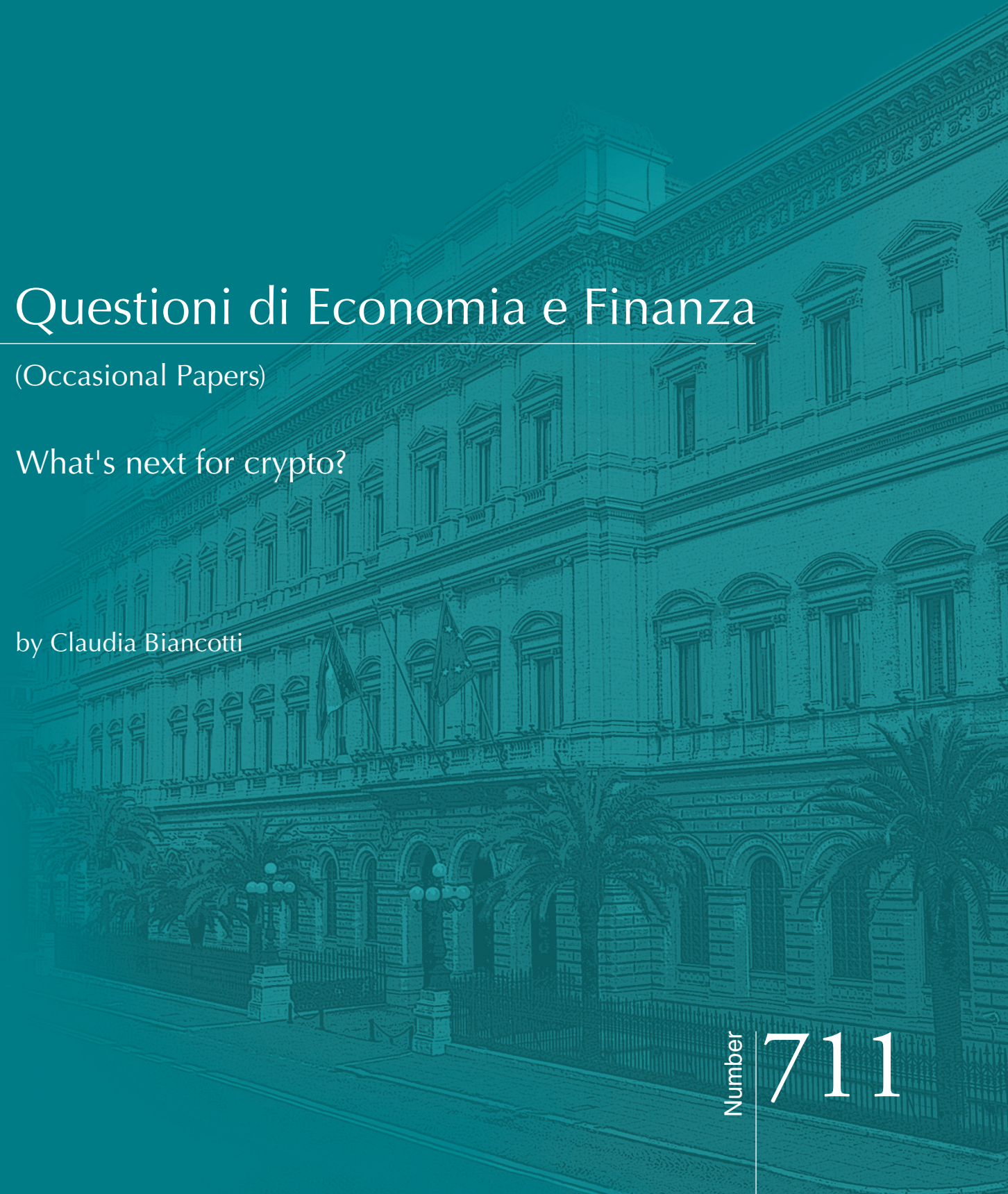
BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

What's next for crypto?

by Claudia Biancotti



September 2022

Number 711

BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

What's next for crypto?

by Claudia Biancotti

Number 711 – September 2022

The series Occasional Papers *presents studies and documents on issues pertaining to the institutional tasks of the Bank of Italy and the Eurosystem. The* Occasional Papers *appear alongside the* Working Papers *series which are specifically aimed at providing original contributions to economic research.*

The Occasional Papers *include studies conducted within the Bank of Italy, sometimes in cooperation with the Eurosystem or other institutions. The views expressed in the studies are those of the authors and do not involve the responsibility of the institutions to which they belong.*

The series is available online at www.bancaditalia.it .

ISSN 1972-6627 (print)
ISSN 1972-6643 (online)

Printed by the Printing and Publishing Division of the Bank of Italy

WHAT'S NEXT FOR CRYPTO?

by Claudia Biancotti*

Abstract

The crypto world is at a turning point. In the spring of 2022, idiosyncratic weaknesses and adverse macro conditions combined to precipitate a major crisis. Is this the end of crypto? Not necessarily. As bad projects fall by the wayside, the industry is being pushed to find technical solutions that will restore public trust and deliver better performances. At the same time, key jurisdictions around the world are deploying regulations that will make the sector more orderly. Innovation and legal certainty may be the twin foundations upon which crypto flourishes, provided that regulators and the industry cooperate constructively and creatively. This will not always be easy, as crypto culture and any legal framework are at odds in some domains. The main examples are: tokens that do not embed claims on any entity, anonymity, and censorship resistance, i.e. the technical impossibility of blocking transactions on permissionless blockchains. Achieving a compromise on many facets of these problems looks possible, while for others, the authorities may have to prohibit behaviour that some crypto enthusiasts consider to be non-negotiable.

JEL Classification: G18, O30, O38.
Keywords: crypto-assets, financial regulation, blockchain.
DOI: 10.32057/0.QEF.2022.0711

Contents

* Bank of Italy, Directorate General for Economics, Statistics and Research.

1. Introduction[1]

The world of cryptoassets faces a major turning point. In the Spring of 2022, adverse macroeconomic conditions and idiosyncratic weaknesses of the sector combined to trigger a systemic crisis. Total market capitalization of the roughly 8,000 active cryptoassets[2] went down from the $2.9 trillion of November 2021 to the $1.1 trillion of August 2022[3].

Amidst failed projects, forced liquidations of leveraged positions, and insolvencies, some observers were quick to announce the end of crypto. This prophecy was made many times before[4], without ever coming true. Is this finally the time?

In this paper, we argue that it does not need to be the case, despite the shortcomings of the industry. The crisis initiated the "great washout" that parts of the crypto community had been waiting and wishing for. A blinding light is now shining on fraudulent practices, risk mismanagement, and other long-standing, structural problems. Bad actors are exiting the market. Good ones have the opportunity to focus solely on building technology, without distractions from yield chasing.

The sector is also finally going to be regulated in a consistent way, at least in advanced economies. G7 jurisdictions are deploying new, comprehensive crypto statutes, some of which have been in the works for years. If authorities and the industry find a way to cooperate closely, so that regulations are not outpaced by technology or circumvented by players in bad faith, then the new rules will finalize the cleanup and restore trust.

---

[1] This paper draws on a long-standing interest in the crypto world. Between 2013 and 2017 I read white papers for many projects, followed industry publications and crypto forums, studied regulatory documents. Then I spent a few years working on other matters, until the subject came back to me almost all at once. To catch up, in the past eight months I listened to over 800 hours of the following podcasts: *Bankless*, hosted by Ryan Sean Adams and David Hoffman; *The Defiant*, hosted by Camila Russo; *Empire*, hosted by Jason Yanowitz and Santiago Santos; *The Breakdown*, hosted by Nathaniel Whittlemore; *Unchained*, hosted by Laura Shin; *Web3 with A16Z*, hosted by Sonal Chokshi; *Overpriced JPEGs*, hosted by Carly Reilly; The *Delphi Podcast*, hosted by Tommy Shaughnessy and Piers Kicks. I also occasionally listen to other general crypto podcasts and am starting to delve into more NFT ones, but the full list is too long to be reported here. Contrary to other crypto media, these podcasts focus not so much on market movements but rather on deeper technology, market design, governance, and social issues. On account of the vast number of episodes involved and the difficulty to track down each snippet of information amongst them – not to mention the fact that a lot of themes are discussed in different places – I will explicitly name sources of my reflections only occasionally, aside from cases where official publications are concerned, or when I am merely channeling a very good idea that is not mine. I am extremely grateful for comments on this work to Luigi Bellomarini, Marco Benedetti, Oscar Borgogno, Carolina Camassa, Paolo Ciocca, Riccardo Cristadoro, Massimo Doria, Giuseppe Ferrero, Giuseppe Galano, Sara Giammusso, Gabriele Marcelli, Sabina Marchetti, Matteo Nardelli, Goran Sarajlic, Michele Savini Zangrandi, Luigi Federico Signorini, Pietro Terna, Giovanni Veronese, and Silvia Vori. Any errors and omissions remain solely mine. This paper reflects my own opinions, which should not by any means be attributed to the Bank of Italy.

[2] Auer, R., M. Farag, U. Lewrick, L. Orazem, and M. Zoss (2022), "Banking in the shadow of Bitcoin? The institutional adoption of cryptocurrencies", Bank for International Settlements Working Paper 1013. More than 20,000 different cryptoassets were issued since Bitcoin first appeared, but many projects were abandoned along the way.

[3] https://coinmarketcap.com/, as of August 11, 2022.

[4] https://www.bitcoinisdead.org/

In this scenario, crypto will not die at all. On the contrary, it will have a chance to grow, perhaps fully achieving the goals envisioned by its advocates – enhanced cyber security across the digital world, effective protection of property rights, product and process innovation in finance and other sectors, rebalancing of power between providers and users of digital services with the so-called Web3 model, creation of opportunities for disadvantaged groups, and more[5]. Regulatory sandboxes and incubators, already available in many jurisdictions, could play a key role in helping the process along.

This best-case scenario, however, may not be so closely within reach. There are several potential roadblocks in the dialogue between regulators and the private sector. Assets traded in traditional financial markets represent claims on definite entities, and/or embed certain legal rights. This is not always the case on crypto trading platforms, which may create a problem of regulatory perimeter. A part of crypto's value proposition remains tied to systems that allow for participant anonymity while providing censorship resistance, i.e. the technical impossibility to block any transaction. Crypto developers generally prefer a higher degree of decentralization and automation to a lower one. Some even see the lack of rules in crypto financial markets as a gateway to financial inclusion and social mobility. These traits do not sit well with legal frameworks.

