

**Crypto**

**2022**

# Outlook

**In-Depth Industry Insights into Markets, Technology and Regulation**



# Intro

## Welcome to Crypto Outlook 2022 – The “all numbers go up” edition



**Dr. Marcus M. Dapp**  
Head of Research

If you hear the words ‘numbers go up’ – what do you think of first: crypto, the coronavirus or the Consumer Price Index?

For the past two years, a roller coaster has gone ‘viral’ and volatile – between disrupted supply chains, rising stock markets seemingly detached from economic fundamentals, quasi-permanent employment disruptions in some sectors, stimulus packages, and money creation. All this has left many of us confused, with a subtle, yet nagging feeling of uncertainty for the future.

Bitcoin Suisse has been built on the strong belief that decentralized digital assets create a net positive for our global society by allowing us to build a financial system on a new foundation that is more resilient against the gyrations mentioned above. We share the view that we need to use the future to build the present and bring the opportunities of the crypto space to the benefit of all, as expressed by President of the Swiss Confederation Ignazio Cassis in the

Preface of this 3rd edition of the Bitcoin Suisse Crypto Outlook Report (c.f. p4).

Comparing and contrasting the traditional and Bitcoin world is one way to discuss the relevant macro trends (c.f. p6). How can we understand Bitcoin’s value proposition in an environment where ‘transitory inflation’ is becoming an untenable thesis? Will Bitcoin survive another blow in the order of the Great Mining Migration out of China? And will El Salvador survive Bitcoin?

The energy debate could be the next blow as it seemingly combines all the critique about Bitcoin into one. Our interview with Alex Gladstein of the Human Rights Foundation takes a deep dive into the ESG debate around Bitcoin and surfaces perspectives and arguments that are often underreported (c.f. p18).

However, there is one vocal contender in the crypto-go-green competition: Ethereum is heading full steam into the “Merger” in 2022, the culmination of its

migration from Proof-of-Work to Proof-of-Stake (c.f. p26) – a change which is touted to make it much less energy intense. However, the complexity of the transition is a real issue.

On top of Ethereum, numbers went up as well. Prof. Fabian Schär, University of Basel, shares his high-level perspective on the unfolding Decentralized Finance space (c.f. p33). His main concerns are regulatory and governance, two areas where he strongly distinguishes between truly decentralized protocols and “decentralization theater.”

Tackling the intermediary question from an institutional perspective, my colleague Ian Simpson from Bitcoin Suisse explores how the evolving crypto-financial tech stack is helping professional investors gain exposure to digital asset markets (c.f. p36).

Last but not least, we have a new section in this Crypto Outlook called “Vires in Numeris”, named after the “trust in numbrs” mantra stemming from the early Bitcoin community. Together with our Trading Desk, we present some of the most illuminating charts of 2021 (c.f. p46), showing quantitatively that it was indeed a year of “all numbers went up” (Almost).

My warmest thanks go out to all guest authors and my colleagues at Bitcoin Suisse for giving their time and sharing their insights, hopes and concerns for crypto for 2022 and beyond.

To all readers, I wish pleasant reading and valuable insights!

*Dr. Marcus M. Dapp*  
*Head of Research*

PS. Bitcoin Suisse Research provides a range of publications on a broad spectrum of topics covering the fast-moving crypto space. If you like this edition of Outlook, please feel free to explore and subscribe to our other publications at [bitcoinsuisse.com/research](https://bitcoinsuisse.com/research).

Impressum  
Bitcoin Suisse AG  
Grafenauweg 12  
6300 Zug  
Switzerland

Bitcoin Suisse (Liechtenstein) AG  
Aeulestrasse 74  
9490 Vaduz  
Liechtenstein

Design & Concept  
Loris Haller

Printing:  
Printoset, Zürich  
Printed in Switzerland

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

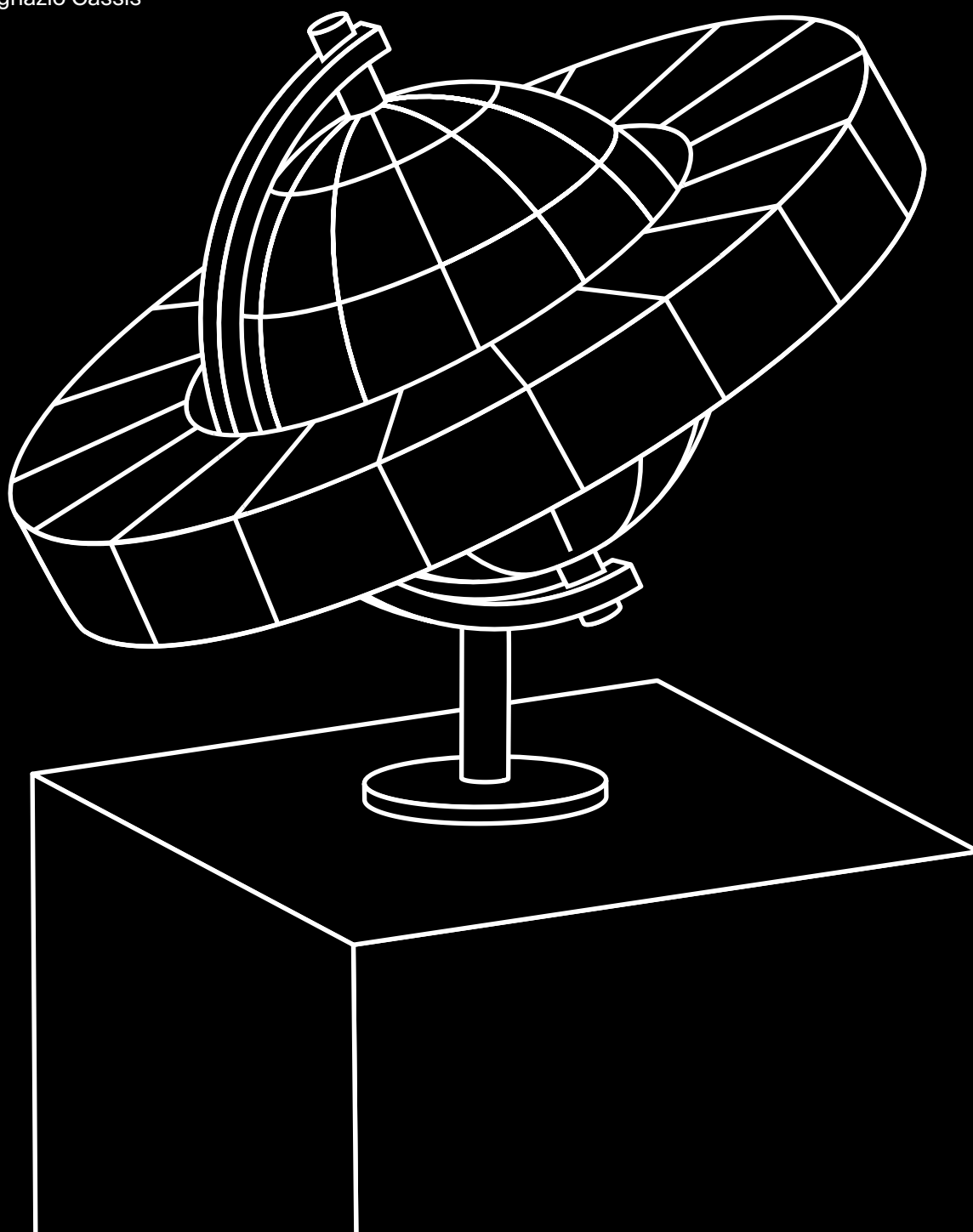
# Contents

<b>President Ignazio Cassis</b> <b>Preface:</b> Building the Future - Now	5
<b>Dr. Marcus Dapp</b> <b>Article:</b> Thinking Beyond 2022	8
<b>Alex Gladstein</b> <b>Interview:</b> Bitcoin, Human Rights, and the ESG debate	18
<b>Dr. Marcus Dapp</b> <b>Article:</b> Ethereum's Long Chain of Forks Towards "The Merge"	26
<b>Prof. Fabian Schär</b> <b>Article:</b> Decentralized Finance: The Road Ahead	33
<b>Ian Simpson</b> <b>Article:</b> From Nodes to New Asset Class - The Evolving Crypto-Financial Tech Stack	36
<b>Spotlight:</b> Protocol Updates and Outlook	42
<b>Bitcoin Suisse Trading Desk</b> <b>Charts:</b> Vires in Numeris	46

Preface

# Building the Future - Now

President Ignazio Cassis



We live in times of unprecedented change and exponential transformation. New technologies and breakthroughs in science are not only changing the economy, but also challenging societies, political systems and the international multilateral order. The rapid development of new technologies has an impact on all our lives and thus on how people organise themselves, how we manufacture things and how we do business together. We cannot predict the future. Like Danish physicist, Niels Bohr, put it: "It is difficult to predict, especially the future." However, even if we cannot predict the future, we can make it possible by anticipating and shaping it.

### **Using the future to build the present**

Every year, Bitcoin Suisse offers a fascinating trend analysis on what is to be expected in the crypto sector in the near future. The Geneva Science Diplomacy Anticipator (GESDA) looks even further ahead. With its vision "Using the future to build the present", the Foundation seeks to understand frontier scientific breakthroughs and leverage them, where appropriate, in the interests of the collective welfare of humanity. What may be in store for us in the next 5, 10 or even 25 years is compiled in the first GESDA Breakthrough Radar<sup>1</sup>, which has recently been published. I highly recommend reading it! What was once confined to the realms of science fiction is much closer today than we might think.

It is no coincidence that GESDA and Bitcoin Suisse are based in Geneva and Zug respectively. Switzerland, as a haven of innovation and a neutral platform for dialogue, is very well positioned not only to anticipate this development, but above all to shape it. With our leading universities and research institutions, a strong financial centre and a regulatory framework conducive to innovation, Switzerland can play an important role in shaping a global environment that addresses the formidable challenges facing our planet.

### **Bringing the opportunities in the crypto space to the benefit of all**

In order to make better use of the potential offered by technological developments, the Swiss Federal Council adopted its first strategy for a digital foreign policy at the end of last year. The strategy identifies four areas of action. One of them is the use of digital technologies to help achieving the Sustainable Development Goals (SDGs) and fulfilling the 2030 Agenda. Digitalisation should never be an end in itself, but rather serve as an enabler and facilitator.

What these developments translated into reality in crypto space look like is demonstrated by the Swiss

Development Cooperation: the SDC uses blockchain technology in order to track legal logging and therefore foster a sustainable timber industry in Peru. At the academic level, the Swiss Embassy in South Africa enabled the establishment of a blockchain Co-Chair between Switzerland and South Africa and organized the Incube Challenge of the ETHZ on blockchain for the first time on the African continent. In addition, the State Secretariat for Economic Affairs (SECO) signed an agreement with the Crypto Valley Venture Capital (CVVC) to support an ecosystem in South Africa with an expertise transfer from the Swiss Crypto Valley.

### **Addressing the challenges to seize the opportunities**

New technologies offer countless opportunities. However, we must not ignore the challenges that come with them. For example, we need to minimise the environmental footprint of new technologies such as blockchain in the future. More research and innovation is needed to ensure that these new technologies support sustainable development.

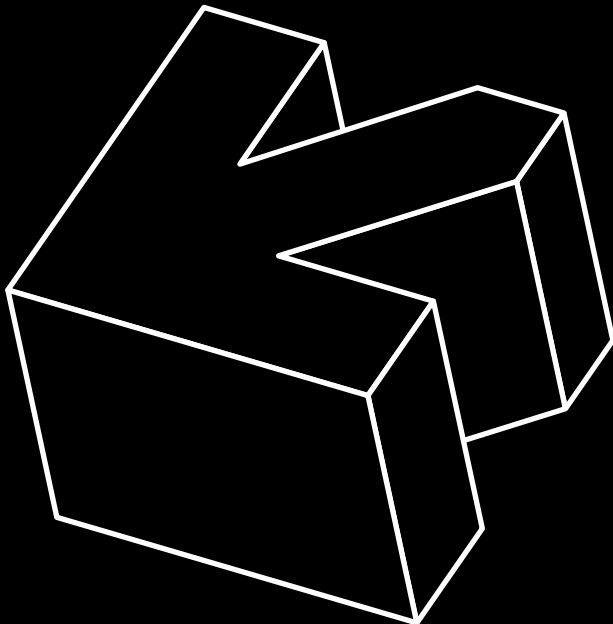
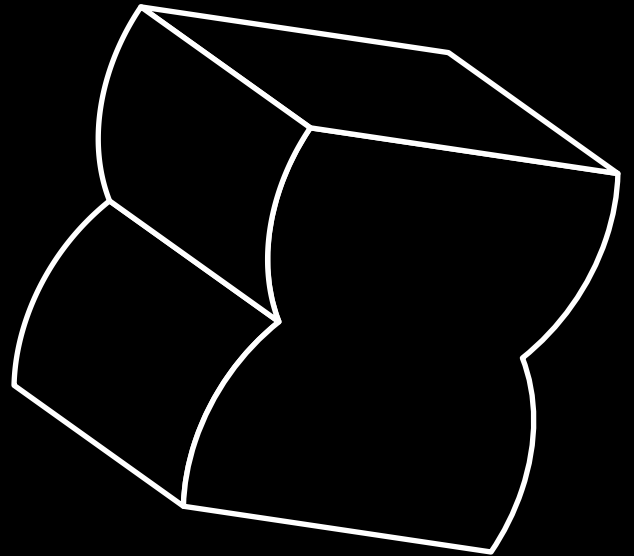
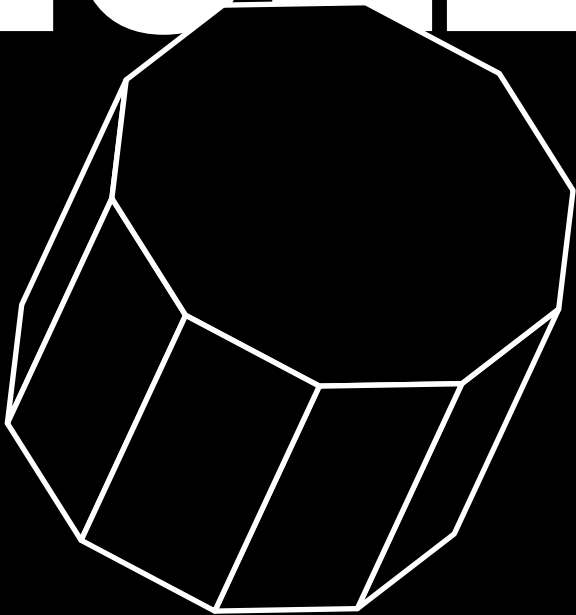
Last but not least, we need to build up new platforms, which shape the global governance of new technologies and the fields of application. In this respect, International Geneva plays a crucial role as it hosts some of the most important international organisations in international governance, which can form a trusted environment for the application of new technologies. So that in the end, we can all benefit from this progress: in Switzerland and around the world.

## **IGNAZIO CASSIS**



Ignazio Cassis is the President of the Swiss Confederation and Switzerland's Foreign Minister. Born in the canton of Ticino, the trained doctor has been a member of the national government since 2017.

# MACRO TRENDS 2022



## Article

# Thinking Beyond 2022 – Macro Trends We See

Dr. Marcus Dapp



**Traditional  
finance and peak  
inflation**

**Fiat money.** In 2021 the “Nixon Shock” had its inglorious 50th year anniversary. Half a century ago, on 15 August 1971, US President Nixon held a speech that ushered in a new monetary era – the era of fiat money. Nixon suspended the convertibility of the US dollar into gold, de facto ending the Bretton Woods agreement that had fixed international exchange rates against a gold-backed US dollar since World War II. With the suspension, Nixon decoupled the US dollar from the pressure to stick to the gold reserves and enabled the government to issue bonds against new currency from the Federal Reserve to address domestic issues like high unemployment. Since then, all major currencies have become free floating fiat currencies and all face similar problems: the amount

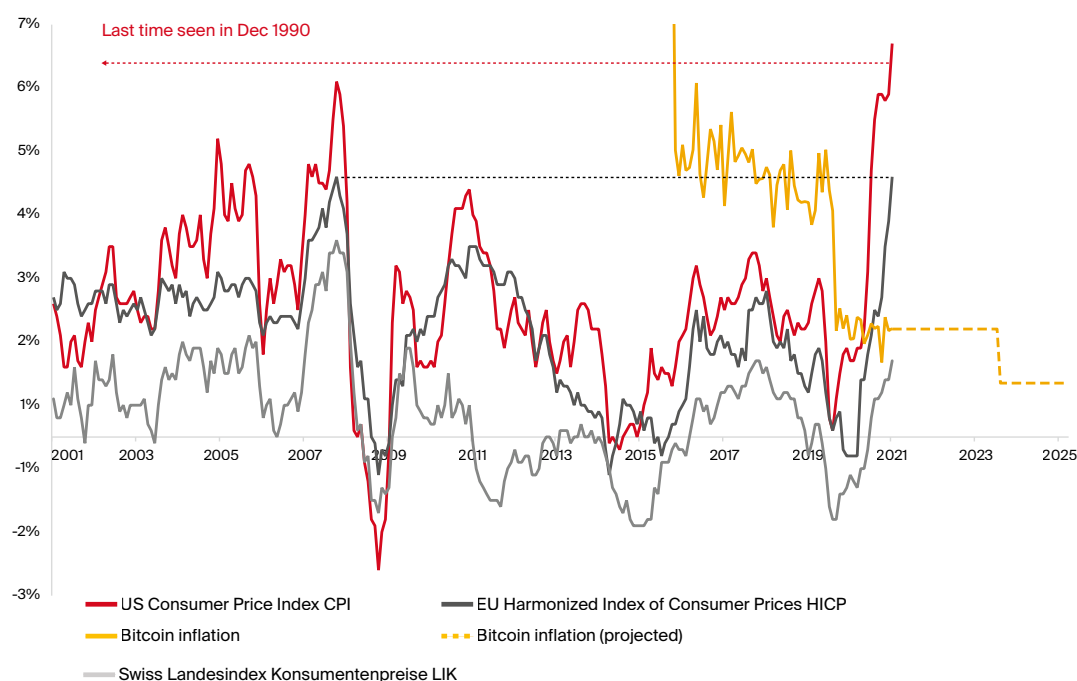
■ Inflation rates, though claimed to be “transitory”, are increasing to new record highs in the US and Europe. Bitcoin reaches new all-time highs against this background putting itself up as a hedge against inflation worries.

■ Two major macro events in 2021 influence the development of Bitcoin in 2022 and beyond. The Great Mining Migration out of China shifted the geopolitical power structure for Bitcoin mining. The step to declare Bitcoin legal tender, catapulted El Salvador onto the global Bitcoin scene and puts subtle pressure on other countries with heavy monetary dependence on the UD Dollar, to get clarity about their national Bitcoin strategy.

■ More sense and sensibility will benefit Bitcoin's sustainability debate greatly in 2022 and beyond. Free, instant, mining-free Bitcoin Lightning payments push the debate beyond energy and show the positive impacts a publicly governed financial system like Bitcoin can have on financial inclusion.



*Illustration 1:  
Monthly inflation  
rates of USA, EU,  
and Switzerland  
2001-2021 (annual-  
ized). Source: FED,  
ECB, SNB, Bitcoin  
Suisse Research*



of money supply is growing over time, leading to high GDP-to-debt ratios and inflated prices in many countries.

**Inflation.** In 2021, the numbers show that inflation rates are surpassing levels last seen at least a decade ago, right before the Great Financial Crisis 2008/2009, and hitting a 30-year peak in the US (illustration 1). The November Financial Stability Report<sup>2</sup> of the Board of Governors of the Federal Reserve System therefore rightly lists “persistent inflation and monetary tightening” as risk #1.

While the Federal Reserve is assuring the public that the inflation rates are “transitory”, they are in fact in a difficult situation. The core of the problem is that fiat money creation is debt creation at the same time. The increase in money supply has also increased the debt of the US (and similar in other regions/nations) as asset purchase programs were paid by the central banks with newly created money. Now, the Fed needs to keep bond yields – the cost for debt – low to protect the government’s debt service. At the same time, the Fed should taper<sup>3</sup>, i.e., reduce Quantitative Easing and maybe increase interest rates, to counter the price pressure coming from inflation.

**“The root problem with conventional currency is all the trust that’s required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.”**

– Satoshi Nakamoto (*The Quotable Satoshi*, [NakamotoInstitute.org](https://nakamotoinstitute.org))

So, which forces will prevail for the 2021/2022 transition? The Fed’s intentions to taper, reduce of quantitative easing and possibly raise interest rates? Or the up-ward price pressure because of the extraordinary money supply increases caused by the Fed in the last 24 months, in addition to the interrupted supply chains and business shut-downs because of COVID restrictions?

