Crypto 2023

Outlook

In-Depth Research Insights into Markets, Technology and Regulation

Bitcoin Suisse

Welcome to Crypto Outlook 2023 – The “Wreckoning” edition

“Who controls the food supply controls the people; who controls the energy can control whole continents; who controls money can control the world.”

— Henry Kissinger, 1974

2022

2022 was a year of wrecking and reckoning. It was about the wrecking of trust in central banks being able to maintain price stability while not damaging their economies and not weaponizing their currencies against other nations; trust in centralized finance (CeFi) companies who demonstrated in 12 months what traditional finance and regulators attempted half a century to eliminate: thou shall not lie and thou shall not misuse client funds; finally, the destruction of a country in Europe and with it, the supply of essential commodities such as energy and food needed in many countries.

Reckoning

It also was a year of reckoning: a large exporting country, after being cut off from international financial networks and access to its own foreign reserves, actively promoted de-dollarization – and it was not alone; weakly-designed algorithmic stablecoins were speculated out of existence as were CeFi companies that were recklessly gambling with their client funds; crypto users worldwide withdrew their assets in the billions from CeFi exchanges due to eroded trust in centralized intermediaries.

2023

So, where from here? We recognize that a cleansing thunderstorm washed out many bad actors in crypto, re-adjusted inflated price levels, triggered moves towards more regulatory clarity for CeFi, and proved once more that truly decentralized approaches are resilient. With that learning, it is time to move on and see what 2023 may bring. As every year, we selected a range of topics, which we think long-term oriented crypto investors should be aware of for 2023 and beyond.

Dr. Marcus M. Dapp
Head of Research

Preface

Prof. Dr. Claudio J. Tessone, Chairman of the UZH Blockchain Center that was ranked first in Europe in CoinDesk’s “Best Blockchain Universities” in 2022, kicks off with the

preface. He uses it to reflect on how the gradual shift in the 2010s from on-chain to off-chain trading influenced incentives and behavior of actors in CeFi in 2022, and what we need to do now to return to excellence.

Macro & Bitcoin

My insight from last year: watching the extraordinary global macro environment deserves an eye on Bitcoin – and Bitcoin needs to be seen through a macro lens. While central banks are literally at the center of forced "demand destruction" to counter high inflation while not creating too much pain with higher interest rates for debt-ridden governments, the decentralized Bitcoin space is showing organic growth, using the bear market to work on institutional and state adoption.

Lightning

As my interview with René Pickhardt, a key figure in the Lightning developer community and a 2022 Bitcoin Suisse Fellow, details, the technology development on Lightning, Bitcoin's Layer-2 protocol for payments, is an area of very active and broad innovation. Despite some of the technology hurdles that are still present on Lightning, new, and unexpected features, such as stablecoins and smart contracts, are expected to emerge in 2023.

CeFi is not DeFi

In 2022, the crypto markets experienced a lot of turbulence, mainly due to "CeFi shenanigans". Niklas Nygaard from our Trading Desk took an analytic look back on the (too) lengthy list of dominoes that fell: Celsius, Three Arrows Capital, Voyager, BlockFi, Genesis, and FTX. How did these extraordinary events affect him as a professional crypto trader, and how did the Trading Desk cope with such situations? What can we and investors learn?

Ethereum 2.0

On to the good news: the prize for most anticipated and largest technical breakthrough in 2022 went hands down to the Ethereum community who successfully executed the Merge – the migration to Proof-of-Stake – amidst a bearish market and regulatory interventions exposing censorship risks across the stack. Dominic Weibel from our Research team illuminates the post-Merge Ethereum roadmap that addresses security, privacy, censorship-resistance, and crucially, scalability in the coming years. The ambition remains high for 2023 and beyond to stay the premier smart contract chain on the market.

Institutional Perspective

How do institutional investors perceive the crypto space? Our CEO, Dr. Dirk Klee, shares his perspective on why and how financial institutions are opening to the crypto space. From trust and regulation to products and services in demand by clients, Dirk shares his thoughts for what to expect in 2023.

Celestia

One thing to expect in crypto is innovation. In his interview with Nick White, COO of Celestia, Dominic Weibel explores the emerging trend called modular blockchains that combines “the best of Ethereum and Cosmos” moulded into one ecosystem. The promise is a new paradigm to solve scalability, dependency on virtual machine environments, and shared security. What emerges as a trend into 2023 has been started by Celestia, so we are happy to share insights from the inventor with you.

Regulation

After 2022, we thought it is a good idea to add a piece dedicated to regulation. In the final article, my colleagues, Dr. Cansu Burkhalter, Dr. Fabio Andreotti, and Oliver Gehrig, investigate the question of how to strike the right balance in regulating crypto from different angles. They provide an overview ranging from international to Swiss developments along a series of acronyms such as CARF, MiCAR and FinSA and how they will affect professional custody and trading in the future.

Citation (W)Rap

Aside from the long pieces, we have a new addition to this year’s Outlook: The “Citation (W)Rap” is our selection of the best quotes-of-the-week from our Weekly Wrap series in 2022. We also decided to continue the “vires in numeris” section we added last year and hope you find our selection of charts useful and inspiring for your crypto investments in 2023.

Crypto Taxonomy

You also get an exclusive Outlook preview of another publication the Bitcoin Suisse Research team is preparing for early 2023: the “Global Crypto Taxonomy” is a systematic way of organizing digital assets into sectors and sub-sectors, helping investors that seek guidance when comparing different digital assets to navigate the heterogenous crypto space.

I cordially thank all invited authors and interview partners who took time to share their thoughts and insights for this edition. My warmest thanks go to all colleagues at Bitcoin Suisse who contributed content, shared their expertise in proofreading, and took great care to package the content into this nice booklet to make it a pleasure to open and browse. Thank you all!

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

Dr. Marcus M. Dapp, Head of Research

Impressum
Bitcoin Suisse AG
Grafenauweg 12
6300 Zug
Switzerland

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
bitcoinsuisse.com

PS. We offer a range of publications in addition to the Crypto Outlook. Feel free to explore and subscribe to our regular research publications at www.bitcoinsuisse.com/newsletters.

Contents

Preface

Prof. Dr. Claudio J. Tessone

UZH Blockchain Center

No space is as temperamental and dynamic as the crypto ecosystem. In the past year, we saw the industry jump from contained optimism to utter dismay. What is fascinating is that this happens to the most technocratic systems we can find widely deployed in human societies. So, how come?

by Prof. Dr. Claudio J. Tessone,
Chairman UZH Blockchain Center

Permissionless blockchains are a gem for researchers: the full data of a self-contained economy in a standardised format. In our research team at University of Zurich Blockchain Center, we resort heavily on blockchain analytics to understand the crypto economy. After analysing a family of long-term blockchains, it is striking to find that in the early years, it was possible to find interrelations between activity in the blockchain and the cryptocurrency prices on what we now call Centralized Finance (CeFi) exchanges. The intuitive reason is simple: the more people use cryptocurrency, the more it drives demand, raising its relative price with respect to Fiat currencies. However, the relation between blockchain activity and price vanished in the second half of the 2010's: most trades occurred off-chain, moving cryptocurrencies and tokens away from mediums of exchange (if there ever were such) or store of value

and becoming mere sources for speculation. Decentralized Finance (DeFi) did not alter this trend, moving a fraction of it once again on-chain.

In the early days of crypto, a first generation of bubbles was created, all triggered by exponential growth of user demand on scarce assets. The second-generation bubbles were not brought on by incorrect crypto-economic incentives, but due to the ecosystem attracting the wrong actors. There is no inherent flaw in the basis of blockchains and Decentralized Ledger Technology (DLT), it is just poor management of the opportunities brought by them.

In the following, I will summarise some thoughts I hope will serve for introspection to the blockchain ecosystem. This, together with the fantastic material brought by the Bitcoin Suisse Research team, is food for thought, trying to find ways for brighter future days.

Not mere technologies

Blockchains are usually presented as a technological revolution, one that builds an intricated web of businesses and services on these tamper-proof ledgers without the need of central trusted parties. As a technology, different protocols are compared according to their data throughput, number of transactions per second, languages on which smart contracts can be written and the cryptographic primitives used to secure them. However, blockchains work based on a set of incentives that try to align agents' behaviour, a goal that they do not always fully achieve. They are governed by closed-knit communities in which decision-making processes have strong power imbalances. The underlying, internal principles of blockchains and crypto-financial services are complex socio-economic-technical systems. Nothing less.

Too often I hear something along the line of "we do not need to know the intricacy of the engineering of our mobile phone to use it. So, neither do we need to understand blockchains in order to use them." This is the most dangerous fallacy that will continue to drive the crypto space into failure after failure. Everybody needs a basic understanding of the social, economic and technical interrelations of a product or service to be able to make informed decisions. This is why education (and not veiled advertisement) is of primordial importance at all levels for students, professionals, and the general audience.

It is all about human behaviour

We as humans do not act rationally and we continuously learn new behaviours. Even if we assume no

wrongdoing, the Terra-Luna debacle showed in cinematic fashion the limits of simplified economic models turned into algorithms. Once rules are fixed, agents have ample time to find holes in their logic. This has happened over and over and will continue happening. The collapse of FTX and Alameda Research – only fully understood in tandem – points to both: the issue of lack of regulation, and the dangers of the proliferation of tokens that wrap each other's value, issued without oversight. In systems that few people understand, obfuscation is so simple to achieve...

To me, it is mesmerising that intelligence and analytic companies with abundant resources failed to issue early warnings of this glaring situation. It is exactly for cases like this that unbiased actors such as research units can shed light on the potential risks present in these economies.

The need to excel

The recent turmoil in crypto has hit all around the world, but – while certainly taking its toll – it has left the Swiss ecosystem still on its feet. To turn this necessary cleansing of undesirable actors into an opportunity, it is mandatory that all the members of the ecosystem excel in their area: regulation, business development, financial advice, compliance, coding, education, and research.

The strength of the Swiss brand is in the hands of each member of the local ecosystem. Switzerland has a unique aura as a worldwide blockchain hub: A unique mixture of advanced yet unobtrusive regulation, multi-faceted stability, and qualified workforce.

This is the moment in which we all remember the importance of different pillars, be it technology, business/economics, or regulation/governance, in a holistic manner. This is the moment in which, irrespective of our roles in practice, government, or academia, we work together supporting each other. This is the moment in which every decision, every new step is done adhering to the highest standards.

Article

Macro view

with an eye on Bitcoin

by Dr. Marcus Dapp

- Central banks cannot print energy or food. A war in Europe adds to the high-inflation environment and will cause supply shortages in 2023 and beyond that need time to solve. De-globalization in favor of national sovereignty is emerging.

- Central banks cannot ease and tighten simultaneously. All major economies fight with high debt levels in the face of interest rate hikes. Debt-based fiat currencies are getting under pressure, and de-dollarization has become a trend.

- Who needs central banks anyway? Despite a dim macro-outlook and too many CeFi shenanigans causing contagion well into 2023, Bitcoin adoption is increasing with nation states and institutions. Technical innovations on layers 2 and 3 bring new use cases to the Bitcoin/Lightning ecosystem.

Geopolitics hit everyone

In 2022, geopolitics hit hard in several aspects. Starting into 2022, the world was still trying to escape the lockdown-induced global supply chain interruptions from the previous year. The Federal Reserve (FED) and the European Central Bank (ECB) had already increased money supplies tremendously[1] when the 24 February 2022 came, and Europe had to witness Russia's invasion of the Ukraine. What was planned to be a swift takeover has turned out to be an enduring stalemate that is ongoing at the time of writing.

The implications are still unfolding and will reach far into 2023 and beyond. According to geopolitical analyst Peter Zeihan, Russia, Belarus, and Ukraine combined form a dominant export region. Together, they rank global first in natural gas, uranium, neon (required for microchips), wheat, potash and fertilizer; global second in crude oil, oil products, steel, seed oil; and global third in coal, gas turbines, aluminum, and titanium[2]. Many countries in the world are depending on these commodities with interruptions having significant short-term consequences (e.g., wheat) as well as long-term (e.g, fertilizer, neon). Rectifying the shortage in certain commodities by building infrastructure in other countries may take years according to Zeihan. What has started as a local/regional conflict will have global impact in 2023 and beyond as other, remote countries will be affected.

Especially the interruption of the energy supply from Russia to Western Europe, caused by sanctions and pipeline blowups, are not only causing human suffering and extraordinary measures by governments, but will have impacts on the economic outlook for Europe as a whole.

In addition to existing embargos, including disconnecting Russia from the Swift system and freezing its foreign currency reserves, the EU and G7 are imposing an import ban and price cap on Russian oil starting January 2023 with the aim to restrict Russian oil exports without increasing global oil prices[3]. The outcome will be determined by whether Russia will be able to circumvent the price cap, how strong its dependence on oil income is and how sensitive the EU and the G7 are to rising oil prices.

All these geopolitical factors only add to the inflationary pressure that was already reaching a new record before the invasion, indeed the highest for decades (illustration 1).

Artificially halting the economy through lockdowns and then balancing the impact through stimulus programs was possible through increasing money supply while accepting a "temporary" increased level of inflation. While stimulus checks could be printed, missing oil, gas, wheat, and fertilizer cannot be "printed" into existence. Deliberate fiscal and monetary action are helpless against the commodity crunch triggered by the Russo-Ukrainian war in 2022. Filling the supply gaps requires investments into reconstruction and infrastructure, which will take considerably more time than its destruction took. At the same time, record-high inflation has debased fiat currencies, making it less affordable to buy scarce commodities from foreign powers. What will happen to our money?

Zoltan Poszar argues for a new monetary era emerging[4]. The era of 1948-1971 (Bretton Woods I) was shaped by gold-backed currencies and the era from 1972 until today (Bretton Woods II) was shaped by treasury-backed currencies. He argues that due to the events in 2022, the new monetary era, which he calls "Bretton Woods III", will be shaped by gold- and even commodities-backed currencies. In one sense, this will revert the monetary system to a pre-WW2 time, in which the potential of governments and (central) banks to increase the money supply was much more restricted. In the new era, he also sees a new digital commodity emerging and playing a role "if it survives until then": Bitcoin.

Throughout 2022, the FED and the ECB were desperate to demonstrate that inflation was not an issue or "only temporary", and that they are in control of the dynamics and on track to push it back to the long-term normal of around 2%, a coincidental and arbitrary number in case you did not know[5].

However, how credible is this claim? If the governments of these central banks were financially sound and in good shape, one could think, okay, it is tough, but they might manage. But the governments are not in good financial shape at all.

Predictions

- Inflation will not reach 2% again anytime soon, maybe never under this currency regime
- The flight to safety will go to scarce commodities and even commodity-based currencies
- At least one international trade between countries, most likely on an essential commodity, will be settled in Bitcoin

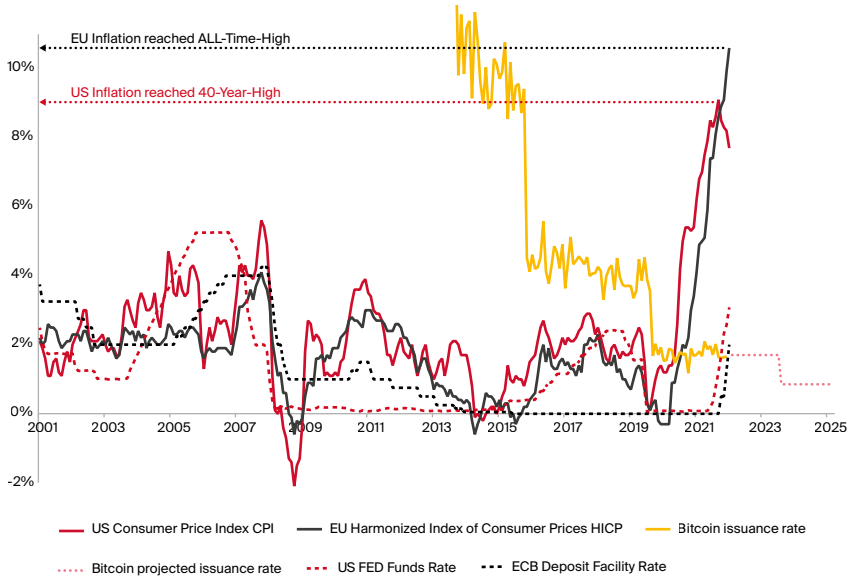


Illustration 1: Monthly inflation and interest rates (annualized), compared to Bitcoin's algorithmic issuance rate. Data: Federal Reserve, European Central Bank, Swiss National Bank. Chart: Bitcoin Suisse Research

Fiat currency and national debt

Fiat currency is created either by a central bank printing it or by any bank, central or commercial, making a loan to somebody. None of these modes of creation are linked to actual economic activity, the generation of value through a product or a service. In other words: every dollar, euro, franc you have in your wallet is the debt of somebody else in the system. Therefore the tendency of having too much money compared to the economic output of a nation. This excess in money supply devalues the money, which we call inflation. However, the interest rates banks, central or commercial, demand from their creditors, have not been created. As every creditor must pay interest in addition to the principal of their loan, they inevitably take it from another creditor's principal. Thus, the debt-based money system is under constant pressure because all creditors chase to repay their principals plus interest while only the money for the principals has been created in the first place… That is why fiat money systems over time tend to put all players, individuals, companies, and governments into debt.

The term "debt spiral" is quickly explained. Imagine, you are in debt and are unable to pay back. A creative solution is to just borrow more and use it to pay back. In other words: you repay short-term debt by accumulating more debt long-term. Once started, you can only escape if your income drastically increases, or your debt gets reduced. If not, the situation is just spiraling downwards from here…

Companies and governments can fall in a debt spiral in similar ways. Companies that are unable to cover their debts beyond interest costs with current operating profit over three consecutive years are called "zombies." A recent Kearney[6] study estimates that nearly 5% of all listed companies around the world are zombies (+250% since 2010). Based on a sample of 70'000 companies, their projections yield that a 50% increase in interest rates would push that figure to 17%, and a doubling would result in 38% zombies – more than a third of all listed companies! The study estimates that nearly $0.5T of capital is misallocated this way and at a "significant risk of default."

Governments create deficits if their expenses for welfare and warfare (and debt service) are higher than their income from taxes (Illustration 2). While overspending is the obvious cause for deficits, an economic contraction can impact the income side and create or exacerbate a deficit. As budget deficits accrue over time, sovereign debt is accumulated[7]. The crucial question for policy makers is whether the sovereign debt is predominantly owed in foreign (FC) or domestic currency (DC).

If owed in FC, the government finds itself in a tough spot because to repay it needs to buy FC using their own DC, which must be earned by the domestic economy first and be available in the form of tax money before it can be spent. As a result, the FC appreciates because of increasing demand and the DC depreciates in value. If the economy now contracts in that scenario, the FC inflows into the country slow and credits contract. That means liquidity and lending dry up while the DC depreciation produces inflation. This dynamic may lead to what Ray Dalio calls an inflationary depression[8].

If the sovereign debt is owed in DC, the government is in a somewhat easier situation as the central bank can monetize the government debt by paying with new currency. However, as there is no additional economic output backing the additional currency, the DC depreciates in value. If the economy now contracts in that scenario, the central bank can "stimulate the economy", i.e., reduce interest rates to expand domestic credit. This effect dissolves when the interest rate reaches 0% - as was the case in the US and EU in 2019-2021 (c.f. illustration 2). Economic contraction then shrinks income and raises debt burden, eventually producing forced selling and defaults – but no currency issues. This dynamic may lead to what Ray Dalio calls a deflationary depression.

For those countries that have their debt denominated and owed in domestic currency, the matter is much simplified. The debt can be monetized: the government can issue debt instruments in domestic currency, which are bought by the central bank by increasing the domestic money supply. Thus, the governments do not need to raise taxes and the domestic economy does not need to earn the money first.

The United States has this "exorbitant privilege" (Charles de Gaulle) of hosting the global reserve currency, which is in almost constant demand by most other governments. They can "export" their inflation. Therefore, one could assume they would be the last nation to be overindebted.

Let's look at some numbers. By 30 November 2022, total US sovereign debt[9] amounted to $31.4T. That is over 5 times the 2022 national budget of $6T, which already includes a deficit of $1.4T (~25% of budget)[10].

The US Congressional Budget Office revealed that interest payments alone (!) amounted to $0.4T (1.6% of GDP) in 2022 and projects a rise to $1.3T (3.3% of GDP) by 2032[11]. Just to keep the debt level steady over the coming decade, US citizens and businesses face a total interest payment burden of $8.1T.

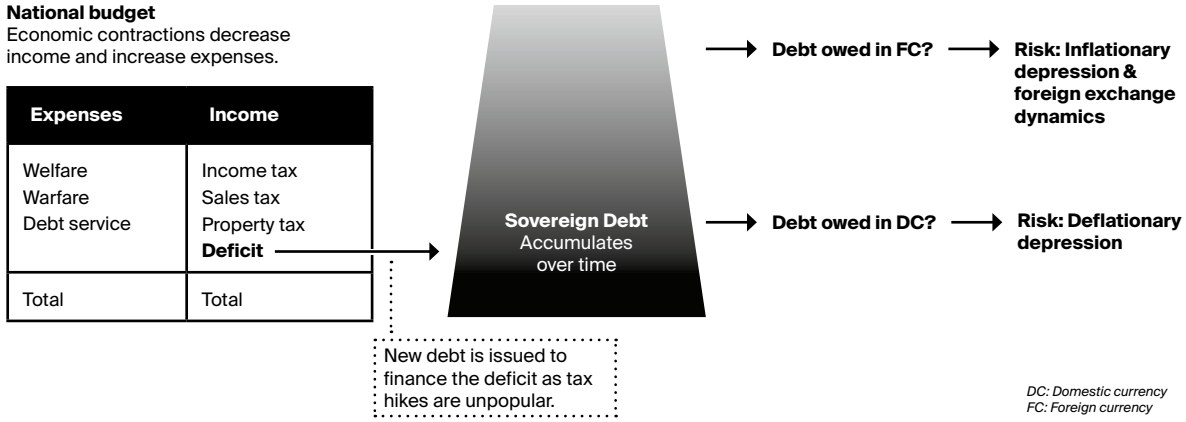


Illustration 2: Dynamics between deficits, sovereign debt, and economic contractions in two debt scenarios enabled by the fiat currency system. Source: Bitcoin Suisse Research

Illustration 3 shows the debt-to-GDP ratio for selected Western countries, which has been trending upwards in all, except Switzerland. The Great Financial Crisis[12] marks the pronounced increase in 2008 and the beginning of the Great Lockdown[13] the sudden spike in 2020. While, in 2008, government spending focused on bailing out failing banks, in 2020, it focused on stimulus programs for various businesses and citizens. In both cases, sovereign debt grew by increasing the money supply. The United States saw record-high domestic inflation in 2022 (c.f. illustration 1) following a record-high debt-to-GDP ratio of 137% in 2021 (c.f. illustration 3). A debt-to-GDP ratio above 100% means that a nation's economy is not able to pay off its debt within one year if the entire GDP would be devoted to it.

What does the aggressive series of seven federal fund rate hikes[14] by the Federal Reserve in 2022 mean for US sovereign debt in 2023 and beyond? The dilemma is that to counter high inflation, higher fund rates are needed. However, higher fund rates will increase the burden of debt service even further.

Which of the three options will the US government choose to reduce sovereign debt (c.f. illustration 2): raise income through tax increases, reduce expenses through cutting welfare and/or military programs[15], or more deficit spending? While the first two options are very unpopular among voters and politicians (and strategically sensitive in the case of defense and current geopolitics), there is not much room left to maneuver: the series of rate hikes will have to come to an end and reverse as monetization

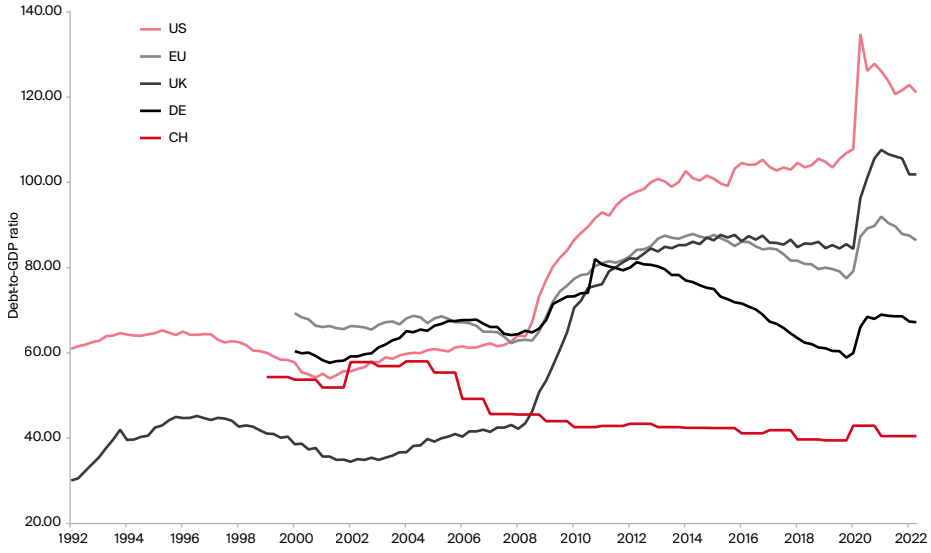


Illustration 3: Debt-to-GDP ratio for selected Western countries (1992-2022, 2000-2022). Data: FRED, Eurostat, GOV.UK, OECD. Chart: Bitcoin Suisse Research

of debt will have to continue. An aggravating factor is the fact that the real interest rate – the effective rate after deducting the inflation rate – is negative. Generally, investors buying sovereign debt through government bonds accept that a risk-free investment has only a low yield. But now it is negative and will remain so until the regime of high inflation and low interest rates changes.

Two final observations: first, in 2022 central banks around the world bought 400t of gold in Q3 alone (+340% YoY) and a total of 673t until 1st November – the highest annual total since 1967[16]. Second, during the 14th BRICS Summit, Russia's president announced that the BRICS nations (Brazil, Russia, India, China, and South Africa) intend to develop a "new global reserve currency" based on their sovereign currencies to "address the perceived US hegemony of the IMF"[17]. BRICS is currently representing 42% of global population and several nations are considering joining BRICS: Argentina, Iran, Saudi Arabia, Egypt, and Turkey are at different stages of the process[18].

We made this lengthy detour on inflation, debt, GDP, and fiat currency as we believe this extraordinary global situation will stay with us for 2023 and much beyond. What will this mean for the US economy and its trade partners? Which foreign countries have US Dollars as national reserves or directly depend on the USD because they are dollarized? Will more countries discover Bitcoin as "pristine collateral and reserve asset"[19] and even follow in the steps of El Salvador and make Bitcoin (secondary) legal tender in their country?[20]

In summary, highly indebted nations are between a rock and a hard place: they need to increase and sustain high interest rates to destroy demand so the inflation rates can decrease. However, the more they stick to this "hawkish" monetary policy, the more their own governments suffer from increased, unsustainable debt servicing cost with no easy solution in sight. Or is there?

Are CDBCs governments' escape hatch?

Would it not be much easier to simply change an algorithm to adjust in real-time the money supply, funds rates, and optional stimulus packages, taxation, and other parameters for the whole economy at once? What sounds like a utopia for central bankers may come true with Central Bank Digital Currencies (CBDCs).

Activities around CBDCs have picked up pace during 2022. The CBDC tracker[21] of the Atlantic Council currently lists 119 projects, of which 11 are launched, 17 pilots, 33 in development, and 39 in research. A selection of countries to watch in 2023 is listed in Table 1 below, including recent updates that the tracker may not have yet picked up.

Interbank (type "wholesale") CBDCs will deliver to central banks and governments the typical benefits of going digital, e.g., higher speed, lower cost, leaner processes, etc. without many down sides. Citizen-facing (type "retail") CBDCs would give central banks for the first time a direct interaction channel to citizens and businesses, circumventing the banking system on which the central bank had to rely on for executing its policies.

Central Bank	Status / Type	Situation
People's Bank of China, China	Launched / Retail	Used in 23 Chinese cities. $14B (100M yuan) transacted in e-CNY between December 2019 (start of initiative) and August 2022[22].
European Central Bank, EU	Development / Both	In September 2022, five companies have been selected for a prototyping exercise with different payment use cases[23]. According to an executive member of the Bundesbank, the digital Euro will not arrive before autumn 2026[24].
Reserve Bank of India, India	Pilot / Both	Pilot with four cities and four banks started in December 2022. The plan is to have a digital Rupee launched in 2023.
Central Bank of Nigeria, Nigeria	Launched / Retail	The eNaira was launched in October 2021. By October 2022, transactions worth $18M have been processed. Beginning 2023, ATM cash withdrawals will be restricted to increase adoption of the eNaira[25].
Swiss National Bank, Switzerland	Development / Wholesale	Involved in several projects together with BIS Innovation Hub and other partners to test integration with core banking systems and cross-border payments[26].
Federal Reserve, United States	Development / Both	In September 2022, the US Office of Science and Technology Policy published a technical feasibility study based on the policy objectives of the US government[27] for a digital Dollar. In two projects the technical requirements and wholesale integration are tested[28].

Table 1: Overview of CBDC initiatives of selected jurisdictions around the world

Considering the precarious macro situation described above, it is important to understand what central banks and governments would be able to do with CBDCs. Above all else, digitizing a sovereign currency does not change the role of the issuing government and central bank in any way. Thus, the management of monetary supply and control over monetary policy will continue to rest with the central bank, no matter the jurisdiction. Implementations will almost certainly not put a focus on decentralization as this presents a conflict of interest with the requirement to stay in control. However, shaped by differing political views, the design of privacy protection may differ widely across jurisdictions. In fact, privacy preservation may turn out to be the key differentiator between competing CBDCs in the future.

The US OSTP feasibility study referenced in Table 1 expressly states that it does not give any recommendations on the pros and cons of technical designs. It reveals, however, that the US policy objectives that frame the design contain several profound conflicting goals. A few examples[29]:

- Preserving monetary policy-making and keeping control
- "Support US leadership in the global financial system, including the global role of the dollar"
- "Minimize energy use" and "improve relative to the traditional financial system"
- Promotion of AML compliance vs. protection of privacy and human rights.

The crucial insight for retail CBDCs is that a central bank could implement monetary policy directly. On the spending side, this may range from paying out stimulus checks, basic income, or other forms of "helicopter money" directly to citizens[30]. On the income side, taxation can be personalized and unpopular policies like, e.g., currency debasement, interest rates, expiration dates, etc. could be implemented at a much finer granularity than ever before[31].

The opportunity for central banks and governments and the danger for citizens and businesses lies in what I termed "surveillance monetarism[32]." While the term "surveillance capitalism" (Shoshana Zuboff) describes the mechanism by which big tech companies ("FAANG") can extract value using surveillance methods based on large-scale data collection and analytics of users, "surveillance monetarism" will allow governments and central banks to micro-control citizens using surveillance methods based on complete financial data collection and analytics[33]. As the China Social Credit system exemplifies, governments differ from tech companies. By the powers vested in them and using the financial data history, they can directly punish or reward behavior: travel prospects, employment, access to funds and financial services, etc[34].

What prevents other governments from implementing similar systems? Hardly any government will come up with a proposal to monitor its citizens from day one, but enough arguments like anti-terrorism, illicit behavior, financial market stability, etc. will be available to justify technical designs that in principle allow surveillance – even if only in the future.

The answer from the DeFi space to CBDCs is stablecoins. Although their merits are undeniable – they offer "stability" in fiat terms plus all benefits of digital tokens like global transferability, speed, etc. – they have their downsides, too[35]. The major event in 2022, and the only major collapse of a DeFi protocol in 2022, was the collapse of the algorithmic stablecoin UST caused by the hyperinflation of Terra LUNA. The less-than-robust stablecoin algorithm proved vulnerable to arbitrage attacks as soon as the peg went too far off the equilibrium. The immutable algorithm was unable to detect and react adequately to the speculative attacks by humans that caused LUNA to hyperinflate... Algorithmic stablecoins are very hard to design in a robust way, the founder was overdoing the boasting of his project and the space will need deep introspection before investors fund the next algo-stablecoin experiment.

However, in general collateralized stablecoins performed quite decently in 2022: they turned out to be useful onramps to crypto in inflation-ridden countries like Argentina, Nigeria, Türkiye, and Venezuela[36]. While none of the reoccurring concerns about insufficient collaterals materialized for any of the major stablecoins, regulators remain on alert on this obvious competition to their fiat currencies[37].

Predictions

- Macro/Debt situation may increase the pressure to speed up introduction of CBDCs.
- So, governments keep pushing but central banks will not launch anything major in 2023.

All together now: CeFi is not DeFi!

As if the macro situation and the LUNA collapse would not have been bad enough in 2022, the crypto space had

to deal with a regrettably long series of collapses that made clients lose billions of funds and hurt the reputation of the entire industry. The too long series of CeFi shenanigans that followed in the months after LUNA caused contagion again and again until year end and into 2023. The first wave consisted of 3 Arrows Capital, Voyager, and Celsius and the final wave of 2022 were the revelations of FTX, which took scam, bankruptcy and fraud to a whole new level (illustration 4).

