two weeks.



Source: coingecko.com, Bitcoin Suisse Research.

The total value locked in DeFi is constantly increasing due to the high annualized yields that can be obtained using various protocols, ranging from 10% to >100% annualized percentage returns on USD-pegged stablecoins in some cases. This has generated a new group of crypto users that call themselves "yield farmers," a concept which was outlined in detail in a previous episode.[3] These yields are subsidized both by the high demand for stablecoins, as well as by traders bidding up the price of governance tokens (such as COMP) which are ultimately crucial for realizing said yields.

Protocol Security Increases

While such high yields on USD-pegged stablecoins may persist for some time, they are certainly surprising given that the USD interest rates outside of the crypto space are at record lows of about 0%. Part of the higher yields can be ascribed to the smart contract risk that is inherent to achieving the yields

through DeFi protocols. However, given that any large DeFi protocol presents honeypots for hackers to the tune of hundreds of millions of dollars' worth of collateral, the security of these protocols becomes a function of time. The longer they exist and are out in the wild for anyone to access and review or exploit, the more unlikely it becomes that they have critical vulnerabilities that would put funds at risk. This is one of the powers of open, permissionless technologies. Thus, on a multi-year horizon, the amount of yield that can be explained by smart contract risk will diminish.

The "Impossible Trinity"

Additionally, in the long run, the yields on USD in DeFi and in the traditional financial markets should converge by force of the "Impossible Trinity". This macroeconomic concept states that it is impossible to have all of the following three parameters at the same time:

- **A fixed exchange rate (such as a peg to the USD)**
- **Free capital movement**
- **An independent monetary policy**

The most spectacular example of the problems that might arise from this in practice occurred in 1992, when the British Pound came under pressure from speculators, eventually leading to a break of the peg to the German mark and devaluation of the GBP, as well as the exit of the UK from the European Exchange Rate Mechanism after a day dubbed "Black Wednesday."[4]

In DeFi, the exchange rate of stablecoins is pegged to another currency or asset by definition. Free capital movement is also a given in the blockchain world, due to its permissionless nature, and introducing government-issued currencies to the crypto space through fiat on-ramps is becoming increasingly efficient.

Hence, the monetary policy of stablecoins such as DAI cannot be independent (which it also does not try to achieve – the task of Maker's governance is simply to read the market for the correct rate). Deviations of the interest rate for (synthetic) USD in DeFi is subsidized by traders and stablecoin users that are willing to pay a premium for access to USD-pegged tokens. This imbalance opens up arbitrage opportunities, which will be exploited once sufficient liquidity is available in the crypto markets, and this will bring down yields.

Credit delegation

Another DeFi innovation that has attracted a lot of interest is the introduction of credit delegation[5] by Aave.[6] Credit delegation essentially enables undercollateralized loans: Person A deposits assets in the DeFi protocol and signs an agreement with Person B that allows them to draw a loan against the collateral of person A. The agreement is automated, in this case, through OpenLaw[7], which aims to bring legal contracts to the blockchain through smart contracts.

Such types of loans have long been the "holy grail" of DeFi since they combat the current restrictions of capital inefficiency that arise from the need for overcollateralization of loans. A typical collateralization ratio in today's DeFi landscape would be the one from MakerDAO Vaults, where a 150% minimum collateralization is required – meaning, for example, that for $300 worth of ETH, only $200 worth of DAI can be generated.

Credit delegation does not remove the need for collateral, it merely shifts the collateral type from a tangible asset (money in the form of cryptocurrency) to an intangible asset, namely the reputation of the borrower. Early agreements will likely be signed between wealthy crypto holders and trustworthy counterparties with high liquidity needs, such as market makers.

The cost of building up this reputation or (opportunity) cost that is associated with losing the reputation must be at least as high as the potential gain from exploiting such an undercollateralized loan, thereby capping the amount that can be lent out.

Decentralized Identities

This also brings up the topic of decentralized identity[8]. A decentralized, undercollateralized lending and borrowing market needs identifiable borrowers that can be held accountable for the loans they take out. As such, initiatives that connect real-life identities (individuals or companies) to on-chain addresses may become a crucial component for future on-chain lending markets.

Such initiatives can take two forms. The first is through a trusted third party that verifies currently used identity documents such as passports and government-issued IDs. This would simply port the legacy system onto the blockchain, but introduces a centralized point of failure (the third party ID verifier).

The second, more progressive form is through "social graphs" (as, for example, developed by BrightID[9]), which means that a network of social connections is established, and people within a small group can vouch for each other's uniqueness.

Being more connected to other groups strengthens the legitimacy of a group, since the denser a network becomes, the harder it is to manipulate it.

A trusted, decentralized identity system would unlock a swathe of new use cases. One of them would be decentralized credit scores to determine the amount of an undercollateralized loan that an on-chain identity can take out. Another obvious use case of verifiably unique identities is voting, where it is paramount that sybil attacks (one person creating multiple identities) are prevented.

Given that controlling such a digital identity that is strongly linked to one's real life identity would likely come with a great deal of power, safeguarding access to the digital identity will be of utmost importance. Similar to the management of a private key that holds significant amounts of cryptocurrency, losing access to the identity would be a major disaster for the individual. Social graphs can also help here via social recovery[10] mechanisms, such as the ones implemented in crypto wallets like Argent[11] or Tatoshi[12]. If a user loses access to the wallet or identity, friends and family can restore it, without being able to access the wallet on their own.

Conclusion

More and more pieces of the puzzle that might eventually represent the decentralized economy are coming together. The vision of where this is heading is to empower people to autonomously take control of their finances, their identity, their social networks, and their access to protocols supporting this. The recent Twitter hacks[13] further highlighted the danger of identity theft and the case for decentralization to avoid single point of failures.

The role of the blockchain in this is to serve as a source of immutable truth. Along the way, permissionlessness will lead to efficiency enhancement in credit and other markets, since anyone is allowed to build and innovate (maximizing competitiveness) and rent-seeking is minimized.

Sources

1 https://yearn.finance/

2 https://mstable.org/

3 Bitcoin Suisse Decrypt Series 2, "Token Incentives in Decentralized Finance"

4 https://www.theguardian.com/business/2012/sep/13/black-wednesday-20-years-pound-erm

5 https://defirate.com/aave-credit-delegation/

6 https://aave.com/

7 https://www.openlaw.io/

8 https://www.bitcoinsuisse.com/research/decrypt/the-identity-of-the-future

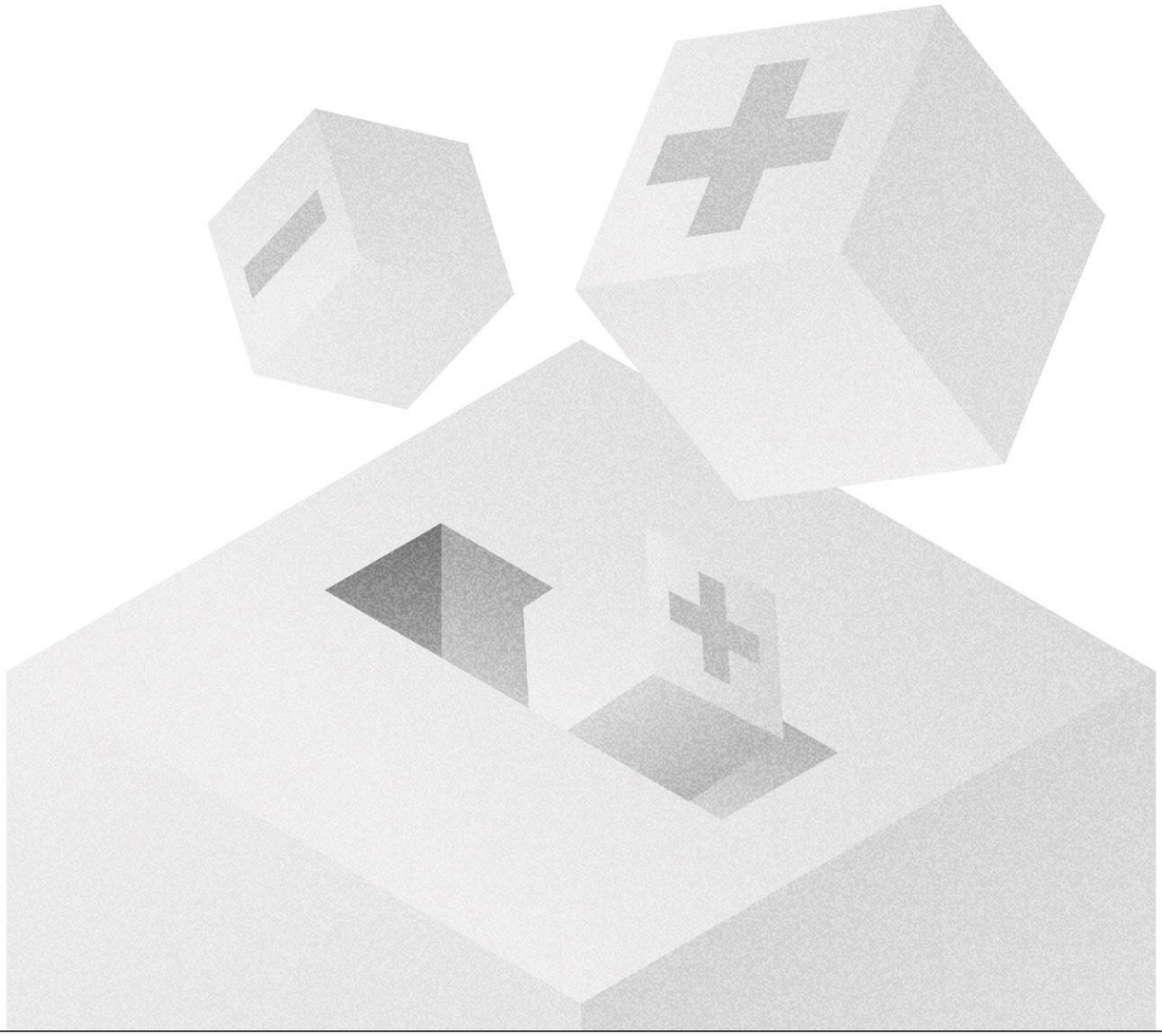
9 https://www.brightid.org/

10 https://www.bitcoinsuisse.com/research/decrypt/the-road-to-mainstream

11 https://www.argent.xyz/

12 https://tatoshi.io/

13 https://www.theblockcrypto.com/post/71906/twitter-account-hacks-timeline



The Aftershock of Governance Tokens

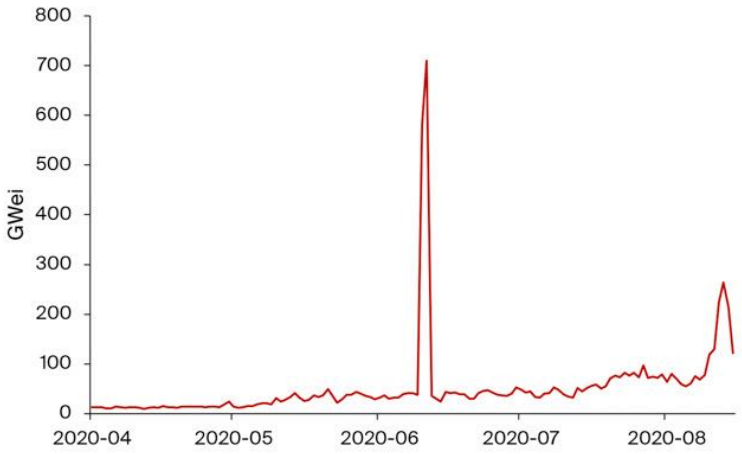
The incentivization of pooling liquidity on Compound through their governance token COMP two months ago has unleashed a wave of innovation in the DeFi space. What has happened since then? And what role do governance tokens play in this phenomenon?

The hype around decentralized finance (DeFi) continues as the total value locked in DeFi protocols has reached $6 billion, and innovation is happening at a breathtaking pace. For example, money market protocol Aave (LEND) has recently announced[1] a series of upgrades, such as fixed rate deposits (allowing users to earn a stable rate for lending) and gas optimizations to bring down the overall cost of interacting with the protocol. Additionally, yield aggregators such as yearn.finance[2] continue to attract interest, since they simplify the optimization of yield farming[3] by providing "Vaults" with pre-defined strategies. One of these strategies involves yield farming on Curve[4], a decentralized exchange designed specifically for swapping assets with similar value, such as various USD-pegged stablecoins or different kinds of tokenized Bitcoin on Ethereum. The governance token of Curve, CRV, has recently been launched, and is the main reason why high yields of currently around 90% can be achieved by farming the protocol.

High Ethereum Fees

Volumes on decentralized exchanges have also exploded. The largest one, Uniswap[5], has processed on average around $250M per day over the past week, or about half of that of major centralized exchanges. Gas usage through decentralized trading on Uniswap has increased considerably and played a part in Ethereum fees skyrocketing.

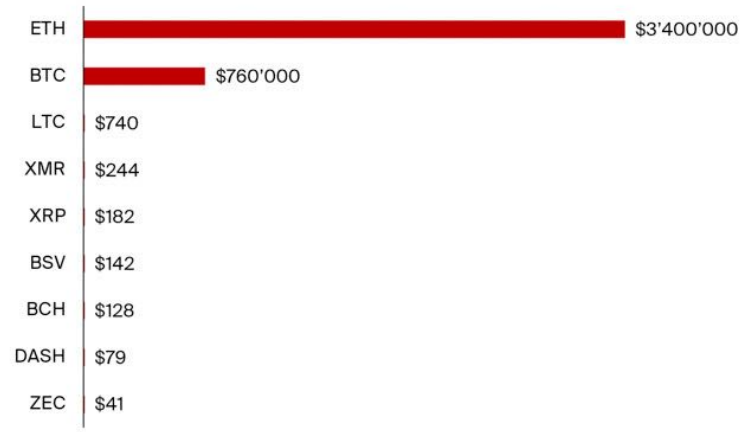
Illustration 1: Daily average gas fees (in GWei) for transactions on Ethereum have strongly increased over the past month. The spike in June was an anomaly mostly due to two transactions that were submitted with absurdly high gas prices.



Source: etherscan.io, Bitcoin Suisse Research.

Overall, total fees paid per day on Ethereum are now significantly more than those paid on Bitcoin. The two largest chains by market capitalization share the vast majority of fees collected among all public blockchains.

Illustration 2: Ethereum and Bitcoin capture the majority of fees paid on public blockchains. Over the past 24 hours, Ethereum and Bitcoin have collected $3.4M and $760k in transaction fees, respectively.



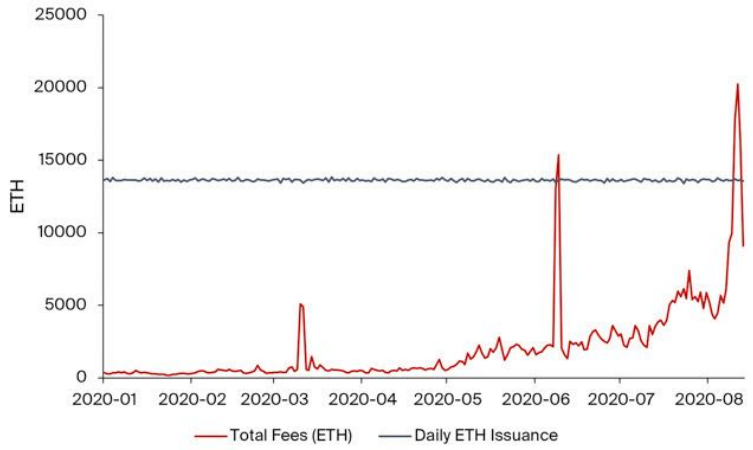
Source: etherscan.io, Bitcoin Suisse Research.