## Bitcoin: inflation hedge and payment solution for nations

**Inflation hedge.** Over 2021, major global stock indices moved moderately and performed through the first eleven months in the range 5%-22%, with the negative exceptions of China's Hang Seng (-11%) and gold (-9%). You may wonder, what fuels this extraordinary market recovery from the 2020 crash and why the markets are chugging along in 2021 when, at the same time, supply chains are disrupted, businesses falter or close because they run out of either material, people, or both, and energy prices are tightening. With the fundamental outlook this weary, what is fueling these markets?

**"Fed put"** is the term for a range of monetary tools<sup>4</sup> (i.a. repurchase agreements as indirect QE, large treasury bond purchases at high prices, lowered federal funds rate for cheap borrowing) exercised in one way or another by all recent Fed chairmen, beginning with Alan Greenspan's policy response to the 1987 Black Monday crash. Over the decades, markets have learned that when a crisis arose with stock markets falling, the Fed would engage in ways that would cause the fall to reverse, leading to moral hazard: more and more speculative behavior by investment banks in markets perceived as "risk-free." This behavior resulted in what was named the "Everything Bubble": a situation where several asset classes show strong performance simultaneously. This is a phenomenon people see again this year.

**"High up on [Biden's] list and sooner rather than later, we'll be dealing with the consequences of the biggest financial bubble in U.S. history. Why the biggest? Because it encompasses not just stocks but pretty much every other financial asset too. And for that, you may thank the Federal Reserve."**

*—Richard Cookson, Bloomberg (4 February 2021)*

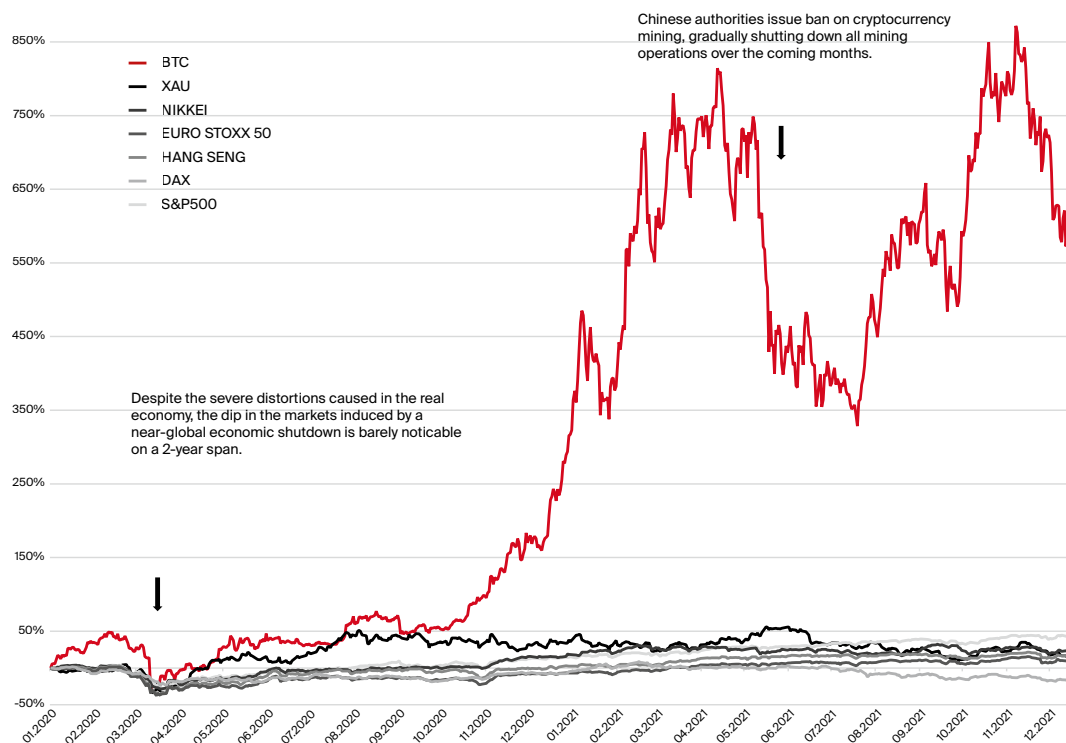
With prices systematically distorted, investors find it harder and harder to make sense of market signals – and to trust them.

**Bitcoin bull run.** Against this precarious macroeconomic backdrop, Bitcoin passed six new all-time highs in 2021 (until mid-December) and is up over 550% between January 2020 and mid-December 2021, while major indices moved in the mid two-digit range, which is surprising enough (c.f. illustration 2, also note gold's relative performance). Despite extreme volatility, investors seem to put increasing amounts of trust in Bitcoin's monetary policy that is the literal opposite of central banks' monetary policies: An absolute hard cap of 21m units and a self-reinforcing, cryptoeconomic assurance that the monetary policy will remain unaltered permanently seems to make for an attractive hedge against inflation worries.

The current Bitcoin bull run began after the 3rd Halving<sup>5</sup> (11.05.2020), when markets also saw increasing adoption by institutional investors throughout that year. Today, public and private companies and trusts collectively own over 7%<sup>6</sup> of the total supply of 21m bitcoin.

Another relevant milestone for Bitcoin investors was reached in 2021. One of the long-awaited traditional instruments that allows investors to get exposure to crypto assets are Exchange Traded Funds (ETF). On 19.10.2021 the first Bitcoin-linked ETF, ProShares Bitcoin Strategy ETF (BITO), launched one day after receiving SEC approval<sup>7</sup>. The futures ETF broke several records on the spot: It was the second biggest ETF debut of all time, trading over \$1 billion on the first day. In general, ETFs allow investors who are unable or unwilling to invest in the underlying crypto asset to invest using a traditional instrument that is known by market players and thus enable a new group of investors to get exposure.

Beyond investment circles, Bitcoin adoption among "ordinary people and use cases related to transactions and individual savings, not trading and speculation" also grew.



*Illustration 2: Performance of major stock indices and gold versus Bitcoin, 2020-2021 YTD*

The 2021 Global Crypto Adoption Index<sup>8</sup>, a country-level metric based on on-chain value received, on-chain retail value received, and P2P exchange trade volume, jumped 880% in aggregate. It is interesting to see that the top 5 countries in this list mostly declared Bitcoin illegal (\*): Vietnam\*, India, Pakistan\*, Ukraine, and Kenya\*, while only one of the mostly Bitcoin-liberal Western countries made it into the top 20, the United States.

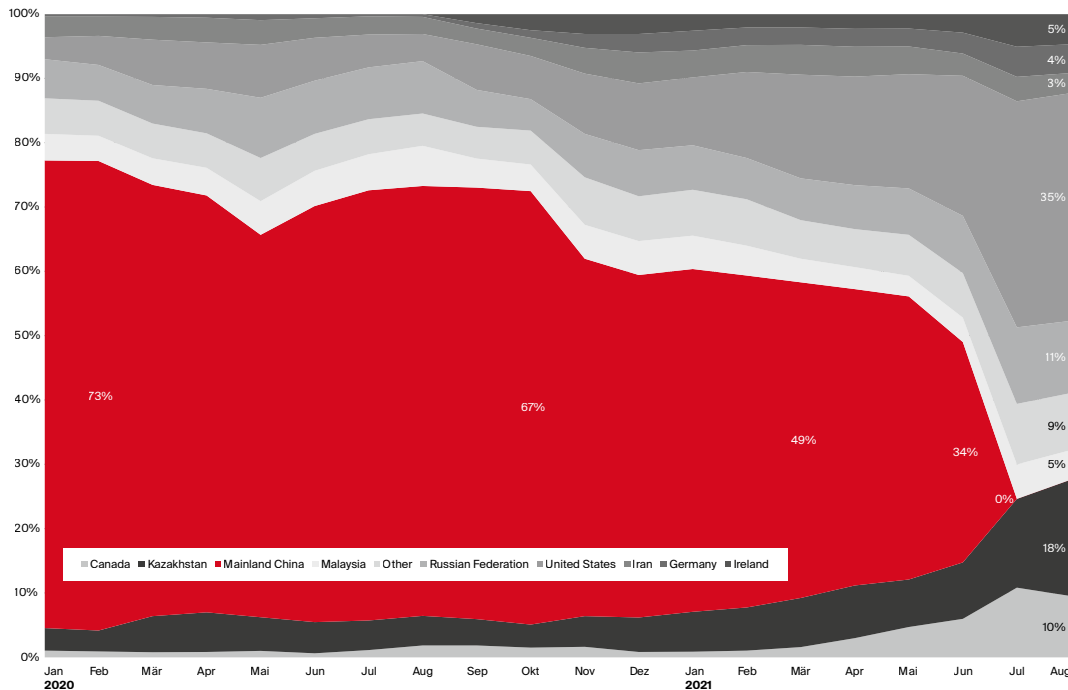
From a macro perspective, three events, one expected, two unexpected, have stood out in overlaying Bitcoin's base dynamic in 2021. Two are of geopolitical significance, touching on the topic of national sovereignty, albeit having contributed to Bitcoin's performance in opposite directions. The third is an obscure technical improvement that may show its profound impact only later.

### **First, the “Great Mining Migration” from China.**

In June 2021, news broke that China issued a ban on cryptocurrency mining, ordering power companies to stop supplying electricity to miners within days. Unlike “bans” in the past, this time, authorities were serious and followed-up until all mining operations in the country stopped. This resulted in a very significant drop in hash-rate and the exodus of many mining operations to other countries, ranging from the United States to Kazakhstan, Russia, and Canada according to the Cambridge Center for Alternative Finance<sup>9</sup> (illustration 3).

The geopolitical implications of this migration may be profound: (1) If reports (e.g., Reuters,<sup>10</sup> Coindesk<sup>11</sup>, etc.) are to be trusted, 2021 is the year China robbed itself of the possibility to exert any control over Bitcoin mining within its own borders. Should at any point in the future, Bitcoin gain more traction as a reserve currency, it will be very costly for China to get back into the game and impossible to ever regain a dominant position. (2) While the migration led to a more even distribution of hash power, it is less than perfect that the role of dominant host simply switched to the next country in line instead of dispersing among several countries: the US now harbors over a third (35%) of the world's Bitcoin hash power, a strength we expect to attain geopolitical relevance in the long term. (3) Miners everywhere learned the lesson that a stable regulatory environment is very important for the mining business in which interruptions are very costly. In the future, they will probably be better prepared to move their operations even quicker to other jurisdictions and overall transform themselves into a “geo-neutral operation” (F2Pool<sup>12</sup>). (4) On a positive note, it can be expected that the energy mix of Bitcoin mining is getting a boost towards “green” as the new locations outside of China, at least in the West, will demand renewable sources of energy for their mining operations and overall provide a more stable regulatory environment for Bitcoin.

Did the drop on hash rate hurt the Bitcoin network? Temporarily for sure. News of a government banning



*Illustration 3: Evolution of country share in Bitcoin mining, last 2 years. Source: Cambridge Centre For Alternative Finance, Bitcoin Suisse Research*

parts of Bitcoin's modus operandi always create uncertainty. However, over time, markets realized that the hash rate was not lost but only reallocated to more welcoming spots, and that the switch took time. Within half a year, the network hash rate is back at pre-ban levels and bestowed the miners who stayed online during that period additional profits as the difficulty rate adjusted downwards.

### **Second, the first Bitcoin Nation is El Salvador.**

The other event of geopolitical significance is that a first nation state adopted Bitcoin as legal tender – an event that most observers expected to happen, if at all, only many years in the future. However, in short succession, the state of El Salvador in Central America, made several steps towards putting the relations of their nation state with Bitcoin on an entirely new footing.

While China decided fully against Bitcoin and with most states struggling with crypto currencies, El Salvador made several bold steps that amount to an “all-in” on Bitcoin:

- 8 June, Bitcoin Law passed by parliament
- 7 September, Bitcoin becomes legal tender besides the US Dollar
- September, with a \$30 present in bitcoin, government onboards 3m citizens in one month

- Sep-Nov, government acquires a total of 1,120 bitcoin for a Bitcoin liquidity fund
- 23 November, government announces \$1bn Bitcoin bond (10 years, 6.5% coupon) to buy bitcoin and build a tax-free “Bitcoin City”

This series of “Bitcoin firsts” for a nation state is staggering. It is very early and unknown territory, but let's think about some of the potential ramifications of these steps:

(1) Against recommendations from the IMF and WB and their refusal to offer technical assistance in the introduction of Bitcoin, El Salvador went ahead, clearly signaling its intention to follow an independent, sovereign financial path. Irrespective of the outcome, this is remarkable for a dollarized country that is not even on the top 100 of the largest economies. Either the government and their advisors are complete fools gambling with their people's financial resources – or they have a playbook only few outside the Bitcoin community really understand. It remains to be seen whether we will see other countries moving as boldly in 2022 or not (yet).

(2) Making Bitcoin legal tender is an aggressive way of making bitcoin available as a government. More than a few critics mocked this approach as non-liberal for a currency that is supposed to bring freedom and financial inclusion. On the other side, one can argue that very few countries are able to follow El Salvador's Bitcoin playbook as very few companies can follow MicroStrategy's

Bitcoin playbook – the decision to go “all-in” on Bitcoin. It takes the riskiest strategy to enable the biggest rewards, not many can follow this strategy.

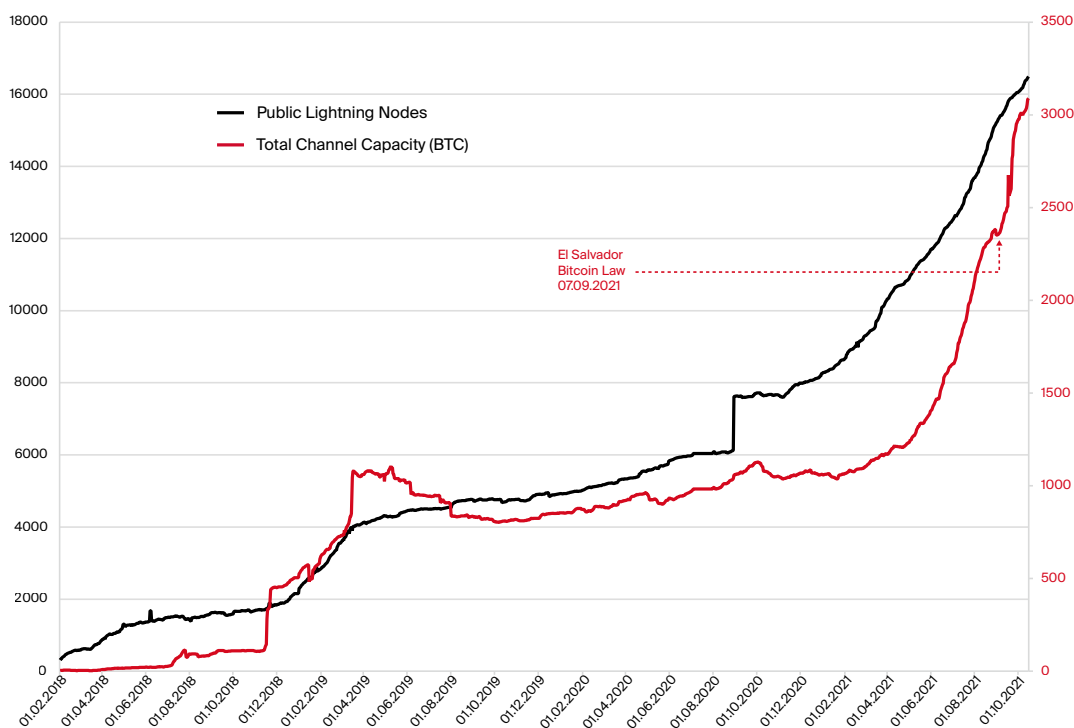
(3) Onboarding 3 million persons in one month also shows what is technically possible with Bitcoin Lightning in a population with more mobile phones than citizens. The side effect is that the 70% unbanked EL Salvadorans now have a safe, fast, and cheap means to receive remittances from their loved ones abroad. In the case of El Salvador, remittances make up 24% (!) of GDP or nearly \$6bn in 2020. Looking at the big picture, what happens if more countries decide to solve their remittance problem using Bitcoin? The World Bank estimates<sup>13</sup> the total of remittances flowing into Central and South America in 2020 to be \$88.5bn. Plus, there is another continent suffering similar problems: Africa receives a similar amount<sup>14</sup> in remittances from abroad, \$83.4bn. To anyone living in any of the 77 countries, the idea of receiving financial support at home (safer) and digital (faster) and without remittance service providers (cheaper) will make immediate sense. Bitcoin being a permissionless technology, these people do not need to wait for their governments to act, they can simply switch.

(4) Owning bitcoin offers the El Salvadoran government an inflation-resistant diversification to the national reserve that is a bearer instrument, not a debt-based fiat currency. Gold would fulfill the same purpose but

is more expensive to hold, much more cumbersome to make available in small quantities and impossible to use online. Given that bitcoin can be used in tiny quantities (“satoshis”, see below), let’s make a quick speculative calculation for the scenario that the country would abandon the US Dollar and switch to bitcoin entirely. Assuming that the government would not buy additional bitcoin, how much value would one bitcoin need to represent in order for 1,120 bitcoin to represent the \$26bn GDP sometime in the future? The price per 1 bitcoin would need to be reflective of \$23m worth of economic activity. Under such a scenario 1 sat would represent a quarter dollar, a useful size that is already transactable today using the Bitcoin Lightning network.

Onboarding millions of people in a short time put the Bitcoin Lightning<sup>15</sup> network – the scalable payment layer built on top of the Bitcoin network – into the spotlight in 2021. Compared to base-layer Bitcoin transactions, the Lightning network offers instant and free payments that do not require mining and scale without clogging up the base network. The number of nodes powering the Lightning network doubled while channel capacity tripled in 2021 alone, as illustration 4 shows.

**Third, “Taproot” was activated.** At block height #709632 on 14 November 2021, Taproot became active.



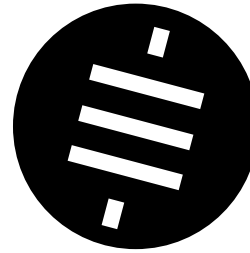
*Illustration 4:  
Evolution of Bitcoin  
Lightning network  
since early 2018.  
Source: Bitcoin Visu-  
als, Bitcoin Suisse  
Research*

While the previous two developments even made it to the mainstream news, the activation of Taproot made much less headline, maybe unjustly, because the soft fork named “Taproot” is considered the most significant upgrade to the Bitcoin protocol since SegWit in 2017.

Taproot introduces Schnorr signatures (BIP-340<sup>16</sup>). They make multi-sig transactions smaller by allowing signature aggregation and they increase privacy as TR transactions will look the same, be they Lightning channel transactions, multi-sigs, or simple standard transactions. Taproot expands smart contract functionality by introducing a new transaction output type, SegWit v1 (BIP-341<sup>17</sup>), and increases privacy by enabling different spending paths of which all are hidden except the one executed. Finally, Taproot upgrades Bitcoin’s script language to ‘Tapscript’, which allows more complex, contract-like control over spending coins. It also introduces upgradeability for the script language itself.

From a user perspective, the benefits of Taproot are increased scalability through smaller transactions, improved privacy for transactions, and a future-proof upgrade to scripting. Taken together, the soft fork lays the necessary groundwork for “Bitcoin DeFi (BiFi)” in the future. It may not be as powerful as Ethereum’s Virtual Machine, however, it achieves smart contract functionality with a much less complex technical architecture than Ethereum, especially considering the migration to Proof-of-Stake and sharding.

→ We invite you to read our in-depth article about Ethereum’s Long Chain of Forks towards “The Merge” in this Outlook edition!



In 2021, bitcoin prices reached levels where it is becoming impractical to say, “0.00018 bitcoin” when referring to a payment amount of \$10. Thus, the denomination of amounts in satoshi, Bitcoin’s smallest unit, is gaining ground. The design initiative SatSymbol.com<sup>99</sup> is soliciting support for the proposal of a satoshi symbol that is based on the Chinese word fēng, meaning “abundance.” One satoshi (sat) is a very small unit. 1 bitcoin = 100,000,000 sat or 1 sat = 0.00000001 bitcoin.

## Sense and sensibility in the sustainability debate

**The unobjective ESG debate.** The China ban and ensuing “great mining migration” as well as the idea of “volcano mining” in El Salvador, have both rekindled the debate about Bitcoin’s energy consumption. Due to increased institutional adoption of Bitcoin and crypto, the debate was further extended into the larger ESG context, which refers to the “environmental, social, and governance” aspects of due diligence screenings for investment allocations and company ratings.



The ESG debate in Bitcoin is cumbersome for several reasons. First, the inner workings of Bitcoin, where and how energy is used and what second order effects result from that, are inherently complicated, multi-disciplinary, and hard to grasp for many people. Second, Bitcoin's transparency makes it compelling to abstract away the complexity and pick easy-to-measure metrics for comparisons. The case in point is the practice of comparing Bitcoin's electricity consumption with that of countries. The most cited<sup>18</sup> country in 2021 was Argentina, with 122 TWh electricity consumption in 2019 according to the US Energy Information Administration<sup>19</sup>, which is the same data source used by the Cambridge Center for Alternative Finance for their meaningless country comparison. Why meaningless? First, Bitcoin is not a country. Second, countries are very different. Which of the following countries uses the most electricity: Ukraine, Norway, United Arab Emirates, or Argentina? Answer: they all consume a similar amount of electricity (1.1% deviation, US EIA data<sup>20</sup>), although they are vastly different in almost all other aspects: population, area, human development, gross domestic product, etc. Electricity use alone says nothing when comparing countries and it says even less if you compare with non-country entities.