This paper is an attempt at facilitating the dialogue between regulators and the industry, by giving each party a somewhat in-depth overview of the other party's challenges. We are not offering solutions to the tough problems, but rather trying to reframe them in a way that contributes to a constructive discussion[6]. The paper also strives to provide a neutral overview of the space to any reader who is interested in approaching it but may have been confused by the ideological wars around the topic.

The paper is structured as follows. In Section 2, we offer a recap of how the narrative of the crypto world has changed compared to the early years, how the sector is now structured, and what its key products are. In Sections 3 and 4, we assume the industry's point of view, discussing the two main challenges it needs to face – mistrust on the part of many, and an ecosystem-wide version of the "blockchain trilemma", i.e. attainment of security, decentralization, and scalability at the same time.

[5] Discussing each of these goals, and how crypto technology may help them come about, is beyond the scope of this paper. Throughout this work, however, we assume that at least some of these objectives are achievable, to varying degrees.

[6] We will not go into a full recap of the many stages the industry went through in the past ten years – the introduction of smart contracts in 2014, the ICO craze of 2017, the "crypto winter" that followed, the DeFi summer of 2020. For a detailed account, the reader can refer to a few excellent books on the subject. See for example Russo, Camila (2022), The Infinite Machine, Harper Collins; Shin, Laura (2022), The Cryptopians: Idealism, Greed, Lies, and the Making of the First Big Cryptocurrency Craze, Public Affairs Book; CoinGecko (2021), How to Defi: Basic, and How to Defi: Advanced; Finn Brunton (2019) Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency, Princeton University Press.

Section 5 is written in a regulator's voice, not touching upon any single national statute, but rather outlining in a general way the idiosyncratic difficulties that exist in regulating crypto. It mostly refers to the financial component of the ecosystem. Section 6 provides our conclusions.

Note that this paper only focuses on permissionless blockchains. It does not address private permissioned blockchains, or technologies related to central bank digital currencies (CBDCs).

2. The crypto industry today

The crypto industry today has become way less strident than it used to be. Created in the wake of the great financial crisis as an alternative to traditional money, cryptoassets originally had a distinct revolutionary tinge. Early adopters touted them as an invention that would disrupt the monetary and financial systems, substituting corruptible humans with transparent, trustworthy algorithms. Those were the years of "Decentralize all the things" memes[7], and an all-or-nothing attitude was the norm.

Over the years, this has changed significantly, including at the very core of the ecosystem. In a February 2022 interview to *The Defiant*, a podcast, Ethereum co-founder and crypto icon Vitalik Buterin elaborated at length on how decentralization is desirable in many human endeavours because it can lead to more stability, certainty, security, and equality. Those are hardly the divisive values of the beginning. While Buterin never was one for confrontational tones, his attitude now appears to be shared by many other entrepreneurs in the sector.

But what activities do actually exist within the sector itself? Tracing a taxonomy of the crypto industry is notoriously difficult, because the underlying technology is modular, and the basic building blocks can be combined in ways that do not quite fit any standard grid. Before attempting to provide some order, two key elements must be kept in mind.

One, everything in this ecosystem is construed as a transaction, including activities that are not financial in nature. In this context, a transaction is understood a change in the state of the world. Sometimes this involves monetary value, e.g. the exchange of bitcoin against ether. Sometimes it does not, e.g. a player of a decentralized videogame changing the color of their avatar. The two dimensions can mix in the same environment – the same player can receive token rewards when they level up. Blockchains serve the purpose of keeping track of all status changes in a secure way, and they are agnostic with respect to the monetary value of transactions. That is determined by markets.

Two, many industry players are active in more than one sub-sector, especially where financial endeavors are involved. In particular, it is important to note that some companies provide settlement infrastructure and complex financial services at the same time.

[7] See https://ericsammons.com/wp-content/uploads/2015/10/decentralize.jpg

This said, the categories of players in the industry can be typified as follows, with some approximation[8] and keeping in mind that overlaps are common[9]:

(a) providers of infrastructure: organizations designing and developing blockchains, or the rails where transactions happen;

(b) validators: organizations or individuals who make a blockchain secure by validating transactions according to a given consensus mechanism. The most used mechanisms at the time of writing are proof-of-work and proof-of-stake (see Section 3);

(c) providers of hardware: organizations producing physical items that are used for the purpose of making the crypto ecosystem work, e.g. computers that are fit for transaction validation, or specialized devices for the secure storing of assets;

(d) providers of financial services: organizations that offer to individuals and other organizations services such as custody of cryptoassets, exchange between cryptoassets and fiat money or other cryptoassets, lending, borrowing, and investing in cryptoassets, payments in cryptoassets[10], and a number of other financial operations;

(e) providers of on-chain services for the management of intellectual property rights (outside of the financial sector): organizations that leverage blockchains to notarize ownership of intellectual property rights and disintermediate their exploitation, allowing owners to directly set usage rules and capture revenue streams. The best-known example is that of NFTs, a special type of token that saw a late-2021 boom in the digital arts[11];

(f) providers of gaming services: at the beginning those were mostly gambling outfits, but now this is no longer the case, as more and more traditional videogames appear in the blockchain space[12];

(g) providers of other on-chain services: organizations leveraging the blockchain's secure notarization capabilities to offer a variety of other services, from credential verification to identity management[13];

[8] This is only a snapshot of the ecosystem as it is now, and e.g. categories related to service provision could diversify significantly in the future.

[9] Note that this is only one of many possible taxonomies. A well-known one is provided by blockchain forensics firm Chainalysis in their 2021 Key Players of the Cryptocurrency Ecosystem report. Our categorization draws on it for some items.

[10] In the early years one of the hottest themes was the possible adoption of Bitcoin and other tokens as a means of payment in the brick-and-mortar world. At the moment, this is not a significant phenomenon. Indeed cryptoassets are often used for payments, but those are almost always taking place within the crypto ecosystem itself, financial services in the lead. This scenario may change with technological progress, and if regulation allows.

[11] According to some, this sub-sector may eventually expand to cater for the management of physical property rights.

[12] Although the relationship between the crypto and the gaming communities is somewhat difficult at the moment, gambling has been singled out as one of the application that may facilitate the entry of crypto in the mainstream.

[13] This latter application has vast potential but, so far, results in the crypto space have been limited.

(h) providers of merchant services: organizations that act as intermediaries between a customer and merchants to enable payment in crypto.

Two other key components of the industry are perhaps best left out of the list, because they cut across all of it.

The first is the issuance of tokens. In the crypto world, nearly everyone issues tokens. First of all, blockchains have their own native asset or "coin", which is the token enabling transactions on that chain. Those coins are also what validators post in proof-of-stake systems to contribute to the security of the chain. In videogames, players receive tokens as a reward for their performance, or as representations of characters and in-game assets that then become tradable. NFTs can be used to ensure fair distribution of royalties on a record or movie, but they can also be sold as pure collectibles. An increasing number of crypto organizations, both in the financial and non-financial sectors, issues governance tokens to certain users, which entitle holders to vote on how the organization should be run (see Section 3.3.1).

The second cross-cutting dimension is the degree of decentralization, much discussed by both industry insiders and external observers[14]. Making use of a blockchain, even a permissionless one where anyone can become a validator node and/or post transactions, does not imply that an outfit is decentralized in the full sense, i.e. devoid of a single person or entity that oversees its functioning and can be a so-called single point of failure. For example, in the crypto financial sector there are several centralized service providers. They use their own servers to offer custodial services to users and provide access to trading, they set the interest rate for deposits and loans, and so on. At the other extreme, there are decentralized finance (DeFi) services where developers launch a protocol, say for the minting of a stablecoin against crypto collateral, and then take a step back leaving the governance of the protocol to a decentralized autonomous organization (DAO; see Section 3.3.1) – a collective of users that have earned or bought governance tokens over time. There are no custodial services to speak of, only self-hosted wallets controlled exclusively by the user.

Most crypto outfits fall somewhere in between.

Box I - A few key numbers

- The European Central Bank (ECB), based on a 2022 survey of six large euro area countries, estimates that as many as 10 per cent of households in those countries may

[14] See for example: Aramonte, S., W. Huang, A. Schrimpf (2021), DeFi Risks and the Decentralization Illusion, BIS Quarterly Review.

own cryptoassets[15]. Small holdings are prevalent and the ownership pattern by income quintile is u-shaped, with high- and low-income households both showing more interest in crypto compared to the middle classes.

- A recent survey by Pew Research puts the share of US citizens over 18 who ever invested, traded in or used crypto at 16 per cent[16], with a peak of 23 per cent among individuals of Asian descent. In the US and the EU alike, young males are the demographic most likely to express an interest in crypto.
- Venture capital funds poured $9.2 billion in the crypto industry in the first quarter of 2022 alone[17], and between $20 and $30 billion in 2021. The majority of those investments targeted US companies and, depending on the estimates, represent 3 to 4 per cent of total venture funding in the country. Preliminary data for Q2 2022 signal a predictable slowdown in investment[18].
- As of January 2022, 38 per cent of total computational power used to produce new units of Bitcoin was located in the US. China came second at 22 per cent, despite a government ban that had seen its share drop to zero over the previous Summer[19].
- In DeFi protocols, users can "lock" funds in smart contracts, e.g. when posting collateral against a loan. Total value locked (TVL) is an imperfect but frequently used measure of interest in the DeFi ecosystem. As of August 2022, TVL hovered around $70bn, down from a peak of roughly $250bn at the close of 2021[20].
- The OECD reports[21] that institutional transactions, defined as those exceeding $1m, dominated DeFi for the better part of 2021. Analysis of blockchain data shows high recirculation of the same funds, pointing to substantial use of leverage. The actors involved are generally crypto-native financial institutions.
- According to market tracker DAppRadar, NFT sales totalled $25bn in 2021, driven by digital art projects. So far 2022 has been slower but some NFT providers seem to be enduring the crisis better than other segments of the crypto world.