This shows that block space in these two chains is perceived as valuable, and users are willing to pay the steep fees associated with transacting on the chains. On the other hand, it also highlights the need for better scalability. For Ethereum, this may lead to a gradual shift from layer 1 to layer 2 using scaling solutions[6] such as zk-rollups in the short to medium term. Eventually, the switch to Ethereum 2[7] should also bring additional scalability – however, a full implementation of all phases of Ethereum 2 is still likely more than two years out.

Potential for Negative Net Issuance?

The massive amount of transaction fees paid on Ethereum also bring up the thought of Ethereum Improvement Proposal (EIP) 1559 again. EIP-1559[8] aims to transfer the volatility of gas prices and hence transaction costs to the volatility of the block size. This would strongly improve the user experience since fees would become much more predictable. On top of that, a large portion of transaction fees would be burned – which would bring down the overall supply inflation through issuance of new coins to miners (PoW) or validators (PoS). This may even lead to a decreasing ETH supply in times of high demand, as would have been the case during several of the last days were EIP-1559 already implemented.

Illustration 3: Total transaction fees have briefly surpassed issuance of new ETH to miners in August.



Source: etherscan.io, Bitcoin Suisse Research.

An additional phenomenon that DeFi has brought about is a rapidly increasing amount of BTC tokenized on Ethereum. In total, there is now more than $500 million worth of Bitcoin[9] tokenized in the form of various ERC-20 tokens, such as wBTC (a custodial solution with around 70% market share) or renBTC (a trustless[10] variation with around 20% market share). These tokens are then used, for example, to mint DAI through MakerDAO – in fact, the Maker wBTC contract is the largest holder of wBTC and stores about 11'400 wBTC[11] (around 42.8% of all wBTC tokens). Another popular option is to provide liquidity to Curve, which accounts for another 6'500 wBTC (24.6% of all tokens).

Role of Governance Tokens

The issuance of governance tokens[12] to protocol users to attract liquidity has kickstarted the current hype around DeFi and attracted large amounts of capital. Their value, however, is still unclear and depends on the governance rights that come with it.

From a game-theoretical perspective, the value of a well-designed governance token is tied to the overall success of the protocol, aligning the incentives of token holders and promoting good governance. However, at the current stage, not all protocols have implemented such mechanisms in their governance tokens. For these, the value of the token is purely based on the possibility of future monetization, e.g. the power to vote on the implementation of a protocol fee that flows to token holders. As such, it is also critical what governance can do, meaning which aspects of the protocol that may relate to the token value they can influence.

For example, in MakerDAO[13], the main parameter that governance can change that should affect the price of their token (MKR) is the stability fee for opening Maker Vaults. Stability fees are charged on outstanding debt to the Maker protocol, converted to MKR tokens, which are then burned to decrease the overall supply. Additionally, governance can approve new assets as collateral (e.g. MANA[14] at the end of July) and change the maximum allowed debt per asset to scale the system and potentially increase the stability fees earned in total, leading to more MKR being burnt. As for most protocols, governance also has the duty to approve upgrades to the protocol and new functionalities.

On the other hand, the token of Compound, COMP, purely serves governance functions and has no mechanism for (in) direct value accrual yet, so its value is closely linked to speculation that this will change in the future. So far, 19 governance proposals[15] have been voted on, of which 16 were passed. Mainly, the changes implemented through the on-chain voting process were related to protocol stability changes, such as setting collateral factors (i.e. how much debt can be borrowed against a specific asset). Governance also has the power to change reserve factors: Compound sets aside a small portion of interest paid by borrowers as reserves. These reserves are controlled by the token holders. By changing this amount and distributing part of excess reserves to COMP token holders, an implicit spread on the lending / borrowing rate could be collected for COMP holders in the future.

Money Markets and Governance Tokens

Another aspect of fully on-chain governed protocols that may seem irrelevant today, but become more important if these protocols grow (much) more in size is the possibility of "hostile protocol takeovers" through a combination of buying tokens and borrowing them from money markets such as Compound or Aave. If sufficient governance tokens are available for borrowing, a malicious actor could try to obtain a majority share of governance tokens through borrowing (driving up lending interest rates in the process and enticing more people to offer their

tokens in the money market protocol) and exploit the protocol in her or his self-interest. This may present a problem especially for smaller protocols with cheaper governance tokens, which potentially require posting less collateral overall. However, many protocols already have mechanisms in place that make such an attack harder or at least less profitable, such as time delays on protocol changes through governance.

Conclusion

The current excitement about DeFi continues to drive innovation. The world of DeFi is one of the first examples of why composability matters: While, for example, MakerDAO is a powerful protocol on its own and created the first fully decentralized USD-pegged stablecoin, its full potential gets unlocked through the interaction with other protocols such as decentralized exchanges (DAI trading against other assets) or money markets (to lend DAI or post it as collateral). The importance of governance tokens will increase for two reasons: Holders will want to find a way to monetize the protocol, and due to the intertwined nature of DeFi, governance decisions can have effects far beyond just one protocol. Network effects are in the process of being established, and – perhaps a remarkable difference to the ICO mania in 2017 – protocols are often mutually reinforcing and adding value to each other instead of fighting for a share of the same pie.

Sources

1 https://medium.com/aave/aave-v2-the-seamless-finance-d52075d97a70

2 https://yearn.finance/

3 Bitcoin Suisse Decrypt Series 2, “Token Incentives in Decentralized Finance”

4 http://curve.finance/

5 https://app.uniswap.org/#/swap

6 Bitcoin Suisse Decrypt Series 2, “Scaling the second Layer”

7 Bitcoin Suisse Decrypt Series 2, “Ethereum’s Path to Serenity”

8 https://www.bitcoinsuisse.com/outlook/ethereum-and-its-transition-to-ethereum-2

9 https://btconethereum.com/

10 https://renproject.io/renvm

11 https://etherscan.io/token/tokenholderchart/0x2260fac5e5542a773aa44fbcfedf7c193bc2c599

12 Bitcoin Suisse Decrypt Series 2, “Token Incentives in Decentralized Finance”

13 https://docs.makerdao.com/maker-protocol-101

14 https://blog.makerdao.com/mana-approved-by-maker-governance-as-collateral-type-in-the-maker-protocol/

15 https://compound.finance/governance/proposals

Shifts in Cryptocurrency Markets

Markets are pricing mechanisms to constantly re-estimate the true value of any traded asset, and crypto markets are no different. Most coins that were relevant in 2013 have faded into irrelevance. Is true diversification possible within the cryptocurrency markets?

Last week, the Chairman of the Federal Reserve J. Powell gave a speech[1] outlining a change to the Fed's inflation goals – instead of targeting 2% annually, they will now aim to achieve a longer-term average of 2%. This means that if inflation stayed below the 2% threshold for a few years, it will be allowed to run "moderately higher" in the coming years. The speech led to quite some volatility in both the dollar index DXY as well as the cryptocurrency markets.

Illustration 1: Powell's speech (which started around 15:10 CET) impacted both crypto markets (BTCUSD, rhs, red/green 1-minute candles) as well as the dollar index (DXY, lhs, in black).

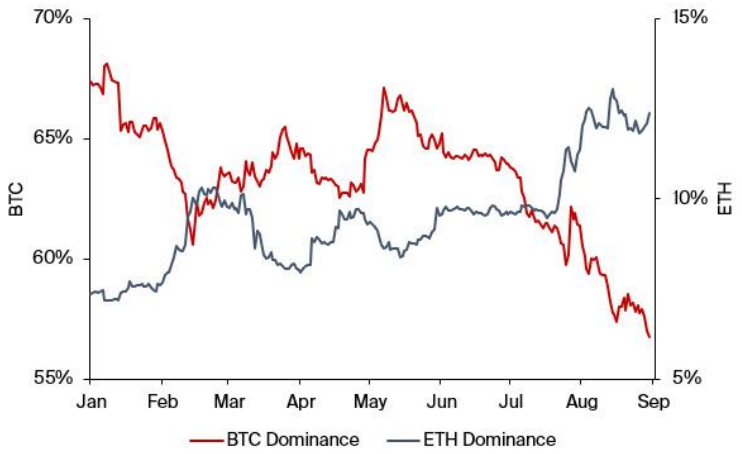
Source: etherscan.io, Bitcoin Suisse Research.

As mentioned in a previous episode[2], Bitcoin has shown an increased inverse correlation to the dollar index, including during its sharp shorter-term movements. If the correlation were to persist also over longer timeframes, that would strengthen the case for Bitcoin as digital gold and a hedge against inflation – retaining its purchasing power in the face of a declining dollar.

Declining Bitcoin Dominance

Meanwhile, Bitcoin's dominance in the cryptocurrency markets has shrunk, and ETH as well as other coins and tokens increased their share in the overall market cap.

Illustration 2: Since the beginning of July, Bitcoin dominance has declined from 63.8% to 56.7%, while Ethereum's share of the total crypto market capitalization has increased from 9.5% to 12.4%.



Source: coinpaprika.com, Bitcoin Suisse Research.

Specifically, tokens related to decentralized finance are in part responsible for the decline of the Bitcoin dominance. The total market cap of DeFi tokens has reached $18 billion[3], or 4.6% of the total crypto market cap (at the time of writing). The rapid growth of the DeFi ecosystem continues, with total value locked currently sitting at almost $9 billion[4].

A Trip Down Memory Lane

The cryptocurrency market landscape is constantly shifting. The winners of today may fade into irrelevance over time – as has happened with seven of the top 10 coins of 2013.

Illustration 3: Only 3 of the top 10 coins of 2013 still occupy a slot in the top 10 of today. Color code: Green = new or higher ranking, red = lower ranking, yellow = same ranking, grey = not in top 100 anymore today.

	Aug. 2020		Aug. 2019		Aug. 2016		Aug. 2013	
#1	Bitcoin	$215.1 B	Bitcoin	$181.4 B	Bitcoin	$9.1 B	Bitcoin	$1.4 B
#2	Ethereum	$47.7 B	Ethereum	$20.0 B	Ethereum	$911 M	Litecoin	$54 M
#3	Tether	$13.3 B	Ripple	$11.6 B	Ripple	$212 M	Ripple	$48 M
#4	Ripple	$12.7 B	Bitcoin Cash	$5.5 B	Litecoin	$176 M	Namecoin	$3.9 M
#5	Chainlink	$6.5 B	Litecoin	$4.6 B	Monero	$121 M	Peercoin	$3.5 M
#6	Polkadot	$5.4 B	Binance Coin	$4.1 B	Ethereum Classic	$110 M	Feathercoin	$1.9 M
#7	Bitcoin Cash	$5.1 B	Tether	$4.0 B	Steem	$100 M	Novacoin	$1.7 M
#8	Litecoin	$4.0 B	EOS	$3.3 B	Dash	$83 M	Primecoin	$1.3 M
#9	Bitcoin SV	$3.6 B	Bitcoin SV	$2.4 B	NEM	$54 M	Terracoin	$0.6 M
#10	Cardano	$3.6 B	Stellar	$1.4 B	MaidSafeCoin	$48 M	Infinitecoin	$0.4 M
Tot.		$317 B		$238 B		$10.9 B		$1.5 B

Source: coingecko.com, coinmarketcap.com, Bitcoin Suisse Research.

While Tether did not increase in value from Aug. '19 to Aug. '20, it was included in the list to highlight the rising importance and prevalence of stablecoins.

A few observations from the table above are noteworthy:

- **The total market cap of the top 10 has increased by an order of magnitude every three years.**
- **Bitcoin remained no. 1 throughout, and Ethereum and Ripple defended their no. 2 and 3 spots since 2016 (disregarding Tether).**
- **Litecoin has continually lost relevance, but managed to remain in the top 10 since 2013.**
- **Seven of the top 10 coins in 2013 and two of the top 10 coins in 2016 do not occupy spots in the top 100 of today anymore.**

This leads to the conclusion that passively investing in the top 10 coins at any point in time to gain "diversified" exposure to the crypto markets may not be the best strategy, and historically, occasional rebalancing would have enhanced returns.

Correlations in the Top 20

Now, "diversified" was put in quotation marks because diversification across assets with high correlations is of limited efficacy. A correlation matrix for the current top 20 coins allows to identify those with low correlations to the "blue chip" coins Bitcoin and Ether.

Illustration 4: Of the top 20 coins, LINK, BSV, CRO, ATOM and OKB have relatively low correlations to BTC and ETH. Correlations based on daily returns with data since March 2019.

	BTCUSD	ETHUSD	XRPUSD	LINKUSD	BCHUSD	LTCUSD	BSVUSD	ADAUSD	BNBUSD	CROUSD	EOSUSD	XTZUSD	XLMUSD	TRXUSD	ATOMUSD	XMRUSD	OKBUSD	NEOUSD
BTCUSD	1.00																	
ETHUSD	0.85	1.00																
XRPUSD	0.74	0.85	1.00															
LINKUSD	0.47	0.55	0.52	1.00														
BCHUSD	0.80	0.82	0.75	0.45	1.00													
LTCUSD	0.79	0.86	0.80	0.49	0.86	1.00												
BSVUSD	0.48	0.53	0.48	0.31	0.62	0.55	1.00											
ADAUSD	0.73	0.82	0.79	0.50	0.76	0.81	0.45	1.00										
BNBUSD	0.70	0.77	0.68	0.48	0.68	0.74	0.48	0.68	1.00									
CROUSD	0.34	0.31	0.27	0.20	0.28	0.31	0.18	0.29	0.28	1.00								
EOSUSD	0.78	0.85	0.79	0.50	0.84	0.87	0.58	0.78	0.70	0.28	1.00							
XTZUSD	0.58	0.65	0.61	0.46	0.52	0.57	0.32	0.59	0.56	0.24	0.57	1.00						
XLMUSD	0.64	0.76	0.81	0.50	0.66	0.73	0.41	0.77	0.66	0.26	0.70	0.59	1.00					
TRXUSD	0.73	0.83	0.82	0.49	0.74	0.80	0.50	0.80	0.70	0.27	0.80	0.57	0.75	1.00				
ATOMUSD	0.36	0.38	0.35	0.29	0.35	0.38	0.22	0.35	0.39	0.06	0.36	0.32	0.34	0.37	1.00			
XMRUSD	0.67	0.71	0.62	0.45	0.65	0.65	0.36	0.61	0.63	0.24	0.65	0.49	0.60	0.65	0.36	1.00		
OKBUSD	0.55	0.57	0.51	0.38	0.50	0.55	0.34	0.50	0.62	0.23	0.51	0.49	0.48	0.53	0.30	0.48	1.00	
NEOUSD	0.76	0.79	0.75	0.51	0.73	0.76	0.48	0.75	0.67	0.28	0.77	0.58	0.69	0.78	0.36	0.63	0.51	1.00

Source: coingecko.com, Bitcoin Suisse Research.

Of the top 20 coins, five seem to offer the possibility for diversification within crypto markets: LINK, BSV, CRO, ATOM and OKB. Nonetheless, correlations remain relatively high and positive, with the lowest ones being around 0.34-0.36 (for CRO and ATOM, respectively). A rising tide still seems to lift all boats, albeit to varying degrees. However, each coin or token offers a different value proposition, meaning fundamental aspects such as tokenomics, absolute valuation and future growth potential should be given at least equal importance relative to portfolio diversification desires.