**Energy.** Several sources provided quantitative data on Bitcoin's electricity use in 2021. The Bitcoin Mining Council (BMC) uses a self-reporting survey whose respondents cover 33% of the global mining hash rate. According to their Q3 data report<sup>21</sup>, Bitcoin uses 188 TWh per year. This is 0.12% of global energy production or 0.38% of energy wasted as 1/3 (!) of all energy generated worldwide is lost due to inefficiencies. Compared with other industries, Bitcoin mining is below gold mining (571 TWh), computer games (214 TWh), and the use of Christmas holiday lights (201 TWh). Based on the past, the BMC predicts a 24x efficiency improvement in Bitcoin mining over the next eight years.

With the energy discussion being center stage, the social impact and governance aspects of Bitcoin gets much less attention. We provide a qualitative overview on these two dimensions (illustration 5).

The positive social impact of Bitcoin stems primarily from its permissionless design: anywhere in the world, anyone can at any time enjoy the financial services Bitcoin offers – send and receive any amount to/from anyone else directly. The only requirement is an internet-connected device. This potential for independent self-empowerment might not be appreciated much in countries with a functioning digital banking system like Switzerland or Western Europe. However, for the

1.7 billion “unbanked”<sup>22</sup> on the planet (31%) this low entry barrier may be life changing. Therefore, 8 of the 17 SDG<sup>23</sup> have financial inclusion as one of their targets. If Bitcoin payments prove successful in El Salvador, knowledge and software tools may spread like wildfire across the Americas and Africa.

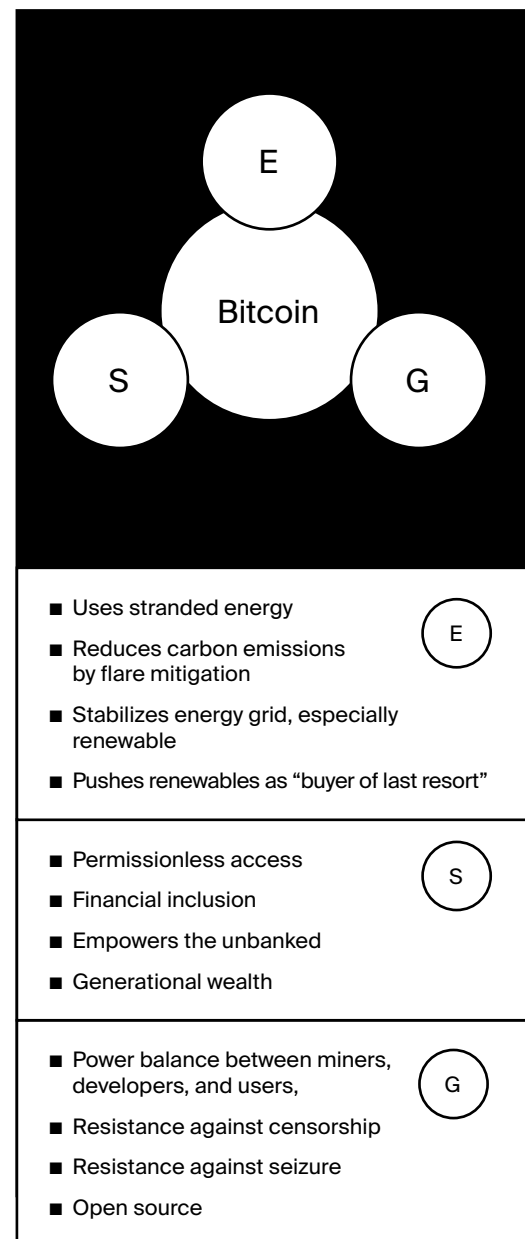


Illustration 5: Bitcoin's contributions to the different ESG dimensions. Source: Bitcoin Suisse Research

→ We invite you to read our in-depth interview with Alex Gladstein on “Bitcoin, human rights, and the ESG Debate” in this Outlook edition!

From a governance perspective, Bitcoin is still often portrayed – also by the media – as an anarchist, opaque, inner circle favoring those who got in early and an overall unfair environment for everyone else (if not taken as an outright “scam”). This portrayal usually stems from a lack of understanding about the way Bitcoin is governed as an open-source project with economic incentives. Power over Bitcoin’s monetary policy is indeed balanced across three powers: developers decide which software rules to “code”/legislate, miners decide which rules to execute, and users (besides being the citizens) judge which software rules they consider legitimate. The current rule set is designed for Bitcoin to be censorship-resistant as well as seizure-resistant, two properties no other form of money currently fulfills.



## Ethereum: Cambrian explosion in the smart contract universe

Whether building on the success of Ethereum during “DeFi Summer 2020” or whether losing patience with the slow development of the platform in terms of performance and consensus, the Ethereum universe experienced a Cambrian explosion in all directions over the last 1.5 years (illustration 6).

What started with new protocols on top of Ethereum extended sideways into new, independent smart contract platforms – some EVM-compatible<sup>24</sup>, some entirely new; some symbiotic, some competitive; but all stirring up the space and unleashing innovative forces in all directions.

The other direction was upward: The DeFi space in the narrow sense powered by Liquidity Pools, Automated Market Makers that enabled borrowing/Lending, Decentralized Exchanges, stablecoins, derivatives, prediction markets, and more got new neighbors. Non-fungible

tokens (NFTs) conquered a space of their own: starting with artwork and animals of various kinds, marketplaces developed, play-to-earn models created GameFi, and most recently people have started to talk about the metaverse, which was there all the time as virtual worlds.

No wonder, the Ethereum developers put all their focus on making Ethereum fit for the next level, cutting the Gordian Knot of blockchain-inherent limitations. Work on Layer-2 scaling solutions exploded in all directions as well: state channels, different types of rollups, side chains, plasma chains, etc.

→ We invite you to read our in-depth article on “Ethereum 2.0” in this Outlook edition!

### Decentralized Finance: “The Road Ahead”

From a quantitative view<sup>25</sup>, the DeFi market exploded in 2021. Total Value Locked (TVL) of all DeFi chains (not only Ethereum) surged from \$21.5b to \$255.1b YTD, which is a factor of nearly twelve. Despite growing competition, Ethereum still dominates the DeFi space with a TVL of \$166b (65%).

In this Outlook edition, Prof. Fabian Schär (University of Basel) highlights several trends in Decentralized Finance (DeFi) he sees unfolding in the next year. We just list them and invite you to read his article on page 33 (1) regulators handling of “decentralization theater”, (2) the market for institutions also in decentralized protocols, (3) improvements of governance beyond governance tokens, (4) the growing malpractice of “Maximal Extractable Value (MEV)” by miners/validators, and (5) scalability and developments on Layer-2.

→ We invite you to read the contribution by Prof. Schär on “Decentralized Finance” in this Outlook edition!

One of the hippest corners in DeFi have been Non-Fungible Tokens or NFTs. An NFT is most akin to a piece of art as it represents a single digital, collectable object. The numbers?<sup>26</sup> Total NFT sales in 2021 YTD were \$300m across \$79,100 sales transactions resulting in a NFT being valued at \$3,780 on average. With popular series issuing 10’000 more or less varied versions of pixelated Bored Apes<sup>27</sup> or CryptoPunks<sup>28</sup>, Sotheby’s herald NFTs as the “future of art”, while a former Christie’s auctioneer thinks the concept makes “no sense.”<sup>29</sup>

While the value of art lies in the eyes of the beholder, NFT use cases can also carry utility: be it in virtual worlds like in DecentraLand<sup>30</sup> or Axie Infinity<sup>31</sup>; in new science funding models like STEM-Genesis<sup>32</sup>; or in a dozen<sup>33</sup> other use cases.



## Conclusion

2021 has been an intense year, not only for the crypto markets. The economic after-effects of various COVID measures weigh heavy on some parts of our societies. While all major stock market indices point upwards over 2021, the increase in inflation takes away some of the conviction about the reliability of these figures.

Against this backdrop, or because of it, Bitcoin has shown an impressive positive performance, hitting more than one new all-time highs in 2021. Three events stood out: The Great Mining Migration out of China had no lasting negative impact on the overall market outlook. Positive impulses from El Salvador's move to accept Bitcoin as legal tender pushed Lightning technology in the limelight and let the use of Bitcoin for small payments surge. Finally, the Taproot upgrade paved the way for "Bitcoin DeFi."

Bitcoin's energy debate has been growing into a full-fledged sustainability debate, which will bring social and governance aspects into the discourse as well.

Ethereum and DeFi are experiencing a Cambrian explosion of protocols, projects, and platforms – with NFTs only being the latest iteration of exploration.

The crypto space is expanding in all directions at an incredible pace. While some developments seem like crazy, exaggerated hype with not much real-life foundation, some others are underestimated and may indeed change the world. Therefore, thinking crypto always demands thinking beyond.

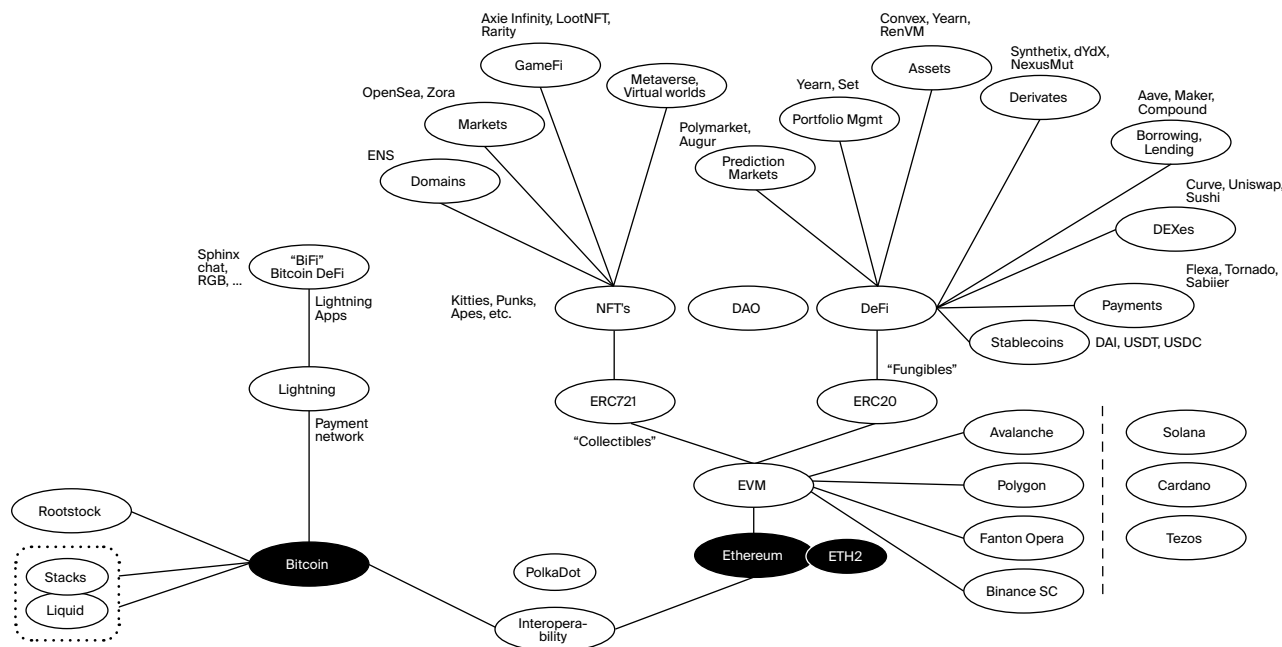


Illustration 6: The Cambrian Explosion of Decentralized Finance incl. example projects.  
Source: Bitcoin Suisse Research

## Interview

# Bitcoin, Human Rights and the ESG Debate

An interview with Alex Gladstein, Chief Strategy Officer at the Human Rights Foundation (HRF)

**Marcus Dapp (MD): Before we dive in – what is the HRF doing and what is your role there?**

**Alex Gladstein (AG):**

Sure, the Human Rights Foundation is a civil liberties organization based in New York and founded in 2005. We work on promoting civil liberties in authoritarian regimes around the world. And I'm the Chief Strategy Officer; I help with growth and fundraising, marketing and external partnerships, and in my time there (I've been there almost 15 years) I've worked very closely with all of our programs and, in particular, focused on the intersection of technology and human rights.

**MD: What is the state of human rights in the world today, while our societies undergo this digital transformation? Which rights thrive and which suffer in the process?**

**AG:** As we shift to a fully electronic world, in terms of the way we communicate and interact with each other, most civil liberties are at risk.

Whether it be your speech, your right to own something, your ability to cooperate or assemble with your fellow humans, your right to privacy... These things are all under attack because governments are able to harness networked computers and analyze massive amounts of data.

You know, modern society is built in a way, where you give up all this information and

you trade off of these different freedoms for convenience and speed and comfort.

I think the “natural order of things” as we move to the electronic society is centralization and surveillance. But thankfully there's a disturbance in the force, a positive disturbance and that is encryption – the ability to individuals to communicate privately with one another, using code, in a way that could not be spied on by even the most powerful government. That made a massive asymmetry and helped shift power back to individuals over time throughout the last few decades. And now it's like a superpower.

That's what the cypherpunks built their legacy on and their goal was to create digital cash. That's what Bitcoin is, what Satoshi created: digital cash. That's very powerful to me, because it helps us to challenge the surveillance state, and it also helps to present a different model of a political economy that's not the post-1971 political economy that we're so used to, but which just takes freedoms away from individuals. In my work at HRF I've been observing both phenomena, the rise of surveillance around the world, but also the rise of arbitrary state power over the money system. These two things come together in Bitcoin and in this global movement of people who are peacefully resisting.

**MD: Talking about money, most people just use it: they consider it a neutral instrument to just go about their affairs. Many cannot explain what fiat money is,**





**let alone question it. What is the role of the fiat money system for nation states today in your perspective?**

**AG:** The important thing to understand is: money is not neutral. It is biased, it has preferences, and it favors those who create it. That is very different from the world we used to be in. It's important to remember that, even though banks essentially have created money for the longest time, in a modern economy it's not necessarily true that the government creates all the money. A lot of what we would consider money is, firstly private-sector created. Secondly, it is credit, promises to pay, and then the whole financial structure that sits on top of that.

**“I think the “natural order of things” as we move to the electronic society is centralization and surveillance. But thankfully there's a disturbance in the force, a positive disturbance and that is encryption – the ability to individuals to communicate privately with one another, using code, in a way that could not be spied on by even the most powerful government.”**

Up to World War I and arguably even up to 1971 in some respects, at least the system through which nations interacted with each other at the geopolitical level was rooted in something real. The way nations balanced their payments with each other pre-World War I, and to lesser degrees as we got closer to 1971, was rooted in this concept that you could settle your debts in gold.

The ultimate monetary good used to be gold. And then, throughout the first 60 years of the 20th century, gold was hunted down, cast out and intentionally demonetized – largely by the US Government – and replaced with American debt. American debt became the highest monetary good, the “US Treasury”, the savings instrument for other nations, as well as the premium collateral for financial markets. So,

the risk-free asset used to be gold, now it was American debt. That process began, arguably, in World War I and was accelerated in the 30's. We went back to the gold exchange standard a little bit in 1944, whereas FDR totally demonetized gold domestically.

The US realized, “Let's try to make a system where everybody uses dollars around the world.” And the way that they convinced people to do that in 1944 was to say that you could redeem it for gold at a fixed rate, \$35 per ounce of gold. People believed us and we tried to hold that peg for a long time.

Originally it was easy because we were this massive creditor nation, and we have this balance of payments surplus. Throughout the Cold War that changed, and after the Korean War we were a debtor nation and this relationship, this peg, started to become very difficult to hold, even in the late 50s. And in the 60s, we had to basically do price-fixing with other governments to the London gold pool and it ended up collapsing. Finally, in 1971 we defaulted on our debt. So, \$50 billion short-term dollar liabilities held by other nations went from being IOUs, like “I owe you gold” to “I owe you nothing,” there is nothing here. The US debt got baked into the monetary base.

That has had profound implications on the world and if you just look at any sort of social indicator since the 70's: inequality, the rise of the 1%, stagnant wages, explosive equities, the rise and the cost of standard of living, making it difficult for the average working-class person versus the obscene wealth accumulated by the 1%. These are some of the things that have happened: the financialization of the world, the hollowing out of the American economy.

These things have happened in the last 50 years. And it's because of fiat money.

I think that the fiat money system is about constraints on government behavior, especially in the US. The US supplies the world with its savings instrument in our debt. This has created some perverse incentives that trickled down throughout not just American society but throughout the world.

Now, that era seems to be - I wouldn't say ending - but it's certainly unraveling a little bit and other countries are starting to do more business between each other in their own cur-

rencies. The dollar is facing extreme pressure. We're seeing inflation, we haven't seen since the 70s, maybe 60s.

You know, there is only one way out for the fiat system: It's to print more money.

In the previous monetary era, you couldn't do that. These countries had to sell off assets, they had to devalue, they had to repeg, they had to cut spending, there were consequences. Today we're in "Modern Monetary Theory" essentially and the only limit is inflation. Well, how do they reduce the money supply? They claim through taxation. I don't think they're going to do that. We've seen this behavior before: Nixon could have devalued, basically repriced the dollar against gold. He didn't have to default on our debt. But then the people would have known that he was debasing the currency and they don't like that.

It's the same thing here: the government's just kicking the can down the road.

And eventually, how are you going to convince people to invest in our debt? You have to raise the interest rates, there is no other way. I mean, who's going to buy American debt that is going to yield negative? Trillions of dollars invested in that way, today. I don't see that lasting forever. People are going to realize they can go to Bitcoin.

I think that dynamics are going to change massively and this whole thing of "interest rates to zero" ... well, good luck, no one's going to buy your debt! People are buying that debt now, because they view it as a risk-free asset, so they're willing to pay. What if I were to tell you that over the next decade there will be a psychological shift and people will start seeing government debt as risky?

**MD: Let's make this concrete. One country this year was hit by "Lightning", so to say. Its name is El Salvador, which means "the Savior" in English. So, what would Bitcoin save the country from?**

**AG:** Bitcoin is a completely different structure than fiat money. It's an asset money that increases your purchasing power as a worker over time. Your wages will go up over time if you save in bitcoin.

That is totally different from today, where wages go down. The time and energy that you put in lose value very quickly over time. With bitcoin they gain value. It's as simple as that. If the Salvadorans start to shift into this economy, they're going to be massively advantaged. Not only are they going to have the asset itself, but they're going to have the lifestyle, the technology, the know-how.

**"Bitcoin is a completely different structure than fiat money. It's an asset money that increases your purchasing power as a worker over time. Your wages will go up over time if you save in bitcoin. That is totally different from today, where wages go down. The time and energy that you put in lose value very quickly over time. With bitcoin they gain value. It's as simple as that."**

Other countries are going to call them to find out how to do this, like they'll have enormous expertise and know-how to get this done. A lot of things can be said about the ruler of the country, who I view as anti-democratic, but that's separate from the decision to adopt Bitcoin as legal tender. They could have chosen a China surveillance coin or God knows anything else. The decision to choose open, decentralized, scarce public money was a remarkable one. And it won't be the last country. There'll be enormous benefits coming to that country, which is hilarious because the economic orthodoxy sees it as a crazy risk.

Every other country is going to adopt Bitcoin one way or another. I don't know whether it's as a reserve asset or as legal tender - it's inevitable.

**MD: The criticism of Bitcoin has taken a specific spin with the ESG (Environmental, Social, Governance) debate: Bitcoin is boiling the planet, wastes energy, proof-of-work, ... What's your take on the position that Bitcoin is bad according to these ESG metrics?**

**AG:** I think our current fiat money system is unsustainable and is rooted in the petrodollar, it's connected with oil. So, we need a different system to break our reliance on oil and fossil fuels.

I think Bitcoin can run entirely on renewable energy and nuclear and that's a bright future for the planet if our money system runs on renewables. The current money system runs on fossils. It relies on this relationship with energy in that way. You're never going to get a green movement, if your money is based on black gold, that's just not going to happen.

I think that people really get hung up on the early history of bitcoin mining and, and how it was all this Chinese coal. It's none of that anymore. China kicked out all the miners. Yes, the energy mix is what it is. I still think it's much greener than most industries by far.

And you have to think of the benefits it provides to the tens of millions of people around the world. We're talking something that is literally empowering tens of millions of people around the world, and it generates like half the carbon footprint of the cruise ship industry.

So, not only is it quite efficient in terms of its impact versus what it does, but I think it's going to get greener over time and it's going to totally change humans relationship with energy. You know, I wouldn't be surprised if in the future, bitcoin mining is built into our homes and our grids.