→ *For more context, read our "Crypto Investing in uncertain times" article in this Outlook edition*

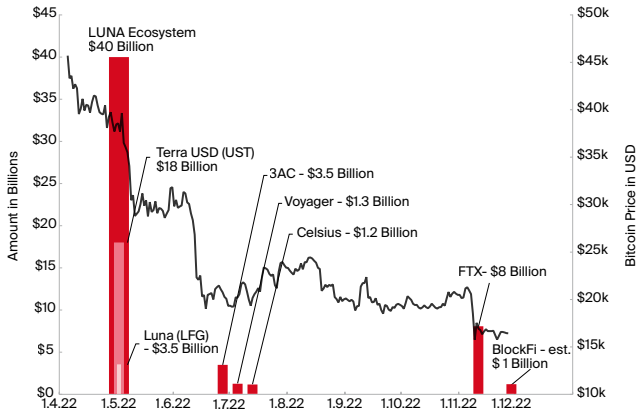


Illustration 4: The 2022 series of collapses in crypto and (the effect on) the Bitcoin price. Data: Bitcoin Suisse Weekly Wraps. Chart: Bitcoin Suisse Research

The CeFi meltdown provides several learnings: investors should learn that CeFi reintroduces counterparty risks that DeFi protocols aim to remove in the first place: the risk that the other party in a deal may not fulfill its part and may default on their obligation. While DeFi carries risks around smart contracts and needs care because code has only limited flexibility to react to extraordinary market volatility, it offers much more transparency: smart contracts can be audited, transactions can be traced on the blockchain and thus the evaluation of exposure and leverage of oneself and potentially other players is much simpler.

Regulators do hopefully learn that focus is to be put on human behavior rather than technology. The reason is that "CeFi" implies an underlying company. With a company, investors need to trust the team to know what they are doing, and their honesty in all aspects of the business: funds are invested as advertised, not lent out in misleading terms – and not stolen (duh!). Furthermore, investors need to ensure risks are clearly communicated, investment strategies adhere to risk policies, and established management practices are applied to minimize risks. Traditional Finance (TradFi) and regulators had the opportunity to learn this over a century to amalgamate it into a set of useful financial regulations that are mostly adhered to, sometimes ignored and sometimes willfully disregarded. CeFi is simply TradFi with digital assets and deserves similar regulation. In contrast, DeFi is transparent code that can be expected to remain unchanged during an investment.

"Crypto ... You keep using that word, I do not think it means what you think it means."

It took TradFi centuries to gradually establish different assets classes like equity, fixed income, real estate, precious metals, etc. Hence, nobody would try to lump them under one umbrella term because they are too different to compare directly: yield generation mechanisms differ (if they are present), risk profiles differ, market dynamics differ, and so forth.

By lumping everything together under a single term "crypto", our industry stands in the way of helping everyone to better understand the commonalities and more importantly the differences between all these coins, tokens, and protocols. Misunderstanding, misjudgment, and ultimately misallocation of investment funds is the result. Especially after a year of many crashes due to inadequate risk management in CeFi companies, our industry would be doing everyone a favor by explaining more clearly the different risk profiles between payment coins, infrastructure tokens, DeFi protocols, or the tokenization of TradFi instruments – because they all behave differently and are different types of investments.

Another consequence of the crises in 2022 was that the awareness for custody risk rose quite significantly. What helps is to provide much more clarity on terms. "On-chain" means assets are secured by cryptographic keys on transparent ledgers and clients can access them when they want.

→ *Check out the preview of the Bitcoin Suisse Global Crypto Taxonomy in this Outlook edition!*

> "Code committed no crime. FTX and cryptocurrencies are not the same thing. FTX was opaque, centralized, and dishonest. Cryptocurrencies usually are open source, decentralized, and transparent."
>
> *– US senator Patrick Toomey, during US Senate hearing on FTX collapse*

The loss in trust caused by too many bad or naive actors who were trusted with too much client funds to literally gamble by rehypothecating tokens against other tokens to no end, is enormous and will set back the space for quarters if not years.

We invite you to read the regulatory landscape article in this Outlook edition!

Predictions

- Contagion in CeFi is not over yet and many funds will not return to exchanges in 2023.
- Move by US regulators to require large scale registration of tokens they deem "securities."

Eye on Bitcoin

For the first time, Bitcoin has experienced a recessionary macro environment in 2022. A dim macro-outlook and CeFi shenanigans presented the perfect storm to see how Bitcoin would react. Over 2022, the USD price of bitcoin dropped by 65.5%, but Bitcoin refused to die for the 467th time[38] with the latest obituary coming from the ECB in November 2022[39].

On a more serious note, it could have been much worse. Bitcoin dropped 65.4% in 2022, in line with the entire crypto market (65.7%) and remained in a stable range under $20'000 during the last months of 2022. A few comments to give a bit of context to these numbers:

First, drawdowns in this order or higher (80%-90%) are nothing new or uncommon for bitcoin[40]. That's it. Even in the absence of all the macro pressures and the LUNA/CeFi shenanigans, Bitcoin could have been falling to a similar level just because it evolves in cycles, and it happened before. Our take: the world has yet to find the actual price, or better, value of Bitcoin, because, as we never had an asset like this before, we have no way of knowing in advance. The market figuring this out over time implies large volatility and only gradual price discovery. At one point we will know what affects the value of Bitcoin, but 2022 was not the year we figured it out for good.

Second, the lamentation about Bitcoin being correlated to (tech) stocks for three quarters in 2022 is shortsighted for similar reasons. 2022 was the first year that Bitcoin's cyclical drawdown coincided with a drawdown across all markets, as the "everything bubble" we discussed in last year's Outlook is morphing into an "everything burst" this year. The consequence? Everything is correlated because everything falls during such broad market downturns. The 2022 class of market entrants was hurt for sure, but long-term investors seem to just wait and hold out according to Glassnode analyses[41].

The extraordinary markets in 2022 caused US stocks and bonds both to turn negative within the same year! A situation that seems to contradict the established wisdom that both asset classes act as mutual counterweights and have therefore formed the basis of the famous balanced fund[42] portfolio (e.g., "60/40"). According to data from New York University[43], only four out of the last almost 100 years show this constellation: 1931 (S&P -44%, Bonds -3%), 1941 (-13%, -2%), 1969 (-8%, -5%), and 2022 (a double whammy: -18%, -18%). Dylan LeClair argues that within 2 years of each of the four, the "US defaulted on its debt[44]", not explicitly but de-facto. We cannot go into deep analyses here, but let's flag a few highlights to get a feeling of the circumstances of these times past:

- In 1933, President Roosevelt issued Executive Order 6102[45] confiscating private gold: citizens had to sell their gold at a price of $20.67 per ounce to the Federal Reserve. One year later, the Gold Reserve Act fixed the new gold price at $35 an ounce, effectively allowing the Federal Reserve to increase the money supply without violating the Federal Reserve Act that required 40% gold backing, a limit nearly reached during the Great Depression.
- In 1941, the US entered WWII, which was financed by raising taxes and issuing war bonds. By 1943, two-thirds of the economy was integrated into war production[46].
- In 1971, the so-called Nixon shock, a series of measures in response to inflation, were initiated by President Nixon. The most consequential one was presented on a Sunday evening: Nixon declared to "suspend temporarily the

convertibility of the dollar into gold or other reserve assets". This statement unilaterally ended the post-war Bretton Woods Agreement of 1948 and ushered in the era of fiat currencies that are not backed by gold anymore[47].

- For 2024, … we probably do good in preparing ourselves to expect extraordinary economic situations that we even may not have experienced in our lifetimes yet because the economic parameters of 2022 have been no smaller outliers than the ones described above.

Third, there is a less obvious connection between the LUNA/CeFi collapses and the Bitcoin price performance. To a significant extent, what was burned last year was "paper bitcoin", IOU bitcoin, or "fake bitcoin."

> "Bitcoin will not be a great store of value if most people are buying fake bitcoin."
>
> *– Jameson Lopp on Twitter, 13 November 2022*

What does Lopp mean by that? Paper bitcoin means bitcoin you own but are not under your control. The "not your keys, not your coins" mantra resurfaced when FTX, the Luna Foundation Guard and other "safe custodians" turned out to not be so safe after all. The core problem is that it requires trust, that your bitcoin is not repurposed for other investments while you entrust the custodian with them. As this repurposing is the source of any yield you could ever get on bitcoin, it is also attractive to entrust a third party with your bitcoin. Many bitcoin were involuntarily sold in 2022 because the DeFi institutions who custodied them (as reserves or as client funds), had to sell them to redeem collateral, other tokens, that their clients enquired to withdraw, or to cover for losses in other investments. These leverage dynamics created additional, and in a sense unnecessary, sell pressure on Bitcoin. Without the maniac search for yield on Bitcoin, much less of this pressure would have been generated during the market downturns. Why? Because Bitcoin is "money" and money does not offer yield because its purpose is to store value in uncertain times and be a medium of exchange in better times. In addition, holding a bearer asset like Bitcoin does not have counterparty or other risks except price volatility measured in fiat currency.

Despite all these pressures – from war, inflation, rate hikes, DeFi mistakes in large stablecoins, CeFi shenanigans – the Bitcoin network just kept chugging along: no bridges hacked, nobody had to put the "blockchain into maintenance mode", transactions were processed every ten minutes on average and fees were bearable throughout the year. In fact, security of the network in the form of hashrate hit five all-time highs in 2022 and the number of nodes as an indicator of decentralization remained stable around 15'000 public nodes (and an unknown number of private nodes on the TOR network).

Short-term investors or recent entrants (since "peak bull" in 2021) have experienced quite a bit of pain – like everybody who joined just before a "-80%" period in the history of Bitcoin. If you think the fundamentals of Bitcoin are intact, and we think they are, then a long-term perspective does this "money experiment" more justice. For such a perspective and in such volatile times, qualitative information about ecosystem developments is more telling for the future than historical charts. So, let's see...

To watch: nation-state adoption. While user adoption of Bitcoin has slowed in the 2022 bear market, it remains above pre-bull market levels with the top 20 adoption countries covering all continents[48].

After El Salvador in Central America (06.09.2021), the Central African Republic (CAR) is the first country on the African continent that introduced Bitcoin as legal tender on 23.04.2022. Both countries depend on a foreign currency: while El Salvador is dollarized[49], the CAR is using one of the two CFA franc (Franc of the French Colonies in Africa) currencies that are in use in 14 former French colonies in Western and Central Africa[50]. As the CFA franc is pegged to the Euro, these countries struggle with economic planning as the monetary policy for them is made in Brussels and the Euro peg makes exports more expensive as they cannot actively manage adequate exchange rates. No wonder, the Machankura project enables Bitcoin Lightning transfers via SMS across eight African countries to counter the lack of internet connectivity[51].

Despite the bear market, El Salvador is continuing its Bitcoin journey and holds 2480 bitcoin at time of writing[52]. On November 17, 2022, the president announced that the country is buying one bitcoin every day. Addressing the primary criticism that citizens have been hit unprepared by the legal tender law in 2021, the NGO 'Mi Primer Bitcoin' has started to educate 11'000 students on Bitcoin in 2022, with plans to extend the offering to 250'000 in 2023. They also created a school curriculum in which students can receive a "Bitcoin diploma" in several public schools, with the aim to reach all schools in the country.[53]

In May 2022, El Salvador hosted the annual meeting of the Alliance for Financial Inclusion to discuss Bitcoin

for nations with 32 central banks and 12 financial authorities in attendance from a range of countries: Paraguay, Haiti, Honduras, Costa Rica, and Ecuador in Latin America, Angola, Ghana, Namibia, and Uganda in Africa, and Bangladesh, Palestine, and Pakistan in Asia[54].

Since December 2022, Bitcoin is recognized as a means of payment and investment asset in Brazil, with the law going into effect in summer 2023[55]. While the law does not render Bitcoin or other cryptocurrencies legal tender, the greater regulatory clarity may encourage businesses to explore it more closely – Brazil is currently the top 7 country in crypto adoption[56].

A second aspect of nation state adoption would be to adopt Bitcoin as a part of the national currency reserve strategy. No country has yet publicly spoken about using or considering the use of Bitcoin in that way – although you could argue El Salvador's Bitcoin stack is more of a reserve than investment money for the time being. In a working paper from Harvard, Matthew Ferranti explores the potential of Bitcoin to serve as an alternative hedging asset compared to gold, which was bought 2016-2021 by countries who faced a higher risk of US sanctions[57]. Coming from a student of Kenneth Rogoff, Harvard economist and Bitcoin critique, it was a bit of a sensation. A group of shareholders of Swiss National Bank also suggested in the 2022 general assembly that the SNB prepares for taking on bitcoin as part of its reserves. Reserves in bitcoin could not be confiscated nor otherwise tampered with as is possible with fiat currencies. For example, Russia's foreign currency reserves including gold were frozen, i.e., not accepted anymore for debt payments after Russia was also disconnected from SWIFT[58].

To watch: green energy contribution. Energy grids pose delicate management challenges. Energy supply must follow demand changes as instant as possible to prevent blackouts or waste of excess energy. The grid is therefore composed of a range of energy producers: from slow reacting but large base load providers up to very fast, but usually small peak load providers. For the same reasons, the same flexibility is desired on the demand side. In tight situations, grid operators ask large industrial consumers to switch parts of their machines off. Again, the larger the machines, the slower they are in reacting.

This is where Bitcoin mining comes in. In the words of the Bitcoin Policy Institute[59]: "Proof-of-work mining has complex and dynamic effects on global energy systems. While mining uses substantial amounts of electricity – currently 0.18% of global energy – it is price-sensitive, interruptible, adjustable, and location-agnostic, which pairs well with intermittent renewable energy sources like wind and solar, as well as stranded sources of energy like waste methane."

The electricity consumption of Bitcoin is substantial, however, considerably less than of those industries relevant to the fiat monetary system: military-industrial complex[60] (30-60x of Bitcoin), banking/finance (22-50x of Bitcoin), and gold mining (2-5x)[61].

The properties of Bitcoin mining make it uniquely qualified as a location-agnostic, very fast-reacting and yet large energy consumer to support the stabilization of energy grids. Mining can be leveraged in three ways to help decrease emissions of existing fossil sources of energy and increase the fraction of renewable sources of energy.

- First, to prevent blackouts, energy grids tend to overproduce. In the case of fossil sources of energy, this not only leads to energy waste but also unnecessary additional emissions. Bitcoin mining can help to reduce emissions by mitigating methane and CO_2 emissions from landfills and flaring/venting of excess gas at refineries. Instead of emitting into the atmosphere, they are used to generate power to run a mining operation. Bitcoin mining helps reducing emissions and supports the financing of such operations[62].
- Second, grids are increasing the fraction of renewable sources[63]. As renewables are intermittent sources (sun does not shine always, wind does not blow always), they contribute to grid volatility, thus making it harder to keep grids stable compared to fossil power plants that provide stable base load. In such situations, Bitcoin mining can help finance the increase of renewables, location-agnostic, while decreasing volatility and preventing blackouts[64].
- Another large source of clean energy that deserves a bigger role in the energy transition according to the International Energy Agency is hydropower[65]. Bitcoin mining can support the financing of more hydropower operations[66].

In one sentence: Bitcoin mining is evolving as a self-financing global search mechanism for the cheapest sources of energy. Since mid-2021, most new renewables undercut cheapest fossil fuel on cost[67]. Hence, we can expect an increasing contribution of Bitcoin mining to a global path of a renewable energy future.

So, although the energy debate on Bitcoin in 2022 has been dominated by energy shortages because of

When	Who	What
February 2022	KPMG Canada	Bought BTC and ETH for its corporate treasury[86]
March 2022	Fidelity	Offers clients exposure to 401(k) pension plans[87]
	MicroStrategy	Takes out loans to buy more bitcoin[88]
April 2022	Goldman Sachs	First lending facility backed by bitcoin[89]
	NASDAQ	Survey reveals 72% of financial advisors would increase their crypto exposure if a Bitcoin spot ETF is approved[90]
May 2022	GS, Coinbase	In a first, Goldman Sachs facilitates bitcoin-collateralized loan to Coinbase[91]
June 2022	No major news	(Worst quarter since 2011 for Bitcoin)
November 2022	No major news	(Yearly low of Bitcoin)

Table 2: Institutions engaging in Bitcoin during first half of 2022

inflation in TradFi and Ethereum's switch to Proof-of-Stake in crypto and the EC contemplating a ban on proof-of-work, regulators and activists need to learn to understand and appreciate Bitcoin's unique potential to contribute to a green energy future. If you hear 'Bitcoin steals energy from poor citizens and boils the planet' you may respond that lazy research or willful spread of misinformation are detrimental to crucial progress, we all need to mitigate climate change – and to fix our broken monetary system.

A closing remark on the "ESG" narrative. While the core idea of caring about the planet is in the utmost interest of humans, the way ESG in TradFi has been implemented does not bring us there. The twisted narrative got a deserved backlash in 2022 as widely reported in TradFi news media[68]. Rather than changing business operations, "ESG" is facing blame as a misused instrument for gatekeeping companies in (or out) of indices to become investable (or not) for institutional investors by introducing criteria that sound noble but have nothing to do with a company's performance (e.g., Tesla being kicked from the DJ Sustainability index).

To watch: institutional adoption. Although crypto news in 2022 was dominated by noises of the now dissolved band "LUNA & the CeFi Collapses feat. FTX", professional institutions continued to seriously engage with Bitcoin and the crypto space. Throughout 2022, the overall amount of Bitcoin in corporate treasuries (plus a few government treasuries) remained stable above 500'000 BTC[69].

At least during the first half of 2022, some institutions showed their continued engagement publicly. Some examples are in Table 2.

In December 2022, MicroStrategy announced Lightning-based products and services in 2023[70]. While most companies in the Lightning space focus on technical improvements or individual solutions, MicroStrategy's integration offering to get Lightning infrastructure ready "in an afternoon" for companies may find a largely untapped market given how early Lightning payments still are.

We invite you to read the in-depth Lightning interview with René Pickhardt in this Outlook edition!

Creating bankable products within the confines of TradFi like ETFs, ETPs, etc. has been one strategy for financial service providers to offer clients exposure to crypto. The regulatory situation with Bitcoin in the US – the largest financial market – is curious in that regard. While 14 futures-based Bitcoin ETFs (including one to short Bitcoin) have been approved by the SEC since beginning of 2021, yet not a single of the 15 applications for a physical Bitcoin ETF have been approved (illustration 5). Honi soit qui mal y pense[71].

The question is: Why is that? The main argument given by the SEC is that the Bitcoin markets can be easily manipulated. If that is the case, then it is not quite clear why that is different to future-based ETFs. Why allow one and not the other? One could even make the argument that a spot ETF is less risky and volatile than one based on futures. Plus, futures are fully dependent and correlated with the physical underlying, contrary to cash-settled derivatives.

Let's assume for a moment that Bitcoin would become this "superior form of money", as the maximalists propose, that would compete with fiat currencies and thus be perceived as dangerous by issuers, i.e., governments and (central) banks. What subtle, non-obvious ways would exist to discourage the use of Bitcoin aside official bans, withdrawal limits at ATMs, transaction limits, registration of wallets, and similar ideas for explicit

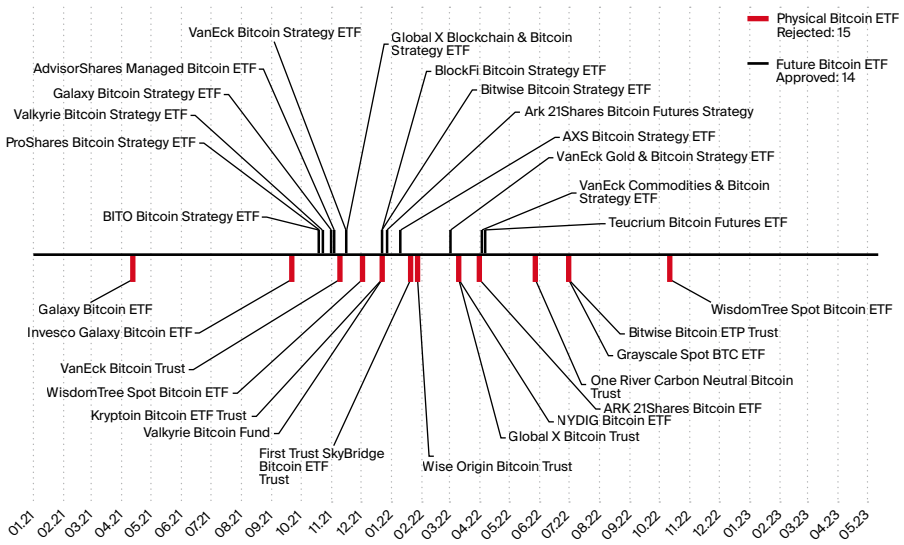


Illustration 5: Approval of Bitcoin future ETF versus rejection of physical Bitcoin ETF by the SEC over the last two years. Data: SEC.GOV Filings. Chart: Bitcoin Suisse Research

regulation? Having seen the measures taken about gold in 1933, 1943, and 1971 (see above), the idea that counter measures would be taken against a competing form of money is not entirely outlandish.

Let's start with a news piece crypto people may have overlooked as it sounds like some unrelated, obscure TradFi problem: in August 2022, gold traders by JPMorgan and other banks were found guilty of "gold spoofing". During an 8-year-period(!), they made use of the "power to move the market, the power to manipulate the worldwide price of gold." That is after JPMorgan, the largest US bank, was fined to pay $920m to settle spoofing allegations in 2020 – the largest fine for any financial institution since the Great Financial Crisis 2008[72]. All in all, ten traders from different banks were convicted – one of the biggest cases of the Justice Department.

Gold spoofing is the manipulation of the gold futures market by creating a false impression of demand, as measured by trading volume. It is done by submitting fake transactions and withdrawing them nanoseconds before an actual transaction can occur, to move the price in the desired direction. What sounds like manipulation was legal until and during the Great Financial Crisis 2008 and only became illegal with the Dodd-Frank Act in 2010[73].

Financial institutions engaging in spoofing just aim for profit without much concern in which direction the gold price moves. Governments, however, have a clear interest that the gold price remains low to protect their fiat currency from (perceived) competition. So, what if the gold price were suppressed by governments to keep "competition" at arm's length? That sounds a bit like a conspiracy question, however news outlets like Forbes[74] report on it and NGOs like GATA[75] have been researching this question for decades. More recently, thanks to Wikileaks we know of a diplomatic cable that was sent from the UK Treasury to the US Secretary of State on 10 December 1974. It is one of the only official documents giving merit to this suspicion[76]. The cable was sent a few weeks before the US government allowed citizens to hold gold again – 40 years after Executive Order 6102 banned the private ownership of gold. The cable is important as it suggests that the governments well understood that promoting a (not yet existing) futures market for gold would create price volatility and thus reduce the desire to hold gold in physical form for the long term.

Today, the ratio between physical gold and "paper gold" (futures, options, ETF, gold contracts, etc.) is estimated to be around 1:200 to 1:250[77]. For every ounce of physical gold there are 200+ ounces documented on paper. A dollar-based estimate says some $11T physical gold (of which central banks hold approx. $1T) stand against approx. $200-$300 trillion paper gold[78].

What are the reasons again, why we see so many future ETFs for Bitcoin, but no spot ETF approved in the US? With a Bitcoin futures ETF, the holder is not in possession of "physical" bitcoin but is exposed to an ETF that holds Bitcoin futures. According to Willy Woo and Seb Bunney, "the futures market dictates 90% of bitcoin's price[79]." While acknowledging the problem, Arman gives two reasons why this dynamic cannot be

sustained with Bitcoin versus gold[80]. First, bitcoin is much easier to custody and spend than gold, making it much more likely that investors will physically hold bitcoin. Second, arbitrageurs who sold bitcoin against a contract will eventually want to build up their bitcoin stack again and thus close/sell the contract.

In summary, while the price suppression problem exists, bitcoin holders have more options than gold holders to mitigate it. In the span from 5 November to 26 December 2022, a total of nearly $20B left exchanges: $6B in BTC, $5B in ETH, and $7B in stablecoins[81].

To watch: Bitcoin for payments. Despite the current crypto winter that also affects Bitcoin, the actual growth of the Lightning network has continued as can be seen in Illustration 6. Both the number of nodes and channels rose by approx. 50%. As channels need capacity to run, the overall channel capacity also rose by nearly 40% in BTC terms and 20% in USD terms, indicating an uptake in network usage. Lightning is well suited for small payments because it enables global, instant, extremely cheap transactions without mining and waiting 10 minutes for a block. That is one of the key reasons its uptake across countries in Latin America, Africa and the Middle East is so compelling according to Alex Gladstein[82].

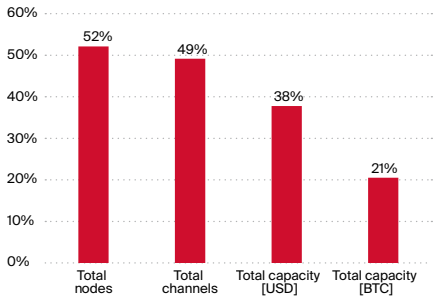


Illustration 6: Bitcoin Lightning network growth over last two years (Jan21-Dec22). Data: BitcoinVisuals, Clark Moody Bitcoin Dashboard. Chart: Bitcoin Suisse Research

To watch: Bitcoin stablecoins. Lightning Labs, the company behind the leading Lightning client in the market, raised $70M in a series B to develop Taro. Leveraging the Taproot[83] upgrade, which is active since November 2021, Taro will enable application developers to integrate digital assets (aka tokens) alongside BTC in applications both on-chain and via Lightning. Specifically, the company sees Taro as an "important step to bitcoinizing the dollar" by issuing assets like stablecoins. The initiative is addressing feedback from several countries with strong Lightning uptake across Latin America and West Africa that says adding stablecoin assets would expand financial access for many communities[84].

To watch: Bitcoin smart contracts. Based on technical ideas by former Bitcoin core developer Peter Todd in 2016, the company Pandora Core maintains the open-source project "RGB." With a somewhat broader vision than Taro, the RGB project aims for a generic smart contract system for Bitcoin and Lightning. While not a token protocol, RGB also enables the issuance of programmable digital assets (aka tokens). The key difference to systems like Ethereum is that smart contracts and their data are managed off-chain using "client-side validation[85]."

Both initiatives, Taro and RGB, are raising the bar for what it technically possible on top of the Bitcoin base layer and the Lightning Layer-2, respectively. Such developments will not only further strengthen the use case of Bitcoin as a payment system but put the idea of "Bitcoin DeFi" into the spotlight by enabling a next level of programmability of the Bitcoin/Lightning tech stack.

Predictions

- A third nation, most likely from Latin America, will declare Bitcoin (second) legal tender in 2023
- A first stablecoin on the Bitcoin/Lightning network will be issued in 2023
- A first non-crypto company will start using Lightning for payments in 2023

Final thought

Fiat currencies are in a crisis, the biggest the most. Nations are trying to reduce their dependency on the US Dollar. Expect more volatility as we go through this process of deleverage and unwind in the years to come. This base dynamic will affect all assets classes, TradFi and crypto alike.

Bitcoin, the decentralized peer-to-peer network to store and transfer value in digital form, is working and is as unstoppable as anything else in crypto. How its price in fiat terms will evolve depends on how the growing group of holders perceive it. Given all its properties, for investors with low time preference the trade is asymmetric with upside potential in the long run. You can also just save it, because in past times, money was meant to be a safe haven, particularly for uncertain times.

The author thanks Denis Oevermann for creating all the charts.
Disclosure: at time of writing, the author holds BTC.

January 2022

«Even if other countries do not believe in the investment thesis or adoption of bitcoin, they will be forced to acquire some as a form of insurance.»

Report of Fidelity Digital Assets on game-theoretic incentives for Bitcoin exposure

«It hasn't gotten better. It's probably gotten just a bit worse, ... »

Jerome Powell on his current outlook on inflation.

February 2022

«I think when all's said and done, investors will be given a choice: they have to invest in something, and if rates are rising, blockchain is going to be the most relatively attractive.»

Pantera Capital CEO on Fed rate hike. (via Pantera Capital)

March 2022

«After this war is over, 'money' will never be the same again...and Bitcoin (if it still exists then) will probably benefit from all this.»

Zoltan Pozsar, global head of short-term interest rate strategy at Credit Suisse (via NASDAQ)

April 2022

«When so much money, energy and talent flows toward a new thing, it's generally a good idea to pay attention, regardless of your views on the thing itself.»

Kevin Roose, The New York Times tech columnist on crypto (via The New York Times)

«(...)it's better to offend millions by standing aggressively for what you believe in than it is to try to keep everyone happy and end up standing for nothing. Be brave. Fight for your values. Be a maximalist.»

Vitalik Buterin, Co-Founder of Ethereum (via Vitalik.ca)

May 2022

«It's not arbitrage if you don't exit the position.»

@mhonkasalo, crypto researcher, on stablecoin depegs that are often resolved by arbitrage (via https://mhonkasalo.substack.com/)

«Worthless.»

Christine Lagarde about cryptocurrencies on Dutch TV last Sunday (via yahoo!finance)

«As we begin to rebuild UST, we will adjust its mechanism to be collateralized.»

Do Kwon on Terra's flawed peg mechanism (via Twitter)

June 2022

«The most important thing is to get something launched. It almost doesn't matter how one designs it.»

Do Kwon on launching Terra 2 that later caused oracle errors impacting funds on Anchor and Mirror (via Twitter)

«Mike do you know even one person who has a problem withdrawing from Celsius?, why spread FUD and misinformation.»

Alex Mashinsky, Founder and CEO of Celsius one day before Celsius halted all withdrawals on June 12 (via Twitter)

«We manage risk and prioritize the security of customer funds first and foremost. We keep things simple. No DeFi lending activities, no algorithmic stablecoin staking or lending, no derivative assets, and certainly no stETH.»

Posted via Voyager's Twitter before they announced a $650m exposure towards 3AC (via Twitter)

July 2022

«Some, like bitcoin, and that's the only one, Jim, I'm going to say because I'm not going to talk about any one of these tokens [that] my predecessors and others have said [are] a commodity»

SEC chairman Gary Gensler (CNBC interview with Jim Cramer, video clip)

«DeFi's smart contracts and transparency seem to be provocative antidotes to the toll takers, opacity, and uncertainty in traditional financial markets. As a result, DeFi should continue to gain share.»

Cathie Wood, CEO, and CIO of Ark Invest on DeFi. (via Twitter)

«This is not an economy that's in recession. But we're in a period of transition in which growth is slowing ...»

Treasury Secretary Janet Yellen on recession fears (via Dailywire)

August 2022

«Also, small grammar nuance: in English when talking about things like proof of stake, we don't say 'it's a security', we say 'it's secure'. I know these suffixes are hard though, so I forgive the error.»

Vitalik Buterin, Co-Founder of Ethereum on Michael Saylor's opinion about ETH being a security (via Twitter)

« Financial privacy should be the norm. People don't like getting their page views tracked by companies running ads - but don't realize their lack of privacy is so much worse in financial services. »

Brian Armstrong, Co-founder & CEO of Coinbase on discussions sparked after crypto mixer Tornado Cash was sanctioned (via Twitter)

«I think the next 10 years is when crypto has to transform into something that is not based on promises of being useful in the future but is actually useful, because a lot of applications are promising in theory, but they're just completely not viable because of scaling issues today.»

Vitalik Buterin, Co-Founder of Ethereum on scalability and adoption of crypto (via Timestabloid)

September 2022

«Telling people they can opt out of inflation by investing in cryptocurrencies is not responsible leadership.»

Justin Trudeau, 23rd Prime Minister of Canada, on crypto investing after Canada inflated M1 money supply by 5.7x within the last 20 years. (via Twitter)

«I could see cryptocurrency having a big role in a Renaissance because people just aren't going to trust the central banks.»

Stanley Druckenmiller, American investor, hedge fund manager and philanthropist, on current macro conditions and central bank policy. (via CNBC)

October 2022

«If Credit Suisse was a DeFi bank we wouldn't wonder if they had enough money, we'd just know.»

Hugh Karp, founder of Nexus Mutual, an alternative risk sharing platform covering smart contract failures & exchange hacks, on recent liquidity concerns regarding Credit Suisse. (via Twitter)

«The lion's share of HNW investors across all regions are conscious and aware of the risk that comes with investing in crypto and are happy to go direct as opposed to the safer option via funds [like ETFs].»

Sergel Woldemichael, Sen. WM Analyst, on key results of GlobalData's 2022 Global Wealth Managers Survey

November 2022

« Money is as or more important to people than religion is. We interact with it every day, in all sorts of manners and just as mathematics or language are immutable and open to the entire human race, so too should the exchange and management of money. That is the principle that makes this entire ecosystem important. That is the principle that justifies everything that we do, and if we lose that, it will be something we will regret for the rest of our lives, because we had that opportunity. »

Erik Voorhees, founder and CEO of ShapeShift, on crypto regulation, Source: Bankless

«This isn't about aiming high and missing. This is about recklessness, greed, self-interest, hubris, sociopathic behavior that causes a person to risk all the hard-won progress this industry has earned over a decade, for their own personal gain. [...] We let clowns ride under our banner while they sell us out for their own interests. We give them power to speak for us but they haven't earned that privilege. When they blow themselves up, it's our house, our reputation, our people which bear the brunt of the damage. [...] Don't trust. Verify. [...] Survival & mission above profit.»

Jesse Powell, Co-founder & CEO of KrakenFX, on the FTX and Alameda disaster (via Twitter)

«Never in my career have I seen such a complete failure of corporate controls and such a complete absence of trustworthy financial information as occurred here. [...] From compromised systems integrity and faulty regulatory oversight abroad, to the concentration of control in the hands of a very small group of inexperienced, unsophisticated and potentially compromised individuals, the situation is unprecedented.»

FTX's restructuring CEO John Jay Ray III, who oversaw Enron's bankruptcy proceedings, in a bankruptcy court filing on the lack of financial oversight surrounding the FTX saga (via WSJ)

December 2022

« The apparent stabilization of bitcoin's value is likely to be an artificially induced last gasp before the crypto-asset embarks on a road to irrelevance »

The ECB on November 30th 2022 on Bitcoin and highly volatile crypto markets (via ECB blog)

Interview

“We need to take the laser eyes seriously!”