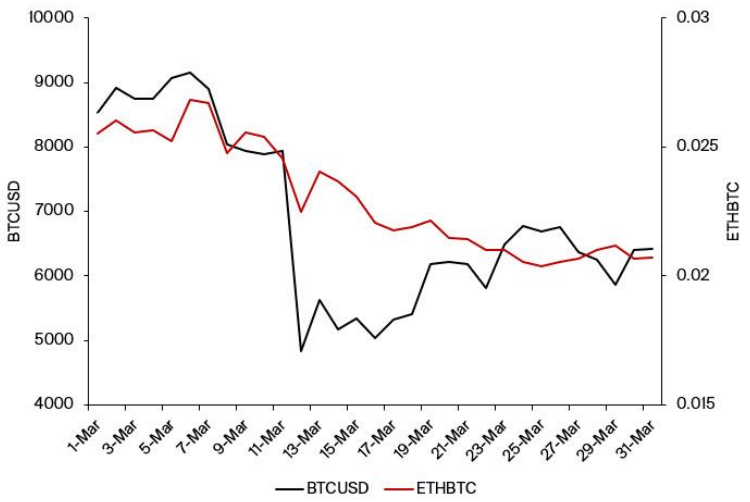
One notable exception from this list of top 20 coins is Polkadot's DOT (currently no. 6 by market cap), which has only started trading very recently and thus, no reliable conclusions can be drawn on its correlation to other coins. In its short trading history, DOT has shown a low correlation to both Bitcoin (0.26) and Ether (0.23).

The Importance of Trading Pairs

One potential reason for the generally strong correlations in the cryptocurrency markets is the nature of trading pairs. Many coins and tokens either used to be or are still traded mostly against BTC or ETH. In the absence of USD trading pairs, this tends to correlate the USD value of the coin or token to the performance of BTC or ETH, and exacerbates downward pressure if altcoin traders wish to exit through a trading route of altcoin to BTC/ETH to USD.

Nowadays, many cryptocurrencies also have liquid USD (or USD-pegged stablecoin) trading pairs. This may lead to decreasing correlations over time. During strong BTCUSD sell-offs, however, correlations tend to be high – as is the case in other markets. As an example, during "Black Thursday" (March 12 of this year), ETHBTC (as a proxy for the altcoin market) remained constant or even sold off together with BTCUSD, meaning that ETHUSD declined by as much or even more than BTCUSD.

Illustration 5: During "Black Thursday" (March 12 of this year), ETHBTC declined slightly as BTCUSD sold off, indicating that ETHUSD declined slightly more than BTCUSD and was strongly correlated.



Source: cryptodatadownload.com, Bitcoin Suisse Research.

Conclusion

In a world where central banks set out to do everything in their power to stoke inflation, potential stores of value such as Bitcoin seem attractive. Within crypto markets, however, Bitcoin's dominance declined in the past months, and the Ethereum ecosystem (ETH as well as DeFi tokens) increased its market capitalization. While none of the new DeFi governance tokens[5] has made it into the top 20 coins so far, the crypto landscape is continuously shifting, and only a few cryptocurrencies have truly stood the test of time.

The correlations between major cryptocurrencies remain high and make "true" diversification difficult, although the emergence of liquid USD or USD-pegged stablecoin trading pairs may decrease correlations in the future.

Sources

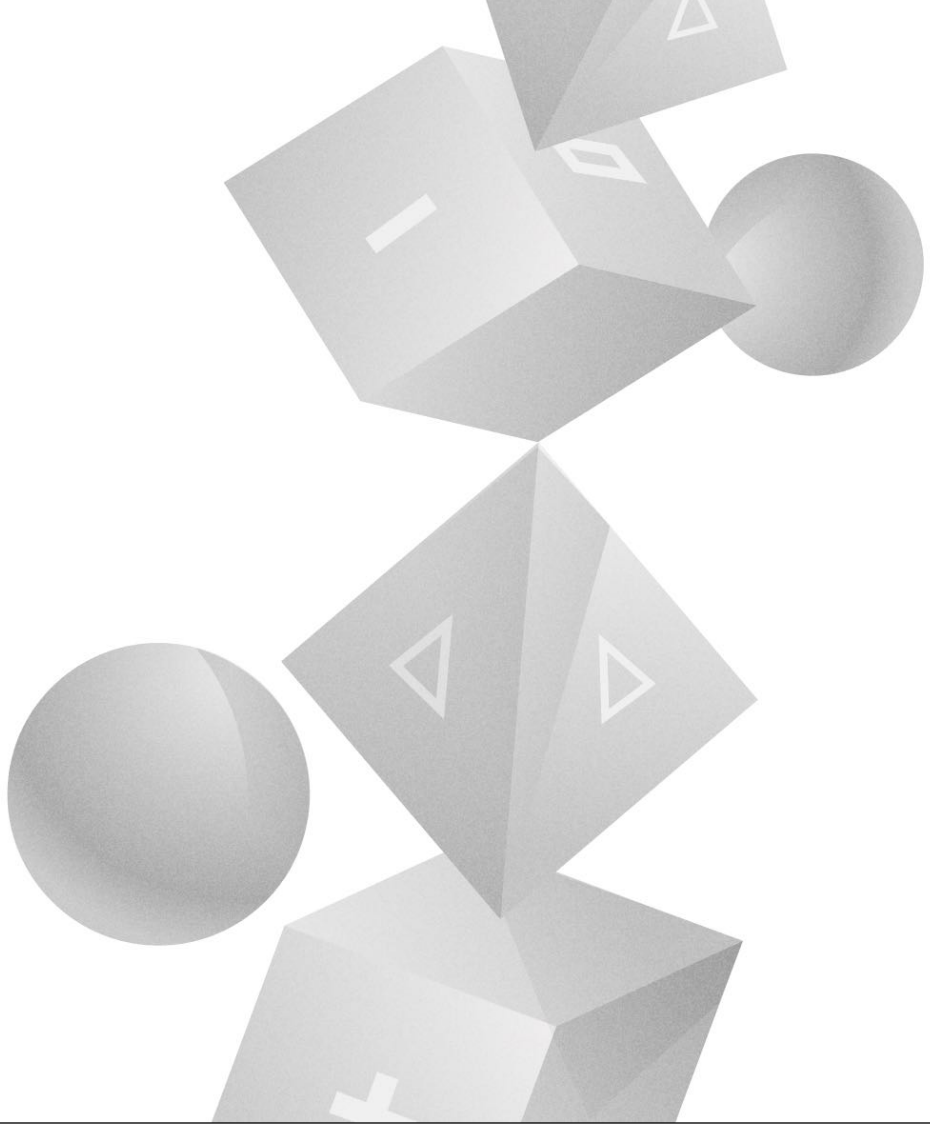
1 https://www.federalreserve.gov/newsevents/pressreleases/monetary20200827a.htm

2 Bitcoin Suisse Decrypt Series 2, "Examining Crypto Volatility"

3 https://www.coingecko.com/en/defi

4 https://defipulse.com/

5 Bitcoin Suisse Decrypt Series 2, "Token Incentives in Decentralized Finance"



Regulations and Innovations

During this year, major changes have come, or are yet to come, to the regulatory landscape of the crypto markets. One of the main goals of these new regulations is to not stifle innovation – and innovation continues to happen at a rapid pace.

Regulatory Advances

The regulatory landscape for crypto assets continues to become more well-defined. Recently, both the European Union as well as Switzerland have made progress towards establishing a legal framework for the issuance and handling of crypto assets.

Perhaps spurred by projects with potentially immediate and global reach, such as Libra[1], finance ministers of Germany, France, Italy, Spain and the Netherlands jointly stated that stablecoins should only be allowed to operate within the EU once regulatory frameworks have been established.

Meanwhile, a draft of the proposal by the European Commission has surfaced[2]. The draft claims to aim at achieving four objectives:

- **to provide legal clarity and certainty for the use of DLT in financial services;**
- **to support innovation and fair competition;**
- **to protect consumers and investors;**
- **to address financial stability and monetary policy risks.**

The proposal outlines that regulation should be harmonized within all EU member states. More concretely, guidelines for the issuance of crypto assets are proposed. According to these guidelines, each issuer of crypto assets must publish a whitepaper (that describes, for example, the rights of token holders) – similar to traditional documentation requirements for financial products, such as key investor information documents or a prospectus. The practice of publishing whitepapers is already customary within the crypto sphere, even though the quality of whitepapers varies. Furthermore, and specifically for asset-backed tokens such as stablecoins or “e-money tokens”, issuers must register as a credit institution or an electronic money institution. Both new harmonized licenses and mandatory use of existing ones will enable what is currently lacking: Passporting from one EU member state to the whole market.

On the topic of stablecoins, one distinction is made: Algorithmic stablecoins that attempt to stabilize the price of the token by controlling supply and demand and without referencing a fiat currency are treated separately, but marketing them as “stable” would be prohibited under the proposal. It is unclear if an algorithmic “stablecoin” that references, for example, inflation metrics like CPI would fall under these regulations.

The proposal also exempts central banks from these regulations, simplifying the issuance of potential central bank digital currencies (CBDCs), which is an area that the ECB and other central banks have been actively exploring.

Swiss DLT Law Passed

Last week, the Swiss Parliament has accepted[3] – without opposition – adjustments to Swiss law that would incorporate and regulate the use of distributed ledger technology (DLT). The law was originally filed in November 2019[4] for discussion in parliament. Its aim is to embrace the opportunities presented by DLT and to improve legal certainty for businesses that incorporate the technology into their processes. It also addresses what happens with crypto assets in the case of bankruptcy. This act also incorporates current practices and interpretations into formal law. Amendments to both civil law and financial markets law will be made; these legally enable a new financial markets infrastructure using DLT-based trading systems, amongst other innovations.

Bitcoin and Schnorr Signatures

Meanwhile, in the crypto space, Bitcoin core developers have gotten one step closer to integrating support for Schnorr signatures[5] in Bitcoin by integrating[6] the relevant Bitcoin Improvement Proposal (BIP-340[7]) into the secp256k1 library. The proposal was originally written in 2018.

Schnorr signatures are potentially superior to elliptic curve signatures (ECDSA, the current signature algorithm of Bitcoin). They allow multi-signature transactions to be indistinguishable in terms of signature size from "normal", single-signature transactions, which enhances Bitcoin's pseudonymity features. Theoretically, they would also help to improve the scalability of Bitcoin, since the signature size from transactions with multiple unspent transaction outputs (UTXOs) as inputs could be reduced.

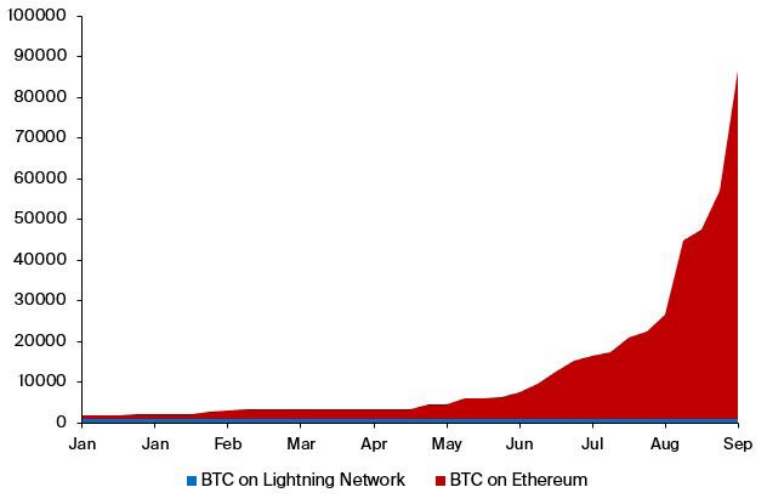
Another feature is that transactions that open and close channels on the Lightning Network, a second layer scaling[8] technology for Bitcoin, would look equal to and be just as expensive as regular transactions.

Bitcoin on Ethereum Grows

The Lightning Network, however, still struggles to get significant traction. It appears that for now, Ethereum de facto acts as "Bitcoin's Layer 2" – the amount of Bitcoin that is now pres-

ent on Ethereum in tokenized form has exploded[9] over the past months, alongside the general hype for decentralized finance (DeFi).

Illustration 1: Currently, close to 90'000 BTC (around $900M) are on Ethereum in tokenized form, whereas the Lightning Network has a capacity of around 1'100 BTC.



Source: btconethereum.com, bitcoinvisuals.com, Bitcoin Suisse Research

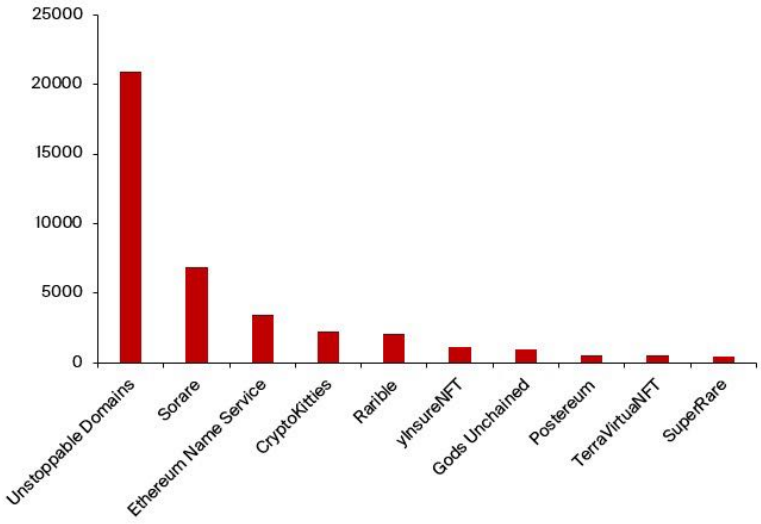
As seen in Illustration 1, the amount of Bitcoin tokenized on Ethereum far eclipses the amount that is locked in the Lightning Network. This is perhaps mostly attributable to the ability to collateralize Bitcoin and "yield farm"[10] with it, achieving high yields on BTC that would otherwise sit idle in cold storage (albeit with a very different risk profile of the returns).

This synergistic interaction between the two largest blockchains (by market capitalization) enhances the value proposition of both chains – Bitcoin can now easily be collateralized using DeFi on Ethereum. If trustless bridges between the two chains (as pursued, for example, by the RenVM[11]) can be established, the whole process becomes permission- and trustless. Especially the permissionless nature would be an advantage of the "digital gold" over normal gold. In the longer term, however, moving Bitcoin off its native chain might also cut into miner revenues coming from transaction fees if it happens in large amounts. This becomes increasingly relevant as the block subsidies are reduced through reward halvings.

ERC-721: Non-Fungible Tokens

Besides the growth of the amount of BTC on Ethereum, another class of tokens is starting to complement the DeFi space: ERC-721 tokens, or non-fungible tokens (NFTs). These tokens are each unique and distinguishable from each other, as opposed to "regular" (ERC-20), fungible tokens.

Illustration 2: Transfer volumes of non-fungible tokens over the past 7 days in various sectors, such as domain names (Unstoppable Domains, Ethereum Name Service), digital collectibles (Sorare, CryptoKitties, Rarible), and insurance (yInsureNFT).



Source: etherscan.io, Bitcoin Suisse Research

Since inception of the NFT markets, over $100M in value[12] has been transferred. Much of this was during the CryptoKitties hype[13] in 2017 and from the decentralized virtual world Decentraland.[14] But other sectors, such as digital collectibles, have also been growing, as shown in Illustration 2.

Digital collectibles are ideally represented by ERC-721 tokens, since each item is unique. These collectibles can, for example, be digital-first art or digitized art, with provable ownership represented on the blockchain.

Another use case comes from the gaming industry, which has shown strong growth[15] over the past decade. Games often offer purchasable in-game items, but true ownership of the item is not achieved since it lies with the issuing company. Transforming such items into NFTs could change that. One blockchain-native example is the trading card game Gods Unchained,[16] where each card is represented by a token.

Beyond these two applications, NFTs also open up the door to integrating more financial products in the DeFi space. One example is insurance – as, for example, yinsure.finance[17] insurance covers that can be traded on the secondary markets. The NFT specifies the insured amount as well as the duration of the cover. While the initial cost of the insurance is set by the NFT issuer (the underwriter,[18] in this case, is Nexus Mutual,[19] a decentralized insurance protocol), the NFT representing the insurance contract can afterwards be freely traded on a secondary market (such as Rarible,[20] in this case).