There's this elegant demand-response thing that can be done with Bitcoin that I'm excited about. If you get enough bitcoin mining, you're not going to have these power crises, when storms come, and you have blackouts. Bitcoin miners can just turn off the power and it can shift over to the grid.

Also, I'm excited about developing countries being able to unlock these renewable resources that they all have – solar, wind, geothermal. They have massive renewable resources, but they don't use them because it's hard to get financing to build those farms and connect them to the grid. Well, now you can get financing to do it if you're mining Bitcoin. So, I'm excited about that energy piece.

**MD: Within the energy and mining debate, there's also much talk about consensus mechanisms. Ethereum is very much pushing Proof-of-Stake, we also know Bitcoin stays with Proof-of-Work. What's your take on that, because people are saying, Proof-of-Stake is much more energy efficient?**

**AG:** I think that's a very surface level understanding of what's going on. Proof-of-work is a way to create a new financial system. Proof-of-Stake is the existing financial system, meaning that the people who have the most capital get to make the decisions. In Bitcoin that's not the case.

If you have billions of dollars' worth of bitcoin versus someone who has \$10, neither of you can change the monetary policy. Wealth doesn't benefit you in that regard. In the fiat system, if you're a billionaire you can get a bailout, you can literally influence the monetary policy. Proof-of-Work exists to create a new standard, a new paradigm, where we're all equal in front of the eyes of the law.

**“The current money system runs on fossils. It relies on this relationship with energy in that way. You're never going to get a green movement, if your money is based on black gold, that's just not going to happen.”**

That requires energy expenditure, and it will, I think, improve our relationship with energy. It will incentivize more renewable energy to be unlocked and it'll put us on a much more intense quest for the cheapest, most efficient energy in the world which I don't think is going to be coal or oil.

The existing financial system is extremely negative for the environment, very tied to fossil fuels. Proof-of-Stake doesn't change that at all. It is just an imitation of the existing system.

**MD: The second aspect of this ESG is the social aspect. On one side, there are people claiming Bitcoin is a Ponzi**

**scheme, it's a bubble or several bubbles. Others say it's about financial inclusion and human rights. How do you see that? What can the social impact of Bitcoin be?**

**AG:** The social impact of Bitcoin is global. Tens of millions of people are benefiting today from Bitcoin from a social perspective. It's giving them financial inclusion and empowerment at a greater scale than any company's ESG initiatives are giving. There's no company ESG initiative that's really helping, say, somebody in rural Sudan. That's probably not going to happen.

**“It allows us to have digital cash, a parallel system that they don't control. Most importantly, it allows us to have a currency that they can't arbitrarily debase. I think those things are all very, very important, even if you live in a wealthy country.”**

However, if they have a cell phone and they can learn about Bitcoin and they can start using it, and they can begin save themselves from that country's rapacious inflation, right? This is something that anyone can use around the world. It's incredibly powerful and I think the most effective investment one can make, is in the Bitcoin network.

The criticisms you mentioned are not true. It's not a Ponzi scheme. It's not something where there is some Bernie Madoff type who's just taking in money and replacing it with other people's money. This is not happening. Everything in Bitcoin is auditable and you can look at it, you could look at all the transactions, you could look what's happening. And what's happening is, people are opting out of the fiat system into something new.

People won't necessarily use it for the ideological underpinnings. They'll use it, because it's better than going to the post, in the same way that people used email because it's better than going to the post office, people are going to use Bitcoin because it's better money. It's better than go to a bank and make a wire - it's

ridiculous. So, I think that the social arguments against Bitcoin are weak and that evidence for Bitcoin being a powerful social tool is staggering.

**MD: Finally, governance: In a conversation with Saifedean Ammous, you were arguing in favor of bitcoin being democratic (AG: Yes!), separation of powers, etc. On the other side, Saifedean argued more for an anarchistic perspective. How do you see that conversation?**

**AG:** It was a great conversation. My point was that Bitcoin is anti-authoritarian. What does “democracy” mean? “Rule by the people.” To me, Bitcoin is ruled by the people, not by the government, not by a king or a dictator. What I was trying to get at was that ‘demos’, the ‘people’, and the word democracy is accurate of Bitcoin.

The point of that whole conversation was merely to show that while Bitcoin is not a democracy in the sense of going to voting, it is a democratic money, because I believe it's ruled by the people and not by a dictator or a king or a tyrant. That's my thesis.

**MD: Would you say, is it easier to make the case for Bitcoin in an authoritarian regime than in Western liberal democracies? Why should your or my fellow citizens care for Bitcoin beyond “number go up”?**

**AG:** Ultimately, Bitcoin matters for the same reasons for everybody, it's just a matter of urgency. In dictatorships all ‘law and order’ collapsed and there's secret police that rules everything. So, it's a little different than in a system where we still have law and order, like in Germany or Switzerland.

But what's happening is gradual increase of control by the government and corporations over money, spending habits and behavior – your life, really. Bitcoin allows us to check this intruding behavior. It allows us to have digital cash, a parallel system that they don't control. Most importantly, it allows us to have a currency that they can't arbitrarily debase. I think those things are all very, very important,

even if you live in a wealthy country.

It matters for everybody, whether you care about privacy or about financial freedom and preserving savings. All of it matters. You want to put your money in a bank in Europe? It's a negative interest rate, right? So, how about not negative interest rates? (laughs) How about I don't give my money to the bank and instead I keep it in bitcoin and I watch it appreciate over time? I think a lot of people are going to start understanding why that's very powerful.

**MD: We don't know what the future holds and for Bitcoin many scenarios seem to be possible. Let's outline two extremes: one is governments trying to ban or stop it. What are your thoughts on banning?**

**AG:** No, I think it's not going to be stopped, but bans are very likely! In fact, they happen all the time. The Chinese Government just banned mining, the Norwegian government is threatening to ban mining, the Nigerian Government is essentially banning use of bitcoin by freezing bank accounts that are connected to cryptocurrency trading platforms. There are all kinds of restrictions. We should expect a proliferation of all kinds of restrictions and bans.

But they're not going to work! So, the government can try as much as it wants. What do you do? It's an idea, it's an invisible asset that can be traded peer-to-peer without government intrusion, it's not possible to stop. I think the way it ends up happening is they realize that it's a fool's errand and they end up figuring out how to benefit from bitcoin.

El Salvador is obviously a good case, there are lots of states in the United States that are good cases, there are cities, City of Miami, the new Mayor of New York City, states like Texas and Wyoming. You have governments even, like Singapore, Switzerland, Norway, whose sovereign wealth funds, their savings really, are either invested directly in bitcoin or exposed to bitcoin companies or assets.

We are going to see a lot more of that and less like a draconian ban which isn't going to work. I mean they can try, but it's just not going to work.

**MD: The other scenario would be "hyperbitcoinization", the thing many Bitcoiners are looking forward to. When do you think will that happen? How will it look like? What will happen to fiat currencies, how will nation states react?**

**AG:** I think we probably have a transition period where we go back to like a gold exchange standard type of thing where governments peg their currency to Bitcoin at a certain exchange rate. I don't know how long that lasts because Bitcoin isn't gold. Gold is not efficient for medium of exchange, it's pretty terrible for that: people want to save it, there are theft concerns. Bitcoin is a very elegant medium of exchange. I don't know how long the fiat system lasts once that first concession is made. It's very possible we live in a world where we just interact exclusively with Bitcoin and Bitcoin instruments. I find it hard to believe that fiat's going to hold on.

Fiat is an experiment, it's relatively recent in history. And I'm not talking about commercial banks creating money. That will continue to be the case in many ways. I'm talking about the underlying, about what the central banks actually have. It's only somewhat recent that they don't have metal or something scarce, that they just have paper promises. That's entirely a creation of the last hundred years.

We've been around for a lot longer than that and I just think that that's going to turn back to bitcoin. And then what does a bank do? You want to deposit your bitcoin with the bank? Well, they're going to have to offer you something very appealing, right? We're talking very high interest. You have to start thinking about it: interest paid in what, in bitcoin? I think the whole system is going to change.

Can banks afford to create loans and deposits in the same way in a Bitcoin system? Probably not, probably slightly different. Again, I still think banks exist, I still think you'll have bank creation of money. And, of course, credit - people are going to borrow and all these things. It'll just be a completely different paradigm.



**MD: 2022 is around the corner. Do you have any predictions for the Bitcoin space, like, for example, on which continent the next Bitcoin country will emerge?**

**AG:** It's hard to say. It's probably one of these things that happens when you least expect it. Would you have picked El Salvador? Really? That was not on anybody's "bingo card" two years ago.

Could it be Ukraine or Columbia, or one of these countries that's hinting at it? Maybe... But maybe it's also a country that nobody's thinking about.

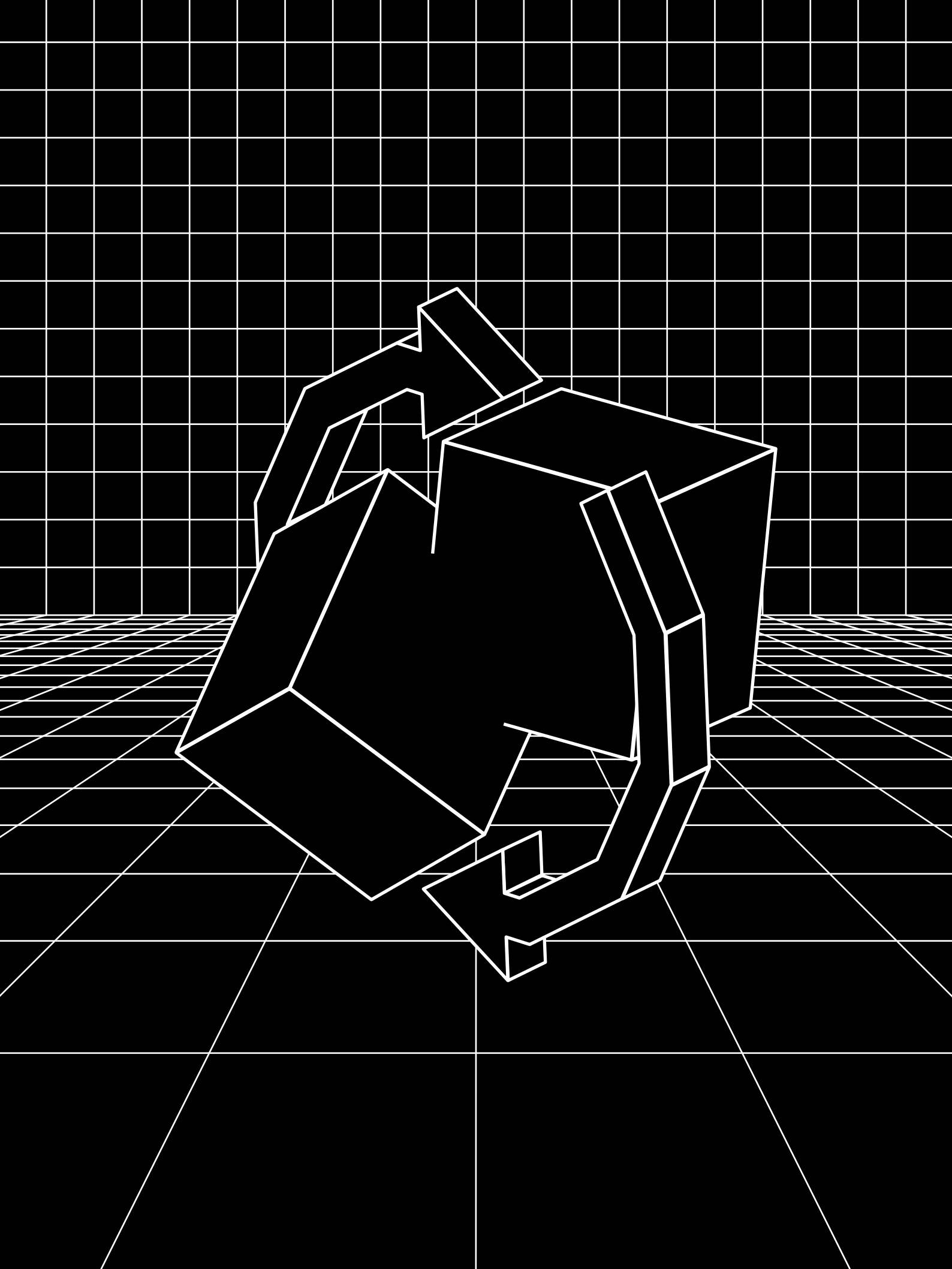
Honestly, I think legal tender is an aggressive step. I don't think there's going to be that many countries that do that in the near future. That was kind of ... puh ... going a decade ahead. But I think governments that buy bitcoin, that integrate it in some way... You have already seen this happen in America at the state and city level, politicians taking their paychecks in bitcoin. That's just going to continue and increase.

Bitcoin is going to be a huge part, I believe, of the 2024 political cycle in the United States. So, hard to say.

**MD: Alex, thanks a lot for your precious time. Where can people learn more about your work?**

**AG:** Follow me on Twitter at @gladstein. You can follow the Human Rights Foundation at hrf.org and you can come visit the Oslo freedom Forum in Norway on May 23 to 25 of next year. We're going to have a full-scale Bitcoin Academy, so I hope you can all come. It's not too far for most Europeans. So come check it out, thank you.

**MD: Thank you very much, Alex.**



# Ethereum's Long Chain of Forks Towards "The Merge"

Dr. Marcus Dapp

■ After a long chain of forks from 2015 until today, during which the Ethereum community stood together as one (except once), the project is reaching the crucial final moment in the migration to Ethereum 2.0. While the community pushes a "rollup-centric" scaling roadmap on Layer-2, which is terra incognita by itself, the Merge on the base layer is the first of its kind and will require all the energy and attention of Ethereum developers in 2022.

■ The stakes could not be higher because next to the many technical changes that must take place in unison for the Merge to be successful, Ethereum is facing small but rapidly growing competition from new platforms that offer cheaper execution of smart contracts already today.

■ The list of decisions worthy of deeper research and debate because of unclear long-term effects is considerable in our view. What will the final monetary policy of Ethereum 2.0 be? Is it optimized for cheap smart contracts or 'ultrasound money' with high price levels? While Proof-of-Stake uses less energy, will it be as secure and immutable as Proof-of-Work?

## A long chain of forks

Software upgrades in distributed systems like blockchain protocols can be more complex than upgrading your browser at. The core question is what happens to those who do not follow the upgrade and stay on the old version. If you do not upgrade your web browser for 5 years, it may start having problems with newer websites, but that's about it. As the underlying TCP/IP and HTTP protocols powering the internet have not changed, everybody continues to be on the "same" internet, just with older or newer browsers. In blockchain lingo, these are "soft forks" (Table 1). If the underlying protocol changes as well, then the situation may change. Then upgraded and non-upgraded clients may find themselves on different "internets" that are no compatible with each other anymore – which is called "hard forking" in the blockchain world. While the first case is not a big issue, the latter is something that requires a high degree of consensus to protect the chain from permanently splitting in two. At the same time, it is the final option if the developer community cannot agree on a common direction for the network: take a copy and go your own way.

With these complexities in mind, the long chain of forks that Ethereum, the platform that pioneered smart contracts and decentralized applications, underwent since its first official release in 2015, is impressive. Most of the hard forks spanning six years across four development phases were planned and uncontentious. Illustration 1 gives an overview including the key changes of each hard fork (EIP are "Ethereum Improvement Proposals").

While the Ethereum community overall managed to avoid long, paralyzing disputes akin to Bitcoin's Blocksize Wars<sup>34</sup>, there was fork, that stirred a lot of debate and discontent. It was when the leading Ethereum developers initiated a hard fork to rectify the "DAO Hack", the siphoning of \$60 million of funds invested in the first decentralized autonomous organization on Ethereum, The DAO. Since that contentious decision, there exists

## Comparison between soft and hard forks

	Soft Fork	Hard Fork
<b>Behavior of old nodes</b>	Can accept new blocks as valid	Do (and can) NOT accept new blocks as valid
<b>Backward compatibility</b>	Yes	No
<b>Consensus rules</b>	Contract, stricter than before	Expand, looser than before
<b>Pressure to upgrade</b>	Optional (same chain stays)	Mandatory. If users do not upgrade, the chain splits into two.
<b>Possible attacks</b>	Unspecific	Double spending (51%) attacks post-fork on the weaker chain because of hash rate split

Source: Bitcoin Suisse Research

Ethereum Classic that kept the original Ethereum consensus rules, while today's Ethereum chain recompensated people who lost Ether to the DAO Hack.

Now this long chain of hard forks on Ethereum 1 is slowly drawing to a close in 2022, as the community is working on the final phase towards The Merge, the

merging of the proof-of-work Ethereum 1 chain into the proof-of-stake Ethereum 2.0 Beacon chain.

Therefore, the focus of many EIP changes during the Serenity phase has been to improve Ethereum's scalability, be it through repricing of gas cost for certain operations (opcodes), improvements to make Layer-2

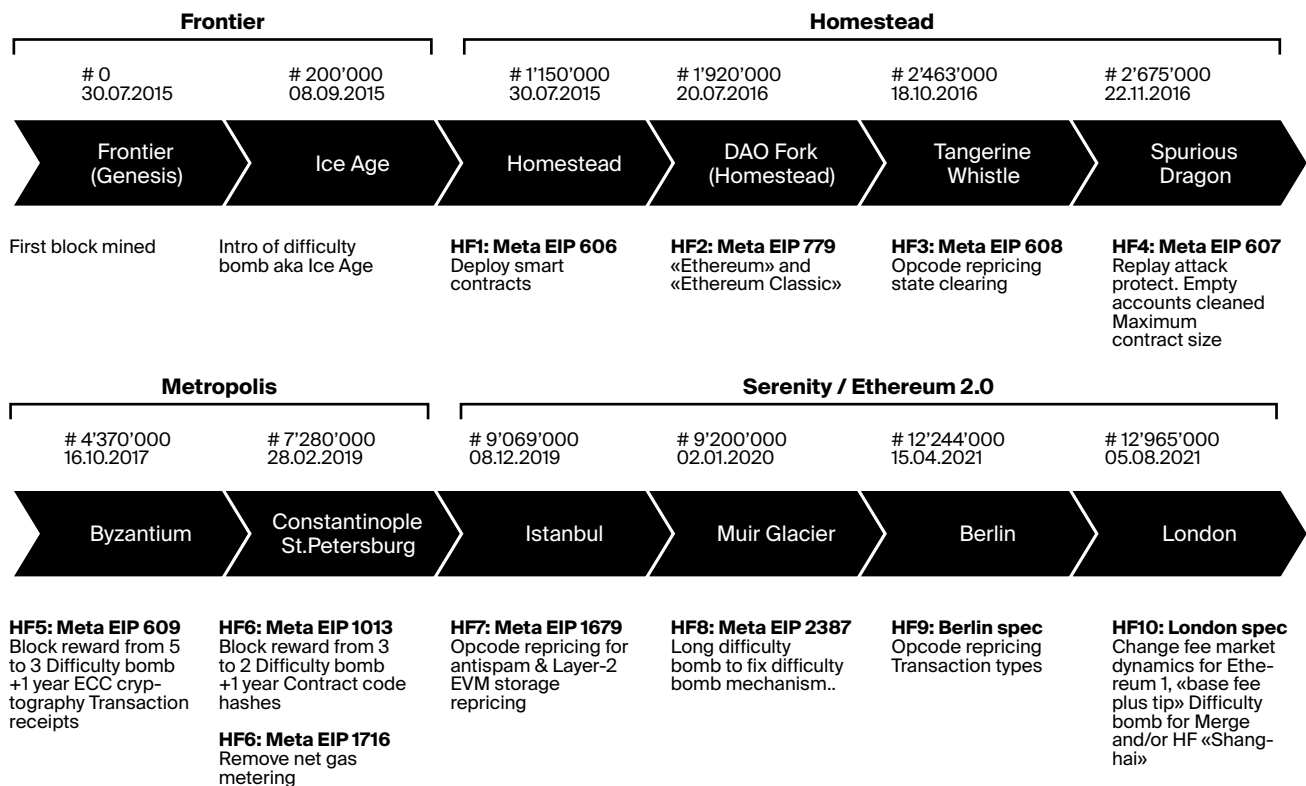


Illustration 1. Ethereum hard forks with key changes, ordered by activation block numbers. Source: Ethereum Execution Client Specifications, Bitcoin Suisse Research

solutions possible or more performant, and to prepare the switch to proof-of-stake.

### A rollup-centric scalability roadmap

The problem Ethereum aims to tackle with the Ethereum 2.0 upgrade, is plaguing all blockchain-based platforms: to be synchronized and get “in consensus”, distributed networks require to send information forth and back between nodes. This coordination requires two things: first, bandwidth – hence debates about different block size designs, like 1MB in Bitcoin and a “gas limit” for blocks in Ethereum. Second, coordination requires time for the information to propagate across the network – hence debates about different block time designs, like 10min in Bitcoin and ca. 13sec in Ethereum. There exists no best solution. Different projects optimize for different outcomes, but all are bound by the Blockchain

on the former two properties. In October 2020, Vitalik Buterin, founder and master-mind of the Ethereum project, concluded that “the Ethereum ecosystem is likely to be all-in on rollups<sup>36</sup> (plus some plasma and channels) as a scaling strategy for the near and mid-term future.”

