SUERF
The European Money and Finance Forum

SUERF Policy Brief
No 501, January 2023

Going native? How crypto technology may help regulators*

By Claudia Biancotti, Bank of Italy

Keywords: cryptoassets, financial regulation, blockchain
JEL codes: G18, O30, O38

The crypto industry suffered a prolonged crisis in 2022. It is now at a turning point, as lawmakers around the world deploy new statutes aimed at curtailing endemic fraud, inadequate risk management, and bad governance. This is a net positive for the ecosystem – without legal certainty, it cannot flourish. In this note, I argue that some crypto-native constructs may usefully complement traditional frameworks in the regulation of both crypto itself and the broader financial system.

1. Introduction

In November 2021, cryptoasset market capitalization reached an all-time high of $2.9tn[1]. One year later it hovered around $800bn as FTX, a large crypto company, filed for bankruptcy amidst fraud allegations. Even before FTX, 2022 had not been kind to the ecosystem. Other multi-billion projects had failed in suspicious circumstances, and high-profile hacks had become commonplace.

As this prolonged crisis unfolded, legislators accelerated their efforts to bring order to crypto. Comprehensive statutes were introduced or are being discussed in the European Union, the United States, and elsewhere.[2] This is a net positive for the space – legal certainty is essential if crypto is to deliver on its promises of enhanced digital security, empowerment of individuals, and improved market efficiency.

The process is, however, incomplete. In this note, I argue that some crypto-native constructs may usefully complement traditional frameworks in the regulation of both crypto itself and the broader financial system.

*This note reflects my own opinions, which should not be attributed to the Bank of Italy. I am on leave until the Fall of 2023. For the sake of brevity, I do not provide an introduction to crypto in the note. Interested readers may find a good starting point in Levine (2022), The Crypto Story. More references can be found in my paper What's next for crypto?

[1] Source for this and other market data in the paper: coinmarketcap.com.

[2] The Market in Cryptoassets Regulation (MiCA) will soon come into force in the EU. In the US, a 2022 presidential Executive Order mandated key agencies to explore regulatory issues. Multiple crypto bills are under review in Congress. The United Kingdom, Australia, Japan, and South Korea adopted or announced similar initiatives.

2. Key concepts

Before delving into the main argument, it is useful to recall why financial regulation exists, and how the crypto ecosystem is organized. The goals of financial regulation in market economies are: consumer and investor protection; financial stability; market efficiency and fairness; prevention of financial crime.[3]

In the simplest possible representation, the crypto technology stack features:

a) an infrastructure or protocol layer, including:
(a.i) layer 1s (L1), also called blockchains, where final settlement of transactions[4] happens;
(a.ii) secondary infrastructure, e.g. tools for scaling L1 capacity, optimizing transaction flow, moving assets across different L1s, and managing L1-application interactions;

b) an application layer, where applications as different as trading venues and video games exist.

Similar to what happens in traditional finance (TradFi), authorities have to evaluate trade-offs when choosing at which level(s) of the stack a regulatory goal is best pursued.

3. Recent regulatory achievements

The contemporary crypto ecosystem is composed of several L1s, with attendant secondary infrastructure, and a large number of applications. Products in all categories exist on a continuum that goes from "managed by a limited number of humans" (centralized) to "managed by immutable code deployed on a blockchain" (decentralized). Most existing laws focus on two portions of the application layer – centralized finance (CeFi) and centralized token issuance. This level of the stack matters for all regulatory goals mentioned above, but it is perhaps most relevant for consumer protection, given the high concentration of retail interest.

3.1 CeFi

CeFi is shorthand for identifiable, centralized entities that offer financial products and services. The best-known type of business is the exchange, originally a venue for purchasing and storing crypto, now evolved to offer a complex trading environment. This is the onramp to crypto for the majority of consumers. Other CeFi businesses include e.g. market making firms, over-the-counter trading desks, lenders, and hedge funds. A sizable portion of CeFi happens off-chain, meaning that internal transactions are recorded in private databases as opposed to a public L1. Where regulation is minimal, this opacity has facilitated criminal activity.

Laws protecting CeFi users have existed for a while in several countries, and now they are being reinforced significantly. For example, under the new EU crypto statutes, exchanges will have strong obligations with respect to the safekeeping of client funds. The legislation also mandates standards for governance and transparency, very problematic areas in the field.[5] New cybersecurity rules aim at guarding against hacks.