[15] European Central Bank (2022), Financial Stability Review, May.
[16] https://www.pewresearch.org/fact-tank/2021/11/11/16-of-americans-say-they-have-ever-invested-in-traded-or-used-cryptocurrency/
[17] https://www.axios.com/2022/05/11/crypto-startup-funding-boomed-in-q1-despite-ongoing-market-slide
[18] https://www.axios.com/pro/fintech-deals/2022/06/14/crypto-vc-dollars-shift
[19] https://ccaf.io/cbeci/mining_map
[20] https://defillama.com/
[21] OECD (2022), Institutionalisation of Crypto-Assets and DeFi–TradFi Interconnectedness, OECD Publishing, Paris. https://doi.org/10.1787/5d9dddbe-en

3. The mistrust challenge

There are different threats to crypto's credibility. While not all of them stem from characteristics of the technology, they tend to be conflated together in a bad image of the sector. The phenomenon is best analyzed by distinguishing four macro categories of such threats: criminal activity (Section 3.1), mismanagement of risk (Section 3.2), bad governance (Section 3.3), and poorly audited code (Section 3.4).

These categories, again, do overlap frequently. Sometimes the overlap is easy to see – say, when a custodian misappropriates customer funds to take gambles in high-risk markets. Sometimes the line is hard to draw, because behaviors that breach regulations in traditional finance may not be clearly illegal in crypto.

Note that some cases that we mention in the following, under the 3.2 and 3.3 Sections, are or may be in the future under investigation for the presence of criminal activity and intent. Pending court judgement, we present them as examples of bad risk management or bad governance. This does not imply that we believe no crimes were committed – such an evaluation is definitely beyond the scope of any research work. The classification will be revised in future versions of this work, should the outcomes of legal proceedings require it.

3.1 **Criminal activity**

Crypto actors can be involved in criminal activity such as fraud, theft, and extortion as targets, perpetrators, or (generally unwitting) facilitators.

3.1.1 *Targets*

Crypto financial institutions are subject to the same types of cyber attacks as their traditional counterparts. Centralized exchanges and other service providers that manage customer funds are a commonplace target. Custodial crypto accounts, also called hosted wallets, can be emptied through phishing or social engineering attacks like ordinary bank accounts. The custodian company can also be hacked directly[22]. Attacks are also possible on non-custodial wallets, but they are harder to carry out.

A different category of cyber attack can target a blockchain directly, perhaps an analogue of trying to hack payment systems such as TARGET2 in the EU or Fedwire in the US. Those attacks are

[22] Consequences for account holders can be worse compared to the traditional world because most crypto transfers are generally irreversible, irrespective of the custodian's preference. Recovery of stolen funds can be complex, although many steps ahead have been taken recently. Note that irreversibility is generally held as a positive value in the crypto community, because it is a bulwark against manipulation, but it has its downsides in case of malicious activity.

historically unsuccessful, as indeed most blockchain infrastructure is very secure. Recently, however, components that connect some newer chains to others were successfully penetrated (see Section 4), resulting in loss of funds.

3.1.2 Perpetrators

Fraud and theft on the part of crypto actors are common. A frequent form is the so-called rug pull, whereby the founder of a crypto venture sells tokens in exchange for fiat money promising services, financial returns, or anything else of value then just disappears. This was exceedingly frequent during the ICO craze of 2017, and it still happens today. A different incarnation is theft of customer funds on the part of companies that offer all sorts of financial services. The company eventually dissolves, managers abscond or concoct tales of external cyber attacks, and customers are left with little to no recourse. Ponzi schemes are quite frequent too.

Criminal enterprises of this type are often accompanied by very aggressive publicity on mainstream outlets, aimed at reaching potential investors that are not interested in crypto per se – indeed, may never have heard about it before – but may be drawn into it by the promise of high yields, only to end up losing their capital. This is why a number of jurisdictions have banned some forms of advertising of crypto investments.

More complex financial crimes happen as well, mirroring the full scope of what can happen in traditional finance, although those may be harder to identify as such because the industry is not fully regulated (see Section 3 above).

3.1.3 Facilitators

Crypto has been associated with various shady trades, such as the sale of illicit drugs, counterfeit items, or hacking services, because of the anonymity it provides to interested parties. Indeed, the "crypto is for criminals" narrative remains a staple of the public debate, despite the industry's efforts to convey a different message[23].

Last but not least, crypto is involved in ransomware attacks, a problem so large that even international fora such as the G7 have given it consideration[24]. The motivations behind ransomware attacks can be very different – criminal syndicates and nation-states alike may launch them to raise

[23] In its 2022 Crypto Crime Report, Chainalysis puts at $14bn in 2021 alone the value received by addresses associated with criminal activities. While this is a big number, according to the same source it amounts to a mere 0.15% of total crypto transactions in the same year. The published number is an underestimate of total criminal activity, since not all addresses used by bad actors are known, not all transactions are easily detectable, not all happen on-chain immediately after a crime, and some borderline events might not have been classified as driven by criminal intent.
[24] G7 Finance Ministers and Central Bank Governors (2020), Ransomware Annex to G7 Statement.

money, but also for more sinister ends, like wreaking havoc on essential services or feeding fears of mass data erasure.

3.2 **Mismanagement of risk**

The 2022 crisis was largely the result of excessive accumulation of risk in the crypto ecosystem. Some forms of inappropriate risk-taking are specific to the industry, while others mirror traditional finance. Bad risk management often intersects with bad product design, i.e. tokens are designed in a way that leaves them exposed to large losses when unforeseen events occur.

3.2.1 *Bad incentive design, also known as "bad tokenomics"*

While designing a crypto project, developers sometimes do not fully understand the economic incentives they are creating for prospective users, and how various systems will react to certain market events, leading to failure of the project and losses for investors. In the following, we provide two very different illustrations.

3.2.1.1 *Algorithmic stablecoins and the Terra-Luna case*

A key trigger for the 2022 crisis came from one of the most decentralized corners of crypto, that of algorithmic stablecoins. As decentralization increases, so does the likelihood of bad tokenomics, because the complexity of the endeavors goes up.

Box II - A very condensed stablecoin primer

A stablecoin is a type of token whose value is supposed to fluctuate very little, contrary to what happens to major cryptos such as Bitcoin or Ether. Stablecoins have sometimes been called the "killer app" of crypto since they are a key component of decentralized finance (DeFi) markets. Anyone participating in those markets who would rather lose the volatility between trades but does not want to exit to fiat every time buys stablecoins instead. Stablecoins are also popular in DeFi lending protocols, i.e. decentralized crypto credit markets. A measure of the popularity of those tokens is given by the number of daily transactions. As of August 2022, Tether (USDT) – the largest stablecoin by market capitalization – recorded roughly 1.4 million of transactions per day, while Bitcoin recorded about 270,000[25].

Stablecoins can be issued by a company that purports to guarantee their stability, by making available a reserve of fiat-denominated assets so that token holders can redeem their coins for a fixed value – generally, one US dollar – whenever desired (the credibility of this promise varies a

[25] Source: Messari.io. The total traded volume in Bitcoin was of course higher, because Bitcoin was worth roughly $20,000, while Tether trades at $1. The figures, however, want to give a sense of how often coins are moved, as opposed to how much the movements are worth.

lot from project to project). This is what we call centralized stablecoins. Some stablecoins, however, are issued in a decentralized fashion by an algorithm. The algorithm is supposed to work in such a way that market participants have the correct incentives to keep the value of the coin stable. Algo stablecoins are particularly prized by a part of the community because they are truer to the original intent of crypto, but they are also hard to get right and the list of successful projects in this area is very short[26].

Stabilization of an algo coin is often based on a mint/burn mechanism involving automated arbitrageurs and one or more other tokens used as reserve, which have their own market value and can be exchanged with the stablecoin at a fixed $1 price at any time. Whenever the stablecoin is priced at less than $1, holders have an incentive to swap their stablecoin for a dollar's worth of reserve tokens. Those who do not own the stablecoin have an incentive to buy it and execute the same swap. A certain amount of stablecoin is destroyed and, with increased demand and diminished supply, the value should go back to $1. The minting of new reserve tokens lowers their value, but this is supposed to be a short-term phenomenon that is reversed as soon as the stablecoin is priced at over $1 and the stabilizing mechanism runs the other way. This, alas, only tends to work when oscillations are within a very narrow band around $1[27]. While arbitrage is indeed automated and fast in DeFi markets, not all tokens have the same degree of liquidity. Both the stablecoin and the reserve token can also, say, incur a major loss for a number of reasons unrelated to the mechanism itself, either as part of a macro trend or for idiosyncratic reasons. This leads straight to de-pegging, or consistent trading under $1, as it would in conventional monetary systems[28]. Whenever something like this happens, trust in the asset rapidly falls to zero, with the value following suit.[29]

[26] MakerDAO, a project that has shown remarkable resilience, is based on crypto overcollateralization. The protocol requires a deposit of Ether, and then allows for the borrowing of newly minted stablecoins valued at $1 only as long as the collateral ratio is 150% or more. When the value of Ether drops, if the collateral is not promptly reintegrated then is liquidated (also see Section 3.2.2). The stablecoin holder pays a hefty liquidation fee, similarly to what happens with margin calls in traditional finance. This is indeed less forgiving compared to projects with a fiat reserve and perhaps one of the reasons, along with well-structured decentralized governance, why it persisted for nearly five years, a very long time in crypto. MakerDAO recently announced investments in safe assets in fiat to bolster its resilience to extreme market conditions. A heated discussion is in progress in the community as to whether this should be done or not. For this one (thus far) successful project, many others sunk when the algorithmic rules proved inadequate.

[27] Note that this is a simplified explanation. Many algo coins have pegging schemes that are more sophisticated. The added complexity has historically been a cause for failure.

[28] For a formal model of algorithmic stablecoins, published as a preliminary draft right after this crisis, see d'Avernas, Maurin, and Vandeweyer, Can Stablecoins be Stable?. The authors show the conditions under which these systems end up in one of two possible equilibria, i.e. zero value of the token or relative stability of the peg. The paper also provides a useful review of the (small) previous literature on stablecoins, both institutional and academic.

[29] While bad tokenomics are a more frequent issue, note that this can also be the result of scams. At least one stablecoin recently de-pegged because of fraud concerns related to the issuers of the token that was backing it.

UST was a stablecoin supposedly worth $1, issued on a blockchain called Terra. Many crypto users bought into it in because it could be invested in a fund called Anchor, run by the same company that issued UST. Anchor offered yearly returns approaching 20 per cent. UST's reserve token, LUNA, enjoyed very high market valuations on the backdrop of enthusiasm around the project. In the Spring of 2022, UST underwent a few days of heavy selling and the stabilizing mechanism proved insufficient. The stablecoin de-pegged and the reserve coin's value went to near-zero, burning roughly $40bn in the space of a few days. Many players in the crypto space, including large funds and lenders, had positions in UST and LUNA. Contagion damage is still being quantified[30].