This allows the market to continuously assign a fair rate for the insurance contract. The major use case for insurance, currently, is within the crypto space – DeFi users take out insurance on the protocols they use (such as Compound, Aave or Balancer). In this case, a new audit of such a protocol by a reputable auditor would likely impact the fair market price of such an insurance cover.

It is also conceivable that NFT markets can be extended to other products with fixed, unique terms – perhaps with a more direct link to the real world, such as mortgages.

Conclusion

Over the past weeks, regulatory uncertainty for the crypto space has been reduced. It remains to be seen if the newly developed regulations achieve their goals of providing a proper legal framework without stifling innovation.

For now, innovation in crypto continues at a rapid pace, and specifically in DeFi. Big opportunities have already been seized, and more may lie ahead in the form of non-fungible tokens. However, the exponential growth that is currently seen is a result of the building blocks[21] that were developed not over the past two months, but through the entirety of 2018 and 2019.

Sources

1 https://www.bitcoinsuisse.com/research/decrypt/stablecoins-navigating-crypto-volatility

2 https://www.politico.eu/wp-content/uploads/2020/09/CLEAN-COM-Draft-Regulation-Markets-in-Crypto-Assets.pdf

3 https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200511~01209cb324.en.html

4 https://www.newsd.admin.ch/newsd/message/attachments/59301.pdf

5 https://www.bitcoinsuisse.com/outlook/bitcoin-in-2020-halving-the-block-reward

6 https://github.com/bitcoin-core/secp256k1/pull/558

7 https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki

8 Bitcoin Suisse Decrypt Series 2, "Scaling the second Layer"

9 Bitcoin Suisse Decrypt Series 2, "The Aftershock of Governance Tokens"

10 Bitcoin Suisse Dectypt Series 2, "Token Incentives in Decentralized Finance"

11 https://renproject.io/renvm

12 https://nonfungible.com/market/history

13 https://www.bitcoinsuisse.com/research/decrypt/scalability-the-missing-piece

14 https://decentraland.org/

15 https://resources.newzoo.com/hubfs/Reports/Newzoo_2019_Global_Games_Market_Report_Press_Copy_v2.pdf

16 https://godsunchained.com/

17 https://yinsure.finance/

18 https://twitter.com/iearnfinance/status/1295987832742391809

19 https://www.bitcoinsuisse.com/research/decrypt/on-chain-derivatives-and-insurance

20 https://app.rarible.com/

21 https://www.bitcoinsuisse.com/research/decrypt/leveraging-blockchain-for-decentralizing-finance

Airdrops and Forks – Free Money?

Airdrops of cryptocurrencies have become a regularly used tool to either market the existence of a coin, or to achieve a sufficiently decentralized initial coin distribution. Are airdrops simply “free money”? And if yes, do forks also fall into this category?

Uniswap, a decentralized exchange using an automated market maker (AMM) model[1], recently surprised the crypto community with the launch of their UNI governance token[2], airdropping it to all users that have used the protocol prior to September 1. Each Ethereum address that had interacted with the Uniswap contracts was eligible for claiming at least 400 UNI tokens, with loyal liquidity providers receiving much higher amounts. At UNI's all-time high valuation of $8.40, this amounted to $3'360 worth of UNI tokens, and at current valuations is still worth around $1'800. The reasoning for this airdrop was that previous, unincentivized users of the protocol should constitute the best community to govern Uniswap in the future.

What is an Airdrop?

An airdrop, in general, is the distribution of a token either through freshly minting it or directly from a treasury (such as a team's reserve of their own token). Recipients can either be holders of other cryptocurrencies, or people who became eligible for the airdrop in other ways – such as interacting with the protocol in the past in the case of Uniswap. The goal of an airdrop is often to build awareness around a project, and to obtain a broader user base. Airdrops have been carried out both for already existing currencies (such as Stellar's XLM) or as a mechanism to achieve the initial token distribution (UNI).

One crucial aspect that projects need to consider when airdropping coins or tokens is the prevention of "sybil attacks". A sybil attack, in simple terms, is the creation of many identities by a single person, mostly in pseudonymous or anonymous systems (such as most public blockchains). This would allow them to obtain much more tokens during the airdrop than intended. In the case of Uniswap, this was subverted by keeping the distribution method of 400 UNI per address private, and then snapshotting a date in the past to check for eligibility. Other airdrops have attempted to prevent sybil attacks through identity checks – such as requiring participants to link their social media profiles, their GitHub account or even a full KYC check. On a cautionary note, potential airdrop participants should carefully verify the legitimacy of a project before undergoing full KYC due to the danger of identity theft.

Large Airdrops in the Past

While most airdrops fail to accrue any significant value for the recipients, a few have managed to gain traction in the secondary markets and temporarily became fairly valuable.

Illustration 1: A selection of airdrops since 2016 that managed to attain significant value. The Decred (DCR) airdrop with an all-time high value of $36'500 stands out.

Airdrop	Eligible	Token Amount	ATH Value	Current Value
DCR	Sign up	282.6 DCR	$36'500	$3'332
UNI	Uniswap users	400 UNI/address	$3'360	$1'828
GBYTE	BTC holders	1.865 GBYTE/BTC	$2'211/BTC	$41.9/BTC
XLM	BTC holders	1'178 XLM/BTC	$1'031/BTC	$88/BTC
OMG	ETH holders	0.075 OMG/ETH	$1.92/ETH	$0.246/ETH

Source: Airdrop summaries linked below, coingecko.com, Bitcoin Suisse Research.

Besides UNI, another airdrop which was not tied to holding another cryptocurrency was the Decred airdrop[3], which ended on Jan. 18, 2016. Interested participants needed to sign up and shortly describe their interest in the project. In the end, 282.6 DCR were distributed to each participant. The coin attained its all-time high two years later, on Jan. 13, 2018, at $129.4/DCR – airdrop recipients who cashed out at this point got $36'500.

Bitcoin holders were eligible for two of the major airdrops listed above: Byteball (GBYTE) and Stellar Lumens (XLM). The Byteball airdrop[4] took place on Dec. 25, 2016 and was available after signing up. 10% of the GBYTE coin supply was initially distributed, with additional airdrops afterwards, totaling 1.865 GBYTE per BTC. At all-time high valuations, this was worth around $2'200 per BTC. Stellar, on the other hand, distributed 19 billion XLM to BTC holders who signed up for it in two snapshots of the BTC blockchain (3 billion in July 2016[5], and 16 billion in June 2017[6]). In total, BTC holders were able to obtain 1178 XLM per BTC, which was once worth around $1'000 (now $88). Since these two airdrops were relative to BTC holdings, they were especially lucrative for large BTC holders.

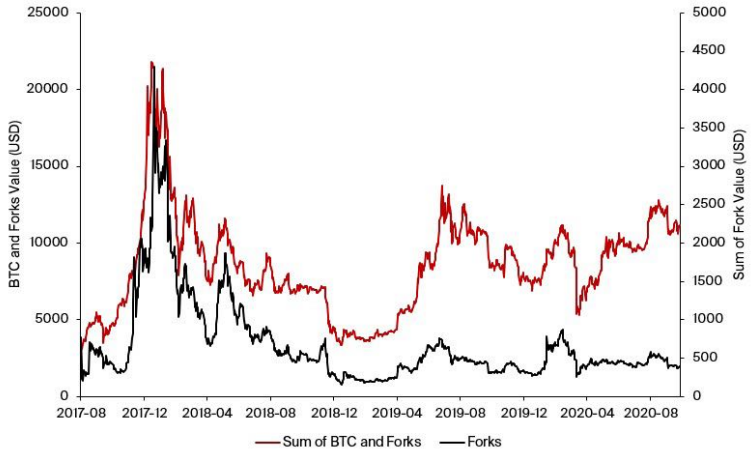
Holders of ETH also got a chunk of the pie when the OMG network (formerly OmiseGo) airdropped[7] 140 million of their OMG token (5% of the total supply) in July 2017. Each address holding at least 0.1 ETH received an airdrop amount proportional to their share in the total ETH supply (93.1 million ETH at the time), without signing up for it. This results in 0.075 OMG airdropped per ETH – at ATH valuation worth close to $2.

Forks: A Special Form of Airdrops?

Hard forks, meaning forks that are backwards-incompatible, can either take place in a contentious or non-contentious manner. The contentious variant, where part of the community disagrees on how the protocol should move forward, usually creates a second branch of the blockchain and leads to a new coin.

Illustration 2: During the heights of the 2017 bull run, the cumulative value of BTC forks (rhs) amounted to $4'300 per coin. Currently, the forks are worth around $400 in total.

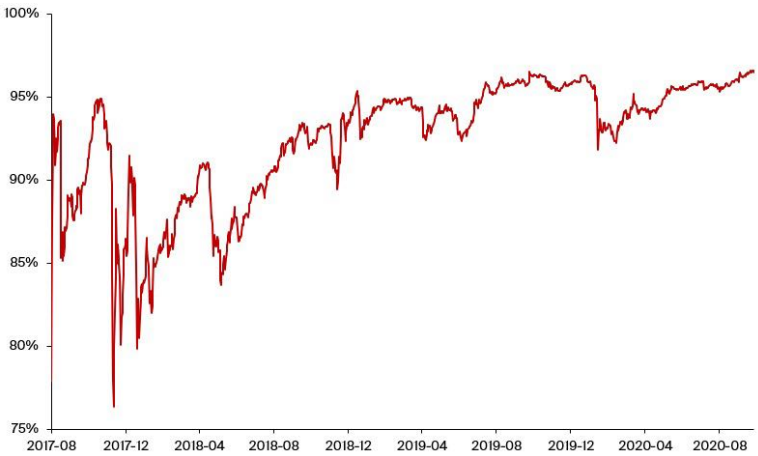
The Bitcoin forks[8] are arguably the most famous ones. Bitcoin first split into BTC and Bitcoin Cash (BCH)[9] on Aug. 1, 2017. Later, additional forks that created Bitcoin Gold (BTG) and Bitcoin Diamond (BCD) occurred in October and November 2017, respectively. Bitcoin Cash further split into BCH and Bitcoin Satoshi Vision (BSV)[10] on November 15, 2018.



Source: coingecko.com, Bitcoin Suisse Research.

The sum of BTC and forks can be considered to be the value of a pre-August 2017 (before the BCH fork) "untouched" BTC coin, since the controller of the corresponding private key can claim her or his share of the forked coins. Another way to look at this data is to study the "BTC fork dominance": What is the share of the value of BTC with respect to all forks?

Illustration 3: While periods following a fork appear to be more volatile (late 2017, Nov. 2018), over time, most value has accrued to BTC so far. Currently, BTC's fork dominance stands around at 96.6%.

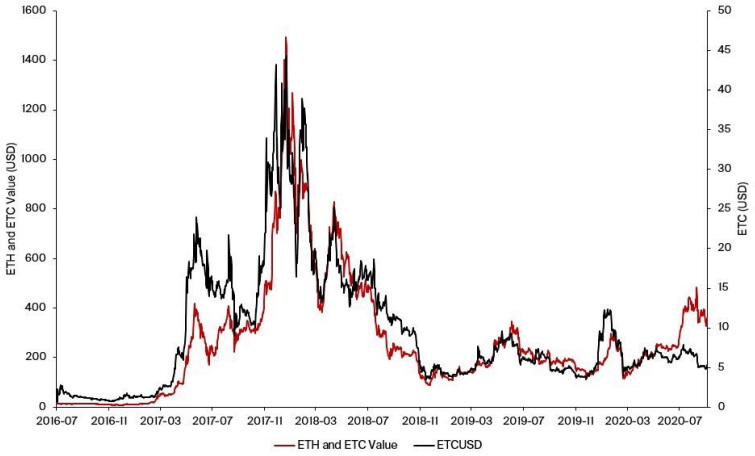


Source: coingecko.com, Bitcoin Suisse Research.

Another significant fork that led to great disputes in the com-

munity was the split of Ethereum after TheDAO in July 2016, an early experiment in building a decentralized autonomous organization (DAO). The smart contract involved was susceptible to a reentrancy attack[11], and 3.6 million ETH were stolen from the contract. The Ethereum community decided to do a hard fork to return this ETH, but not everyone agreed: Out of this incident, Ethereum Classic (ETC)[12] was born, where the hacker remained in possession of the ETC.

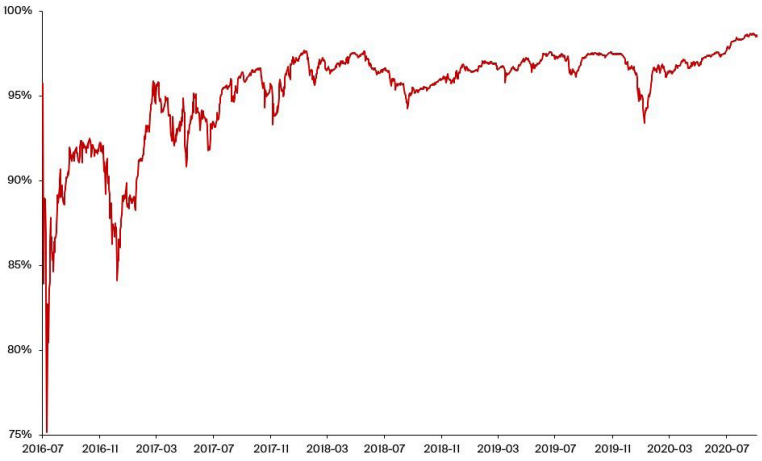
Illustration 4: Prices of ETH and ETC have been relatively strongly correlated throughout their existence, although ETC never managed to achieve meaningful share of the overall Ethereum market cap.



Source: coingecko.com, Bitcoin Suisse Research.

This can again be expressed differently, and perhaps more elegantly, by looking at the "ETH fork dominance". It denominates how much of the value of a pre-July 2016 ETH coin is now captured by the current ETH.

Illustration 5: After an initial volatile phase where the ETH fork dominance dropped down to almost 75%, ETH has now captured almost all of the Ethereum market cap (currently around 98.5%)



Source: coingecko.com, Bitcoin Suisse Research.

Looking at the performance of forked coins overall, so far, the majority of the value has accrued to BTC and ETH.

Are Airdrops and Forks Printing Money Out of Thin Air?

Whether airdrops and forks have value is in the hands of secondary market participants. They can be thought of similar to the recent yield farming craze[13] for governance tokens, where APRs of >100% could be achieved that were essentially subsidized by secondary market buyers. As in any market, sustainably high prices can only materialize if long-term investors decide to provide buyside liquidity, otherwise "free money" sellers will quickly depress prices.

Not all airdrops and forks are equal, though – while many end up losing the majority of their market cap, those that can create actual value and build strong communities may lead to a justified increase in the total cryptocurrency market capitalization.