An interview with René Pickhardt[103], independent Lightning developer and data scientist, about scaling Bitcoin, the Lightning network, unreliable payments, user experience, and the importance of staying focused

by Dr. Marcus Dapp

Marcus Dapp (MD): You present yourself as an independent open-source Lightning developer. Could you explain what that means, and why you think it’s important to have independent open-source developers in the Bitcoin/Lightning space?

René Pickhardt (RP): Two terms are essential in understanding what I do – software and open source. As a core principle I believe that knowledge wants and should be free, software in this case is a form of speech. The concept of open-source goes against the popular opinion that copyright protection is needed to make a living as a programmer – I want to prove the opposite.

Open-source development means that source code is made freely available for modification and redistribution by others. The value proposition of Bitcoin is to be a decentralized peer-to-peer network. The concept requires a certain level of ownership, meaning users should investigate it, review it, help, and see if they can contribute to the network.

From a “Bitcoiner” perspective there is a reasonable case to be made that independent developers are important because they do not have company interests. They work to the best of their knowledge and try to do what is best for the project.

The community supports four major clients[92] to connect to the Lightning network: Core Lightning by Blockstream, LND by Lightning Labs, Eclair by Acinq, and LDK by Spiral. Most active developers are funded by one of those companies which can be a problem. This can be compared to lobbying and that is why independent developers are needed. I consider myself a “pleb” [community slang for the normal, non-rich Bitcoiners, ed.] and I am not invested in major Bitcoin companies. I’m just an open-source activist, I’ve been active in open educational resources and open access before. This is a huge part of my motivation to be in this space.

MD: During last year’s turmoil with multiple CeFi companies, some Bitcoiners on Crypto Twitter were raising the slogan: “Bitcoin is not crypto.” What is your view on this statement?

RP: I initially had to learn what crypto is and there is a crystal-clear difference in my head. In another interview I said that in my perception, Bitcoin started as a very honest project with a very concrete problem to solve – with-

René Pickhardt

out marketing or profit in mind. But as soon as Bitcoin showed that it could attract people and make people perceive it as money, alternative currencies were created because the code can be easily copied. It is very attractive if you print your own currency and make people believe it's a currency. Since the underlying technology is already complicated enough for people to understand, it's hard to see the differences… All these projects after Bitcoin seemed to me very different, which is why I decided early on to ignore them.

MD: Could you elaborate a little bit on these differences?

RP: In my view, one of the first competitors was Litecoin. What did they do? They went and changed the block time and the proof of work algorithm. As a technical person, I don't see a huge difference. But as a human being, I see a huge value proposition in people agreeing on using the same system, agreeing on a standard protocol. The Internet would not work if everybody had their own networking protocol, and we would not have the Internet Protocol that connects all these networks. By principle, it never made sense to me to have all these alternative currencies that are being brought into circulation. I would even say, if anybody had a good idea how to fundamentally improve a currency through a technological breakthrough, it should go back into Bitcoin in my opinion.

MD: There is a lot of debate and confusion about who controls the Bitcoin system. How do you see the three groups: miners, developers, and users, people running nodes in the network. How is power distributed in the Bitcoin network?

RP: I have no idea (laughs). I wish I knew. Maybe it's good not to know, maybe that is part of the answer. There is this narrative that says the users have the ultimate power, which boils down to the argument that users eventually decide which software to use. You could argue that this is highly democratic, and we have seen situations where users didn't have consensus on what they perceive to be Bitcoin and where the network split off. There are enough arguments to say the users have the final verdict.

MD: From what you see working on Lightning, would you say Bitcoin has become sufficiently decentralized today? Should we do more?

RP: How do you define «decentralized»? The term is rather vague, everyone has their own perception of what it means... It's crazy to me that the community of Bitcoin developers is rather small, given how much economic interest the system receives globally. On the other hand, software scales extremely well. It makes sense to me that a small number of developers can make a big difference.

MD: Now, let's dig into the Lightning network. What is the challenge in scaling Bitcoin and making the promise by Satoshi Nakamoto, of having a peer-to-peer payment network, a reality?

RP: When I say scaling Bitcoin, I include Lightning, because for me it is just an application of Bitcoin. Even in the earliest versions of Bitcoin you could do 2-of-2-multisig[93] transactions, a key enabler for using Lightning. Now, on Lightning you have issues around liquidity: I do have a payment channel with somebody and in there I can transact as much as I want, but I'm limited to the amount of bitcoin that is locked in this payment channel. If somebody else has a payment channel with whom I'm interacting, I can use my payment channel to send that person money and ask that person to forward the money. (c.f. Illustration 1).

This is a classic routing problem, and it is easy to compare it to classic road traffic. But: roads don't deplete, if you have a lot of traffic; and if you have congestion, at some point in time some cars will somehow pass by, and the jam will resolve.

On Lightning, money often flows in one direction, to one peer, and the channel may become depleted after some time. We do not know how much liquidity a peer has prior to asking them to route our payment. This is mainly due to technical and privacy reasons, but it brings a degree of uncertainty with it.

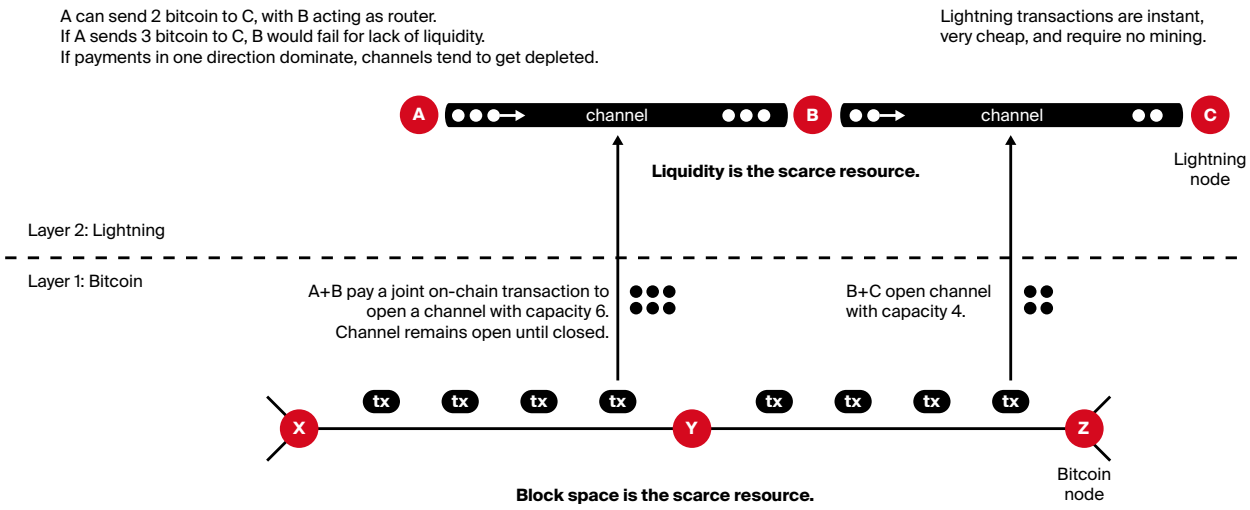


Illustration 1: How do Lightning payments on top of Bitcoin work? Source: Bitcoin Suisse Research

Put differently, the Lightning network as a technology is not always reliable. I say it is "unreliable by design", which got me a lot of push back, but I stand by the statement. The protocol is as unreliable by design as the Internet Protocol is. Developers should introduce more reliability features and there are countless ideas floating around. Another big issue to tackle is user-friendliness.

When you think about it: it is a wild concept that you can make a payment and within a second a person in Australia has control over the money – without a third-party involved. That we can invent something like this and develop it, is a breakthrough for society and it is still one of the most under-recognized technologies, not only in the "crypto space", but in society in general. Installing and maintaining your Lightning node and making sure that it is always available and ready to be used – that's a different story. This is certainly also part of the challenge of getting scaling adoption, not on a technical but on a sociological level.

MD: You hinted that scalability is not only a technical question, but also a social and practical question. One criticism is: Even if Lightning would work, it wouldn't be possible to onboard 8 billion people because we need too many base layer transactions to open all these channels. How do you envision to onboard the next half a billion people?

RP: The question is who wants to use the technology and how. Take the internet as an example: almost no user maintains their own web server – and even people that have their own website usually have it hosted somewhere else.

It is probably similar for Bitcoin: it is completely counterintuitive, almost absurd and grotesque: you invent peer-to-peer money and then you decide, it's too complicated, let somebody else handle it for me. In my mind that doesn't make too much sense, but I do understand that there are situations where people would want that. For example, we have a community of people who accept Bitcoin as intended: I have self-sovereignty, control, I know what I'm doing. Now I want to interact with somebody, and they don't care about any form of money and are very willing to just have some service provider because that's the least friction for them. They just don't share my problem. From a very practical perspective, I would assume many of the 8 billion people will eventually use some form of custodial service provider if Bitcoin were to be universally used and accepted. And if I am wrong, we would have to think about how we change the limitations that we currently have. That is a very, very future problem. I think the solutions are obvious, but there is too much time to not tackle them…

MD: In a piece for BitMex you discuss the Price of Anarchy from selfish routing on the Lightning network[94]. Could you explain what the piece is about and how it relates to the scaling discussion?

RP: I have been tricked by Bitcoin when I read the White Paper[95]. It seemed very convincing to me, and I was certainly not an expert on decentralized systems, I had no questions about scaling whatsoever. The paper appeared to be somewhat scientific, it even had a limitation section where the probability of a double spend was estimated. I would argue that Satoshi was aware of the question of how many transactions you can do with this system, but he didn't raise this question at all in the White Paper. That helped not only me, but a few others to get convinced of Bitcoin, whereas others, experts in the field, were saying, this will never work and dismissed it. I think the critics have been very much on point on a technical level. You needed to have somewhat naive people who said, "yes, it all makes sense, and we will show you!" Only later, you hit the roadblock and realize, we really need to fix the transaction limit if we want to have payments, and a cash system needs payments. So, that is why the Lightning network exists.

With all this in mind, the Lightning network makes a very convincing case. You have this payment channel, it's off-chain, and inside we can transact as often as we want, just limited by Internet bandwidth and that's not a real limitation. Luckily, I had a little bit more knowledge about networks. Yes, I found it very convincing that it can achieve a certain amount of scale, but from the very beginning I had a certain amount of skepticism because a network like this has its own challenges. I think I can grasp these challenges much better nowadays. Much of my research has been centered around the question of how far the "Lightning network effect" goes. How much scaling can we achieve? How many payments can we really make?

MD: Why is that a question when you just said it's only limited by bandwidth and so potentially limitless?

RP: Nuance matters here. It is potentially limitless but only if you and I have a payment channel, and we transact back and forth with high frequency all the time. And two other people have their payment channel and they're doing the same. Then it scales linearly with the number of payment channels and our very specific transaction behavior. You can see from this example that this is probably not how such a network would be organized. In my intuition, such a network would be organized as a small-world network[96] from the topology. Small-world networks tend to have highly centralized nodes which might be a limiting factor as everybody wants to route across them. How much traffic can they handle?
In a more scientific way, we know that in networks with routing you have selfish behavior. Let's say you have a network and millions of participants who want to pay each other. How do you optimally fulfill all these payment requests, given the network constraints like some channels are small, some are big, some are cheaper, etc. This is a classical optimization problem in mathematics, and these are usually hard to solve. On Lightning, because it is a peer-to-peer network, we don't want to have a central coordinator who does all this optimization work, and we don't want to introduce credit or something in between. We want to settle in real-time, how do we do it?

I, as the sender, decide what route I take. Which route do you take if you travel to Berlin? You take the quickest route. Now everybody takes the quickest route and then the quickest route gets congested. Given the network topology, you have this selfish behavior as an effect. To handle the congestion, you can have retrials and things don't go optimally anymore for anybody. How much more expensive (fees, waiting time, etc.) does it get for everybody to fulfill their payment requests in comparison to having a central coordinator? This, defined in a general form, is called the "Price of anarchy[97]." I was trying to define it properly for the Lightning network because to understand how far the network scales, you want to first understand how painful it is when everybody is acting selfishly.

For example, I'm known for the so-called "Pickhardt payments", the provably optimal

way of delivering a payment. But is this a good thing? It is the most selfish way people can use the network!? If the price of anarchy is high, well then maybe it would be better if we never had discovered them even though for an individual it's still good to use them. That's the absurd thing about networks, right? So, theoretically you have infinite scale on Lightning, but practically speaking, for it to be useful, the network needs to have a certain topology. That topology is not centrally coordinated, but there's another form of selfish behavior: with whom do you open your payment channels? Routing nodes engaging in selfish behavior can be very bad for the network. There's a lot of market economics and game theory involved and those are extremely hard problems.

MD: So, you spend a lot of your time on network and statistical analysis of flows through the Lightning network?

RP: Well, the flows I usually don't see, but one thing that people who run nodes have discovered is that channels tend to be one-sided. There's depletion because people send money, it doesn't go forth and back all the time. Technically it can, but practically there is more demand in one direction than in the other, usually. In Pickhardt payments (c.f. info box) we estimate the probability that the channel has a certain liquidity to decide if we want to use it for making a payment. But if a channel usually is one-sided, that's a different prior to my probability distribution, and just assuming uniform distribution as we did in the paper. A lot of people already knew channels deplete, and that the probability distribution has a certain shape. With this paper I was able to derive the probability distribution just from looking at the public information on the network. This is because the size of the channels and the fees that are being charged are observable, and at that time routing decisions were mainly made by fees. Therefore, one can see how much more frequently the channel is expected to be used in one direction than in the other direction.

What is the crucial learning from this work? A payment is not a path finding problem, it's a transportation problem. You transport satoshi through channels from A to B. And you transport them through a network, that's why you have a flow problem, and you want to minimize the cost of this flow. It's a very different problem! For four years of Lightning Network development, people have looked at the wrong optimization problem.

MD: Wow. So, you made a lot of people happy?

RP: No, I created a lot of anger (laughs). One of the issues is that the minimum-cost-flow problem[98] is computationally heavy if you have a base fee involved[99]. It was clear that people would also want to optimize for fees and not only for probability. So, I'm coming up with a beautiful solution, saying, "Look guys, the problem here is how we designed the protocol as it allows this base fee. Now the payment problem for everybody to solve is very hard…

Pickhardt Payments

In the words of the inventor:

Easy version: As the Lightning network uses the concept of payment channels between users (c.f. Illustration 1), we want to make routing decisions based on the likelihood of channels having enough liquidity to route our payment. Pickhardt Payments are the provable optimal way of conducting bitcoin payments over the Lightning Network by focusing on probabilities about remote liquidity.

Scientific version: Pickhardt Payments are the method of delivering satoshi from one Lightning network node to another by using probabilistic payment delivery[104] in a round-based payment loop that updates our belief of the remote liquidity in the Uncertainty Network and generates optimally reliable and cheap payment flows[105] in every round by solving a piece-wise linearized minimum-cost-flow problem[106] with a separable cost function.

MD: If we would only have the dynamic fee rate, then it would be much easier? What prevents us from removing the base fee? Would you need to change the protocol for that?

Oh, a lot easier, yeah! With only a fee rate, the problem is linear because the fee rate is just a linear function. However, it's a protocol change, and protocol changes in Bitcoin and Lightning are supposed to be difficult, I guess (laughs). It's funny, until I published the paper, everybody talked about the fee rate, and nobody cared about the base fee. The base fee has unintended side effects even when the design choices seemed reasonable at the time. Personally, I find it absurd that the question to remove the base fee got so politicized, because half of the network already changed configurations and does not charge a base fee anymore (c.f. #zerobasefee hashtag on twitter). It's completely voluntary and a lot of reasonable node operators skip it. This already shows that people make decisions even if it does not benefit them directly.

You do not need to change the protocol, but the default base fee is 1 sat only. In all fairness, a 1-sat base fee is not hurting because I can just ignore it. But as people always talk about security: if the base fee stays in the protocol, of course it is scalable by the node operators, because if they know that people will have to pay the base fee, then they can charge 2 sat, and then 3 sat. When do you start caring for the fee? It is very reasonable to make this change permanent, and we have very strong theoretical arguments. As I said, everybody routing selfishly may not be the best thing for the network, either.

MD: Cool. Let's move to the last topic: Layer-3, things on or on top of Lightning. The Taro project by Lightning Labs made the headlines in 2022, saying they will bring stablecoins to the network. The RGB project has also been chugging along for making smart contracts possible. How do you see smart contracts enabling digital assets/tokens on Bitcoin/Lightning? Have you investigated these projects?

RP: Well, as I said earlier, I am very principled and I think it's good if we have Bitcoin. I do not see the direct use case of issuing other tokens. Specifically, the obsession with stablecoins – I really do not get it. I mean, I do get it from a VC/company point of view because a stablecoin for companies is literally an interest-free and risk-free loan because if the thing burns up, got hacked, well... they say "we are bankrupt." I do understand why stablecoins are extremely interesting for rich and wealthy entities. But for me as a Bitcoiner, I do not need a stablecoin.

How fees work on Lightning

Payment fee = Base fee + Fee rate

The base fee and the fee rate are chosen by each routing node. The base fee often is only 1 sat or even 0 sat for those nodes that follow Pickhardt's recommendation to skip it to improve routing (hashtag #zerobasefee). The fee rate depends on the amount transferred. It is given as an amount in satoshi per satoshi transferred. These median figures[107] at time of writing are to illustrate the scale:

base fee: 0.001483 sat = $0.000000269
fee rate: 0.000024 sat per sat = $0.000000004360 per sat

1 sat = 0.00000001 bitcoin

As all routing nodes make their own decisions on the fees, one can look at the network as a fee market for routing. This information is used to find best routing paths through the network.

Pickhardt's work fundamentally improved the approach to this core optimization problem and thus made the Lightning network faster and cheaper for all users.

MD: The argument usually brought up is, stablecoins make on-ramping of people easier because they have something that is already crypto, a token, but it's still not as volatile...

RP: A stablecoin on the Lightning network brings together the worst of all worlds. The entire idea of Bitcoin is to be an alternative electronic peer-to-peer cash system with no trusted third-party. The US Dollar is certainly a system with a trusted third-party. A stablecoin introduces another trusted third-party, we could call it fourth-party. We just discussed how dif-

ficult it is to solve the transportation problem on the Lightning network to achieve decentralized money and I am willing to take the pain. But why would I take "doubly-trusted" money and put it on a technology that is extremely poor for this? That does not make any sense to me. I am not buying it. There is a high financial interest of people trying to sell the story of stablecoins as bridge technology. I personally do not think they are bridges.

MD: RGB is trying to follow a broader vision and bring to Lightning what people call smart contracts. What's your opinion on that? Are you saying it's not needed? Well, does it not make sense to have some functionality on top of making payments, for financial primitives like insurance, three groups decide on something, and then payments flow; or more complex mechanisms that people have been using for centuries in financial markets to do certain transactions, to reduce risks, to limit uncertainty about the future, etc.?

RP: I'm not an expert at finance, so I don't know. Technologically, it seems like a project where people are putting a lot of effort in. As I said, as new technologies come, it makes sense to back port them eventually. Look, if there's reasonable demand for reasonable problems, sure that helps. The cash case is difficult enough. If we cannot solve the cash case properly then I don't have to think about…

Maybe I'm a little bit too stubborn or blindsided here. Sometimes it makes sense to think about other problems to progress with your initial problem. You see, people outside of our world make fun of us for laser eyes, right? I think the entire laser-eyes meme is about being laser-focused. While I never put laser eyes on any of my pictures, I'm sure I was pretty laser-focused on solving these problems and this is where I'm coming from.

MD: Last topic: adoption. After El Salvador's big announcement in September 2021, you could see Lightning capacity jump to 3'000 bitcoin. Since then, it further increased to 5'100 bitcoin capacity. I would assume that if people lock bitcoin into Lightning, they do something with it, they are not just putting them there. Do you share that view, and where are all these Satoshi's used currently?

RP: I think mempool.space[100] shows a geographic map of where all the Lightning nodes are located. The last time I checked there was no node in El Salvador, which I personally find quite remarkable. Given the fact that even among Bitcoiners there's this outcry that El Salvador's official Chivo[101] wallet doesn't work properly, and it is not self-hosted... Well, there is that.

And to be fair: 5000 bitcoin? I think on the first day Satoshi started mining, you could mine more than 5000 bitcoin in one day. What is deployed on the Lightning network is an extremely tiny fraction of all the bitcoin there are. So, while we do see some form of exponential growth, we probably need quite a few more years to see adoption at scale.

Fedimint
Fedimint is a new protocol for the emerging approach of "community custody" that allows a community (village, association, community bank, etc.) to entrust a group of trustworthy individuals to become a collective of custodians allowing everyone to transact privately.
www.fedimint.org/

Impervious
The first Bitcoin Lightning-native web browser featuring a suite of peer-to-peer tools for communications, data transport, and payments, built directly into a web browser.
www.impervious.ai

RGB
Scalable and confidential smart contracts system for Bitcoin Lightning network. It represents a post-blockchain, Turing-complete form of trustless distributed computing which does not require to introduce tokens; although digital assets can be realized.
www.rgbfaq.com

Taro
New Taproot-powered protocol for issuing assets on the Bitcoin blockchain that can be transferred over the Lightning network for instant, high volume, low fee transactions. The immediate goal is to enable the issuance of stablecoins on Bitcoin.
https://docs.lightning.engineering/the-lightning-network/taro

MD: Where will it come from? Even if El Salvador is not using Lightning proper by having their own nodes, you could argue that a country making such a decision creates demand. Also, financial institutions are interested in Bitcoin, maybe rather for investment than as payment. And then, there are the 'plebs', literally everywhere, it's hard to know where clusters, maybe even circular economies of users, are emerging. How will this evolve in the next year and beyond?

RP: I think, with the Lightning network, we are reaching a tipping point where Bitcoin becomes so usable for people to quickly build an application. I can imagine that back in 2012, using Bitcoin to accept payments on your website was quite a pain. Nowadays with Lightning and maybe Lighting service providers[102], it is much easier to use Bitcoin. I learned at university that technological cycles usually take two generations. I have no reason to believe that Bitcoin and Lightning should be faster. Because you need the young people who come in, who grow up with it, see it. If I were a student in a university now and I wanted to create a startup and stumbled into the problem of payments, I would use Lightning. But then, some students grow exponentially with their companies, but most of them fail, to be frank. So, it takes time.

MD: Any interesting Lightning applications you have seen like games or others?

RP: Let's look at gaming. I'm surprised that tipping on the Internet in general is not working with something like Bitcoin as of right now. Companies, especially for micropayments, tend to take huge cuts. You could argue that the price fluctuation of Bitcoin is less than the usual cut. Apparently, not even there, people are picking this up. And this would be closest to gaming because streamers are often being tipped. I would love to see that happening; to me it makes sense.

MD: Do you think there is any chance that Elon Musk will make the "right decision"? Would it boost adoption of Twitter

RP: Lightning Strike made the announcement this year at the Miami Bitcoin Conference, that they have so many payment service providers in the United States who are potentially able to integrate Lightning. I remember retweeting this and saying that this technology is "unreliable by design." But you know: Bitcoin seems to be so useful that we got a second chance. Technically, people learned by 2013 that it is too hard to use and not interesting. They tried and it did not work. And it seems like we are getting a second chance. Maybe this is the chance, and the technology needs to be finished first, peer-to-peer money is a tough concept – we need to give it time.

MD: So, what would you like to see happening in your space to become ready?

RP: We need decent user experience. Entering this space as a technical person is one thing, but this is not the norm. Everyone should experience a user-friendly interface which they can understand. The protocol user experience also needs to improve due to severe issues with user experience and protocol definition. One example is backing up Lightning nodes. A core concept in crypto is "not your keys, not your coins." But here, we have to say "not your keys, not your revocation transaction and state database, not your coins." That is not ideal.

MD: So, a long way.

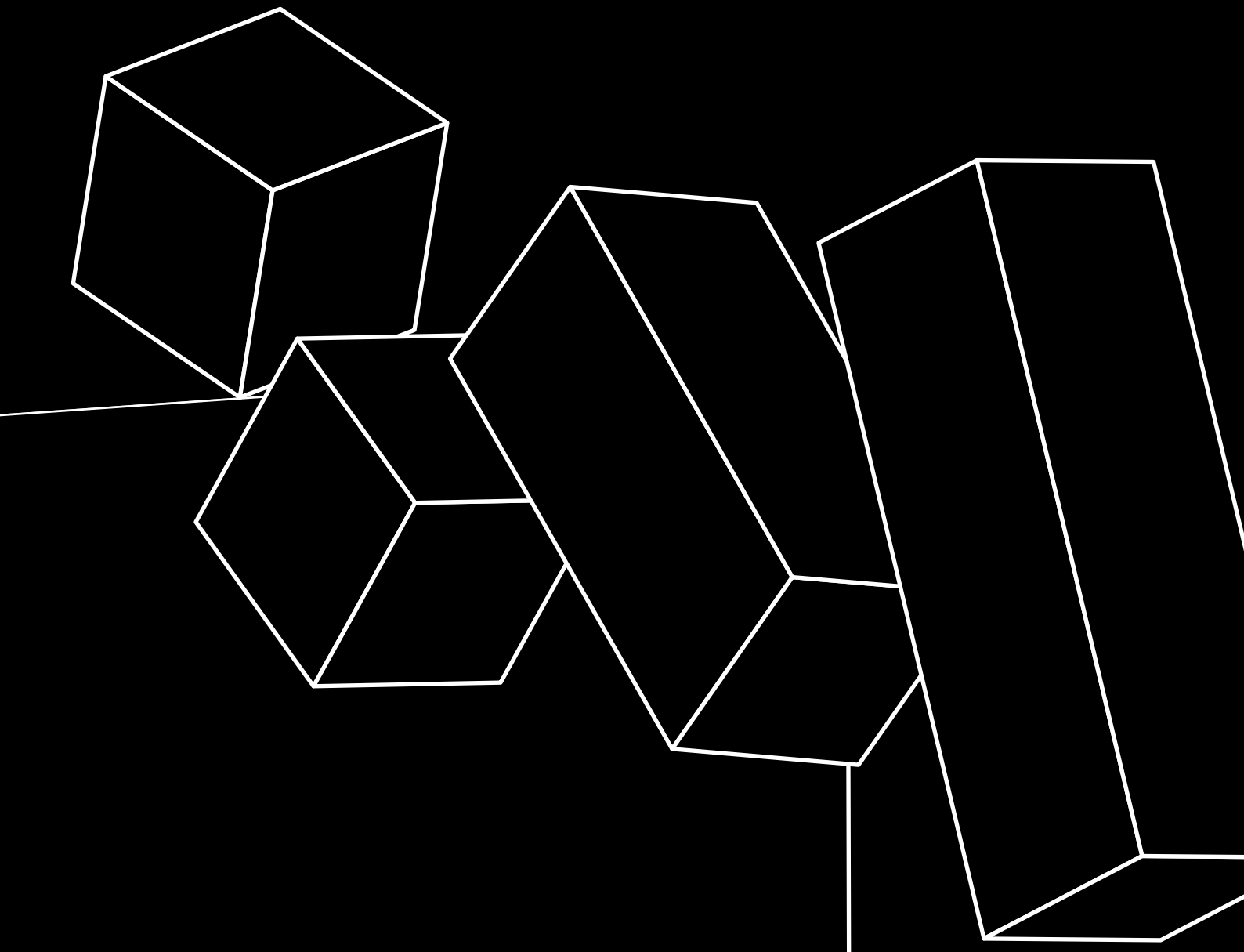
RP: And that is the point! When Lightning is just being used in a custodial way, it is very hard to compete against solutions such as PayPal. Guess what, people are already on PayPal, the network effect is already there, the dollar is the sole "stablecoin", and it works in whatever jurisdiction the people wish to use it with their currency. We need to achieve the same level of user experience while allowing self-custody of your own assets. If that won't happen it will be challenging to convince people that do not lay their focus on privacy. User experience is everything. Which is why I am looking at the reliability of the Lightning network.

At the Lightning Conference, Christian Decker (Core Tech Engineer at Blockstream and Bitcoin enthusiast) said that 5% of all

payments could not settle meaning there is a success rate of only 95% that your payments go through. If we fix these things, then we can think about stablecoins. Do not slow down but refocus: take the laser eyes seriously!

MD: Thank you, René!

This is a heavily abridged version of the interview. For the full transcript and video, please visit www.bitcoinsuisse.com/outlook-2023/pickhardt-full-interview.



Article

Crypto Markets Withstanding Uncertain Times

Multiple market cycles in the crypto market have shown that even large and established crypto custodians or exchanges may disappear very quickly. In 2022, events such as the collapse of Three Arrows Capital, Celsius, and FTX had a lasting impact not only on consumers, but also on public perception of the crypto market.

by Gian Stäuble

Global geopolitical tensions, challenging macroeconomic environments, and difficult market conditions have shaken the confidence of many investors. As a result, the markets are under pressure and the underlying promise of crypto and blockchain technology needs to be remembered to restore trust.

We are now shedding light on some of these important developments to understand how they unfolded affecting clients across the globe, including insights into the happenings around FTX last November from Niklas Nygaard, a Senior Trader at Bitcoin Suisse. We provide a look behind the curtain on how Bitcoin Suisse reacted swiftly in these turbulent times and what learnings could be taken.

Celsius Network

June 2022 - Celsius Network, a centralized finance (CeFi) platform, custodied digital assets on behalf of investors and offered rewards in return. According to their terms of use, this granted them the right to "use or invest such digital assets in Celsius' full discretion". As these operations were not isolated from risk, deposited assets "may not be recoverable" if Celsius would be unable to meet its obligations[108]. On Sunday, June 12, 2022, Celsius announced they would halt all withdrawals, swaps and transfers between accounts due to what they called "extreme market conditions[109]". At the time, Celsius was used by more than 1.7 million users. They also ran a native platform token "CEL", which fell over 70% in value after the firm's announcement. Later in July 2022, Celsius filed for bankruptcy[110].

On September 8, 2022, Oren Blonstein, the Chief Executive Officer of Celsius, outlined a plan to revive the firm to Celsius' employees[111]. At the time of writing, it remains unclear whether Celsius will be successfully restructured or if its assets will be liquidated and its business closed.

Three Arrows Capital & Voyager Digital

June 2022 - Three Arrows Capital (3AC), a prominent cryptocurrency fund with ~$18 billion in assets, was hit by the market downturn as the contagion from the developments around Celsius spread. The fund faced massive liquidations on FTX, Deribit, and BitMex after it suffered from closely linked exposure to the LUNA collapse and the stETH-ETH depeg. In the process of unwinding positions, one wallet linked to 3AC was seemingly forced to sell more than 60'000 stETH to pay off loans and debts, contributing to the stETH-ETH depeg and getting even more entities in trouble[112]. On June 27, 3AC then defaulted on a $670 million loan consisting of 15'250 Bitcoin and 350 million USDC that was issued by Voyager Digital. On the same day, a British Virgin Islands' (BVI) court ordered 3AC into liquidation, forc-

ing them to liquidate assets tied to their BVI company. In August, the advisory firm Teneo was appointed to handle the liquidation of 3AC[113]. It has been reported that the founders, Kyle Davis and Su Zhu, are not being cooperative in tracing and recovering the firm's assets to make investors whole[114].

July 2022 - Troubled broker Voyager Digital had to file for Chapter 11 bankruptcy protection after 3AC's default. Voyager Digital was then set to be acquired by FTX US for $1.4 billion after FTX won in a U.S. bankruptcy auction. This plan was terminated after FTX itself filed for bankruptcy[115].

BlockFi

November 2022 - On November 28, following its decision to suspend withdrawals on November 11, crypto lender BlockFi filed for bankruptcy following a contagion spread from FTX's bankruptcy filing. BlockFi is owed a total of $1 billion by FTX and its trading firm Alameda Research. FTX and its over 100 affiliated companies' bankruptcy filings included Alameda Research defaulting on a $671 million loan from BlockFi, as well as frozen FTX accounts worth $335 million. BlockFi's decision to file for bankruptcy was directly linked to the implosion of FTX. The entanglement and interdependence of BlockFi and FTX started earlier that year, when FTX provided a line of liquidity of up to $400 million to the troubled crypto lender BlockFi, in return for reserved rights to acquire BlockFi at a capped acquisition price of $240 million. Calculating the damage done, BlockFi issued a statement, estimating roughly 100'000 clients to be affected and claiming its assets and liabilities to be in the range of $1 - $10 billion. Currently, BlockFi holds $256.9 million in cash and stated plans to continue operations after a successful restructuring[116].

Genesis

November 2022 - After a series of events unfolding with the FTX downfall, Genesis remains struggling to raise new cash in order to avoid bankruptcy. Genesis Global Trading is an OTC crypto platform which, alongside its sister company Grayscale, are owned by their parent company Digital Currency Group (DCG). Genesis got dragged into the growing pool of troubled crypto corporations due to multiple toxic loans and bad debt holding $175 million locked up in trading accounts held by FTX. Further, it lent $2.36 billion to blown up hedge fund 3AC and has a total of $2.8 billion in outstanding loans leading to a warning by Genesis of a potential bankruptcy in case no funding is found. A disclosure on Tuesday, November 22, revealed that a total of $575 million is owed to Genesis by its parent company DCG, alongside a rumor of an IOU of $1.1 billion[117]. On January 19, 2023 Genesis filed for Chapter 11 bankruptcy protection.

