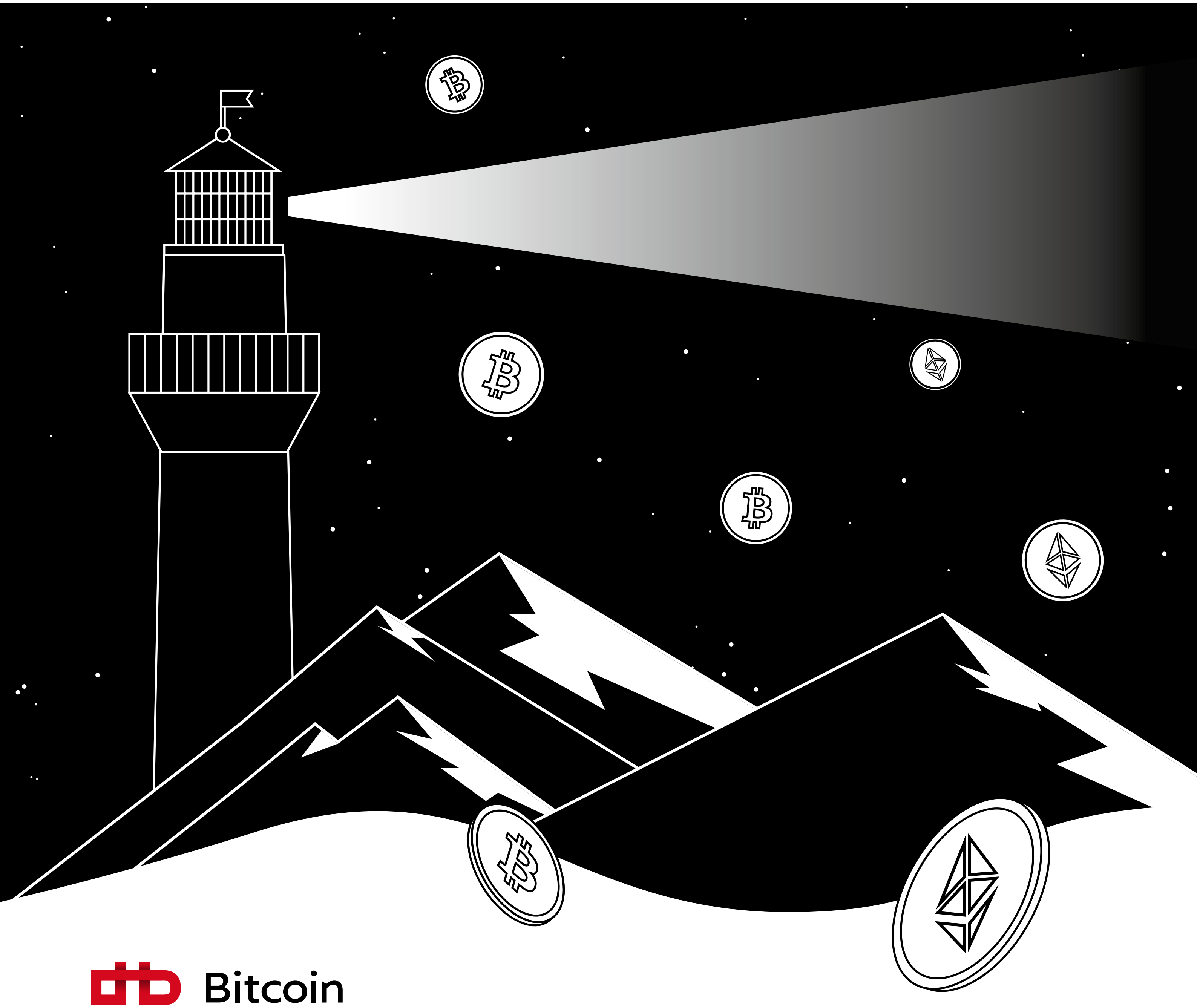
Crypto 2020

Outlook

In-Depth Industry Insights into Markets, Technology and Regulation



Bitcoin
Suisse

Impressum

Bitcoin Suisse AG
Grafenauweg 12
6300 Zug
Switzerland

Bitcoin Suisse (Liechtenstein) AG
Aeulestrasse 74
9490 Vaduz
Liechtenstein

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

Discover Our Services
Prime Brokerage • Custody
Colletaralized Lending • Payments
Staking • Tokenization

bitcoinsuisse.com

Authors:
Raffael Huber
Joseph Lubin
Ian Simpson
Demelza Hays
Marco Schurtenberger
Stefano Frick
Mona El Isa
Thomas Nägele
David Riegelnig

Design & Concept
Loris Haller

Printing:
Printoset, Zürich
Printed in Switzerland

About the Crypto Outlook 2020

The cryptocurrency space is constantly evolving and does so at a breathtaking pace. With an exciting year ahead of us, Bitcoin Suisse Research has compiled the Crypto Outlook 2020. The report focuses on a wide range of strategically important topics in the crypto asset industry and provides insights from key industry leaders. What are the trends, challenges and chances to keep an eye on in 2020? The Bitcoin Suisse Crypto Outlook 2020 helps answer this question.

Contents

Contributors

Dr. Raffael Huber

Dr. Raffael Huber is leading the Bitcoin Suisse Research Department, which conducts research on a broad variety of topics ranging from blockchain data analytics to market opportunities. He is in charge of Bitcoin Suisse Decrypt, which provides focused insights into selected subjects ranging from cryptocurrency fundamentals to market analyses. He holds a PhD from ETH Zürich.

David Riegelnig

David Riegelnig held several senior management positions at Credit Suisse and was Managing Partner of an algorithmic trading company before joining Bitcoin Suisse. During his 20-year career, David worked as an IT auditor, headed 1st and 2nd line risk control functions and was an entrepreneur. David has been an active investor in the field of blockchain and cryptocurrencies in recent years. He earned a Master's degree in Business Administration from the University of St.Gallen.

Ian Simpson

A veteran of the Swiss Crypto Valley ecosystem since early 2017, Ian Simpson joined Bitcoin Suisse in August 2019 after serving as Head of Communication at the Crypto Valley Association (CVA) where he supported the association's growth to over 1400 members. Previously, he was Head of Communications at Lakeside Partners (now CVVC). While working with the CVA, Ian was involved with a range of initiatives including the Worlds of Exchange conference in Zurich, the Crypto Valley Conference on Blockchain Technology as well as the CVA presence on the international stage in New York and Singapore. Ian has been a contributing author to CoinDesk, the leader in blockchain news.

Thomas Nägele

Thomas Nägele advises international finance, technology and industrial enterprises, operating in the fields of blockchain/DLT, telecommunications and internet, as well as public institutions. As a Liechtenstein Attorney and being a software developer, he focusses on Internet/IT law, as well as civil and corporate law. Besides being Attorney and legal Advisor, he teaches at the University of Liechtenstein and gives lectures and presentations on the newest legal developments. He co-drafted the Liechtenstein Blockchain Law (Trusted Technology Law).

Joseph Lubin

Joseph Lubin is a co-founder of Ethereum and the founder of ConsenSys, a full-stack, global blockchain company and the world's leading Ethereum accelerator. Lubin has established himself as a guiding force in the fast-growing blockchain industry and a powerful advocate of decentralized technology.

Demelza Hays

Demelza Hays teaches finance at the University of Liechtenstein, and is the author and editor of the Crypto Research Report (CryptoResearch.report). Prior to joining the University of Liechtenstein as a Ph.D. student in Business Economics, she completed her Master's in Economics at the Toulouse School of Economics.

Stefano Frick

Stefano Frick joined Bitcoin Suisse in August 2019 as COO Bitcoin Suisse (Liechtenstein) AG. Before joining Bitcoin Suisse AG, he was working for different financial intermediaries in Liechtenstein. In his most recent position, he successfully implemented and headed the Risk Management department at Bank Frick in Liechtenstein. Stefano holds a bachelor's degree in business administration as well as a Master's degree in accounting and finance from the University of St. Gallen. Currently he is completing an executive Master of laws (LL.M.) in banking and financial market law from the University of Liechtenstein.

Mona El Isa

Mona El Isa is the Co-founder and CEO of Avantgarde Finance Ltd. Mona was formerly the co-founder and CEO of Melonport AG, the company which developed Melon, the pioneering on-chain asset management protocol, delivering it successfully to main-net in March 2019. Before that she spent 5 years working in fund management, first at Jabre Capital and then launching her own long-short equity fund, where she discovered first-hand the major problems facing the fund industry today. Mona is also a former star-trader at Goldman Sachs, promoted to Vice President by the age of 26 and made the "top 30 under 30" list in Trader Magazine in 2008 and Forbes Magazine in 2011 after profitably trading the 2008 and 2011 crashes. Mona is the founder and President of MAMA, an industry association working to bring about a suitable regulatory regime for on-chain asset management.

Marco Schurtenberger

Marco Schurtenberger is a seasoned professional in information & cyber security as well as data protection, and has a vast experience in IT compliance, IT risk management and regulatory and statutory IT audits. Before he joined the Tezos Foundation in November 2019 as a Technology Officer, he worked at PwC Switzerland in IT Risk Assurance FS Banking since 2012 as a security consultant and auditor. Prior to PwC, Marco had roles in the field of Information Security at KPMG and Compass Security. He holds a Master of Science from ETH Zürich.

Interview

with Niklas Nikolajsen & Dr. Arthur Vayloyan

BITCOINS

Dr. Arthur Vayloyan, CEO of Bitcoin Suisse

Interviewed by Ian Simpson

"Bitcoin is the archetype of an anti-fragile system, the epitome of the hyper-accelerating IT era we are living in." — Dr. Arthur Vayloyan

Why are Bitcoin and crypto here to stay?

Arthur: Bitcoin is the archetype of an antifragile system, the epitome of the hyper-accelerating IT era we are living in. Many blockbuster innovations started in the garage, as ideas created by a handful of extremely gifted people. And here comes Bitcoin. A global currency designed in the garage? Pretty impish. So, it's no surprise it was first ignored and then ridiculed by many of the very important people of our current establishment.

But not everyone joined the "Bitcoin is doomed to fail soon"-choir. And even before Bitcoin appeared, Milton Friedman, who was quite a visionary predicted: "The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A." This sums it up pretty well – in the era of the internet, you need money that is native to the internet. It's that simple.

Niklas: Bitcoin, as an asset class as well as a settlement and payment network is, by now, more than 10 years old. It offers a valuable alternative to the traditional fiat currencies, both as a means of payment/settlement as well as a store of value. It is the world's first truly digital money, in the form of data – which provides great advantages in terms of utility, transparency and automation.

Adoption of Bitcoin has never been higher and continues to grow. Based on this, I see no reason why Bitcoin will not continue to grow in importance, in adoption, as well as in value - and why it will not also be around to celebrate its 20-year anniversary, 10 years from now.

Before we look forward to 2020 and beyond – can you give us a short recap of the major ups and downs of the crypto market in 2019?

Niklas: Throughout 2018 and 2019, the crypto markets have been undergoing a severe correction, after the markets went well ahead of themselves in 2017, when Bitcoin rose from 1000 USD to 20'000 USD. A great number of new blockchains launched themselves into the market, raising very large amounts of Bitcoin and Ether in the so-called ICO boom, most of them with a promise to become the next Bitcoin or Ethereum – and few of them able to deliver on this promise. This has undermined the confidence in crypto assets in general and furthermore, the release and liquidation of the collected assets from the ICO entities has been negatively impacting the markets.

I believe, however, that with Ethereum currently undergoing a transformation into ETH2 and with Bitcoin approaching its reoccurring inflation halving, this will change in 2020, where I predict around February, that a positive trend will once more take hold.

What trends have you observed over this time?

Arthur: It appears that just about everything will be connected over the Internet, which isn't a totally pleasant thought. As such, a myriad of new peer-to-peer markets will emerge. And a peer can be just about anything – a human, a machine, a building, anything. But in order to function properly, these markets need price-discovery mechanisms and an adequate means of payments. This is where Bitcoin, or some other technical variation thereof, comes into play.

Niklas: Throughout 2019, we have seen major crypto assets reel from the 2018 correction and try to find their true market value. Bitcoin started the year near 4'000 dollars, went as high as 13'000 dollars, and settled end-of-year at around 8'000 dollars. Ethereum has been under pressure all year, due to the uncertainties related to the launch of ETH2. The aftershock of the ICO boom and the 2018 correction have, in my view, been the major drivers of the market throughout 2019, much larger than the impacts provided from the regulatory- and industry side, and the trend has been towards stabilization.

It would appear that the large correction is over – and possibly we'll be seeing a 'crypto spring' replace the crypto winter, as the months of 2020 turn warm.

There is a growing acceptance of cryptocurrencies as a new asset class. Is it enough to treat them like any other investable asset? Why or why not?

Arthur: It will take a while until cryptocurrencies, or more generally crypto assets, will be broadly seen as an established, alternative asset class. For this to happen, we may have to wait a few years. But looking at our most recent partnerships with Amun, Emaar or Worldline, we can clearly see where the journey is heading. And as such, I strongly suggest to consider crypto assets as a potential investable asset class and to maybe even enrich your total wealth with a suitable portion of crypto assets and hodl them. Just a thought, of course…

Quite honestly, crypto technology is constantly changing and evolving. What technical developments can we expect to have strong impact in 2020?

Niklas: Crypto technology – as well as those of the surrounding ecosystem, are still very much in their infancy. However, development is ongoing, not just on the technology side, but also in regards to the regulatory frameworks and the ecosystem in general.

Amongst things to watch out for in 2020 are, in no particular order: The launch of ETH2, the migration of the ETH-based ecosystem to ETH2 as well as the development of Decentralized Financial Services (DeFi). The launch of the Telegram (TON) network as well as Libra, is also something to watch out for. Then, of course, the elephant in the room: The Bitcoin halving. Many things will happen in 2020 and it is going to be a very exciting year.

Bitcoin Suisse has applied to be a licensed crypto bank and securities dealer. Everyone wants to know what this will change for the company? What insights can you give us?

Arthur: We have established ourselves over the past six years of operations as a trusted, safe and reliable partner for all our clients. And we will further develop our excellent service offering along the path we have chosen since 2013. We are constantly improving and innovating to expand our offering and are regularly entering into strategic partnerships with renowned global brands. But without a doubt, even more would be possible under the umbrella of a bank and securities dealer license.

Niklas: Bitcoin Suisse is an evolving business and we always have been. In the summer of 2020, we will celebrate our seven-year anniversary and you only get to become that old in the crypto markets if you can continuously improve, innovate and re-invent yourself.

With regards to the future licenses, less will change than most would imagine. We will, of course, offer cash accounts for our clients, in their own name. We will also be able to more cost effectively manage deposits, something which will make our pricing much more competitive. We will start trading crypto securities, stablecoins – and synthetics, such as mini-futures and products to short the major crypto assets. We will be expanding our credit/loan and liquidity business, and we will expand our staking offering.

Last, but not least – we will be launching an offering for the public, likely in the form of a SPV, that they may invest into Bitcoin Suisse, as to increase our company capital from the current approximately 50M CHF, to around 100M CHF, providing for a much stronger balance sheet as we enter the world of banking.

Over and over again, we have heard the refrain "the institutionals are coming" – meaning that larger financial institutions will dive into the crypto asset market and have a

Niklas Nikolajsen, Founder of Bitcoin Suisse

significant influence. Is this a factor to watch out for in 2020 – or should we even care?

Arthur: Yes, we care – a lot. The various adjustments on the legal and regulatory side will be the main thing that enable institutionals to embrace, first opportunistically and then later systematically, the benefits of the crypto asset market.

And despite the prolonged crypto winter, we see a crypto summer of innovations, be it on the technology side (think Ethereum 2) or on the regulatory front (think FATF and Travel Rule). And I am proud to say that we have been very timely in developing a new service offering for ETH2 staking for all our clients and proposed a comprehensive open source solution regarding the missing "Crypto-SWIFT" via the OpenVasp.org initiative. So on several fronts, we see the advancements that will bring more and more interest from institutions.

Two decades after the new millennium, we have seen many monumental changes in society, business and beyond. What part will crypto play in the next decade or two?

Arthur: The price/performance improvement of technology will continue to accelerate. And the world is moving towards the better, contrary to what media would have us believe. The rapidly growing abundance in major areas of our life (energy, water, food) will allow us to fundamentally re-write the social contract between humans and soon, between men and machine as well! But of course, this great journey towards the better will not be without some turbulences in the interim. And as long as humans are cut out of the same mould, it will probably never be different.

When I was born, three billion people lived on this planet. Two billion were living in so-called extreme poverty. Today, we have over seven billion people and the number of people living in extreme poverty is well under one billion. And this trend will not stop. Assuming further progress, extreme poverty can soon be put in the museum, as Professor Yunus (Noble Peace Prize winner from Bangladesh) phrased it. Now, couple that with the ever-increasing connectivity of people and you cannot but assume massive innovation beyond imagination. But to just wait for the better is not an option. Because luck meets the prepared. A constant call to action is required. Our clients and partners can count on us.

Niklas: More than most people think. After centuries of a financial and also societal system built on representatives, internal ledgers and central trusted parties – consensus systems, open ledgers and decentralized systems will have a huge impact on almost everything.

There are many diverse schools of thought on crypto assets – and a good many myths. Are there some main myths that we should be aware of and which should be "debunked?"

Niklas: Yes – crypto assets were not invented, nor propagated for the purpose of dark markets and shady business. Quite the opposite, they are here to replace and improve upon the essentially intransparent, inefficient and flawed system of centralized trust and centralized or delegated control – which tends to benefit the few and not the many.

Arthur: A myth? "Bitcoin has no intrinsic value!" To still hear this from reasonably well-educated people surprises me quite a bit. Yet another myth? Satoshi Nakamoto.

What has Switzerland done right so far concerning cryptocurrencies and blockchain technology? Where do you feel there is room for improvement?

Arthur: Politics matter. And in Switzerland we are privileged to have a rather decentralized, bottom-up political system. And the icing on the cake: our top executive body, the Federal Council, shines with a very innovative attitude towards the many possibilities of this new technology. This is quite unique in the world and one of the success factors of this small country with such a global reach in many of the most innovative fields.

Niklas: Yes. I have never seen anything, perhaps except the Mona Lisa, which could not be improved upon, and for that reason, I do not feel that it would be appropriate to use this space to list criticism.

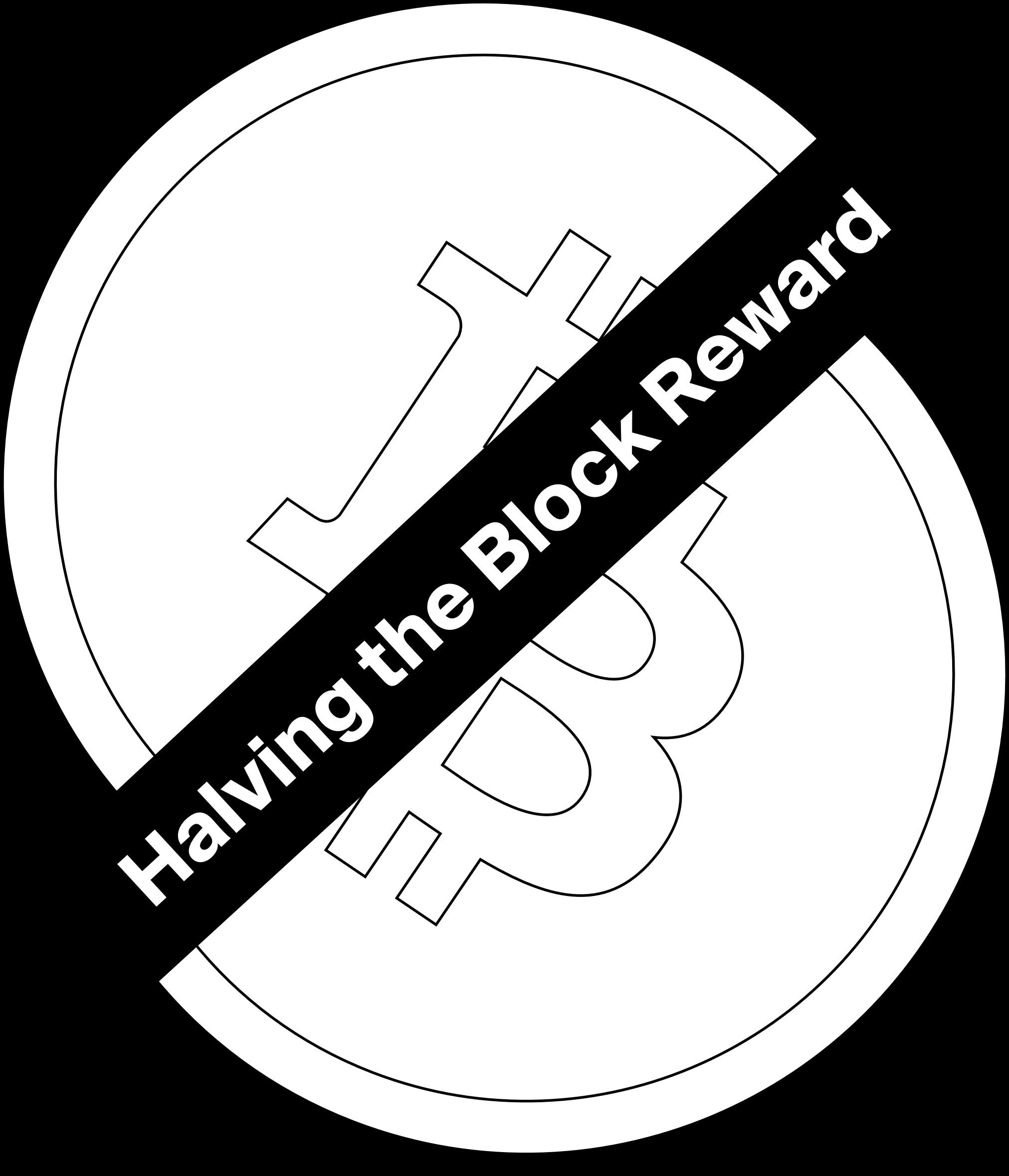
When I reviewed various jurisdictions, trying to choose a place for my future Bitcoin company some 9 years ago, Switzerland came out on top. I feel to this day that this was the right decision and I can only praise the Swiss jurisdiction as a place to do business, in crypto or otherwise.