Sources

1 Bitcoin Suisse Dectypt Series 2, "Token Incentives in Decentralized Finance"

2 https://uniswap.org/blog/uni/

3 https://medium.com/@dcrthegreat/decreds-airdrop-explained-2bf1c587c779

4 https://wiki.obyte.org/Airdrop#Current_rules_and_rates

5 https://www.stellar.org/blog/bitcoin-claim-lumens

6 https://www.stellar.org/blog/bitcoin-claim-lumens-2

7 https://www.omise.co/omisego-airdrop-update-2

8 https://iconow.net/list-of-bitcoin-forks/

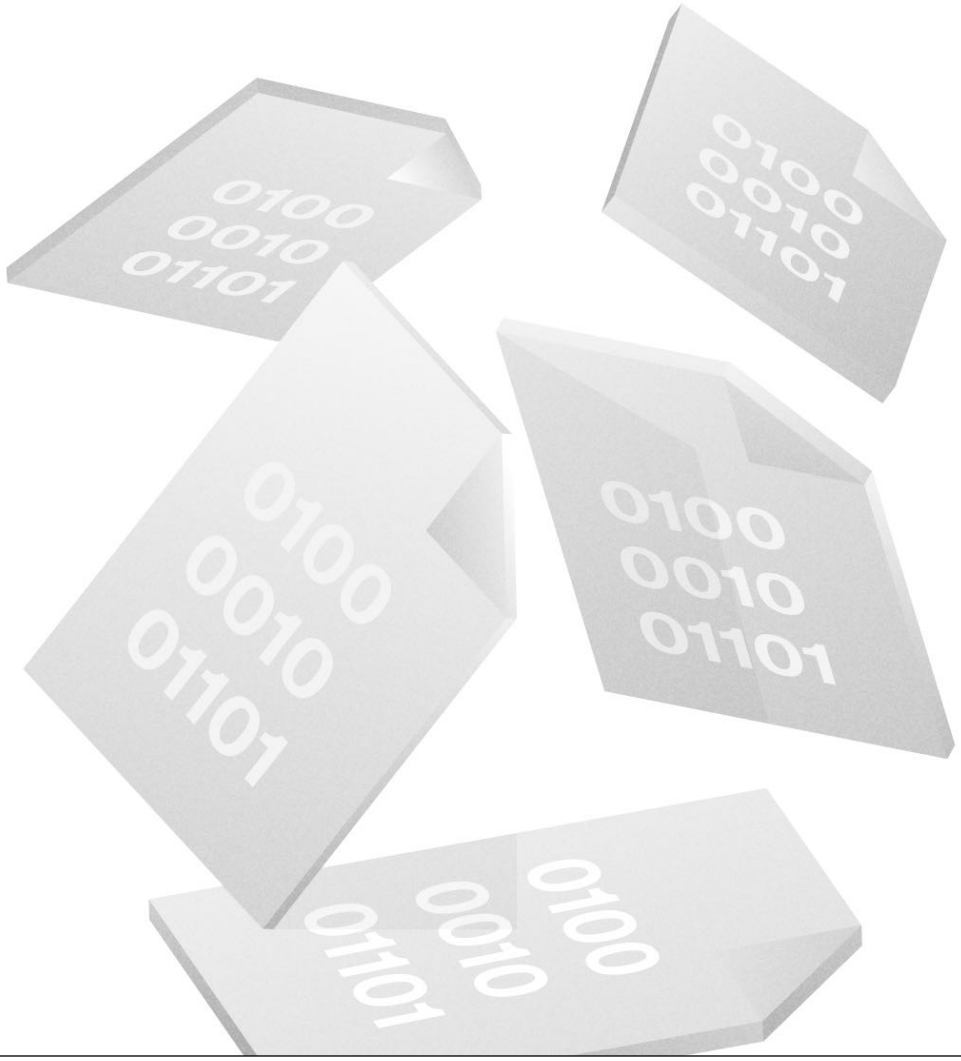
9 https://www.bitcoinsuisse.com/fundamentals/what-is-bitcoin-cash

10 Bitcoin Suisse Decrypt Series 2, "Bitcoin SV: Back to Genesis"

11 https://medium.com/@zhongqiangc/smart-contract-reentrancy-thedao-f2da1d25180c

12 https://github.com/ethereumbook/ethereumbook/blob/develop/appdx-forks-history.asciidoc

13 Bitcoin Suisse Decrypt Series 2, "The Evolving Open Finance Ecosystem"



Evaluating Smart Contract Security

Smart contracts allow for broad automation of financial and other operations, removing unnecessary intermediaries. However, interactions with smart contracts always bear risks of bugs in the code. A model based on game theory could help to quickly estimate how safe a smart contract is.

"Code is law". This (controversial) mantra illustrates one particular property of a trustless system based purely on code: There is no direct recourse against exploits of bugs in smart contracts. As such, smart contract risk is a major factor to assess when using blockchains with such capabilities.

During the recent hype around decentralized finance (DeFi)[1], hundreds of millions of dollars flowed into smart contracts, often even ones without an audit by reputable firms. Part of the DeFi yields can be argued to come from the fact that smart contract risk always remains – any piece of code can contain bugs. Thus, the question becomes: How does one judge how risky a certain smart contract is?

Smart Contract Audits

Traditionally, the first factor to look out for is an in-depth, high quality audit (or multiple audits) which tries to find possible exploits. On a technical level, these can simply be bugs in the code that would lock funds in the contract or leave them at risk of being stolen. However, the economic dimension also needs to be considered: Are there any design choices that allow a malicious actor to exploit the system for profit?

Additional consideration should be given to the level of decentralization (do so-called admin keys that grant full power exist?) and the potential impact of governance decisions. Governance of protocols is often in the hands of token holders (e.g. in a decentralized autonomous organization, a DAO). In this case, security measures such as a time delay for the implementation of governance decision can give protocol users enough time to react.

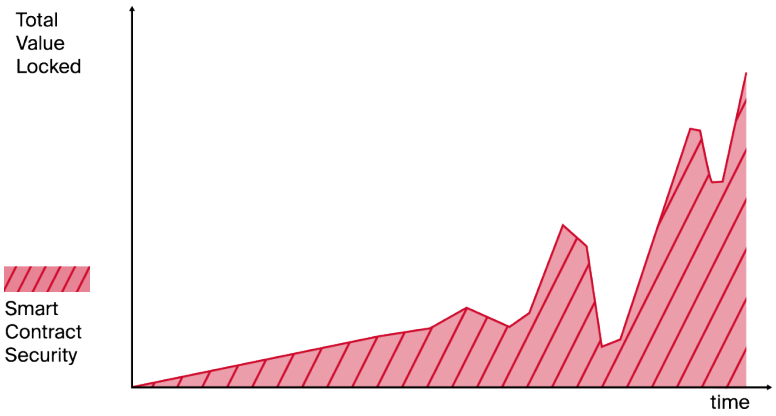
Overall, however, the assessment of smart contract risk remains highly complex and only a small minority of crypto users will be able to properly judge it for themselves. Thus, a way to gauge the security of a smart contract more simply could complement the fundamental approach via audits.

The Game-Theoretical Approach

From a game-theoretical perspective, the security of a smart contract is a function of its time in existence as well as the total value locked/secured by the contract. This can be illustrated with an intuitive example: Imagine a situation where one must place $10M into one of two smart contracts. Each of the two smart contracts already hold $100M, but the first smart contract did so for one year, whereas the second contract is only one week old. The logical choice, given no other information,

would be to place it into the first smart contract. The example can also be inverted to account for value locked, where both exist for one year, but one has $100M locked and the other one only $10M. Mathematically speaking, the smart contract security is the integral over time of the (time-dependent) total value locked function.

Illustration 1: Smart contract security increases both with time passing, as well as with a higher amount of money secured by the smart contract. It can be interpreted as the entire area below the total value locked curve.

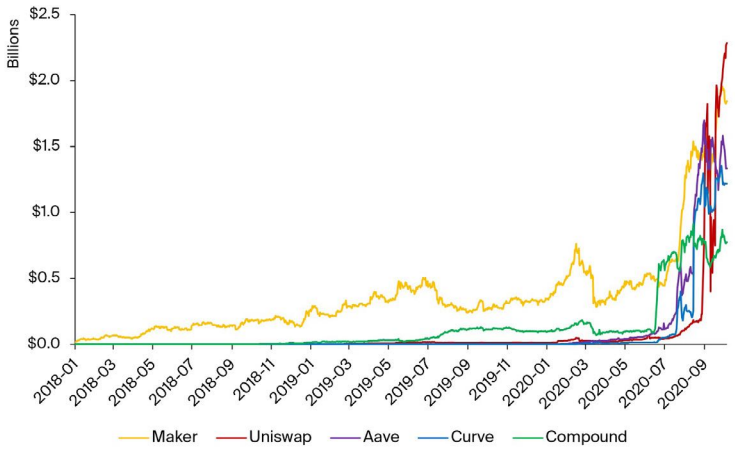


Source: coingecko.com, Bitcoin Suisse Research.

Smart contracts that secure large amounts of money are essentially a perpetual bug bounty program, where the maximum bounty is the value locked in the smart contract. Flash loans – which enable anyone to borrow unlimited amounts, although only if the loan is returned within the same block/transaction – have made exploiting bugs more capital efficient. The bug bounty program is hence open to anyone in the entire world, irrespective of available capital.

The DeFi boom in the recent months has boosted these bounties to multiples of their previous levels. While Maker accounted for the majority of value locked in 2018/2019, since the start of liquidity mining in Compound, all major protocols have increased their total value locked (TVL) to >$500M.

Illustration 2: The total value locked (TVL) – and thus the "bug bounty" for finding catastrophic exploits – has skyrocketed in the last months. In the years 2018 and 2019, Maker has been the undisputed king of DeFi by TVL.



Source: defipulse.com, Bitcoin Suisse Research.

Based on this data and the considerations above, it is possible to generate a "ranking" for smart contract security of DeFi protocols by summation of the value locked over time. The top 15 protocols by TVL at the time of writing were considered, but the methodology is readily scalable to hundreds of contracts.

Illustration 3: In the ranking of smart contract security by the methodology outlined above, Maker, Compound, and Synthetix take the top spots. The score of Maker is normalized to 100.

Rank	Protocol	Security Score
#1	Maker	100.0
#2	Compound	32.5
#3	Synthetix	27.1
#4	Aave	25.8
#5	Uniswap	19.9
#6	Curve	18.7
#7	Yearn	12.7
#8	Balancer	10.9
#9	InstaDApp	8.6
#10	Bancor	4.5
#11	dYdX	3.1
#12	NexusMutual	1.4
#13	SetProtocol	1.0
#14	mStable	0.9
#15	Loopring	0.6

Source: defipulse.com, Bitcoin Suisse Research. The formula for calculating the Security Score is: 100*Sum of daily TVL(project)/Sum of daily TVL(Maker).

In this model for security, the top 5 spots are occupied by DeFi heavyweights Maker, Compound, Synthetix, Aave and Uniswap.

Shortcomings of the Model

While this model is appealing due to its simplicity of both design and security score calculation, the simplification comes with multiple tradeoffs and should hence only be viewed as a rough estimate of how trustworthy a smart contract is.

To list a few of the tradeoffs or approximations that the model makes:

- **Smart contract upgrades and upgradeability are not considered (such as, for example, Maker's switch to multi-collateral DAI from being solely ETH-backed)**
- **It does not consider past exploits and subsequent bug fixes, which should reset the score to zero**
- **Composability of DeFi is not considered – for example, Yearn (#7) uses a multitude of other protocols on the list in the background and should thus never score higher than any of the protocols it uses**

There are other refinements that could be made, such as evaluating whether time in existence should be weighted more strongly ("Are $100M locked for 1 week as valuable for security as $10M locked for 10 weeks?") or if there are diminishing marginal benefits to TVL once it crosses a critical threshold, arguing that a $100M "bug bounty" attracts as many capable eyes as $1B does.

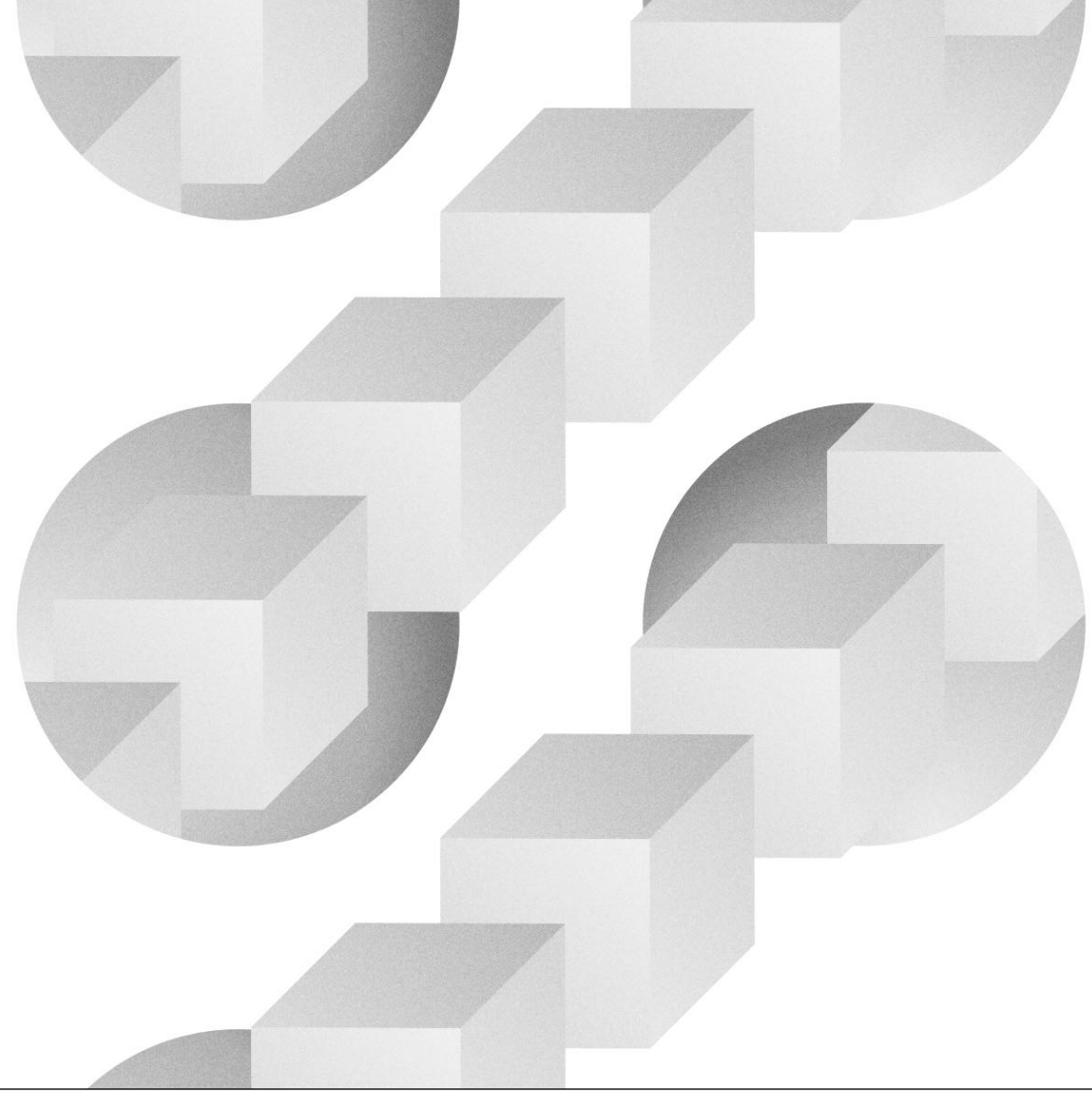
Additionally, the model may also be extendable to smart contract wallets, as well as smart contracts that do not "lock" value inside directly, but handle large volumes of transfer (such as relayer contracts).

Conclusion

The model of evaluating smart contract security from a game-theoretical perspective and attempting to gauge it through a combination of time in existence plus value locked is simple in its design and highly scalable, since all necessary data is readily available on the blockchain. Thus, it may serve as a quick, first estimate of a smart contract's security. However, a thorough assessment of smart contract risk remains a complex problem, and a more fundamental analysis of the risk should always complement the model.