[3] This is a simplified version of the taxonomy in Armour et al (2016), Principles of Financial Regulation.

[4] Crypto technology is not meant for financial applications exclusively. In blockchain parlance, a transaction is a piece of information conveying any change in the state of the world. Here I focus on the financial system alone.

[5] Besides allegedly engaging in outright crime, FTX also had chaotic governance and no formal accounting system.

3.2 Centralized token issuance

Centralized token issuance refers to the process whereby an identifiable entity creates a digital asset on a blockchain. The token is then sold to the public or to selected parties. Trading tokens is risky, since most of them do not embed a direct claim on any entity, and determining their fair value is not straightforward. At best, buying newborn tokens can be likened to investing in early stage technology companies[6], in a liquid form that was generally not available to retail in the past. At worst, it means throwing money into the void. In the initial coin offering (ICO) craze of 2017, investors lost billions to projects that failed or did not exist.

Regulating tokens is hard, but lawmakers are finding solutions. For example, one bill[7] proposed in the United States posits that a token with certain characteristics should be classified as a security as long as it is centrally managed, and a commodity if it ever reaches a state of effective decentralization. Each of the two categories comes with a pre-existing set of obligations, and a supervision regime.

Extra attention has been directed to stablecoins, i.e. tokens whose value is supposedly pegged to a fiat currency or other real-world assets. Promises notwithstanding, crypto history is ripe with stablecoins that lost their peg and collapsed. Stablecoin use can impact financial stability and monetary sovereignty. The EU now mandates that stablecoins be backed by audited reserves, and envisions volume caps in some cases.

4. Outstanding challenges

4.1 Centralized applications

Several fronts are still open in CeFi. Some are specific to a type of service provider – say, what licensing regime should apply to crypto lenders? Other issues are cross-cutting, e.g. fair valuation of tokens on balance sheets and/or when pledged as collateral.

The key outstanding challenge in digital asset issuance is perhaps that of non-fungible tokens (NFTs), often retail-facing. Scams abound, yet the newness of NFTs means they remain largely unregulated.

Other unsolved issues exist in the centralized application space, such as conflicts of interest, competition, and privacy. Most of them can be mapped to TradFi or non-crypto tech equivalents. While adjustments in regulatory tooling could still be beneficial (see Section 5), no radical change in paradigm is needed.

4.2 Decentralized applications

Decentralized applications are sets of computer programs that, once published on a blockchain, run autonomously. No further developer intervention is needed – at times, it is not allowed. The programs are called smart contracts, and financial applications in this category are collectively known as decentralized finance (DeFi). User keep their tokens in self-hosted wallets, i.e. on their own devices, with no custodian.

[6] This analogy was proposed by Chris Dixon, a partner at the US venture capital firm Andreessen Horowitz, on the Web3 with a16z podcast.

[7] Lummis-Gillibrand Responsible Financial Innovation Act, introduced in the US Senate on July 6, 2022.

The simplest example is the decentralized exchange (DEX). Users wanting to exchange token A for token B send A to the address of the DEX contract. The contract calculates the price based on public algorithms, and sends B back to the user. All of this is visible on-chain. Another popular use case is overcollateralized lending.

During the FTX crisis, and others before, a mantra of crypto supporters was "DeFi unaffected". There is a measure of truth to this, but there are also important regulatory problems, especially with respect to preventing financial crime and ensuring market efficiency and fairness:

i) by the very nature of DeFi architecture, users are pseudonymous. There is no know-your-customer (KYC) or anti-money laundering (AML) functionality in most retail-facing DeFi contracts;

ii) there is also no way to condition user activity on financial literacy. DeFi often offers products on the high end of risk, such as leveraged derivatives trading;

iii) DeFi is a very young endeavor, with no significant volume before 2020, and many remaining imperfections in contracts leave markets open to manipulation;

iv) sometimes, applications that are presented as decentralized and autonomous are neither. Developers may keep so-called admin keys[8] giving them inappropriate access to funds, and even use decentralization as a smokescreen to cover other dubious activity.

4.3 Infrastructure

Permissionless L1s, or L1s where anyone can send and/or validate transactions, are at the heart of crypto.[9] The best-known examples are Bitcoin and Ethereum. While most users only interact with the application layer, any transaction they perform is ultimately settled on an L1. So, are L1s similar to central bank systems such as TARGET2 and Fedwire, the locus of final settlement in TradFi? Yes and no. They perform the same function, i.e. they provide certainty that a transaction happened. But they perform it in a very different way.