“Crypto assets are here to replace and improve upon the essentially intransparent, inefficient and flawed system of centralized trust and centralized or delegated control - which tends to benefit the few and not the many.”

— Niklas Nikolajsen

Bitcoin in 2020

Written by Dr. Raffael Huber



In May 2020, the block reward paid to miners will be halved from 12.5 BTC to 6.25 BTC per block.

The block reward reduction has previously led to price rallies and strongly impacts the profitability of miners.

Bitcoin's role as a store of value is becoming increasingly important. It shows a low correlation to other asset classes such as equities and gold.

Looking Back: Bitcoin in 2019

What is Bitcoin?

Bitcoin is the oldest cryptocurrency and was launched on January 3, 2009. It solved the double-spend problem for a decentralized electronic cash system, ensuring that bitcoins can only be spent once. Bitcoin does so by bundling transactions in blocks and chaining them together – a process which is secured through cryptographic technology and computational resources (proof-of-work). Today, Bitcoin is still the largest cryptocurrency by market capitalization and captures about 66 % of the total market cap of cryptocurrencies. Bitcoin trades at $7.6k at the time of writing.

Last year, Bitcoin has made its recovery from the "crypto winter" in 2018. Starting the year at $3.7k, Bitcoin has rallied throughout the first half of 2019 to reach almost $14k in late June, and then corrected to the levels of around $7.6k at the time of writing. With a year-to-date return of 105 %, Bitcoin has been the best-performing asset class of 2019. For comparison, the S&P 500 and the tech-focused Nasdaq 100 posted returns of 25 % and 33 % year-to-date, respectively. Market accessibility has been further improved, with physical delivery Bitcoin futures launched in late September.

On the technical side, Bitcoin Core developers have continued to update their node software, currently sitting at version 0.19.0. This brought about several improvements, such as native hardware wallet compatibility. Also, "bech32" addresses – which are less error-prone due to the lack of distinction between upper- and lowercase letters and offer benefits for SegWit – are now the default in the GUI.

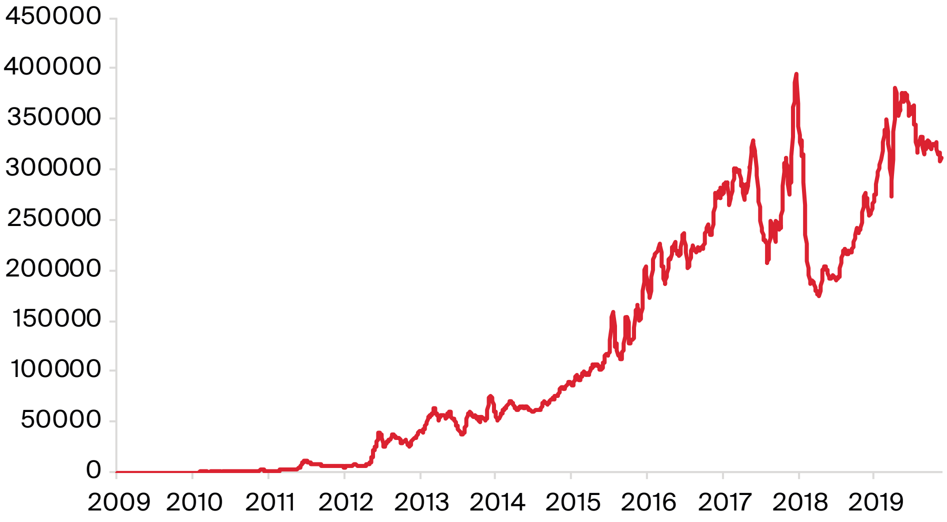
Additionally, Electrum – one of the most commonly used Bitcoin wallets – has announced support for Lightning Network payments. The Lightning Network has grown further in 2019 and increased the total capacity among all channels from 525 BTC in January to 825 BTC currently.[1]

More fundamentally, research into the implementation of Schnorr signatures continues as an alternative to the current elliptic curve signature algorithm. Originally proposed as a Bitcoin Improvement Proposal by Bitcoin developer Pieter Wuille, Schnorr signatures would contribute to the scalability of Bitcoin, as well as to improved privacy: Multi-signature transactions would be indistinguishable (in terms of signature size) from normal, single-signature transactions on the blockchain. Additionally, the requirement for block space coming from single-signature transactions with multiple unspent transaction outputs (UTXOs) as inputs would be significantly reduced – since only one signature would be required regardless of the number of inputs.

[1] https://bitcoinvisuals.com/ln-capacity

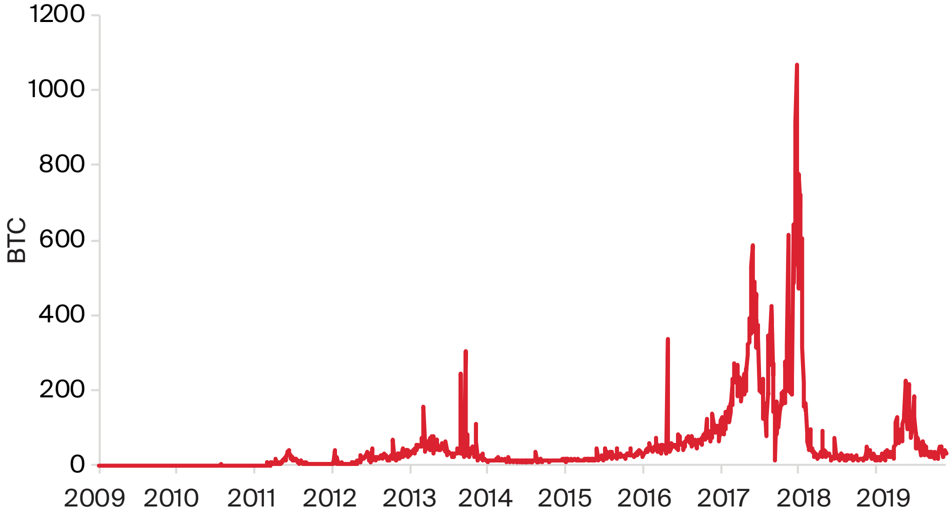
The State of the Bitcoin Network

BTC Daily Transactions



The number of transactions per day has been increasing from Q3-Q4 of 2018 through the first half of 2019 and sits now at around 300'000 transactions per day.

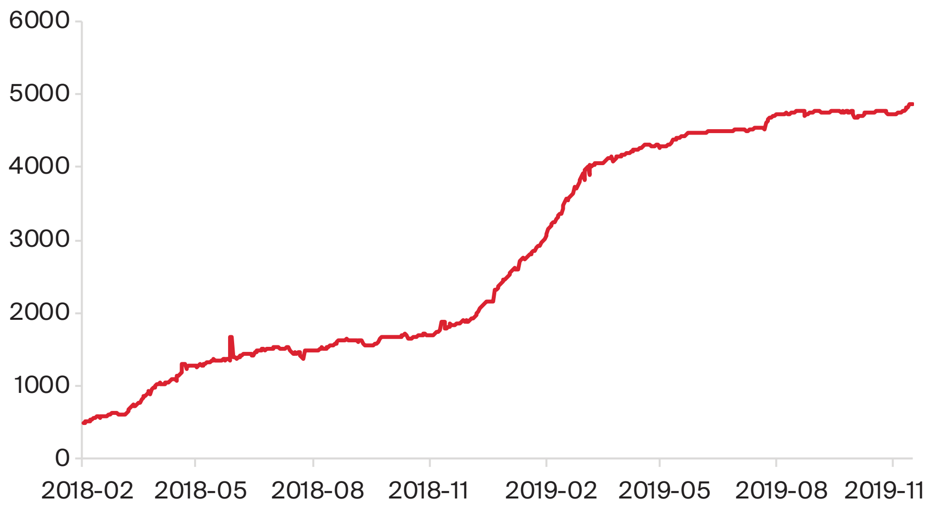
BTC Total Transaction Fees per Day



Bitcoin transaction fees paid to miners amounted to around 20 BTC per day in 2019. Upwards spikes in transaction fees typically correlate with increasing market volatility.

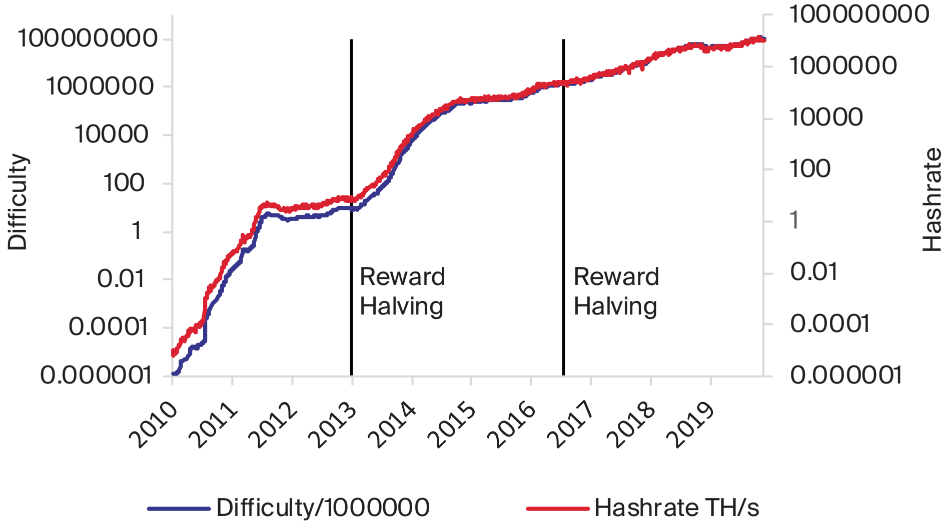
Illustration source: blockchain.com, Bitcoin Suisse Research.

Lightning Nodes with Channels



The Lightning Network, Bitcoin's second-layer scaling solution that enables micropayments through payment channels, has seen strong growth of the number of connected nodes in late 2018 / early 2019. Currently, there are around 5'000 nodes present in the network.

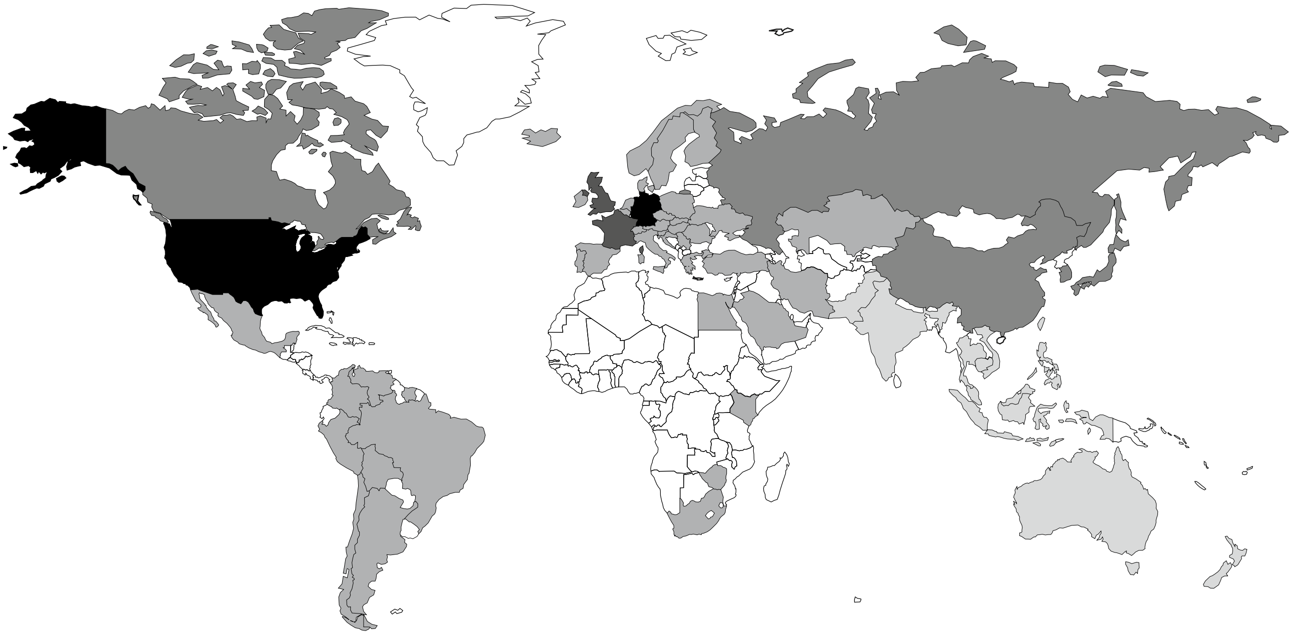
BTC Hashrate and Difficulty



After a slight dip in hashrate (and difficulty) towards the bottom of the bear market in late 2018 / early 2019, Bitcoin's hashrate – and hence security – continues making all-time highs.

Illustration source: blockchain.com, Bitcoin Suisse Research.

Bitcoin Node Distribution



Nodes

2500

1250

1

Bitcoin is a truly global network with nodes hosted in almost 100 different countries. The leaders are the United States, Germany, and France, with China ranked 9th by number of nodes.

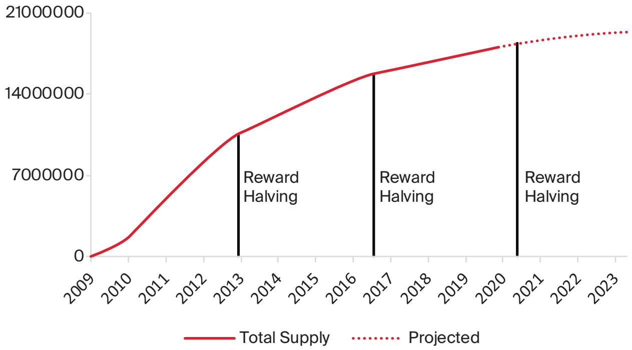
Illustration source: bitnodes.earn.com, Bitcoin Suisse Research.

The two last "halvening" events, which cut the block reward handed out to miners in half, occurred in November 2012 and July 2016. Following the 4-yearly rhythm that is deeply embedded in Bitcoin's protocol code, the next "halvening" is set to take place around May of 2020.

Bitcoin's "Monetary Policy" Changes in 2020

At block number 630'000, the reward handed out to miners for finding the block will be reduced from the current 12.5 BTC to 6.25 BTC. The predefined schedule for issuing new bitcoins ensures scarcity: There will never be more than 21 million BTC in circulation, and any attempt to change that – e.g. through a hard fork – will most likely encounter massive resistance from the Bitcoin community.

BTC Total Supply



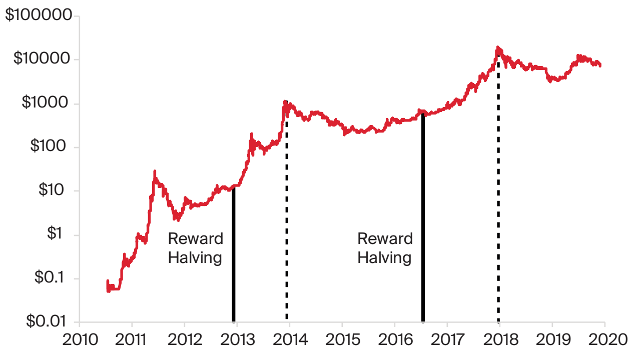
Source: blockchain.com, Bitcoin Suisse Research.

Bitcoin issuance halves every 210'000 blocks, or approximately every 4 years. Currently, the rate at which bitcoins are issued to miners sits at about 3.6 % of the total supply per year. In May 2020, this number will be reduced to about 1.8 %.

The maximum supply of 21 million BTC will be reached in 2140. However, since issuance slows down with time due to the halvenings, the majority of bitcoins that will ever be in existence have already been mined today. The current total supply sits at around 18 million BTC, or 85.7 % of the maximum supply. Additionally, it is worth noting that a significant number of bitcoins have most likely been lost – meaning the original owner has lost access to the private key that controls them. A study[2] estimates that 2.3 to 3.7 million BTC have been lost permanently, which further reduces the effective total supply.

In the past, the block reward halvings have led to extended price rallies following the event.

BTCUSD



Source: 99bitcoins.com, Bitcoin Suisse Research.

The Bitcoin price has increased significantly following the previous reward halvings. From the time of the halvening (black line) to the next peak (dashed line), returns on investment of 9'143 % and 2'890 % were achieved, respectively.

The question is now whether the third reward halving will lead to a similar price rally. In principle, the halvening is a predictable event, and all information is publicly available – the supply side increase of the supply and demand equilibrium will be lower. Thus, under the efficient-market hypothesis, the halvening should be "priced in" – however, this was not the case for the first two halvenings as Bitcoin's price history shows. In a network whose economic incentives for miners are directly correlated to network security due to higher or lower hashrate, price is certainly a non-negligible variable.

Effects of the Halvening

After May 2020, the block reward will pay less for network security. This will heavily impact the economics of the mining business. The cost to mine one BTC depends on a variety of factors, such as electricity costs, mining difficulty and hashrate per unit of power. A recent study estimated the cost to mine 1 BTC at an electricity price of $0.05/kWh to be around $5.6k.[3] This cost will increase considerably post-halvening, affecting especially miners using older mining gear and leading to the obsolescence of equipment with lower hashrate-to-power ratios.

In the past, however, halvenings have not led to decreases in hashrate (see page 20). After both instances, the subsequent price rallies ensured that miners remained profitable. The time after the first

[2] https://blog.chainalysis.com/reports/money-supply
[3] https://coinsharesgroup.com/research/bitcoin-mining-network-june-2019

halvening also marked the advent of the ASIC (application-specific integrated circuits) mining area, leading to immense efficiency gains over older methods such as CPU, GPU or FPGA (field-programmable gate arrays) mining – a fact which left its footprint in the hashrate chart.

A block reward halving drastically changes how much the protocol pays out to miners irrespective of network usage (i.e. transaction fees) – next time from 1'800 BTC per day to 900 BTC per day. Currently, transaction fees only account for about 2 % of the total miner revenue.[4] Since the total miner revenue is tightly correlated with the hashrate and hence the overall network security, there are three possible outcomes. The first is that the Bitcoin price will rally as it did after the first two halvenings – in this case, miners will remain profitable and hashrate will continue to go up. The second scenario in which on-chain transaction volumes and total transaction fees would strongly increase leads to the same outcome. If neither of the two happen, however, then the hashrate could be expected to decrease due to miners with the highest production costs per BTC becoming unprofitable.

The second scenario – an increase of on-chain transaction volume – is also closely related to the heated block size debate that ultimately led to the hard forks that created Bitcoin Cash (forked from Bitcoin) and Bitcoin SV (forked from Bitcoin Cash). Both competitor chains aim to solve Bitcoin's current scalability limitations by increasing the block size and hence allowing to accommodate more transactions per block. Bitcoin currently has a block size limit of 1 MB, although the use of SegWit – which solves Bitcoin's transaction malleability and helps with scaling – effectively allows the inclusion of up to 4 MB worth of transactions. Bitcoin Cash's block size limit is 32 MB; Bitcoin SV lifted the limit to 2 GB in July 2019 with the Quasar protocol upgrade. This highlights the different approaches to scaling between the chains: While Bitcoin plans to achieve scaling off-chain through second layer solutions such as the Lightning Network, Bitcoin Cash and Bitcoin SV proponents argue that scaling should mainly take place directly on-chain.

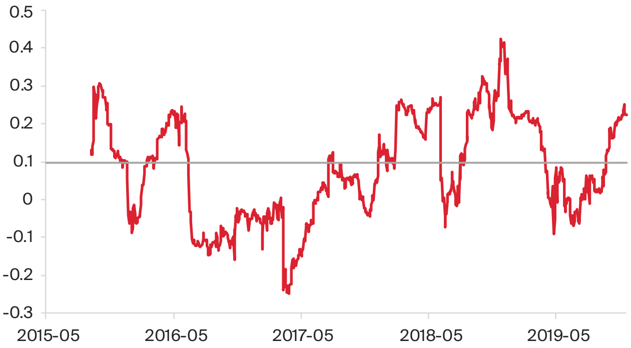
Another interesting fact to note is that both Bitcoin Cash and Bitcoin SV are projected to undergo their block reward halvings in April 2020 – one month earlier than Bitcoin. Since all three chains also share the same hashing algorithm, much of the hashrate of BCH and BSV will most likely switch over to Bitcoin for a month (until its halvening has also happened).

Bitcoin's Role as an Investment and a Store of Value

Debt is increasing globally – recently, it was estimated that global debt would rise to $255 trillion by the end of 2019.[5] Interest rates are already negative in Europe and Switzerland, and the Federal Reserve lowered their target rate to 1.5 % - 1.75 % at the end of October 2019.[6] Bitcoin was born out of the financial crisis that started in 2007 and offers a hard money system due to its defined issuance schedule. This is especially relevant today in countries with currencies that have issues of trust due to continuous inflation by the government, such as Argentina or Venezuela – where localbitcoins (a peer-to-peer trading platform) volume has reached record highs.[7] In these economies with capital market restrictions, Bitcoin serves as a store of value, similar to gold – with the additional characteristic that it is considerably harder to seize by oppressive governments.

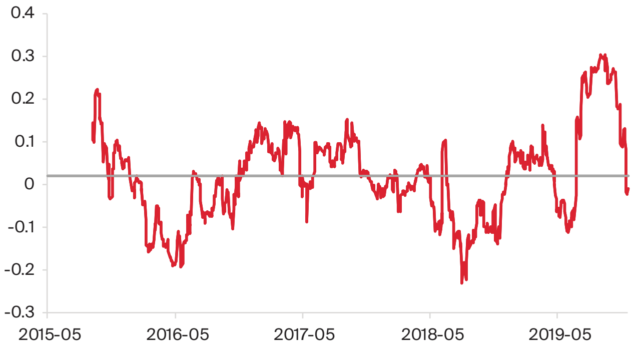
But also in countries where the people still feel safe holding the local currency, Bitcoin makes sense as part of a well-diversified portfolio due to one feature: its low correlation to other markets such as equities or gold.