Sources

1 Bitcoin Suisse Decrypt Series 2, "The Evolving Open Finance Ecosystem"



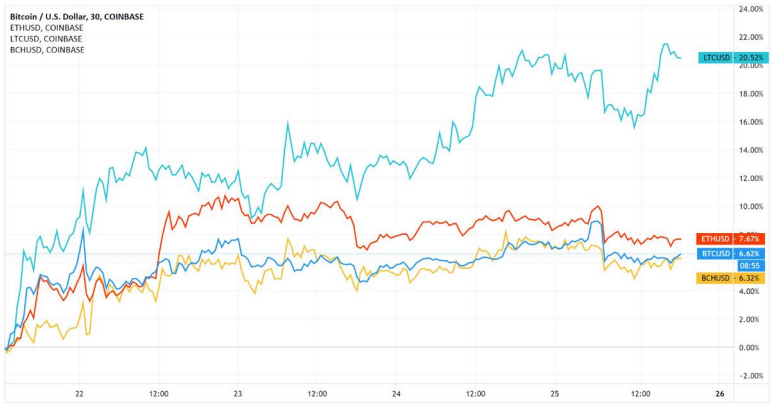
Onboarding the Next Wave to Crypto

One of the core challenges for cryptocurrencies and their underlying blockchains is how to achieve wide-spread adoption among the public. During the past weeks, several steps in that direction have been made. How did this impact the markets? And what are the longer-term implications?

The global adoption of cryptocurrencies continues at a rapid pace. Last week has seen another push, this time coming from fintech giant PayPal, who announced[1] that they will bring cryptocurrencies to 26 million merchants in early 2021. Their 300+ million customers will also be able to purchase Bitcoin, Ether, Litecoin and Bitcoin Cash directly, and use them as a means of payment in their day-to-day transactions.

The cryptocurrency markets reacted positively to the news: Since the announcement, the total crypto market cap rose from ca. $370 billion to $405 billion at the time of writing (+9.5%).

Illustration 1: All four currencies to be listed on PayPal initially have risen since the announcement just after noon on Oct. 21. Litecoin managed to outperform and is up +20.5% at the time of writing.



Source: tradingview.com.

A phenomenon that is occasionally seen in the cryptocurrency markets is that a coin or token experiences a sharp short-term price increase once it gets listed on a major exchange. One recent example of this are the listings[2] of REN and BAL on Coinbase on Oct. 1 – the price of REN increased by +19.1% that day, that of BAL by +13.1%; however, the sustainability of these short-term price increases warrants closer inspection. In the future, it is not inconceivable to see volatility in the markets following "PayPal listings".

Meanwhile, the crypto features that PayPal offers are very limited – crypto transfers in and out of an account or between users will be disabled, at least initially. This means that purchases there give no access to the trustless, disintermediated crypto ecosystem and transactions can always be censored (as opposed to on-chain transactions on public networks). Users will also not be able to explore the quickly growing DeFi ecosystem, as well as other crypto-native features and decentralized applications.

Escape the Walled Garden

In the end, what might arise is a situation similar to the early days of the Internet: Early providers, for example AOL, enabled going online through proprietary software, but the full depth of the web remained inaccessible. This familiarized users with the concept of using the computer to gain access to distributed information. Similarly, PayPal may familiarize users with the concept of holding cryptocurrencies as a means of payment/store of value.

If history is any indication, though, human curiosity will drive people out of the walled garden of the PayPal solution, and incentives such as a non-zero interest rate savings account in DeFi in a world where yield is scarce will encourage this.

Central Bank Digital Currencies

Also, the news might be relevant in light of potentially upcoming central bank digital currencies (CBDCs). Recently, Federal Reserve Chair Powell mentioned[3] that the U.S. is looking closely into digital currencies, and that 80% of central banks globally are. As such, CBDCs might become a reality sooner than would have been thought possible a year ago, and the push that the online realm received through the pandemic may have been a supporting factor. The proposed models for CBDCs differ in their details, but perhaps the most important distinction is between "wholesale CBDCs" (serving mostly financial institution as a digital settlement currency) and "retail CBDCs" (accessible to the public, as an addition to or a replacement for physical cash), with a spectrum of hybrid solutions in between. While wholesale CBDCs might bring incremental efficiency enhancements to the financial sector, it is the retail CBDCs that would represent a paradigm shift and whose economic implications be far greater. To name one example, a retail CBDC might allow implementation of monetary policy measures on a broad scale much more easily – be it in the form of applying negative interest rates directly to a CBDC, or in the form of distributing "helicopter money" to all wallet owners/citizens.

Bitcoin's Layer 2?

Bitcoin has long struggled to find consensus around a suitable way to scale the blockchain (the dispute over which has also spawned Bitcoin Cash[4] and Bitcoin SV[5]), and the Lightning Network has so far failed to gain any significant amount of traction.

The current global payments infrastructure could serve as an intermediate-term "second layer" scaling solution that still

relies on trust. PayPal's push towards cryptocurrencies may be an early, global step towards this (if/once crypto deposits are enabled), whereas in Switzerland and Europe, integration of cryptocurrencies with the payments infrastructure is advanced most prominently through Worldline[6].

This would also be aligned with one potential vision[7] for scalability that early Bitcoin contributor Hal Finney had – Bitcoin would serve as a limited supply reserve currency, while day-to-day transactions are handled through existing infrastructure. However, there should still always be the option to transact in a permissionless, censorship-resistant fashion directly on-chain.

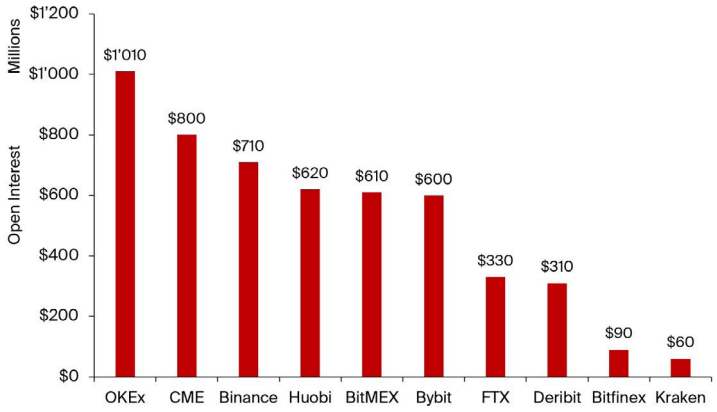
"I see Bitcoin as ultimately becoming a reserve currency for banks, playing much the same role as gold did in the early days of banking. Banks could issue digital cash with greater anonymity and lighter weight, more efficient transactions."

- Hal Finney

Institutional Market Grows

The attention the crypto space received from well-known financial institutions and investors is growing. In fact, the CME Bitcoin futures market, which is often seen as an indication of institutional participation due to its accessibility through the traditional financial infrastructure, is now the second largest in the market as measured by open interest (representing the amount of current positions in a derivative).

Illustration 2: The total open interest in derivatives now stands at over $5 billion across exchanges. The CME Bitcoin futures have recently claimed the number 2 spot, with $800 million in open interest.



Source: skew.com, Bitcoin Suisse Research

Prominent investors have reaffirmed their investment hypothesis for Bitcoin as an alternative asset class or an inflation hedge. Paul Tudor Jones, an American billionaire hedge fund manager, reiterated[8] on his small single digit percentage allocation (originally disclosed in May[9]) to Bitcoin; JP Morgan noted[10] Bitcoin's "considerable upside"; and Fidelity published[11] a report on Bitcoin's role as an alternative investment. The stance of central banks[12] towards monetary policy that may have led to people thinking more in detail about the value of money remains largely unchanged, and talks of additional stimulus have been occupying traditional markets. If worries around inflation down the road grow, Bitcoin may present a credible alternative way to store wealth.

"I've never had an inflation hedge where you have a kicker that you also have great intellectual capital behind it. So that makes me even more constructive on [Bitcoin]. If you think about it, if you're long [the US] 2s30s [yield curve] you're effectively short the bond market, that's your inflation hedge. You're really betting on the fallacy of mankind rather than its ingenuity and entrepreneurialism."

- Paul Tudor Jones

Sources

1 https://newsroom.paypal-corp.com/2020-10-21-PayPal-Launches-New-Service-Enabling-Users-to-Buy-Hold-and-Sell-Cryptocurrency

2 https://blog.coinbase.com/balancer-bal-and-ren-ren-are-launching-on-coinbase-pro-9f81ebfccbb5

3 https://www.bloomberg.com/news/articles/2020-10-19/powell-says-fed-has-made-no-final-decision-on-digital-currency

4 https://www.bitcoinsuisse.com/fundamentals/what-is-bitcoin-cash

5 https://www.bitcoinsuisse.com/fundamentals/what-is-bitcoin-sv

6 https://www.bitcoinsuisse.com/news/bitcoin-suisse-and-worldline-offer-crypto-payments-acceptance-switzerland

7 https://www.bitcoinsuisse.com/research/decrypt/scalability-the-missing-piece

8 https://www.cnbc.com/2020/10/22/-paul-tudor-jones-says-he-likes-bitcoin-even-more-now-rally-still-in-the-first-inning.html

9 https://www.scribd.com/document/460382154/May-2020-BVI-Letter-Macro-Outlook

10 https://markets.businessinsider.com/currencies/news/bitcoin-price-considerable-upside-forecast-competes-gold-alternative-currency-jpmorgan-2020-10-1029716041

11 https://www.fidelitydigitalassets.com/bin-public/060_www_fidelity_com/documents/FDAS/bitcoin-alternative-investment.pdf

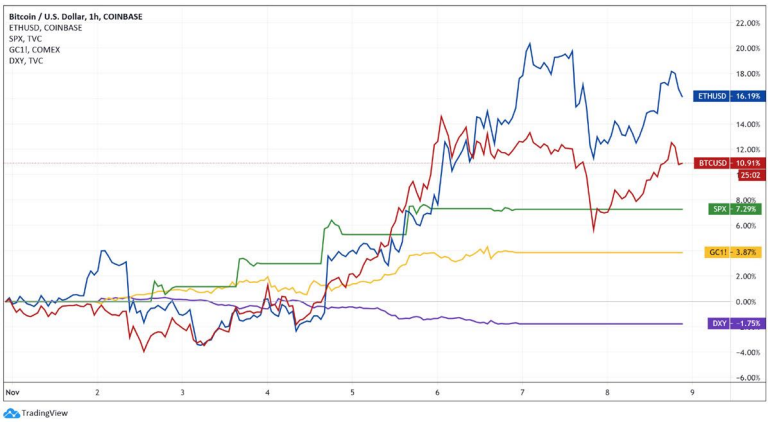
12 Bitcoin Suisse Decrypt Series 2, “Turn on the Moneyprinters!”

Ethereum 2 Is Coming

The deposit contract for Ethereum 2 was officially launched on Nov. 4. The genesis of the beacon chain, which is at the heart of Ethereum 2's architecture, is now likely to take place on Dec. 1. What are the implications for Ethereum? What changes, and what stays the same?

Last week, all eyes were focused on the U.S. presidential election on Nov. 3. As the event unfolded and uncertainty in the markets about likely outcomes was reduced, strong performances across the board were observed.

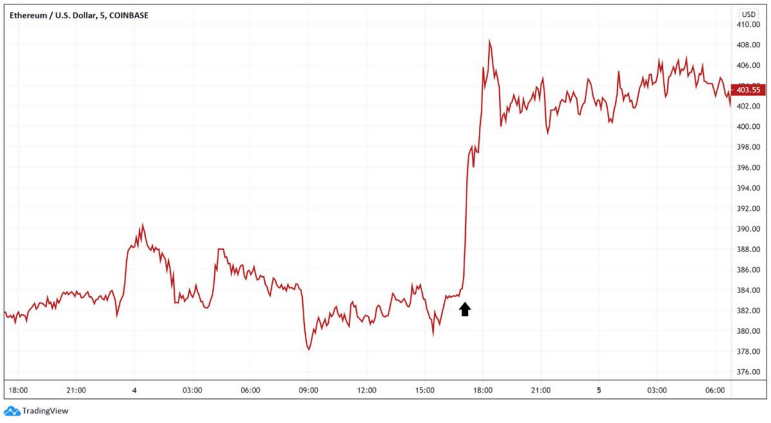
Illustration 1: Since the beginning of November and through the U.S. election week, BTC and ETH both performed strongly, up 11% and 16% at the time of writing, respectively. The dollar showed continued weakness.



Source: tradingview.com.

However, while the attention of the world was pointed elsewhere, the crypto space achieved another major, long-anticipated milestone: the official launch of the deposit contract[1] for Ethereum 2. The price of ETH reacted impulsively to confirmation that this was the official deposit contract through a tweet[2] by Ethereum co-founder Vitalik Buterin.

Illustration 2: ETHUSD at the time of the official deposit contract announcement. The black arrow indicates the timing of Vitalik's tweet, which was followed by a sharp 5% increase.



Source: tradingview.com

The deposit contract itself was already deployed[3] on Oct. 14, although the authenticity of the contract remained unclear. A bit of trivia: The deposit contract was deployed from an address funded through tornado.cash[4], a privacy protocol on Ethereum leveraging zero-knowledge proofs[5], and the rest of the funds

were donated[6] to WikiLeaks.

The launch date for the beacon chain (Ethereum 2 Phase 0, see below) is now set for Dec. 1 barring any unforeseen complications. For this to occur, 524'288 ETH need to be deposited to the deposit contract, corresponding to the 16'384 validators required to start the new blockchain (since each validator needs exactly 32 ETH). Roughly 47'500 ETH have been deposited so far (Nov. 8).

What Changes?

The main change for crypto markets that the launch of the beacon chain will bring is ETH staking. ETH will immediately become the cryptocurrency with the highest market capitalization that runs under Proof-of-Stake and hence offers the possibility to stake. The rewards for staking[7] are expected to fall in the 10-15% range initially (0.8-2M ETH staked), and drop relatively quickly down to 6-10% (2-6M ETH staked) if more people decide to stake their ETH.

These large amounts of ETH locked up in the deposit contract might also lead to higher volatility for ETH markets. Additionally, the fact that ETH staking exists and is likely to pay out decent rewards also means that borrowing and lending rates for ETH in DeFi protocols[8] such as Compound or Aave could adjust.

The participation rate in the beacon chain (meaning how many people decide to stake) will also show whether the economic incentives are properly designed and sufficient to attract enough validators. It will be the first test with real capital at stake to demonstrate that what worked well in various Ethereum 2 testnets (such as Medalla[9]) will also work in mainnet reality.

In the short term (until Phase 1.5, see below), overall issuance of ETH will also increase, since the cryptocurrency will be used to secure both the current Proof-of-Work Ethereum chain as well as the new beacon chain. This will bring overall issuance from currently about 4% to roughly 6%.

What Stays the Same?

Ethereum will not become immediately more scalable because of the launch of the beacon chain – the benefits to scalability will only show up at later stages of Ethereum 2. On a sidenote though, other scaling techniques[10] have recently been shown to be promising.

Staked ETH will not be transferable at least until Ethereum's Phase 1 – which is why it is also called "beacon ETH", "bETH",

or “ETH2” until full fungibility with non-staking ETH is restored. This also means that part of the overall newly issued ETH (projected to be around 6% annually) will remain locked up for some time. In a previous episode[11] on Ethereum 2, the possibility of an ETH2 futures market developing was also outlined, with some thoughts on possible liquidity premia for such a market.

The current Ethereum chain will continue operating as usual – at a later stage, the plan is to merge it with the new Ethereum 2 chain. This also means that the only action that is required by ETH holders is to decide whether to stake or not to stake.

Ethereum 2 Phases and Current Developments

The phases that Ethereum 2 will go through have been outlined in detail in the Outlook2020 report[12]; here is a short recap of the most important facts:

- **Phase 0: This phase involves the launch of the beacon chain. It does not represent a fully functional Ethereum blockchain yet, but simply provides the base layer and serves as a test for the economic incentive structure of ETH rewards for validators.**

- **Phase 1: In phase 1, sharding is introduced. Shards can be thought of as separate blockchains running on top of a coordination chain (in this case the beacon chain), and this parallelization of the blockchain is expected to lead to significant scalability advantages. “Beacon ETH” might become transferable already in this phase.**

- **Phase 2: Finally, this phase is when the new Ethereum chain will become fully functional, including e.g. smart contract capabilities. The old (current) Ethereum chain would be integrated into the new chain as a shard.**

Research on the individual phases happens in parallel, not in sequence – problems and roadblocks that later phases face can be solved while earlier phases are still in the process of implementation.