The ecosystem aggregated an unprecedented variety of risks. The high yield offered by Anchor was only sustainable as long as the reserve token maintained a formidable market valuation, given how other ventures of the company were not particularly profitable. Rules around UST redemption were not always clear. There was no backstop in case of critical events affecting both UST and LUNA – a $2.3bn bitcoin stash that was meant for that role proved to be largely insufficient. There was no plan at all for a worst-case scenario. The system was just expected to "run on its own" in any market condition. Incentives for holding the token were, all in all, quite fragile, and they collapsed under pressure.

3.2.1.2 *The Otherdeed sale*

Otherside is a metaverse videogame under development by Yuga Labs, a market leader in the NFT space. In the Spring of 2022, Yuga Labs announced the first public sale of Otherdeed, or NFTs representing property titles for virtual land plots in Otherside.

The starting price of each NFT was around $7,000, probably lower than expected by most potential buyers, which created formidable demand. A queue of bids put a lot of pressure on the Ethereum network, whose transaction fees – or "gas fees" – increase proportional to the demand for block space. In the end, roughly $160 million were spent on gas fees alone because of unprecedented congestion. Some buyers paid gas fees for more than twice the price of the virtual plot. Others lost money outright as the transactions did not go through, but gas fees were debited nonetheless[31].

All of this happened because the initial price was set at a low level, and issuers of the tokens decided to forego an auction mechanism for a flat price. This price was denominated in fungible tokens issued by the company that was offering the land plots. Had the tokens appreciated on the back

[30] It will be difficult to get precise numbers because many funds and family offices that invested in this product do not have legal disclosure obligations on the extent of exposures.
[31] Yuga Labs eventually issued refunds for such cases.

of a successful sale, both the company and its customers would have benefited. Instead, in the immediate aftermath of the fact the tokens lost a quarter of their value. They enjoyed a very partial recovery sometime later, only to be eventually dragged down with everything else during the crisis.

3.2.2 *Excessive leverage*

Excessive leverage is a problem affecting all sorts of financial markets. In crypto ecosystems, however, it may become more extensive and more pernicious compared to traditional finance. In the absence of regulation, the only limits to leverage are those set voluntarily by centralized lenders and decentralized lending protocols. During the expansion that preceded the crisis, limits were loose and a risky link was established between those two components of the industry.

A financial institution – say, a crypto hedge fund – would go to a centralized lender and borrow a certain amount of assets against crypto collateral. Then they would carry those assets over to the DeFi environment, in turn posting them as collateral for other loans. The centralized lender, on the other hand, would take the collateral received, and repost it to perform their own DeFi trades, sometimes unbeknownst to the borrower. This was sometimes mixed in with crypto funds deposited by retail customers, who enjoyed higher yields compared to customers of traditional banks, but may have not been aware of what such yields implied in terms of risk[32].

Over time, a complex web of interdependencies arose, with a degree of aggregate leverage that was unknown to participants themselves, and high correlation risk since all the trades involved the same asset class. These dynamics, along with exposure to UST and potentially shady operations that are not yet fully understood[33], loomed large in the court-ordered liquidation of Three Arrows Capital in the British Virgin Islands and the subsequent bankruptcy filing of the fund in the US[34]. These

[32] Voyager, a crypto broker that recently filed for bankruptcy, is being investigated by the US Federal Deposit Insurance Corporation (FDIC). Voyager's marketing language, according to the regulator, may have led customers to believe that their deposits on Voyager's platform were insured by the FDIC in the same fashion as traditional bank accounts.

[33] Before 2022, Three Arrows Capital was a Registered Fund Management Company (RFMC) headquartered in Singapore. This is not a crypto-specific legal entity. Then it moved its headquarters to British Virgin Islands (BVI). The Monetary Authority of Singapore (MAS) recently issued a censure to Three Arrows, concerning violations dating back to when it was headquartered in the city-state (provision of false information and long-standing breach of asset thresholds; see the MAS press release here). No penalties accompanied the censure, but MAS announced that it was committed to further investigation. In the BVI, a court ordered the liquidation of the fund in June 2022. Eventually, Three Arrows – headed by US citizens – filed for bankruptcy protection in a New York Court. The proceedings can be expected to be quite lengthy and complex, as first indications surface of a complicated corporate structure spread over multiple jurisdictions. This is a typical example where bad risk management may eventually turn out to intersect with financial crimes (see Section 3.1.2)

[34] https://www.cnbc.com/2022/07/02/crypto-hedge-fund-three-arrows-files-for-chapter-15-bankruptcy.html. The court-appointed liquidator, US advisory firm Teneo, briefly posted online an affidavit which describes findings on 3AC's situation in great detail. The post was since taken down, but a copy is available here.

documents also show the possibility of wrongdoing. Excessive leverage combined with UST holdings was also a factor in the distress of Celsius[35] and BlockFi, two large centralized lenders.

As we write, centralized exchange FTX was offering to extend credit to some of those players, while acquiring part of their assets at a favorable price. The ecosystem had a mixed response to this development. While some appreciated the sector's attempt at restructuring without bailouts funded by taxpayer money, others were fearful of excessive concentration of funds and power in a single company or a small group of companies[36].

3.3 **Bad governance**

This is a problem that plagued crypto since the beginning, but today it is assuming specific contours on the backdrop of technological change. Leaving aside the endeavors that went for a traditional, centralized corporate structure, the key question is: assuming one believes that decentralization is essential to security and fairness, like many in crypto do, how should the governance of a project be designed? Who gets to decide on changes in protocol rules, affecting the validation mechanisms of transactions and the minting and burning of tokens? Who has the right to intervene in case of major problems? Who can delegate the auditing of smart contracts? And so on. All of these choices have important consequences for the portfolios of token holders, and while the answer to the questions is ideally "the user community", it is hard to translate this into actual organizational structures.

Box III - Bitcoin governance

Bitcoin, the only major crypto venture with no known founder, is governed by a mechanism whereby anyone can propose a change to the protocol (known as a Bitcoin Improvement Proposal, or BIP) on the bitcoin-dev mailing list, where a loose group of core developers congregates, or other decentralized venues. At some point, a proposal that is generally well-received becomes official, i.e. gets assigned a BIP number and is published to the Bitcoin Core GitHub repository. This does not mean it is approved yet. The developer community further scrutinizes it for flaws both technical and economic. A lot of proposals die at this stage. Even if they don't, they eventually go through – assuming someone has coded them – only if a majority of validator nodes and/or miners agree to deploy them. For this reason, Bitcoin is extremely slow to change.

[35] Celsius eventually filed for bankruptcy in July 2022.

[36] Interestingly, true DeFi – say, lending protocols that are actually decentralized and automated – did not encounter any major issue during the crisis. This is largely down to the overcollateralization that such protocols require of borrowers and to the automated liquidation mechanisms that intervene as soon as a certain collateral threshold (generally between 130 and 150 per cent of the loan) is no longer met. While this system may trigger perilous liquidation cascades in times of generalized market distress, it has not happened so far.

Several early communities have seen a significant amount of squabbling, which sometimes terminated in implosion and sometimes did not. This is still happening today, but we will not focus on this issue here, as infighting within companies is not quite specific to the crypto ecosystem. Rather, we look at decentralized autonomous organizations (DAOs), a crypto-native model of governance that some industry players consider superior to traditional options. While it may have potential in terms of reducing coordination costs and improving transparency of decisions, so far it also showed a number of weaknesses.

3.3.1 *DAO basics*

A DAO is a set of smart contracts that govern how a blockchain, cryptoasset, or other project is managed. The contracts assign certain rights to entities that hold governance tokens (see Section 2). The most important are the right to propose changes in projects and the right to vote on change proposals. The contracts also establish rules on how many tokens are needed to present a proposal or participate in a vote, which majorities are needed for which decisions, and so on. Those rules vary across DAOs. The contracts also have the ability to hold and transfer funds, i.e. DAOs can also double up as company treasuries or investment vehicles. A record is kept of what is happening in the governance space at all times[37].

Most crypto projects necessarily start as entirely centralized, with a small group of founders and investors calling all the shots, but some have the explicit goal of ultimately turning to a DAO for governance[38]. There are some affinities between DAOs and shareholder assemblies in traditional public companies, but it is important to note that governance tokens do not necessarily represent equity.

In the first stage of DAO creation, founders set the rules for the minting and distribution of governance tokens – DeFi platforms may distribute them, say, for contributing liquidity to automated money markets. Newer blockchains may use them as rewards for running decentralized applications on their infrastructure as opposed to more established ones. Indeed, there are many distribution

[37] For a very interesting snapshot of what is being discussed within some 850 DAOs at any time, see the Messari Governor at https://messari.io/governor/overview.

[38] DAOs usually exist to manage ongoing endeavors, but some are born for a one-off operation – say, crowdfunding for a specific goal. According to some, single-purpose DAOs are going to become popular because they are an optimal channel for the trustless convening of people who do not know each other in pursuit of a shared goal. The first major endeavor of this kind, a group forming a DAO to buy a copy of the US Constitution, almost attained its goal. After losing the auction, however, controversy emerged on the subject of what to do with tokens that should have been used, say, to decide which museum should have the copy, but were now rendered useless. Refunds were complicated by high gas fees.

schemes, from those entirely focused on the financial resources contributed to a project to the horizontal ones that reward participation in community discussion. Eventually, the DAO is supposed to decide by itself if new governance tokens have to be minted, which rights they should confer, and to whom they should go.

3.3.2 *DAO pitfalls: concentrations of power*

DAOs are, in principle, a way to extend decentralization. Sometimes, however, the opposite result obtains. Many governance token holders, especially for the biggest projects, do not even read proposals on dedicated forums, and they do not participate in the votes even when good delegation mechanisms are available. They hold the tokens because they hope for price increases, with an intent to resell. This led many DAOs to adopt low quorums for approving change proposals. This means that even when the tokens look fairly distributed, say with no entity exceeding a 10 per cent threshold of token ownership[39], a few holders can get changes through. For smaller DAOs, concentration of voting power can assume forms that are even more evident, with one or a few individuals or groups owning a disproportionate share of governance tokens[40].