Bitcoin / S&P 500 90-Day Rolling Correlation



[4] https://www.bitcoinsuisse.com/research/decrypt/transaction-fees-markets-for-block-space/
[5] https://www.reuters.com/article/us-global-markets-debt/global-debt-to-top-record-255-trillion-by-years-end-idUSKBN1XP1FB
[6] https://www.federalreserve.gov/monetarypolicy/files/monetary20191030a1.pdf
[7] https://coin.dance/volume/localbitcoins

Bitcoin / Gold 90-Day Rolling Correlation



Source: Yahoo Finance, Bitcoin Suisse Research.

Bitcoin has a low correlation to both equities (with the S&P 500 as an example, top) as well as gold (GLD, bottom).

Since mid-2015, Bitcoin has shown a correlation of 0.096 to the S&P 500, and a correlation of 0.020 to gold while providing an overall return on investment of about 3'000 %. Thus, holding Bitcoin in a portfolio would have improved both diversification as well as risk-adjusted returns. This may also hold true in the coming years, especially if central banks continue their expansion of the monetary base and keep encouraging investments through their policies.

Conclusion

Bitcoin is stronger than ever, with fundamental metrics such as hashrate continuing to make all-time highs. The most anticipated event in 2020 is the block reward halving, which reduces the issuance to miners from 12.5 to 6.25 BTC per block. This has led to significant prices rallies in the past, with beneficial effects to overall network security due to keeping miner profitability high and encouraging longer-term investing into mining equipment.

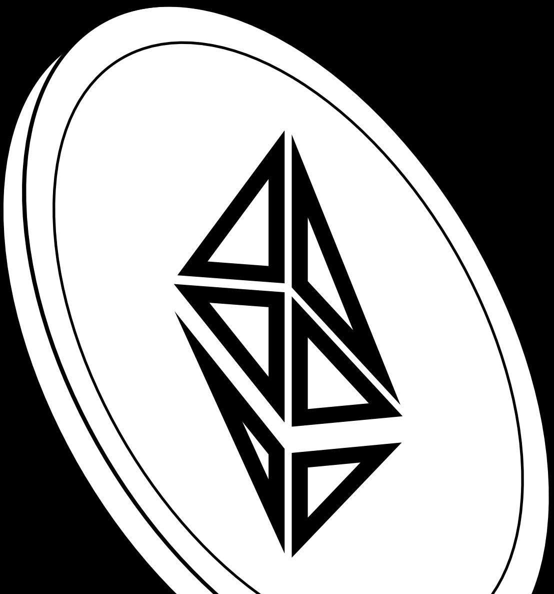
In order for network security to remain at current levels after the halvening in May 2020, either the price has to increase, or transaction fees need to make up for lost miner revenues. The Bitcoin competitors Bitcoin Cash and Bitcoin SV aim to solve this issue by increasing the block size, which enables more transactions and hence more fees in total which subsidize the network. Bitcoin's scaling approach is still focused on the development of second-layer solutions such as the Lightning Network; since fewer transactions would then need to be recorded directly on the blockchain, increasing fees would be tolerable.

Bitcoin also remains attractive as an investment – not only due to historical performance, but also due to its low correlation to other markets. Holding Bitcoin is in part also a bet on a future store of value – perhaps a more relevant use case than ever, with growing recession fears across the globe.

Ethereum and its Transition to Ethereum

Written by Dr. Raffael Huber

2



A new blockchain, called Ethereum 2, will be launched in 2020 and will employ a proof-of-stake based consensus algorithm.

Ethereum 2 will have vast implications for scalability, security, decentralization and tokenomics.

The ETH issuance rate would be considerably lower in the long run than it is today with the current specifications of Ethereum 2.

Looking Back: Ethereum in 2019

Last year, development of the Ethereum blockchain has progressed significantly. In February, the network underwent the Constantinople hard fork – a planned upgrade which introduced various improvements to scalability and efficiency. Additionally, the upgrade delayed the "difficulty bomb", which is an algorithm that exponentially increases the mining difficulty on Ethereum until mining becomes unfeasible (a period dubbed "Ice Age"). The goal of the difficulty bomb was to ensure an eventual transition to proof-of-stake. The block reward was also reduced from 3 to 2 ETH in Constantinople.

The next protocol upgrade of the current Ethereum chain occurred in December with the Istanbul hard fork. Istanbul brought several changes, such as reducing the cost of zero-knowledge proofs ("ZKPs", originally introduced in the Byzantium hard fork[1]) or enabling interoperability with Zcash. Cheaper ZKPs in combination with a technique called Optimistic Rollup[2] allow for around 3'000 transactions per second[3] on Ethereum – a large improvement to scalability.

However, the perhaps most intriguing development on Ethereum has not occurred on the protocol level, but on the blockchain directly: the rise of decentralized or open finance (DeFi), with an USD value of currently about $660 million locked in DeFi at the time of writing.[4] The articles "The Decentralized Finance Revolution on Ethereum" and "How Decentralized Finance is Automating Central, Commercial, and Investment Banking" of this report provide an in-depth overview of this fascinating development.

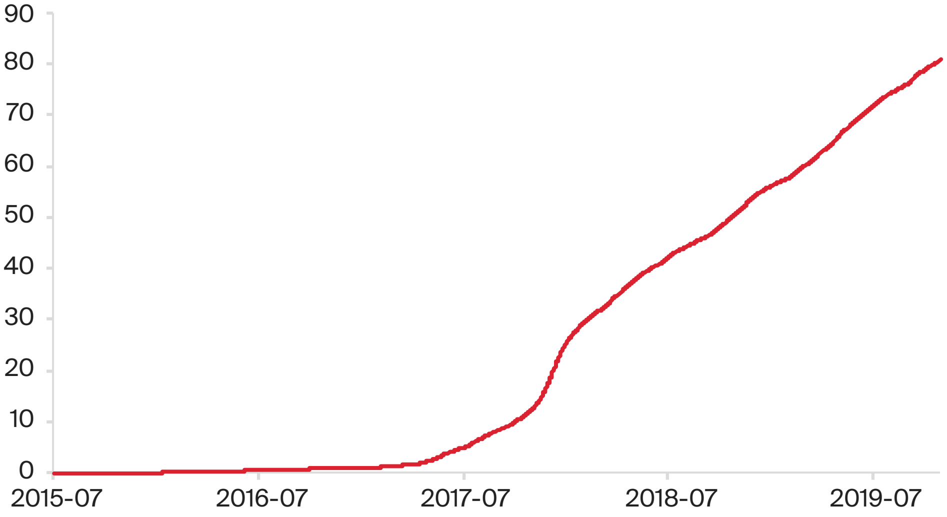
What is Ethereum?

The Ethereum blockchain was launched in July 2015 with the vision of creating a "world computer". Its core features are programmability as well as enabling fast cryptocurrency payments. The capability to execute complex code on the blockchain enables "smart contracts" – contracts that are enforced automatically through code.

[1] https://blog.ethereum.org/2017/10/12/byzantium-hf-announcement/
[2] https://medium.com/plasma-group/ethereum-smart-contracts-in-l2-optimistic-rollup-2c1cef2ec537
[3] https://twitter.com/VitalikButerin/status/1196896377877471233
[4] https://defipulse.com/

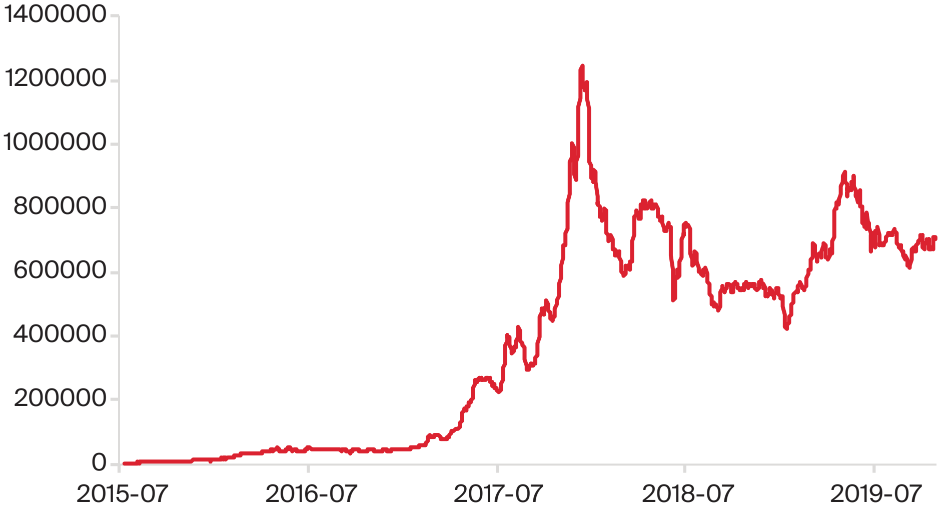
The State of the Ethereum Network

Unique Addresses (in millions)



The number of unique addresses on the Ethereum blockchain keeps increasing linearly since mid-2017.

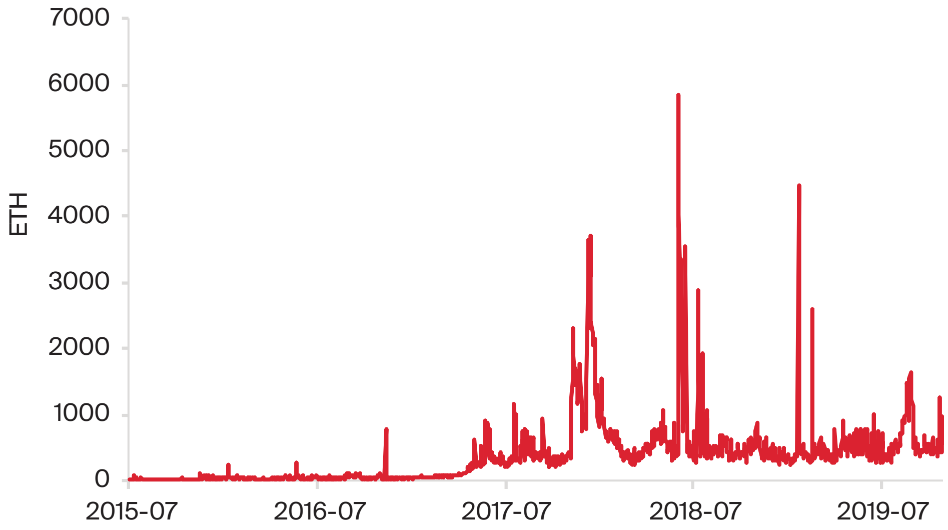
Transactions per Day



Currently, about 700’000 transactions are confirmed every day on Ethereum, which translates to a throughput of about 8 transactions per second.

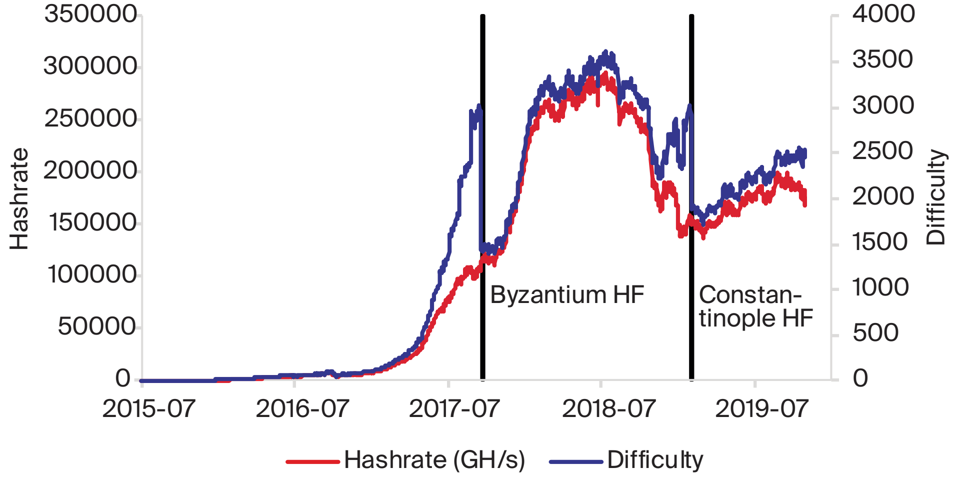
Illustration Source: etherscan.io, Bitcoin Suisse Research.

Total Transaction Fees per Day



On average, about 520 ETH per day in transaction fees were paid to miners in 2019.

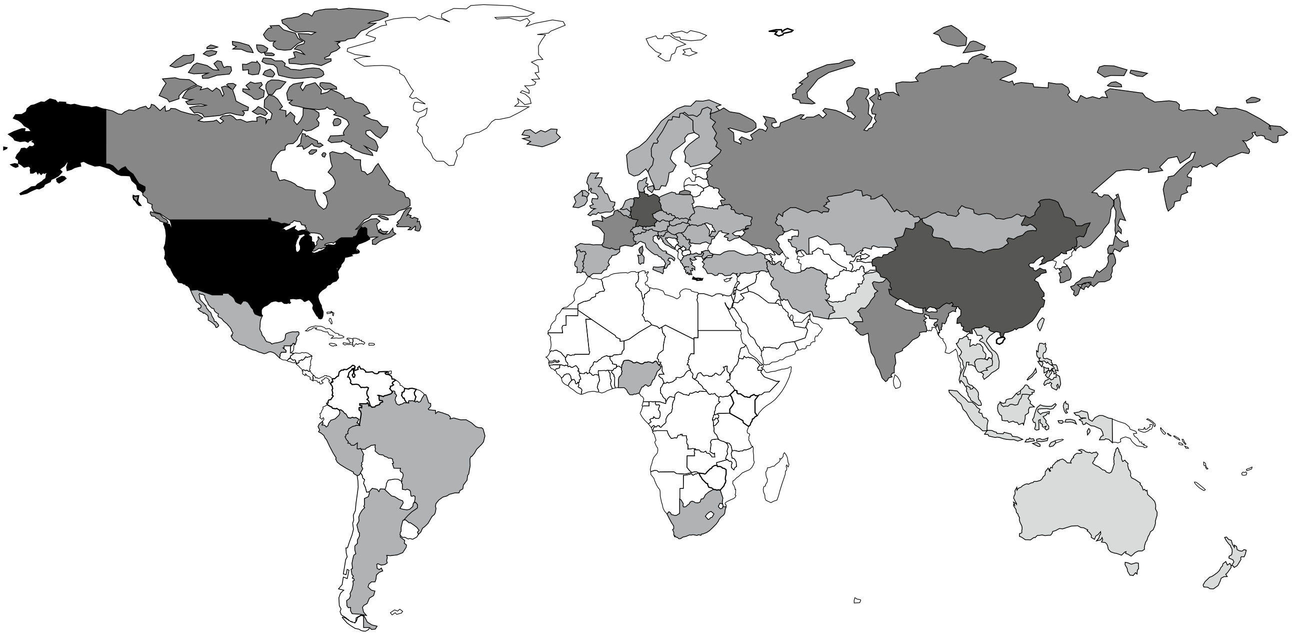
Hashrate and Difficulty



The Ethereum hashrate (red) has been on the decline throughout the bear market in 2018 but started recovering in 2019. The Byzantium and Constantinople hard forks reset the difficulty (blue) to lower levels.

Illustration source: etherscan.io, Bitcoin Suisse Research.

Ethereum Node Distribution



Nodes of the Ethereum network are distributed across the globe, with the most nodes hosted in the U.S., China, and Germany.

While the distribution of Ethereum nodes is fairly decentralized, concentration in mining pools is more of a centralization concern. The three largest mining pools combined – Sparkpool, Ethermine and f2pool2 – are responsible for about 64 % of the total hashpower. However, the requirements to help secure the Ethereum network are about to change – with *Ethereum 2*.[5]

[5] There has been quite some discussion in the community about what the terminology of the new chain and its cryptocurrency (beacon ether “bETH”, ETH2, eth2, ...) should be. In this article, the new chain will be called “Ethereum 2”, and the new cryptocurrency “ETH2” throughout.

Ethereum 2: Overview and Recent Developments

Throughout 2020, major changes are coming to the Ethereum blockchain. As part of its Serenity upgrade, a new chain called Ethereum 2 will be launched. This will mark the start of Ethereum's transition from a proof-of-work based consensus algorithm to proof-of-stake. In short, this means that the current model of mining will be abandoned – instead, the network will be secured by validators that sign off on transactions and include them in blocks. The computational resources required from validators will be much lower than in proof-of-work, which means that energy consumption – a highly controversial topic surrounding mining in general – will no longer be an issue anymore in the future for Ethereum.

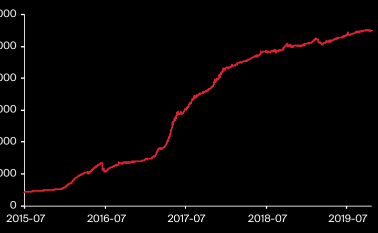
The switch to proof-of-stake is highly anticipated, as it will be the most fundamental change to Ethereum ever since its launch in July 2015. The transition will be separated into multiple phases. However, the research part of later phases does not rely on completion of the previous phases – only the actual implementation does, meaning that a delay in e.g. Phase 0 does not necessarily affect Phase 1 and 2.

Phase 0

In this phase, the beacon chain will be launched, and validators will be able to put up ETH2 as stake to sign off on transactions, secure the network and earn rewards.[6] This will necessitate the setup of one validator per 32 ETH2, as each validator requires exactly 32 ETH2.

The launch is expected in Q1 2020, but a testnet running smoothly for at least one month is required first. Initial trials of Ethereum 2 node client interoperability were successful. The first step is then to migrate part of the ETH from the current chain to this completely new blockchain through a deposit contract – a smart contract which will enable a one-way bridge to move ETH from the legacy chain to the beacon chain. At the time of writing, the deposit contract is ready to be deployed, but developers are holding off until a final, inter-blockchain standard for one type of digital signatures (called Boneh-Lynn-Shacham or BLS) has been agreed upon.

Addresses with >32 ETH



The number of addresses holding at least 32 ETH has been steadily increasing, potentially indicating that smaller ETH holders are accumulating to stake once the beacon chain is live. This graph will spike once large ETH holders split up their holdings into chunks of 32 ETH to stake.

[6] https://www.bitcoinsuisse.com/research/specials/ethereum-2-matters-validator-economics

Upon launch of the beacon chain, ETH2 will be issued on a 1:1 basis for each ETH that has been sent to the deposit contract. Most likely, this new cryptocurrency will initially be non-transferable at least until Phase 1. As such, it is highly likely that a futures market for the digital asset will evolve – and hence also a different price for ETH2 and ETH, which will converge when the legacy Ethereum blockchain becomes part of the new chain (see Phase 2).

The goal of this phase is to establish whether the base layer structure (i.e. the beacon chain) is stable, and to evaluate whether the economic incentives to stake and validate are sufficient.

Phase 1

During this phase, the shard chains will be established. Each shard can be viewed as a separate blockchain, and the beacon chain will act as a coordination layer between the shards. In the original proposal, the implementation of 1024 shards was planned. However, Vitalik Buterin proposed[7] to reduce the number of shards to 64 – which would simplify cross-shard communication, meaning that interactions between shards (e.g. a token transfer from shard A to shard B) would proceed more smoothly.

Validators will be randomly assigned to shards from the pool of all validators. This reduces the chance that any set of validators could collude to take over a shard. Obtaining a truly random seed to base this decision on is hard, however – at least until quantum computers can provide provable randomness.[8] In the meantime, randomness will be brought to Ethereum 2 through a complex algorithm that includes verifiable delay functions (VDFs). These functions are known to take a certain amount of time (102 minutes in Ethereum 2) to compute, and take arbitrary numbers provided by validators as inputs. The result will serve as a random seed for validator assignment to shards.

This "parallelization" of the blockchain through sharding will raise its capacity to around 1.3-2.7 MB/s, which should support a throughput of around 10'000 transactions per second initially – and potentially more, with the addition of more shards in the future as well as the efficiency optimizations currently happening on Ethereum (see above). For comparison – a global payment system such as VisaNet handles around 1'700 transactions per second on average.

Phase 2

This phase will introduce the full set of blockchain functionalities to Ethereum 2. It will be possible to execute smart contract code and transfer any tokens on the blockchain. The legacy Ethereum chain will be folded into an execution environment of Ethereum 2, meaning it will simply become a shard in the new chain – and all ETH remaining on the old chain will be transformed into ETH2. The state execution engine will be based on eWASM – Ethereum-flavored WebAssembly[9] – and allow the compilation of high-level languages suitable for smart contracts.

Hence, this phase will also mark the end of the two-token model of ETH and ETH2 – at least in theory. There is a noteworthy chance that miners on the legacy Ethereum chain will conduct a hard fork and try to maintain the chain. If unsuccessful, miners will have to redirect their hashpower towards other proof-of-work chains mined with GPUs.

Overall, it should be mentioned that especially the later phases of Ethereum 2 are still subject to discussion and the final implementations have not been decided upon. The timeline is also unclear – but the typical Silicon Valley mantra of "move fast and break things" does not work for an infrastructure that is securing billions of dollars' worth of assets.

[7] https://notes.ethereum.org/@vbuterin/HkiULaluS

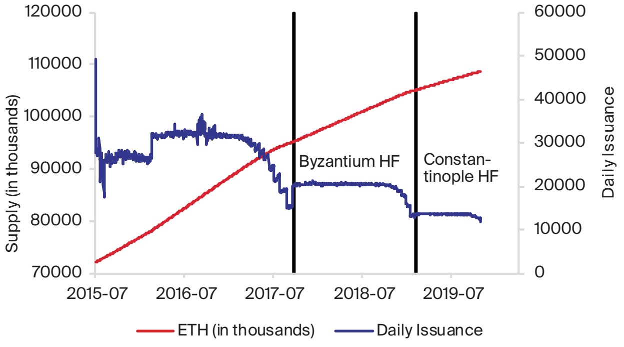
[8] https://fortune.com/2019/10/23/google-quantum-cryptocurrency-the-ledger/

[9] WebAssembly is a type of code that can be run in modern web browsers and allows to "translate" programming languages such as C++ or Rust into machine code. It is maintained by the Web3 Consortium. Contributors include Microsoft, Google, Apple and Mozilla.