FTX

November 2022 - The week of November 7 saw FTX-related headlines all over, leading to a culmination of Sam Bankman-Fried (SBF) stepping down as CEO and one of the world's largest crypto exchanges filing for Chapter 11 bankruptcy. The filing revealed that FTX (crypto exchange) and Alameda Research (connected trading firm) have liabilities that range from $10 billion –to $50 billion. Even the U.S. entities collapsed which according to some SBF's thread on Twitter were supposed to be "fine". The avalanche started with a CoinDesk report that leaked the balance sheet of the dangerously intertwined Alameda Research revealing that a significant amount of their balance sheet was held in FTT, FTX's platform utility and access token. Despite having limited utility and liquidity, FTT was extensively leveraged in DeFi, on FTX and as collateral in Alameda's books[118]. FTX reportedly bailed out Alameda that suffered losses connected to 3AC and the Luna collapse in May 2022 and accepted Alameda's FTT collateral in exchange for funds that at least in portion belonged to their customers. New information came to light when The Wall Street Journal published an article titled "FTX Tapped Into Customer Accounts to Fund Risky Bets, Setting Up Its Downfall", revealing that FTX had $16 billion in customer assets and gave $10 billion to Alameda who blew[119] it. Following a tweet from Changpeng Zhao (CZ), CEO of Binance, stating that they will liquidate their FTT holdings received as FTX exit equity, a bankrun on FTX started. Shortly after, FTX halted withdrawals followed up by a post of CZ announcing a non-binding LOI between FTX and Binance, only to then back out of the deal one day later because of "issues […] beyond our ability to control or help."

Contagious effects already started to pop up as Genesis confirmed having $175 million still on FTX, with crypto lender BlockFi, who previously was bailed out by FTX, being highly exposed, or CoinShares having a $30.3 million exposure[120]. U.S. SEC and Justice Department, among other jurisdictions, started investigating FTX. Several crypto projects were affected as well as FTX ventures that funded various projects such as Solana (FTX holding $1 billion in SOL) or recently launched Aptos. It is yet unclear if wrapped tokens like oBTC ($290 million) and soETH ($640 million) are issued by FTX too.

Interview on FTX with Niklas Nygaard, Senior Trader at Bitcoin Suisse

Can you elaborate on your personal experience of the FTX downfall?

Having a strong personal interest in the crypto markets I always stay up to date with Crypto-Twitter (CT). As always, in hindsight there were earlier signs; however the first telling hint came on November 2, 2022, when Coindesk published an article leaking the balance sheet of Alameda Research, SBFs second company which is mostly known for their arbitrage trading in Korea and Japan in 2017 and more recently for having been a major market maker on FTX. At this point FTT, FTX's native token, intraday performance stood at -10%, at a volatility certainly not unknown in crypto markets, hence not overly alarming at that point in time.

It took Caroline Ellison, CEO of Alameda, four days to react to the rumors on Twitter. Without providing more insights, she claimed that the leaked balance sheet was merely a snapshot and that it did not account for another >$10 billion held by its other corporate entities.

A dispute started to unfold on CT between SBF and CZ on November 7, 2022, continuing in the following days, while Caroline Ellison did not comment any further. The dispute mainly concerned two topics, the FTT that Binance was holding, which they were planning to dump, and a possible acquisition of FTX by Binance. At this point my optimism had turned into hopium (*urban definition of false hope).

What were your first thoughts after hearing about the FTX case?

As a collapse of FTX seemed unlikely, my first reaction was admittedly disbelief.
I was sceptic that FTX was indeed insolvent given the prior reputation of the company throughout the crypto industry. FTX had been a major player as one of the world's largest crypto exchanges. They were well renowned and a great proponent for adoption by making countless financial contributions to various projects as well as sponsorships.

After it had become clear that FTX had reached a point of no return my focus switched increasingly towards Binance and its financial health given their position in the industry and their involvement in the situation.

How did Bitcoin Suisse weather these turbulent times?

As is often the case in turbulent times, trading volumes spiked and the workload in the trading team intensified. Having said that, I am proud to work in a company that managed their exposure related to the collapses and mitigated the risks appropriately. This was largely thanks to our business model: as we are not tied to only one crypto exchange but work with a range of major exchanges and trading partners globally, Bitcoin Suisse operations remain stable even in times of increased market volatility. We carefully select our trading partners and evaluate them on an ongoing basis. In my opinion, this approach is one of the reasons why we are considered a place of stability and security since 2013.

What are learnings after this whole situation?

Learnings should be that prudent risk management is extremely important, even more so in an industry that is based on trustless and permissionless technology, where CeFi-players are actively operating. There is certainly a need for increased regulation in many countries, where it still lags behind reality. What has happened is a symptom of a rapidly growing industry whose guardrails have not evolved enough, at least in certain states. It is important to keep in mind though that the fundamental problem was not DeFi technology, but - as far as can be assessed today - criminal business practices and a complete failure of all controls by CeFi companies operating in the crypto space.

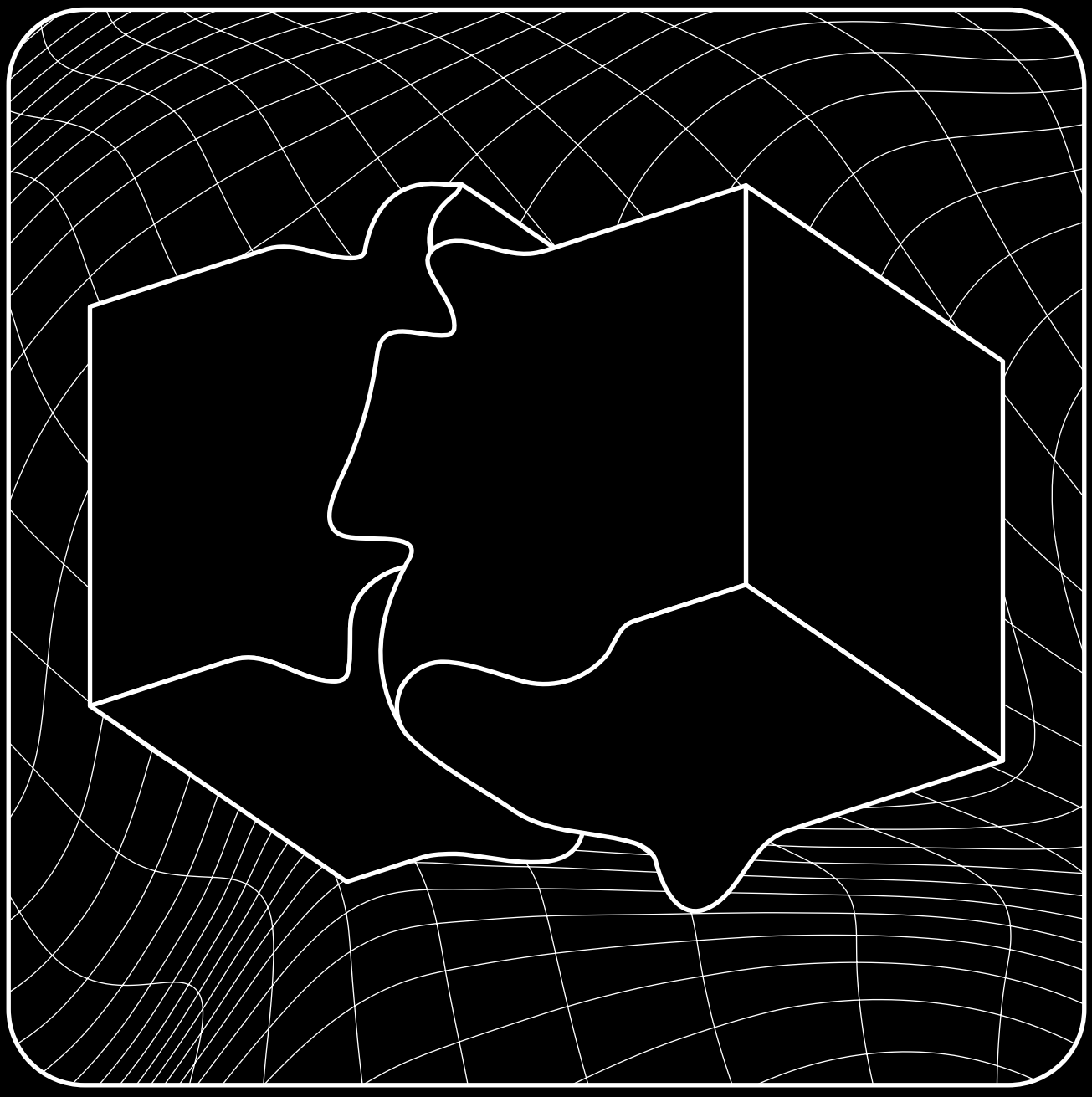
(When) do you think the market will recover from the developments since the FTX collapse?

I hope that the events end of last year – albeit costing the consumers dearly while creating challenging conditions for the crypto industry – will still help push the industry towards more permissionless and trustless solutions in the form of decentralized exchanges, which would be in the very philosophy of Satoshi Nakamoto. At the same time, the events had a lasting impact on public percep-tion of the crypto market and as a result, regulators are coming increasingly forward to fill the gap of appropriate regulatory frameworks. The collapse of 3AC, Celsius, and FTX certainly took their toll on trust from consumers which has to be restored over time. With that being said, I believe that we are in the midst of one of the most defining phases in the history of the crypto industry and I am confident the crypto market will recover; however, the time frame and speed of this recovery remains yet to be seen. We have seen other crypto winters and from that experience we know that with the current shakeout and recovery process always come new opportunities.

Article

The Post-Merge Ethereum World

by Dominic Weibel



■ Ethereum's transition to Proof-of-Stake in September 2022 was arguably the most significant landmark event in blockchain technology since Satoshi bootstrapped Bitcoin's genesis block almost 14 years back. A first of its kind, an open-heart surgery on a distributed ledger securing billions of dollars went through without any hiccups, a monumental achievement for consensus and coordination of like-minded individuals across independent researchers, client teams and infrastructure providers.

■ The Merge brought a reduction in energy consumption in the range of 99.84% to 99.99% almost eliminating its carbon footprint, a significantly reduced net inflation and a lower barrier of entry for users aiming to secure the network. Despite MEV Boost, a first iteration of proposer-builder separation, being utilized to avoid economies of scale and protect decentralization, the transition to Proof-of-Stake and new regulatory scrutiny exposed looming censorship risks across Ethereum's tech stack. Moving forward, solutions will not only rest on the shoulders of the social layer but also on the comprehensive roadmap. Being around 55% complete post-Merge, it will address issues including security, privacy, censorship-resistance and more.

■ A significant part of the roadmap deals with scalability improvements that will unlock the full potential of rollups and streamline Ethereum to a lean protocol. As the Layer 1 narrative loses steam, activity is drifting towards scaling solutions such as Arbitrum, Optimism and Polygon. 2023 will be decisive for promising blockchain architecture paradigms as (multi-)monolithic and modular approaches line up to compete.

The Merge

Some years down the road, 2022 will likely not be remembered as the year where flawed stablecoins and most of the CeFi industry blew up but as the defining moment in blockchain history where Ethereum successfully transitioned from Proof of Work (PoW) to Proof of Stake (PoS). With it, a tremendous effort finally culminated since its first proposal in 2017[121]. As the Merge block finalized in epoch 146'876 in September 2022, Ethereum managed to complete its mainnet transition to PoS in a flawless fashion. The Merge passed without any hiccups after a marathon of merged testnets and shadow forks, see Illustration 1, marking the conclusion of a multiyear effort that mitigated technical and operational risk of upgrading a ~$150b network in open-source development.

Switching the core consensus mechanism of Ethereum without downtime was a spectacular technical feat that overall involved more than two years of testing and more than 100 bi-weekly calls[122]. Described as hot swapping airplane engines in-flight of a network that also secures >$163b in ERC20s and $22b in NFTs, the Merge upgrade was activated in two phases. "Bellatrix" activated on the consensus layer responsible for transaction validation and block production. It prepared the Beacon Chain to include user transactions from the execution engine and updated the fork choice rule to LMD-GHOST[123], that identifies the fork with the greatest accumulated weight of historical attestations. Consecutively, "Paris" triggered the actual merge on the execution layer that was previously tied to PoW and is responsible for transaction bundling, execution, and state management.

> "There's a much easier way to do the Merge: We shut down for three days, do the thing and flip the switch back on and it restarts. […] So getting this switch to happen, basically seamlessly in a way that was like incentive compatible with miners, was pretty wild."
>
> *– Tim Beiko, protocol support lead since January 2021 at the Ethereum Foundation.*

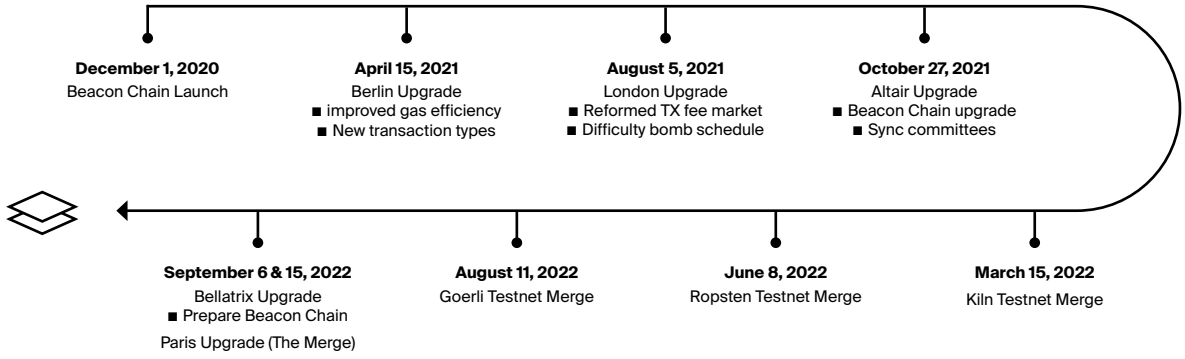


Illustration 1: Timeline of upgrades leading to the Merge. Data: Ethereum.org. Graphic: Bitcoin Suisse Research

Proof-of-Stake

Transitioning to PoS completely changed the way of verifying transactions, securing the network, and issuing rewards as it relies on economic voting and slashing to keep validators in check. Introduced by Scott Nadal and Sunny King[124] in 2012, it was first adopted by the Peercoin blockchain in 2013 and now dominates the crypto industry since most of the protocols in recent years launched with PoS powering their blockchain.

By formally adopting the Beacon chain as the new consensus layer, validators instead of miners are now assigned to participate in consensus to secure Ethereum as they propose and attest blocks. Validators are specialized nodes that coordinate transaction processing and block creation by locking ETH. They are chosen at random by an algorithm rather than competing in mathematical puzzles with hash power. A validator either serves as single block proposer or as one of many block attesters within a committee[125].

During the Merge, a validator participation rate way above the mandatory 66% led to a quick justification of

the first epoch. The network subsequently reached finality by hitting two justified consecutive epochs completing the Merge (an epoch consists of 32 slots that last 12 seconds each and offer the opportunity to propose a block to the canonical chain). Finality means that no changes afterwards are possible, except for a critical consensus failure. The PoS transition not only decreased block times from ~13.3 seconds (determined by mining difficulty) to 12 seconds but also introduced deterministic finality after 12.8 minutes (2 epochs) instead of probabilistic finality after around 1.5 minutes in PoW.

While miners previously proved to have capital at risk by expending energy, validators risk capital by pledging native collateral to actively participate in securing the underlying blockchain. They get rewarded for doing so, or slashed (penalized) for inactivity or malicious behavior. Notably, PoS is only part of the consensus mechanism and functions as a Sybil attack protection, an attack vector which works by creating multiple identities. In PoS, votes are weighted by the amount of stake and thus, spinning up nodes is pointless without backing them with stake. As an attacker needs an overwhelming stake, it significantly increases the cost of attack and mitigates the risk of a Sybil attack. For instance, the cost and difficulty of an attack increased five-fold, and with the enhanced confidence induced by the Merge, it will grow higher as new validators join to protect the network.

As Vitalik Buterin states[126], PoS offers more crypto-economic security (disincentives for the same cost), enables easier recovery of attacks and offers lower barriers to entry because of reduced hardware requirements. PoS is also more resilient to force majeure, as a recent drop in BTC hashrate due to the ongoing blizzard in the U.S. showed[127]. Meanwhile, Ethereum was running at nearly 100% without any validators dropping off. On the flip side, PoS might lead to higher wealth concentration, being a closed system that requires weak subjectivity[128] (state root checkpoints implemented to undermine attack vectors such as long-range attacks). Moreover, PoS is less battle tested and brings increased implementation complexity.

Despite aiming for PoS since its genesis, Ethereum was initially forced to leverage PoW that was known for its robustness and security guarantees, while PoS took years of dedicated research and development. In hindsight, this hybrid approach was crucial to bootstrap the distribution of its native asset ETH and therefore enabled a higher degree of decentralization heading into PoS. As most networks that launched in the recent years utilized it as consensus mechanism, PoS can now also be considered to be more reliable.

The Merge is one of the most significant catalysts in Ethereum history as it impacts the network on several fronts. As we outline, it came with various first and second order effects.

Energy

First order effects not only included a change in Ethereum's security model and block confirmation times, but also massive changes in monetary policy and energy efficiency. Despite PoS having the same goal of achieving distributed consensus as PoW does, its lack of computational intensity leads to an impressive reduction of energy required. Neither expensive mining hardware nor operational cost of miners must be compensated any longer by protocol emissions. Therefore, PoS brings increased energy-efficiency and reduces its environmental footprint, by means of electricity consumption and carbon emissions, by 99.98% and 99.992%, respectively[129]. The Crypto Carbon Ratings Institute generated bottom-up estimates of the electricity consumption of various node hardware and client setups, yielding an estimate annual energy consumption of 0.0026 TWh and a reduction of carbon emissions from 11'000'000t CO2e pre-Merge to 870t CO2e post-Merge. For instance, PayPal consumes 100x more energy, see Illustration 2, where other ballpark estimates of industries are found for context (one should take these estimates with a grain of salt since they are subject to a broad range of assumptions). Other data suggests that the power consumption on the network fell from May's high of 93.98 TWh, where we also saw a peak in hashpower, to around 0.01 TWh. Even with the most conservative estimates and comparing the new energy expenditure to the lowest energy consumption in 2019 at 4.75 TWh per year, the PoS transition still yields 99.8% energy reduction.

As Illustration 2 further indicates, Ethereum generated $19b in mining rewards, taking into account block subsidy and transaction fees, in 2021. Correlated to the drop in energy consumption, these block subsidies dropped to zero post-Merge. As a result, an estimated $5b of mining GPUs and ASICs[130] chased new purpose or were sold on secondary markets. One shelter was offered by the contentious PoW hard fork. However, the mean hash rate compared to pre-Merge Ethereum in September (~860 TH/s[131]) dropped to ~70 TH/s immediately after the fork. 100 days later, it is down to only 16 TH/s[132] indicating a massive miner escape that matched the price decline of ETH PoW at around 80%. As Ethereum made up around 97% of the total daily miner revenue for GPUs, these miners struggled to find mineable coins

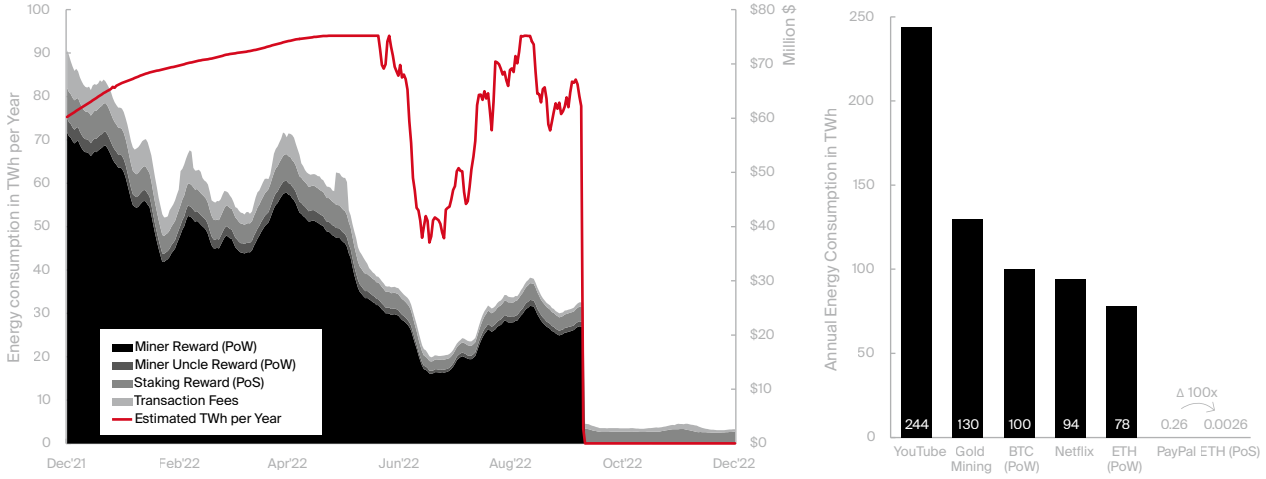


Illustration 2: Change in energy consumption and block subsidy post-Merge (Left) and annual Energy consumption of various entities. Data: The Block, Digiconomist, Ethereum.org. Chart: Bitcoin Suisse Research

within the crypto ecosystem and were partwise forced to pivot towards data-center oriented businesses.

As crypto starts to demonstrate real-world utility, we expect energy to be a key topic in the years ahead. Multiple headlines across the globe indicated in 2022 that PoW chains have come under more regulatory scrutiny due to their environmental impact. With ESG concerns rising, not only enterprises and governments will be under continued pressure to curb energy consumption, but PoW chains that fail to demonstrate utility will arguably see more criticism too. PoS blockchains on the other hand are more resilient to such criticism and therefore suited for ESG compliant institutional adoption.

Shifting consensus gears achieved improved sustainability for Ethereum. One could consider it as one of history's largest decarbonization events. According to Ethereum researcher Justin Drake, the PoS transition reduced global electricity consumption by 0.2%[133]. The significance is further amplified by both an acceleration in climate change[134] and a looming energy crisis induced by the Russo-Ukrainian War. Yet, one might also argue that Bitcoin mining in the context of geopolitical tensions alongside a deglobalization trend could serve as a catalyst towards clean energy and simultaneously balance the electrical grid.

We invite you to read the macro view with an eye on Bitcoin article in this Outlook edition

To avoid greenwashing, it is important to note that Ethereum itself added the previously mentioned 0.2% in the first place and switching consensus does not address the substantial carbon debt accrued since Ethereum's genesis block. To repay Ethereum's carbon debt however, there is a nascent movement known as ReFi (Regenerative Finance). ReFi builds tools to make Ethereum carbon negative via incentives for land generation, carbon capture through regenerative agriculture and other strategies. DeSci[135] (Decentralized Science) might become another major innovation and momentum catalyst in 2023, fostering open, decentralized markets for research and academia via e.g. biotech DAOs or IP-NFTs enabled by blockchain technology. As such, significant improvements in publishing, reproducibility, replicability, funding, IP, data storage and access are enabled.

Issuance & Burning

The next major first order effect is the network's updated gross inflation. The Merge represented a major revamp of Ethereum's monetary policy. Miner subsidies were eliminated in one swoop and drastically reduced the daily ETH issuance, since validator rewards are only a fraction compared to the compensation required for energy expenditures of miners. It brought Ethereum's daily network issuance, that started back in 2015, at 26k ETH under PoW, down to 1.7k ETH post-Merge. On an annual basis, the issuance dropped down to 0.62m ETH post-Merge from 4.9m ETH pre-Merge, thus by ~87%. Illustration 3 shows Ethereum's supply distribution to date. Notably, the PoS issuance only accounts for less than 1% of Ethereum's circulating supply, despite the Beacon Chain launching two years ago in December 2020. To catch up with historical PoW rewards, PoS would have to run for approximately 110 years.

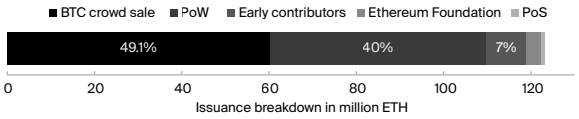


Illustration 3: Issuance breakdown of Ethereum's circulating supply. Data: Ultrasound, Chart: Bitcoin Suisse Research

Since the Merge went live around four months ago, PoS issued 4.8k ETH instead of 1.2m ETH running on PoW. At current valuations, that is $2.88m compared to $1.27b, see Illustration 4, or equal to eliminating $120m of potential monthly selling pressure. While Ethereum lowered its annual net inflation from 3.5% to 0.004%, Bitcoin currently inflates only 1.72% annually, but issued $1.36b in dollar terms, more than Ethereum PoW since the Merge. With the current block rewards, Bitcoin's inflation is 430 times higher than PoS powered Ethereum. Looking at gold, around 3'000t of gold are estimated to be mined per year. That supply expansion brings around $192b of new annual supply to the market at an annual inflation of around 1.6%.

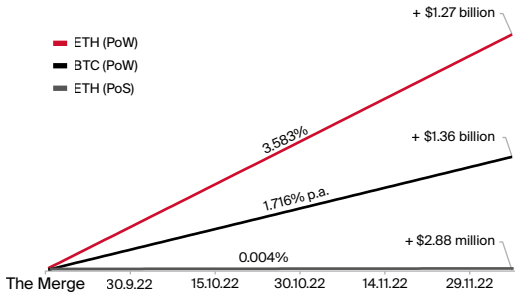


Illustration 4: Changes in monetary policy and its supply impact. Data: Ultrasound, Chart: Bitcoin Suisse Research

Not only did PoS substantially reduce Ethereum's gross inflation, but it did also change Ethereum's supply dynamics. By design, it lowered the sell pressure on its native asset ETH as validators are not forced to cover capital expenditure and operational expenditure. For instance, 50'000 BTC was sold in 2022 by Bitcoin miners. Projecting that to the current market cycle, ETH prices might have dropped much deeper in a low liquidity environment with an additional 1.2m ETH in circulation.

Ethereum's issuance is designed to attract more validators if the staking ratio is low. The network issuance, therefore, varies based on the amount staked and follows a root function (maximum annual issuance equals 940.87 times square root of N, where N is the number of validators)[136]. It closely interacts with Ethereum's base fee burn feature that depends on blockspace demand and removes ETH from circulating supply. Since validators took over, two deflationary periods, one closely after the Merge and one with activity picking up related to the downfall of FTX, were present to date. Ethereum's net inflation (gross inflation – burned supply) becomes deflationary if burnt transactions implemented with EIP-1559 exceed the network's staking issuance rate. Since EIP-1559 went live last summer, Ethereum burned about 85% of all transaction fees. With EIP-1559, Ethereum turned a major flaw, being high gas fees, into a mechanism that benefits holders of the underlying base asset ETH.

Overall, 2.8m in ETH, at an average burn rate of 3.8 ETH/min, or $8.77b has been burned[137] within the 510 days since EIP-1559 was activated. That's on average 3.22x more than Ethereum's post-Merge issuance of around 1.18 ETH/min. Substantial demand that drives burning is induced by NFTs and especially DeFi, see Illustration 5.

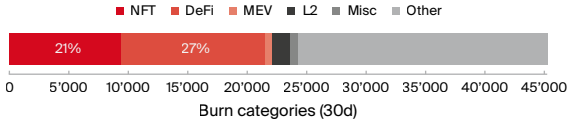


Illustration 5: Average burn by category over the last 30 Days. Data: Ultrasound. Chart: Bitcoin Suisse Research

One crucial part for burn activity is MEV (Maximal Extractable Value), that the block proposing validator can extract in PoS. Instead of miner subsidies, validators are now eligible to gain the execution layer rewards aside from the protocol issued consensus layer rewards. Execution layer rewards are directly proportional to the transaction activity and can be referred to as a combination of rewards consisting of tips and rewards generated through MEV (primarily available to validators who run MEV Boost). Technically, validators receive execution layer rewards as additional tips for prioritizing, including, excluding, or reordering transactions.

Consensus layer rewards on the other hand are inversely proportional to the amount of ETH staked and refer to the rewards from the issuance of new ETH. Validators receive these rewards, also considered inflation rewards, for participating in the security of the Ethereum blockchain either as block proposers, attesters, or members in sync committees[138]. The largest part of the consensus layer rewards for validators, making up for 84.4%[139], are attester rewards that validating nodes receive for correct and timely votes on the source checkpoint, target checkpoint and chain head block. Additionally, validators are eligible for rewards participating in sync committees in varying proportions.

An average validator is currently able to yield 7.8% annually, composed of 55% issuance, 33% tips and 12% sourced from MEV, see Illustration 6 where the average annual rewards are broken down for a validator staking 32 ETH.

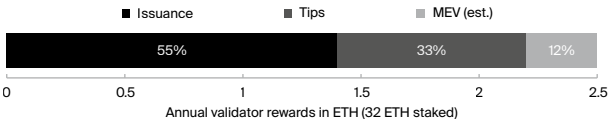


Illustration 6: Breakdown of annual validator rewards that yield 7.7% APR at time of writing. Data: Ultrasound. Chart: Bitcoin Suisse Research

For the time being, we expect the new supply dynamics to shape a range between a slightly deflationary and slightly inflationary environment. As blockspace demand is comparably low in prolonged downtrends, we observe that Ethereum's burning feature is nonetheless balancing out the inflation rewards for validators. Hence, it is bringing the net inflation close to 0% despite being in a sustained period of low average transaction cost, with $5/transaction[140]. In 2021, the average transaction cost was mostly above $20. Long-term, Layer 2 (L2) momentum along with a change in the Layer 1 (L1) narrative, and an uptick in activity might bring the issuance into a deflationary environment. Especially when headed into an uptrend again, that is known for stimulating on-chain activity. Like a Bitcoin halving on steroids, the Merge reduces the overall network inflation, and with that, sell pressure linked to network issuance decreases on the supply side. As with Bitcoin halvings, we expect to see the new supply dynamics heavily in play as soon as demand hits the industry again. Ethereum's inflation adjusted staking APR is already best in class and will likely have material impact across multiple industries. Introducing yields to the largest smart contract platform might also induce institutional interest. Yet, transforming ETH into a yield-bearing financial instrument comes with regulatory risk. As such, SEC's Chairman Gary Gensler did not hesitate to signal that Ethereum's new PoS mechanism might draw attention of the SEC, as staking could trigger securities laws[141].

→ *We invite you to read the regulatory landscape article in this Outlook edition*

Looming censorship

On August 8, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned the privacy protecting crypto mixer Tornado Cash and 44 smart contract addresses associated with it[142] for aiding thieves in laundering stolen money from exploits. These sanctions fueled controversies around Ethereum's censorship resistance and exposed substantial attack surface. It also sparked the question why a single jurisdictional entity should have cross-jurisdictional sovereignty on a neutral, permissionless and decentralized network.

In crypto, censorship is a spectrum that can range from weak to strong censorship and often derives from centralized points in the tech stack. Weak censorship usually occurs above the validator level and refers to a mild form of transaction censorship. It happens via frontends, via centralized infrastructure providers such as Infura or Alchemy that are capable of restricting transactions flowing through their nodes, or within the block production pipeline that results in an on-chain inclusion delay of transactions subject to censorship. In this block production pipeline, we face builder centralization and centralization of trusted MEV relays that represent another layer of possible censorship.

It can also happen on the validator level if a fraction of validators actively participates in block censorship. Yet, if the fraction is insignificant, other validators will eventually pick up the transaction. Same applies to block producers as non-censoring block producers ultimately pick up non-compliant transactions. As of writing, there is a 99.99% chance to have a OFAC non-compliant transaction included within 5 minutes instead of 12 seconds. Strong censorship, however, happens on the validator level rooted in block proposer attestations[143] and means that censored transactions never get included in any block. Strong censorship is possible if a certain entity controls the machine layer consensus by hitting an aggregate of 51% consensus threshold. If this ever happens, the only way out is via social slashing and a minority fork, viable means as validator level censorship-resistance is mandatory in order to protect and maintain Ethereum's integrity as well as its core value proposition offering equal access to anybody.

"My personal opinion is if we allow censorship of user transactions on the network, then we basically failed, and this is the hill I'm willing to die on. If we start allowing users to be censored on Ethereum then this whole thing doesn't make sense. […] I think censorship resistance is the highest goal of Ethereum and of the blockchain

space in general so if we compromise on that there's not much else to do in my opinion."

– Marius van der Wijden, developer from the Geth client team, on protocol level censorship resistance

As Ethereum successfully transitioned to PoS, all eyes are now on potentially centralizing forces within the upgraded network and the threat of censorship looming alongside. Ethereum faces points of centralization almost across the entire tech stack. However, there is a plethora of strategies to mitigate potential risks moving forward that rely on not only the protocol layer but also the social layer.

Remote Procedure Calls (RPC) and Frontends

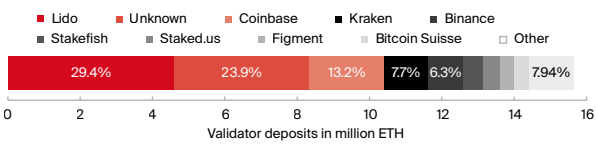
Many dApps have centralized frontends that allow censoring access as seen multiple times in 2022. More importantly, these dApps usually leverage RPC nodes in the background to communicate user intends. Infura and MetaMask for example blocked wallets trying to interact with Tornado Cash. Recently, ConsenSys also announced an update to its privacy policy affecting wallet provider MetaMask and its default RPC Infura[144].