3.3.3 *DAO pitfalls: lack of transparency*

Another issue is pseudonymity of participants (see Section 5), which imperils the very transparency that DAOs aim to achieve. Many organizations are proud to publicize their contribution to a DAO. This is the case, for example, of student societies in universities, certain companies, specialized investment funds, and individual crypto advocates. On the other hand, looking at the list of delegates for any major DAO inevitably returns many hexadecimal wallet addresses with no associated name. Some correspond to non-human entities, smart contracts that vote according to preset rules. Others correspond to unknown humans. As research on the legal status of DAOs continues, on the backdrop of laws passed in Wyoming that treat a DAO like a limited liability company, this is certain to become an issue – because of the non-humans and the unknown humans both[41,42].

3.3.4 *DAO pitfalls: governance attacks*

[39] https://sybil.org/#/delegates/

[40] Foul play has also been hypothesized for some projects, with founders retaining for themselves a large share of governance tokens, not using them yet and not informing the public correctly about their future intentions.

[41] Anonymity of shareholders also exists in the non-crypto world. This, however, only means that the public cannot access the identity of a company's shareholder, while the company itself can. This is not the case for DAOs.

[42] For further discussion of the legal implications of DAOs, see O. Borgogno (2022), Mind the Gap. Making DAOs Fit for Legal Life, forthcoming, Banca d'Italia.

Finally, some DAOs are easy targets for governance attacks, or attacks that use weaknesses in governance contracts to perform actions that, while not formally prohibited by the DAO, are clearly against its interest. Recently, an attacker obtained a so-called flash loan on a DeFi platform, i.e. an uncollateralized loan that is extended and repaid in the same block, or set of transactions that gets validated at the same time[43]. A flash loan can be for any amount because if the borrower fails to repay it the platform just deletes any transaction made with the money, returning it to the lender. The loan was used to buy a majority of governance tokens for the DAO running Beanstalk, another DeFi project. The attacker then proposed to send all the DAO's money to his own address, approved the proposal single-handedly, resold the tokens, and repaid the loan, all in a matter of minutes. This is a very blatant version of a governance attack, but subtler ones exist too.

3.3.5 *DAO tooling*

A brand new sector of "DAO tooling" is emerging in the industry to address these issues. It focuses on bridging the gap between standard corporate governance knowledge and blockchain technology. Right now the actors involved are all from the private sector, but DAO tooling could become a strong point of cooperation between the crypto ecosystem and regulators (see Section 5). DAOs are one of the most evident examples of how the crypto industry can get into trouble even when in good faith for trying to reinvent everything from scratch, even in the presence of similarities with products and mechanisms that already exist in other sectors. Domain knowledge accumulated outside of the ecosystem is often ignored, and evitable errors follow.

3.4 **Poorly audited code**

Last but not least, poorly audited code is often a concurrent cause in all sorts of problems. "Code is law" is one of the original crypto mantras, but what about bugs? Indeed, one of the first DAOs – a venture capital endeavor called simply The DAO, running on Ethereum – had a loophole in code that was exploited by an attacker in 2016. The attacker syphoned off all the funds that The DAO held. This forced Ethereum developers to introduce a hard fork, i.e. rewrite history by resetting blockchain contents to a pre-attack block. An unplanned hard fork is one of the most serious dysfunctions that can happen in crypto, because it compromises the whole concept of immutability and independence from human whims.

Today's industry pays more attention to such problems. Bug bounty programs are established. A number of firms specialize in code auditing or smart contract verification, i.e. confirmation that a

[43] This is one of the DeFi instruments that, rather than mirroring traditional finance, actually do something that was not quite possible before. The lifecycle of a flash loan is counted in seconds or minutes depending on the blockchain.

contract's functioning matches its specification. Reputable actors share the results of audits and verification on their websites. However, this is a static process, not performed on a continuous basis. Users may be sure that version 2.0.2 of the protocol was audited, but sometimes a new audit does not come until version 4.3.1, one year later. Again, bad code is not a crypto-specific problem, but the absence of regulatory standards implies that companies have weaker incentives to keep their audits current.

4. The technology challenge

In the very early years of crypto, those who wanted to propose an alternative to Bitcoin needed to have their own blockchain, where they launched so-called "altcoins". Most altcoins were copies of Bitcoin with minor technical changes. So, the settlement infrastructure for each coin was separate, but there was little diversity.

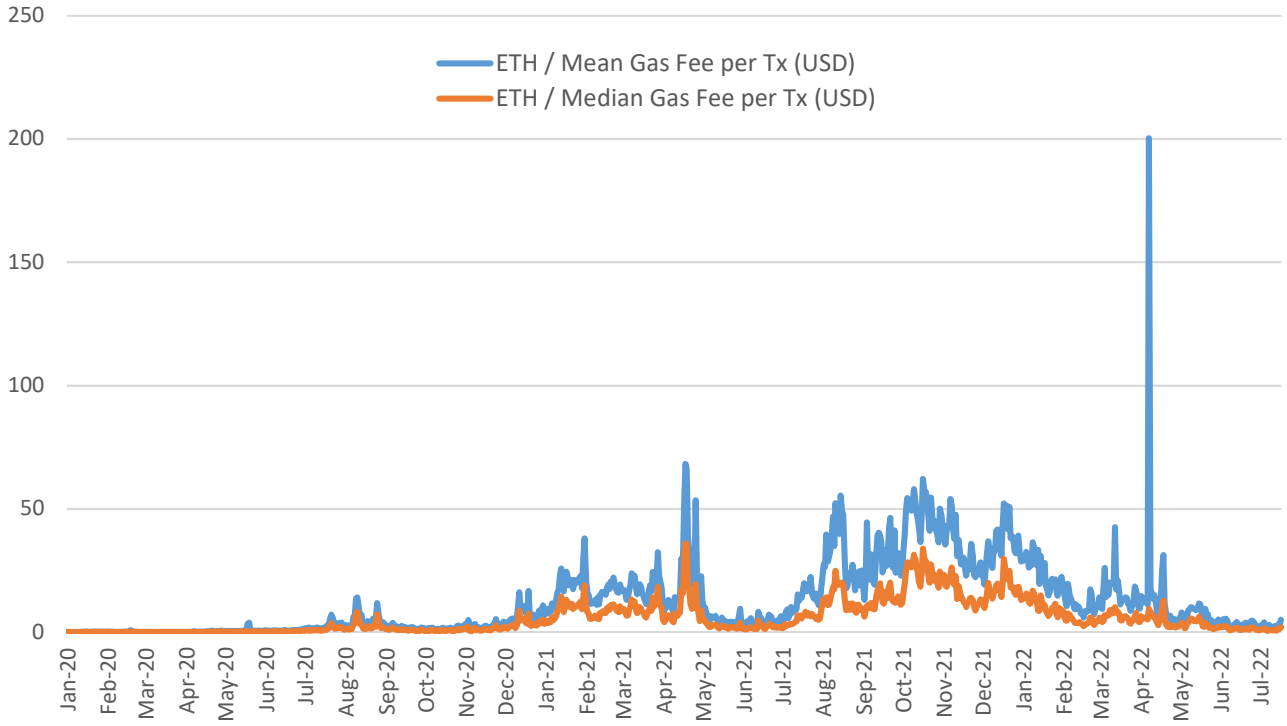
This changed with Ethereum, whose blockchain supported the writing and execution of code. Anyone could now issue their own tokens by just uploading a block of instructions called a smart contract, and paying a gas fee to the network validators. The token issuer had the advantages of a secure infrastructure without having to build it from scratch and maintain it. With time, standards emerged – for example, ERC-20 for fungible token and ERC-721 for NFTs – that simplified the issuance of the most common forms of cryptoassets. The same was true for applications. Developers could upload the code for, say, a crypto exchange market and have it run on-chain as a DApp rather than having to build a centralized website. This allowed for a reduction in costs, improved security, and closer alignment with the crypto ethos.

For several years the focus shifted from building blockckains to issuing tokens and building DApps on Ethereum.

This is now – in turn – changing. As the number of cryptoassets grew exponentially, the number of DApps did too, markets expanded, smart contracts became more complex, and execution of code became more computationally burdensome. As a consequence gas fees on Ethereum climbed significantly starting in mid-2020, never to revert back to the low levels of previous years. After that, small transactions were no longer possible, as fees exceeded the value involved (Figure 1; the Otherdeed spike discussed in Section 3.2.1.2 is clearly visible). This was and still is an ordinary occurrence, even in the absence of extreme events.

Figure 1

Mean and median gas fees on the Ethereum network, 01/20-07/22



Source: Coinmetrics

In addition to this, strong misgivings had been brewing in the crypto community for a while about the desirability of a single infrastructure upon which the whole industry, except for Bitcoin, rested. The founders of Ethereum had indeed aimed at building a "world computer", but they had never really wanted it to be the only one. So, while convinced that their product was the best, they welcomed competition in the form of creation of numerous new blockchains.

The landscape today is multi-layered, and it struggles with the simultaneous attainment of security, decentralization, and scalability – an ecosystem-wide version of the blockchain trilemma.

4.1 *Layer 1, Layer 2, and sidechains*

There are a number of so-called Layer 1 blockchains (L1), where the chain used for settlement is the same one where code for all sort of transactions and DApps is run. Ethereum is still the biggest among those offering smart contract functionality, but it now has competitors such as Solana and Avalanche. L1s can differ quite a lot on a variety of grounds, e.g. consensus protocol or fee structure. This class of blockchains aims at being the most complete and secure.

Then there are Layer 2 blockchains (L2), also called L2 scaling solutions, which are always built on top of a chosen L1. They aim at offering users and developers cheaper and/or faster transactions while still leveraging the security of the L1 for final settlement[44]. There are many technical options to implement a L2[45], but the general idea is that many user transactions posted on the L2 blockchain are aggregated together, pre-validated by the L2 with low-cost algorithms, and then submitted as a compressed bundle or "roll-up" for final validation to the L1, This reduces fees because the L2 charges little to users and the L1 only charges the L2 for one transaction – that concerning the bundle – rather than the hundreds of individual transactions in the bundle. The throughput is also significantly larger, hence the "scaling" definition. Some L2s, such as Optimism and Arbitrum, are general-purpose. Others only support a certain DApp[46]. L2s, like L1s, generally issue their own native tokens, but this is not always the case.