Ethereum 2: Implications for Tokenomics

The switch from proof-of-work to proof-of-stake will also bring about significant changes to the economics of Ethereum. Currently, ETH is issued at a rate of about 4.8% of the total supply per year.

ETH Total Supply and Daily Issuance



Source: etherscan.io, Bitcoin Suisse Research.

Daily issuance of ETH to miners has been subject to various changes over the years and is now sitting at around 12'500 ETH per day.

This issuance rate has undergone several changes throughout the years. With the Byzantium hard fork in October 2017, the block reward handed out to miners was reduced from the original 5 ETH per block to 3 ETH. Constantinople further reduced the block reward to 2 ETH in February 2019. However, the difficulty bomb – which raises the mining difficulty and hence increases the time between blocks – was also delayed at the time of the forks, making sure total rewards do not drop further due to longer block times.

With Ethereum 2, this issuance rate will change again. Initially, the rate will increase slightly due to rewards being handed out on the beacon chain as well as the legacy chain. Assuming a (generous) 30 million of staked ETH, the annual issuance on Ethereum 2 would amount to 0.62 %,[10] bringing the overall issuance on both Ethereum chains combined to about 5 %.

However, once Ethereum 2 is used to secure the legacy chain or – at the latest – the current chain becomes a shard, the issuance rate will be drastically lower. The 4.8 % of the total supply currently handed out over the year to miners will be unnecessary, leaving only the issuance on Ethereum 2 – which could range from about 0.4 % to 1.2 % with the current specifications. This would be equivalent to two of Bitcoin's halving events conducted at the same time. Only time will tell how this change in the supply and demand equilibrium will impact the price of ETH – and the effects of this issuance rate change will be hard to separate from other price drivers. Also, the beacon chain first must prove that the currently suggested numbers are sufficiently attractive for validators to secure the network.

[10] https://docs.google.com/spreadsheets/d/15tmPOvOgi3wKxJw7KQJKoUe-uonbYR6HF7u83LR5Mj4

EIP-1559

There is an additional proposal in the works that could strongly affect the total net ETH issuance: Ethereum Improvement Proposal 1559, or EIP-1559.[11] The goal of this proposal is to simplify the fee markets by replacing the current first price auction model – where users regularly overpay on fees – with one that includes a "basefee" plus a tip for the miner or validators that includes the transaction in a block. The basefee would be burned, making the ETH of everyone more valuable, and miners or validators would only receive the tip. The main advantage of this way to structure fees is that they would be much more predictable: The basefee is known *before* creation of the block. This is in contrast to the current model, where network users only know what the minimum fee to get a transaction included was *after* a block has been mined.

Burning a large part of the transaction fee would also mean that the net issuance of ETH will be lower. As shown on page 29, about 520 ETH per day are paid to miners as fees – or about 190'000 ETH per year. EIP-1559 would result in an additional decrease of the annual issuance rate of about 0.2 %. Depending on transaction volumes and fee markets, this could eventually even lead to negative issuance rates in the future.

Conclusion

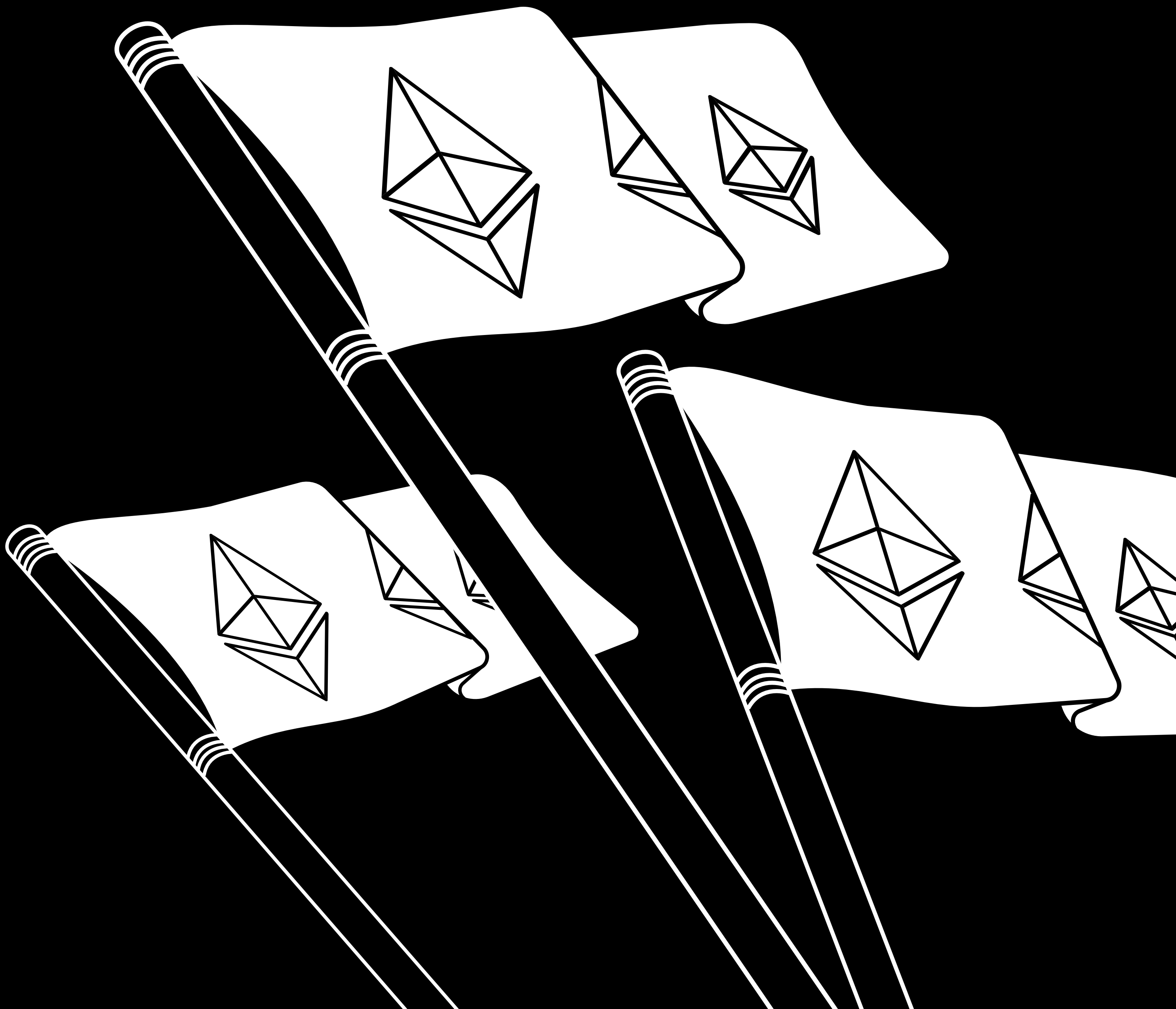
Ethereum's largest and most impactful network upgrade is coming in 2020 and the years ahead. The switch to Ethereum 2 will have vast implications for its scalability, security, decentralization, and economics. Throughputs of around 10'000 transactions per second are anticipated, and abandoning proof-of-work might improve decentralization as well as the carbon footprint of the network by strongly reducing the amount of computational work validators have to perform.

After a slight initial increase, the total issuance of ETH/ETH2 will drop to levels significantly below the current benchmark of around 4.8 % in the long run. Over the course of the next years, it will be interesting to see how the ETH market reacts to this shift of the supply and demand equilibrium.

[11] https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md

The Decentralized Finance Revolution on Ethereum

Written by Joseph Lubin



Composable, interoperable decentralized finance (DeFi) tooling will unlock billions in previously untapped value.

Stablecoins will make DeFi accessible in emerging markets and accelerate global adoption of blockchain-based systems.

Novel smart-contract governed payment structures will emerge, such as intermittent licensing payments or pay-as-you-go parametric insurance.

Author: Joseph Lubin

Stewart Brand famously said at a Hackers conference in 1984, “Information wants to be free.” While he meant “free” in terms of cost, the idea also applies to the movement of information through physical space and across social groups: the Internet enables information to flow better across the planet. The initializing blockchain use case of Bitcoin proved that value, like information, can now move freely across borders, through databases and digital infrastructures.

> **“(...) value, like information, can now move freely across borders, through databases and digital infrastructures.”**

Ethereum makes digital money highly programmable, enabling distributed users to execute code in the form of smart contracts. Beyond speculation and storage of value, Ethereum enables many aspects of traditional finance to run on open networks, with on- and off-ramps to allow greater interoperability with fiat currencies, other cryptocurrencies, and traditional assets.

Just over four years after Ethereum launched, major markets, major governments, and major banks are all part of the experiment: over a trillion dollars’ worth of transactions have settled on Ethereum. Two years ago, there was practically no such thing as open decentralized finance (DeFi), or the manufacturing of financial instruments using open blockchains. In that short time, we have seen a host of open, permissionless financial tools not just emerge, but explode on Ethereum. These systems make the existing financial system more potentially accessible by way of open protocols and transparent data.

From payments and commerce, to banking and lending, to capital markets, to managing investments, to insurance and asset tokenization, DeFi has begun to reach into every major area of the global financial infrastructure. Today there is just under $700 million invested or staked in the DeFi ecosystem, which has generated over $50 million in premium. The number of new addresses grew 1,589% in Q2 of 2019 alone.[1]

A particularly exciting area of DeFi growth in 2019 was the diverse stablecoin space. This past year saw the announcement of Facebook’s Libra and JPMorgan Coin, while the projects with major traction like Tether and DAI gained further momentum – their combined market cap is over $5 billion as of this writing, more than double what they were a year ago. Signature Bank’s Signet and Wells Fargo’s stablecoin both saw great user adoption in 2019, as did the Gemini dollar and Coinbase’s USDC. The transactional growth of just Ethereum-based stablecoins quarter over quarter is greater than that of PayPal’s Venmo.[2]

The wide variety of stablecoins on Ethereum are making the network increasingly functional as a fiat payment platform, as discussed by Omid Malekan in a recent article titled “The Speculative Case for $1000 ETH.”[3] A user has multiple protocol options to choose from, none of which charge more than a few cents in fees, unlike virtually every legacy payment option, which can cost retailers several percentage points of their revenue. When we consider that the combined market cap of legacy payment providers today is over a trillion dollars, it’s not hard to imagine that Ethereum-based options that make payments easier and cheaper could start to gather considerable momentum.

[1] https://reports.credmark.com/TheCryptoCreditReport-q3-2019.pdf
[2] https://www.newsbtc.com/2019/07/31/ethereum-stablecoins-post-better-quarterly-growths-than-venmo/
[3] https://medium.com/@omid.malekan/the-speculative-case-for-1000-eth-if-ethereum-is-valued-as-a-fiat-payment-fintech-platform-7024549998a3

One of the great attributes of Ethereum, and therefore a core feature and advantage of DeFi, is composability: I might have a bank account, a financial savings account, and another account to bring in equities, bonds, or derivatives, but making them work together or moving value between them is clunky. Now those elements can interact and even be configured into composite structures or flows with interoperable smart contracts and Ethereum DeFi dashboards. Adding a new application to the Ethereum World Computer makes that application available to, and interoperable with, many other applications on the platform. Hosts of financial primitives can be combined like Lego bricks and deployed swiftly, inexpensively and globally with ease. With ConsenSys's Codefi offerings, along with OpenLaw, the marginal cost of manufacturing and distributing a new financial instrument is dropping towards zero.[4]

A creative and intrepid DeFi explorer (Definaut?) could receive a stablecoin payment, convert it to Ethereum, and use some of the amount to fund a Maker collateralized debt position, or CDP – getting the long-term benefit of growth on the Ethereum while being able to use the money.[5] She might use another piece of the amount on an exchange to purchase a different coin, send that coin to Compound and earn interest on it, cash out that interest to buy yet another coin on another exchange, and use it to invest in a tokenized asset or in a risk-free lottery like PoolTogether, all while hardly noticing the fees. That is a powerful change from existing payment channels and can happen in a fraction of the time, to say nothing of attempting any of this across national borders. Now value can move around as freely (easily and cheaply) as information.

Stablecoins offer emerging markets entry into the DeFi ecosystem and participation in a wide variety of previously inaccessible financial applications. Reduced friction across borders and less volatility than local fiat currencies make stablecoins particularly attractive in these markets. Last year, a ConsenSys partnership with Oxfam used DAI to distribute humanitarian aid delivery vouchers in the South Pacific island nation of Vanuatu, which is prone to frequent natural disasters.[6] The program used a voucher token wrapped around a DAI token, which could only be unwrapped and redeemed by verified members of the program's whitelist – an AML measure that also took advantage of mainnet security and ensured regulatory compliance.

Developed markets, too, could soon rely increasingly on price-stable currencies as the major monetary systems of the world are challenged. We've seen the yield curve inverting and central bankers around the world have been engaging in quantitative easing for quite a while. As they try to stimulate national and global economies, more rapid quantitative easing will eventually cause a loss of trust in these centralized fiat currencies. Various configurations of price-stable blockchain-based currencies built on top of state-issued currencies or other instruments could prove to be a promising new model.

Countries are already becoming increasingly comfortable with the notion of minting their own digital currencies, pegged to some fiat asset, as a means of reducing transaction fees and increasing transaction speed. The British Virgin Islands recently announced the development of a digital currency pegged 1:1 against the US dollar. Their goals are to reduce transaction fees and increase transaction speed. The central bank of France will soon begin testing a central bank digital currency (CBDC), while the People's Bank of China and the Marshall Islands are also set to roll out plans for digital currencies next year.

"Cash flow is so important to small businesses that they are eager for a way to cut settlement time, and digital currencies will provide that solution."

We will see other payments innovations in the coming year. Apple's latest push into mobile payments, Apple Pay, and Facebook's rollout of Facebook Pay to support in-app payments on WhatsApp, Instagram, and Facebook are part of a larger trend towards mainstream comfort with mobile payments, not to mention massively popular platforms like AliPay and WeChat Pay in Asia. Mobile payments through Apple Pay and services like Venmo and the Venmo card are already familiarizing consumers with the idea of money existing on their phone, and will act as an on-ramp towards the download of a mobile wallet. Consumers and businesses alike will begin to realize that money transmission can, and should be, as simple as sending a text message. Cash flow is so important to small businesses that they are eager for a way to cut settlement time,

[4] Codefi is ConsenSys' commerce and open decentralized finance group. For more information, visit https://codefi.consensys.net

[5] A MakerDAO Collateralized Debt Position or CDP, is an Ethereum-based smart contract that creates Dai in exchange for collateral, which it holds in escrow until the borrowed Dai is returned.

[6] For more information, visit https://consensys.net/social-impact/project-unblocked-cash-case-study/.

and digital currencies will provide that solution. It takes days for ACH transfers to settle, whereas blockchain-based payments are received nearly instantly. Such payments effectively settle in a few minutes on a highly decentralized and secure network like Ethereum and a bit more slowly on the Bitcoin network.

Blockchain-based payments provide users with more granular control over how merchants are able to use their funds. Whereas with a credit card there is an implicit understanding that the merchant will not charge you for a recurring subscription service more than you initially signed up for, you are entrusting the merchant with your credit card, rather than with that amount of money. With a smart contract agreement, the buyer has complete certainty that the upper bound of a payment will never exceed the authorized amount, and can authorize the cancellation of that subscription at any time. Blockchain-based payment platforms, such as ConsenSys Codefi's Daisy, allow anyone to accept recurring payments without absorbing credit card fees or requiring the customer to trust merchants with their credit card data.

Novel payment structures such as state channels mechanisms, which let parties interact directly off-chain and settle when ready on the mainnet, can allow merchants to nimbly process micro-transactions of fractions of a cent. Other payment structures will emerge that are uniquely suited to smart contract-governed payments, such as regular subscriptions payments, intermittent licensing payments (for music or other content, perhaps), or an auto insurance provider offering a parametrized insurance policy that charges fractions of a cent for each second behind the wheel of a covered car, adjusting the rate based on time of day and region travelled.

All of this is happening on the Ethereum blockchain. These areas of innovation, combined with increasing momentum in enterprise applications of Ethereum, tokenization of assets, and software contained within these new subsystems as they mature, will all begin to combine to form the substrate for the new global digital economy – and they will amplify one another.

The global economy needs an objectively trustworthy frame of reference to coordinate logic and transactions between business networks. That frame of reference is shaping up to be the Ethereum mainnet, which will function as the global settlement layer for digital assets of the future web. In order to be maximally secure, it must also be maximally decentralized in its architecture. If the goal is building, or re-building, a more secure, reliable, and interoperable global financial system, it is suboptimal to architect it on centralized, open platforms subject to censorship, single points of control and failure and other kinds of potential improper manipulation.

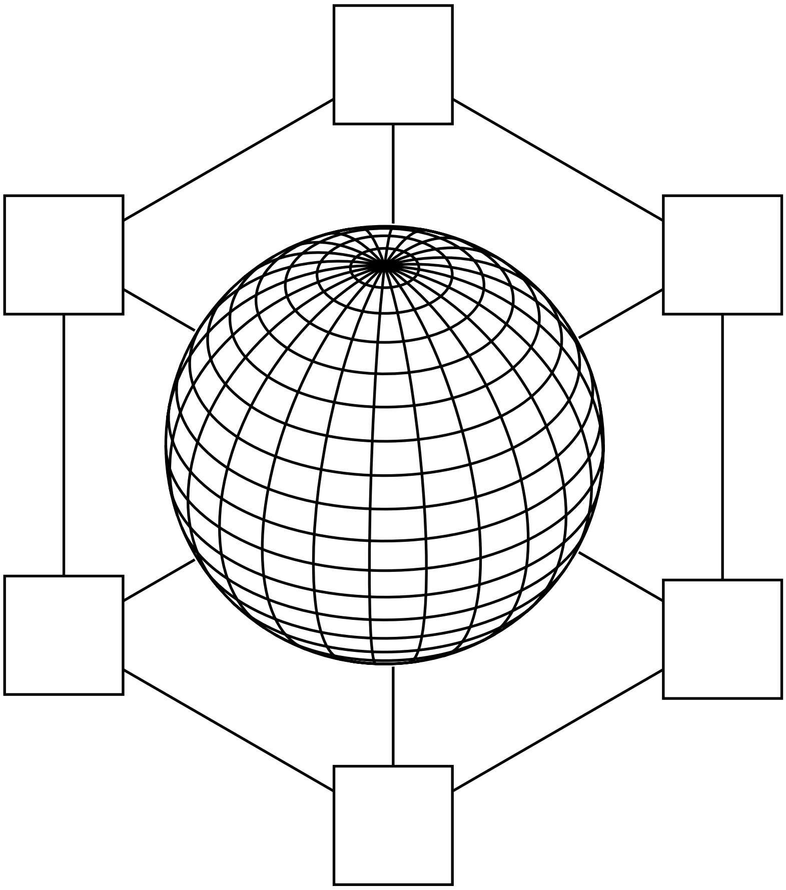
Atop and alongside the maximally decentralized trust foundation and global settlement layer of the Ethereum mainnet, the future of decentralized protocol technology will consist of many functional elements: for trusted transactions, automated agreements, smart software objects, storage, bandwidth, heavy compute, identity, reputation, proof of location, legally enforceable agreements, certificates, equity and real estate tokenization and ease of fractional ownership, financial inclusion, clearing and settlement in the instant of the transaction, and more.

So many aspects of our global financial infrastructure are built on outdated software platforms, and vulnerable database architectures, use antiquated and sluggish cross-border settlement systems, and little of it is fluidly interoperable. Financial institutions are, of necessity, reconciliation companies that fix misunderstandings and broken transactions between disparate databases that each house a fraction of the understanding of a transaction. When things go right, they are able to offer financial services to their corporate and consumer customers. It doesn't have to be this way. Blockchain financial infrastructure will allow such institutions to interoperate with one another on a new trust foundation that represents a single share source of truth. Trillions of dollars in wasted or untapped value is waiting to be unlocked by this new decentralized protocol financial tooling.

But the potential for blockchain in 2020 goes far beyond DeFi and payments: it is about automating trust to facilitate collaboration, and enabling digital scarcity to allow for the creation of digital assets; it is about convergence of platforms, reducing inefficiencies, doing business faster and better than ever while creating healthier economic dynamics in the process. I have no doubt that this will be an exciting, and likely defining, year for our ecosystem.

How Decentralized Finance is Automating Central, Commercial, and Investment Banking

Written by Demelza Hays



The decentralized lending market has $477 million in outstanding loans and is expected to become a billion-dollar industry in 2020.

Similar to LIBOR, a decentralized inter-protocol offered rate (DIPOR) is being developed that will serve as a benchmark for decentralized finance loans, interest rate swaps, and total return swaps.

Cryptographic stablecoins suffer from the stablecoin trilemma that forces issuers to choose two out of three goals: decentralization, capital efficiency, and collateralization.

“What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”
— Satoshi Nakamoto

The cryptocurrency and blockchain revolution is about removing unnecessary intermediaries from financial transactions. Over the past six years, large cryptocurrency exchanges and brokers have gradually expanded their services. Originally, they provided deposit accounts and trade settlement. Today they offer stablecoins, lending, staking, crypto payments, and derivatives. However, the market is fragmented with different exchanges, custodians, brokers, and market makers.

In 2020 and onwards, cryptocurrency companies will compete to have the largest network of users by providing the most user-friendly and lowest cost on-ramp into crypto from fiat. Similar to the consolidation of investment banks and commercial banks after the repeal of Glass-Steagall in the 1990s, cryptocurrency companies are becoming megalith companies that provide a whole gamut of financial services from security token underwriting and listing to retail checking accounts. In response, decentralized finance (DeFi) applications are being developed that increase the variety and quality of services in the entire industry.

The decentralized finance movement is taking us back to Satoshi Nakamoto's original vision of conducting financial transactions online without an intermediary. In contrast with the centralized services provided by crypto banks and exchanges, decentralized finance refers to financial services that allow users to keep custody of the private key that controls access to their wallet. There is already $670.9 million worth of cryptocurrencies locked in Ethereum-based DeFi smart contracts with MakerDao Dai accounting for 50 % of that market.[1] When including EOS-based DeFi applications, the figure swells to $892 million currently locked in decentralized finance smart contracts.[2] For example, the DApp EOSRex has almost $300 million locked in it.[3]

According to the Financial Stability Board, there are four main ways that DLT will impact financial services: payments and settlements, trade finance, capital markets, and lending.[4] This article focuses on the two main areas where decentralized finance applications built on public and permissionless distributed ledger technologies like blockchains are expected to disrupt banking, including central banking, in 2020: decentralized stablecoins and decentralized lending.