When researching blockchain scalability, one distinguishes between on-chain (Layer-1) approaches that modify the consensus protocol and off-chain (Layer-2) approaches that require no modifications on the base layer but may use base layer security to operate (Illustration 2).

Rollups are Layer-2 scaling techniques that bundle (“roll up”) many transactions together and only send a proof of that bundle to the Layer-1, thus releasing the load on Layer-1. Depending on the proof logic, one distinguishes between optimistic rollups and zero knowledge rollups. Optimistic rollups are “optimistic” that

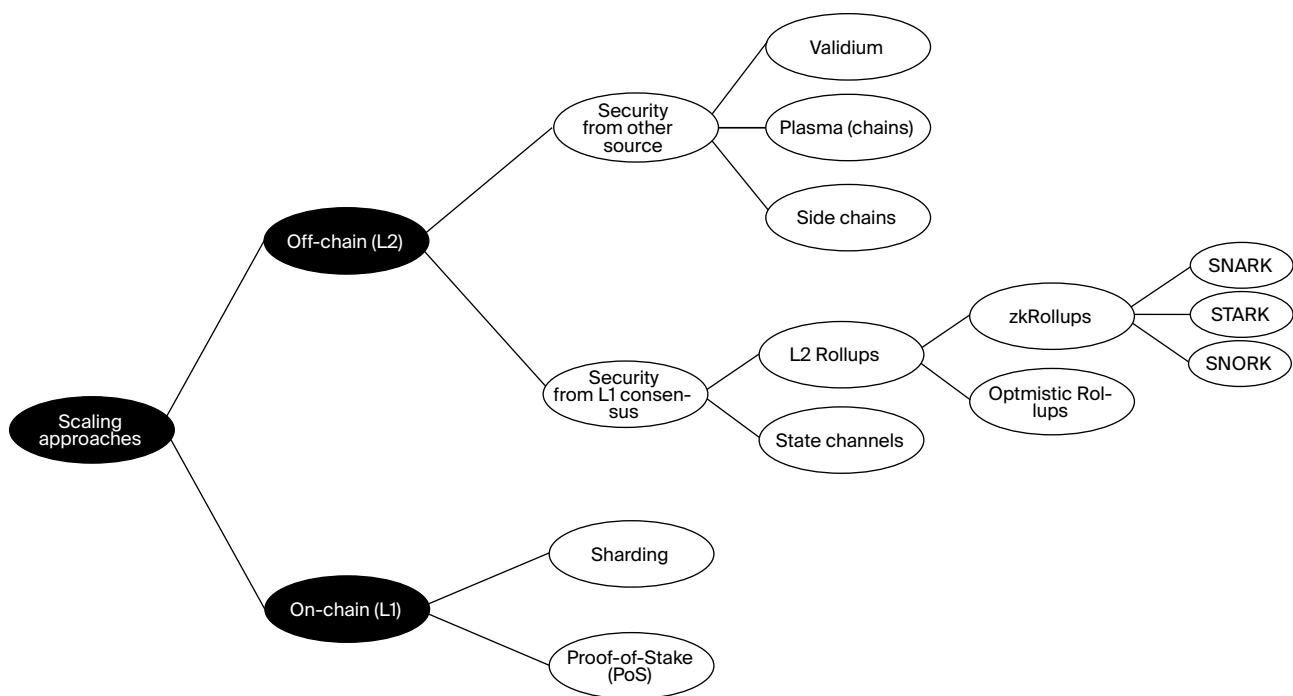


Illustration 2. Overview of scaling approaches for blockchain systems.  
Source: Bitcoin Suisse Research

Trilemma, the blockchain reformulation of the CAP theorem<sup>35</sup> from Computer Science developed in the 80s. It states that only two out of three goals can be achieved simultaneously in blockchain systems: decentralization, security, or scalability.

As blockchain proponents have a hard time sacrificing decentralization or security, much research and development over the last years went into finding solutions to scalability that would minimize the effects

the transactions are correct and only use fraud proofs when needed. Zk-Rollups on the other side offer validity proofs for every transaction bundle.

Rollups continue to be an area of active research and experiments and projects are active across the entire space. We expect the next year to provide more clarity in which direction the Ethereum project will head on the second layer. But first, the project has an immediate challenge on Layer-1.

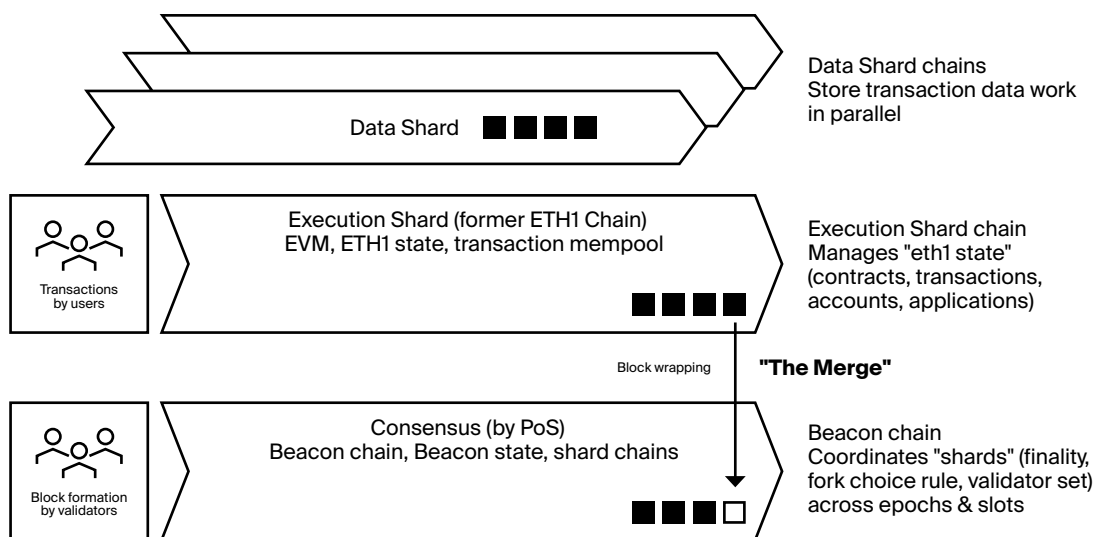


Illustration 3. The Merge connects the Beacon chain with the Execution Shard (former Eth1 chain).  
Source: Bitcoin Suisse Research

### Mastering the Merge amidst competing chains

The Ethereum community is facing two challenges that have been growing over 2021 and can be expected to intensify in 2022. The first is in-house: the switch from Proof-of-Work to Proof-of-Stake. The Merge aims to transform the Ethereum 1 chain into an execution shard and then connect it to the Beacon chain<sup>37</sup>, which is already live and running since 1 December 2020 (deposit contract live since 4 November 2020). The second is coming from the markets: several other smart contract platforms have gone live and challenge Ethereum on its weak spot, transaction fees and transaction throughput.

**The Merge.** The ambitious goal is to swap the core consensus mechanism from Proof-of-Work to Proof-of-Stake while introducing sharding – all without disrupting operations. The word “merge” is a bit of a misnomer in our view. Instead of merging one chain into another as the word suggests, the original chain is split up. The different components of Ethereum 1 are dissected into a consensus chain (Beacon), an execution chain (former Eth1), and multiple data shards. Therefore, one needs to decide where storing of accounts, transactions, blocks, etc. happens as well as where and how computing of finality, consensus, fork choice, etc. happens (Illustration 3).

Developers expect several improvements<sup>38</sup>: (1) higher security as slashing discourages chain reorgs and thus push “block finality”; (2) PoS removes the high energy consumption of PoW (by up to 99% as estimated); (3) setting the stage to introduce data shards later to increase the available blockspace; (4) Priority fees will go to validator controlled address on Execution layer instead of to miners, making ETH liquid again and allowing vali-

dators to withdraw stakes; (5) ETH supply issuance will drop from currently ca. 3.5% to ca. 0%.

As is obvious, the migration is a very complex and thus risky undertaking. Aside from the inherent design and software complexity of the Merge, the Ethereum chain holds tokens and manages smart contracts in excess of half a trillion USD. Thousands of users, developers, and businesses around the world rely on the functioning of Ethereum 24/7. Pulling this migration off without disrupting the functioning of the Ethereum network is a nerve-wrecking process that according to the latest information, is expected to be done in the middle of 2022<sup>39</sup>. We will see whether the developer community will be successful and on time in summer 2022.

**Competition.** The second challenge is the fast and vocal competition in the market segment of smart contract platforms. The competition can be grouped in

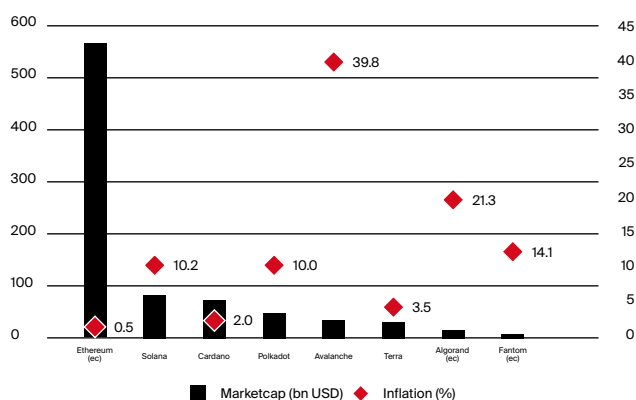


Illustration 4. Ethereum competitors by market capitalization.  
Source: Messari, Bitcoin Suisse Research

projects that are compatible to Ethereum and its virtual machine (EVM) and those that are not. The EVM is the unit that executes smart contract code, written for example in the Solidity programming language. A platform that is EVM-compatible offers developers the advantage to not have to rewrite smart contracts again using a different language and therefore not undergo new code audits. In addition, the existing ecosystem of decentralized apps and users can be directly targeted. The market entry barriers are significantly reduced in this scenario. On the other side, platforms that decide against this compatibility feature, have all freedoms in implementing their vision for an improved smart contract platform: consensus protocol, fee mechanism, and other technical design decisions (Illustration 4).

**Inflation and utility tokens.** Ethereum still looks good with these metrics: the platform with the highest market cap is also the one with the lowest inflation rate (under 1%), while some of the competitors exhibit 2-digit inflation rates that make fiat currencies look good. Does inflation matter at all? In contrast to a pure monetary coin like Bitcoin, which has an ever-decreasing inflation rates built-in, the question which inflation rate is adequate for a smart contract chain is less obvious

Low inflation may increase the token price (in fiat terms) over time, which is what investors seek. High inflation rates on the other side, may just mean that many tokens are created that users and developers can take to run smart contracts cheaply. The less a “gas” token is used as money, the better it is suited to power smart contracts and vice versa (aka utility token). It will be interesting to see how the differing interests between developers, users and investors will play out in the longer run – especially on the Ethereum platform that changes the economics quite radically.

### **Emergence of “ultrasound money”**

Two developments impact the circulating supply of ETH on the path to Ethereum 2.0. One is caused by the switch to Proof-of-Stake (PoS), the other one was deliberately introduced to change the fee dynamics.

Proof-of-Stake is powered by validators who stake tokens (a bit like in poker) instead of spending energy for producing the next block and keeping the network secure. It’s a bit like poker: You put on a stake and if you lose (i.e., do not adhere to the consensus rules), your stake is slashed. How large will the effect be? Due to the various changes, the future monetary policy aka token supply for Ether is very hard to anticipate without modeling<sup>40</sup> it.

No mining takes place in Proof-of-Stake. Instead, special nodes called validators, coordinate to process transactions and block creation by locking a minimum amount of Ether. This stake can be foregone if they behave malicious and manipulate the block creation process to their advantage. The protection lies in slashing of their stake and not in investing energy to create blocks.

What are the economic effects of staking on the supply? Most obvious, the circulating supply is reduced by the amount staked.

From December 2020 to November 2021, the amount of Ether staked for Proof-of-Stake<sup>41</sup> on the Beacon Chain grew from 656 160 ETH to 8 391 388 ETH (+1280%), which permanently removes ca. 7% of the total circulating supply<sup>42</sup> of ETH.

The question of supply dynamics is further complicated by the fact that the dynamics of the (“gas”) fee market in Ethereum have been modified significantly by activating EIP-1559<sup>43</sup> in the London hard fork. Before EIP-1559, the fee market was an auction in which users bid to get their transactions included by miners and all fees went to the miners. This change introduced a new mechanism of calculating fees per transaction and per block with a particular twist. Now, transaction fees consist of two parts: a mandatory base fee and an optional miner tip. While the miner tip continues to go to the miner, the base fee is burned. Since activation<sup>44</sup>, the mechanism removed a total of 1,087,615 ETH from the supply through fee burning, reducing the net issuance by 507,000 ETH (68%) in the period August-November 2021.

Combined, staking and fee burning have a dampening effect on the supply of ETH. Some argue that with these changes, Ethereum is moving into a deflationary monetary policy that is stronger than Bitcoin’s inflation reduction over time, leading to “ultrasound money”<sup>45</sup> in the end.

### **Discussion**

The long history of exploits in the mainly Ethereum-based DeFi space<sup>46</sup> and the approx. \$1.5b loss of funds in 2020 and 2021 are testament to the fact that the crypto space is technically very demanding. While the number of web3 developers may still be limited, the number of computer science experts able to reliably analyze cryptographic protocols is vanishingly small.

In that context, Ethereum is headed for a fundamental transformation that turns the system upside down. The complexities and risks of dissecting the consensus components and spreading them across multiple chains are mind-blowing. A few aspects to keep in mind:

**Complexity.** The migration to Ethereum 2.0 is a complex undertaking with several moving parts that change simultaneously and are not easy to anticipate in their consequences: Merging to PoS, mapping Ethereum 1 into an execution shard, complex fee market dynamics, split into execution and multiple data shards, etc. How the cryptoeconomic dynamics will play out longer term is very hard to assess even with simulation<sup>47</sup>.

**Economics.** Tightening the ETH supply because of staking may be good for investors, but it is less beneficial for those (many more) people who want to develop, run, and use smart contracts on Ethereum because it makes much more expensive measured in USD or other fiat currencies. Cheap gas is good for driving, not for investing in the oil industry.

The new fee mechanism exacerbates this trend. This strong limitation of the supply towards “ultrasound money” is a double-edged sword for a smart contract platform whose ambition is to be a world computer rather than a world currency.

Ethereum’s primary focus has always been to be the “world computer”, executing smart contracts and powering decentralized applications. However, as the recent price developments have shown, people also like to just invest in Ether as a “currency”, not worrying about developers and smart contract users per se. The interests do not seem to be fully aligned and we will see how the changing dynamics will work out in 2022 and beyond.

Finally, burning fees that users had to first earn/buy while validators receive newly created Ether as staking rewards is vaguely reminiscent of the Cantillon effect<sup>48</sup> in fiat money systems: the ones “closest” to the money printer profit most of newly created coins while those at the end of the money trail have to deal with the reduction in value the market realized in the process. It will be important to watch the evolving monetary policy of Ethereum 2.0 as it is deliberately kept flexible.

**Competition.** All these changes promise a bright future for Ethereum, but the biggest short-term issue that is dragging users and developers to other platforms is not immediately addressed: high to very high transaction fees to run smart contracts for DeFi, NFTs, and other booming markets. Ethereum may be on the right track but may still not win the race against time.

**Proof-of-Stake.** While the mainstream opinion sees Proof-of-Stake winning the energy consumption debate, the more technical debate of whether Proof-of-Stake is as secure and immutable as Proof-of-Work is not so easy to decide.

Different points of criticism have been voiced in the past and we recommend consulting the cited sources for

details. (1) Voskuil<sup>49</sup> argues for the need for a source of security external to the blockchain because otherwise overcoming censorship is impossible should a censor reach the majority stake because it cannot be unseated anymore. (2) BitMEX’s “Guide to PoS”<sup>50</sup> from 2018 already mentions the “Nothing at Stake” problem and the long range consensus attack. “Nothing at stake” means that in the case of two simultaneous blocks, a staker can use the same tokens to stake on both blocks, thus increasing rewards without additional risk to the detriment of convergence of the network to one single next block. In other words, stakers can easily change their mind and back different (fork) chains, while in PoW that would cost a lot of energy, so miners must make a decision and stick to it. Second, the long-range consensus attack problem is the problem that attackers could get hold of an “old” private key that held a large amount of tokens in the past. Simply using it to rewrite history in their favor is easy as there is no “energy wall” preventing catching up with the main chain. The solution, setting regular checkpoints, requires nodes to be online 24/7 or trusting other nodes for syncing when getting back online. (3) Nguyen is worried about Ethereum’s resilience in dealing with worst-case scenarios<sup>51</sup> and gives a summary of PoS critiques<sup>52</sup>, which we lack the space to dive into here.

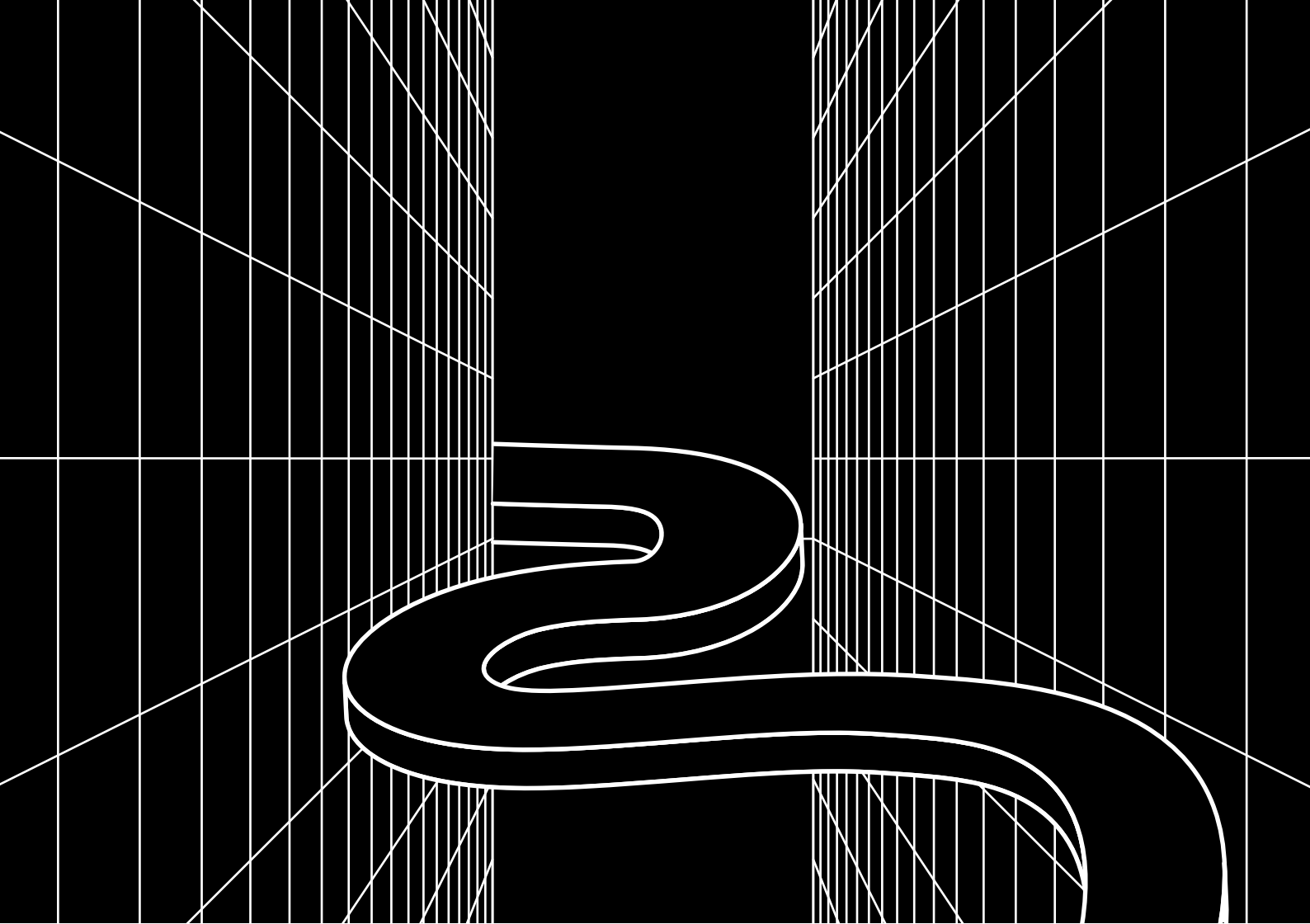
Altogether, a few years into the Proof-of-Stake debate, the final verdict on the security merits is still pending. More research and debate are needed in our eyes to come to a clear understanding, analysis, and decision. The fact that the two largest permissionless blockchain protocols disagree on something as fundamental as the security models of the underlying consensus protocol should be a matter of concern to the crypto community.