To fight weak censorship above the validator level, there is a clear roadmap to decentralize infrastructure via in-browser light clients instead of going through RPC endpoints. In PoS, light clients that figure out the tip of the chain via sync committees are way easier to build and it's reasonable to expect that even MetaMask will move to light clients post-Merge, therefore enabling users to route around and avoid endpoint censorship. A viable short-term workaround is switching the wallet provider (e.g. XDEFI wallet, Rainbow, BlockWallet or Frame instead of MM), the RPC (e.g. SecureRPC by Manifold, Pocket Network, Alchemy) or a combination of both. Some RPCs also offer additional features such as private transactions, censorship resistance and to some degree front-running protection. However, the best solution by far is running a node to guarantee direct blockchain access instead of relying on a centralized API and node infrastructure providers such as Infura or Alchemy. Anyone is free to sync their own, self-verified copy of Ethereum by running a node. Despite no staking capital required, nodes serve a critical role in securing the network by holding all block proposers accountable and offer additional benefits such as improved security, privacy and censorship resistance. It also counters risk associated with node hosting, which represents another point of centralization and attack vector, not only regarding operator diversity, but also jurisdictional diversity. Illustration 7 for instance shows the global distribution of Beacon chain nodes. These entities reside in jurisdictions that underly various regulatory risk that

Dependencies on centralized frontends, such as Uniswap's, can be avoided by having multi-jurisdictional decentralized frontends, IPFS/ENS frontends, running local UIs or by engaging directly with the smart contract and therefore going around all checks and friction. Aside from the frontends and RPCs, oracles, stablecoins, source code hosting services or upgradeable smart contracts offer more attack surface.

Validator level

One of the Merge's second order effects was boosting user confidence towards staking. As liquid staking derivatives recovered from significant depegs, while staking deposits accelerated, concerns about validator centralization grew quickly. Validator deposits printed new ATHs with 487'656 validators now staking 15'659'191 ETH[145] within the deposit contract, thus removing 13% of the overall circulating supply. 44.8% of that stake, however, is controlled by only three entities, Lido, Coinbase and Kraken (note that Lido is a DAO and consists of 30 independent operators[146]), see Illustration 8. These entities provide staking services and are either centralized exchanges or staking pool services with a varying degree of decentralization. With liquid staking derivatives, users can take advantage of yield prospects in DeFi without compromising network security. While liquid staking offers PoS networks the chance to increase their meager security, it has the potential to become a centralizing factor over time. Validator centralization does also have second order effects as it contributes to client homogeneity. A lack of client diversity[147] poses a risk of network outages if for example there is a client error, or a client is under attack. Slashing penalties in PoS help to encourage operators to adopt a diverse stack of clients to ensure uptime and network liveness.



llustration 8: Distribution of vaildator deposits in the Beacon Chain smart contract. Data: Nansen. Chart: Bitcoin Suisse Research

As the overall integrity and security of Ethereum's PoS can only be guaranteed with no one entity surpassing crucial consensus thresholds, an excessively concentrated

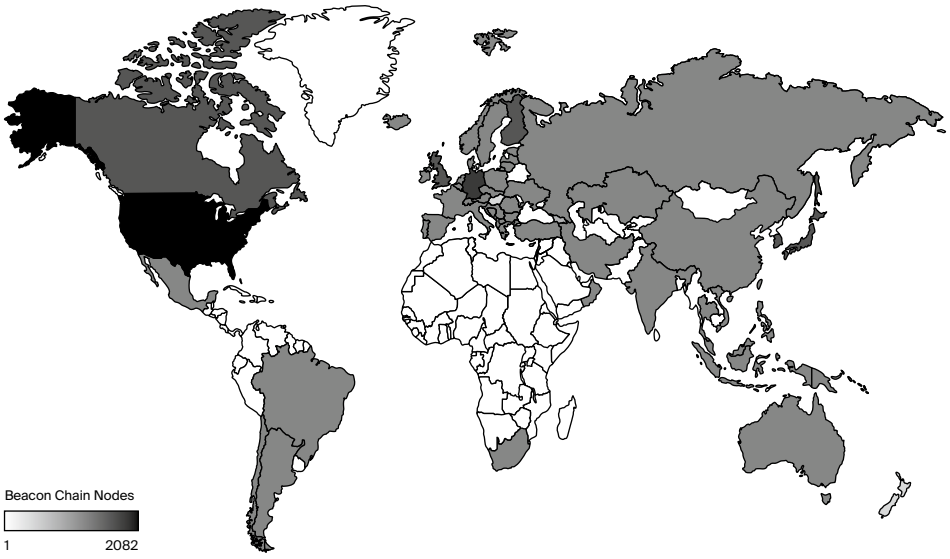


Illustration 7: Global distribution of Beacon Chain nodes.
Data: Miga Labs. Graphic: Bitcoin Suisse Research

stake can call into question the decentralization and neutrality of the network. One entity holding a third of the stake can already cause concerns, as it breaks Byzantine fault-tolerance, a crucial characteristic of the consensus protocol that enables resilience against dishonest players.

Staking via a centralized entity is convenient, requires almost zero know-how and often allows staking with less than the minimum 32 ETH required for solo staking. Even if PoS was designed to lower the entry level complexity for validators, independent staking still comes with significant friction regarding risk tolerance (slashing), technical know-how (setup and operation) and investment size (32 ETH to spin up an individual validator). Thus, small holders and anybody with less technical expertise are almost forced to use some form of staking service with a ranging degree of trade-offs. Aside from staking with centralized exchanges, liquid staking solutions such as Lido, Rocketpool or Stakewise are popular. Rocketpool, is noteworthy as it offers additional permissionless node operation, enabling greater decentralization and less capital requirement (16 ETH +16 ETH delegated from retail stakers) as anyone can operate a node, known as Minipools. Moreover, Lido takes a 10% cut of the rewards (5% treasury, 5% node operators) while Rocketpool takes a 15% cut from retail stakers of which 100% goes to node operators. Stakewise is another interesting project offering modular staking and distributed validator technology (DVT) support. Notably, Stakewise is the only one aiming to pay out 80%-100% of fees earned to SWISE token holders. Solo staking and fully decentralized services like Rocketpool's have the biggest impact on decentralization and resilience of the network. Solo staking also allows to actually propose self-build blocks. An average solo staker proposes 5.36 blocks per year earning 1.27 ETH at 0.237 ETH per proposed block to date. Running a validator node moreover guarantees direct access to the network without dependencies on RPCs that might track one's data.

Improving validator centralization heavily relies on the social layer. Any user staking ETH can actively choose how and where he aims to stake and hereby contribute to improving jurisdictional and operator diversity[148]. If there is ever a threat of strong censorship on the validator level, there is a multitude of solutions in the pipeline that aim to prevent said threat: Enshrined proposer-builder separation (PBS) that removes the requirement for validators to trust relays, MEV smoothing that removes variance of MEV and MEV burning[149], single slot finality[150] to speed up deposits and withdrawals, statelessness[151], DA sampling and zero-knowledge (zk) EVMs that will significantly reduce hardware cost, a reduction in necessary stake size, privacy preserving deposits and staking, anti-slashing hardware and finally, encrypted mempools that will help both against censoring builders and proposers (validators).

We expect that not only liquid staking solutions will gain more momentum in 2023 but also staking innovations such as Obol[152] or SSV[153]. Obol provides DVT (Dis-

tributed Validator Technology), also known as secretly shared validator technology, a middleware solution alike MEV-Boost, that can enhance the operation of an Ethereum validator by allowing multiple non-trusting operators to run distributed validators. Applying DVT will lead to improved resilience, greater stake decentralization and reduced slashing risk. In combination with the reduced sell pressure from a lower gross inflation in PoS, increased staking activity triggered by the Shanghai upgrade will likely remove more liquid supply from the market.

Block production pipeline

Economies of scale was considered to be a huge threat heading into PoS. Economies of scale of validator entities could have potentially triggered MEV (changing the transaction order to build blocks with the highest possible economic value) flywheel effects by having substantial amounts of staked ETH. To avoid centralizing forces within the validator set, Flashbots preemptively introduced MEV-Boost, a middleware that validators can adopt to capture MEV-rewards. It enabled a fairly even distribution of MEV across the entire validator set. So far, MEV-Boost succeeded in preserving validator level decentralization in that it allows any validator to plug into sophisticated MEV extraction techniques. Therefore, it democratized access to MEV as validators are not forced to redelegate their stake, yet still mine profitable. MEV-Boost also lowered gas cost as block auctions were put off-chain.

However, it introduced other centralizing forces within the block production pipeline like relay and builder centralization. The block production pipeline consists of searchers and their own private order flow, that leverage certain strategies. These include front-, back-running, arbitrage, sandwich attacks and liquidations to find MEV-opportunities. They then bundle up these transactions and forward it to builders. Builders aggregate transactions to craft the most economically sound blocks. Finally, proposers (validators) receive the blocks (execution payload) via relays. Extracting MEV is highly profitable. Since January 2020 a total of $686m was extracted, while $1.49m was wasted on failed MEV-transaction fees[154].

As MEV-Boost provides a substantial financial advantage to validators who use the software to sell blockspace to block builders, its adoption propelled to 90.79% of network adoption[155]. While builder centralization seems to be a non-issue as of writing (Flashbots builder's market share fell from ~80% in September to ~25% in December), relay centralization is a real threat. Illustration 9 depicts the percentage of OFAC compliant blocks funneled through MEV-Boost. Censoring relays being most adopted, with Flashbot's relay dominating the landscape at almost 70%.

OFAC compliant in that context means that relays won't include transactions that interact with Tornado Cash or other sanctioned wallet addresses, as outlined by the OFAC. There are currently 11 relays competing in MEV-Boost, with four of them censoring. Unfortunately, these four currently make up around 80% of all blocks added to the chain. Across 30 days, the ratio of OFAC compliant block has been at almost 70%. The fact that most blocks routed through MEV Boost are OFAC compliant raises concerns. It creates the impression to financial authorities, that they can enforce compliance requirements by applying pressure to large custodians. The prevalent dominance of censoring relays is a patronizing obstacle, that at its core represents a dangerous and regressive development.

In 2023, centralizing forces within MEV are likely to be one of the key topics. Recent shifts in the relay landscape give reason for hope. Not only did more non-censoring relays recently join the battlefield, but the dominance of OFAC compliant blocks seems to have peaked in late November, indicating a trend shift towards more diversity and competition. More entities will likely be brave enough to choose a relay diversity approach to boost non-dominant relays. With the threats being exposed and more awareness due to CeFi blowups, we expect this trend to be sustained in 2023. Moreover, an interim solution in 2023 is arguably provided by Flashbots, that is building an open-sourced upgrade to MEV-Boost known as the Single Unifying Auction for Value Expression (SUAVE). SUAVE is a MEV-aware and privacy-first encrypted mempool which provides transaction opacity and eliminates any central points of control, including Flashbots itself. Notably, Flashbots also open sourced its relay in August, and its builder in November, thereby reducing the risk of builder centralization. Medium-term solutions include encrypted mempools, enshrined PBS and inclusion lists.

Censorship-resistance is a mandatory feature for future proof blockchains. If Ethereum wants to be a self-sovereign public good with secure blockspace and equal access for everybody, it must have immunity from nation states. It is important to understand that censorship-resistance will, to a significant extend, be up to the conscious end users and the community actively choosing and supporting permissionless applications and services built atop Ethereum.

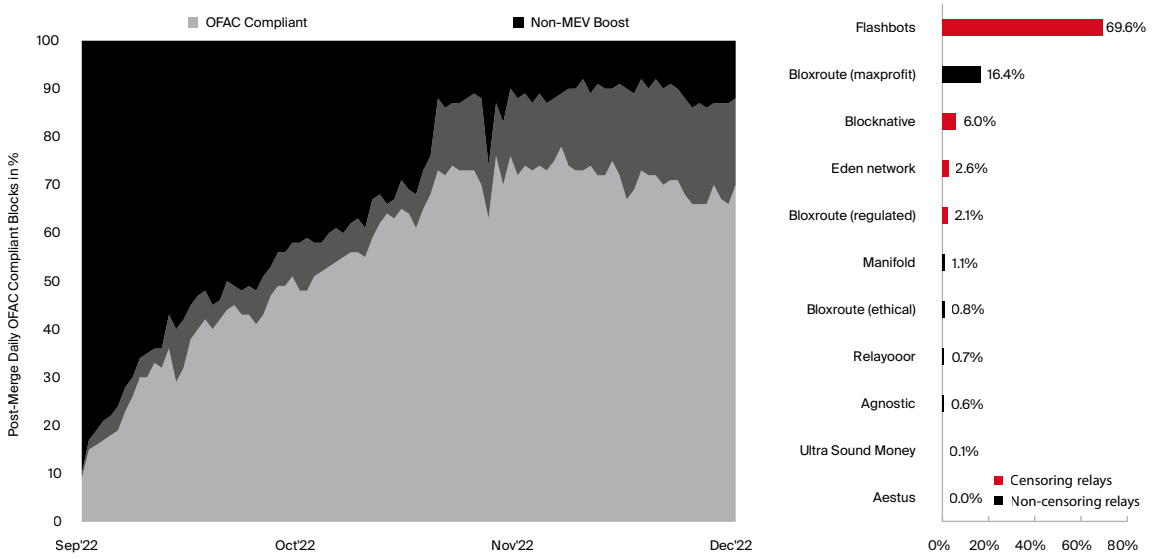


Illustration 9: Post-Merge OFAC compliant blocks and dominating relays. Data: MEV Watch, Rated. Chart: Bitcoin Suisse Research

Roadmap

Despite the Merge being one of the most significant structural shifts of any large-scale crypto asset to date, it was only one part of Ethereum's comprehensive roadmap that aims to improve the network around scalability, decentralization, security, hard disk requirements and elimination of tech debt. Just two months after the Merge, Vitalik Buterin revealed a new roadmap organized in six categories, see Illustration 10: The Merge, The Surge, The Scourge, The Verge, The Purge, and The Splurge. With the recent roadmap update[156], not only more precise milestones were added in each category, but also a new item, The Scourge. It aims to ensure reliable and credibly neutral transaction inclusion as it deals with MEV-challenges and forces of centralization.

Scheduled for March 2023, the next highly anticipated Ethereum upgrade after the Merge is the Shanghai and parallel Capella upgrade. As interest of financial authorities is rising with the mess caused by FTX, it's important to have withdrawals enabled as soon as possible to avoid regulatory tail risk of potential censorship-enforcing jurisdictional actions. Capella will upgrade the Beacon chain (consensus layer) and Shanghai targets the execution layer, formerly tied to PoW. Enabling withdrawals is crucial. Since the launch of the Beacon chain, all staked ETH plus the consensus layer rewards remain locked, while execution layer rewards like Tips and MEV are distributed concurrently. Aside from EIP-4895 (withdrawals), EIPs that are prioritized in Shanghai are EIP-3860 (initcode), EIP-3651 (coinbase address) and EIP-3855 (new instruction called "PUSH0"). Instead of Proto-Danksharding, developers recently agreed to include EIPs related to EOF implementation. EOF implementation is the first major code change since its inception targeting the EVM, Ethereum's execution environment.

Beyond the activation of withdrawals, the next major upgrade for Ethereum will be centered around activating the Surge related Proto-Danksharding (EIP-4844). Initially planned for implementation with Shanghai, it was recently shifted to the next upgrade in favor of avoiding any delay for withdrawals and potential tension induced by the complexity of the upgrade. EIP-4844 will introduce a new transaction type that allows "blob" carrying (instead of calldata) for L2 batch settlement in a specific blockspace allocation that is expected to massively boost L2 scalability. Consider Danksharding to be an afterburner to rollups making them more efficient and cheaper. For Proto-Danksharding, there is no fundamental change to how the underlying blockchain technically works. It's also a precursor for full Danksharding, a design that uses a merged market fee where shards share the same block proposer for different blocks. According to Dankrad Feist, responsible for the technical lift, Danksharding brings Ethereum from being capable of serving one million people to one billion people. Notably, the introduction of PoS is an enabler for sharding. While it's not preventable that PoW miners collude their hashpower on a single shard to take over control, PoS randomly

Stage	Description	Next Goals	Past Goals
Merge	PoW → PoS	Withdrawals Distributed Validators Single Slot Finality	The Merge
Surge	Improvements to scalability (L2) and privacy	EIP-4844 implementation Basic and full rollup scaling via data availability sampling	EIP-4844 specification
Scourge	Improvements for decentralization and censorship resistance	MEV burn Distributed builders Enshrined frontrun. protec.	Off-chain iteration of PBS
Verge	Simplifying verifications while ensuring transaction privacy and encryption	Verkle tree spec. and impl. Statelessness Fully snarked Ethereum	EVM DoS issues resolved Basic light client support via sync committees
Purge	Removing old data and network history	Implementation of EIP-4444 (history expiry) State expiry specification	Beacon chain fast sync Eliminate gas refunds EIP-4444 specification
Splurge	Fix everything else	EVM improvements Account abstraction (ERC-4337) Verifiable delay functions	EIP-1559 ERC-4337 specification

Illustration 10: The road ahead for Ethereum. Data: Vitalik Buterin. Illustration: Bitcoin Suisse Research

assigns validators to a shard preventing from choosing the shard they want to participate in. The initial execution sharding approach is currently skipped for Ethereum's rollup-centric roadmap[157], which prioritizes modularity and Data Availability for rollups. Other EIPs of importance are EIP-4488, complementing Proto-Danksharding by reducing calldata cost, EIP-4337, introducing Account Abstraction[158] enabling users to employ smart contract wallets instead of an externally owned account (EOA), and EIP-1135 which should reduce gas costs for the Layer 1 and is heavily lobbied by the Uniswap team who is building their V4 product with that upgrade in mind.

While the Merge kept us on tenterhooks for years, we expect subsequent upgrades from Ethereum's well-defined roadmap to take shape at a considerably higher pace in 2023. The Shanghai hard fork enabling withdrawals already sets the tone and is a legitimate proof that the core developers have the user's best interest in mind. Active withdrawals might induce a sustained period of increased yet limited liquid supply entering the market. Validators will need to enter an exit queue with limited batchwise unstaking per epoch (50k ETH are allowed to exit the active validator set per day). The unlocking of staked funds will arguably go hand in hand with a substantial confidence boost and hence attract new (solo) stake that was hesitant previously. This caution is very much indicated by a comparably low staking ratio in Ethereum. We expect that deposits outpace withdrawals even in the short- to medium-term. A higher staking ratio would result in improved network security along with a reduction in staking pool and liquid staking reliance. Withdrawals will moreover allow activist staking again, where stakers are free to actively reshuffle their funds to achieve more distributed validator pools. This will also avoid validators being trapped in regulatory crossfire. In 2023, Proto-Danksharding will unlock a plethora of new financial and non-financial use cases including social media, gaming, and metaverses that rely on more scalability. It will also reinforce Ethereum's approach to modularity by outsourcing execution to rollups. Yet, "blobs" will arguably not solely solve rollup scalability as it brings a massive demand of on-chain data, state bloat and technical complexity.

Ready, Layer 2

To date, the most sophisticated and promising L2 scaling technology that supports general purpose EVM-code are rollups. A rollup off-chain bundles transactions which reduces transaction fees and network congestion. This transaction bundle is senttowards an Ethereum smart contract, inheriting Ethereum's security guarantees, settling on the L1 and enabling anyone to reconstruct the correct

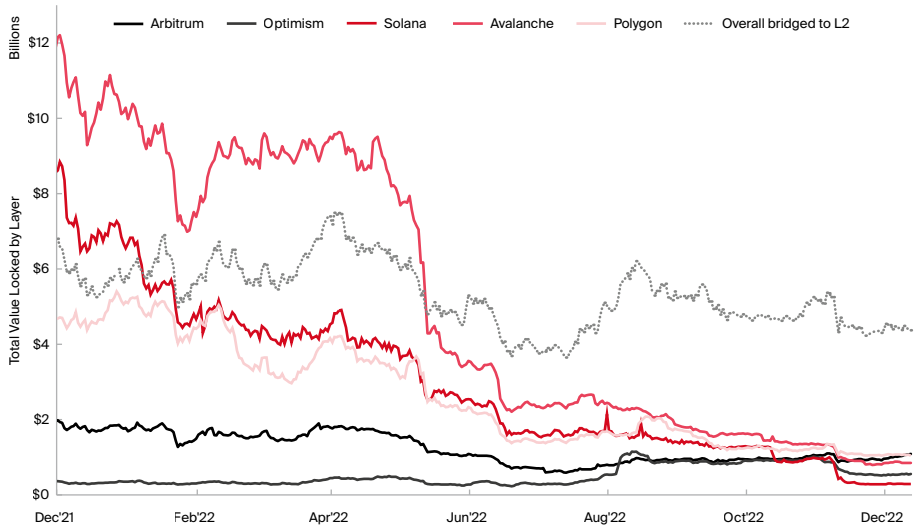


Illustration 11: YoY TVL on Rollups (grey) and selected alternative L1s (red). Data: Defillama, L2Beat. Chart: Bitcoin Suisse Research

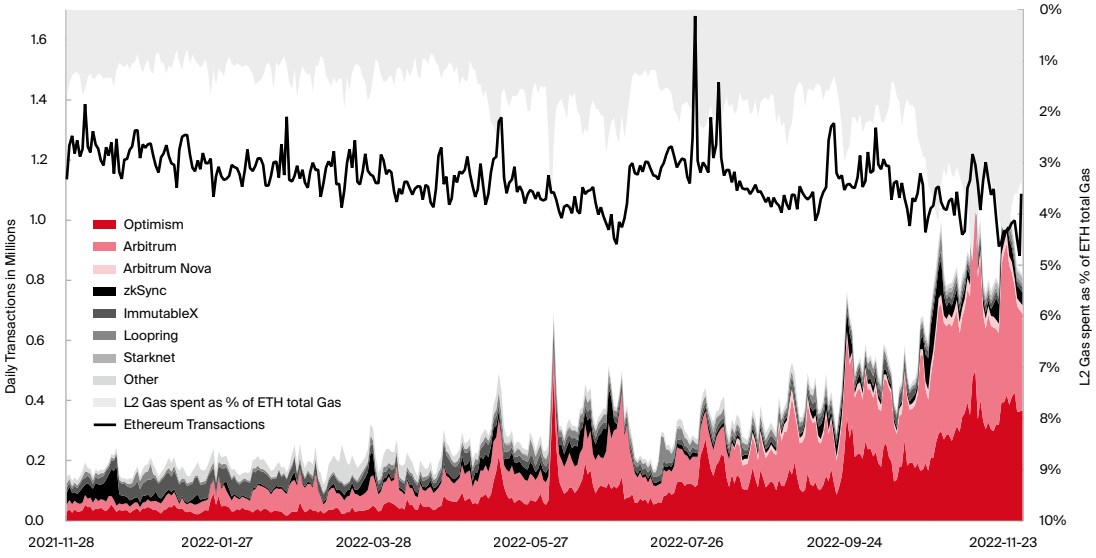


Illustration 12: Transaction activity on optimistic (red) and ZK-Rollups (grey) compared to Ethereum Mainnet. Data: Orbiter Finance, Dune. Chart: Bitcoin Suisse Research

state. The data is handled by sequencers and validators.

Within recent years, unsustainably high transaction costs on Ethereum haunted users and induced a wave of alternative L1 smart contract platforms alongside L2 scaling solutions atop Ethereum. While the expanding set of protocols with varying design tradeoffs created viable alternatives for developers and investors alike, 2022 revealed substantial interest in rollups. Underpinned by low transaction cost, Ethereum's rollup-centric roadmap began to materialize in '22 while alternative L1s such as Avalanche, or Solana dropped massively across most relevant metrics. Even Ethereum suffered declines across the board, as for instance, its total value locked (TVL) shrank from the peak in November '21 at $110.28b (22.9m ETH) to $22.9b (1.06m ETH) in December '22. The best relative performance in TVL, despite declining, was seen in both Arbitrum and Optimism (Illustration 11), where optimistic rollups are indicated in yellow and alternative L1s in red. In fact, Arbitrum and Optimism steadily climbed up the TVL leaderboard and are now the 4th and 7th largest chains by TVL, respectively. Arbitrum managed to take over former giants such as Avalanche (TVL peaked at $12.21b, now at $0.77b) and Solana (TVL peaked at $10.17b, now at $0.21b). Solana's drop was remarkable as its ecosystem was closely linked to FTX and its downfall. Solana is now trading at single digits, down from the November '21 peak of $259.96 and hence wiped out more than 96% of its value. Overall, scaling solutions have largely been dominated by Arbitrum, Optimism, and dYdX, which currently account for over 90% of the TVL across all Ethereum-based rollups[159].

The momentum of rollups was also reflected by a huge uptick in transactions. As of writing, they increased scalability of the underlying base layer by 2.44 times (7d average)[160]. It takes into account how many more transactions are settled on Ethereum on top of its native base layer transactions. For a one-month duration, the scaling factor currently lies at 1.84, including non-general purpose L2s[161] with Ethereum at 12.27 transactions per second (TPS), Arbitrum at 3.49 TPS and Optimism at 4.96 TPS. As a result, the L2 transaction count caught up with Ethereum's and even outmatches it occasionally, see Illustration 12.

While transactions on Ethereum where mostly rangebound this year, L2 transactions, especially those executed on Optimism and Arbitrum, grew substantially. Optimism grew in weekly transactions from around 0.3m in January to 3m in December while Arbitrum grew from 0.25m to around 2m. With increasing adoption, rollups also start to account for a significant percentage of gas spent on Ethereum. It's no outlier anymore that rollups range above 4% of the overall gas spent on Ethereum. For instance, the Arbitrum sequencer is constantly among the top gas spender on Ethereum. Given further adoption of L2s, sequencers of different rollups might soon be the tenants paying the highest rent to get their data stored on the L1 and to benefit from Ethereum's security. However, these tenants also extract value from the base layer since the rollup's sequencer is responsible for adding and ordering transactions and hence captures the majority of the MEV. This revenue can either accrue to the L2 token, to potential L2 validators or fund public goods within the rollup's ecosystem.

Heavy, Layer 1

In 2022, L1 ecosystems across the board suffered from CeFi blowups and heavy macro conditions. Ethereum showcased good resilience among smart contract platforms. Bitcoin, Tron, Binance and Matic even outperformed ETH by a good margin year-over-year (YoY), see Illustration 13.

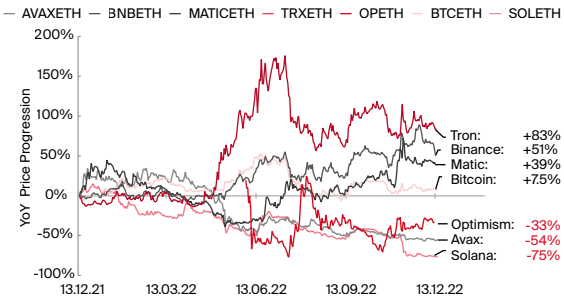


Illustration 13: Relative performance of selected protocols against ETH as base asset. Data: Tradingview. Chart: Bitcoin Suisse Research

From 159 blockchains that offer smart contract functionality, Ethereum accumulates 59.7% of the total TVL and accounts for around 47.6% of the volume on decentralized exchanges (excluding L2)[162]. Notably, 2022 saw a trend shift coinciding with the collapse of Terra Classic. While 2021 was characterized by an ever-declining Ethereum TVL dominance as more L1s and L2s emerged, 2022 marked a bottom in May at 49.8% indicating a saturation of blockspace. Since then, Ethereum's TVL dominance consistently climbed back up to ~58%.

We invite you to read Vires in Numeris section with more data on L1 and L2 ecosystems

As blockspace scarcity dwindles with more L1s and L2s on the battlefield, most monolithic and multi-monolithic chains suffered from a lack in revenue and blockspace demand. As of writing Polkadot, Ripple, Stellar,

EOS, Ethereum Classic, Litecoin and Monero have a combined market cap of almost $40b, yet only processed daily transactions worth $4'000 while Ethereum did more than $2'900'000. For instance, Polkadot also saw a steep drop-off in winning bids for parachain slots, down to an average bid of $0.69m in Q4 2022 from average bids of up to $109m in November 21[163]. Illustration 14 provides key metrics for selected protocols ranging from monetary policy, revenue, and decentralization.

As shown in Illustration 14, Ethereum's post-Merge inflation adjusted yield (nominal staking yield - inflation rate) is among the highest of all leading smart contract platforms. These yields will also influence the floor for DeFi lending rates due to arbitrage. The tokenomics of Avalanche, Solana, and Ethereum differ, but the underlying model shared by each of these networks has a burn mechanism to validate transactions and thus impact the net inflation. The rather high staking yields of Polkadot, Near, and Cosmos indicate a high inflationary monetary policy that dilutes users that don't opt to stake. The adjusted yields are outlined for the lowest barrier of entry staking solutions such as delegating to staking pools. That's how delegating stake in Cardano even yields negative returns if adjusted for inflation.

Protocol	Marketcap	Inflation	Adjusted Yield	Staking Ratio	Validator Count	7 Day AV Fees	P/S Ratio*
Ethereum	$159.9b	0.004%	3.86%	13.55%	487'656	$2.9m	151.1
Cardano	$10.9b	3.59%	-0.15%	71.33%	3'233	$7.1k	4'206
Polygon	$8.3b	6.79%	3.15%	37.08%	100	$34.3k	663
Polkadot	$6.3b	7.08%	6.92%	45.8%	297	$0.9k	19'178
Solana	$5.1b	6.48%	1.43%	70.02%	1,851	$25.9k	539.5
Avalanche	$4.3b	5.22%	2.83%	60.3%	1'212	$12.3k	957
Near	$1.5b	4.80%	6.69%	39.16%	139	$1.1k	3735
Cosmos	$2.9b	13.28%	5.98%	64.6%	175	n/a	n/a
Tezos	$0.9b	2.21%	0.69%	76.97%	390	n/a	n/a

** Based on annualized 7 Day average Fees*

Illustration 14: Key metrics of selected EVM and non-EVM chains sorted by market cap. Data: Crypto Fees, Staking Rewards, Near explorer, Polkadot.JS, Polygon Staking, Solana, Cosmos Hub, Avalanche explorer. Table: Bitcoin Suisse Research

We expect that adjusted yields on Ethereum face headwinds in '23 as withdrawals get enabled in March. Notably, the staking ratio of Ethereum still ranges lowest by a significant margin compared to other PoS platforms.

Among the smart contract platforms, Ethereum remains the central hub for novel applications and disruptive technology. To date, it's the blockchain with the most weekly active developers (2'199)[164], measured in number of distinct developers tagged to open-source repositories with at least one repository commits per week, ahead of Polkadot (1'074) and Cosmos (656). It also has almost 70x more validators than all outlined PoS protocols in Illustration 14 combined. Blockspace demand driving revenue is a reliable sign of a robust and healthy network. On a smart contract platform, the cumulated transaction fees and network revenue are therefore directly correlated. The lower the Price-to-Sales (P/S) ratio value, the better. Ethereum yields the lowest and Polkadot the highest P/S value.

As rollups offer unique benefits while sourcing the full security of Ethereum's decentralized trust pool, we expect sustained rollup adoption that becomes a new breeding ground for both DeFi and NFT innovation alike. Not only looming rollup airdrops but also the launch of a multitude of zk-rollups forged by Polygon, Scroll, Starkware or Matter Labs will heat up the rollup race in '23 and boost EVM dominance. They will enable a new level of data privacy,, efficiency, identity use cases, social networks, voting and games. Their complexity and maturity could leave them more vulnerable to centralization and security vectors in the short-term, however. While the EVM continued to dominate among smart contract platforms (83% of overall TVL), a growing number of alternative execution environments and appchains was present as well. We expect that 2023 will bring more clarity around the most permeating blockchain design. While the L1 narrative loses steam, promising blockchain architecture paradigms such as multi-monolithic and modular approaches like Celestia line up to compete. Cosmos and Polkadot allow liquidity from appchains to flow between previously siloed ecosystems while L3s allow application specific execution layers on top of L2s that can provide the base layer security of Ethereum. The era of Ethereum killers seem to fossilize and alternative L1s will rather compete with L2s.

We invite you to read our in-depth interview with Nick White, COO at Celestia Labs, on Celestia and the modular blockchain paradigm in this Outlook edition!

Continued momentum of L2s and the synergy emerging with Ethereum's roadmap towards modularity will likely reinforce its position as the dominant smart contract platform. While we might see a giant blend condensed in a multi-modular blockchain future, its most important modular component, being its substantial pool of decentralized trust, will be leveraged via restaking primitives such as EigenLayer, Therefore, Ethereum will maintain its gravitational pull towards users, developers,

and innovation going forward. As rollup technology is still immature, it usually comes with a basket of risks[165]. It is tainted with security and trust assumption such as upgradeability, sequencer or validator failure, mechanisms available to force an exit, multisigs or a varying reliance on the fraud or validity proofs. We expect to see substantial progress on that front indicated by e.g. Arbitrum decentralization upgrades or external sequencers like Stackr Network[166] or Espresso, a middleware[167] that is able to replace an internal, centralized sequencer. Eventually, they will close the gap and achieve to inherit the full security guarantees of Ethereum. Rollups currently also lack cross-L2 interoperability that we consider to be of major importance. Composability and liquidity fragmentation will be major challenges as we face adoption. Regarding scalability, the data availability (DA) bottleneck is being targeted by the upcoming Proto-Danksharding that will unlock a part of the peak theoretical performance of rollups. Heading into the next cycle, we consider rollups to be key infrastructure as they significantly enhance speed and cost without sacrificing security and decentralization – a true contender for solving the blockchain trilemma.

Fat ecosystem

In the last two years, we saw a drift from fat protocol to fat application. The fat application thesis argues that value tends to primarily accrue to the protocol instead of the application layer. In contrast, web2 represents fat application where most value accrues to applications built on top of web2 infrastructure. Taking the Ethereum ecosystem as a proxy, we observe that the fat application thesis took over with the rise of DeFi and NFTs, as Illustration 15 indicates. Overall, $330b in asset value lives on Ethereum. Only 44.5% is made up of Ethereum's native asset ETH while the majority resides in ERC20s, making up 49% of the total value secured. Notably, all this value is currently secured by 15.9m ETH or $19.3b, leading to a security ratio of 17.1 times.