Decentralized Stablecoins Are Disrupting Central Banks

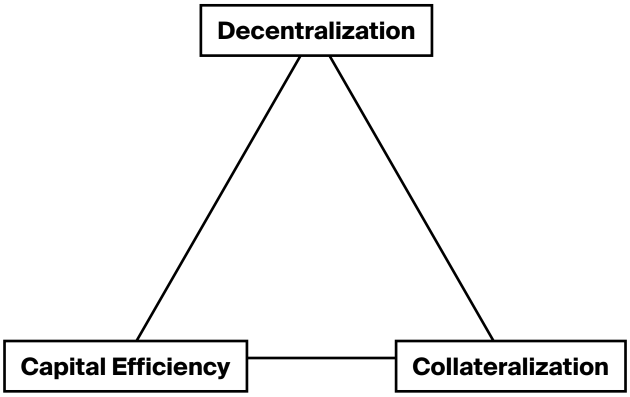
The increasing interest in blockchain and distributed ledger currencies has prompted central banks to release cryptographic national currencies. Nine countries have either already launched or will soon launch a cryptographic version of their currency including Singapore (Monetary Authority of Singapore), China (People's Bank of China), Cambodia (National Bank of Cambodia and Soramitsu), Thailand (Bank of Thailand), Brazil (National Social Development Bank), Venezuela

[1] http://defipulse.com/
[2] https://defi.review/
[3] Although the DeFi Pulse is one of the leading data sources for decentralized finance use, Alethio and DeFi Review are also frequently used.
[4] https://www.fsb.org/wp-content/uploads/P060619.pdf

(Petro), France (Bank of France), Sweden (Riksbank), and a select cohort of Caribbean nations (Bitt). Central bank digital currencies (CBDCs) will compete with corporate issued stablecoins by tech giants, such as Facebook's Libra, and private issued stablecoins, such as MakerDao Dai. Whether government, corporate, or private, currency issuers must make decisions with regard to token economics. For example, what type of collateral should be used to back the coin's value on the market, if the coin's value should be pegged to another asset, if the blockchain should be public or private, and the optimal inflation rate.

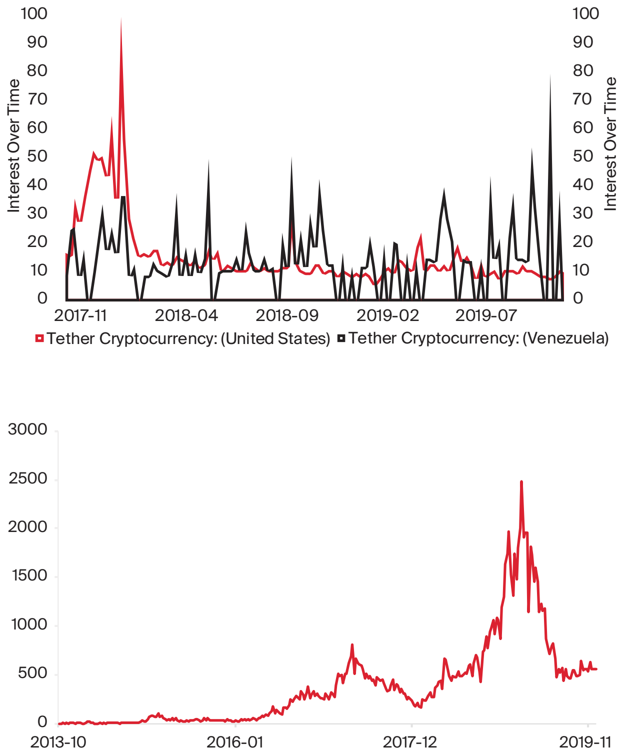
However, cryptographic stablecoins suffer from the stablecoin trilemma that forces issuers to choose two out of three goals: decentralization, capital efficiency, and collateralization.[5]

The Stablecoin Trilemma



In this context, decentralization refers to how transactions are validated in the network. This means that anyone has the ability to setup a miner or staking node and begin validating tractions instead of relying on a central authority to approve all transactions. Capital efficiency refers to coins that have 100 % collateral backing or less, and collateralization refers to coins with more than 100 % on-chain collateral backing. Stablecoins such as MakerDao Dai, EOSDT, and Neutral have two out of the three qualities, decentralization and collateralization. However, they are capital inefficient. Stablecoins such as Gemini Dollar and Tether are decentralized and capital-efficient; however, they have 100 % or less on-chain collateral backing and require users to trust the issuer. This is where most of the central bank digital currencies fit in. Finally, there are decentralized stablecoins that are capital-efficient that rely on algorithms to stabilize their value. Basis was the most famous coin in this category; however, the project was stopped by US regulators before being released to the market.[6]

The urgency of creating central bank digital currencies is bolstered by the growing retail demand for decentralized cryptocurrencies and stablecoins. In countries with high inflation, residents can purchase Bitcoin and then convert Bitcoin into stablecoins like Tether and MakerDao Dai. According to the International Monetary Fund (IMF), Venezuela's inflation rate in 2019 is estimated to be 10,000,000 %.[7] This has triggered an increase in interest in cryptocurrencies, such as Bitcoin, and stablecoins, such as Tether. Bitcoin transactions accounted for $7 million per week before the government enacted limits on Bitcoin transactions in February. Furthermore, stablecoins can be used in countries that have strict capital controls,[8] such as Argentina, where individuals are only allowed to purchase up to $10,000 a month worth of U.S. dollars.[9]



Source: coin.dance, Google Trends, Incrementum AG.

Venezuelans Demand Bitcoin and Increasingly Search Tether Cryptocurrency on Google.

[5] The State of Stablecoins 2019 Hype vs. Reality in the Race for Stable, Global, Digital Money.

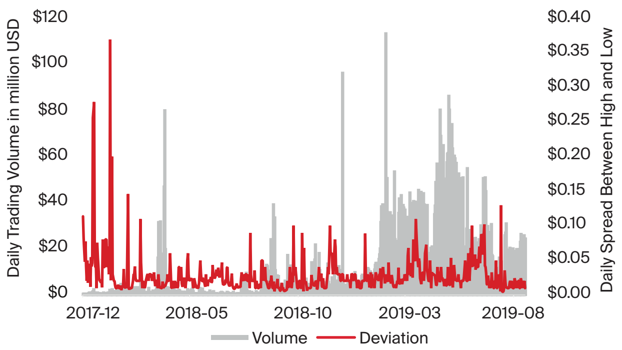
[6] https://www.theblockcrypto.com/daily/5122/stablecoin-project-basis-is-shutting-down-and-returning-the-majority-of-capital-raised-to-investors

[7] https://www.imf.org/en/Countries/VEN

[8] https://outlierventures.io/wp-content/uploads/2019/06/Mapping-Decentralised-Finance-DeFi-report.pdf

[9] https://www.bloomberg.com/news/articles/2019-09-01/argentina-imposes-currency-controls-as-debt-crisis-escalates

Decentralized cryptocurrencies, such as Bitcoin and Ether, and stablecoins, such as MakerDao Dai, can be used to send value over the internet without intermediaries.[10] The largest decentralized finance stablecoin is MakerDao Dai with approximately $317 million worth of Ether or 1,753,031 ETH locked up in MakerDao Dai collateralized debt positions or "vaults" (at the time of writing).[11] This amounts to 1.62 % of all outstanding Ether. Locking up Ether allows users to create Dai. There are currently 96 million Dai in circulation, which has a USD value of approximately $96 million because Dai is pegged one-to-one with the US dollar. The amount of Dai locked up has had a positive correlation with the price of Ether in the past, which means that as the price of Ether increases the amount of ETH locked up in MakerDao Dai vaults has increased.



Source: coinmarketcap.com, Incrementum AG.

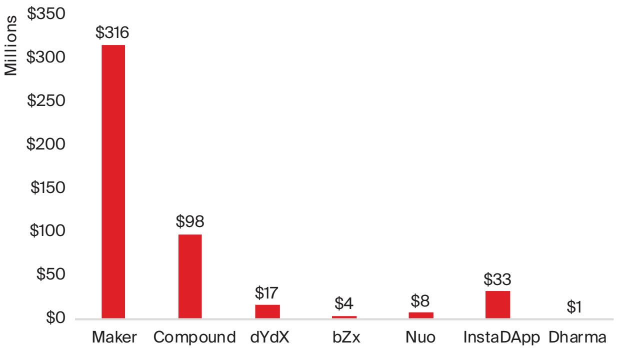
MakerDao Dai Intraday Volatility and Daily Trading Volume

The stablecoin market is expected to grow larger in 2020. Investors in low-interest-rate and negative-interest-rate countries, such as Switzerland, can earn higher annual returns on stablecoins via staking and lending interest rates. For example, Dai deposited on Compound is earning 5.7 % APR.[12] Germany's recent regulation enabling banks to store cryptocurrencies on the behalf of clients is likely to extend federal deposit insurance to stablecoins, further professionalizing the industry.[13]

Decentralized Lending Will Become a Billion Dollar Industry in 2020

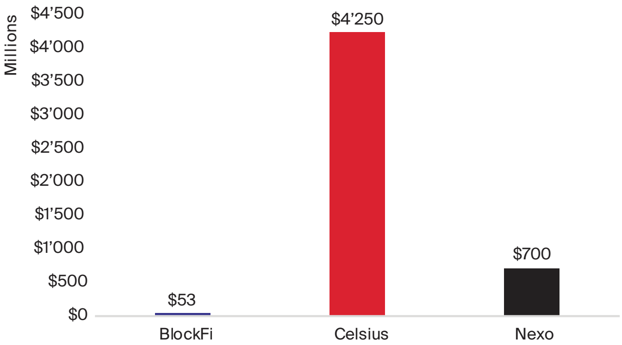
The main service of banks is to pool risks and match maturities of clients that want to lend and clients that want to borrow. Smart contracts enable pooling of risks and matching maturities to be automated and executed on a blockchain. Therefore, one of the largest impacts of decentralized finance applications on banking is peer-to-peer lending and borrowing that allows clients to keep control of their private keys. Decentralized crypto lending platforms, such as Maker, Compound, and dYdX, have approximately $477 million in assets loaned. In contrast, centralized platforms, such as Celsius, Block Fi, and Nexo, have completed over $5 billion in cryptocurrency loans to date.

The advantages of decentralized finance loans are that they are lent on non-discriminatory basis, meaning that the same rates are available to any borrower regardless of that individual's characteristics. The terms and conditions of DeFi loans vary depending on the platform; however, many DeFi loans do not have a minimum loan amount or lending period. On average, decentralized lending platforms have lower interest rates than centralized cryptocurrency lending platforms. Interest rates for truly DeFi lending platforms such as Compound have much lower interest rates (0.02% per annum for ETH) than centralized crypto lending platforms like Celsius Network (3.40 % per annum for ETH).[14]



Source: defipulse.com, Incrementum AG.

Total USD Value of Loans or Borrows from Decentralized and Centralized Crypto Lending Platforms in Millions of USD



[10] Decentralized finance stablecoins do not include stablecoins such as Tether that require a central party to manage reserves of tangible or physical assets.
[11] https://mkr.tools/system
[12] https://compound.finance/
[13] https://www.coindesk.com/german-banks-allowed-to-sell-and-custody-crypto-assets-from-2020-report
[14] https://www.bitcoinsuisse.com/research/decrypt/on-chain-derivatives-and-insurance/

The stablecoin MakerDao Dai only allows users to "borrow" from themselves instead of lending out cryptocurrencies to other people. This is why DeFi apps, such as Compound and dYdX, are gaining traction. They allow investors to lend out cryptocurrencies to other people, which competes with the traditional service of pooling risks provided by banks. Although the process is complicated, sophisticated investors are locking up Ether and other cryptographic assets in MakerDao smart contracts, "creating" Dai. That Dai is then sent to the Compound smart contract in order to lend out to borrowers and earn interest. Dai already accounts for double digit percentages of volume on the lending platforms Compound and dYdX.

In 2020, arbitrage between debt markets and staking markets will lead to a narrowing of the spread in crypto interest rates on lending and staking returns. Investors can borrow coins from low-interest decentralized lending platforms and lend them out on high-interest centralized lending platforms. Investors can also borrow 32 Ether for low rates on DeFi platforms and set up Ethereum nodes earn approximately 4 % per annum after the switch to proof of stake in Q1 of 2020. However, lending and staking have different liquidity profiles and risks. Different lending and staking applications require investors to locks up coins for varying periods of time. Centralized solutions have credit risk while decentralized solutions have technical risks, such as a bug in the smart contract code. Also, staking Ether requires technical expertise and nodes that are not online all of the time will be punished by Ethereum's slashing mechanism that will take ETH from the node's staked coins and kick out the validator from the network.

In fact, The Block is working on a LIBOR-type rate for decentralized finance called DIPOR.[15] In 2020, DIPOR is expected to provide a smart contract-based interest rate for each cryptocurrency, based on the volume-weighted interest rates for that cryptocurrency that are being offered on the various DeFi lending platforms.[16] The MakerDao governors that hold MKR tokens and decide when to increase and decrease the MakerDao Dai stability fee could use the DIPOR rate as benchmark. For example, if Dai is trading at $0.95 cents, this means that the supply of Dai on the market is too high relative to the demand. The governors could raise Dai's stability fee above the DIPOR rate in order to encourage users to borrow Dai from other lenders instead of opening up new Dai vaults that add more Dai into circulation.

The disadvantages of decentralized lending platforms include capital inefficiency, because trustless smart contracts require over-collateralization. DeFi lending suffers from the same trilemma as stablecoins discussed in the previous section. The average amount of collateral invested in MakerDao Dai vaults is currently 319.83 % and has been as high as 600 % during 2019. Development teams are working on a smart contract-based way to take collateral above the 150 % requirement and automatically invest that collateral in Compound so that the depositors of over-collateralized debt positions can earn interest on their deposits. This is referred to as "superfluid" liquid in the cryptocurrency space because the same collateral is pledged for multiple contracts. This development is expected to increase the interconnectivity of the decentralized finance applications and increase the overall systemic risk similar to rehypothecation and over-leveraged collateralized debt positions during the subprime mortgage crisis of 2008.

Conclusion

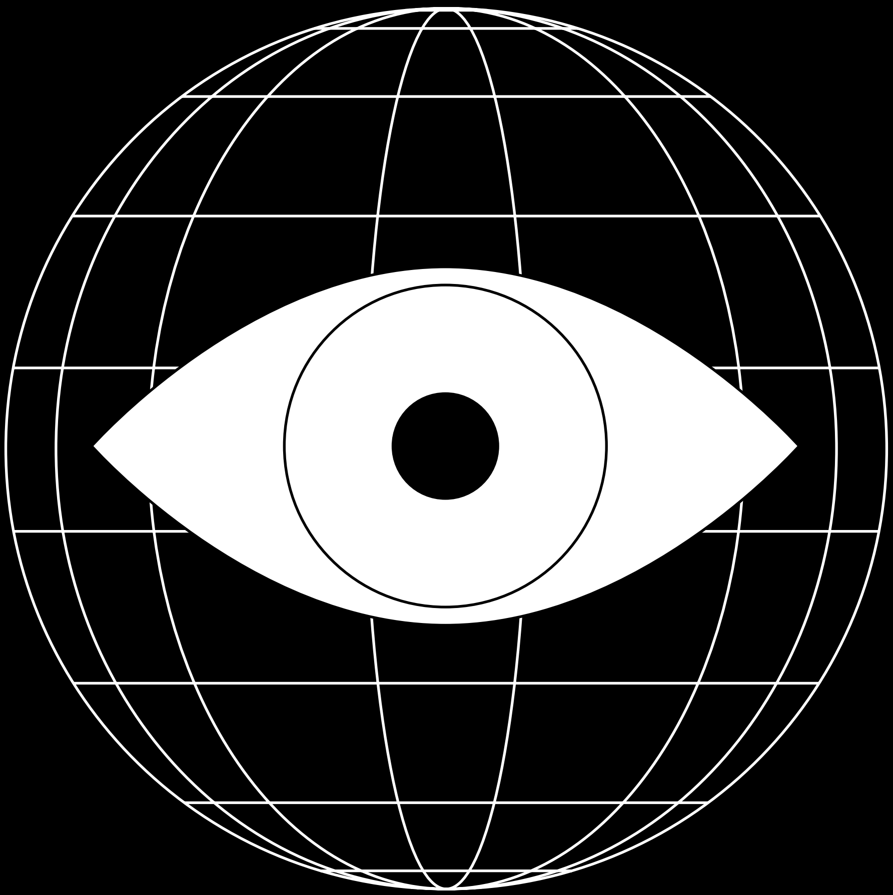
The DeFi movement in 2020 is expected to witness the emergence of new smart contract applications such as synthetic tracking of all financial assets, such as gold, shares, and bonds, via collateralized debt positions on Ethereum, staking of fractional amounts of cryptocurrencies with wallets that allow users to hold private keys, and decentralized credit ratings for pseudonymous accounts based on the user's repayment record and details of the loan, such as duration, amount, and interest rate. An exciting area that is expected to impact asset management is the "social trading" trend. Social trading apps like settle.finance and TokenSets allow asset managers to share the performance of their crypto portfolios on social media, and their followers can automatically execute the same trades that their asset manager makes while still controlling the private key to their funds.

Overall, DeFi applications that are simple to use and understand like stablecoins are expected to gain adoption by the broader market of non-crypto retails investors that live in countries with high inflation and capital controls, whereas DeFi applications that are difficult to use and understand like minting synths on Synthetix and total return swaps on UMA and Rainbow Network can be expected to gain adoption by large cryptocurrency holders and traditional hedge funds.

[15] The London Interbank Offered Rate (LIBOR) is the average interest rate that banks are willing to lend to other banks for in the London interbank market.
[16] https://www.theblockcrypto.com/genesis/19324/introducing-dipor-libor-for-open-finance

Public or Private?

Written by Marco Schurtenberger



■ Public blockchains inherently provide more overall network security because the large number of network nodes preserves immutability.

■ Developments in encryption and privacy technologies diminish concerns about confidentiality on open blockchains.

■ Using public blockchains can save costs for companies by decentralizing the maintenance of the network.

Why Public Blockchains Are the Future

What makes public blockchains more likely to succeed in the long run over their private counterparts? What are the benefits and disadvantages of both types of blockchain, and which is best suited for a given purpose? This piece defines both public and private blockchains and presents a short overview of their similarities, differences, and respective use cases.

What are public, and what are private blockchains?

The name says it all – public blockchains are entirely open to the public and accessible to anyone, which means that anyone with an internet connection is allowed to contribute to and interact with a given blockchain. Thus, any person can download a public blockchain's software and run their own node, allowing them to verify its information and/or add new blocks to the blockchain.

Due to being open for anybody's contribution, popular public blockchains such as Bitcoin, Ethereum, and Tezos are composed of thousands of nodes actively contributing to the maintenance of their blockchains. This forms a global and decentralized network of independent nodes where each node communicates with and verifies the work of other nodes instead of a single entity, or a small group of entities, controlling the system.

On the contrary, running nodes in a private blockchain (e.g. Hyperledger and/or R3 Corda) is only possible for parties which have been granted access beforehand. Restricting access to a private blockchain can be achieved via different methods such as authentication through identity management systems or operating a blockchain in an isolated network.

An analogy for public vs. private blockchains is the internet vs. intranets. When commercial computer-use started to gain traction in the 1980s, many enterprises used intranets. Like the internet, an intranet is a network, however, only authorized users are allowed to access it, whereas anyone may access the internet. Over time, far greater innovation took place on the internet and intranet-use fizzled out.

While the terminology in the blockchain industry is still evolving and not widely agreed upon, a synonym for private blockchains is "permissioned blockchains", whereas public blockchains are often called "permissionless blockchains". Private / permissioned blockchains are operated by pre-selected participants such as members of a consortium. This means, the participants in private / permissioned blockchains are known and on- or off-chain controls (such as a regulatory or audit body) are established to validate whether these participants act in good faith. Because all participants are known, misbehaviour, such as including a counterfeit transaction in a block, can be punished (e.g. punishment may be in the form of a previously defined and agreed upon fine).

Since everybody is able to join a public / permissionless blockchain, its participants may be anonymous and incentivized by the chance to earn that blockchain's native currency as a reward when correctly behaving according to the blockchain's protocol and rules. In Proof-of-Stake based blockchains (see box below for a short definition) such as Tezos, participants also can lose part of their stake if they do not follow protocol rules and are accused by another blockchain participant called an "accuser". The accuser then earns this stake for its performed verification work. Each blockchain, whether private or public, needs a control system to ensure participants behave in the correct way according to a blockchain's protocol and rules.

What are open and closed blockchains?

In addition to the definition of public and private, "open" and "closed" are also commonly used terms to describe who can read (i.e. collect and analyze) data on a blockchain. Data stored in an open blockchain can be read by any blockchain participant, whereas in a closed blockchain only a few participants are capable to read data.

Given these two word pairs 'public / private' and 'open / closed', there are four basic characteristics possible to describe a blockchain. Each of these characteristics serves different use cases:

1. Public and Open:

This actually characterizes the type of blockchain people are typically referring to when they speak about public blockchains. Public and open blockchains are available for everybody and written data is accessible and readable by everybody as well. Thus, public and open blockchains support use cases such as public/transparent ledgers where everybody can read and verify data (e.g. account balances of currencies or other assets like in-game assets/trophies or which kind of sport bets have been placed by the blockchain's participants).

Proof-of-Work vs. Proof-of-Stake:

Proof-of-Work (PoW) and Proof-of-Stake (PoS) are two possible methods ("consensus algorithms") to determine which blockchain participant is allowed to add and validate blocks in a blockchain. Participants are financially rewarded for adding and validating blocks to a blockchain. Such rewards typically include a "block reward" plus transaction fees from a block.