In crypto, a transaction is settled once it is written to an L1 by a group of independent, possibly anonymous peers, not a legal authority. The peers, called validators or miners, are responsible for the security and integrity of the network. They participate in a cryptography-based consensus process, which certifies that a given transaction is valid. The underlying code is public, and no intervention of trusted third parties is needed. This construct, called *trustlessness*, is the foundation of crypto philosophy.

L1s are the toughest challenge for regulators, for three reasons. One, even if they worked perfectly, they would prevent achievement of certain goals. L1s are intrinsically global, and they are built around the idea of censorship resistance – blocking transactions should be impossible. In the Summer of 2022, the US imposed sanctions on Ethereum addresses linked to North Korean hackers. US-based validators largely stopped settling related transactions. Since not all validators are in the US, this only resulted in delayed settlement.

[8] For more on this, see OECD (2022), Why Decentralized Finance Matters and the Policy Implications.

[9] There are instances of centralized (permissioned) L1s, e.g. enterprise blockchains. I will not focus on them here because they do not constitute a majority of the ecosystem, and also do not require particularly innovative approaches.

Two, L1s do not always work perfectly. For example, validators on many L1s have some leeway in choosing the order in which transactions are settled. This power can be used for market manipulation, e.g. a validator may delay a price-moving buy order on a token until they have bought the token themselves. This is known as the maximum extractable value (MEV) problem.[10]

Last, but definitely not least, there is a looming cybersecurity issue. An L1 is only secure as long as validators actually compete. Should they collude, they would be able to attack the blockchain and change the contents, e.g. allowing double spending of the same token. So far, no such attack was successful against any major L1, but signs of centralization creep are visible throughout the ecosystem. The consequences of a large L1 going down could be far-reaching, because all applications built on top of it would become unusable too.

Security issues also affect secondary infrastructure. Bridges that allow for the movement of assets across L1s have proven vulnerable to hacks. There is a degree of opacity in some application programming interfaces (APIs) provided by centralized companies, and other off-chain infrastructure components.

5. Leveraging crypto technology for financial regulation and supervision

Governments and international institutions are already at work on the challenges described above. While most initiatives build on traditional frameworks, some are starting to incorporate the idea that crypto-native tools may be used in regulation and supervision.[11]

Regulators and crypto developers have more in common than they think. Both sides aim at making the financial system more transparent, accountable, accessible, and fair. Synergies are possible, despite different starting points. The pseudonymous author(s) of the Bitcoin white paper thought that legal frameworks could not meet these goals, so they introduced trustlessness. The construct works, in a mathematically verifiable sense, and it can help regulators too. On the other hand, thirteen years of crypto history show that code alone is not enough to prevent malfeasance. This is why laws, authorities and courts continue to be needed.

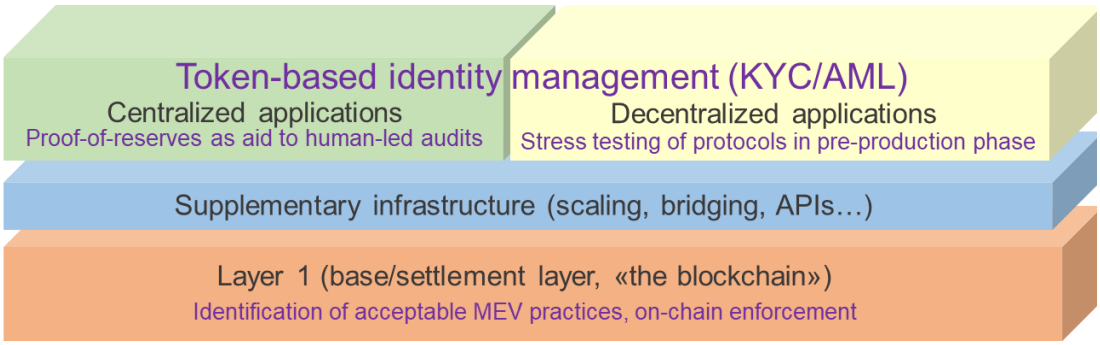
The adoption of crypto tools in regulation is not without challenges. Knowledge gaps need to be addressed in the industry and regulatory agencies alike. Caution is required, because most of the technologies involved are still experimental. Finally, the ideological divide is not entirely bridged, although it is not as deep as it used to be. A method of smart compromise may be useful – say, crypto stalwarts will have to accept that full anonymity in finance is a no-go, yet regulators may choose to favor privacy-preserving solutions over alternatives. In some jurisdictions, this would mesh well with existing data protection statutes.