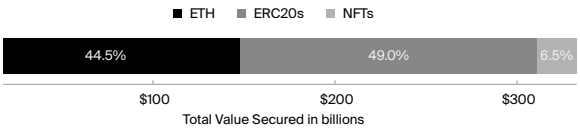


Illustration 15: Distribution of Total Value Secured on Ethereum. Data: Ultrasound. Chart: Bitcoin Suisse Research

While deploying dApps on top of Ethereum is permissionless, core network upgrades are permissioned and tend to slow down with increasing lindyness as the protocol ossifies towards its final form. The sovereign trust network established in the process is of immense value though. As the EVM unleashes open, permissionless innovation, there is a continued value exchange between dApps that consume decentralized trust and pay back fees in return. Hence, a system of organic mutuality emerges.

In 2023, we expect two major catalysts that likely counteract the fat application trend, at least to some degree: a boost in staking ratio initiated by the Shanghai upgrade that enables withdrawals and the onset of restaking primitives. Restaking primitives such as EigenLayer enable safeguarded middleware like bridges, oracles, sidechains, rollup sequencers or MEV relays and core infrastructure such as data availability layers by leveraging or re-directing staked funds such as ETH as security. As a result, Ethereum's massive pool of decentralized trust will not only be recycled, but will also substantially underpin ETH's utility while broadening its economic bandwidth. EigenLayer acting as a general-purpose marketplace for decentralized trust will provide a mechanism of internalizing modularity by recycling trust within the ecosystem. Since building decentralized trust is hard, EigenLayer will lift the overall security of dApps that incorporate middleware with low security guarantees such as bridges. For instance, re-staking only 1-2% of staked ETH would take over the existing security of most middleware[168]. While pooling Ethereum's trust layer across periphery infrastructure, restaking substantially improves capital efficiency and the overall value proposition of ETH, yielding increased staking rewards. On the flipside, restaking increases slashing risk as it's basically just another form of rehypothecation and leverage. However, EigenLayer providing access to Ethereum's cryptoeconomic security will dramatically reduce scaling cost for middleware, core infrastructure and its decentralized tech stack. Aiming for launch in 2023, it brings disruptive potential and might alter the way decentralized networks are designed. As it funnels more utility into the protocol layer, we expect that cascading synergy effects will eventually lead to a holistic thesis, the fat ecosystem, where value organically flows in tandem between the organisms (applications) and the physical environment (protocol) they live in.

The Outlook

The negative effects of various CeFi collapses hit hard in ’22 while a hazard around other major players is still looming. Yet, crypto is a tough cookie and we are cautiously optimistic about 2023 being a decisive year for the industry. While Ethereum pulled off a seminal moment in blockchain history with the Merge, it elevated its sustainability objectives, amplified its supply dynamics towards negligible issuance and redesigned its security model along a major efficiency improvement. Shipping the Merge heavily fed into Ethereum’s value proposition and will act as a confidence catalyst for further implementations of its ambitious roadmap. In 2023, we expect a vortex of upgrades that will initially enable withdrawals via the Shanghai and Capella upgrade. Following up, none other than Proto-Danksharding will hit Ethereum’s mainnet, that in a first iteration will optimize Ethereum’s blockspace into a data availability engine. This paves the way for full-fledged outsourced execution via Ethereum’s rollup centric roadmap and bulletproofs it for the modular blockchain age. We expect more awareness and progress towards censorship-resistance and a flight to self-custody. Likewise, we will see a continued battle, be it via internal or external infrastructure, towards optimizing MEV that is considered to be the Millenium Prize Problem of the industry. As Ethereum strives towards long-term protocol ossification, restaking primitives will unlock synergy effects enabling the fat ecosystem and further underpin Ethereum’s widely developed and capital heavy base layer. As multiple narratives converge to shape the future of blockchain architecture, anyone following the industry has all the reasons to be excited.

The author thanks Denis Oevermann for the important and valuable support creating the charts.

Disclosure: at time of writing, the author holds ETH, NEAR, XTZ, SWISE, RPL, MATIC, AVAX and ATOM.

Interview

Institutional adoption of crypto assets 2023

Dr. Dirk Klee

CEO of Bitcoin Suisse

by Thea Niederer

Cryptocurrencies have been gaining increasing attention and adoption in recent years, with more and more individuals and institutions exploring the potential benefits of using digital currencies. Despite this growth, however, institutional adoption of cryptocurrencies remains relatively low. In this interview, we will explore some of the factors that have held back institutional adoption of crypto and discuss some of the steps that could be taken to increase the adoption of cryptocurrencies among institutions. We will also look at some of the potential benefits of institutional adoption of crypto and consider the role that regulators and other stakeholders may play in driving this trend. In this interview, we are speaking to Dr. Dirk Klee, Chief Executive Officer at Bitcoin Suisse AG, about institutional adoption and potential future developments.

Thea Niederer (TN): The year 2022 was without a doubt a challenging one in the crypto world, with the crypto winter persisting into 2023. As you have been in the financial industry for a significant time, what are your takeaways of previous crypto winters regarding market developments and volatility? What is your outlook in this regard?

Dr. Dirk Klee (DK): Indeed, we are not only in a crypto winter, but also in a time with countless bankruptcies and rumors in the industry. What is special this time is that we see a combination of TradFi and crypto winter. For experienced players, low crypto prices for a longer time are not unusual. When it comes to Bitcoin, prices are linked to its halving event, which happens roughly every four years. The next halving will take place in 2024 and, considering previous halvings, the price will subsequently start to increase.

The crash in prices is also linked to the failure of several large market participants, among them FTX or Gemini. These crashes are symptoms of a rapidly growing industry in which regulatory guardrails in certain countries have been underdeveloped. Crypto exchanges such as FTX have moved to countries with little or no regulation, but still have global client reach. The misuse of client funds to finance other businesses is not a crypto-specific problem, but rather an issue of excessive leverage and a complete failure of corporate and financial control.

Nonetheless, we have seen positive changes in the market too. The volatility of cryptocurrencies has decreased. This is one of the main attacking points of the crypto industry, and we are now seeing it becoming more moderate.

TN: Seeing that you also have a lot of experience in building scalable platform-technology – how would you rate the interest of current institutional financial players in crypto technology right now and for 2023?

DK: Institutions are catching up and are noticing the possibilities the crypto space has to offer. 2022 already showed that some big institutions are entering the space. We see that happening with Goldman Sachs relaunching its trading desk for digital assets. Fidelity is launching a Bitcoin exchange-traded product in Europe and JP Morgan is developing a digital token and blockchain platform. I have worked at BlackRock, and it is interesting to me to see them disclosing their involvement in crypto, as it was previously commented that clients were not interested in digital assets. Blackrock has come around and opened to crypto and blockchain technology in the light of increased client interest.

Crypto has proven its resilience over the past months and it will do so even more in 2023. After the first institutional movers gained their advantages, others are following. It is important to understand that even in a crypto winter, the industry is not standing still. We and other players are developing and building our expertise and technology further – as we have learnt from traditional finance (TradFi) that new products and services will be launched once the market relaxes. The low prices and scandals might cause a delay; however, it can also serve as a necessary cleansing process before everyone starts to recognize the role of digital currencies in our society.

Another big momentum encouraging institutional adoption evolves around ESG. With the Ethereum Merge in 2022, the original Ethereum mainnet merged with a separate Proof-of-Stake (PoS) blockchain called the Beacon Chain, now existing as one chain. The Merge reduced Ethereum's energy consumption by ~99.95%. Institutions often have certain sustainability standards they must comply with which are met by such industry moves.

TN: You have mentioned trust and regulations, it is safe to assume those will be driving forces for institutional adoption in 2023. What kind of developments are you expecting and how will those be implemented without impeding innovation in the space?

DK: An important point I would like to mention is that the underlying problem in the latest crashes was not blockchain technology

but Centralized Finance (CeFi) practices in the crypto space without proper regulations and processes in place. The players that failed combined different roles and responsibilities that should be separated in the same institution such as custody, clearing, market making, brokerage, and advisory. I would argue that adequate regulation will enable innovation since the trust of clients and partners will be improved by establishing a sensible regulatory framework.

Trust and regulation are important in any financial system, including the market for cryptocurrencies. Trust is important because it helps to ensure that parties to a financial transaction can have confidence that the transaction will be carried out as agreed. In crypto the motto is "don't trust, verify" as assets are transferred without the need for central authority. The goal here is to create transparency in processes, hence trust the concept.

Regulation of institutions in the crypto market is also important because it helps to protect consumers and prevent financial crime such as money laundering and fraud. Cryptocurrencies are often associated with these types of activities, which should be put into perspective. The numbers are showing that 2-5% of global GDP is subject to money laundering, while it's less than 1% out of all crypto transactions that can be attributed to illicit transactions.

Regulation can also help to create a more stable and trustworthy market by providing clear rules and guidelines for how cryptocurrencies should be bought, sold, and used. Switzerland has so far taken a very proactive and innovative-friendly, technology neutral approach to regulation. As a "CeFi-adjacent" firm enabling clients and providing access to DeFi and crypto, we seek to apply for a bank license in Switzerland. Fulfilling regulatory requirements and undergoing advanced scrutiny will make Bitcoin Suisse an even more credible and trustworthy player in the industry than it already is.

The European Parliament is currently discussing Markets in Crypto-Assets Regulation (MiCAR). MiCAR regulates the issuance, offer to the public, trading, custody, advice, and portfolio management of crypto assets. MiCAR has been released in 2022 and is expected to enter into force in 2023.

Looking at the global crypto market, some crypto regulations stand out. The United States activated the Infrastructure Investment and Jobs Act (IIJA) on November 15, 2022. IIJA mandates that a broker will have to report any digital asset transfer moved to the account of an unknown person or address. The new rules stand to put tremendous emphasis on a broker's Know Your Customer (KYC) and tax information reporting systems.

The United Arab Emirates (UAE) aim to become a major worldwide hub for virtual assets. Dubai has made significant progress by establishing the Virtual Assets Regulatory Authority (VARA), the first authority in the world solely dealing with virtual assets. In 2018, the international financial center Abu Dhabi Global Market (ADGM) developed the first Virtual Assets legislation. VARA is in the process of creating a thorough and adaptable regulatory framework that will cover all virtual asset operations, license requirements for all Virtual Asset Service Provider (VASP) categories, and supervisory frameworks to monitor, evaluate, and reduce continuing risks.

To Bitcoin Suisse, it is important that the regulations in place make sense. They should be adequate but not hinder innovation unnecessarily. Our ambition as a crypto-native organization is to create access to DeFi applications based on trust, safety, and consumer protection.

TN: Thank you for setting the ground in terms of current developments, regulatory frameworks, and technological advances in the crypto space. Now take a closer look at the actual products and services you see most interest for in 2023?

DK: Custody is the most asked for service right now. We understand that our clients want peace-of-mind storage of their crypto assets. Secure custody of cryptocurrencies is all about how you store your seed phrase and how you use it. Originally, crypto is created for self-storage. Due to increasing institutionalization of crypto, the need for trusted custodians emerged. Bitcoin Suisse for instance

holds client assets either in separated custody on a client-specific blockchain address or in collective custody. In the former case, client assets can be segregated in the event of the default of Bitcoin Suisse. In the latter case, client assets are covered by a bank guarantee from a Swiss bank. Businesses thrive for the highest possible security.

Another service in demand from clients is trading and brokerage. We have talked enough about the risks, and everyone has learnt to look for limited counter-party risk. In 2022, we have seen other players risking client funds by not pre-funding trades. Swiss regulations are clear and we only trade for our clients through the most liquid exchanges worldwide. Most important, we take over the risk of dealing with exchanges for our clients through the most trusted and liquid exchanges worldwide.

Especially after the Ethereum Merge in 2022, Proof-of-Stake blockchains and with that, the service staking is becoming more and more popular. We see this as another signal for increasing demand for crypto by institutional clients, as it is an attractive solution to enable investors to obtain asset returns similar to yields from traditional financial products. Staking cryptocurrency is an ecologically friendly technique to secure the network because it does not demand a lot of processing power. Staking also contributes to the blockchain's increased effectiveness and security.

Lastly, and what I believe to be the fastest growing service is the need for advice and guidance in the crypto market. Especially in the institutional world, expertise in crypto is limited. Experienced, trusted partners are asked to provide insights into the crypto market, mechanisms, and projects. We have seen this a lot, as we have been actively in the space for almost 10 years now. As I have previously mentioned, the industry experiences a large number of scams and attempted fraud. Nevertheless, there are trusted partners in the crypto industry that seek to protect consumers and enable the use and adoption of DeFi applications in a safe and transparent manner.

TN: Last year was marked by considerable setbacks on the path to more widespread crypto adoption. Which chances and opportunities do you see in the financial space to further strengthen adoption of crypto assets and blockchain technology?

DK: In general, I think that increasing accessibility and education about cryptocurrencies, as well as improved security and stability of firms offering crypto products, will help to increase adoption. Additionally, partnering with established financial institutions and businesses may also help to build trust and confidence in cryptocurrencies. This will also further drive institutional adoption.

Usually, bear markets and developments, such as those we have recently seen, take time. In these times businesses focus on developing and innovation, while the macro environment is recovering. Over the upcoming time, more good things will emerge and we will see that the latest crashes are helping to improve the overall crypto space, as bad actors are getting flushed out of the market.

It's a great chance to move away from speculation and hype, towards blockchain innovation and how it can enable a more efficient financial system. There are some great real-world applications and tokenization projects that bring opportunities for crypto adoption in the market. Overall, weak players and projects will be left out and trust – regaining and rebuilding it - moves into the center of attention. Regulations that are on the horizon can create space for innovation in a safe way, and we as a crypto-native organization encourage technology-friendly approaches.

Thank you.

A Preview to the Bitcoin Suisse Global Crypto Taxonomy

The Bitcoin Suisse Global Crypto Taxonomy (GCT) aims to help investors navigate what we call “crypto space” today by differentiating better between the different coins, tokens, and protocols. However, instead of taking a technical approach that would, for example, distinguish by Proof-of-Work/Proof-of-Stake or fungibility of tokens, or by Layer-2 rollup type, we take the primary purpose of the digital asset in focus, its financial properties, and functions. In other words, we take an investor’s perspective to create a taxonomy that helps investors navigate this emerging, complex, and dynamic space.

For each sub sector, the GCT will feature a definition and set of inclusion as well as exclusion criteria. We will start with an initial set of classified digital assets and extend the scope over time. The structure of the GCT will also be regularly reviewed to always reflect our latest in analytics and conceptual thinking of the crypto space.

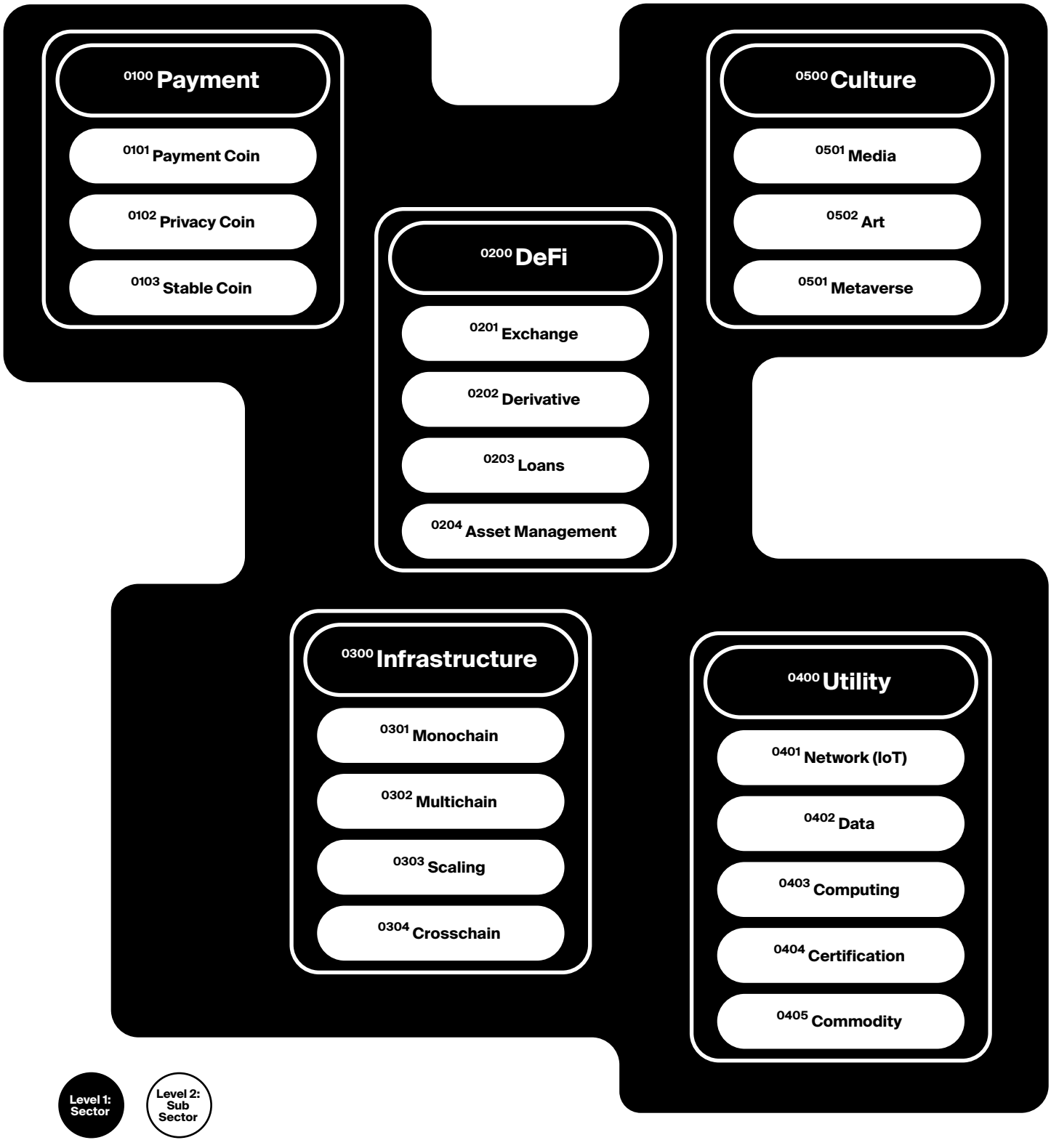
The GCT will be published in the first quarter of 2023.

What is a taxonomy?

A taxonomy is a scheme to classify elements into types inside a hierarchy. In biology classifies organisms, economics classifies companies, etc. It is done to describe systematically similarities and differences to better identify and group elements. All this help to structure a new space and thus understand it better.

Although the “crypto space” already exists for many years, only few attempts have been made in the last two years to create taxonomies for coins, tokens, and protocols.

The Global Crypto Taxonomy



Interview

“Modularism, not maximalism”

Nick White

COO of Celestia Labs

An interview with Nick White, COO of Celestia Labs, about the modular blockchain paradigm, solving the data availability problem, plans to bootstrap the Celestia ecosystem, and the shape of the future blockchain landscape.

by Dominic Weibel

Dominic Weibel (DW):
Let's start with a brief introduction of yourself, your blockchain background and the road that led up to Celestia.

Nick White (NW):
It's my pleasure to be here and I am excited to talk about modular blockchains and Celestia's role in the broader movement. I'm Nick White, COO of Celestia Labs and I first learned about blockchains in 2014. When I learned about Bitcoin, it didn't really stick. And then I learned about the theory in 2016 which kind of peaked my interest. Throughout 2017, I started going down the rabbit hole, educating myself, first through books, then blogs and Twitter, and finally research papers. By then I realized that the biggest problem facing blockchains was scalability, because until we had solved that problem, blockchains wouldn't be able to reach their full potential and they wouldn't have the impact that they could because it would be too expensive for people to use around the world.

In 2018, I set out to solve that problem. I co-founded a project called Harmony and we took an approach of using Proof-of-Stake and sharding, which were very new technologies back at that time to solve the scaling problem for blockchains. That went really well.

But then in 2020, I was reading this white paper called Lazy Ledger, and it just immediately struck me as a genius idea of essentially modularizing the blockchain stack. It separates execution from consensus and data availability (DA), which is typically all handled within one monolithic protocol, into separate layers. As a result, you get flexibility, scalability, and cross-chain communication. It was clear to me that this was the future of blockchain infrastructure and so I very quickly got in touch with the founders and ended up joining the project. Closely after that Lazy Ledger rebranded to Celestia.

DW: At a very high level, what is Celestia? Please talk us through the differences and nuances between modular vs. monolithic architecture and its underlying first principles.

NW: Celestia is trying to build next generation blockchain infrastructure that solves the problems that have held back blockchains from being as useful and as ubiquitous as they could be. There's a lot of different problems.

First and foremost, it is scalability, which is that most blockchains up until modular blockchains have had a finite capacity. They're like a laptop or a mainframe computer that has a certain amount of memory. It has a certain amount of capacity to run applications, and once you exceed that, it breaks down. We wanted to build a system that can actually expand the capacity as needed, as more people want to use it. That's one of the goals that modular blockchains aim to achieve.

Another issue is that monolithic blockchains come preloaded with an operating system. Ethereum has the EVM (Ethereum Virtual Machine), Solana has the Solana VM. And those sort of operating systems dictate what applications you can run. It's similar to having a Windows machine, a Macintosh machine or Android or iOS. The operating system that the blockchain runs, limits you on what kind of applications you can build. A modular blockchain doesn't even come with an operating system installed on it. You as the developer decide what you want to run. It adds this whole other dimension of flexibility for developers that they don't have in a monolithic framework.

Finally, modular blockchains provide a somewhat Holy Grail, which is shared security, where multiple blockchains share the same security framework by pooling their resources into one place and communicate with each other in a secure way. Whereas in the wild when blockchains connect with each other they end up having all kinds of vulnerabilities in cross-chain communication. Therefore, modular chains solve those three problems, and I could explain a little bit more about what exactly is going on in terms of splitting up the different layers and why we call it modular.

Data Availability (DA)
Data availability refers to a guarantee of nodes being able to download all transaction data from block proposers that previously published the entire data from the block header (includes metadata) to the block body (includes processed transactions) of their respective blocks. This allows nodes to verify blocks by re-executing transactions. Since all full nodes host this data, it is limited and expensive.

DW: We get to that "splitting up" and the building blocks now. To dive in a bit deeper, it would be great if you could guide us through the fundamental definitions in the modular stack, and the building blocks that are consensus, data availability (DA), execution and settlement.

NW: It could be helpful to use an analogy here. If you think of a blockchain like being a soccer game, consensus would be making sure that everyone sees the same order of events like each player when they kick or pass the ball. It happens in the same order among all people watching in the stadium. If we don't have an agreement upon what things happen and in what order, we're not actually watching the same game, right? So, consensus is all about ordering events.

DA is basically that you want to make sure that everyone is able to view the game. If it turns out that someone covers your eyes, and you miss part of the play then you won't be able to know what actually happened, and then what? Someone could have covered your eyes while committing a foul, but you didn't see it, and everyone pretends nothing happened and they get away with breaking the rules. So, DA is basically making sure that everyone is actually able to see the game.

Execution is basically enforcing the rules of the game. When someone commits a foul, you know there's a referee that can blow the whistle and confirm this person committed fraud that needs to be punished, or we restart the game, or we do a penalty kick.

And finally, settlement doesn't quite fit in this analogy, but it is a way of resolving disputes. Let's say there are two referees who disagree on the call. Then settlement provides a place where those two referees can duke it out and you can decide which one is making the correct call.

In a monolithic blockchain all these functions happen at the same time. The beauty of modular blockchains is that you can split those out into separate functions, and then those layers that specialize, like Celestia does in consensus and DA, get really optimized for that one purpose. For instance, you can build very specific execution layers that plug into it, and so you end up having a very specialized, scalable system.

To stimulate that soccer analogy, a monolithic blockchain is comparable to a single stadium that plays only one single game, such as soccer. It cannot expand the size of the stadium. If more people want to participate, it cannot contain more people because it is fixed in size. It can also only serve to play soccer as it only knows the rules to soccer. A modular blockchain is not a fixed stadium, it is more like an ever-expanding field. You can play soccer on that field, tennis, or basketball. You can play any kind of sports you want, and there isn't any fixed capacity. As more people want to play, you can increase the size of the stadium. So, a modular blockchain is equivalent to the Olympic Games with tons of different events, enabling a huge number of players and diversity while the monolithic blockchain is just one single, limited stadium serving one game.

DW: Very digestible analogy. Taking these core functionalities or modular building blocks, what kind of modular stack combinations make sense to you? Is the Holy Grail having consensus and DA together on the base layer like Celestia is aiming for? Or do you also envision modular blockchains that have other, more exotic combinations?

NW: You can get very exotic as you can have each layer running separately. There are, however, some benefits of coupling consensus and DA specifically, such as interoperability. And in general, if you are running a rollup, which is an execution layer, you're already relying on

another external layer for DA, adding another sort of dependency. That also counts for consensus that can make the architecture slightly convoluted and overly complex. Whereas if you combine consensus and DA together, it makes the overall stack more efficient and reliable. Since part of interoperability is that you can rely on the ordering of the other chain you want to talk to, that it has the same ordering as your chain and the same DA, you also get better interoperability guarantees. It's a nuanced concept. However, I fully expect there to be more exotic combinations. For example, one thing that we've built is the Quantum Gravity Bridge, which allows someone to build a rollup that uses Ethereum for consensus and settlement and Celestia for DA. The advantage in that variant is that Celestia is very cheap as there's a lot of block space, but Ethereum has lots of assets and users. By settling to Ethereum you get access to that ecosystem by splitting the consensus and DA parts and coupling settlement and consensus together. It can get complicated, but there's a limited number of different configurations at the end of the day.

DW: I personally find it especially hard wrapping my head around the degree of freedom you get with a modular stack when it comes to the execution and settlement environment. Only looking at the rollup possibilities, offering sovereign rollups, settlement rollups and smart contract rollups, and the range of potential combinations is mind bending. It will be very exciting to see how this evolves and how the design space is utilized in the future.

Let's focus on some properties that Celestia will offer once launched. Celestia is sometimes referred to being a hybrid approach that offers the best of both worlds between Cosmos and Ethereum by having sovereignty, shared security, that you already mentioned, and peer to peer bridging. Why are these aspects so important and where do you consider the trade-offs of going modular and having no settlement layer?

NW: I really like that you brought up this topic of Ethereum and Cosmos because when I think of the evolution of blockchain architectures, Ethereum was a massive leap forward because it created this shared smart contract platform where developers could write a new application and deploy it very easily without having to create a new blockchain. And out-of-the-box it would have the shared security of the Ethereum network behind it. And that's beautiful because it becomes very easy to build new applications and those applications can connect to each other, interoperate and be composable.

But then the downside of that is that everyone's building on the same finite computer, right? And as more applications get built and more users come online, those applications are fighting for resources. And eventually the machine gets overloaded, and you end up having congestion and the fees spike. And so Ethereum has this problem of scalability, but also has a problem with sovereignty, a more nuanced concept. Blockchains are coordination mechanisms, and if you are a developer writing applications, you want to be able to control that application at the social level. If something bad happens, you want to be able to reallocate resources, undo a hack or just upgrade. Let's say I want to make a change to the EVM. I want to be able to upgrade the EVM to better support my application. Unfortunately, that application is locked within the broader social consensus and sovereignty of Ethereum, so you don't actually have application-level sovereignty. Ethereum was a massive step forward but had those two drawbacks.

Cosmos then came online with a different vision, which is sort of the Internet of blockchains. Being able to build sovereign blockchains according to the Cosmos vision was very important because people want to be able to customize their blockchain for their application. They want to be able to fork it, upgrade it and do what they want. The second pillar of the Cosmos vision was the relevance of scalability. By having every application run on its own blockchain, it is comparable to every application running on its own computer. Each computer has way more capacity than if you are trying to stuff all those applications on a single computer. But what they gave up in their design was that each application must be deployed on a new blockchain. Thus, you

lose the ease of deployment that you have with Ethereum, where you just write a smart contract, press deploy, and it is done. What they also lost was this shared security component as all the applications that are built upon the Ethereum security layer do not have to bootstrap a new secure consensus network from scratch.

Those two networks had those two problems, and basically Celestia is like the marriage of those two visions where we can get all four of the above. Because Celestia is like Ethereum in that it provides this shared security layer. It makes it very easy to deploy your own blockchain and is similar to a consensus network that you can deploy your application logic to. Yet, it also gives you sovereignty because your execution layer only plugs into Celestia. Celestia has no governance control nor dictates what you do with your execution layer. Moreover, it does not suffer from scalability problems. As it uses data availability sampling (DAS), you can expand its capacity with the number of nodes in the network. So unlike Ethereum, it won't run into congestion problems in the future and that's why it is basically the best of both worlds. It takes the best of Ethereum and the best of Cosmos and brings them together into one ecosystem. And we call that the Internet of modular blockchains.

Data Availability Sampling (DAS)
Data availability sampling refers to a cryptographic method for verifying DA without downloading the entire block data. Light nodes utilize DAS by doing numerous rounds of random sampling small subsets of block data. The node's confidence in available data grows with each round of data sampling until a predetermined threshold that indicates DA is reached. DAS enables cheap hardware (such as light nodes) to take over more important tasks within network security and throughput, that were previously solely reserved for full nodes.

In the future Ethereum will pursue a modular blockchain development path. However, they started out as a monolithic blockchain with a EVM, a fully monolithic state machine. The problem is this adds friction and is not fully modular. The benefit however is that Ethereum comes with a built-in settlement layer, meaning a place where rollups can post their proofs in order to bridge and resolve disputes, a useful tooling when building rollups.

Now, Celestia has explicitly decided not to do that, because we want to be as modular as possible. Therefore, if we enshrine a settlement layer, first of all, it's not credibly neutral. We end up starting to try to compete with other settlement layers that might want to be built on top of Celestia. And second of all, we also compromise the modularity and create more overhead on people that are using the Celestia network.

Rather, what we want to encourage is that people build settlement layers on top of Celestia, and there are already several teams that are doing that. It does not make sense to choose one single settlement layer because there's going to be lots of different ways of optimizing the settlement layer for different kinds of rollups or different kinds of use cases. It also seems premature to say that the EVM is the destined execution or settlement environment. So luckily, we are not locked into any of those decisions now. The downside is that there is not a native way to bridge the Celestia token up to the second layer. There are trusted ways to do so, but there is no trust minimized way to do that which you can do in the Ethereum ecosystem. However, I think it is a problem that we're aware of and working on. I think there's going to be good solutions that emerge, and we already have the beginnings of some, but it is a downside.

DW: Very interesting. Adding as a side note as it matches context: I recently saw a talk from the founder of EigenLayer and he also came up with this aspect of having Ethereum modularizing its decentralized trust pool for example. And I guess that's one problem or one challenge that Celestia is facing, starting a new protocol or chain that must bootstrap the network in the first place.

The modular blockchain paradigm is recently all over the place, and it seems to be the hot topic of '23. As modular blockchains are get-

ting traction, more projects enter the space. Could you shine some light on how Celestia differs to modular projects with similar approaches such as Polygon's Avail, EigenDA or even rollup provided DA such as StarkEX, zkPorter or Arbitrum Nova and their design considerations?

NW: Celestia was the first modular blockchain network and sort of the first data availability layer to be built. We were first to testnet, and I think likely the first to launch to maintain later this year. But there's been a lot of other projects that have come online. First of all, Ethereum has adopted a modular sort of blockchain development roadmap, which is very exciting. And then other projects like Polygon have come online. And as you mentioned, zkPorter and even Arbitrum Nova, StarkWare and EigenDA. A lot of people are building their own DA solutions.

Compared to Ethereum, Celestia has no enshrined settlement, so we are just going pure DA, sort of maximally modular. And we think that is the right long-term architecture and design decision. With Polygon Avail, they're choosing an architecture that's based on KZG commitments, which are lot more computationally expensive, slower and have a lot of drawbacks that we think are, at least for now, not the right sort of commitment scheme to use. And the other problem I would say with Avail is that they're not credibly neutral because they are also building their own rollups and their own ecosystem. And so Celestia is, on purpose, not delving into the rollup development side of things. Imagine if Ethereum was building their own Uniswap or their own applications and thereby competing with the developers on their chain. We think that is a) not credibly neutral and b) likely won't attract the right kinds of developers.

And so, I think that's one issue that Avail has, and I would say something similar in regard to the other rollups like Arbitrum or StarkWare that are building their own DA solutions. A lot of them are a) just not actually the fully fledged data availability sampling solutions and b) they're isolating the ecosystems as they are building a rollup and their own DA solution. It's like a monolithic ecosystem that behaves like a vertically integrated sort of siloed thing. Yet, the benefits of this modular blockchain stack are that you do not have to build everything on your own and end up sharing security and this ecosystem, having interoperability with different rollups. If Arbitrum, StarkEX, zkSync and all the Polygon rollups are running on their own DA layer, it defeats the original purpose of why we're building the modular paradigm in the first place and that's why we say modularism, not maximalism. We want to have this open ecosystem where everyone's building in a shared way. A place where we collaborate rather than trying to carve out our own siloed piece of the pie and not share with other people.

DW: That's a compelling perspective, especially considering the roadmap of Ethereum that is also heading into the modular direction. Hence, as Celestia will be maximally flexible, modular stacks that leverage Celestia's DA can plug into Ethereum like Celestiums are aiming for.

As we move on, let's briefly focus on the consensus engine of Celestia. With the DA layer of Celestia running on a PoS blockchain built with Cosmos SDK, are there any exciting new technical quirks when it comes to Celestia's Core consensus mechanism? And will Celestia be plugged into Cosmos Hub?