For example, PoW is used in Bitcoin and Ethereum and participants have to solve a mathematical "puzzle". Solving this puzzle requires a lot of computational power (hardware and electricity) and the first able to solve the puzzle is allowed to add a new block to the blockchain (a process called "mining"). The difficulty to solve the puzzle is proportional to the total amount of computational power attempting to solve a given puzzle. Since a lot of computational power goes into trying to solve a given puzzle, the Bitcoin blockchain, for instance, was in July 2019 consuming an amount of energy equal to that of Switzerland.[1]

PoS based blockchains do not consume such a massive amount of energy, since the party allowed to add (in Tezos this process is called "baking") or validate a block is determined beforehand. All participants have an opportunity to validate blocks proportional to their tokens ("stake") to bake or validate the next block.

[1] https://www.bbc.com/news/technology-48853230

2. Public and Closed:

A use case for this kind of blockchain for example is voting or polling. Everybody can write his/her vote or opinion to the blockchain, but only the creators of the ballot box are allowed to read the voting results. Public and closed blockchains are often used for medical, legal or financial use cases where customers or prospects can store confidential and / or personal information[2] for restricted access by the corresponding entities.

3. Private and Open:

This type of private blockchain is commonly used in supply chains, where only suppliers are able to write the supply status to the chain, but every private blockchain's participant can track the status and see the information.

4. Private and Closed:

Private and closed blockchains enable use cases where only trusted and known members are able to write and read the data in the blockchain (e.g. an interbank blockchain where banks exchange assets).

Public and Closed	Public and Open
Voting Voting records Whistleblowers	Currencies Betting Video Games
Private and Closed	**Private and Open**
Construction National Defence Law enforcement Military Tax Returns	Supply Chain Government financial records Corporate earning statements

Why use a private / permissioned blockchain?

Companies often choose private blockchains over public ones because they:

- are required to implement very specific use cases (e.g. enabling them with a customized private blockchain to execute transactions faster)

- have concerns about data privacy and confidentiality, or

- operate in regulated areas requiring the use of a private blockchain.

A private blockchain provides more control over the blockchain for these companies or consortiums, since they decide who is able to write data and participate.

A private blockchain is only operated by authorized members or sometimes even only by a subset or one of these members. Thus, a private blockchain is more centralized than a public blockchain consisting of thousands of nodes.

Having consent within this group of permissioned members would even allow them to remove blocks and reverting to an older state. To get such a consent or agreement between a small group of permissioned blockchain participants is easier than in a global, decentralized blockchain with thousands, or tens of thousands, of participants with different backgrounds and goals.

Moreover, operating a private blockchain means as well that the company or consortium requires people with appropriate expertise and experience to run the private blockchain. In addition to required human resources, costs for infrastructure and licences have to be considered as well. Private blockchain technology and services are often offered by startups and the private blockchains are developed and / or strongly customized for a specific use case by these startups. This exposes the company to additional counterparty risks resulting in potential scenarios where the startup is no longer available (e.g. due to bankruptcy).

[2] Important note: Confidential or private data should never be stored on a blockchain, since data may get decrypted in the future. Thus, the blockchain does only store the hash (so called "anchoring") of the data and confirms the content of the data. The data itself is stored off-chain in a secure and access restricted location.

Is a private blockchain more secure due to its private nature?

A private blockchain seems at first glance to be more secure, since one might ask: how can you hack a private blockchain which is “locked away” and only accessible for authorized participants?

Ho ver, this assumption does not take into considerations that employees including suppliers, consultants and contractors are the top source of security incidents[3] and also that hackers have already demonstrated the capability to successfully intrude networks (see for instance the “Cloud Hopper Attacks”[4]).

Would it not be better to rely on a public blockchain and its globally distributed community, where different parties with different backgrounds, experiences, and expertise are using and testing the public blockchain on a day-to-day basis and announcing and fixing security weaknesses in case they detect one?

In addition, the source code of most public blockchains is publicly available and can be reviewed by anybody. This concept of open source software is popular and widely adopted by a vast amount of applications but as well as by operating systems (e.g. Linux or Android). A main advantage of open source is that everybody is invited to inspect the code for understanding and verification of functionality and security. Thereby, no faith is required in a company or sub contractor that they correctly and timely implement or fix security critical functionality. To compare it to the previously mentioned analogy of the internet vs. intranets, more innovation can take place on public blockchains as they are open and accessible for anyone to tinker with.

What type of blockchain will most likely be used in the long run?

With recent developments in encryption and privacy technologies (e.g. zero knowledge proof techniques), public blockchains are able to overcome some of the concerns many companies often have, especially when it comes to privacy and confidentiality. In addition, so-called layer 2 scaling technologies for blockchains, such as Plasma (Marigold on Tezos) or Lightning foster faster and more scalable public blockchains. As a result, common reasons to implement a private blockchain are vanishing as recent tech developments make them irrelevant.

Using a public blockchain instead of a private blockchain can also help companies to save costs since they are not responsible for running and maintaining the entire blockchain network and can instead focus on the integration of their use cases into the blockchain and further innovation. Also, the difference of blockchain types between open and closed will disappear due to some of the technological improvements mentioned above, but this type definition will be still valid to characterize use cases.

Furthermore, we predict that public blockchains and their usage will go through a similar development cycle like the internet. In the past, at a very early stage of the internet, companies were running their own networks (Intranets) with dozens of servers hosting their required applications. Today, a lot of companies obtain their applications directly from the internet (“cloud”) and thus costs for running and maintaining internal networks and application systems are replaced by paying the access to the internet via a local internet provider.

Finally, blockchains will only succeed if they create value. Much like the internet, value from blockchains relies on connectivity and network effects, which accrue on public chains and are fragmented on private ones. For example, tokenized assets such as digital stocks or bonds cannot pass between private chains, meaning that to own a digital security tokenized on a private chain, one would have to be a member of the consortium governing the private chain - given the size and scale of private and public capital markets, it would be virtually impossible to bring all participants onto one private chain network, and value would be destroyed because of fragmentation rather than created. With public chains, more market participants can engage, enabling greater connectivity and exchange of value, thereby providing additional value to all participants. As public chain technology continues to advance, the fundamentally superior economics of public chains will inevitably lead to an obsolescence of private chains and a robust digital economy based on public blockchains.

[3] https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html
[4] https://www.schneier.com/blog/archives/2019/07/details_of_the_2.html

Conclusion

Public blockchains are a very good alternative to traditional solutions especially where different parties want to digitally ensure and record accountability, transparency, and immutability of states such as ownership of goods, balances of assets, proof of origin, proof of possession, etc. Thus, public blockchains are rapidly becoming a technology with which any business sector can find applicable use cases.

Reasons to use a private blockchain become more and more obsolete with ongoing implementation of newly developed encryption and privacy techniques by public blockchains such as Tezos. Using a public blockchain like Tezos provides access to a global, decentralized blockchain with an immense community behind it. This allows companies to focus on their use cases and innovation, and leave the costs of operating the blockchain itself to the community and its validators. Much like the internet, the future is brigth for public blockchain in this space.

The Regulatory Framework for a Tokenized Economy – TVTG Liechtenstein

Written by Stefano Frick and Thomas Nägele

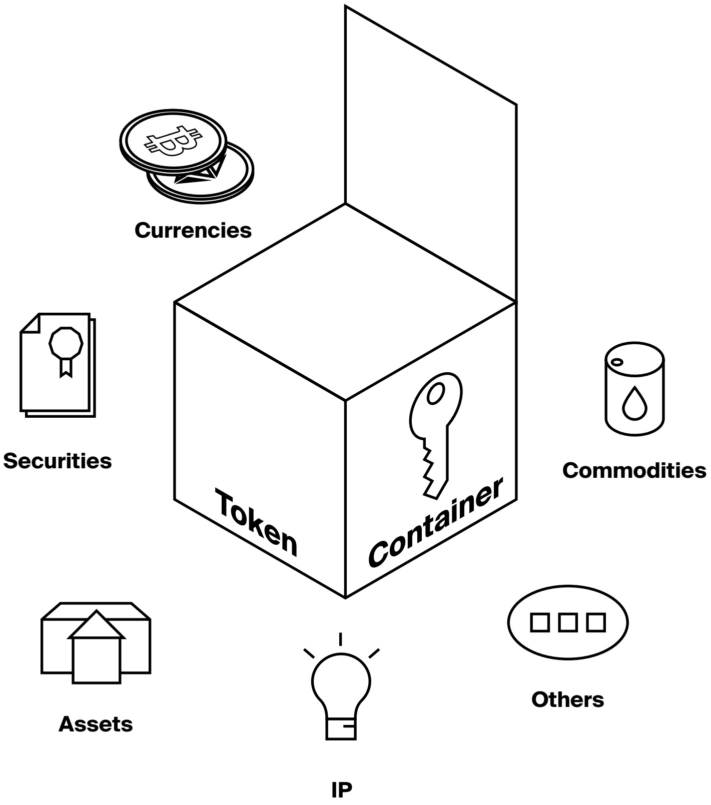
The “Token Container Model” enables a technologically neutral and agnostic token definition and therefore bridges the gap between the digital and the physical world – everything can be tokenized.

The neutral approach of the TVTG offers all sectors sufficient flexibility to enter into new business models. The legal certainty provided by the law will encourage new market participants.

The legislation affords consumers a basis for trusting new technologies that was not necessarily present before.

In October 2019 in Liechtenstein, the Blockchain Act/Token & TT Service Provider Act (TVTG) unanimously passed through its second reading in parliament. Enacted into law on January 1st 2020, this legislation provides the world's first comprehensive regulation of the token economy. But what is this law, and what does it mean for the future of Liechtenstein, as well as the future of regulation surrounding blockchain and crypto on a global scale?

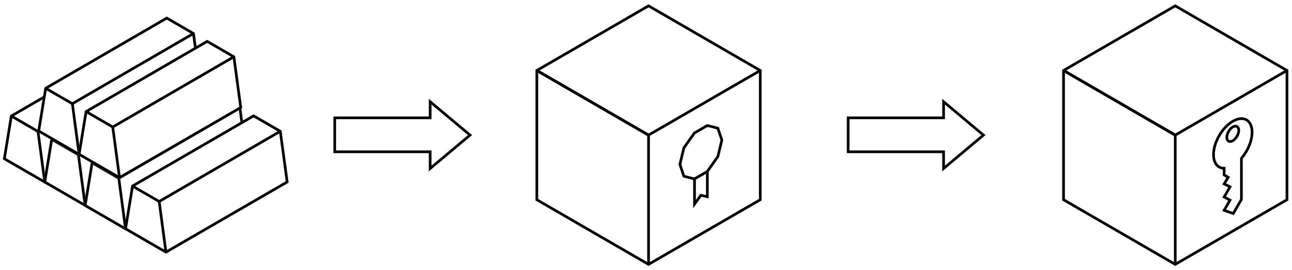
The outstanding professionalism of the government and regulator show why Liechtenstein is well-positioned to continue its pioneering role in the blockchain space and will continue to strengthen its important position in future. The Blockchain Act is another step towards that goal and is the first law worldwide that governs the token economy.



The heart of the TVTG is the "Token Container Model" (TCM) which enables a technologically neutral and agnostic token definition. Within this model, a token serves as a container that links the digital world with the physical world. This can be something physical, a property, gold, stocks, bonds etc., a service but also a digital code, such as Bitcoin. From this, it follows that the TCM offers not only a legal certainty of already existing rights, but also rights to digital information based on blockchain systems.

Furthermore, recognizing the need for a bridge between the offline physical world and the online digital world, the TVTG introduces the role of the "Physical Validator" as a registered intermediary tasked with ensuring that the right to the underlying represented by the token is actually present. On this note, the TVTG also provides a civil law basis for what constitutes an effective transfer of the represented right to the token from party A to B, as well as what constitutes an effective transfer of these newfound digital assets in general. Expanding on the role of the Physical Validator, Liechtenstein is a country especially well-suited for providing these kinds of services, due to the trust history within the country. The token is defined as a piece of information on a TT ("trustworthy technology") System which can represent claims or rights of memberships against a person, rights to property, or other absolute or relative rights and is assigned to one or more TT identifiers.

Here, the Physical Validator would ensure that the gold actually exists. If errors occur in this process, then the Physical validator bears the responsibility.



Takes physical asset in custody or verifies the physical object

Token represents the right

Disposal over the token results in the disposal over the right

To expand on the example of tokenized gold, we can say that several other service providers will be necessary. For example, a "Token Generator" is needed to set up the smart contract and the "Token Issuer" will issue the token. In relation to storage, there is the important role of the "TT-Key-Depositary" who is responsible for the storage of the private keys. Many other roles are also affected, and this shows how regulated and structured the tokenization will be based on the Liechtenstein "Blockchain Act". Besides the "TT Key" that allows for disposal, a "TT identifier" is necessary to accomplish the clear assignment of the token.

Another very interesting case is the tokenization of shares. In this situation, the TVTG makes it possible to bridge the gap between the classic financial industry and distributed ledger technology. Small and medium-sized companies, for example, can tokenize their shares and thus make them tradable.

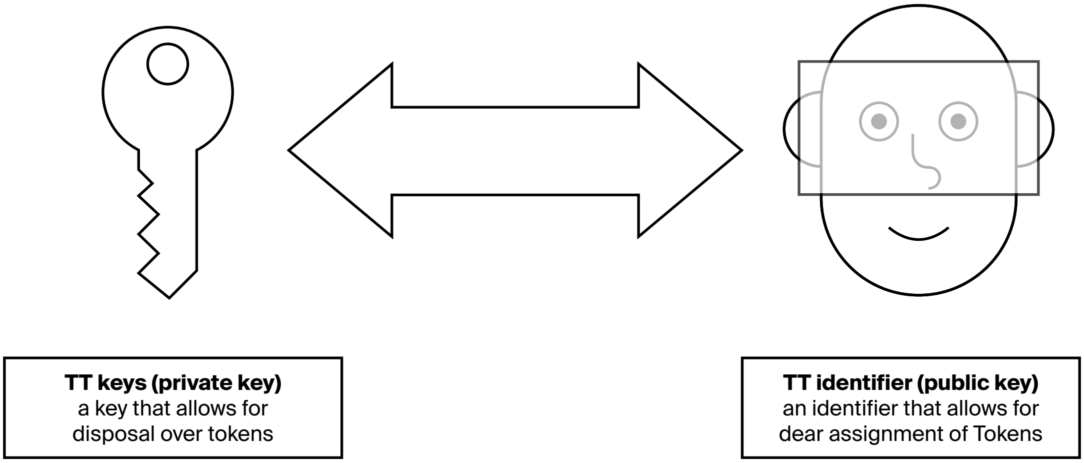
The clearly defined assignment of roles in the token economy offers financial institutions, among others, new opportunities along the value chain. For example, a registered "TT-Generator" can also exercise the role of a "TT-Key-Depositary" when storing the private keys as well as the role of a "TT-Exchange Service Provider" when trading crypto assets for fiat money. Companies can therefore assume several roles, meaning that customers can benefit from a single point of entry into the token economy.

The TCM is thus neutral, which allows for representing of rights to other kinds of tokens, including tokens that might be classified as utility tokens, stable tokens, etc. in other jurisdictions. Avoidance of this classification in favor of a more neutral approach shows the innovative nature of the TVTG. As opposed to other jurisdictions which highlighted these pre-existing definitions in their legislative framework, Liechtenstein has opted for the most neutral approach possible in order to accommodate change and innovation within the space. Therefore, the TVTG offers all sectors sufficient flexibility to enter into new business models and allows entrepreneurs to occupy niches and grow within a regulated environment.

This new legislation is being implemented in a country where the regulator responsible for its enforcement, the Financial Market Authority (FMA), already possesses the requisite know-how for dealing with these projects. With an entire department dedicated to the fielding of Fintech related inquiries, the FMA already has built up their knowledge base surrounding blockchain and crypto projects. This will only serve to grow the blockchain community here once the legislation is in place.

Although many argue that regulation in the blockchain sector is contrary to the peer-to-peer nature of the technology itself, the TVTG was carefully crafted in a manner that bridges the gap between pre-existing regulations and these new technological innovations, without creating unnecessary regulatory hurdles where technology already does the job. Rather, the framework is designed to ease the transition from traditionally centralized and regulated intermediaries to decentralized systems. The Act also aims to assist in curbing money laundering activities by subjecting service providers to AML and CFT regulations.

Contrary to what is often assumed, serious companies in the industry are looking for such a regulated environment. Therefore, the new roles and requirements regarding service providers within the TVTG create a support network for entrepreneurs seeing to become TT service providers, with the help of friendly


TT keys (private key)
a key that allows for
disposal over tokens
TT identifier (public key)
an identifier that allows for
dear assignment of Tokens

regulatory oversight. It can be assumed that the legal certainty created by the TVTG will spur companies from various sectors to consider enteringthe market, which will, in turn, tend to lead to a growth in competition. From a client perspective and for the Liechtenstein financial market as a whole, a healthy competitive situation is very positive and can be assessed as advantageous.

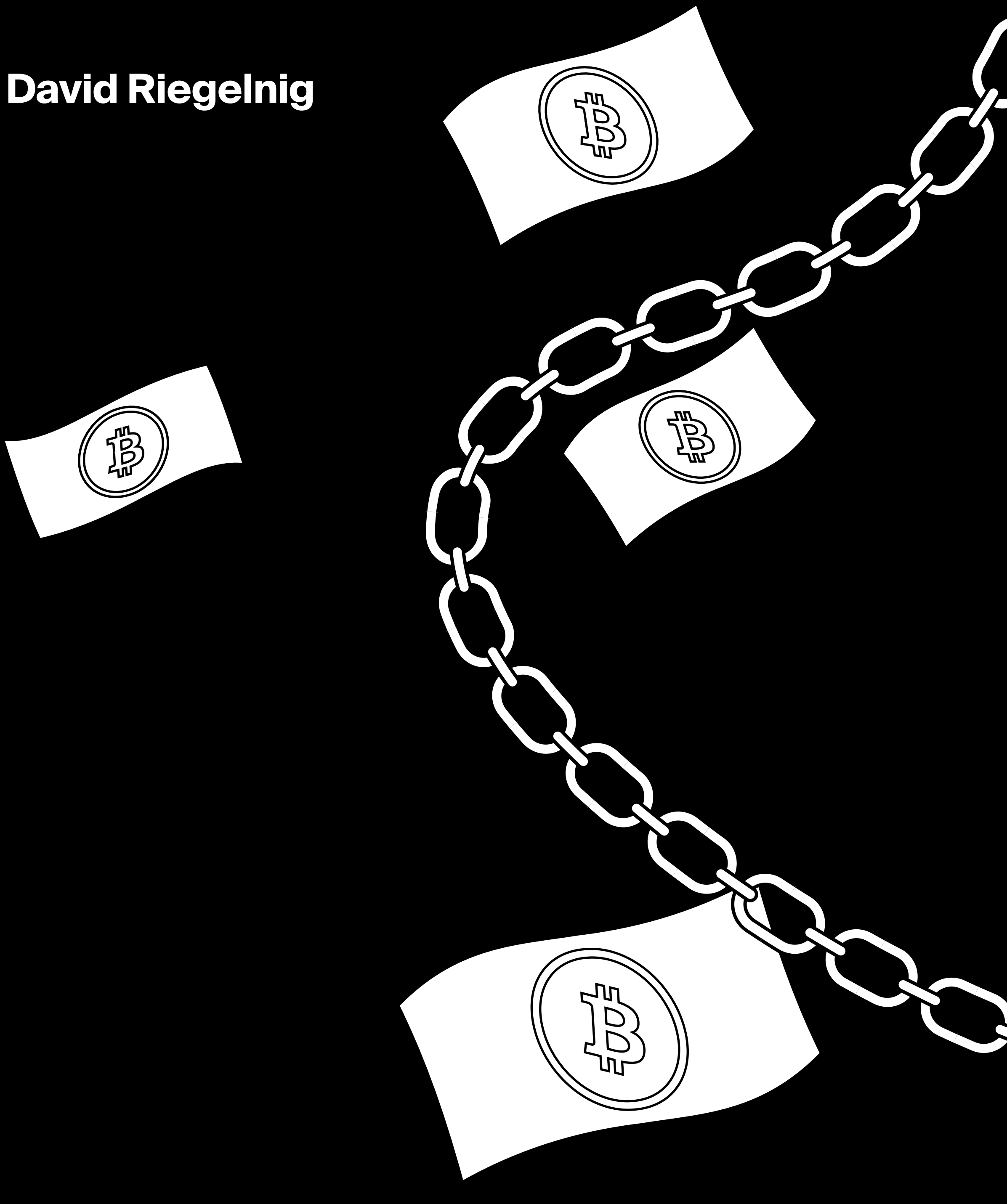
Furthermore, the legislation affords consumers a basis for trusting in these new technologies that was not necessarily present before and facilitates the customers' search for suitable partners within the token economy. It can be expected that the law and the associated legal certainty will lead to Liechtenstein gaining in importance as a fintech and blockchain location for entrepreneurs and consequently allowing the location to benefit from new market participants. In addition, regulation discourages dubious market participants, which proactively minimizes reputational risks.

Ultimately, taking into consideration Liechtenstein's reputation as a financial center, the country is well-suited to provide all the services necessary to enable token-based projects to flourish. For example, Liechtenstein's membership in the European Economic Area allows for the passporting of certain licenses and services to Europe as a whole, affording entrepreneurs access to the European single market. Although this passport ability does not include the registration requirements that are specific to the TVTG, it is the hope that this model will give way to a European-wide framework of a similar spirit. In fact, the structure and spirit of the TVTG already serves as inspiration for other jurisdictions, even those outside of Europe.

Only time will tell what the ultimate effect of this legislation is, but it is clear that the prospects are bright, and the blockchain community here looks forward to inviting more innovators to Liechtenstein to drive change that will undoubtedly be felt on a global scale.

The Travel Rule – Crypto Meets Global Regulation

Written by David Riegelnig



In 2020, most jurisdictions will introduce the obligation for financial intermediaries to exchange customer data when transferring cryptocurrencies on behalf of their clients. The so-called "travel rule" is part of the global regulation against money-laundering. What has been standard to traditional payments for a long time, poses a challenge to the crypto-financial industry.