While L1s and L2s are the most popular solutions, two other categories are worth mentioning. Some projects aim at providing a Layer 0 (L0) first and foremost, i.e. a set of tools to build ecosystems of connected blockchains. One popular choice is Cosmos, which has its own L1, and also powers some 50 other L1s – including a couple of well-known ones – with its Tendermint consensus mechanism. A competitor is Polkadot, which states its purpose as powering a network of blockchains. Another is Polygon, which offers both an L2 for Ethereum and a separate ecosystem building capability[47].

Finally, there are sidechains. Those are independent blockchains, often specific to a single DApp, that are connected to a chosen L1 via a software called a bridge. Contrary to L2s, they do not rely on the L1 to provide security. Their own security mechanism may copy that of the corresponding L1, but it may also include modifications. A sidechain is a scaling solution like a L2, in that it seeks to provide lower fees and higher speed. It aims at obtaining this goal by optimizing the validation algorithms for the specific type of DApp it supports.

[44] In the Bitcoin ecosystem, L2s are also meant to support smart contracts, which cannot be deployed on the L1. Any DApps consequently need to be built on an L2. The largest Bitcoin L2 is currently the Lighting Network (see https://lightning.network/how-it-works/). Mostly aimed at making payments faster, it encountered strong growth in 2022 through integration in some centralized personal finance apps (see e.g. Arcane Research, The State of Lighting Vol 2, April 2022). Users may not even know that they are on this network as opposed to the main Bitcoin chain. DApps such as RGB (https://www.rgbfaq.com/faq/what-is-rgb) and Taro (see https://lightning.engineering/posts/2022-4-5-taro-launch/), addressing digital rights management and digital asset issuance respectively, are built on the Lightning Network.

[45] See https://ethereum.org/en/layer-2/

[46] This was, for example, the case for derivatives exchange dYdX, until it announced that it was going to have its own L1 running on Cosmos (see below).

[47] Polygon is classified by some as an L1.

4.2 *Security, decentralization, and scalability*

This dynamism of infrastructure projects is, at its core, a very positive factor because competition can ultimately benefit users and developers, while enhancing the quality of technology. There is, however, one significant challenge. Can the ecosystem *as a whole* be simultaneously kept secure, decentralized, and scalable – not just in the technical sense, but also in the sense of providing accessibility to everyone at a reasonable cost?

The security and decentralization problems can be looked at together, in the light of three key issues:

(a) not all blockchains are equally secure. Some of them are poorly designed, or have a number of validator nodes that is too low to ensure adequate protection against attacks. A frequent complaint in the industry is that venture capital funds, now a core actor of the crypto scene, want a short time to market for new blockchains[48]. There is a case of misaligned incentives, in that a new chain can generate early profits by planning an airdrop, or a free distribution of tokens, which can appreciate very fast given sufficient hype around the project. As it is often the case in the broader IT market, security can be overlooked in the rush to meet a deadline. When it comes to infrastructure, this is especially dangerous. Sidechains, often built at low cost and high speed, are one of the weak points of the system. It is not the only one, though; for example, the popular L1 Solana has experienced episodes of extended downtime[49];

(b) interoperability is demanded by users and developers, but so far it has not been achieved securely. Blockchains don't talk to each other well, with the only exceptions of L2s and their own L1s in the best designed cases. L0s aim at constructing whole ecosystems of blockchains, but those right now do not connect easily to anything else. This is, in part, a structural feature. A co-founder of Tezos, an L1, explained to the Bloomberg *Odd Lots* podcast that full interoperability would imply exact replication of each chain's consensus mechanism on all other chains (this does not apply to L2s because, as discussed above, they ultimately use their L1's consensus). This would be very expensive and would slow transactions down, so if users want to access platforms and tokens that are on different chains they have to use dedicated systems. The most popular option so far is called a bridge, and it is very difficult to implement safely. Hackers recently stole $600m from the bridge connecting Ronin, a sidechain built for the Axie Infinity video game, to Ethereum. Another $190m were stolen from the Nomad

[48] On this and connected issues also see S. Marchetti (2022), Web 3, Blocksplained, forthcoming, Banca d'Italia.
[49] https://status.solana.com/uptime

bridge services provider. Newer architectures are being tested intensively, but so far the market did not deliver a reliable solution;

(c) the system-wide relationship between security and decentralization is non-linear, at least for now. Within-chain decentralization always means more security, if done well. This is not the case for across-chain decentralization – there may be too much of a good thing, and this creates a conceptual problem for crypto. In theory, deploying many blockchains with different governance models, each supporting different applications, marketplaces, and tokens is a way of protecting the system from any hegemonic attempt. This works in a political sense but also technically, because on any chain other than Bitcoin there is a risk, no matter how remote, of transaction censorship performed by founders and/or developers. If there are many chains, one of them going rogue does not damage the whole system. On the other hand, if a sizable share of those chains are not truly decentralized, not technically reliable, or they involve shady actors, perhaps it is best to stick with a few options whose trustworthiness is already universally recognized.

4.2.1 *Accessibility as a component of scalability*

When it comes to broad accessibility and transaction cost containment, which make for scalability in a full, beyond-just-technical sense, we need to keep in mind that blockchains compete in two-sided markets, as they need to attract users on one side and developers on the others. Both sides have switching costs, given the interoperability constraints.

For every new L1, L2 etc. that they choose, users may need to install a different wallet, buy a new type of token, familiarize with wallet interfaces that are still in a development phase, and so on – that is, if they want to forego a centralized intermediary to save on fees, approach crypto the way it was conceived, and access DeFi services that are just not available on the big platforms. This requires attention and effort even on the part of users that are mildly competent with computers[50]. Developers can in principle deploy their DApp on any chain, but they need to adapt it first, which has a cost. The largest DeFi endeavors already exist both on at least one L1 and on the top L2s, because users of the latter are growing and projected to grow even more. It is not always easy, and generally the deployment of L2 versions is gradual. Deployment to an L1 different from the native one takes even more work and consideration.

There are partial solutions to this issue that can help even in the absence of a fully interoperable ecosystem. The problem is easier on the user side. So far, blockchain companies have been

[50] Sometimes, software bugs can lead to monetary losses, although this is expected to improve as the system matures.

notoriously inattentive to UX/UI (User Experience/User Interface) design, especially in frontier segments[51]. Investors are starting to take notice and, as the market expands, it is likely that monetary incentives for improving in this dimension will arise. Some products in this vein are already being deployed, although none works particularly well at the time of writing.

The developer problem is tougher because it falls under the within-chain/across-chain decentralization tradeoff described above. Ultimately, scaling vertically on L2s built on the same L1, or a handful of L1s, is going to be less costly and more secure than scaling horizontally on many L1s, and it is also likely to offer users lower transaction fees. Two-sided markets tend to concentration, and a prevalence of two or three L1s with multiple L2s may be the form that concentration takes in crypto infrastructure[52]. Such concentration could be partly tempered if developers of at least some popular DApps chose to build their own single-purpose L1, creating market and infrastructure niches that are not easily accessible by the general-purpose L1s and their L2s. This is, however, a costly and complicated choice for protocols and users both.

5. The challenge for regulators

At the outset, policymakers saw crypto as little more than a vehicle for crime and speculation. Involvement of financial authorities was mostly confined to general warnings to the public, research papers, and cooperation with law enforcement by way of financial intelligence units (FIUs).

Today, major jurisdictions around the world are deploying comprehensive crypto laws with an eye to fostering innovation while ensuring consumer protection, preserving financial stability, and defending monetary sovereignty. Central banks and market watchdogs have a key role in developing and enforcing the rules.

Box IV - Authorities and crypto: a timelapse

Cryptoassets received attention from authorities since the early 2010s. At the time, the police was involved more frequently than regulatory agencies, e.g. in identifying online drug dealers who accepted Bitcoin as payment. Then some jurisdictions introduced licensing regimes for crypto exchanges and other service providers, mostly lightweight versions of frameworks conceived for traditional institutions. The focus remained mostly on prevention of crime, through the imposition

[51] Poor UX/UI design is also one of the factors that can expose users to fraud, by increasing the difficulty of interaction with the ecosystem.

[52] Indeed, there is already talk of L222, for "Layer 2 (primacy) in 2022", an acronym coined by crypto investors and journalists Ryan Sean Adams and David Hoffman. We could perhaps add another 2 for the two-sided market.

of know-your-customer (KYC) and anti-money laundering (AML) requirements e.g. for centralized exchanges.

The situation started to change in 2019, when Facebook (now Meta) announced the intention of issuing Libra, a stablecoin backed by a basket of safe assets denominated in various currencies. The plan caught the attention of policymakers, including international standard-setting bodies. Facebook's sheer size, at over 2.3bn daily active users[53] spread all over the world, meant that a private digital coin could potentially displace legacy payment systems and pose a wide array of risks, especially in weaker economies.

It was somewhat surprising to see the word "stablecoin" migrate from Bitcointalk[54] jargon to official documents. The G7 Working Group on Stablecoins published a key report in October 2019[55], effectively accelerating exploration of the crypto space by policymakers despite the fact that Libra had, indeed, very little in common with actual crypto.

The Libra project was eventually renamed to Diem and then abandoned by its proponents, but the genie was out of the bottle. As DeFi boomed in Summer 2020, and the industry as a whole saw sustained growth in 2021, regulators familiarized with the language, got into the mechanics of products and protocols, and thought about how to bring some order in what was no longer an experiment of negligible size.

The EU is at the most advanced stage, with the Markets in Crypto Asset Regulation (MiCAR) expected to come into force within the year, together with a new cybersecurity law applicable to all providers of financial services, including crypto[56]. A statute establishing a pilot regime for DLT-based securities trading is already active. In the US, a presidential Executive Order in May 2022 mandated several agencies to explore a number of regulatory issues and report back within six months. The UK announced in April that a regulatory package was coming, part of an effort to make the country a hub for the industry. Japan deployed stablecoin regulation in June. Other countries, such as Canada, Australia, and South Korea, are working on updating their crypto laws. A notable

[53] This figure refers to 2019 and has since grown.
[54] Bitcointalk.org is a popular online forum for Bitcoin discussion.
[55] https://www.bis.org/cpmi/publ/d187.htm
[56] Regulators in some EU countries have already released clarifying documents, in advance of full effectiveness of the EU law. For a recent example see Bank of Italy (2022), Communication on Decentralized Technology in Finance and Crypto Assets. The document's aims are "first, to remind supervised intermediaries, supervised entities and all those who work in various capacities in decentralized ecosystems, including as users, of the opportunities and risks associated with the use of these technologies in finance and with crypto-asset-related activities and services (issuance, custody, trading, loans, payment services […]; second, to highlight a number of aspects that are important for defining, on the part of the abovementioned entities, safeguards to mitigate the risks associated with the use of decentralized technologies and/or trading in crypto-assets."

exception to the trend of writing statutes that ultimately aim for an orderly functioning of the industry is China, where any and all use of crypto was banned in the Summer of 2021[57].