NW: We are built on the Cosmos stack, so we use Tendermint and the Cosmos SDK, but we also have modified a lot of those things to add in the capabilities for data availability sampling and to support the core use case which is being a DA layer. Therefore, we have made lots of different changes, but at our core, a lot of it is based on Tendermint and the Cosmos SDK. The good thing about that is that we do get IBC support out-of-the-box. Also, we get support for all different kinds of wallets and block explorers out-of-the-box, which is advantageous.

One of the challenges for doing data availability sampling, is that there is a lot of networking complexity because most blockchains do not really have this topography where all these light nodes are requesting random sam-

ples of data. And so that was among the first modifications made, building a component of our node software that handles all that complexity, both in networking and the different kinds of requests that you get. It's just a totally different functionality that the blockchain needs to have when you want to support something like data availability sampling and to be able to reconstruct blocks. So that's one of the big things. The other big thing is within Tendermint.

The way that the blocks are encoded to support data availability sampling is novel. We had to encode the blocks using this thing called 2D Reed-Solomon erasure coding and so we had to really modify Tendermint to be able to encode that block box in a new way. We had to create new kinds of transaction formats that are all about paying to include just a blob of data rather than paying for a typical transaction and pack the block in an effective way. Because we want to have very large blocks in the future, we had to think about how to gossip the block data and the mempool in an efficient way, so that we can build blocks very quickly while essentially minimizing bandwidth overhead. This is a high-level summary of some of the bigger changes that we've made and some engineering innovations that we have done under the hood.

DW: Speaking about development, I just recently got an e-mail for the upcoming incentivized testnet and I wondered if you are happy with the current progress especially within the Mamaki testnet and what the biggest obstacles have been? As we inch closer to mainnet launch in 2023, Celestia will start its network from scratch. How is Celestia tackling this problem of new protocols having to bootstrap its decentralized trust network? Are there any mechanisms and incentives planned to catalyze network distribution and get more validators on board?

NW: First of all, we're very happy with the progress. To build a live network that supports data availability sampling is a major engineering achievement, not just for Celestia, but for the blockchain industry overall. We're doing pioneering work, and that is not easy. We are on track for the mainnet launch this year, which is exciting.

In terms of bootstrapping the network, we do have an incentivized testnet coming up later this quarter. That's going to be one of the primary ways that we start out this validator community, get a lot of people on board running nodes and educate the community more broadly about all the different node types. This will form the seed for the network launch later this year. A lot of those same validators would be the core original validators of the network. Decentralization and bootstrapping this new consensus network are aspects that we take very seriously. Over time, we want to increase the number of nodes in the network.

However, one of the beautiful things about Celestia and the way it is designed is you do not have to trust the validators. You do not have to worry about them being honest or not, because if you are running a light node, which anyone will be able to do on their smartphone, you can self-verify that the validators are not cheating you or doing anything wrong. Therefore, you don't have to trust based on assumptions derived from the validator set. You can just directly verify the network yourself. Thus, we are not as dependent on having this sort of decentralized network of validators as it is still critical but not security critical because the validators are very limited in what they can do. That underpins the original vision of blockchains as you do not have to delegate your trust to another source. The whole point is peer-to-peer by which each peer in the network can verify the chain directly themselves. If I start delegating my trust to another group, even a highly decentralized group of validators, it starts to look more like a consortium, more like web2 and not like web3. Therefore, things like Solana, at least in their current form, don't really achieve what blockchains are meant to do from our perspective, because even if there's a bunch of different nodes, no user has any ability to verify what is actually happening on the chain. You're just trusting this group of validators who you do not know that they do the right thing.

DW: Looking forward to a future, where everybody can participate in consensus by running light nodes from private phones.

Moving into 2023, apart from the Celestia mainnet launch of course, what are you most excited about and how do you envision the crypto landscape to shape in the upcoming years? Will we move away from yet another monolithic Layer1 only offering incremental improvements to a modular blockchain world? What role will Ethereum play in that future and what role will other (multi-)monolithic Layer1s play? Is the future both modular and multichain as we will see with Celestia that is plugged into Cosmos? Or will application specific Layer3s even render appchains and multichains obsolete?

NW: Answering the broader question, it's no surprise that I'm very excited about modular blockchains because I think they are going to solve the core problems of blockchain infrastructure. To date, everyone has been trying to solve that problem. That's kind of why there's been so many Layer1s, right? While everybody thinks to have found the solution, we are trapped in this perpetual cycle of a new Layer1 that has some new cool fancy thing without any actual fundamental innovation. So modular blockchains is the first time that people have gone back to the drawing board and realize that there is a fundamentally better solution, a new foundation to build upon and we can innovate on top of this. In a sequential way, moving forward, rather than just a cycle where we are going to loop, which is where we were stuck with this monolithic blockchain world. So that's obviously the foundation of what I'm most excited about now.

Within the modular blockchain stack, there's a lot of things to talk about. For instance, one is zero knowledge (zk) technology. There's been a huge amount of innovation in the zk rollup space and there are a lot of teams who are building the foundation to make zk rollups a lot more practical. What is special about zk rollups is that they have better interoperability and finality properties. They also have better verification that eliminate complexities of fraud proofs that are utilized by optimistic rollups.

I'm also excited about people building rollup SDKs. Celestia provides the base level infrastructure that you can plug into but there's so many other pieces that need to come into play to make it easy for anyone to deploy a new rollup. Developer tooling like SDKs, is a big part of that. Another part of this are decentralized sequencer networks.

Even though a rollup can outsource its decentralization to a network like Celestia, you still must have someone to run the rollup execution layer nodes. It can be one node, or it can be a set of nodes, but ideally that could be a service that you can also tap into. Hence, there are several people working on making that itself into a service, essentially sequencing as a service. With the possible combinations of these things together, the rate of innovation will absolutely explode, and I think that might only be a couple of years away.

That leads me to another component, which is people building new types of execution environments. There are teams that build a new gaming execution environment. A lot of the people who are building games now are building on the EVM or the Solana VM without realizing the constraints that this imposes. I cannot share too much because they are still in stealth. But if you start over, you can create an execution environment that has pre-built-in a lot of the primitives that you would want if you are building gaming applications. They want to basically build the operating system for blockchain gaming. Overall, there is just a lot of innovation that still has not really been tapped into from that perspective.

It is amazing to see the Cambrian explosion of different ways that people are interpreting the modular blockchain thesis and expanding on it on all these different dimensions.

DW: Very exciting. There seems to be a huge momentum ahead as we are almost able to provide the infrastructure for global adoption. Thank you very much for your precious time, Nick. We wish the team and you the best of success with the mainnet launch in 2023, that so far promises to be explosive.

Article

Striking the Right Balance in Regulating Crypto

Since the emergence of Bitcoin in 2009, the adoption of crypto assets has grown rapidly, and they have become an integral part of the global financial system. Rapid proliferation of such new assets has triggered repeated calls for regulation. Regulatory concerns to date have focused mostly on consumer protection, anti-money laundering, countering terrorist financing and potential transmission channels to financial stability risk.

by Dr. iur. Cansu Burkhalter,
Dr. iur. Fabio Andreotti, Oliver Gehrig

Policymakers worldwide struggle to monitor risks and implement consistent regulations in this rapidly evolving sector. Today, regulatory measures vary significantly by country: outright bans towards crypto exchanges in China or against privacy tokens in South Korea, consumer protection initiatives and certain regulatory guidance from US court rulings, a tax reporting standard from the Organisation for Economic Co-Operation and Development (OECD), anti-money laundering regulations from the EU, warnings about the risks of initial coin offerings (ICO) and regulatory approvals of crypto exchanges in Japan as well as adoption of Bitcoin futures contracts in the US.

Looking at the developments domestically, Switzerland became a stronghold for the crypto industry due to the neutral stance adopted by Swiss regulators regarding new and emerging technologies. Switzerland was one of the first countries to enact legal regulations for blockchain technology. Moreover, the Swiss Federal Tax Administration has clarified the taxation of cryptocurrencies through a working paper in 2019, generally subjecting them to wealth tax and in some instances income tax in a fair and transparent manner, thereby removing any ambiguity concerning taxation of crypto assets. Such initiatives create reliable and clear rules-based frameworks.

Crypto has also been associated with fraud and undue exuberance since its emergence. The early days of crypto were marked by hype and speculation, which led to the ultimate failure of some projects, causing financial losses for investors due to the lack of clear regulations. However, as the industry has matured, we have seen many new successful projects offering genuine technological innovation. Regulations that are not unduly biased by bad actors but maintain a constructive approach towards an orderly integration of crypto assets into the existing financial system are key to promote further growth of the crypto industry.

Proportionality and technology neutrality are the core tenets of crypto regulations. A technology-neutral approach should be pursued regarding the regulatory treatment of blockchain activities that is proportionate to the level of risk. Wherever possible, any differences in legal treatment should arise from (and be tailored to)

	OECD	EU	USA	SINGAPORE	CHINA	SWITZERLAND
Regulation/ Standard/ Rule	Crypto asset reporting Framework (CARF)	Markets in crypto assets Regulation (MiCAR)	Infrastructure Investment and Jobs Act (IIJA)	Proposal on Regulatory Measures for Digital Payment Token Services	Ban	Distributed Ledger Technology Act ("DLT Blanket Act")
Purpose	CARF provides for the reporting of tax information on transactions in Crypto-Assets in a standardized manner, with a view to automatically exchanging such information	MiCAR regulates the issuance, offer to the public, trading, custody, advice and portfolio management of crypto assets	IIJA mandates that a broker will have to report any digital-asset transfer moved to the account of an unknown person or address. The new rules stand to put tremendous emphasis on a broker's Know Your Customer (KYC) and tax information reporting systems.	The proposal sets out regulatory measures for licensees and exempt payment service providers that carry on a business of providing a digital payment token service under the Payment Services Act 2019.	The People's Bank of China (PBOC) banned financial institutions from handling Bitcoin transactions in 2013 and went further by banning ICOs and domestic cryptocurrency exchanges in 2017.	The Act aims at adjusting Swiss laws to take advantage of cryptocurrency innovation. The Act included a new type of license category for cryptocurrency trading venues.
Status	CARF was released by the OECD on October 10, 2022.	MiCAR was released on June 30, 2022, enter into force is expected 2023.	IIJA became law on November 15, 2022.	In progress	No changes expected in the near future	The Act entered int force as of February 1 and September 1, 2021.

Table 1: Overview of crypto regulation in selected jurisdictions
Source: Bitcoin Suisse Legal and Bitcoin Suisse Risk & Compliance

material differences in the business or risks associated with the technology. Prematurely created regulations that are excessively broad and overly complex would stifle the further adoption of crypto assets as a key component of the financial services industry.

> "An effective regulatory framework should ensure that crypto asset activities posing similar risks as traditional financial activities are subject to the same regulatory outcomes."

Meanwhile, it should take account of novel features of crypto assets and harness potential benefits of the underlying technology. Both traditional finance (TradFi) and crypto finance adhere to similar principles with respect to addressing anti-money laundering (AML) and countering the financing of terrorism - but not always through identical rules.

International Regulatory Developments

Crypto Asset Reporting Framework (CARF)

Unlike traditional financial products, crypto assets can be transferred and held without the intervention of an established financial intermediary and without any central administrator having full visibility on either the transactions carried out or on the crypto asset holdings. Therefore, crypto assets can be perceived as undermining existing international tax transparency initiatives, such as the Common Reporting Standard (CRS).

Many jurisdictions have already established reporting regimes requiring virtual asset service providers to report transactions to both the agencies in charge of combating money laundering and the financing of terrorism, as well as tax administrations. However, countries do not currently have information on operations carried out through crypto exchanges located abroad, since such exchanges are not obliged to share information with central banks, tax authorities or other public bodies.

In October 2022, the OECD released a stand-alone framework for the automatic exchange of information on crypto assets, the so-called Crypto Asset Reporting

Framework (CARF), which ensures that crypto asset transactions are brought into information reporting rules. The CARF mirrors many of the reporting requirements of the CRS regime and introduces sweeping new third-party information reporting requirements for crypto assets that far exceed the CRS reporting obligations imposed on traditional financial assets and market participants.

The definition of crypto assets targets those assets that can be held and transferred in a decentralized manner, without the intervention of traditional financial intermediaries, including stablecoins, derivatives issued as crypto assets, and certain non-fungible tokens (NFT). The definition is meant to ensure that all assets covered under the new tax reporting framework also fall within the scope of the Financial Action Task Force (FATF) recommendations, ensuring intermediaries' due diligence requirements can build on existing anti-money laundering (AML) and know-your-customer (KYC) obligations. The following four types of relevant transactions are reportable under CARF:

- Exchange from crypto assets to fiat currencies and vice versa
- Exchange from and to different forms of crypto assets
- Reportable retail payment transactions above USD 50'000; and
- Transfers of crypto assets.

The OECD will continue working with participant countries and industry stakeholders to ensure that CARF will be implemented consistently globally. It is expected that countries will start transposing CARF into national law as of January 1, 2026. The European Union has already released the proposal for the directive which will capture the requirements brought by CARF.

Markets in Crypto Assets Regulation (MiCAR)

Most crypto assets do not qualify as financial instruments within the definition of the respective European Union (EU) regulation, the Markets in Financial Instruments Directive (MiFID). For all crypto assets that are not considered financial instruments, there is no unified European regulation so far. Therefore, there still exists market fragmentation within markets governed by national regimes, without the possibility of the freedom of service by means of passporting crypto services throughout the European crypto space, as it is possible for TradFi institutions such as banks. This fragmentation also implicates the unintended consequences of regulatory arbitrage and uncovered risks. Addressing the above-mentioned shortcomings, the EU authorities are in the final stage of the legislative process to issue a landmark crypto asset regulation – the MiCAR.

MiCAR will bring uniform European requirements for crypto asset issuance. For instance, issuers must publish a white paper for investors containing specific information about the crypto assets to be issued. MiCAR also regulates the liability of issuers. It defines crypto assets as a digital representation of a value or right that can be traded via a distributed ledger (e.g., a blockchain). Crypto assets that are not redeemable and that represent a unique real asset – known as non-fungible tokens – fall outside the scope of MiCAR. The same applies to crypto assets with the same characteristics as existing financial products or instruments. This means that tokenized securities and other instruments are covered by existing MiFID rules. Stablecoins, however, do fall within the scope of MiCAR: Specific and additional rules will apply to issuers of stablecoins, especially regarding the assets that serve as reserves. MiCAR distinguishes between stablecoins whose value is linked to multiple fiat currencies, commodities, or crypto currencies (known as Asset-Referenced Tokens, ARTs) and stablecoins whose value is linked to the value of a single fiat currency (Electronic-Money Tokens, EMTs).

Alongside crypto assets and their issuance, MiCAR also regulates certain crypto services. These include operating trading platforms, exchange services (crypto to crypto or regular currency) and custody services for crypto assets. The professional provision of advice and portfolio management services for crypto assets are also considered crypto services by MiCAR. Providers of crypto services must obtain a license from a financial supervisor within the European Economic Area (EEA) or EU and comply with consumer protection as well as with disclosure requirements. Their governance structures and information security systems must be in order, they must detect and respond appropriately to conflicts of interest, have a complaints procedure and provisions on outsourcing in place. Transaction service providers must also put in place effective systems and procedures to detect market manipulation.

Under MiCAR, issuers of stablecoins or anyone offering crypto services must obtain a license to do so from their domestic financial supervisor within the EEA or EU. This license allows MiCAR-regulated activities to be undertaken in all EEA countries. The MiCAR regulations are currently being finalized and are expected to come into force in the coming months. MiCAR rules for issuing stablecoins are expected to come into force 12 months after publication, the other regulations after 18 months. In addition, European Supervisory Authorities

(ESAs) are anticipated to soon start developing detailed technical standards for implementing the new rules. The new MiCAR rules are expected to take effect in 2024.

Regulatory Developments in Switzerland: Custody

Swiss lawmakers have been quick to recognize the new opportunities offered by blockchain and DLT technology. The way blockchains and cryptography work enables property-like legal implications as in the physical world. Clearly, the most important part of the so-called "DLT Blanket Act", a new piece of legislation adopted in 2020, has been the clarification of what happens to crypto assets of clients in the event of bankruptcy of a Swiss crypto custodian. Extensive discussions paved the way for Bitcoin (BTC), Ether (ETH) and all the other crypto assets to now enjoy the same bankruptcy protection as physical objects.

When it comes to crypto custody from a legal perspective, we can distinguish three main cases:

In the first case, the client has exclusive control over his or her crypto assets. Even if the client relies on wallet software run by a third party, the client will not have to take legal action against that third party in the event of bankruptcy. In the second case, the custodian and the client have shared control over a crypto asset belonging to the client. The fact that the custodian also has a relevant cryptographic key to control the assets does not change the legal situation in the event of bankruptcy. Ownership of the assets firmly remains with the client even after the opening of the bankruptcy proceedings. Finally, in the third case, the custodian has sole control over a crypto asset belonging to the client. According to the recently revised Swiss Act on Debt Enforcement and Bankruptcy, if the custodian undertakes to always keep the crypto assets available for its clients and the crypto assets are individually assigned to them, their crypto assets are fully protected in the event of bankruptcy of the custodian. In such a case, clients would have a direct claim against the bankruptcy estate to hand over the crypto assets in kind. In other words, clients who held BTC before the opening of bankruptcy proceedings would eventually receive their exact BTC back. In addition, such custody works much like a segregated account at a traditional bank because company funds are not commingled with clients' assets on the blockchain

At Bitcoin Suisse, we refer to the third case as Separated Custody. As described, this type of custody ensures that client assets are bankruptcy remote. We offer Separated Custody in two versions with different features: Clients with a Bitcoin Suisse Crypto Account generally have their assets stored on client-specific blockchain addresses; clients with a Bitcoin Suisse Vault Account have permanently assigned blockchain addresses and retain as much control as possible within a custodial environment. On the other hand, if client assets in the Bitcoin Suisse Crypto Account are held in Collective Custody, they are generally fully protected by a default guarantee from a Swiss bank as required by Swiss banking laws (certain groups of clients may be exempted according to current regulation – however, this does not affect their crypto assets held in Separated Custody).

Unlike cases like Mt. Gox where former clients are still waiting for their payouts and will likely only get an equivalent amount in fiat, clients holding their assets in Separated Custody with a Swiss custodian must not fear that their crypto assets fall into the bankruptcy estate or are converted into fiat claims against their will. We can therefore conclude that Swiss lawmakers have solved a crucial matter of the crypto industry in a very efficient and customer-friendly way. At Bitcoin Suisse, we have worked hard to take advantage of the new rules for the benefit of our clients.

Application of Existing Regulatory Standard to Crypto: BEX/FIDLEG

Legal and Regulatory Basis

The duty of Best Execution derives from both private and supervisory law. Under private law, the Best Execution principle is based on contract law. Service providers who execute orders on behalf of their clients typically have a legal relationship with their clients that is governed directly or by analogy by agency contract law or the like. Accordingly, the service provider owes the client loyalty and care when executing transactions assigned to him.

For financial service providers to which the Swiss Financial Services Act (FinSA) applies, this principle is further specified in art. 18 FinSA. Thus, financial service providers subject to the FinSA must ensure that the best possible result is achieved in terms of cost, time and quality in the execution of their client orders.

Even though Bitcoin Suisse is currently not subject to the FinSA, we are committed to adhering to Best Execution industry standards known from traditional finance to achieve the best possible outcome for our clients.

Best Execution in TradFi vs. Crypto

To ensure a proper trading process and investor protection, end clients and certain service providers representing such end clients do not have direct access to the markets on which specific products are traded. Consequently, these market participants must rely on the services of third parties. Client orders shall be executed in such a way that the best possible result for the client is achieved. In particular, the third-party provider shall promptly conclude client orders at the best possible market price at a generally recognized, suitable execution venue that guarantees the orderly execution of the transaction, considering the limits, conditions and restrictions set by the client. When executing the order, the service provider shall strive to achieve the best possible overall result for the order in question.

In both TradFi and crypto, Best Execution refers to the practice of executing transactions at the best possible price, considering factors such as speed, cost, and likelihood of execution. This is typically accomplished using advanced trading tools and algorithms that provide access to a wide range of liquidity sources. Achieving Best Execution in crypto can be difficult due to its complex landscape of centralized exchanges, decentralized marketplaces, and the corresponding counterparty and protocol exposure. While the principles of Best Execution are similar in both TradFi and crypto, the approaches and strategies for achieving it can differ significantly. To successfully achieve Best Execution in this environment, it is necessary to have a deep understanding of the underlying markets and the industry.

Best Execution. Applying Best Execution does come with many considerations, simply hitting the best price on the market does not guarantee Best Execution. The likelihood and speed of execution are also crucial factors to be considered. Looking at order book depths, identifying the best trading venue(s) to execute while maintaining a sound and tight counterparty exposure is key for being able to deliver Best Execution. The following paragraphs focus on selected practical aspects of how to ensure that our clients get the best possible results when trading with Bitcoin Suisse.

Liquidity. There are two types of liquidity most relevant to executing trades: market liquidity (how much can you trade at a given price x?) and funding liquidity, which is required by the trade venue to allow trading and settlement.

Market liquidity varies heavily depending on the token to be traded. Large trades, if not executed in a smart way, potentially cause material price changes. A diversified network of crypto trading venues (exchanges, brokers) does not only help increase the available liquidity on which can be traded but also allows to trade tokens that are not extensively listed across crypto markets. The most liquid order book does not help if there are no funds available on the account to trade with. Managing funding liquidity is a key feature of our Best Execution approach. But how much should one hold on to a single trading venue anyway?

Trading Venue. To select a trade venue and determine a prudent counterparty risk limit for it, Bitcoin Suisse applies its proprietary counterparty risk methodology. In simple terms, that means qualitative and quantitative factors are assessed and added up and the result is being assigned to a risk tier.

All our trading venues must fulfill certain minimum criteria to be onboarded as eligible trading counterparty. Since we are taking over the counterparty risk for our clients, we put our own capital at risk to protect our customers. Our various order types allow Best Execution trading for customers considering their preferences on how to execute. A principal order is a trade versus Bitcoin Suisse's own books. At the time of the trade, we scan available liquidity across the different order books from our trade venues and compile the best bid/ask price for the asset in the form of a snapshot. If the customer

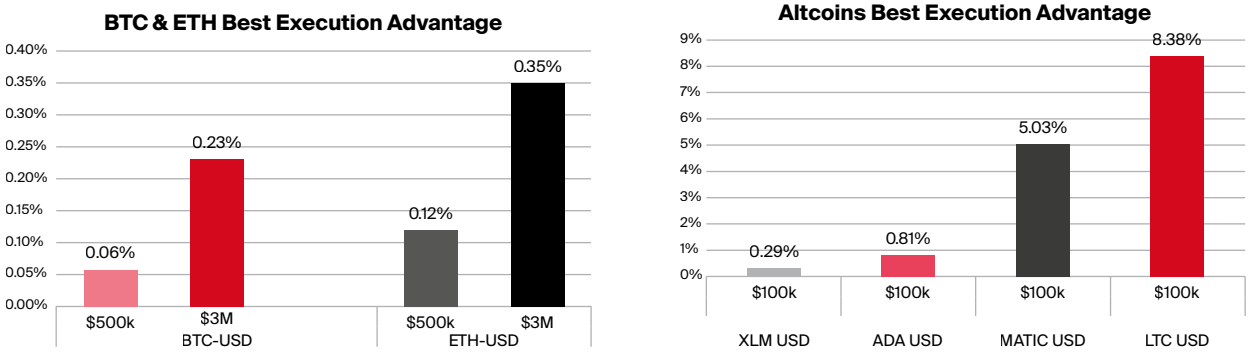


Illustration 1: Multi-exchange trading vs. single market execution.
Data: CoinRoutes, 20 random snapshots, December 2022. Chart: Bitcoin Suisse Trading Desk

decides to trade, the compiled price is locked in, and the trade is instantly settled. This form of order is best suited for immediate trades as execution is instant. The client has funds available in the account directly after trading, as Bitcoin Suisse is taking care of pre-funding and consequent hedging of the trade at its own risk.

For larger trades with lower time constraint, agency orders are normally the preferred choice. Under our agency model, we still protect the customer against counterparty risks and are able to execute the order in a way that minimizes market impact, hence achieving a better price on the order at the expense of longer execution time. Upon completion of the desired order amount, our clients get the actual traded price – which is most often better than a direct market order.

Best Execution Outlook 2023

Best Execution is an integral part of the TradFi sector. With MiFID in the European Union and FinSA in Switzerland, a lot has been done on the regulatory side to protect customers the best way possible. We strive to make this happen in the crypto space, too. If we want our markets to be competitive with traditional financial markets, we need to apply comparable standards, offer comparable client protection, and serve our customers with a high level of quality and security. Therefore, we are looking into upgrading our current Best Execution Policy to a standard comparable to MiFID/FinSA in 2023. With this step we mark our commitment towards meaningful regulation of crypto markets which profits all; the clients, the crypto space and all its participants.

Conclusion

The regulatory developments described signal that there is a clear desire to provide legal clarity. However, regulation of crypto markets is still at an early stage and there has been a lack of consistent regulation in this rapidly evolving sector across different countries, with some implementing outright bans and others adopting more supportive measures. Highly heterogeneous international regulatory requirements and uncertainties regarding the evolution of regulation can make it difficult to operate a crypto financial services provider. In addition, crypto markets are currently going through turbulent times.

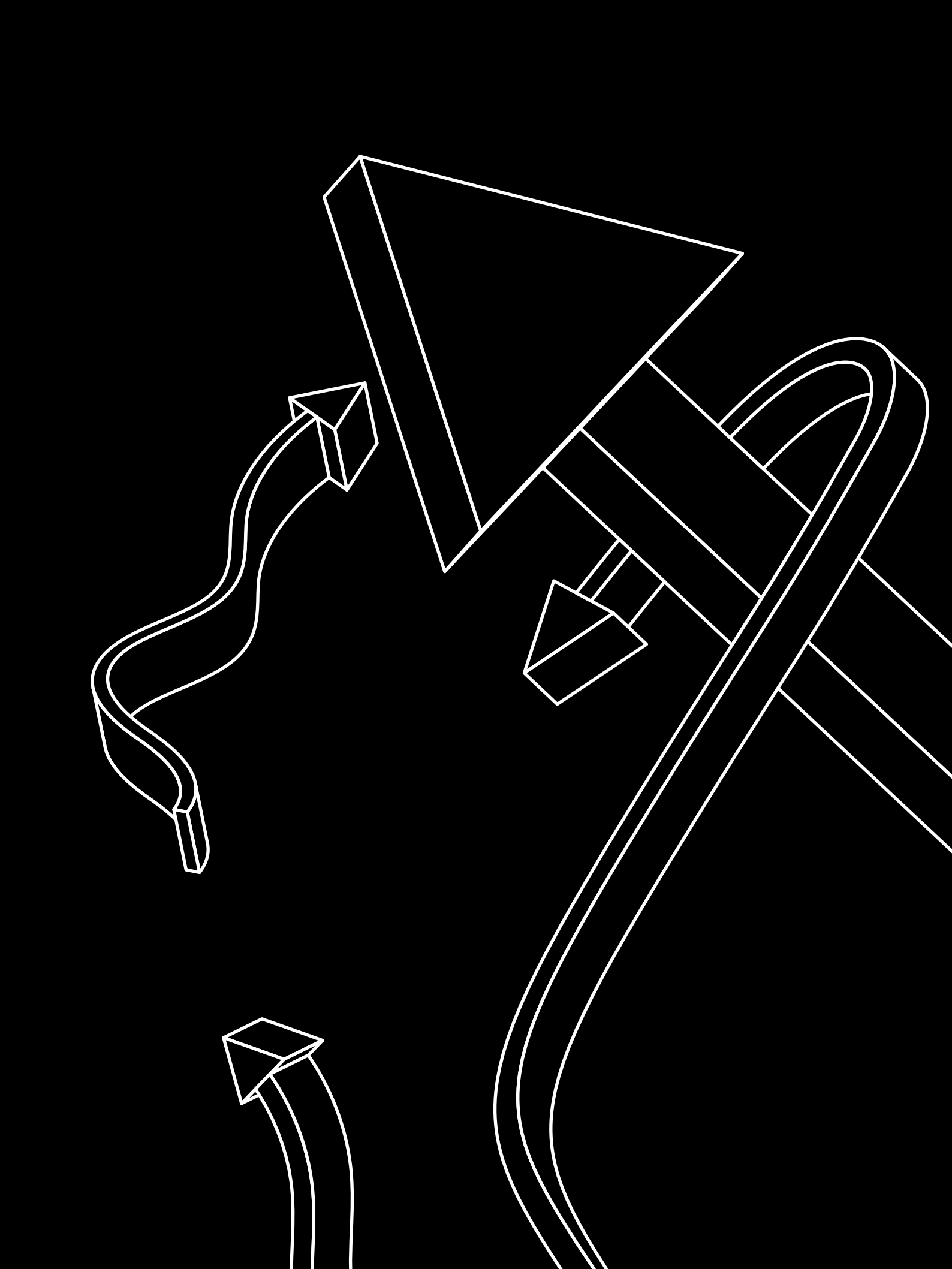
"Crypto markets are going through very similar if not the same events as TradFi, however with a speed factor of 10x. It is key to review the lessons learned from TradFi and apply the good parts for crypto, too."

– Lothar Cerjak, Chief Trading & Brokerage Officer

To promote the growth of the crypto industry, it is important to implement globally harmonized regulations and regulatory frameworks to be proportionate and technology neutral, considering the risks and benefits of crypto assets, and applying similar regulations to activities with similar risks as traditional financial activities. Switzerland has taken a neutral stance towards crypto assets and has implemented clear regulations for blockchain technology and the domestic taxation of cryptocurrencies, which has made it a hub for the industry.

At Bitcoin Suisse, we see our role not only in adhering to existing rules, but also in pioneering regulation and helping the industry to find standards that enhance customer protection and mature the crypto market. We believe that prudent and sensible regulation is paramount to the sustainable growth of crypto.

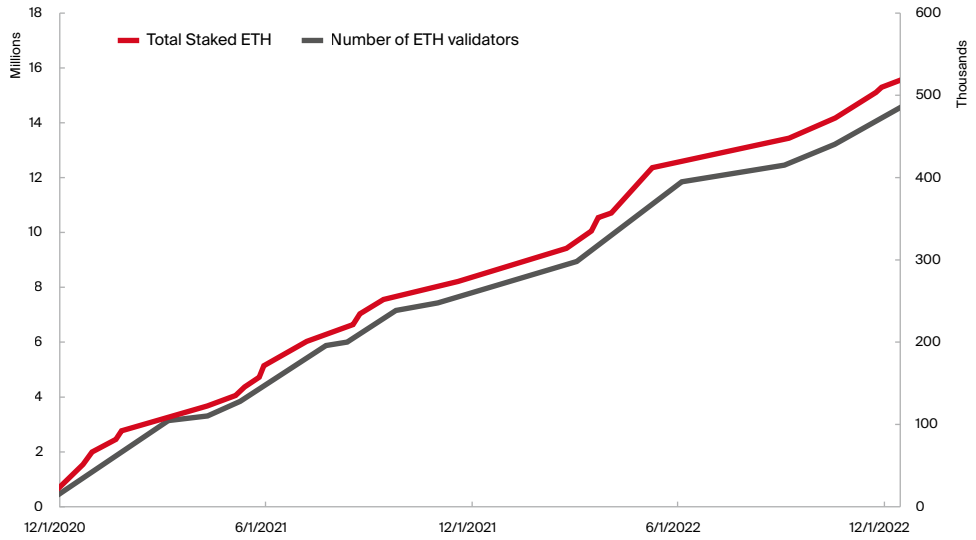
The authors would like to thank Julien Binder, Markus Perdrizat and Ronnie Studer for their contribution to the research and writing of this article.



Vires in Numeris

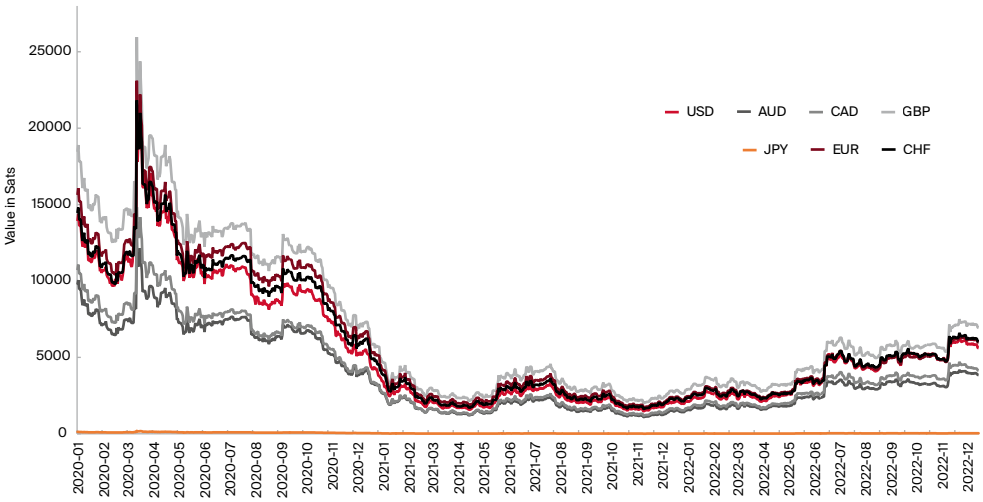
Together with Sander Jorgensen and Marlon Turgay from the Bitcoin Suisse Trading Desk, the Research team created a selection of charts that we hope you find as thought-provoking as we did for 2023 and beyond.