Several newer developments that have found broad community support are related to the introduction of a “Phase 1.5”. Phase 1.5 would integrate the current Ethereum chain as a shard in Ethereum 2, leading to a sharp drop in ETH issuance (by about

66%) and the end of Proof-of-Work on Ethereum. Even more recently and in the light of promising scaling techniques such as zero-knowledge rollups, a "Phase 1.5 and done"[13] approach found more support[14].

In this approach, shards would serve as data availability layers: Their main purpose would be to immutably record zero-knowledge proofs of transactions and smart contract interactions. Most of the actual transfers and contract execution would happen on the second layer. The argument for this is that second layer solutions[15] already today offer possibly greater scalability gains than what the original Ethereum 2 roadmap could bring. It is the combination of the two that has the potential to bring Ethereum to >100k transactions per second needed for a globally used settlement layer while remaining sufficiently decentralized.

Conclusion

Ethereum 2 is finally within reach, but the path towards a fully functional proof-of-stake based Ethereum chain is still long. Nonetheless, this is a major step for Ethereum overall, and one that has been planned since the very first block in July 2015. The years of research might finally pay off, and the rewards in terms of chain security and scalability can be reaped.

Sources

1 https://etherscan.io/address/0x00000000219ab540356cbb839cbe05303d7705fa

2 https://twitter.com/VitalikButerin/status/1324018999458295809

3 https://etherscan.io/tx/0xe75fb554e433e03763a1560646ee22dcb74e5274b34c5ad644e7c0f619a7e1d0

4 https://tornado.cash/

5 https://www.bitcoinsuisse.com/research/decrypt/the-identity-of-the-future

6 https://etherscan.io/tx/0x8aa30f7d95cd5f22dd02e59434c0e66794c6e370ed2659ea532ed6fe49f9cce5

7 https://www.bitcoinsuisse.com/research/specials/ethereum-2-matters-validator-economics

8 Bitcoin Suisse Decrypt Series 2, "The Evolving Open Finance Ecosystem"

9 https://beaconscan.com/

10 Bitcoin Suisse Decrypt Series 2, "Scaling the second Layer"

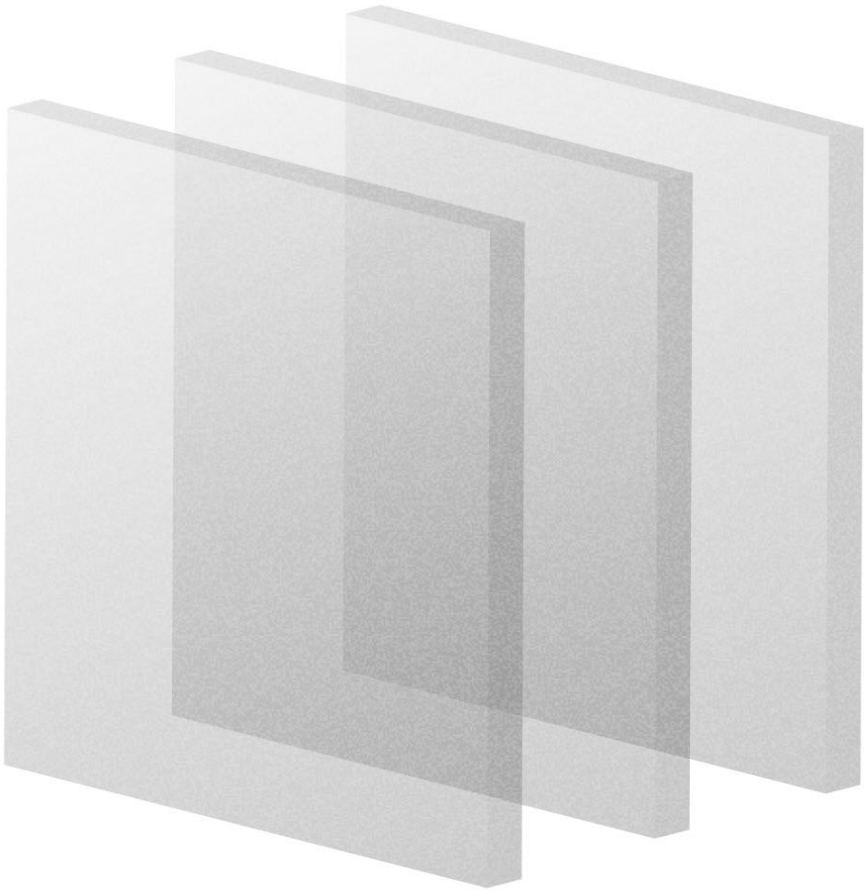
11 Bitcoin Suisse Decrypt Series 2, "Ethereum's Path to Serenity"

12 https://www.bitcoinsuisse.com/outlook/ethereum-and-its-transition-to-ethereum-2

13 https://ethresear.ch/t/phase-one-and-done-eth2-as-a-data-availability-engine/5269

14 https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698

15 Bitcoin Suisse Decrypt Series 2, "Scaling the second Layer"



Scaling the Decentralized Economy

Debates around scalability are as old as the crypto space itself. While in 2017, the “transactions per second”-mania spawned many layer 1 protocols, the understanding and scope of the term ‘scalability’ nowadays goes beyond simple throughput.

Scalability has been a long-standing topic of discussion in the crypto space. Already very early on, the necessity and future of Bitcoin's block size limit was debated[1], which much later led to the forks BCH and BSV. In the year 2017, a related metric – number of transactions per second – was brought into focus and was often used as a selling point for novel base layer protocols (which mostly sacrificed decentralization to achieve higher throughput), as both Bitcoin[2] and Ethereum[3] struggled with high transaction fees.

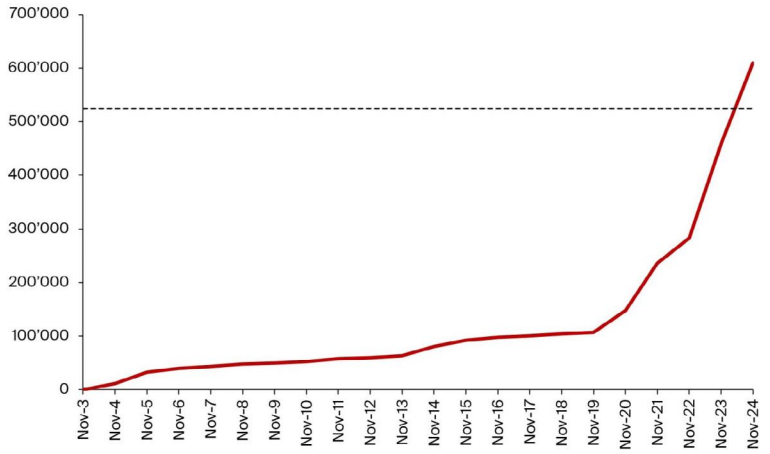
However, this type of "technical" scalability is not the only way the crypto ecosystem needs to scale. The overall crypto space, as measured by its total market capitalization of ca. $570 billion at the time of writing, is still small on a global scale. Plus, while the number of users and developers involved in crypto has grown at an astonishing pace, real world applications are still scarce. What is needed to scale technically, economically, and socially?

Technical Scalability

The approaches to scale from a technical side have been outlined in detail in a previous episode[4]. In the meantime, several developments have occurred.

Ethereum 2, which ultimately aims to increase Ethereum's base layer capacities, has met the criterion of 524'288 ETH in the deposit contract needed for the beacon chain genesis[5] on Dec. 1 – with around 600k ETH deposited currently.

Illustration 1: The pace at which ETH is being sent to the deposit contract has picked up. The 525k ETH threshold needed to ensure genesis of the beacon chain on December 1 has been reached.



Source: etherscan.io, Bitcoin Suisse Research.

On top of that, the implementation of second layer solutions is progressing, for example through the collaboration[6] of Optimism and Synthetix (using optimistic rollups[7] to scale). The

major challenge for DeFi protocols will be to switch to a second layer either all at once, or not at all – a gradual transition may run into problems, since composability is such a strong value proposition for the DeFi ecosystem and would temporarily be interrupted in this case.

On a protocol level, Polkadot's parachains[8] also hold a lot of promise. As a heterogeneous sharded system, the design of parachains allows for optimization for certain use cases, such as high transaction throughput or strong privacy guarantees. This means that base layer scalability can be achieved as required through a specific parachain.

For Bitcoin, the Lightning Network remains the scaling solution of choice. Recently, Lightning Pools[9] were introduced, which enable buying and selling of Lightning channels, and thus effectively created a market for liquidity in the Lightning Network. Overall adoption remains limited, though, and the total value locked currently stands at around $20M (or slightly more than 1'000 BTC).

Economic Scalability

The total crypto market capitalization currently is around $550 billion. The price of its native currency is an important metric for any public blockchain, since it is directly related to the security budget of a chain. Capital and operational expenses for miners and validators (who secure the network) still need to be paid in fiat currency. Thus, attacking a network becomes more costly the higher the price of the native token both in Proof-of-Work and Proof-of-Stake based system, and the network can hence secure more value.

The total value in the crypto space also represents the maximum amount of available collateral to build out the system. Not all collateral is equal; the native currency is the most trust-minimized and universally accepted collateral within one blockchain, but migration of one coin to another blockchain – in whatever form this takes place – to use as collateral is to be expected when the economic incentives are there. This has indeed happened with the surge of DeFi and tokenized Bitcoin[10] on Ethereum (currently more than $1 billion). While this is the first time a fully on-chain debt-based economy has grown to significant size and found its product-market fit, Bitcoin has been the main driver for the powerful, widespread off-chain (and mostly centralized) ecosystem consisting of spot and derivatives markets, lending and borrowing (e.g. miners collateralizing their BTC to fund operations instead of selling), and its continuously higher

acceptance as means of payment[11].

Scaling up the size of the decentralized economy can happen in two ways – either simply through higher prices for cryptocurrencies, or through onboarding more collateral into the system. This might happen in the future, for example, through the tokenization of traditional assets such as stocks, derivatives or real estate. The quality of this collateral would be worse than the native currency, since its value will likely rely on centralized counterparties (such as a company), but could still help to scale up the ecosystem.

Social Scalability

In the end, it is reasonable to assume that what provides most value to users of all kinds will get adopted most quickly. As such, the overall user experience as well as user interfaces matter a lot – a simple, one-click savings account in DAI would likely attract more users than the same savings account which needs to be set up by going through all the steps (of various approvals and transactions) individually. Simple onboarding mechanisms and accessibility are crucial to attaining social scale.

Similarly, a decentralized economy needs developers that create new decentralized applications and add to the value of a blockchain. This requires open-source libraries and code to build, easy to use software development kits and interfaces, and previous knowledge should be easily transferable.

A growing userbase will also bring up more discussions about the values and "unbreakable principles" of any blockchain. There is usually some loose social consensus about what those principles are – for Bitcoin, for example, one could name the limited supply of 21 million coins, its censorship resistance, or that the trustless verification of the entire chain should be easily possible (hence putting some constraints on acceptable node requirements). Despite being a global, decentralized system, this unwritten social contract between all community members is what unites and defines Bitcoin (and other cryptocurrencies). Over time and as the number of holders grows, this social contract becomes widely accepted, its clearer definition lowers the barrier to entry and the underlying protocol might ossify and adopt changes to it more slowly.

Conclusion

This framework of thinking about scalability could help to more easily identify strengths of certain protocols – while Ethereum's smart contract capabilities might allow it to more easily onboard

new collateral and scale economically, the social contract of Bitcoin is unrivaled in its simplicity and trust that it has built up over the past decade. Ultimately, improving all three aspects of scalability (technical, economic, and social) in some way will be needed for wide-spread adoption.

Sources

1 https://bitcointalk.org/index.php?topic=1347.msg15366#msg15366

2 https://www.bitcoinsuisse.com/research/decrypt/transaction-fees-markets-for-block-space

3 https://www.bitcoinsuisse.com/research/decrypt/scalability-the-missing-piece

4 Bitcoin Suisse Decrypt Series 2, “Scaling the second Layer”

5 Bitcoin Suisse Decrypt Series 2, “Ethereum 2 Is Coming”

6 https://blog.synthetix.io/why-optimism/

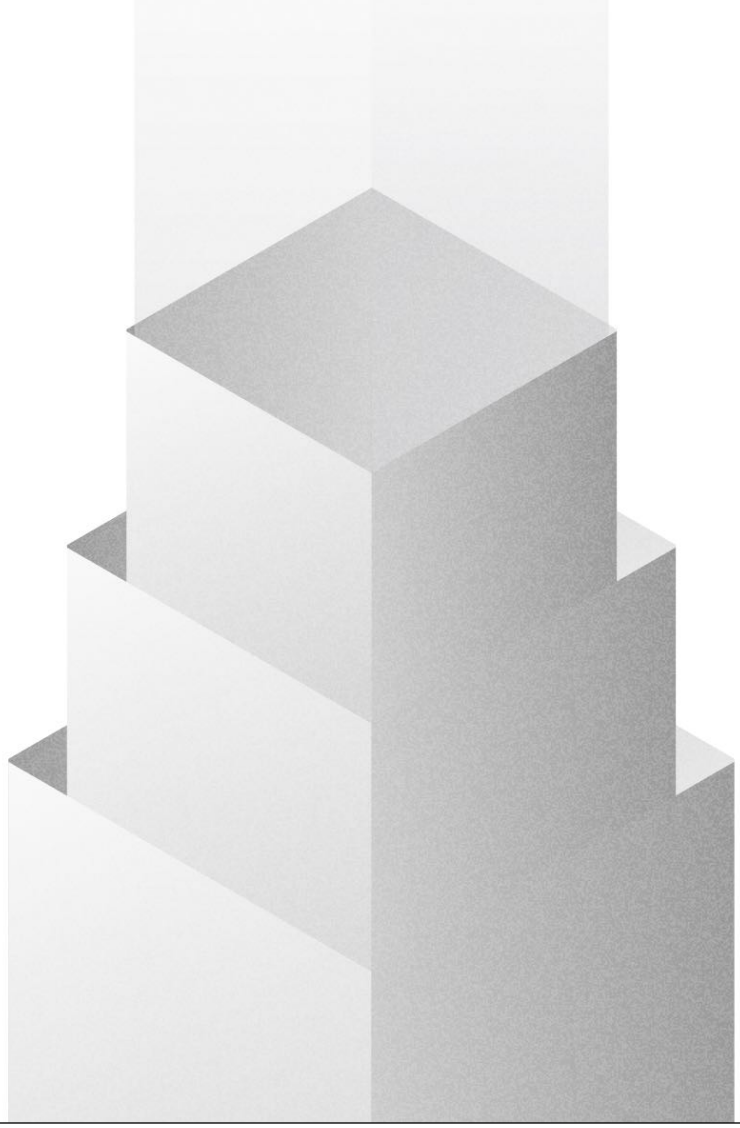
7 https://medium.com/plasma-group/ethereum-smart-contracts-in-l2-optimistic-rollup-2c1cef2ec537

8 https://wiki.polkadot.network/docs/en/learn-parachains

9 https://lightning.engineering/posts/2020-11-02-lightning-pool/

10 Bitcoin Suisse Decrypt Series 2, “The Aftershock of Governance Tokens”

11 Bitcoin Suisse Decrypt Series 2, “Onboarding the Next Wave to Crypto”



The Year 2020 in a Nutshell

“Black Thursday”, the Bitcoin block reward halving, DeFi hype, as well as the launch of both Ethereum 2 phase 0 and Polkadot – this year has certainly been exciting for the crypto space. What were the most important events? How did cryptocurrencies perform overall?