International standard setting bodies (SSBs) for the financial sector also provide both policy guidance and analytical insights, including in the context of G7 and G20 discussions. The Financial Stability Board (FSB) issued a statement on the international regulation and supervision of crypto asset activities in July 2022[58], the latest contribution in a multi-year workstream aimed at better understanding the ecosystem and minimizing the risks that stem from it[59]. The Bank for International Settlements (BIS) routinely publishes research on crypto, often focusing on issues that would otherwise remain unexplored outside of the industry[60].

Discussing the contents of specific laws or recommendations is outside the scope of this paper. We will also not focus on areas where the goals of the industry and those of regulators converge, such as contrast of theft, scams, and rug pulls (see Section 3). Once rules are in place, a solid habit of cooperation between watchdogs and the law-abiding portion of the crypto world can and will minimize the impact of ordinary bad actors[61]. The same dynamic should hold where cybersecurity is concerned (see Section 4), although regulators need to pay way more attention to the variability in blockchain infrastructure than they have done so far if the goal is to be achieved.

Rather, we want to focus on three challenges that are especially hard to meet. One is the existence of tokens that do not represent any claim on any entity, yet are traded as financial assets in crypto markets. This has no equivalent in the traditional world and it is inherently hard to regulate.

The second is the enduring commitment of the ecosystem to the values of decentralization, anonymity, and censorship resistance. These were key tenets of crypto in the early days and remain important in a number of projects that may potentially offer value to investors and users, yet they do not mesh well legal frameworks. Those elements are not even confined to the more informal,

[57] China was previously a key actor in the industry, especially where Bitcoin mining and centralized exchanges were concerned. There is some evidence (see Section 2) that some Chinese miners are circumventing the law, but it is very difficult to predict whether a crackdown will happen in the near future or not. Crypto bans also exist in Algeria, Bangladesh, Egypt, Iraq, Morocco, Nepal, Qatar, and Tunisia. In other 15 to 20 countries, mostly in Africa and the Middle East, crypto is not illegal but the restrictions on use cases are quite heavy.

[58] https://www.fsb.org/2022/07/fsb-statement-on-international-regulation-and-supervision-of-crypto-asset-activities/

[59] Also see, among other documents, the February 2022 FSB Assessment on Risks to Financial Stability from Crypto-Assets and the October 2021 Progress Report on the implementation of the FSB high-level recommendations on regulation, supervision and oversight of global stablecoins.

[60] See e.g. references in notes 14, 56, and 72.

[61] At first, regulators will need to be very careful in choosing who to talk to. Crypto history shows that even mainstays with large businesses and a dedicated following can be ill-intentioned.

regulation-averse part of the crypto world. Rather, they are interwoven to various degrees in the whole industry[62].

The third challenge is co-operation between regulators and the industry, which is essential to prevent obsolescence and circumventing of laws, yet needs to find a form that is convincing and fruitful for all parties involved.

5.1 Assets that do not represent any claim on any entity

At first glance, crypto trading platforms and protocols look a lot like traditional financial markets, except for the 24/7 working hours. They allow users to swap tokens against each other, buy and sell derivatives, pledge tokens as collateral for more complex trades, and so on. On closer inspection, however, they have a specificity that sets them apart from any other trading venue, and creates a major hurdle for authorities. They list a variety of tokens with very heterogeneous content (see Section 2). Only some of these tokens would be classified as financial assets in the non-crypto world, yet all of them are available for trading with the same tools, on the same app or DApp.

In traditional financial markets, traded assets represent a claim on a definite entity, and/or embed certain legal rights. In crypto markets, this is true only for certain assets, e.g. regulated stablecoins that carry a claim on the issuer, or tokens that are legally classified as securities. With the evolution of crypto statutes in many jurisdictions, the share of tokens with a clear legal profile is going to increase – see e.g. the DAO law in Wyoming, which also address governance tokens (see Section 3.3.3), and the assessment on NFTs that will be conducted by the EU Commission in the next eighteen months[63]. The industry is also hard at work on improving the transparency of smart contracts that create entitlements for token holders.

Despite these evolutions, certain assets will always fail, sometimes by design, to represent any claim on any entity. Bitcoin is the prime example and, given the size of its capitalization, it is hard to ignore. The same is true for ether and for most of the native coins of L1s and L2s (see Section 4.1), not to mention the so-called meme coins, and a large number of obscure tokens. Retail users may buy those assets for many reasons, including but not limited to paying for on-chain transactions, pure

[62] To name but one example, Coinbase – a large centralized exchange listed on Nasdaq – recently offered a self-hosted wallet app to its clients. Centralized exchanges typically hold client funds in custody, which gives them visibility on transactions and the ability to report and/or block any suspicious activity. Self-hosted wallets, conversely, are controlled by the token holder alone. Nobody else is able to initiate transactions on her behalf, or track what she is doing. Tracking can actually be achieved sometimes through forensics techniques, but those are more costly and complicated than simple monitoring by an exchange. The exchange probably offered the app because customers wanted to access DeFi services that require this type of wallet. Yet self-hosted wallets have been criticized by some legislators because they may facilitate illegal operations.

[63] https://en.cryptonomist.ch/2022/07/01/mica-officially-approved/

speculation, interest in on-chain security, and belief in a particular project[64]. A certain share of buyers eventually participates in further trading within the ecosystem.

When it comes to this category of assets, authorities face a dilemma. On the one hand, they have to draw a line between "what is traded on a crypto platforms", i.e. practically everything, and "what is a matter for regulators". On the other hand, some tokens that are not backed by anything and do not incorporate any claim attract interest from the general public (see Box I), which calls for at least some form of consumer protection.

Jurisdictions may eventually differ on the approach to this problem. The EU left Bitcoin outside of the scope of MiCAR, for the time being. ECB President Christine Lagarde recently called for a follow-up that would cover it, alongside crypto staking and lending. She did not provide specifics on which approach should be taken[65], although some suggestions may surface soon from discussions that are happening within various EU institutions.

In the US, Securities and Exchange Commission (SEC) Chair Gary Gensler repeatedly stated that Bitcoin is a commodity[66] and should therefore fall under the authority of the Commodity Future Trading Commission (CFTC). The bipartisan proposal for a Responsible Financial Innovation Act[67] goes in a similar direction. Commodity regulation, for the purposes discussed in this paper, would be less stringent compared to – say – securities regulation, yet it would still institute protections e.g. against insider trading. A decision is expected in the coming months, as agencies complete the reports required under the Executive Order of May 2022 (see Section 5).

All in all, assets that do not embed any claim may end up being the part of the crypto ecosystem least touched by financial regulation. They would obviously remain covered by general consumer protection law and criminal law. Financial education could play a key role in making potential users more aware of the high level of risk associated with these assets.

[64] One particularly interesting case, where the gap between the ecosystem and regulators is perhaps at its widest, is investment in native tokens of a blockchain on the back of a positive evaluation of the infrastructure's attractiveness for DApps. If there are many DApps on a blockchain, and they are consistently used, the native token will be in demand because it is necessary to pay for code execution. Barring the excessive issuance that plagues some projects, the token will appreciate. An investment driven by this reasoning is not a purely speculative play, yet the token does not confer any equity in the company building the blockchain – it is bought in anticipation of an increase in its use value, even if the coin is not legally classified as a utility token.

[65] See video: https://twitter.com/paddi_hansen/status/1539284632608329729?s=20&t=wQd1N_5adTu-hEqqkZVXeA.

[66] https://www.marketwatch.com/story/gensler-labels-bitcoin-a-commodity-as-crypto-prices-stabilize-11656340239?link=MW_latest_news

[67] https://www.congress.gov/bill/117th-congress/senate-bill/4356/text

5.2 Decentralization, anonymity, and censorship resistance

5.2.1 Why is there a problem?

If the crypto industry was wholly composed of centralized entities, from exchanges to lenders, from token issuers to hedge funds, regulation and enforcement would not be particularly hard. Existing laws would have to be adapted to take new technologies into account, but authorities would know whom to supervise and courts would know how to apportion liability in case something goes wrong. Nation states could also exert control on access to financial infrastructure for domestic and external power projection exactly like they do now, even in the most liberal of jurisdictions[68].

This version of the industry may still have advantages over traditional counterparts, e.g. it may still offer faster settlement of transactions, which in turn would reduce risks and costs associated with posting collateral. Indeed, traditional financial institutions are showing interest in buying settlement, treasury, and liquidity modules from crypto outfits, provided they comply with KYC and AML requirements[69]. A centralized crypto industry may also still enable small companies to go public at affordable cost, via tokenization of equity. NFTs issued by a centralized entity could still help optimize the management of intellectual property rights.

The list can go on but, according to a part of the crypto community, this would no longer be crypto the way it is meant to be. Gone would be the degree of cyber security implicit in the absence of single points of failure (SPOFs), i.e. individual components of a system whose disruption can compromise the system as a whole. Gone would be the so-called democratization of finance afforded by DeFi protocols, where trading fees are low, anyone can get credit provided they post enough collateral, and anyone can access complex, supposedly high-yield trades that mainstream institutions only offer to certain clients[70].

Most importantly, in a centralized version of the industry there would be less room for the anonymity of different types of actors. This is a bold red line for some. At the user level, individuals may not want to disclose their personal data to a centralized exchange more than they do a bank. At the blockchain level, anonymity of validators is what makes a network censorship resistant. If participants in the consensus mechanism are unknown, they cannot be forced to stop or change any payment, or message delivery, or smart contract execution[71].

---

[68] See e.g. D. A. Baldwin (2020), Economic Statecraft: New Edition, Princeton University Press.
[69] See for example Compound Treasury.
[70] For example, in the US only accredited investors can participate in certain trades. An accredited investor is identified based on income, wealth, and professional knowledge parameters.
[71] Censorship resistance can also be attained by anonymizing the transaction itself, so that even identified validator would not be able to tell what to censor, but this is technically more complex.