## Conclusion

Ethereum has embarked on an ambitious journey by performing the largest transformation of a blockchain project ever attempted. The stakes are high (no pun intended) as Ethereum is by far the largest smart contract platform in the DeFi space, with the most users, developers, funding, and buy-in. The switch to PoS and the separation into dedicated chains/shards is hands down the most ambitious attempt of Layer-1 scalability and will catapult Ethereum into another league if successful. At the same time, the staggering complexity and fundamental concerns raised by some experts cast doubt on the viability of the mega project.

Time will tell. Twelve months from now, we should have a much clearer picture of where Ethereum is going, and which will be the smart contract platform of choice for the crypto community.





Article

# Decentralized Finance: The Road Ahead

Prof. Fabian Schär

- Regulators will identify “decentralization theater” better by separating really decentralized protocols from somewhat centralized ones and thus improving regulatory oversight over the latter.
- Despite all decentralization efforts, the need to have the support of trusted third parties when navigating the web3 space will stay with some users. Institutions that help clients with the nitty-gritty aspects of holding crypto currencies or DeFi instruments will have a market.
- Protocol governance needs to become better; governance tokens alone are not enough. More innovation and experimentation are needed. DAOs need to come up with innovative solutions that allow pseudonymous governance in networks without identity credentials.
- The question in scaling is how centralized exchanges will react to Layer-2 scaling efforts that often lead to more privacy-preserving solutions. Will they ease the load on main chains or lead to rebound effects and increase the overall use of well-working solutions?

Decentralized Finance (DeFi) is one of the hottest topics of 2021. DeFi refers to a blockchain-based ecosystem that employs smart contracts to create financial protocols in an open, transparent, composable and mostly non-custodial way (Schär 2021). The amount and speed of innovation in the DeFi space is exciting and the possibilities are seemingly limitless. Pretty much any metric that tracks DeFi growth has skyrocketed. DeFi has been the cover story of a recent issue of *The Economist* and as a result traditional financial intermediaries have started to pay attention.

However, this short article is not about the current state of DeFi, nor is it a general introduction. Instead, I will look ahead and try to anticipate what is yet to come, i.e., the DeFi-related topics that have a high probability of becoming important in the next year or and beyond. As an academic I feel obliged to add a disclaimer and state the obvious: This is not a scientific article. There is no sophisticated methodology underlying these statements and this is certainly not investment advice. The topics I am going to discuss reflect my observations and are based on my personal expectations.

## Regulation

DeFi regulation is something that is being fiercely debated in the community and reveals that the understanding of what DeFi actually is differs significantly, depending on who you ask. This leads to a situation, where the label “DeFi” is used in a somewhat liberal fashion, including projects that make use of heavily centralized aspects, have external dependencies and special privileges. I expect policy makers and regulators to step in and crack down on solutions that play “decentralization theater.”

Regulation will likely split the DeFi space in two separate categories. On the one hand, there will be protocols that are completely decentralized. These protocols neither can, nor should be regulated. On the other hand, there will be protocols that are somewhat centralized. For these protocols, I expect a move towards regulatory compliance. If they fail to do so, they will be shut down – something that can easily be done, if the protocol is not truly decentralized. As a result, any protocol that currently is in the grey area will most likely have to pick a side and act accordingly.

## Institutional interest

There are several examples of financial intermediaries which are trying to engage with DeFi protocols. What may seem counterintuitive at first does actually make perfect sense. DeFi offers consumers a choice. They can choose to engage with the protocols directly. This option is very positive. However, it would be naïve to assume that everyone would choose to exercise this option and decide to manage everything themselves. Many people would rather pay someone to do this for them. As such, there is a place for financial intermediaries, even if we assume that our base infrastructure will become completely decentralized.

Accordingly, I expect that financial intermediaries will start to explore how they can offer products and services on top of DeFi, and engage with some of these protocols. This exploration may be boosted by an increase in regulatory certainty around the topic, and the fact that some DeFi developers plan to create separate versions of their protocols, exclusively for financial intermediaries. Now, whether this is something that makes sense and if restricted protocols should still be called “DeFi” is up for debate, but putting any ideological discussions aside; from today’s perspective, it seems like something that has a relatively high probability of happening.

## Governance

Most DeFi protocols (or more generally speaking any Decentralized Autonomous Organization – DAO) need

some flexibility to remain upgradable or to change parameters in the contract. Governance systems define how these changes can be proposed, locked-in and executed. This is usually done through a voting mechanism.

DeFi protocols face the issue that they cannot rely on identities. Instead, voting is usually done through governance tokens. If the governance token allocation is relatively concentrated, this can be an issue. In Nadler and Schär (2021) we have proposed an algorithm that allows us to unwrap complex on-chain ownership structures and assign governance tokens to the beneficiary address. We have shown that the token distribution differs significantly across various protocols, but in some cases is highly concentrated.

DAO and DeFi governance will likely be an important topic in 2022. Regulatory pressure may accelerate discussions around this topic and we may see new proposals that are built on a mix of token voting, elected representatives and on-chain identities.

### **Maximal/Miner Extractable Value (MEV)**

When people who are new to the space talk about DeFi, they usually worry about hacks. While hacks certainly are something one should keep an eye on, there is one topic that will likely become more important in 2022, i.e., Maximal Extractable Value<sup>53</sup> or MEV.

The term refers to a relatively broad action set that allows the block proposing entity to extract rent, when successfully assembling a block. Attacks include but are not limited to the act of copying and swapping out profitable arbitrage transactions, sandwich attacks, and the provision of highly concentrated (just in time) liquidity on sophisticated constant function market makers with custom liquidity density functions.

I expect this topic to take center stage and hope that we will see proposals of how the network can respond to these issues.

### **Scalability and Layer 2**

The race to Layer 2 will continue in 2022. Various scaling solutions will get more traction and we will see an increasing amount of transactions that are being executed through roll-ups.

The effect on transaction fees cannot be predicted. On the one hand, the increasing popularity of Layer 2 solutions may reduce the burden on the base layer. On the other hand, Layer 2 may further increase the overall popularity of the system and thereby even increase demand for space on the base layer.

What will be interesting to observe is, how centralized exchanges will respond to the Layer 2 trend. In

particular, direct on- and off-ramps may not only foster the popularity of Layer 2, but also minimize the burden of these solutions on the base layer. Similarly, we will likely see further advancements on the Ethereum roadmap and with the various initiatives that try to increase cross-chain interoperability.

### **Conclusion**

All of this being said, there will be many surprises along the way. What is true for most things in life also counts for the blockchain space: Expect the unexpected.

Yes, there are some DeFi topics that seem to be obvious candidates to enter center stage in 2022. But there will always be topics that seemingly came out of nowhere and will have a lasting impact on the space.

## Article

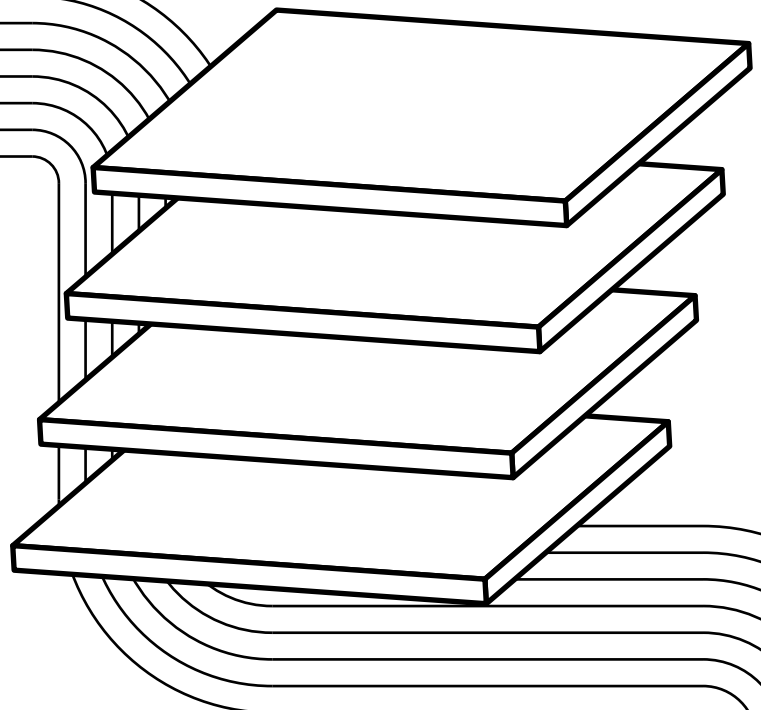
# From Nodes to New Asset Class - The Evolving Crypto-Financial Tech Stack

Ian Simpson

■ The crypto-financial tech stack has reached a level of sophistication and professionalism that helps professional and institutional investors consider cryptocurrencies an investable asset class.

■ Trading and custody solutions for crypto assets mirror the general functionality of traditional capital market infrastructure, but present unique challenges.

■ Adding DeFi to the existing tech stack structure may prove difficult and lead to trade-offs between usability, decentralization, and market demand.



The Bitcoin Faucet was ingenious.

Launched by Gavin Andresen in 2010, the website gave away 5 BTC per day to every person who came along. The main purpose was simple: get as much bitcoin into the hands of as many different people as possible.

Today, the exchange of bitcoin and cryptocurrencies has exploded from a mere trickle to become a large global market.

But a widening crypto world brings with it both challenges and opportunities. Many early adopters of bitcoin and other cryptocurrencies had a keen interest in the technology, but the latest generation of investors is further removed from the fundamentals. They may have a strong belief in decentralization, but only a minority of them will ever run their own full-node or even have a mobile wallet.



## LOTHAR CERJAK

Lothar Cerjak is Head Trading and Brokerage at Bitcoin Suisse.

### **Are crypto markets becoming more and more like traditional markets, also on the technology side? Is this a good thing?**

Generally, we can observe an increasing level of professionalism in the crypto trading industry. The infrastructure of crypto exchanges and liquidity providers has constantly been improving and this - combined with higher trading volumes from large trading institutions and increasing trading automation - has brought more efficiency to the markets, which is good. Nevertheless, due to the decentralized landscape and the high paced innovation of the industry, the crypto markets will likely not become as technologically synchronized as traditional markets.

### **Can we envision a future where centralized and decentralized crypto exchanges are more closely connected? Why or why not?**

The biggest part of the market liquidity is currently available on centralized exchanges. However, the interest for decentralized finance applications and the capital deployed therein has increased exponentially over the last 18 months. It can also be observed that centralized exchanges are increasingly investing into building DeFi products and infrastructure. This indicates that a way is being paved for more interconnectivity between centralized and decentralized trading venues. Nonetheless, there is certainly more regulatory clarity required for DeFi applications to be fully embedded in the trading procedures of regulated brokerage entities. In addition, the increasingly important topic of scalability is expected to lower barriers to entry for decentralized exchanges by tackling the currently elevated transaction costs, hence making them available for a wider audience.

### **Can the integrated technology and offering of major crypto exchanges like Binance, Coinbase or Kraken really provide the best possibilities for people trading cryptos? Why or why not?**

As the crypto exchanges are very diverse in terms of liquidity, domicile, regulatory status, technology infrastructure and client base it is highly recommended to operate through a broker and resilient partner such as Bitcoin Suisse, which is connected to multiple trading venues to ensure best execution for trades. When trading volatile assets in the crypto market it has proven to be a wise choice to not only rely on one exchange but to 'trade smart' - in other words letting a trading system source the best liquidity and conditions for trades with a 'best execution' service.

They just want easy exposure to the upside of a nearly \$3 trillion (and growing) market.

This evolution towards being a completely new asset class also has significant infrastructure implications. As markets become more sophisticated, that base-layer blockchain technology first outlined in the Bitcoin whitepaper<sup>54</sup> is getting connected to other infrastructure which enables the increasingly complex financial products being built around crypto assets. From global spot trading venues with multi-billion dollar volumes to derivatives exchanges and exchange-traded products of various flavours, the tech implications of crypto's move into the so-called "big leagues" are enormous.

It gives rise to several questions:

How is the current tech stack behind crypto financial services developing? What do investors require from the services they use to access crypto? How will DeFi get integrated into the current web of financial service solutions being built for crypto assets?

Perhaps most importantly, what does the evolving crypto-financial services tech stack mean for investors and users - both individual and institutional?

### **Trading - from peer-to-peer to financial marketplace**

Since the infamous hack of the Mt. Gox exchange<sup>55</sup> in 2013, the technology used to trade cryptocurrencies has been one of the main focus points of the fledgling crypto-financial services industry. At the time of its founding in 2010, Mt Gox seemed a godsend and ended up processing over 70% of all bitcoin transactions at the time of its failure.



## MARKUS PERDRIZAT

Markus Perdrizat is Head Product Management and Custody at Bitcoin Suisse.

### **Custody of crypto assets is getting more and more sophisticated – is it also getting more secure, actually? Why or why not?**

Since the beginning of crypto assets, custody has been a high-risk business. We've all heard stories of people whose assets were stolen, or who lost the private keys required to unlock the digital assets. Billions have been lost that way. However, we established a new level of custody security when we were one of the first custodians to offer HSM-based enterprise custody in February 2018 with the Bitcoin Suisse Vault. Since then, the situation has improved quite a bit for assets that are stored with professional custodians.

### **How do you see the integration of hyper-secure storage and more “active” crypto-financial services like trading and staking? Can you give an example of how this works?**

You know, Bitcoin and crypto was a case for early adopters who just believed that Bitcoin will have more value in the future, for a variety of very good reasons. In the meantime, we see thousands if not millions of developers building decentralized financial applications on blockchains that mimic all the functions of the traditional financial services world. With this has come the expectation that also crypto capital needs to earn a yield. Your money needs to work for you, just like in the traditional world. Let's take the case of staking, which is actually similar to giving somebody a credit and getting it back with interest. Except that with blockchain and staking, you lock up your crypto capital to increase the transaction security of the network, and the network pays a handsome reward for that.

### **Why is it important for banks and other financial institutions to get started with custody of digital assets now?**

Digital assets have reached a market size that it's clear they can't be ignored. At the same time, crypto technology has reached a level of stability and maturity that make it possible for even a relatively conservative financial institution to start working with crypto companies. Bitcoin Suisse started developing our technology stack 8 years ago, and we now have 100 people working on information technology. Custody allows a bank to establish the required capabilities to deal with digital assets from a regulatory and cyber risk perspective and get more familiar with digital assets before adding more complicated products to the mix.

But the theft of 850'000 BTC highlighted the technical fragility of a centralized exchange like Mt Gox. In essence, these trading venues take upon themselves most (if not all) of the tasks that are carried out by an array of providers in traditional markets: account handling, custody, order matching and execution as well as settlement and clearing.

Like traditional market infrastructure providers, centralized crypto exchanges rely on an order book and a high-speed matching engine to bring together buyers and sellers. These have improved in sophistication and execution power such that today the largest exchange worldwide, Binance, is purported to process more than USD 750 billion in trading volume.

But while the “integrated nature” of crypto exchanges such as Coinbase, Binance and Kraken allows for a relatively smooth user experience, the custodial nature (private keys of crypto assets are held by the exchange, not users) and the fact that assets are predominantly held in pooled custody with those of other clients, has made them targets - in more ways than one.

Centralized exchanges face the permanent threat of hacks. They can also come under pressure from high usage during peak trading times.<sup>56</sup> And this has led to criticism - including strong words from Ethereum co-founder Vitalik Buterin, who famously said in 2018<sup>57</sup>: “I definitely hope centralized exchanges burn in hell as much as possible.”

One response to the weaknesses of centralized, custodial trading venues was the rise of decentralised exchanges<sup>58</sup> (DEXes), of which Uniswap, Pancake Swap, and Curve are some of the more prominent examples. Here market participants can pool their assets to create liquidity and market-making is accomplished with the aid of a blockchain-based protocol and smart contracts. Fees can be automatically distributed to users who provide liquidity.

Proponents point out that decentralized exchanges adhere more to the original principles of blockchain technology with peer-to-peer trading, lending and borrowing taking place in a trustless way. In this sense, they represent a “return to the roots” of bitcoin as a peer-to-peer system.

While user experience was somewhat difficult in the beginning, DEXs have greatly improved over the past year and DEX volumes have continued to grow<sup>59</sup> as have new innovations beyond simple swapping of assets. The introduction of Uniswap's V3<sup>60</sup> - with more flexibility for the allocation of capital and a new fee structure - now opens up more possibilities, while other exchanges such as dydx<sup>61</sup> offer decentralized options trading.



Despite these innovations in decentralization, centralized exchanges remain the dominant players for trading of crypto assets.<sup>62</sup> New players such as FTX<sup>63</sup>, which saw its market share grow dramatically since May 2020<sup>64</sup>, are also getting in the game and indications are that the space could expand even more with fintech giant Revolut purportedly aiming to build its own exchange.<sup>65</sup>

With so many to choose from, the market infrastructure for crypto assets remains relatively fragmented and the proliferation of DEXes adds to this challenge. With liquidity spread across different venues, price differences may appear and traders lose out.

However, a number of companies, such as CoinRoutes<sup>66</sup> and AlgoTrader<sup>67</sup> have already developed sophisticated smart order routing services which help connect the order books of centralized exchanges to avoid single-exchange lock-in. The same is also happening on the decentralized side of the trading space, with DEX aggregators, such as 1Inch.Exchange, ParaSwap and Tokenion growing in popularity.<sup>68</sup>

These services help bridge the broad global market and even enable best-execution services<sup>69</sup> to allow large trades without affecting price in a negative way.

### **Crypto custody - how to hodl**

The custody of crypto assets has also experienced a significant evolution since the early days of the Bitcoin Faucet. And here again, there is evidence to indicate that the industry is developing strong infrastructure worthy of a new global asset class.

While the basis of crypto custody is simple - hold the private key safely and securely - the technology used to do so may vary, and does, depending on user needs. Paper wallets and rudimentary desktop wallet applications may have offered the power of personal control for early crypto holders, but they do not meet the requirements of institutional investors with billions in crypto assets to safeguard.

Crypto custody as part of the trading process is especially important. Pooled custody of client assets on exchanges has sometimes exposed them to hacks, which according to certain estimates<sup>70</sup> reached an average of \$2.7 million per day in 2017 and 2018. While most blockchain protocols themselves have remained secure, the 2nd and 3rd layers of the technology stack used to administer crypto exchange infrastructure, client data

and the keys of so-called “hot” (online) wallets can often be vulnerable.

For this reason, crypto-financial service providers were quick to start developing more secure solutions. Starting with the hand-held Trezor wallet, cold (offline) storage of cryptocurrencies moved into more sophisticated systems. Some employ Hardware Security Module (HSM)-based systems, while others use Multi-Party Computation (MPC) to make sure private keys do not need to be physically stored in their entirety nor are revealed to potentially malicious parties.

This suits the needs of institutional investors much better - for several reasons. First, such systems are designed with multiple layers of security and the technology used to keep private keys from being exposed, for instance HSMs, has been battle-tested for other use cases beyond cryptocurrencies. Second of all, there is the possibility to engage multiple persons in the process of transferring assets, something that is often necessary in financial institutions where multiple approvals or levels of oversight are needed. And thirdly, these systems can be audited to ensure their quality and integrity - a key requirement for banks, asset managers and other professional organizations.

With increasing demand among more sophisticated investors and institutions, a growing number of players have developed their own systems for integrated digital asset custody. The world's largest custody bank BNY Mellon has invested heavily<sup>71</sup> in adding crypto asset support over the last year, with the stated aim of building a custody system at the same level as it uses for the more than \$40 trillion in traditional assets it currently has under custody.<sup>72</sup> The latest edition of PwC's Crypto Hedge Fund report<sup>73</sup> also highlights the fact that crypto funds are moving towards closer integration of custody solutions within their own infrastructure.

One area that may drive demand for high-quality crypto custody services - and force even more development of the crypto-financial tech stack - is the trend towards holding bitcoin and other crypto assets in companies' corporate treasuries. With strong advocates such as MicroStrategy and Square, which both have bitcoin on their balance sheet, the trend continues to gain attention<sup>74</sup>, especially as inflation and low-interest rates persist.



## **Staking – towards crypto-native financial services**

The new frontier of the crypto-financial tech stack begins with the addition of support for services that are native to blockchain-based assets. One of these is staking.<sup>75</sup>

Early interest in popular proof-of-stake blockchains such as Tezos and Cosmos gave rise to services allowing crypto asset holders to earn staking rewards without the need to operate staking nodes or maintain infrastructure. This was a boon for the first wave of non-technically oriented investors in crypto assets.

The launch of Polkadot<sup>76</sup> (and previously its canary network Kusama) as well as the Beacon Chain of Ethereum 2<sup>77</sup> in 2020 accelerated the interest in participating in proof-of-stake blockchain networks. This has translated into a current market capitalization<sup>78</sup> (at time of writing) of all major staking currencies valued at nearly \$500 billion and the total value staked reaching approximately \$380 billion.

Several major exchanges such as Binance, Kraken and Coinbase have built staking services into their client offering. Bitcoin Suisse also offers an integrated service<sup>79</sup>, which connects trading accounts directly with staking accounts.