In the following, I provide a few examples of possible regulatory use of crypto-native instruments. These are just sketches, and should not be read as draft statutes or technical blueprints. In the crypto community, research is already underway in each of the areas, but not often in connection with regulation.

[10] For an introduction to MEV on the institutional side, one can refer e.g. to 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. On the industry side, see e.g. this episode of the 0xResearch podcast, from crypto research and media company Blockworks.

[11] For example, the EU recently published a tender for a Study of Embedded Supervision of Decentralized Finance.

Figure 1: Examples of regulatory interventions (in purple) leveraging crypto technology across the stack



a) KYC/AML. Currently, an entity seeking to access regulated financial services (traditional or CeFi) needs to go through KYC/AML verification. The process is repeated whenever a service provider is added. This results in dispersion of sensitive personal data. Meanwhile, DeFi users remain anonymous, with increased risk of illicit activity. Regulators could condition access to any financial service, centralized or not, to the possession of a non-tradable token, issued e.g. by a public authority, which attests to successful KYC/AML verification[12,13]. Zero-knowledge proofs[14] could ensure that service providers only get access to the information they need, and not to any other data stored in the token. In turn, the token issuer could be algorithmically bound to only use the information gathered for certain purposes;

b) Stress testing. The open-source nature of smart contracts means that anyone can try to break them. This has been exploited for criminal ends, but also opens an opportunity for legitimate stress testing in pre-production phase. For example, supervisors could verify whether a DeFi lending protocol has sufficient safeguards against market manipulation, or the accumulation of bad debt in case of liquidation cascades. More generally, crypto's "Don't trust, verify" habit – a collective red-teaming of sorts – is healthy from a regulatory point of view, both in abstract terms and because of the accumulation of knowledge and data it created;

c) Balance-sheet audits. After the 2022 collapses, there was a rekindling of the debate on proofs of reserves (PoR). Those are cryptographic constructs which, say, an exchange can leverage to credibly show that they still have customer funds. Current implementations are imperfect[15], and even in the future it is unlikely that algorithms alone can prove the solvency of a company. PoR may still be useful to supervisors as a time-saving aid for human-led audits;

d) MEV control. This is a hard problem, like most in the L1 space. It is also a good example of complementarity between regulators and the industry. Crypto developers have a general sense that some forms of MEV extraction are good, e.g. arbitrage across exchanges resulting in price alignment. Other MEV practices, like the front-running of user trades mentioned in Section 4, are frowned upon. Sophisticated experiments are being deployed to enable the former and prevent the latter, not without risks[16,17]. The sheer amount of human capital involved suggests that a solution will eventually be found, but it should not rely solely on the community's evaluation of what is acceptable. Regulators should lead the way and indicate where the hard limits are, mapping concepts such as market manipulation, insider trading, and anti-competitive behavior to specific actions in the MEV world[18]. ■

[12] KYC portability is not new and can be solved through other means. See e.g. the literature on verifiable credentials.

[13] For a discussion of tokens of this type see for example E. G. Weyl, P. Ohlhaver, and V. Buterin (2022), Decentralized Society: Finding Web3's Soul, mimeo.

[14] Zero-knowledge proofs were born in the 1980s. For applications in crypto ecosystem, see here.

[15] See V. Buterin (2022), Having a Safe CEX: Proof of Solvency and Beyond for an example of advanced research.

[16] For a technical discussion in the context of Ethereum, see here.

[17] See here for an overview of Flashbots, the market leader in this area, and here for market dominance statistics.

[18] MEV could also provide an ideal starting point for a reflection on enforcement in global permissionless L1s. Compared to the case of sanctions mentioned in Section 4, it is not as politically charged, and could catalyze broader agreement.

About the author

Claudia Biancotti *joined the Research Department of Banca d'Italia in 2002. She is interested in how digitalization is changing the economy and society, with a focus on security implications and shifts in power balances at the national and international level. Her latest work focuses on cybersecurity, the rise of decentralized systems and cryptoassets, and dual-use technology. Claudia was a visiting fellow at the Peterson Institute for International Economics in Washington, DC in 2018-2019, and a seconded national expert at the European Central Bank in 2009-2010.*