The year 2020 is slowly coming to an end. It has certainly been an extraordinarily eventful year, also for the crypto space. This episode recaps the most important events for the markets and highlights crucial fundamental developments – from "Black Thursday" (March 12) to the recent launch of phase 0 of Ethereum 2.

The Time Bitcoin Almost Went to Zero

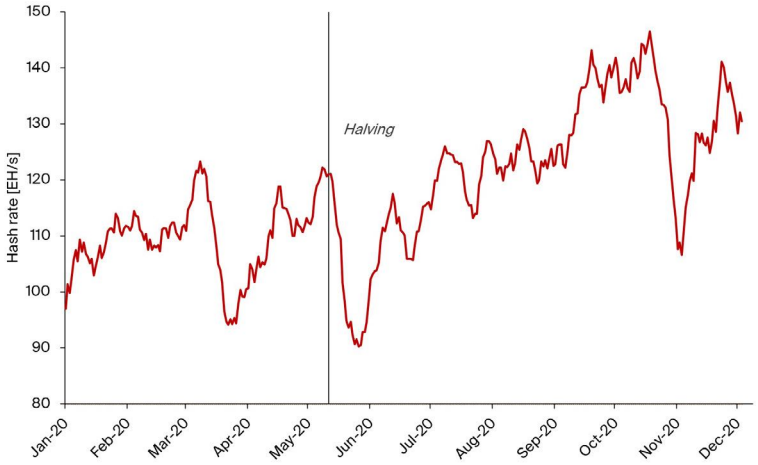
One of the most memorable moments this year clearly occurred on March 12/13, when the Bitcoin price (and that of most other cryptocurrencies) dropped by more than 50%. All markets globally were crashing, perhaps due to the realization that the pandemic would take a stronger toll on the economy than expected, and correlations moved towards 1 during this flight to safety[1]. In the crypto market, the effects were exacerbated by leverage in the system: Bitcoin was collateralized, and dollars borrowed against it, either to fund operations (e.g. by miners) or to buy more Bitcoin (by speculators). When prices started their rapid descent, these collateralized BTC started to get liquidated and accelerated the downwards movement. At times, there were more than $200 million worth of Bitcoin long positions waiting to be sold into the market on derivatives exchange BitMEX alone – more than the entirety of the bid side of their orderbook down to $0. The market was visibly in shock, as illustrated by wide bid/ask spreads of up to $600-$700[2] and massive discrepancies between prices on different exchanges, a situation which only slowly recovered over the following days.

In hindsight, this event marked the bottom for the months to come. Excessive leverage had been purged from the market, and prominent investors, such as Paul Tudor Jones[3], used it as an opportunity to enter the crypto world.

Bitcoin Block Reward Halving

Soon after, on May 11, the Bitcoin "Halvening" took place and the reward for each block was reduced from 12.5 BTC to 6.25 BTC. As outlined in the Outlook2020 report[4], this had major implications for Bitcoin's budget for network security and on the revenue of miners[5]. One important factor in the analysis is the Bitcoin price – a higher price means that miners might remain profitable even post-halving without improving efficiency.

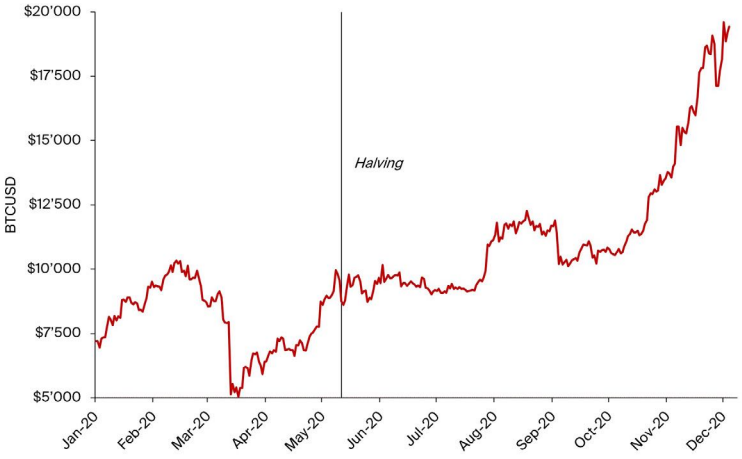
Illustration 1: After the block reward halving, unprofitable miners ceased operations and were quickly replaced by more efficient miners.



Source: blockchain.com, Bitcoin Suisse Research.

After this year's halving, the hash rate initially dropped, but recovered and rose quickly as Bitcoin started to make yearly highs. So far, Bitcoin has rallied +120% since the halving. In comparison to the two previous halvings, this is more aggressive than in 2016-2017 (+55% over the same duration), but much less than in 2012-2013 (+700%).

Illustration 2: "Black Thursday" in March marked this year's bottom, and since the block reward halving in May, Bitcoin has rallied +120%.

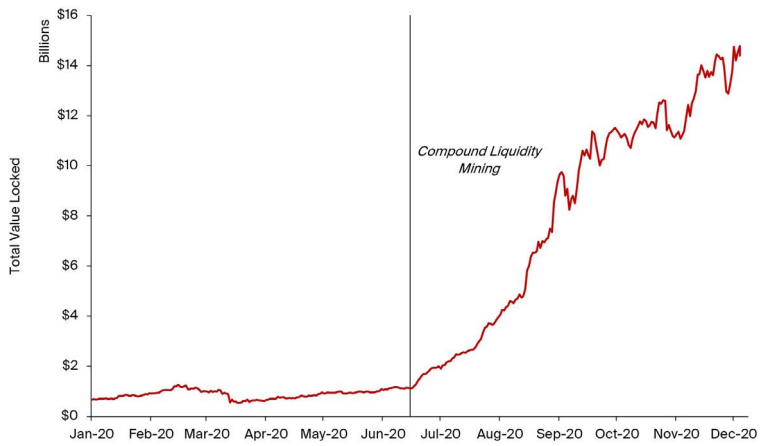


Source: coingecko.com, Bitcoin Suisse Research.

DeFi Summer

Besides the halving, the focus during this summer has been on the decentralized finance (DeFi) space, where innovation happened at a breathtaking pace[6]. The total value locked (TVL) in DeFi protocols has risen exponentially since the money market protocol Compound announced that it would hand out its native governance token, COMP, to users of the platform.

Illustration 3: Since the announcement of Compound's liquidity mining program, the total value locked in DeFi has risen substantially and now stands at around $14.5 billion.



Source: DeFipulse.com, Bitcoin Suisse Research.

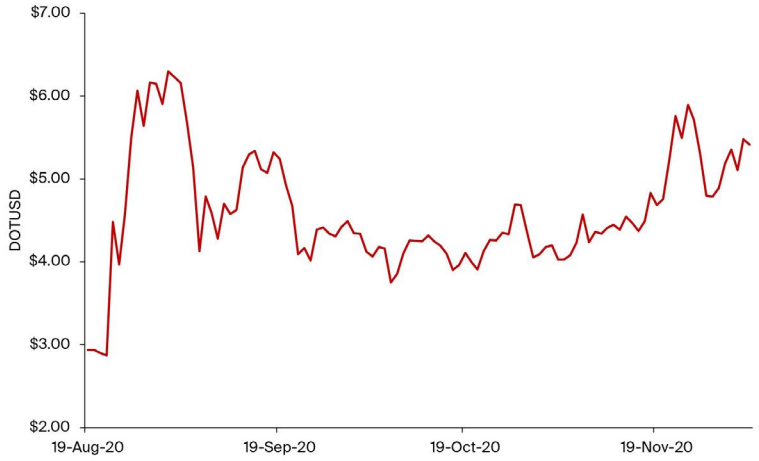
Compound did not remain the only protocol to announce the launch of a governance token[7], and the model of handing it out directly to users as rewards for participation gained traction. It also created the phenomenon of "yield farming"[8], in which savvy DeFi users quickly move from one protocol to another to maximize their yields and were often able to achieve yields of >100% annually. These activities did not come without risk, though, and smart contract exploits happened quite often – as such, it was (and still is) crucial to closely evaluate the security[9] of a smart contract.

Polkadot Launch

Another significant milestone from a fundamental side was the launch of the interoperability-focused blockchain Polkadot in May, which had been anticipated by many in the crypto community since 2017. As a first on-chain community vote, a redenomination[10] of DOT and Planck (its smallest unit, similar to a Satoshi for BTC or Wei for ETH) by a factor of 100 was successfully conducted.

DOT immediately secured itself a spot in the top 10 by market cap, and has so far shown a low correlation[11] to BTC and ETH.

Illustration 4: DOT became a top 10 coin by market capitalization immediately after the start of trading.

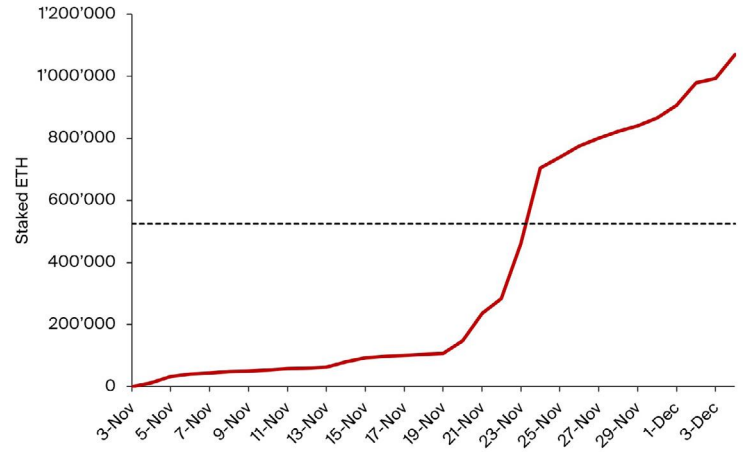


Source: coingecko.com, Bitcoin Suisse Research.

The Beacon Chain – Ethereum 2 Phase 0

Last but not least, Ethereum also managed to take its first step towards the network upgrade Ethereum 2.[12] The Beacon Chain, or phase 0 of Ethereum 2, which represents the coordination and consensus layer for later stages of the upgrade, had its genesis block[13] on Dec. 1, at 12:00:23 UTC. More than 1 million ETH has been staked so far, with a return (denominated in ETH) of around 15-16%.

Illustration 5: The amount of ETH sent to the deposit contract has crossed 1 million, and more ETH is staked daily at a rate of ca. 36'000 ETH/day (or more than 1'000 additional validators per day).



Source: etherscan.io, Bitcoin Suisse Research.

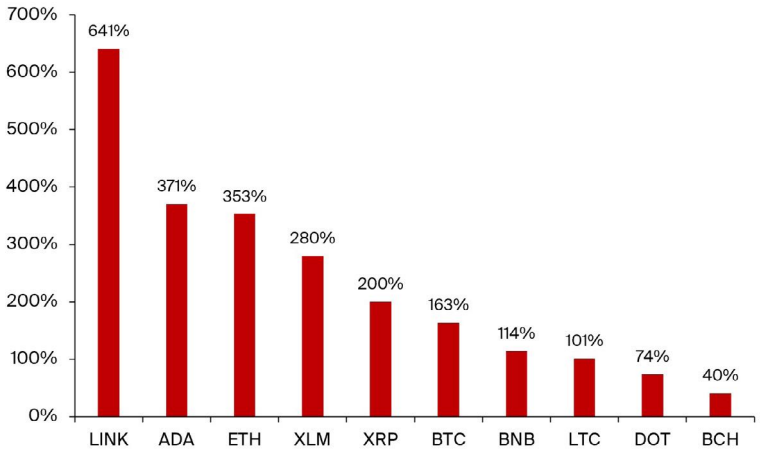
Which Tokens Performed Best?

Cryptocurrencies outperformed other asset classes by a fair margin this year so far. Bitcoin and Ether managed to return +163% and +353%, respectively. For comparison, the S&P 500 stands at a year-to-date return of +14.2%, whereas the Nasdaq

100 achieved +43.6%. Precious metals also had a good year, with gold up +20.9% and silver up +34.5%.

Of the top 10 coins by market capitalization, decentralized oracle[14] platform Chainlink (LINK) continued to outperform other cryptocurrencies and received a lot of attention from investors, as weak oracles were often the source of DeFi exploits.

Illustration 6: The top 3 performers of the coins in the top 10 by market cap this year so far were LINK, ADA, and ETH.



Source: coingecko.com, Bitcoin Suisse Research.

Looking a bit further, into the top 100 by market capitalization, the range of returns achieved year-to-date (or launch-to-date) was quite wide and varied from more than +5000% (AAVE) to -52% (FIL). It is noteworthy, however, that for some of the worst performers, the cost basis for many holders is much lower, as they obtained them through liquidity mining programs (BAL, SUSHI), in a public sale (FIL[15]), or airdrops (UNI).

Illustration 7: Of the top 100 coins, Aave (LEND/AAVE), Kusama (KSM), and yearn.finance (YFI) performed best, whereas Filecoin (FIL), Sushi (SUSHI) and Balancer (BAL) showed the worst performance.

Best Performers		Worst Performers	
Coin	YTD Return	Coin	YTD Return
AAVE	+5129%	FIL	-52%
KSM	+4193%	EGLD	-33%
YFI	+3401%	SUSHI	-24%
BAND	+2963%	BAL	-9%
UMA	+2449%	NEAR	-2%
CEL	+1613%	UNI	5%
RUNE	+1368%	ONT	8%
RSR	+1333%	EOS	15%
OCEAN	+1168%	BTT	15%
REN	+1008%	ATOM	25%

Source: coingecko.com, Bitcoin Suisse Research.

Conclusion

Seasonally[16] speaking, December has historically shown to be rather calm. Developments on other fronts not covered explicitly in this episode – such as new regulations[17] or prominent investors and companies[18] allocating part of their portfolios or treasuries to crypto – certainly deserve closer evaluation as well.

In short, the year 2020 has been great for the crypto markets, both from a fundamental as well as a performance perspective. Many exciting breakthroughs have been achieved, such as the launch of the Ethereum 2 beacon chain or that of Polkadot, and cryptocurrencies have yielded attractive returns to investors in comparison to other asset classes

Sources

1 Bitcoin Suisse Decrypt Series 2, “A Flight to Safety”

2 Bitcoin Suisse Decrypt Series 2, “A Flight to Safety”

3 https://www.scribd.com/document/460382154/May-2020-BVI-Letter-Macro-Outlook

4 https://www.bitcoinsuisse.com/outlook/bitcoin-in-2020-halving-the-block-reward

5 Bitcoin Suisse Decrypt Series 2, “Block Reward Halvings and the Rational Miner”

6 Bitcoin Suisse Decrypt Series 2, “The Evolving Open Finance Ecosystem”

7 Bitcoin Suisse Decrypt Series 2, “The Aftershock of Governance Tokens”

8 Bitcoin Suisse Decrypt Series 2, “Token Incentives in Decentralized Finance”

9 Bitcoin Suisse Decrypt Series 2, “Evaluating Smart Contract Security”

10 https://polkadot.network/results-of-dot-redenomination-referendum/

11 Bitcoin Suisse Decrypt Series 2, “Shifts in Cryptocurrency Markets”

12 Bitcoin Suisse Decrypt Series 2, “Ethereum’s Path to Serenity”

13 Bitcoin Suisse Decrypt Series 2, “Ethereum 2 is Coming”

14 https://www.bitcoinsuisse.com/research/decrypt/connecting-blockchains-to-real-life

15 https://filecoin.io/blog/sale-completed/

16 https://www.bitcoinsuisse.com/research/decrypt/seasonality-of-bitcoin

17 Bitcoin Suisse Decrypt Series 2, “Regulations and Innovations”

18 Bitcoin Suisse Decrypt Series 2, “Onboarding the Next Wave to Crypto”

Bitcoin Suisse AG
CH-6300 Zug
bitcoinsuisse.com