But whereas trading and custody of crypto assets closely mirror the operations of traditional markets, staking services present new challenges. Assets are staked and locked (making them unavailable for trading) for different periods of time, depending on the protocol. Rewards may be distributed at different rates and correct handling of validators and staked assets is essential to maximizing rewards.

In short - this level of the crypto-financial services tech stack requires a significantly higher level of technical acumen and more thought-through processes.

The building of an integrated tech stack that includes staking services also resurfaces the topic of custody. Staking services may be both custodial (private keys are held by the service provider) and non-custodial (keys held by the user/customer). Many large staking service providers, especially crypto exchanges and brokers such as Bitcoin Suisse and Kraken operate custodial staking services. On the one hand, this approach streamlines customer experience and removes a technical burden from clients. On the other hand, it requires a significant level of trust in the professionalism and know-how of the service.

In this sense, the link between custody and staking - along with many other emerging crypto-native financial services - is a key linchpin in the growing technical stack of crypto-finance. It is also likely to evolve quickly as

new proof-of-stake blockchain networks 'go live' and demand for staking services grow.

The combination of highly secure custody services and crypto tech know-how has made it possible for institutions to begin exploring the potential of staking for their clients. ConsenSys's CodeFi staking service<sup>80</sup> is one offering specifically aimed at larger firms. Multiple banks, including some based in Switzerland, have launched staking products for their clients. In the current low-interest-rate environment, being able to earn returns of 6, 10 or even 13 percent on crypto assets<sup>81</sup> is extremely attractive.

## **The full(er) crypto stack - future prospects**

Since the days of the Bitcoin Faucet, technical infrastructure and tooling for crypto assets has developed significantly. Professional custodians for secure storage, multi-exchange brokerage system for best execution trading and increasingly easy-to-use staking services- the crypto-financial tech stack has never been more robust - and also diverse.

As a result, more professional investors are comfortable thinking of cryptocurrencies as a new, investable asset class. With strong tech and professional providers in place, exchange-traded products (ETPs) and exchange-traded funds (ETFs) are being launched at a rapid rate, with assets in such products tripling to over \$9 billion by some reports.<sup>82</sup>

Across the global landscape, tools and systems to support crypto asset markets are becoming more integrated and user-friendly. It is now possible for both private clients and institutions to access prime brokerage services, control assets from secure, cold storage and even stake those assets and earn rewards, all through a clean, easily manageable interface.

Re-staking of crypto assets, one-click bonding and un-bonding and even tokenization of locked staking coins to enable trading are all examples of how a full-stack approach is benefiting clients and bringing crypto, at least from an accessibility point-of-view, to the level of more well-known asset classes.

But crypto tech is not slowing down. The explosion in decentralized finance (DeFi), with more than \$100 billion now in Total Value Locked (TVL)<sup>83</sup>, has brought with it many more opportunities. Most of these, such as yield farming, lending and even decentralized payments are inherently crypto-native and unique to the blockchain world. This will challenge the tech stack of crypto-financial service providers even further.

To meet the next wave of innovation, more tools and tech will need to be built. Some already are, with popu-



lar retail wallet MetaMask having recently launched an institutional version<sup>84</sup> to offer wider access to DeFi and decentralized applications (dApps). Others, like decentralized lending protocol Aave have announced enterprise-focused versions<sup>85</sup> of their platform. This may lead to more access to decentralized finance protocols and the activity taking place on them, but it may also lead to the packaging of DeFi into more traditional-like structures and eventually compromising on decentralization.

In the end, the flow of innovation in crypto-financial technology continues as strongly as ever, and the tech stack continues to grow, challenging some norms, while also adhering to others.

For many new investors, it may be just as easy to get into bitcoin and crypto today as it was to take BTC from the Bitcoin Faucet - which is a good thing. Those who wait for the ideal user experience or institutional services, however, may just miss out on some early trends like DeFi (or whatever comes next) while the tech stack catches up.



**What are the main technical challenges for people who want to stake on proof-of-stake blockchain networks?**

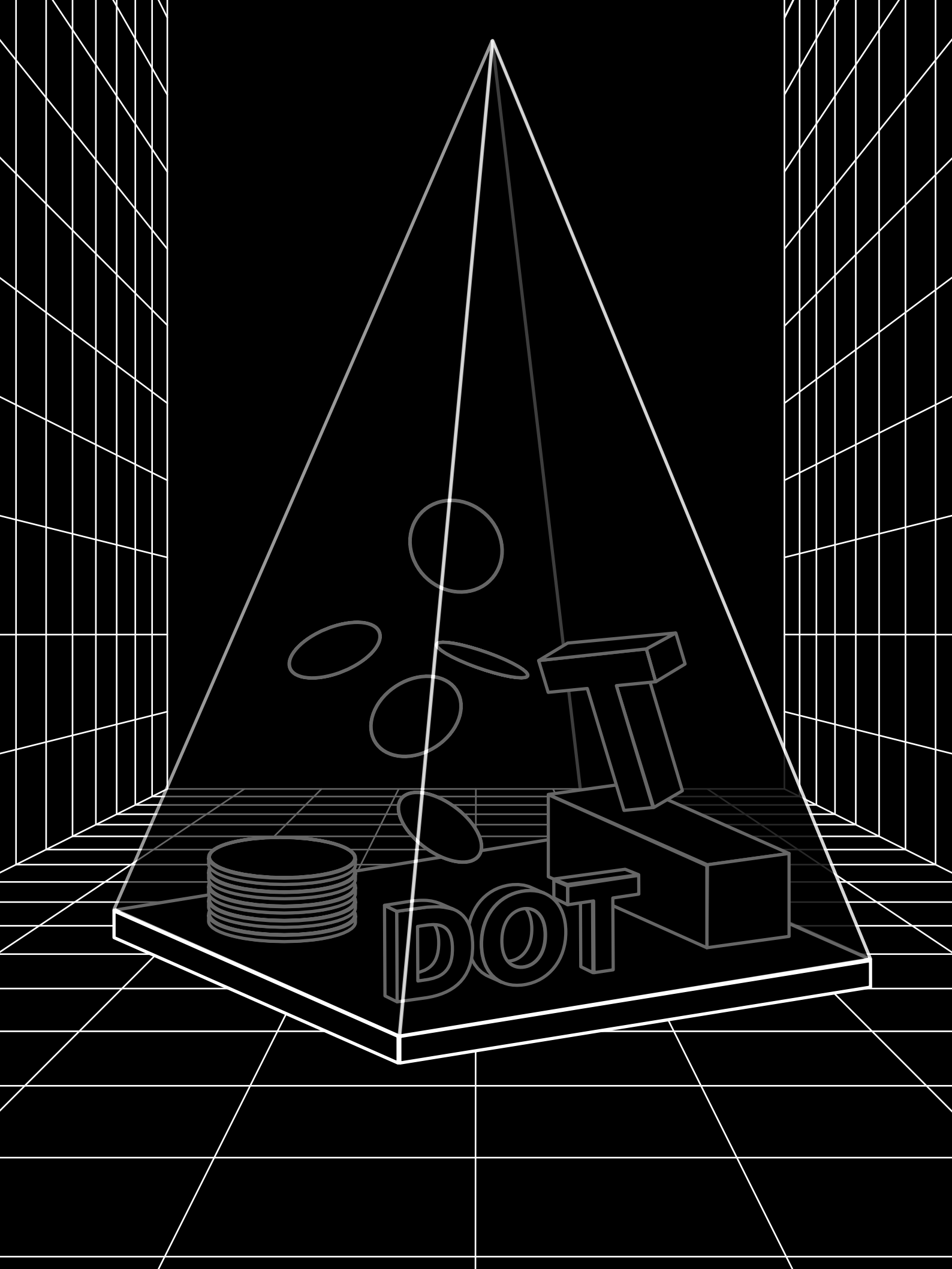
Proof-of-stake puts your stakes at risk if you are not an honest and reliable validator in the blockchain network. It's easy to decide to be an honest validator, which means that you don't intend to attack or cheat the blockchain. However, there are technical challenges in being a reliable validator: you need to be up to date, i.e., running the right validator software, you need to show up, i.e., have a very high uptime and you need to know what to do when things get shaky, i.e., react quickly and correctly in case of network instabilities or similar events. So, the technical discipline of running validators is the combination of data centre operations combined with deep insights and links into the technology and community of staking projects.

**Does the industry trend from proof-of-work to proof-of-stake blockchains bring advantages in all aspects or are there any arguments which might limit this trend?**

The trend towards proof-of-stake blockchains will certainly continue and lead to a range of blockchains with slightly different designs, strengths and resulting use cases. These range from Decentralized Finance to the Internet of Things and other applications. The one exception which will likely not follow the trend is Bitcoin. The main argument is its stability, which can be derived from the simplicity of the proof-of-work algorithm in combination with a track record of more than 13 years. Proof-of-stake blockchains are more complex to design and therefore it is harder to assess their stability under extreme conditions or edge cases such as a strong concentration of assets with a few owners. My expectation is that overall, this trend will continue with this one exception.

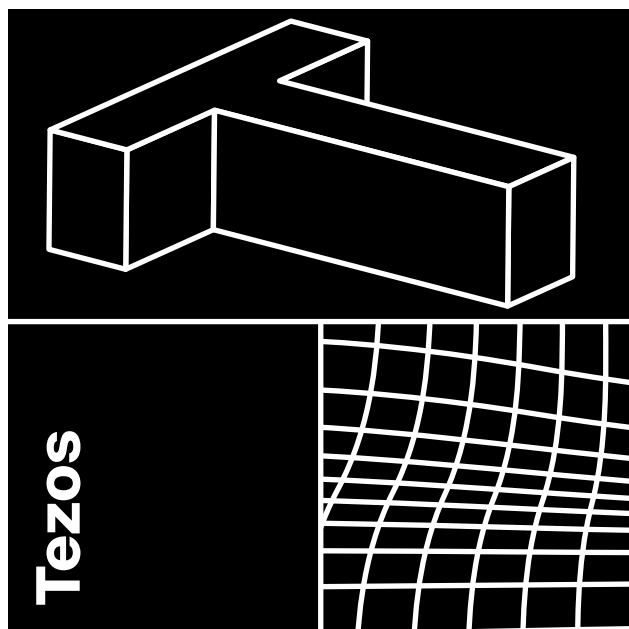
**Do you think that banks and traditional financial institutions may eventually set up their own staking services? Why or why not?**

I very much expect that banks and traditional financial institutions will eventually offer staking services. It could even happen in an integrated way that is almost invisible to the clients - like cash accounts which, in some countries, are implicit money markets, i.e., interest bearing accounts. Incentive-wise it's a give and take: the ones holding a currency should use it to secure the network and are incentivized to do so through resulting rewards. The institutions operating the blockchain systems get a service fee which is deducted from the reward. It's all about the balancing of incentives and those protocols and institutions striking the right balance will succeed and grow.



Spotlight

# Protocol Updates and Outlook



## Tezos

### What progress has been made in 2021?

The Tezos ecosystem continued to grow in 2021. With its built-in “self-upgradeability”, the Tezos protocol completed four upgrades in 2021 (Edo, Florence, Granada and Hangzhou) further improving tooling, core functionality which lowered gas consumption for smart contracts and doubling the transaction speed, and more.

These improvements have directly resulted in contract calls increasing from over 150,000 in January to nearly 6 million in September.

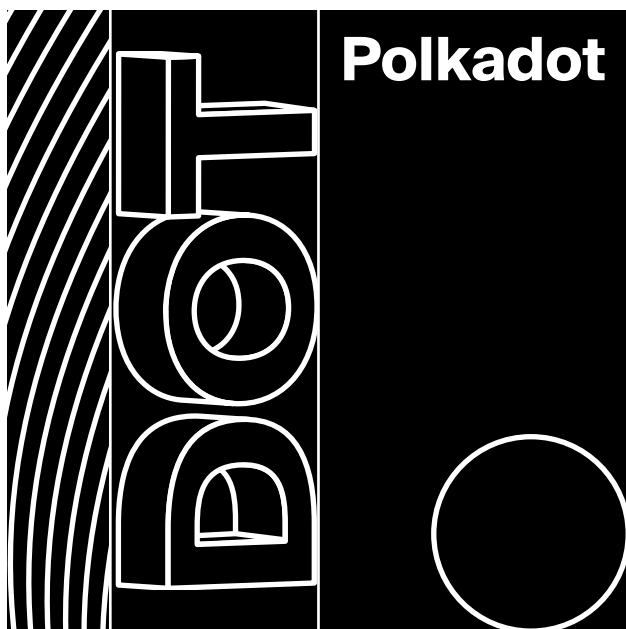
Tezos has attracted a diverse NFT community of artists, collectors, and builders, including rapper PitBull.<sup>86</sup> Meanwhile, Tezos’ nascent DeFi ecosystem has grown to include a range of yield farming platforms and multiple AMMs and DEXs, most recently with the launch of DeFi protocol Plenty.<sup>87</sup>

Several notable brands chose to build solutions on Tezos including Formula 1 racing teams Red Bull Racing Honda and McLaren Racing, as well as Société Générale and music NFT platform OneOf.

### What is coming up in 2022?

The momentum in adoption that Tezos has seen from NFTs is likely to continue, as artists, collectors, brands and more continue to build the future of digital engagement on the blockchain. The topic of the Metaverse continues to emerge as a focus for brands around the world as energy-efficient NFTs, coupled with low transaction costs, allow for broad large-scale NFT powered initiatives that can create further opportunities for Tezos as a leading Proof-of-Stake blockchain.

If 2021 was the year of the NFT, 2022 may be the year of the Metaverse, with NFTs gaining mass adoption through utility via social, gaming and more. The Tezos blockchain and its technology stand to benefit as users value its energy-efficiency and negligible transaction costs.



## Polkadot

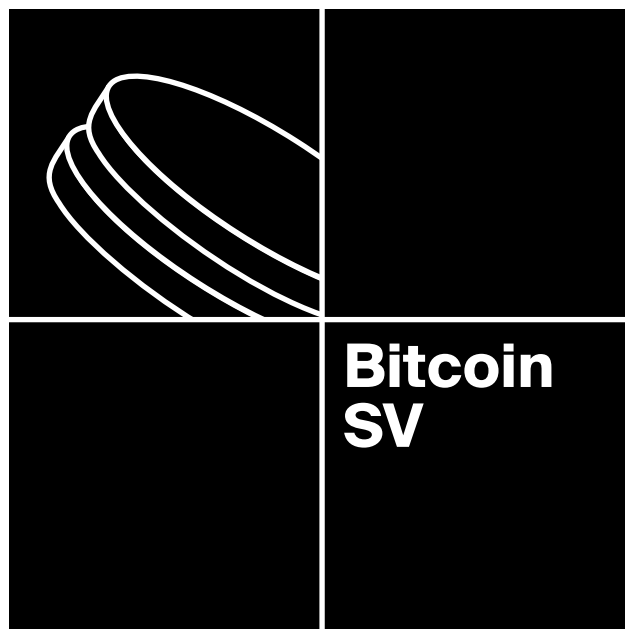
### What progress has been made in 2021?

The year 2021 saw the launch of the first parachains on both Kusama and Polkadot, an important step for the development of the Web3 ecosystem. In March 2021, Statemint<sup>88</sup> was proposed with the goal of adding a common-good parachain to the Polkadot network in order to support generic assets. After Statemint, the Kusama instance of Statemint, was launched as the first fully-functional parachain on Kusama in June, it was further upgraded in July.<sup>89</sup> The official launch of parachain auctions on Polkadot, came after the community accepted Motion 118<sup>90</sup>, which set out the schedule of parachain auctions, spanning 2021 and 2022. The first auctions saw the Acala Network win the first auction<sup>91</sup> in November with a total of 32,515,989.5 DOT contributed, followed by Moonbeam and Astar Network. On Kusama, a total of sixteen parachain teams registered crowdloans for the second batch of auctions and received contributions from 37,225 unique accounts (49,766 total across both batches of auctions) totalling 1,348,589 KSM in contributions.

### What is coming up in 2022?

The planned rollout of parachain auctions continues in 2022, with the final auction based on Motion 118 scheduled to commence on 3 March 2022. Kusama parachain auctions also continue, with the current round of slots open up to 11 May 2022.<sup>92</sup> With the rollout of parachains, the original vision of the Polkadot network comes to

a completion based on its road map. Future upgrades, including full-featured XCMP and parathreads, are envisioned, but will be implemented via the network's governance mechanism.



## Bitcoin SV

### What progress has been made in 2021?

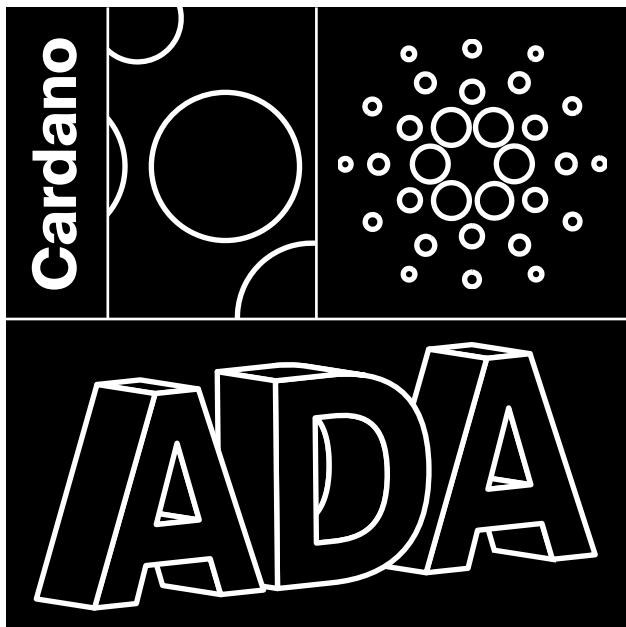
2021 has been a busy year for the BSV blockchain and ecosystem, with several technical milestones achieved. In May, there were nearly 4 million transactions recorded in one day, helped by a single block mined by Taal containing 1.3 million transactions<sup>93</sup>, matching a previous record. Multiple days in August saw over 2 million transactions added to the chain, with the iGaming company Cryptofights generating many of these transactions. On August 16, the BSV network processed a record 1.247 GB size block<sup>94</sup> – a block not just significant for its size, but for its underlying economics: it was the first time that the transaction fees earned (6.33 coins) were higher than the fixed subsidy amount (6.25 coins) for the block. The record for the largest block was subsequently broken<sup>95</sup>, with the world record – achieved on the BSV network – now standing at 2 GB.

Later in the year, on September 3, the BSV blockchain became the most data-rich blockchain and since that time has grown to a total size of over 2 TB. Importantly, despite the increased traffic and demand on the network throughout 2021, the median transaction fee has remained under 1/50th of a U.S. cent throughout the year.

### What is coming up in 2022?

There are strong expectations for the wider BSV ecosystem in 2022, as well as major technical milestones on the network roadmap to achieve. The most important moment expected to occur next year is the release of Teranode – a multi-machine implementation of the Bitcoin SV node software that utilises horizontal scaling to unlock increased capacity on the network (a live demonstration at CoinGeek Zurich earlier this year processed more than 50,000 transactions per second). What will be interesting is how this additional capacity to the network is utilised.

The year 2021 saw companies leveraging the BSV network for a host of activities. nChain released its platform, Kensei, in July 2021, and signed up company and Crucial Compliance, both firms enhancing their existing offerings by leveraging blockchain's immutable data integrity functionality. In 2022, it is expected to see greater understanding and acceptance of the broad applicability of data integrity, especially in iGaming and CBDC solutions.



## Cardano

### What progress has been made in 2021?

Recent hard forks, such as adding native tokens in March and smart contract capability in September, have brought a wide range of users into the Cardano ecosystem. Aggregators<sup>96</sup> of Cardano projects estimate there are approximately 274 projects in development or actively running on

the Cardano network. These projects range from insurance, payments, lending & borrowing to wallets, stablecoins, decentralised finance, and decentralised exchanges.

Cardano now has over 2 million native assets.<sup>97</sup> This has brought multi-asset support to the ecosystem, which allows users to create custom tokens and carry out transactions directly on the Cardano blockchain. All of this has led to the rapid growth in transaction volumes in the past year, even exceeding a milestone of 22 million transactions<sup>98</sup> and more than 2 million native wallets.

### What is coming up in 2022?

Cardano's roadmap follows five phases, with three done and two left. Basho and Voltaire are focused on scaling the network to billions of enterprise grade transactions and growing governance on chain.

The next year is about realizing the full potential of Cardano as the focus transitions from early deployment and feedback to optimization and scale. As core components – including wallet connectors and the Plutus Application Backend (PAB) – are finalized and integrated into mainnet, Cardano aims to see even greater growth in network activity.