Censorship resistance is an essential correlate of *trustlessness*, one of the key aims of crypto at the time of its inception. Bitcoin was originally born to enable secure transactions between peers, without any need to rely on a trusted intermediary. Transaction integrity was to be guaranteed by a transparent algorithm alone, so that any abuse could be ruled out. Enabling any third entity to interfere with transactions deeply undermines this concept[72].

5.2.2 What can regulators do?

Of course, authorities cannot onboard all the community demands described above. Allowing for full anonymity of all crypto players would prevent effective supervision of the industry, enforcement of regulation, and taxation of any gain from trading tokens. Censorship resistance has costs in terms of crime prevention but, most importantly, is seen by some policymakers as a threat to national security. More generally, governments are unlikely to buy into the "rule of code" and "code is law" memes that are so popular in crypto, not least because of the failures encountered over the years.

There are, however, many actions that can be taken to preserve the positive contributions of the original crypto ethos without suspending the rule of law. They do require a degree of compromise, which already exists in some newer statutes.

When it comes to security, it is hard to argue against decentralization in an abstract sense[73]. Yet decentralization does not necessarily mean lack of legal accountability. While some crypto actors are keen on "non-governance", i.e. complete and immutable automation of protocols, in real life most decentralized projects are ultimately governed by someone – for example, members of a DAO (see Section 3.3.1). Legislating DAOs and similar arrangements may be the key to balancing relevant interests in this domain.

On the subject of democratizing markets, we should first note that consumer protection and antitrust remedies already exist in case of exploitative conduct on the part of financial institutions, new or old. Such remedies could be reinforced where needed.[74] Market access is already being

[72] Researchers at the Bank for International Settlements recently noted that, at least on some blockchains, validator nodes may have both the technical means and the economic incentive to meddle with transaction order, sometimes leading to temporary censoring – or delays in validation of transactions accompanied by fees that should have guaranteed priorirty execution. Part of the crypto community seem to accept this practice, seeing it as a component of the incentive schemes for validators. It is, however, dangerous and certain variations would be illegal, as a form of insider trading, if performed in traditional finance. See R. Auer, J. Frost and J. M. Vidal Pastor (2022), Miners as Intermediaries: Extractable Value and Market Manipulation in Crypto and DeFi, BIS Bulletin 58.

[73] As noted in Sections 2, 3 and 4, decentralization varies greatly across projects, not all smart contract code is well-written or regularly audited, and not all blockchains are equally secure. This statement is meant to refer to the conceptual construct, not the actual implementation.

[74] Where present, regulations that confine specific trades to the wealthy or to those with a certain professional status could also be softened.

expanded by a new generation of mobile apps, which allow for the trading of both traditional assets and crypto. DeFi may certainly help in going further, especially once the current UX/UI limitations (see Section 4.2.1) are overcome. Crypto maximalists, however, will have to accept that infinite reposting of the collateral and total absence of credit checks are just not compatible with the orderly functioning of any financial system.

The problem of user anonymity is difficult, but partial solutions can be found. For example, peer-to-peer transactions between ordinary crypto users may be allowed to remain anonymous if under a certain amount. At a more complex level, regulators could tap into the very extensive body of research on digital identity and encourage the use of identification technologies that reduce information leak to a minimum.

Such technologies would, at the very least, allow for anonymity of interested parties vis-à-vis anyone but authorities – no need to provide personal information to exchanges or any other company[75]. Even more sophisticated algorithms can be deployed, and more are likely to be available, given the fast pace of research in the field[76]. Those can be fused with suggestions from the industry, such as the recent proposal of soulbound tokens[77], or non-transferable NFTs that embed information about a single individual and could be used in identity and credential verification.

Validator anonymity and censorship resistance are the toughest problems to crack, especially when it comes to high-decentralization, high-automation blockchains. To name but one soft option, regulators could uploading their own smart contracts to such blockchains, to track transactions and raise red flags for suspicious operations. This is, however, not equivalent to being able to block a transaction – it is a choice that preserves the integrity of the ecosystem, at the cost of slow, *ex post* trudges through blockchain forensics labs and the courts.

One alternative option is demanding that developers embed certain controls in protocols, when the chain is at the still-centralized nascent stage, the way some addresses are already blacklisted on a voluntary basis by many protocol founders. When and if the chain becomes entirely decentralized, the updating of controls would have to be done directly by authorities, but the type of actions allowed

[75] This solution would still leave maximalists unhappy, but a world of total anonymity or sovereign identities (created on-chain by users, and not certified by any government body or any other group of users) is simply not possible within any existing legal frameworks, especially where finance is concerned.

[76] For a rewiew of this rich, rapidly growing literature see L. Ante, C. Fischer and E. Strehle (2022), A bibliometric review of research on digital identity: Research streams, influential works and future research paths, Journal of Manufacturing Systems, 62: 523-538, https://doi.org/10.1016/j.jmsy.2022.01.005.

[77] See E. G. Weyl, P. Ohlhaver, and V. Buterin (2022), Decentralized Society: Finding Web3's Soul, http://dx.doi.org/10.2139/ssrn.4105763

to them could be constrained from the beginning in a transparent way to prevent abuse.[78] This is a solution that partly sacrifices crypto values, but allows for faster enforcement of regulations.

5.3 A method of cooperation

The examples of possible compromise given in the sub-section above are just that – examples, given to offer a broad view of what is at stake. Finding actual answers to the regulatory dilemmas, complete with legal and technical specifications[79], will require authorities and the best part of industry to join forces in exploring solutions.

This is especially important because large knowledge gaps exist on both sides of the issue. As remarked in Section 3.3.5, some crypto players have a tendency to reinvent the wheel while overlooking decades of accumulated culture in finance, corporate governance, and the law. On the other hand, authorities may face a staffing challenge whereby they do not have enough people who simultaneously understand technology and regulation[80]. It is also very hard to find professionals with these interdisciplinary skills on the job market.

One preferred environment for cooperation may be that of regulatory sandboxes, which already exist on the premises on many national authorities and international standard-setting bodies. Although those take different forms across jurisdictions, the key idea of a sandbox is experimentation in a controlled environment for a limited amount of time – innovative companies are allowed to test their products under simplified regulatory frameworks, sometimes with limitations on market exposure. They receive constant feedback from authorities, who in turn have the opportunity of gauging the real-world impact of applicable rules. Other eligible venues may be innovation hubs, which may look like incubators and accelerators in some jurisdiction, and research centers in others.

In these contexts, crypto – *per se*, as in DeFi or DAOs, not as in blockchain technology embedded in traditional endeavors – has not been very popular. This is partly because of sheer newness, and perhaps partly because of mistrust on both sides. Some in the regulatory community may see crypto as inherently pernicious, while many in crypto see legal formality as a passé construct. A simple

[78] Another, even more radical possibility would entail forcing developers to hand over so-called admin keys, or credentials that allow for protocol modification. Aside from the fact that in some cases admin keys do not exist, this type of practice has been sharply criticized by information technology scholars in the wider context of giving governments backdoors to encrypted systems. Among the arguments presented is the multiplication of cybersecurity risks. One especially authoritative reference on this matter is Abelson et al (2015), Keys Under Doormat: Mandating Insecurity by Requiring Government Access to All Data and Communications, MIT Press.

[79] Standard-setting could be a very important object of cooperation in the technical space.

[80] The US recently outed itself in this sense, but the situation is unlikely to be different in other countries.

attempt at knowing each other better and finding a common language may go a long way. Many fronts that are already open within the industry could provide starting points for working together[81].

Cooperation in experimenting with new products and new rules would not eliminate the need for enforcement, which is necessarily one-sided, whenever illegal activity occurs. It might, however, considerably lower the level of latent conflict, resulting in fewer barriers to effective supervision for regulators, and easier access to an understanding of the law for those in the industry who want to comply. In turn, this would lead to reduced legal risk across the ecosystem, benefitting investors and users too.

6. Conclusions

The crypto industry is at a key junction. In the Spring of 2022, failure of certain large projects and adverse macro conditions combined to precipitate a systemic crisis. As asset prices plummeted, specialized funds went bust, and companies folded, ills that long plagued the sector – fraud, theft, inadequate risk management, bad governance – became all the more evident.

So is this the end of crypto, as announced by some? In this paper, we argue that it does not need to be the case. The crisis triggered a washout of bad actors, which is still in progress. At the same time, major jurisdictions around the world are deploying broad-ranging regulation for the ecosystem, finally allowing for an orderly functioning of a sector that was so far quite unbridled. Those new rules may be the bedrock on which good, innovative actors flourish. Indeed, without the distraction of crazy yields from shady schemes, many companies are already hard at work on product, especially but not exclusively in the infrastructure sector. They could do much more under the new laws.

There is, however, an important condition to be met. Regulators and the crypto industry have to learn how to cooperate constructively and creatively. They need to fill each other's knowledge gaps and experiment together with new products and new rules, lest legislation is quickly outpaced by

[81] During the Otherdeed sale (see Section 3.2.1.2), Yuga Labs required a KYC step – not based on wallet addresses, but on actual passports. The request was driven by economic reasons, not money laundering concerns. The point was ensuring that no individual could have more than a certain number of virtual land plots. More important under the political profile, KYC has also been advocated by teams developing decentralized products and DeFi professionals involved in token airdrops, to fight the plague of bots making tens of small automated transactions on new protocols just to show participation and get governance tokens for free. These examples show how part of the crypto world, and even some in its most privacy-oriented corners, acknowledges that KYC has a value. It does so for its own internal reasons, which may differ from regulatory ones, but there still is a point of convergence that should be leveraged. Authorities may reasonably argue that introducing legal, standardized KYC practices with safeguards against information leaks is better than letting companies handle sensitive user information, especially if done in a non-transparent way. This would not convince everyone, especially in some jurisdictions, but it could be a start.

technology or outwitted by players in bad faith. Since the two communities are not always on the best of terms, this will require determination and effort.

This paper aims at being a part of the effort, but papers alone will not do much. It is very important that protected environments such as regulatory sandboxes and innovation hubs, which already exist on the premises of several national and international financial authorities, are leveraged to the maximum in establishing a dialogue, creating a common language and working on real-world problems.

As a final caveat, cooperation does not mean smooth sailing, not all the time. There are substantial issues were crypto and any legal framework are at profoundly at odds. The big examples are tokens that do not represent any claim on any entity, anonymity, and censorship resistance, i.e. the technical impossibility to block any transaction on a permissionless blockchain. Attaining a compromise on many sub-domains of these problems looks possible, while on others authorities may have to prohibit behavior that some crypto enthusiasts consider sacred.