Proof of Success – Growth in staked ETH and Ethereum validators



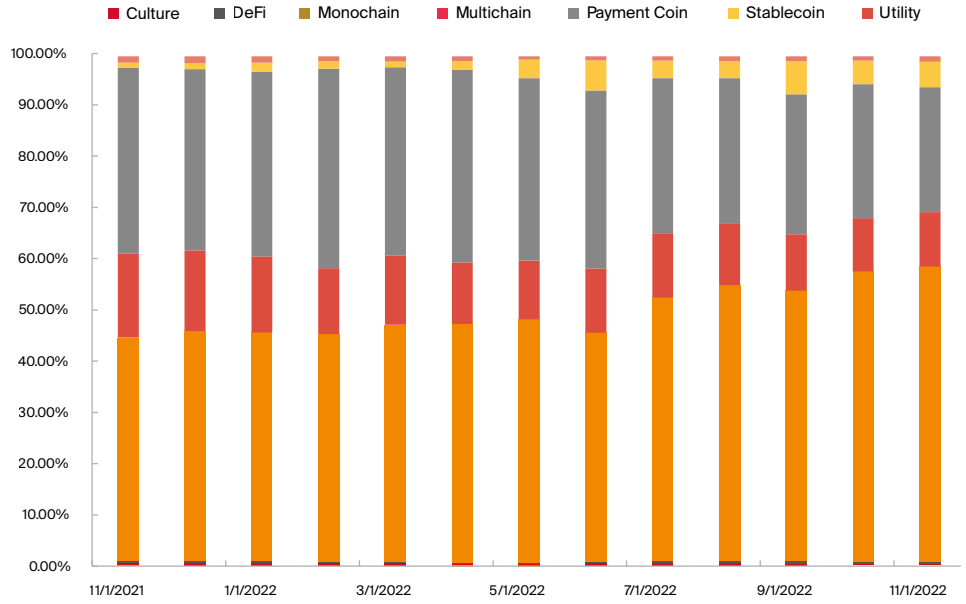
Ethereum's switch to Proof-of-Stake went without a glitch in 2022 and cemented its role as the premier smart contract chain. Data: Dune, on-chain data

In Bitcoin we trust? Price of major fiat currencies measured



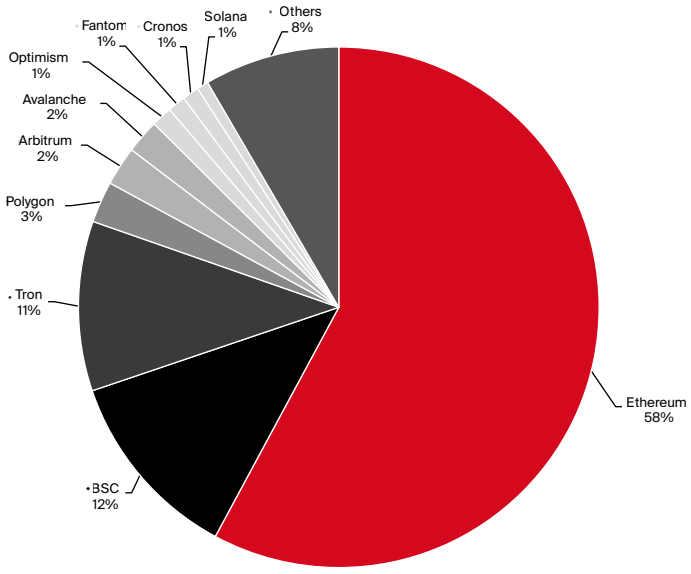
While the fall of Bitcoin in 2022 is clearly visible, it may be too early (again) to declare Bitcoin dead. Data: TradingView

Chains under custody. Which types of token did Bitcoin Suisse clients hold throughout 2022?



You can see some of the DeFi pain but also growth in the Monochain sectors. See the taxonomy page to learn more about the sector groups. Data: Bitcoin Suisse Custody

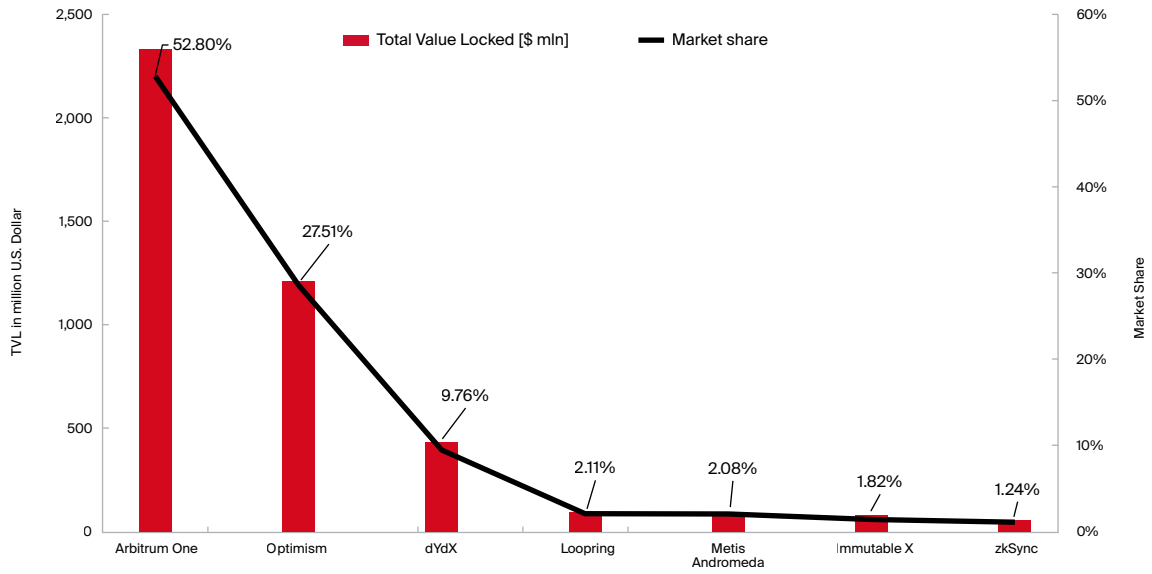
Ethereum and the ten dwarfs. How much total value do the smart contract chains lock?



Total TVL $41.63 bln

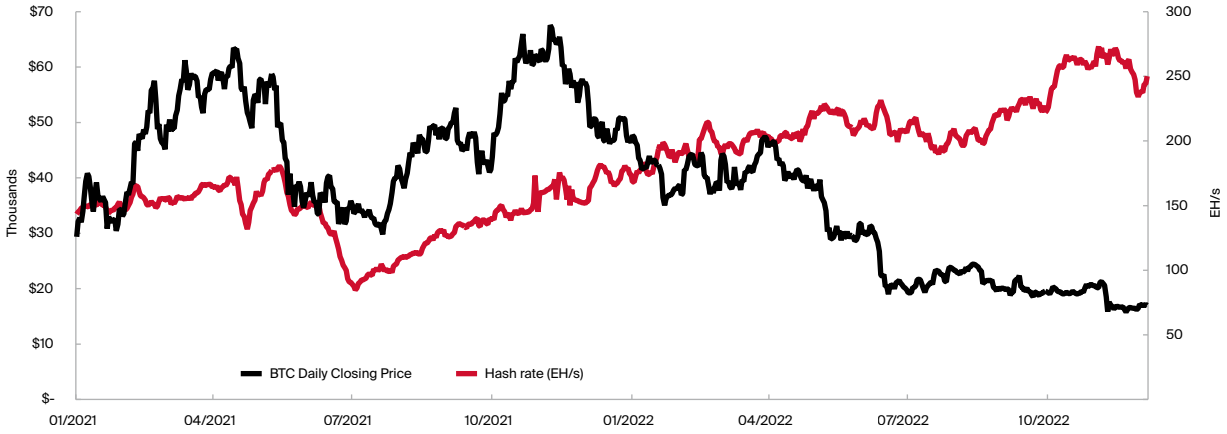
Ethereum has locked orders of magnitude more funds than all the rest combined Data: defillama

Ready, layer 2? Market shares and total value locked of leading L2 chains.



The market is clearly skewed towards the top two that mak up 80% of the market Data: L2Beat

Security at any cost. Bitcoin's hashrate keeps rising.

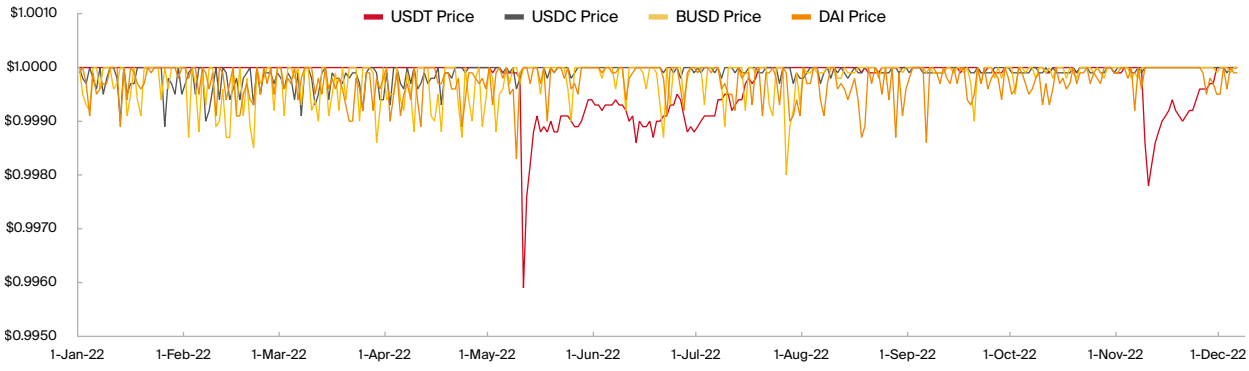


Despite the falling price, Bitcoin hashrate hit a series of new all-time highs in 2022 Data: Blockchain.com, Yahoo Finance

The soundness of money. Gold versus Bitcoin.

The trend of gaining value against gold over time has not been reversed despite the market downfall in 2022. Data: TradingView

Stablecoin stability. How well did the top four protect their peg?



Not all stablecoins survived 2022 and although Tether was tested more than once, it is back on track as well. Data: Coingecko

Contributors

Prof. Dr Claudio J. Tessone

Professor Claudio J. Tessone heads the Blockchain & Distributed Ledger Technologies group at the University of Zurich (UZH). He is also co-founder and Chairman of the UZH Blockchain Center, a competence center hosting more than 20 professors across four faculties covering the most varied fields in the space. Coordinating research, education and networking, the Center has been ranked 1st in Europe for the second year (and 3rd worldwide) in 2022 by CoinDesk's ranking of Blockchain Universities. Prof. Tessone studies blockchains as a paradigm of socio-economic complexity: linking microscopic agent behavior, incentives, and interactions with their emergent properties. The main pillars of his research include consensus analysis and modelling, crypto economics, large-scale blockchain analytics and forensics, and design of token-based economies.

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 at ETH Zurich, Uni Berne, TU Munich, fotiss Munich) and teaching with side trips to the public and NGO sector. Marcus studied computer science and technology management at ETH Zurich and received his PhD in 2009.

René Pickhardt

René Pickhardt is an independent Lightning Network open-source developer and researcher. As a world leading expert for payment reliability René is particularly known for having discovered the optimal method of conducting Bitcoin payments over the Lightning Network - which are also being referred to as Pickhardt Payments. He also co-authored the book Mastering the Lightning Network and answered over 300 questions about this technology on bitcoin.stackexchange.com.

Dr. Dirk Klee

Dirk Klee has been Chief Executive Officer at Bitcoin Suisse AG since April 2022. Throughout his 25+ year career, Dirk has established himself as an experienced, innovative leader who is passionate about building and leading client-focused businesses. Prior to joining Bitcoin Suisse Dirk has been CEO Wealth Management with Barclays Bank UK, COO International Wealth Management at UBS and CEO at BlackRock Germany.

Niklas Nygaard

Niklas Nygaard first joined the ICO department of Bitcoin Suisse in February 2018 shortly whereafter he joined the Trading team. He has since an early age taken part in various political organizations which led him to increasingly advocate for decentralization. He grasped the Bitcoin whitepaper in late 2013 since which he has had a full focus on the crypto space and its developments.

Dominic Weibel

Dominic Weibel joined the Research department of Bitcoin Suisse AG in March 2022. Previously, he was a research fellow and PhD student at the Technical University of Kaiserslautern where he explored the ultrasonic fatigue behavior of carbon fiber reinforced polymer composites. The emergence of distributed ledger technologies and their potential impact on future societies made him change professions. He went down the rabbit hole starting in 2017.

Dr. iur. Cansu Burkhalter

Dr. iur. Cansu Burkhalter joined Bitcoin Suisse AG as the Head Tax Compliance and Cross Border in March 2022. She is mainly focusing on international tax and cryptocurrency regulations. Prior to this position, Cansu held various compliance roles at Swiss banks, including leading the Client Tax Compliance team at Credit Suisse. She is a qualified attorney and holds a PhD in law from the University of Zurich.

Dr. iur. Fabio Andreotti

Fabio Andreotti joined the Legal Team of Bitcoin Suisse AG in December 2021 and has been Co-Head Legal since October 2022. He studied and received his PhD in law from the University of Zurich. His main focus is on regulation of financial markets, cryptocurrency and blockchain technology as well as network governance.

Oliver Gehring

After working over a decade in traditional finance Trading in Zurich and London, Oliver Gehrig joined Bitcoin Suisse AG in January 2022 as Head of Business Management for the Trading & Brokerage Division. He studied Business Administration with a focus on Banking & Finance at ZHAW in Winterthur and at the University of Zurich.

Thea Niederer

Thea Niederer joined Bitcoin Suisse AG in September 2021 and has since taken the position of Senior Marketing Manager. She holds a Bachelors in Communications from the University of Lucerne and a Master's degree from Queen Mary University of London in Marketing. She has experience in B2B marketing and digital media and a passion for new technologies and innovations.

Sander Jorgensen

Sander Jorgensen joined Bitcoin Suisse in March 2018 as an Account Manager in the ICO department and is currently a Senior Trader in the Trading team. He graduated from The Higher Commercial Program (HHX) in mid-2017, specialized in business and international economics. Prior joining Bitcoin Suisse he worked as a OTC trader and has been active in the crypto space since 2016.

Gian Stäuble

Gian Stäuble joined Bitcoin Suisse AG in June 2019 and has since taken the position of Head of Marketing. He holds a Degree in Digital Business Management and before joining Bitcoin Suisse has gained experience in digital marketing and advertisement. He is passionate about crypto, tech and marketing.

Denis Oevermann

Denis Oevermann is an Investment Analyst and Crypto Researcher at Bitcoin Suisse since 2022. He has more than 5 years of experience in crypto, with prior publications on crypto asset valuation and quantitative DeFi valuations. He has a background in Economics and Finance, holding a Master of Finance degree in Asset Management and Quantitative Finance from the University of Amsterdam.

Nick White

Nick White is COO of Celestia Labs. Celestia is the first modular blockchain protocol and aims to make decentralized apps more scalable, flexible and sovereign. Nick previously co-founded Harmony, a high-performance blockchain, and holds bachelor's and master's degrees in electrical engineering from Stanford University.

Marlon Turgay

Marlon Turgay has been with Bitcoin Suisse since 2017, witnessing the development of decentralized finance in all market conditions since. Marlon is a Senior Trader at Bitcoin Suisse and is currently obtaining a Bachelor's degree in Banking & Finance from the University of Zurich.

References

01. https://www.tradingview.com/symbols/ECONOMICS-EUM2/

02. Peter Zeihan, Keynote ECC 2022, https://www.youtube.com/watch?v=UA-jOLF2T4c

03. https://www.bruegel.org/blog-post/will-european-union-price-cap-russian-oil-work

04. Zoltan Pozsar, https://www.credit-suisse.com/about-us-news/en/articles/news-and-expertise/we-are-witnessing-the-birth-of-a-new-world-monetary-order-202203.html

05. https://www.nytimes.com/2014/12/21/upshot/of-kiwis-and-currencies-how-a-2-inflation-target-became-global-economic-gospel.html

06. https://www.kearney.com/financial-services/article/-/insights/the-walking-debt

07. https://www.investopedia.com/terms/s/sovereign-debt.asp

08. https://www.bridgewater.com/big-debt-crises/principles-for-navigating-big-debt-crises-by-ray-dalio.pdf

09. https://fiscaldata.treasury.gov/datasets/debt-to-the-penny/debt-to-the-penny

10. https://www.govinfo.gov/content/pkg/BUDGET-2022-BUD/pdf/BUDGET-2022-BUD.pdf

11. https://www.pgpf.org/blog/2022/06/what-is-the-national-debt-costing-us

12. https://en.wikipedia.org/wiki/2007%E2%80%932008_financial_crisis

13. https://en.wikipedia.org/wiki/COVID-19_recession

14. https://fred.stlouisfed.org/series/DFEDTARU

15. In fact, just before Christmas, the US President signed the 2023 record defense budget of $817B. Source: https://www.defense.gov/News/News-Stories/Article/Article/3252968/biden-signs-national-defense-authorization-act-into-law/

16. https://www.gold.org/goldhub/research/gold-demand-trends/gold-demand-trends-q3-2022/central-banks

17. https://economictimes.indiatimes.com/news/economy/policy/brics-explores-creating-new-reserve-currency/articleshow/94628034.cms

18. https://www.arabnews.com/node/2127586

19. We dedicated two Decrypts to this topic: https://www.bitcoinsuisse.com/research/decrypt/season-2022/bitcoin-pristine-collateral-and-reserve-asset-part-i and https://www.bitcoinsuisse.com/research/decrypt/season-2022/bitcoin-pristine-collateral-and-reserve-asset-part-ii

20. To learn more: https://en.wikipedia.org/wiki/Bitcoin_Law

21. https://www.atlanticcouncil.org/cbdctracker/

22. https://www.scmp.com/tech/policy/article/3195744/china-digital-currency-transactions-total-100-billion-yuan-end-august

23. https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews220916.en.html

24. https://www.bitkom.org/EN/Digital-Euro-Summit/

25. https://www.nfcw.com/2022/12/08/380838/central-bank-of-nigeria-limits-cash-withdrawals-to-drive-cbdc-and-digital-payments-adoption/

26. https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Technical-Evaluation-US-CBDC-System.pdf

27. https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Policy-Objectives-US-CBDC-System.pdf

28. Profile of USA on https://www.atlanticcouncil.org/cbdctracker/

29. These policy goals are consistent with the G7 public policy principles for retail CBDC published in October 2021: https://www.gov.uk/government/publications/g7-public-policy-principles-for-retail-central-bank-digital-currencies-and-g7-finance-ministers-and-central-bank-governors-statement-on-central-bank

30. Learn more from: https://en.wikipedia.org/wiki/Helicopter_money

31. https://www.bitcoinsuisse.com/research/theme/privacy-in-the-era-of-cryptocurrencies

32. https://link.springer.com/chapter/ 10.1007/978-3-030-71400-0_1

33. Further reading: https://www.btcpolicy.org/articles/why-the-u-s-should-reject-central-bank-digital-currencies

34. https://www.bertelsmann-stiftung.de/fileadmin/files/aam/Asia-Book_A_03_China_Social_Credit_System.pdf

35. https://www.bitcoinsuisse.com/research/decrypt/season-2022/un-stablecoins

36. https://cointelegraph.com/news/global-inflation-mounts-how-stablecoins-are-helping-protect-savings

37. https://www.rba.gov.au/publications/bulletin/2022/dec/stablecoins-market-developments-risks-and-regulation.html

38. https://99bitcoins.com/bitcoin-obituaries/, performance figures from TradingView.com

39. https://www.ecb.europa.eu/press/blog/date/2022/html/ecb.blog-221130~5301eecd19.en.html

40. https://www.tradingview.com/chart/JvEkI6g5/

41. https://newsbtc.com/news/bitcoin/glassnode-bitcoin-long-term-holder-conviction-not-lost/

42. https://www.investopedia.com/terms/b/balancedfund.asp

43. https://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/histretSP.html

44. https://youtu.be/uB-MUGChTp4w?t=604 (5 mins)

45. https://en.wikipedia.org/wiki/Executive_Order_6102

46. https://en.wikipedia.org/wiki/War_economy#World_War_II

47. https://link.springer.com/chapter/ 10.1007/978-3-030-71400-0_1

48. https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/#top-20

49. https://en.wikipedia.org/wiki/Currency_substitution

50. https://en.wikipedia.org/wiki/CFA_franc

51. https://machankura.com/. A short documentary highlights this and other Bitcoin projects across Africa: https://www.youtube.com/watch?v=d5AvBsxRMYk

52. https://nayibtracker.com/

53. https://miprimerbitcoin.medium.com/un-a%C3%B1o-increíble-logros-de-mi-primer-bitcoin-en-2022-55d9395ecab8

54. https://bitcoinmagazine.com/markets/el-salvador-president-nayib-bukele-announces-countries-to-discuss-bitcoin

55. https://bitcoinmagazine.com/legal/brazil-enacts-bitcoin-payments-bill

56. https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/#top-20

57. http://med.a51.nl/sites/default/files/pdf/Cryptocurrency_in_Central_Bank_Reserves.pdf

58. https://www.bbc.com/news/business-60521822, https://finance.yahoo.com/news/g-7-frozen-russia-assets-222049235.html, https://www.aljazeera.com/news/2022/3/25/gold-russia-ukraine-war.

59. https://www.btcpolicy.org/research-categories/mining-energy

60. The military-industrial complex is, among other purposes, required to maintain the fiat currency system. Source: https://link.springer.com/chapter/ 10.1007/978-3-030-71400-0_1

61. Source of comparisons: https://bitcoinminingcouncil.com/wp-content/uploads/2022/01/2022.01.18-BMC-Q4-2021.pdf. Factors are calculated lower and upper bounds of 100-200 TWh/year energy use for Bitcoin. See chart „Total Bitcoin electricity consumption at: https://ccaf.io/cbeci/index

62. Galaxy Mining report, archived at https://www.lopp.net/pdf/On_Bitcoin_Energy_Consumption.pdf

63. https://www.iea.org/news/renewable-power-s-growth-is-being-turbocharged-as-countries-seek-to-strengthen-energy-security

64. Galaxy Mining report, archived at https://www.lopp.net/pdf/On_Bitcoin_Energy_Consumption.pdf

65. https://www.iea.org/reports/hydropower-special-market-report

66. Example: https://www.coindesk.com/layer2/miningweek/2022/03/25/how-northern-italian-hydropower-producers-became-bitcoin-miners/

67. https://www.irena.org/news/pressreleases/2021/Jun/Majority-of-New-Renewables-Undercut-Cheapest-Fossil-Fuel-on-Cost

68. Several critical reports about ESG appeared in 2022: https://hbr.org/2022/03/an-inconvenient-truth-about-esg-investing, https://www.wsj.com/articles/esg-loser-funds-costs-basis-points-blackrock-500-environment-green-sec-11657461127, https://www.economist.com/weeklyedition/2022-07-23, and https://www.wsj.com/articles/esg-cant-square-with-fiduciary-duty-blackrock-vanguard-state-stree-the-big-three-violations-china-conflict-of-interest-investors-11662496552.

69. https://bitcointreasuries.net/

70. https://cointelegraph.com/news/microstrategy-to-offer-bitcoin-lightning-solutions-in-2023

71. Slogan of the Order of the Garter https://en.wikipedia.org/wiki/Order_of_the_Garter. English: “May he be shamed who thinks evil of it.” German: «Ein Schelm wer Böses dabei denkt.»

72. https://www.bloomberg.com/news/articles/2022-08-10/jpmorgan-precious-metals-traders-found-guilty-in-spoofing-trial

73. https://en.wikipedia.org/wiki/Dodd%E2%80%93Frank_Wall_Street_Reform_and_Consumer_Protection_Act

74. https://www.forbes.com/sites/greatspeculations/2019/05/20/yes-gold-is-being-manipulated-but-to-what-extent/, also https://www.fool.com/investing/general/2011/09/13/is-gold-being-suppressed.aspx

75. https://gata.org/about

76. https://wikileaks.org/plusd/cables/1974LONDON16154_b.html

77. https://www.usmoneyreserve.com/news/executive-insights/paper-gold/

78. https://europhoenix.com/blog/an-upcoming-paper-gold-crisis-by-les-nemethy-and-alberto-scalabrini/

79. https://lookingglasseducation.com/what-the-us-government-doesnt-want-you-to-know/

80. https://bitcoinmagazine.com/markets/bitcoin-futu-

res-market-explained-price-manipulation

81. https://news.bitcoin.com/more-than-19-billion-in-btc-eth-stablecoins-left-exchanges-since-the-onset-of-ftxs-collapse/

82. Alex Gladstein, Check your Financial Privilege, BTC Media LLC, 2022.

83. https://www.coindesk.com/tech/2021/11/13/taproot-bitcoins-long-anticipated-upgrade-activates-this-weekend/

84. https://lightning.engineering/posts/2022-4-5-taro-launch/

85. https://www.rgbfaq.com/what-is-rgb

86. https://www.bloomberg.com/news/articles/2022-02-07/kpmg-canada-adds-bitcoin-ethereum-to-corporate-balance-sheet

87. https://edition.cnn.com/2022/04/26/success/fidelity-bitcoin-401k/index.html

88. https://decrypt.co/96313/microstrategy-takes-out-205m-bitcoin-backed-loan-buy-more-bitcoin

89. https://www.bloomberg.com/news/articles/2022-04-28/goldman-offers-its-first-bitcoin-backed-loan-in-crypto-push

90. https://www.nasdaq.com/articles/majority-of-financial-advisors-want-to-increase-bitcoin-exposure%3A-nasdaq-survey

91. https://bitcoinmagazine.com/business/goldman-sachs-partners-with-coinbase-for-banks-first-bitcoin-backed-loan

92. The open-source client software needed to run a Bitcoin Lightning node

93. A 2-of-2 multi-signature transaction requires two different private keys, usually two different entities, to perform a transaction. Such transactions are used to open (and close) payment channels on the Lightning network.

94. To learn more, visit https://blog.bitmex.com/price-of-anarchy-from-selfish-routing-strategies/

95. To read the Bitcoin White Paper, visit https://nakamotoinstitute.org/literature/bitcoin/

96. To learn more, visit https://en.wikipedia.org/wiki/Small-world_network https://en.wikipedia.org/wiki/Small-world_network

97. To learn more, visit https://en.wikipedia.org/wiki/Price_of_anarchy

98. The minimum-cost flow problem is an optimization and decision problem to find the cheapest possible way of sending a certain amount of flow through a flow network. https://en.wikipedia.org/wiki/Minimum-cost_flow_problem

99. For the technically inclined: Yet, optimizing for fees is hard because if you have a base fee then the problem is known to be NP-complete because the fee function is not linear from 0 to 1. You have this jump of using the channel, so it is non-linear. Minimum-cost-flows are known to be NP-hard if they are non-linear.

100. The website www.mempool.space is a blockchain explorer tool for Bitcoin.

101. Chivo Wallet is provided by the government of EL Salvador. https://www.chivowallet.com/

102. Lightning Service Providers (LSP)" provide onboarding support for new users by offering stable network connections, channel management, liquidity, and other services.

103. René Pickhardt's website is https://www.rene-pickhardt.de/

104. Paper: https://arxiv.org/abs/2103.08576

105. Paper: https://arxiv.org/abs/2107.05322

106. Paper: https://github.com/renepickhardt/mpp-splitter/blob/pickhardt-payments-simulation-dev/ Simulation: https://github.com/renepickhardt/mpp-splitter/blob/pickhardt-payments-simulation-dev/

107. https://1ml.com/statistics

108. https://celsius.network/terms-of-use

109. https://celsiusnetwork.medium.com/a-memo-to-the-celsius-community-59532a06ecc6

110. https://www.reuters.com/technology/crypto-lender-celsius-files-bankruptcy-2022-07-14/

111. https://cointelegraph.com/news/celsius-ceo-plans-to-restructure-firm-to-focus-on-crypto-custody-report

112. https://www.bitcoinsuisse.com/research/decrypt/season-2022/defi-dominoes

113. https://www.cnbc.com/2022/06/29/crypto-hedge-fund-three-arrows-capital-plunges-into-liquidation.html

114. https://beincrypto.com/three-arrows-founders-suzhu-and-kyle-davies-pull-a-do-kwon/

115. https://www.cnbc.com/2022/11/25/binance-others-line-up-bids-for-bankrupt-voyager-after-ftx-collapse.html#:~:text=Digital%20currency%20lender%20Voyager%20Digital,revised%20bids%20for%20the%20company.

116. https://www.reuters.com/technology/crypto-lender-blockfi-files-bankruptcy-protection-2022-11-28/

117. https://bitcoinsuisse.com/industry-blog/the-weekly-wrap-25-november-2022

118. https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/?out-

putType=amp&utm_campaign=Research%20newsletter&utm_source=hs_email&utm_medium=email&utm_content=65750014&_hsenc=p2ANqtz-9DK1eWUJb67HQg11zotZmXSZRbQTLIOfrSf_lgJ3AZZLwGQ7QY7G8gDLwP9wXaJuaLSfM_B6M4xHm6vAtkVV5kmTmhBWyD1bM5rFbA3l8hqOUbg1M

119. https://www.wsj.com/articles/ftx-tapped-into-customer-accounts-to-fund-risky-bets-setting-up-its-downfall-11668093732?reflink=share_mobilewebshare

120. https://decrypt.co/114105/coinshares-confirms-30-3-million-exposure-ftx

121. https://arxiv.org/abs/1710.09437

122. https://www.galaxy.com/research/insights/tags/ethereum

123. https://arxiv.org/pdf/2003.03052.pdf

124. https://whitepaper.io/document/139/peercoin-whitepaper

125. https://kb.beaconcha.in/glossary

126. https://vitalik.ca/general/2020/11/06/pos2020.html

127. https://www.theblock.co/post/197861/bitcoin-mining-hashrate-declines-more-than-30-amid-americas-big-winter-storm

128. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/weak-subjectivity/

129. https://carbon-ratings.com/dl/eth-report-2022

130. https://twitter.com/WuBlockchain/status/1552837630278385664

131. https://charts.coinmetrics.io/network-data/

132. https://2miners.com/ethw-network-hashrate#:~:text=Ethereum%20PoW%20network%20hashrate%20reflects,505%20813%20633%20h%2Fs

133. https://twitter.com/VitalikButerin/status/1570299062800510976?s=20&t=a-zD5hbswn_xSXgY-Yksvzg

134. https://public.wmo.int/en/media/press-release/eight-warmest-years-record-witness-upsurge-climate-change-impacts

135. https://ethereum.org/en/desci/

136. https://eth2book.info/altair/part2/incentives/issuance

137. https://www.theblock.co/data/on-chain-metrics/ethereum/cumulative-value-of-burned-eth-after-eip-1559

138. https://coinshares.com/research/ethereum-staking-yields

139. https://eth2book.info/altair/part2/incentives/rewards

140. https://messari.io/asset/ethereum/chart/txn-fee-avg

141. https://www.wsj.com/articles/ethers-new-staking-model-could-draw-sec-attention-11663266224

142. https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220808

143. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/attestations/

144. https://twitter.com/etherEumJoseph/status/1596198718339948552?s=20&t=deigZW4AUrFsowqTXPQJig

145. https://beaconcha.in/

146. https://operators.lido.fi/

147. https://clientdiversity.org/

148. https://www.rated.network/?network=mainnet&view=pool

149. https://ethresear.ch/t/burning-mev-through-block-proposer-auctions/14029

150. https://members.delphidigital.io/reports/the-hitchhikers-guide-to-ethereum/

151. https://twitter.com/peter_szilagyi/status/1563051603846115328?s=20&t=3Au0sH-Q9o98TpSKH2pWmdQ

152. https://obol.tech/

153. https://ssv.network/

154. https://explore.flashbots.net/

155. https://www.mevboost.org/

156. https://twitter.com/VitalikButerin/status/1588669782471368704?s=20&t=7dNBkxuW7iP4k20_HDqEug

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

158. https://eips.ethereum.org/EIPS/eip-4337

159. https://l2beat.com/scaling/tvl/

160. https://l2beat.com/scaling/activity

161. https://ethtps.info/

162. https://defillama.com/chains

163. https://parachains.info/auctions

164. https://www.gokustats.xyz/developers

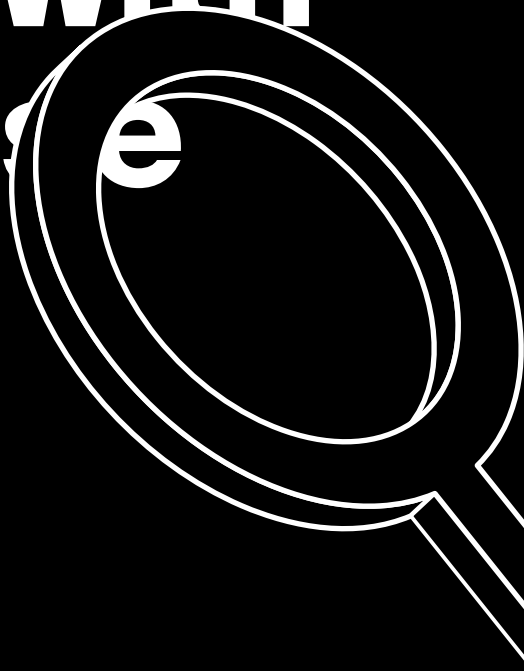
165. https://l2beat.com/scaling/risk

166. https://mobile.twitter.com/0xstacked

167. https://www.espressosys.com/blog/decentralizing-rollups-announcing-the-espresso-sequencer

168. https://messari.io/report/eigenlayer-to-stake-and-re-stake-again

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
our publications

Learn more about
Bitcoin Suisse Research

Bitcoin
Suisse

Bitcoin Suisse AG
CH-6300 Zug
bitcoinsuisse.com