In the first few years after the Bitcoin white paper was published, hardly anyone imagined what a store of value it would become, nor the potential of cryptocurrencies to rival traditional payments. 'Be careful what you wish for', comes to mind when thinking about the regulatory attention the crypto space receives nowadays.

The Travel Rule for Cryptocurrencies

Last June, the Financial Action Task Force (FATF) issued new requirements for cryptocurrencies to combat money laundering and terrorism financing. The 37 member countries are expected to adopt these regulatory rules within one year.

The influential intergovernmental organization has had cryptocurrencies on its radar for quite a while. Last year, it started to include "virtual assets" in the regulatory framework and introduced the term "virtual asset service provider" (VASP, see box).

Yet the implementation of some of the most recent guidance is a challenge for the crypto-financial industry.

This is particularly true for Recommendation 16, often referred to as "travel rule". It requires any VASP to obtain, hold, and transmit originator and beneficiary information when transferring virtual assets to or from another VASP on behalf of their clients.

Under the new guidance, the sending customer's name, address and account number must be transmitted as well as the name and account number of the recipient.

Not a new idea

The travel rule is not a new invention. For most countries, it has been part of the regulation on wire transfers at least since the 1990s.

What is a Virtual Asset Service Provider (VASP)?

Any natural or legal person who (...) as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- **exchange between virtual assets and fiat currencies**
- **exchange between one or more forms of virtual assets**
- **transfer of virtual assets**
- **safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets**
- **participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset**

From a regulatory perspective, applying the rule to cryptocurrencies is therefore seen as leveling the playing field between different funds transfer systems.

However, contrary to traditional wire transfers, the rule requires an additional exchange of information that is per se not necessary for blockchain-based transactions. The need for industry participants to agree on standards for such an additional information layer is what makes the requirement difficult.

Peer-to-peer transactions are not affected

Unlike traditional wire transfers, cryptocurrencies are often (or even typically) transferred between parties that are not financial intermediaries or VASPs. These peer-to-peer transfers remain out of scope.

The unequal treatment of transfers among intermediaries versus peer-to-peer transactions has been criticized. It was argued that the travel rule in its current form will be not effective to combat criminal activity, instead putting a burden on the crypto-financial industry. However, service providers which are active in the space will have no alternative but to adhere to the rule.

Possible solutions

Implementing the travel rule is not as easy as it first seems. Imagine you as a VASP receive the instruction from a client to transfer 10 Bitcoin to an unknown blockchain address. How do you know whether the destination address is controlled by another VASP, which triggers the obligation to send originator and beneficiary information? If this can be determined, how is the information transmitted and in what format? What happens if the client refers to the wrong VASP by mistake or even on purpose? Finally, how can it be assured that client data is protected along the way?

Different solutions are currently being discussed by the VASP community. Initial ideas where suggesting centralized approaches, such as global registration of addresses controlled by VASPs, which would obviously undermine the benefits arising from the blockchain. Increasingly, the discussion focuses on decentralized and open protocols. Some ideas suggest the usage of blockchain.

In a recent blog post, Andy Bryant from bitFlyer summarized the different technical solutions across two dimensions: Firstly, whether it follows a centralized or decentralized approach, and secondly whether the solution utilizes a blockchain or not.[1]

	Non-Blockchain	**Blockchain**
Centralized	Centralized Database Swift-like network	Inter-VASP network Permissioned Ledgers
Decentralized	Off-chain certificate authorities Point-to-point tunnels	Decentralized Trust Networks Cooperative digital storage and data retrieval tool

[1] https://www.andybryant.me/blog/2019/9/25/using-instant-messenger-to-explain-the-fatf-travel-rule-fornbspvasps

Implications

Irrespective of the way it is implemented, the travel rule will have an impact on the crypto-financial ecosystem. For a VASP, compliance will be less costly when receiving cryptocurrencies from another VASP, together with the mandated originator information, than obtaining the necessary background on a transaction made from the customer's private wallet.

For this reason, there are concerns that VASPs might prefer transactions from other VASPs to the extent that it will weaken the peer-to-peer nature of cryptocurrencies.

On a more positive note, the travel rule does address the most important regulatory concerns about cryptocurrencies: their usage in money-laundering and to evade sanctions.

Even though the fear of illicit transactions is often exaggerated – blockchain compliance company Chainalysis reports that they accounted for less than 1% of all Bitcoin activity in 2019[2] – such allegations hinder further acceptance.

Therefore, while the travel rule is a significant burden to those active in the space, it will at least place cryptocurrencies on more equal footing with traditional payment systems. One less excuse for delaying adoption.

OpenVASP

Bitcoin Suisse has proposed an open standard to facilitate compliance with the travel rule for virtual assets. Called OpenVASP, the protocol is designed to:

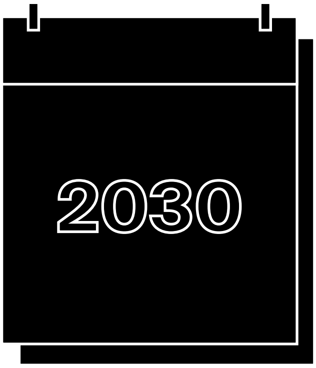
- **pursue a decentralized approach without the usage of a central component**
- **work with any blockchain or distributed ledger technology (DLT) used for the underlying virtual asset transfer**
- **put privacy of transferred data at the center of its design**

More information can be found on the initiative's website: www.openvasp.org

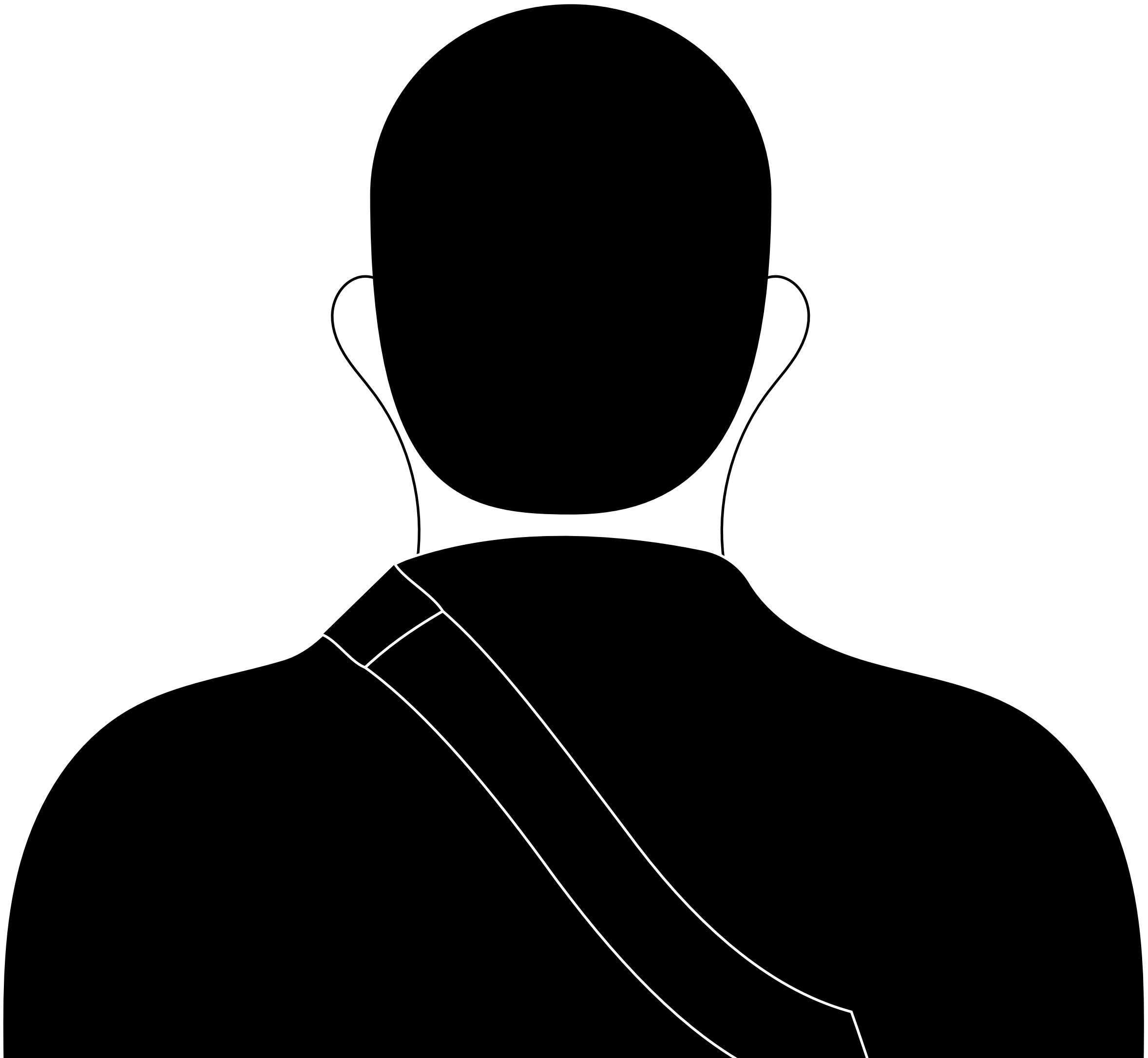
[2] https://www.bloomberg.com/news/articles/2019-07-01/bitcoin-criminals-set-to-spend-1-billion-on-dark-web-this-year

ARTICLE

A Day in the Life of an Asset Manager... in the Summer of



Written by Mona El Isa



It's 19th June 2030. Sam pours herself a cup of coffee and starts to think about the day ahead. She checks to see if there have been any market developments since she left work yesterday. There were some breathless headlines overnight as BTC's recent bull run took it through the $100,000 level, apparently in anticipation of the UK abandoning its fiat currency altogether following the recent, successful example of the Swiss. This was widely expected and hardly noteworthy in her opinion. News wise we were in the quiet summer lull.

She opens her Melon terminal to check her firm's client dashboard. It makes for more interesting reading. She clicks on Cent's Melon page to see who is the most tipped investment writer of the last 24 hours. The first indicator she looked at was her favorite Santiment's 'Crowd Bias Index', an algorithm which tracks mentions of 'buy', 'bought, 'bounce' and similar bullish keywords on crypto social media channels, and recently had a solid track record for gauging crypto sentiment and signaling trend reversals. The index had been making all-time highs in the past few days and typically was a sign of impending sell-offs (ironically, overwhelming crowd bullishness is often a profoundly bearish signal). It reminded her a bit of Bloomberg's "Fear and Greed" index back in the day. Bloomberg, Reuters…she was once so dependent on these tools, almost completely replaced by crypto data sources like Messari and Santiment today. The firm she founded almost exactly around the same time she stopped using Bloomberg ten years ago now manages $50bn in client assets and counts pension funds, university endowments and insurance funds as her clients.

Her firm runs a range of different strategies, all using tokens and all enabled by blockchain technology. She checks in to the Melon Monitoring tool and recalls when she first read about Avantgarde Finance building this tool, which levered a combination of the Melon protocol and the graph protocol to build an on-chain reporting tool for funds, something that she found mind-boggling at the time. She checked her asset managers' league ranking only to find that her flagship smart-contract insurance fund is now in the top 50 worldwide. Yesterday was the end of the quarter, performance and management fees should now be deposited in the fund's wallet. She reminisces back to how complicated quarter ends used to be - so much time wasted on paperwork and briefing investors. Today things are so transparent and fully automated. She remembers how people laughed at her in 2020 when she pitched her idea for the first smart-contract insurance fund underwriting insurance premiums on slashing risk that delegators on staking networks are exposed to when using the Unslashed network. It had been so hard to convince people to take her seriously ten years ago. She scrolled down the rankings to see that the Axiezen fund had leapt from 7th in the rankings to 3rd due to a phenomenal month. She was glad to see them doing so well given they'd also had a tough start getting anyone to buy into the idea of a crypto collectibles fund on Melon back in 2020. She clicked into their monthly on-chain report to see what had led to this high performance. Axozen's strong performance seemed to be attributed to a combination of virtual reality land plots from Decentraland getting a lot of hype after a famous rap-artist mentioned he was going to bid for it. In the end, she never did find those investors. She launched her fund with her own savings, leveraging the Melon protocol, the cheapest and easiest way to set up a fund on-chain. At the time of her launch (2020), the Melon ecosystem was running the first ever Crypto Fund Manager competition. The prize pool was close to $1 million in 2020 for the best performing on-chain 12 month track records. Today, that prize pool is closer to $100 million and is structured in the form of seed capital by some of the largest for-profit Decentralized Autonomous Organisations (DAOs) who sponsor the annual tournament (including some of the pioneers in the field like the Da0, Moloch and Unidao). She really had been lucky to see all of this so early. Over time, continued steady on-chain provable performance attracted investors and clients, enabling her to set up and run her firm today.

She pulls up various charts on her Melon terminal showing the fund's recent transactions, current portfolio allocation vs peers, investor flows and performance attribution data and wonders if recent team hires have damaged the team's balance. She now takes a look at how her other funds are doing. Her second best performing fund Melonai has also been crushing it. She's been crowdsourcing data from open information marketplace Erasure Bay and using it for her own on-chain portfolio.

Suddenly she's distracted by a screen alert she receives, informing her that the verification process for a new customer has just started. She clicks the alert and watches as, over the next few seconds the Melon protocol goes through its paces: first verifying the client's eligibility and digital identity using Iden3's latest screening tools.

The client is now onboarded and she watches as the tool helps recommend fund investments of interest, helps configure the client's risk tolerance, desired account restrictions (no exposure to sub-investment grade corporate bonds, no portfolio duration greater than 2.5 years) and willingness to give two weeks notice before redemption.

By the time of her next sip, the client is onboarded and invested. When she started in the business twenty years ago, it took months and required huge overheads to maintain the staff required to manage the client on-boarding process. Now it takes seconds and costs virtually nothing. She finishes her coffee, shuts down her terminal and makes her way to the centre of town. Today is the Melon Council DAO meeting, one of the most important events of the year. She was recently nominated by some of the fund managers to represent the network's users and she's feeling pretty excited as this is her first meeting as a member of the DAO. The Melon network now secures $4 trillion in crypto assets under management (5% of the world's total asset management industry and growing fast) and counts 50,000 users. The hot topics this year will be an analysis of trading volumes on all the decentralised exchanges (DEXs); the Council is debating whether to continue maintaining all 20 or focus on the 80-20 rule; 80% of the volume comes from 20% of the exchanges. Another big issue is inflation - now that the ecosystem has matured substantially, there is a user-led movement to reduce gas fees on the network. And also there'll be the latest review of projects applying to the Melon Council DAO for funding. Who would have thought back then that a16z, Placeholder, Dragonfly, Fenbushi, Bitcoin Suisse and Blackrock would all be sitting on the Melon Council DAO 10 years ago. She takes her notes, grabs her Aragon DAO voting key and runs to catch the elevator so that she's not late.

Outlook 2020

Okay, so I got a little bit carried away with my 2030 outlook. But none of this is as far away as some of you might think. The building blocks to asset management 3.0 are all being built right now. The Melon Protocol, the underlying infrastructure for on-chain asset management, was released to the Ethereum main-net in March 2019, it now has four projects building tools and applications on top of it, and a growing user base - currently 144 active funds and nearly a quarter of a million USD's worth of assets under management, with many more funds planning to come on line in 2020.

I think 2020 will be a critical year for crypto. Let me explain why. Normally, the market takes care of pricing things correctly. At the moment, however, this doesn't seem to be the case with crypto. Some really economically sound token models are significantly (in my opinion) underpriced, while other questionable token models (and products) are massively overpriced, with prices over emphasising the value of the network. Frankly, I think that's down to data, or the lack thereof, but I'll return to that later. The reality is that current token prices tell us virtually nothing - partly because there is hardly any liquidity and partly because it's too early to see usage pick up. In fact, current token prices are giving us negative information. One of my favourite examples is there are two DEXs (which I won't name): DEX A and DEX B. DEX B trades more daily average volume and has a more sensible token model. DEX A's market cap is more than six times higher.

> **"The building blocks to asset management 3.0 are all being built right now."**

The bad news is that this mis-pricing combined with some of the more questionable token models may be the death of some very good projects and teams in 2020 that are dependent on their token model for sustainability until the usage picks up. There's not much that can be done about bad token models, except iterating on models. This is happening in some cases; sometimes token models are getting better, sometimes it seems they're actually getting worse. The best of the models will probably find a way to reflect usage of a network into the value of a token without compromising network integrity or stakeholders' interests. But 2020 could be the year that a lot of really promising projects fall by the wayside.

The good news is that the same risks described above also provide fantastic opportunities. The projects that do survive will be very well placed for the next decade. From where I'm sitting there have never been more alpha generating opportunities for the taking. My outlook for 2020 will be that smarter investors will start to get involved and bring valuations to more rational levels. And for those who want to be part of the first wave of on-chain asset management pioneers and do it publicly, transparently and with full fund automation, on-chain price record and integration with DEXs - there's always Melon. But how do we get from here, where the foundations of asset management 3.0 are being built but still a little shaky, to the fully decentralised, democratised, and frankly more efficient world of on-chain asset management I describe above?

What I'm advocating is nothing short of system change - we need (good) projects to flourish and for this we need not only greater demand, but also the right enabling conditions, favourable legal and regulatory frameworks and new kinds of institutions and networks. Here are the key elements we need to start putting into place in 2020:

Driving demand

Increasing adoption levels will be essential, especially in 2020. This means raising awareness of the benefits of on-chain asset management, showcasing good use-cases and ensuring that the technology is as safe and easy to use as possible. Adoption can also be encouraged via the right incentives. To that end, we'll be making a very exciting announcement in 2020 - stay tuned!

Funding projects to scale

Increasingly, more and more projects from the 2017 ICO wave are delivering on their promise from a tech-perspective, hitting main-net as promised. However, it is now time for those same projects to focus on driving usage on the networks. By funding solid token projects to accelerate UX/UI improvements, educate users and spread usage through distribution channels, investors can really help bridge the funding gap and earn attractive investment upside, as token values increase in line with greater adoption (this will be the case with well thought out token models).

Data, Data, Data

The devil is in the data. One of the reasons why some projects are under/over valued is useless metrics being given too much weight - e.g. exchange listings, daily trading volume, venture funds invested etc. We also need a better way of assessing what projects have done versus what they have promised (signal vs noise), much better token modelling, comparison metrics and valuation frameworks. Most investors today invest after they've seen the traction and are too afraid to take a view on where the traction is coming from next. This is why projects like Messari are so important to the ecosystem.

New regulatory frameworks

Regulations for the off-chain world are not fit for purpose for decentralised finance. Decentralised technologies make some risks negligible (e.g. custody, risk management, fraud, embezzlement, delivery vs payment etc.). However, traditional law was designed on the assumption that technology could not mitigate or eradicate these risks - this needs to change. In particular, regulators need to consider accepting smart contracts in place of financial intermediaries.

Safe spaces for experimentation and innovation

We need to be able to test things in practice but in a way which both protects investors, and engages regulators. The best way to do this is through regulatory sandboxes. We would urge regulators to provide more opportunities for such sandboxes and hope to test use cases in this way in 2020.

Networks and organisations to champion on-chain asset management.

It's essential in such a fast paced yet relatively new field, that we have champions to raise awareness about the benefits of blockchain technology, work with regulators and grow the DeFi community. That's why in 2017, we helped set up the Multichain Asset Managers Association (MAMA) to carry out projects, organise events and strengthen the community to help bring about a more appropriate regulatory regime for on-chain asset management. In 2020, MAMA, now at 60 members, will be bringing the first live use-case of Melon into a fully regulated environment, publishing a manifesto and leading initiatives at Oxford University, the University of Basel and the Frankfurt School Blockchain Center.

Culture

If we want the field to grow and mature, we will also need to work together. This requires openness, transparency and spaces for collaboration. That's why we organise an annual on-chain asset management conference to bring ecosystem participants together: the first ever, M-0, was held in Zug. Its success was followed by M-1 (also in Zug) and the next (M-2) will be held at Oxford University in 2020.

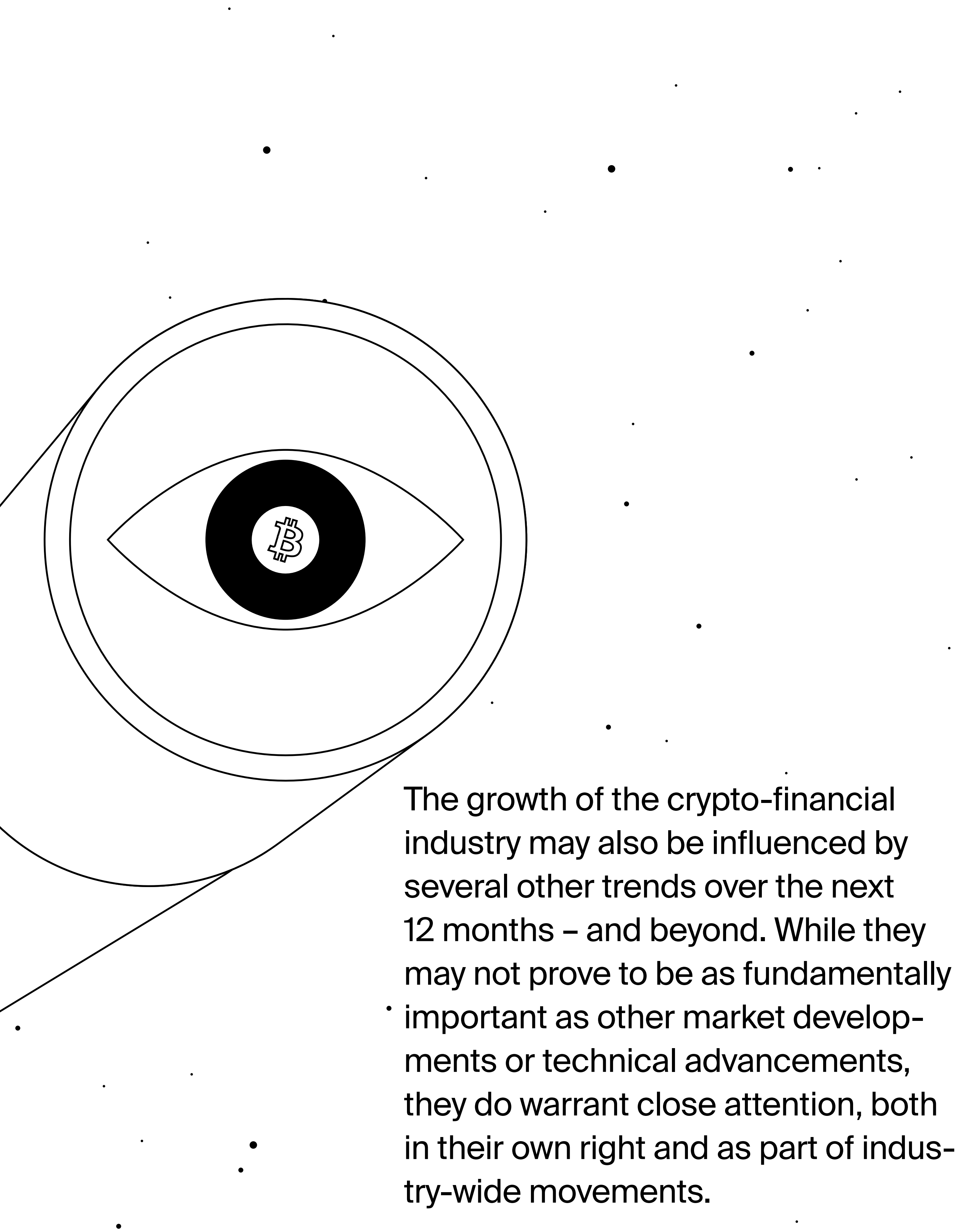
And if we do all of this, where do we get to?