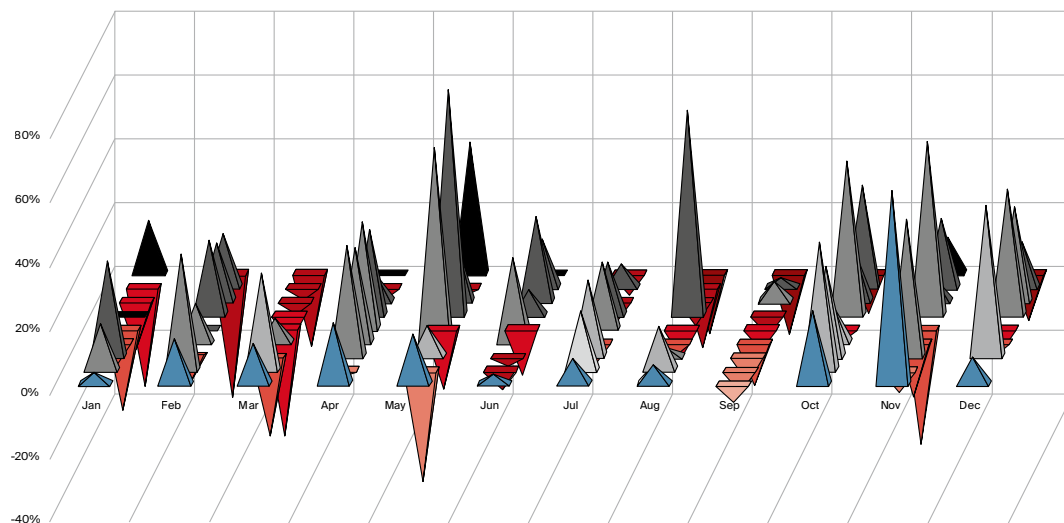
Additionally, Cardano is on a trajectory towards creating native assets which will differ substantially from other blockchains. In the future, a native asset on Cardano may come with its own governance features, which have the same security guarantees as ADA, the Cardano blockchain's native cryptocurrency. There are also plans to extend the Distributed Innovation Fund, Catalyst, and its voting mechanisms from 292 000 votes in its latest funding round to 400'000 in the next round.

*The Protocol Updates and Outlook section was produced support from Dr. Michaela Pettit (nChain), Reid Yager (Blockhaus/TQ Tezos) and Renagh Mooney (Cardano Foundation).*

# Vires in Numeris

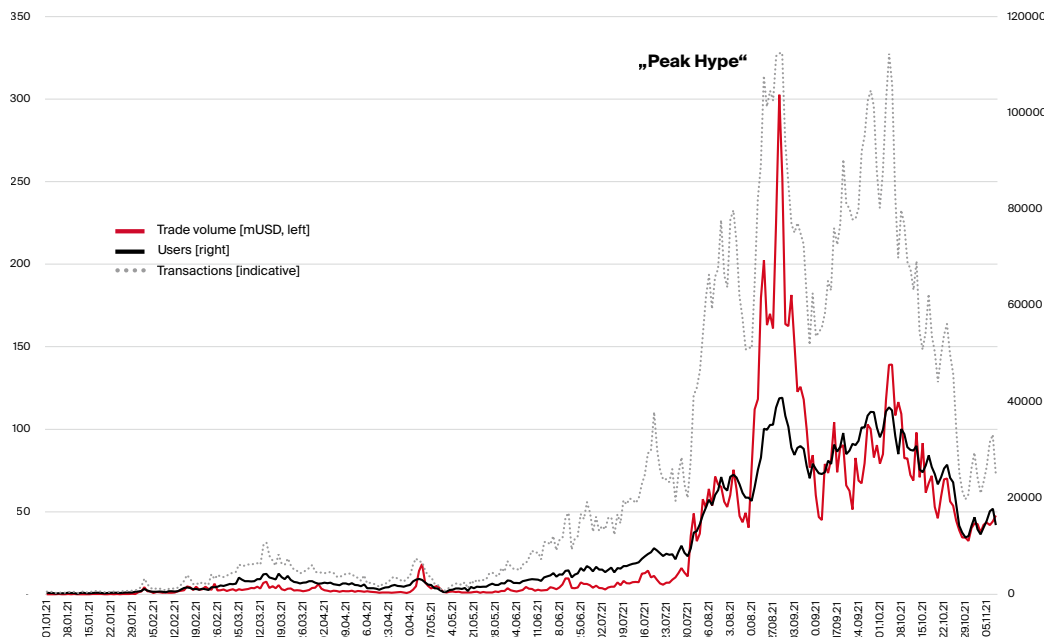
Together with our colleagues from the Bitcoin Suisse Trading Desk, we created a few charts that we hope you find as thought-provoking as we did for 2022 and beyond.

**Sell in May? Bitcoin monthly returns over the years (grey/red) and on average (blue)**



*Historically, the strongest month is November and the weakest September. The yearly average is +167%. DATA: bitcoinmonthlyreturn.com*

**Big waves on the “Open Sea”. The largest marketplace for NFTs (Jan-Oct 2021)**



*Up to the peak, the user base doubled while trade volume tripled. Have you noticed how transaction numbers show two equal peaks? DATA: dappradar.com*

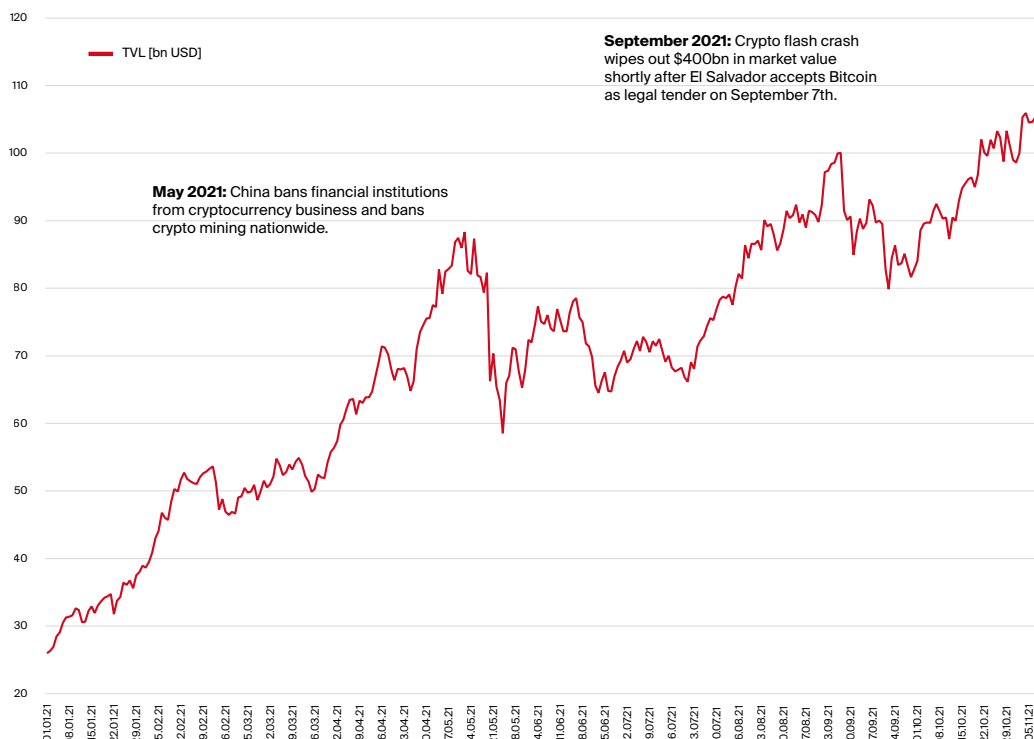


## Chains changing hands. Top 9 tokens traded on Bitcoin Suisse Online (Jan-Oct 2021)



*Note the immense growth rates across the board. Bitcoin, with over 200% growth, is at the bottom of the chart. DATA: Bitcoin Suisse Trading Desk*

## Money at work. The Total Value Locked in Decentralized Finance protocols (YTD 2021)



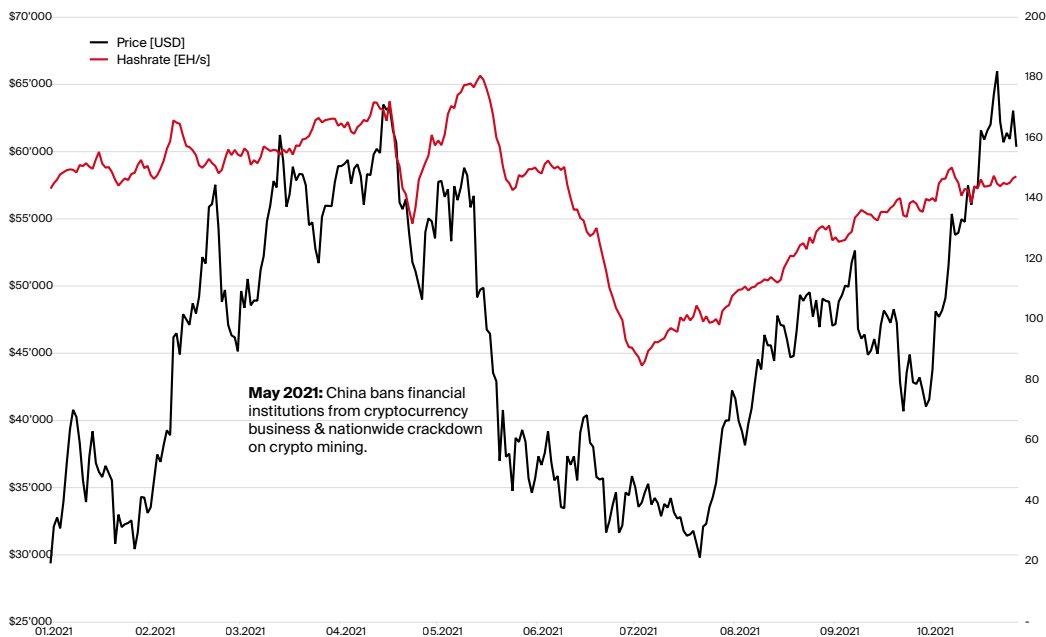
*Despite two major drawdowns, the TVL keeps on rising, ending up 4 times higher. DATA: defi-pulse.com*

## New chains on the block. Performance of Ethereum competition on Layer 1



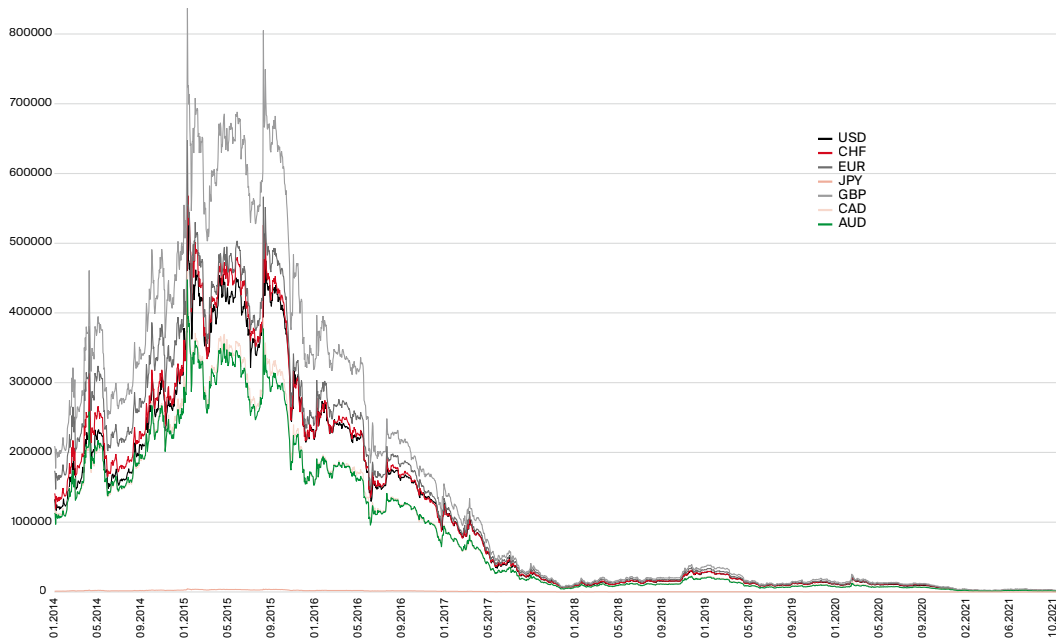
*In only one year, several competing platforms outperformed Ethereum. Ethereum's double challenge in 2022: master the Merger and hold steady against them. DATA: coingecko.com, finance.yahoo.com*

## Probably nothing. The Great Mining Migration out of China



*The ban removed 50% of hashrate, reducing Bitcoin's network security significantly. Yet, within half a year, it nearly recovered. What are the geopolitical consequences for nations who want to take control over the Bitcoin network? DATA: block-chain.com, finance.yahoo.com*

## How much is that in bitcoin? Oh, so little?



*The 1-unit price of major reserve currencies (1 USD, 1 EUR, etc.) measured in bitcoin satoshis as unit of account. DATA: blockchain.com, finance.yahoo.com*

## Bitcoin - more than worth its weight in gold?



*The price of an ounce of gold, the epitome of stable money for millennia, measured in bitcoin as unit of account. DATA: blockchain.com, finance.yahoo.com*

# Contributors



## **Ignazio Cassis**

Ignazio Cassis is the President of the Swiss Confederation and Switzerland's Foreign Minister. Born in the canton of Ticino, the trained doctor has been a member of the national government since 2017.



## **Dr. Marcus Dapp**

Marcus Dapp joined Bitcoin Suisse AG as Head of Research in September 2021. He spent most of his professional life in academic research (ETH Zürich, Uni Berne, TU Munich, fortiss Munich) and teaching (Golden Owl award 2012, ETH D-GESS) with side trips to the public (IT strategy City Government Munich) and the NGO sector (co-founding board member, Open Knowledge Germany). Marcus studied computer science and technology management at ETH Zürich and received his PhD in 2009. His interest in the effects of digitization on economics and society led him to explore a wide gamut of topics over the years; spanning from open digital innovation, intellectual property rights, open source and data to finally peer-to-peer crypto currencies.



## **Alex Gladstein**

Alex Gladstein is Chief Strategy Officer at the Human Rights Foundation. He has also served as Vice President of Strategy for the Oslo Freedom Forum since its inception in 2009. In his work, Alex has connected hundreds of dissidents and civil society groups with business leaders, technologists, journalists, philanthropists, policymakers, and artists to promote free and open societies. Alex's writing and views on human rights and technology have appeared in media outlets across the world including, BBC, CNN, The Guardian, The New York Times, TIME. He has spoken at universities ranging from MIT to Stanford, presented at the European Parliament and U.S. Department of State, and participated in Singularity University events around the world, where he serves as faculty and lectures on bitcoin and the future of money.



## **Pascal Halter**

Pascal Halter joined Bitcoin Suisse in June 2021. Previously, he was working for over two years at a Zug-based commodity trading firm, where he was managing the company's physical positions and valuations as well as commercial reporting. He holds a Master's degree in Energy, Trade & Finance from Cass Business School in London.

**Sander Jorgensen**

Sander Jorgensen joined Bitcoin Suisse AG in the beginning of March 2018. He graduated in 2017 from the Higher Commercial Examination Programme, since then he has been working fulltime in the crypto community.

**Prof. Fabian Schär**

Fabian Schär is Professor for DLT and FinTech at the University of Basel and the Managing Director of the University's Center for Innovative Finance. He advises various global institutions on these topics and published a book with the MIT Press.

**Ian Simpson**

A veteran of multiple companies in multiple countries, Ian Simpson joined Bitcoin Suisse in August 2019 after serving as Head of Communication at the Crypto Valley Association where he supported the association's growth to over 1400 members. Prior to that, he helped grow the blockchain startup ecosystem in Switzerland at CVVC and scale up a leading provider of advertising and marketing technology solutions at Clearcode S.A. in Wroclaw, Poland. He studied history and French at Middlebury College in Middlebury, VT and has been a contributing writer to CoinDesk, a leader in blockchain news.

**Marlon Turgay**

Marlon Turgay joined Bitcoin Suisse as an intern in early September 2017. During his internship, he acquired a thorough understanding of cryptocurrencies. After his military service, Marlon rejoined Bitcoin Suisse in June 2018 as Junior Trader. Marlon holds a maturity diploma in Economics & Law which he completed in 2017.

# References

- [illegible]



52. <https://hugonguyen.medium.com/work-is-timeless-stake-is-not-554c4450ce18>
53. <https://www.bitcoinsuisse.com/research/decrypt/arbitrage-and-frontrunning-in-defi>
54. <https://nakamotoinstitute.org/bitcoin/>
55. <https://www.wsj.com/articles/BL-263B-352>
56. <https://www.reuters.com/technology/binance-trading-volumes-soar-despite-regulatory-crackdown-2021-10-04/>
57. <https://techcrunch.com/2018/07/06/vitalik-buterin-i-definitely-hope-centralized-exchanges-go-burn-in-hell-as-much-as-possible/>
58. <https://defiprime.com/exchanges#ethereum>
59. <https://www.theblockcrypto.com/data/decentralized-finance/dex-non-custodial>
60. <https://uniswap.org/blog/uniswap-v3/>
61. <https://dydx.exchange/>
62. <https://www.theblockcrypto.com/data/crypto-markets/spot>
63. <https://ftx.com/>
64. <https://www.bloomberg.com/news/articles/2021-11-11/ftx-us-says-daily-trading-volume-jumped-500-last-quarter>
65. <https://www.coindesk.com/business/2021/11/04/revolut-looks-to-hire-tech-lead-to-build-a-crypto-exchange/>
66. <https://coinroutes.com/>
67. <https://www.algotrader.com/>
68. <https://www.theblockcrypto.com/data/decentralized-finance/dex-non-custodial/dex-aggregator-trade-volume>
69. <https://www.bitcoinsuisse.com/prime-brokerage>
70. [https://www2.deloitte.com/content/dam/Deloitte/xen/Documents/finance/me\\_Digital-Custodian-Whitepaper.pdf](https://www2.deloitte.com/content/dam/Deloitte/xen/Documents/finance/me_Digital-Custodian-Whitepaper.pdf)
71. <https://www.cnbc.com/2021/02/11/bny-mellon-to-offer-bitcoin-services-a-validation-of-crypto-from-a-key-bank-in-the-financial-system.html>
72. <https://www.bnymellon.com/us/en/about-us/about-bnymellon.html>
73. [https://www.pwc.com/gx/en/financial-services/pdf/3rd-annual-pwc-elwood-aima-crypto-hedge-fund-report-\(may-2021\).pdf](https://www.pwc.com/gx/en/financial-services/pdf/3rd-annual-pwc-elwood-aima-crypto-hedge-fund-report-(may-2021).pdf)
74. <https://www.fidelitydigitalassets.com/articles/corporate-treasurer-bitcoin>
75. <https://www.bitcoinsuisse.com/fundamentals/what-is-staking>
76. <https://polkadot.network/blog/web3-foundation-initiates-launch-polkadot-is-live/>
77. <https://ethereum.org/en/eth2/beacon-chain/>
78. <https://www.stakingrewards.com/staking/>
79. <https://www.bitcoinsuisse.com/research/specials/staking-with-bitcoin-suisse-a-guide>
80. <https://consensys.net/code-fi/staking/>
81. <https://www.stakingrewards.com/>
82. <https://etfgi.com/news/press-releases/2021/06/etfgi-reports-assets-invested-digital-asset-etfs-and-etps-listed>
83. <https://defipulse.com/>
84. <https://consensys.net/blog/metamask/introducing-metamask-institutional/>
85. <https://www.theblockcrypto.com/linked/118822/permissioned-defi-platform-aave-arc-gears-up-for-launch>
86. <https://www.coindesk.com/business/2021/12/01/tezos-based-nft-platform-oneof-inks-pitbull-to-multiyear-deal/>
87. <https://finance.yahoo.com/news/defi-tezos-becomes-more-feature-140000977.html#:~:text=Plenty%20is%20a%20full%20scale,interface%20and%20high%20farming%20yields.>
88. <https://www.parity.io/blog/statemint-generic-assets-chain-proposing-a-common-good-parachain-to-polkadot-governance/>
89. <https://polkadot.network/blog/statemine-upgrade-launches-new-phase-of-parachain-functionality/>
90. <https://polkadot.network/blog/polkadot-is-ready-for-parachains/>
91. <https://www.coindesk.com/tech/2021/11/18/acala-wins-first-polkadot-parachain-auction-with-13b-in-dot-committed/>
92. <https://kusama.network/auctions/>
93. <https://whatsonchain.com/block-height/686012>
94. <https://whatsonchain.com/block-height/700597>
95. <https://whatsonchain.com/block-height/700606>
96. <https://www.cardanocube.io/>
97. <https://datastudio.google.com/u/0/reporting/3136c55b-635e-4f46-8e4b-b8ab54f2d460/page/ve4AC>
98. <https://datastudio.google.com/u/0/reporting/3136c55b-635e-4f46-8e4b-b8ab54f2d460/page/s0XCC>
99. <https://satsymbol.com/>

# Learn more with Bitcoin Suisse Research!



Subscribe to receive insightful updates from our Research Team on the latest developments from all around the crypto world.



Subscribe to  
The Weekly Wrap



Subscribe to  
Bitcoin Suisse Decrypt



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.