The ultimate prize is truly democratized asset management. Generally speaking, the entire investment industry has suffered for far too long as a result of high barriers to entry. This means that once you pass a certain threshold of size, you no longer have to be too concerned about performance because investors usually care about size first. Institutional investors are highly unlikely to back anyone with less than $200m AUM and less than a 2 year audited track record. Since the cost of survival beyond a year is typically about 200m AUM - this creates a chicken and egg situation and may explain why discretionary managed investment products struggle to outperform passive investments.

The idea that anyone, anywhere, regardless of background, age and education can now set up an on-chain investment fund, with a fully transparent performance track record over time, with close to no capital is staggering. By having large, sponsored prize pools associated with this effort, we can imagine a whole range of exciting nascent web3 investment products becoming available, coupled with talented managers building those projects. What we're really excited about is being able to unlock the talent that has been hidden in the shadows for far too long and seeing it breathe a little freshness into some of the complacency we see in investing today.

Other Trends to Watch

Written by Ian Simpson



The growth of the crypto-financial industry may also be influenced by several other trends over the next 12 months – and beyond. While they may not prove to be as fundamentally important as other market developments or technical advancements, they do warrant close attention, both in their own right and as part of industry-wide movements.

Interoperability Between Blockchains

Much like in the early days of the internet, the landscape of blockchain protocols and the cryptocurrencies which help power them is still largely fragmented. Bitcoin and Ethereum as well as a handful of other chains have developed into relatively stable ecosystems – each as a walled garden in and of itself.[1]

This conundrum, whereby the technology of Web3 has been faced with the same challenges as that of Web2, poses a serious challenge to the further adoption of blockchain technology. According to Gartner, it is precisely this lack of interoperability standards that stands in the way of "pervasive blockchain deployment across financial services ecosystems."[2]

But there are major efforts underway to address this problem. One of the more ambitious and well-known interoperability blockchains is Polkadot, the brain-child of Ethereum Co-Founder Dr. Gavin Wood. Much like Cosmos, another one of the more established projects in the space, Polkadot addresses the interoperability challenge by creating a multi-chain by means of several so-called "parachains" which are connected to each other, as well as "bridges" to link to external chains.

With the support of the Web3 Foundation as well as a number of high-profile investors, Polkadot is aiming to launch its live network in early 2020.[3]

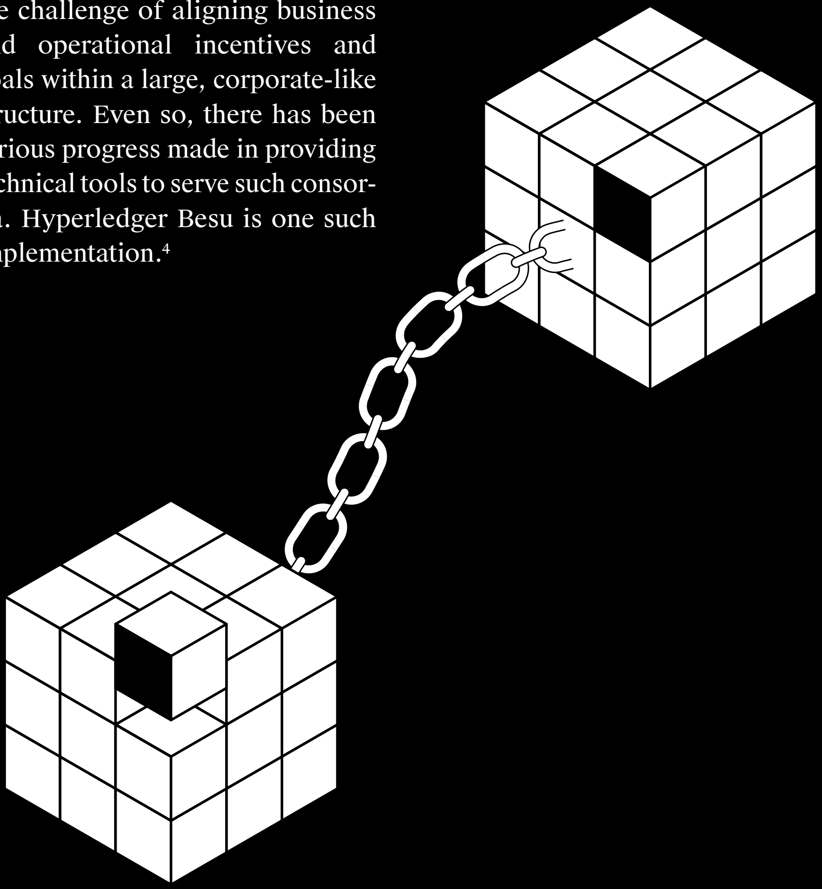
The burning question for it and other interoperability chains is whether such fundamental infrastructure will indeed lead to a broad acceptance of blockchain as a base-layer technology for critical industries such as finance, healthcare, and supply chain management. In these cases, the need to preserve confidentiality has placed an emphasis on private blockchain implementations which may or may not play well with the broader, "world-wide web" of blockchains. At the same time, these industries are large enough (and international enough) to make it difficult to imagine a single blockchain that will meet the needs of all stakeholders in every location and every situation.

Some have tried to pursue the consortium model to build a cross-business or -industry consensus and promote standards. The Enterprise Ethereum Alliance is one such group, while Hyperledger, with IBM as a major contributor, forms another.

This would seem to be the less efficient approach, however, given the challenge of aligning business and operational incentives and goals within a large, corporate-like structure. Even so, there has been serious progress made in providing technical tools to serve such consortia. Hyperledger Besu is one such implementation.[4]

Ultimately, the challenge of ushering in a (near) universal standard for Web3 applications and technology will likely be a market-driven decision with a winner chosen by those who find it easiest to use and most aligned with their needs.

The year 2020 may well see the first baby steps in the development of a wider, more inter-connected blockchain "web" – but it will likely be some time before we see a robust ecosystem without walls emerge.



[1] https://consensys.net/research/avoiding-blockchain-balkanization/
[2] https://www.gartner.com/en/newsroom/press-releases/09-16-2019-gartner-says-blockchain-deployments-across-financial-services-ecosystems-are-at-least-three-years-away
[3] https://medium.com/polkadot-network/polkadot-the-foundation-of-a-new-internet-e8800ec81c7
[4] https://wiki.hyperledger.org/display/BESU/Hyperledger+Besu

Stablecoins

When viewed through the prism of relative cryptocurrency price volatility, the appeal of stablecoins is easy to understand. This past year has seen a rise in their popularity and increased discussion around their usefulness, especially since the announcement of the Facebook-backed Libra project in July. Some of Europe's top institutions have weighed in on the topic of stablecoins,[5] with the European Central Bank issuing a report on the subject and the Swiss regulator FINMA releasing guidelines on their treatment.[6]

In general, stablecoins do not generally seem to offer a compelling investment case since their value is, by nature, pegged to some other currency or asset. They can, however, play a role in decentralized finance systems, with one of the more popular stablecoins, DAI, being the result of one of the most advanced DeFi setups developed to date. Stablecoins also have the potential to facilitate blockchain-based applications where a common, stable digital currency is needed for interactions with the app's smart contract layer.[7] This provides reason to believe that the market for stablecoins will continue to increase.

In addition, macroeconomic forces point to greater interest in a stable crypto-like currency. China recently made known its interest in developing a nation-wide digital currency,[8] a fact which some believe will spur acceptance of the Libra project by US and European regulators. The Swiss National Bank (SNB), in cooperation with the Bank of International Settlement (BIS), has indicated that it will explore the same idea, with a mind to integrate it into DLT infrastructure.[9] If these two initiatives, among others, were to move forward significantly over the coming year, it could have a strong influence over other crypto trends, in particular tokenization and decentralized finance.

Tokenization

As one of the most popular buzzwords associated with blockchain technology, the concept of tokenization is often misunderstood.

Simply defined, tokenization is the process of assigning the rights to and attributes of an asset to a digital token which lives on the blockchain. The explosion of Ethereum-based tokens issued in initial coin offerings in 2017 drew widespread attention to the concept of tokenization in various form; it also inspired regulatory efforts to classify tokens and make legal sense of them. In Switzerland, FINMA has outlined three main token types: utility, payment and asset.[10]

Over the last year, the excitement over utility tokens – those used to confer access or usage rights to an application or protocol - has generally subsided. However, a second generation of utility tokens may become more relevant in the future: Corporate utility tokens issued by companies for such use cases as loyalty and referral programs. One such token will be issued by Emaar, the Middle East's largest real estate and property development company.[11] Tokenizing such loyalty and referral programs has the potential to reduce friction costs and improve accessibility.

Today, interest in tokenization is also focused in large part on the possibilities of so-called asset tokens, which may represent the partial ownership in a real estate property, revenue-sharing rights in a collective investment scheme or any other of a myriad of possibilities. Tokenized equity for the shares of small- and medium-sized businesses and tokenized corporate debt is also a hot topic.

Problems, however, arise because there is no universally accepted standard for the legal treatment of the many and varied asset token propositions being explored in different countries. There is also limited market infrastructure for trading and storing them, not to mention service providers who may legally deal in such tokenized securities.

It is also questionable whether the more exotic use cases for asset-backed tokens, such as tokenized collectibles, wine and art, offer a sufficiently strong value proposition for them to be widely accepted.

Nevertheless, the market infrastructure which may eventually open up the possibility of tokenized equity and debt continues to develop - albeit slowly and sometimes by fits and starts. Despite having launched a prototype of its digital exchange, SDX Chairman Thomas Zeeb recently admitted that the development may be somewhat too early for the banks which are financing the project.[12] Meanwhile, a proof-of-concept for the settling of tokenized shares coordinated in cooperation between Swisscom, Deutsche Börse and three Swiss banks was successfully completed.[13]

These advancements provide reason to believe that if tokenization is to truly take off, it may well get its first boost from Switzerland. The only doubt is whether there will be enough demand from investors and those tokenizing assets to sustain the innovation in the long-term.

[5] https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf
[6] https://finma.ch/en/news/2019/09/20190911-mm-stable-coins/
[7] https://www.bitcoinsuisse.com/research/decrypt/stablecoins-navigating-crypto-volatility
[8] https://fortune.com/2019/11/01/china-digital-currency-libra-wakeup-call-us/
[9] https://www.bis.org/press/p191008.htm

Crypto Payments

The ability to pay for everyday items with cryptocurrencies has long been seen as a barometer for the level of crypto asset adoption. As it was originally styled to be a "peer-to-peer electronic cash system," Bitcoin was expected to provide a universal medium of exchange to pay for anything and everything.

Today, that goal remains only partially realized at best. As the price of Bitcoin and other crypto assets took off in late 2017, transaction fees also rose dramatically, making it less attractive to use them as a day-to-day medium of exchange. The lack of universal infrastructure for accepting crypto payments, as well as regulatory uncertainty in some countries have also factored into the low adoption rate of crypto payments.

Despite these mixed results, it is important to watch the crypto payments space, both on a retail and institutional level. Payment providers are increasingly aware that consumers value the opportunity to pay in a variety of ways, meaning that all options (including paying with crypto) should be made available.

Worldline, Europe's largest payment system provider, confirmed this fact in announcing its partnership with Bitcoin Suisse to integrate crypto payments into its point-of-sale terminals and in online shopping. Facebook's Libra project has put a focus on the ability to execute cross-border retail payments seamlessly, something that cryptocurrencies can and should play a central role in.

At the institutional and international level, there is growing interest in developing cryptocurrency-like payment systems, such as the one proposed by BRICS[14] or the solution being explored by the Monetary Authority of Singapore and JP-Morgan for cross-border payment and settlement.[15] In these cases and others like them, process efficiency seems to main focus, rather than decentralization of finance. Whether there are any long-term benefits remains to be seen.

Beyond supporting payments for goods and services in order to realize Satoshi's original vision of peer-to-peer electronic cash, increased usage (and transactions) of cryptocurrencies payments is key for another reason. The transaction fee paid by those transacting plays a significant role in the overall network security by incentivizing miners. As the Bitcoin block reward continues to shrink, this will be more and more important, since these transaction fees can help guarantee the security of the system.

If second-layer solutions and other technical integrations advance over the next year, bringing crypto payments to shops and inter-bank systems as well, then adoption will contribute to an even stronger ecosystem.[16]

[10] https://www.finma.ch/en/documentation/dossier/dossier-fintech/entwicklungen-im-bereich-fintech/
[11] https://www.theblockcrypto.com/linked/43591/owner-of-burj-khalifa-worlds-tallest-building-launching-its-native-token-on-jpmorgans-blockchain
[12] https://www.finews.com/news/english-news/38773-how-banks-hold-back-the-digital-exchange?_ga=2.128259852.1010220954.1574064555-1629039672.1552572799
[13] https://www.swisscom.ch/en/about/news/2019/11/19-wertpapiertransaktionen-mit-tokens.html

Institutional Crypto-financial Products and Services

Throughout the latter part of 2017 and deep into 2018, crypto market watchers repeatedly hailed the arrival of so-called “institutional money.” While a large number of crypto investment funds did spring up and many venture capital firms turned their focus to crypto companies during this time, their numbers were not as significant as imagined[17] and the sharp influx of money from professional investors failed to materialize.

Now, nearly two years on, it is still too early to speak of a sustained wave of investment from institutions. Several factors have contributed to this situation:

- **Lack of regulatory clarity regarding cryptocurrencies**
- **Low level of blockchain and crypto technical understanding**
- **Lack of traditional crypto-based financial products**
- **Fear of potential KYC/AML complications**

Regulatory approval, and in particular, fears of market manipulation, have been a major stumbling block to the approval of crypto exchange-traded-funds (ETFs) in the United States, where, for instance, Bitwise has faced a roller-coaster process trying to gain the SEC’s blessing for its product.[18]

There are, however, other signs that institutional-grade products and services are on the rise. Crypto custody providers are now able to offer banks and asset managers the level of security needed to satisfy their requirements. For a crypto derivatives trading platform such as the Intercontinental Exchange-supported Bakkt this is key. Bakkt’s physically-settled monthly Bitcoin futures contracts, despite their slow start, have steadily increased in popularity – another sign that once the pieces are in place, there is strong potential for institutional crypto products.

In Switzerland, the country’s major stock exchange, SIX, has listed ten crypto-based exchange-traded-products (ETPs) over the last 18 months. At the same time, SIX itself has begun intense development work on its next-generation infrastructure, the SIX Digital Exchange, which has the aim to eventually trade not only cryptocurrency-based traditional financial products, but also an entirely new asset class of tokenized assets.

Mass adoption of crypto ETPs and ETFs may still be a few years away, but 2020 is likely to see more foundational work done, thus preparing the way for more institutional money to flow into the market.

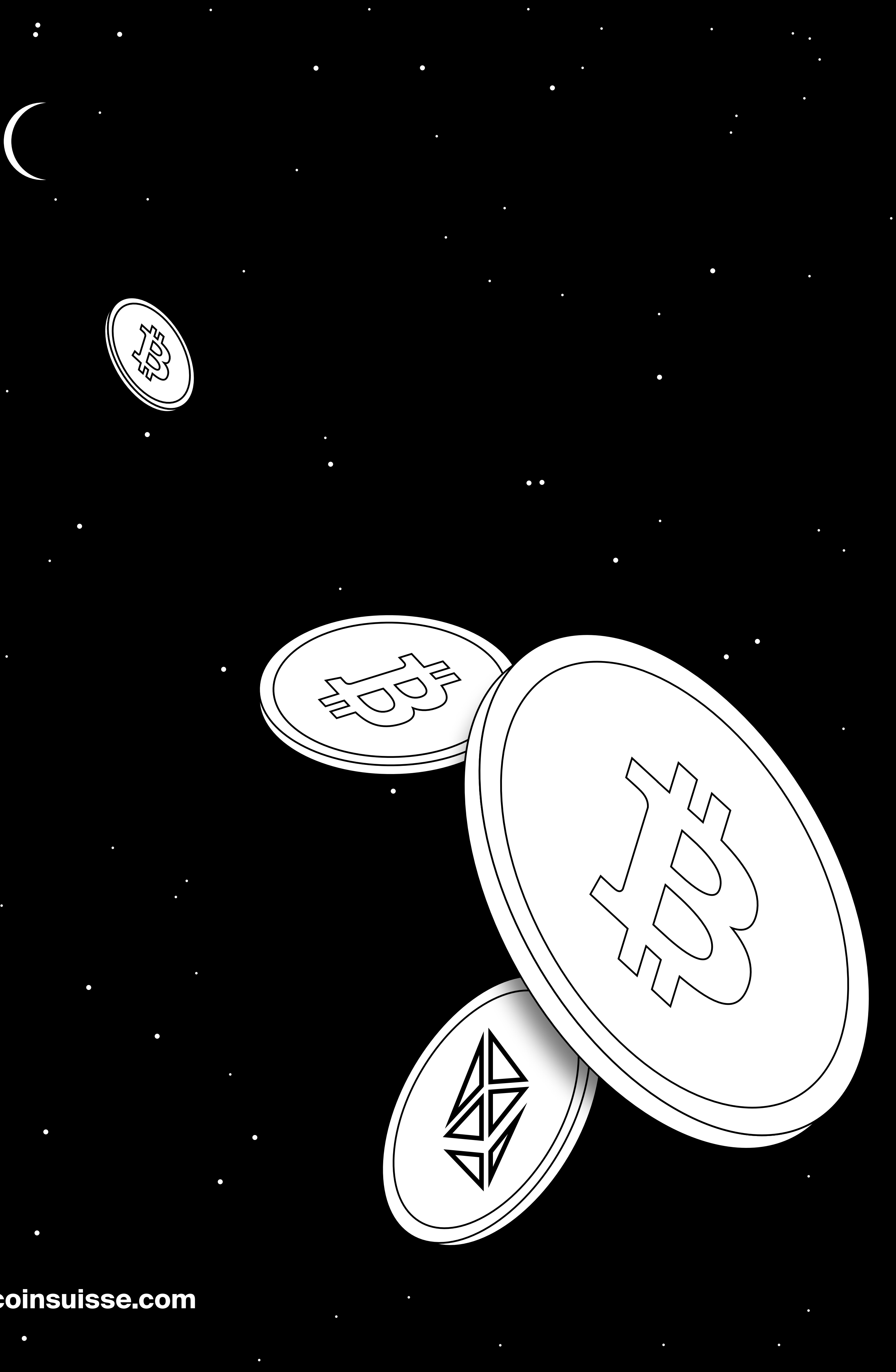
[14] https://www.theblockcrypto.com/post/47230/brics-member-nations-propose-creating-a-cryptocurrency-for-payment-settlements
[15] https://www.theblockcrypto.com/linked/46597/singapores-central-bank-jpmorgan-develop-a-blockchain-system-for-cross-border-payments
[16] https://www.bitcoinsuisse.com/research/decrypt/transaction-fees-markets-for-block-space
[17] https://www.pwc.com/gx/en/financial-services/fintech/assets/pwc-elwood-2019-annual-crypto-hedge-fund-report.pdf
[18] https://www.coindesk.com/what-to-make-of-the-secs-latest-bitcoin-etf-rejection

Bitcoin
Suisse

Bitcoin Suisse AG
CH-6300 Zug
bitcoinsuisse.com

Disclaimer:

The information provided in this document pertaining to Bitcoin Suisse AG and its Group Companies (together "Bitcoin Suisse"), is for general informational purposes only and should not be considered exhaustive and does not imply any elements of a contractual relationship nor any offering. This document does not take into account nor does it provide any tax, legal or investment advice or opinion regarding the specific investment objectives or financial situation of any person. While the information is believed to be accurate and reliable, Bitcoin Suisse and its agents, advisors, directors, officers, employees and shareholders make no representation or warranties, expressed or implied, as to the accuracy of such information and Bitcoin Suisse expressly disclaims any and all liability that may be based on such information or errors or omissions thereof. Bitcoin Suisse reserves the right to amend or replace the information contained herein, in part or entirely, at any time, and undertakes no obligation to provide the recipient with access to the amended information or to notify the recipient hereof. The information provided is not intended for use by or distribution to any individual or legal entity in any jurisdiction or country where such distribution, publication or use would be contrary to the law or regulatory provisions or in which Bitcoin Suisse does not hold the necessary registration or license. Except as otherwise provided by Bitcoin Suisse, it is not allowed to modify, copy, distribute, transmit, display, reproduce, publish, license, or otherwise use any content for resale, distribution, marketing of products, or other commercial uses. Bitcoin Suisse 2020.



bitcoinsuisse.com