University of Amsterdam

IViR

Trust in Context : The Impact of Regulation on Blockchain and DeFi

Balazs Bodo

Primavera de Filippi

Amsterdam Law School Legal Studies Research Paper No. 2022-07

Institute for Information Law Research Paper No. 2022-01

Trust in Context :
The impact of regulation on blockchain and DeFi

Balazs Bodo (UvA) - bodo@uva.nl & Primavera de Filippi (CNRS) - pdefilippi@gmail.com [1]

'The Impact of Emerging Technologies on Trust and Governance'

(*special issue of Regulation and Governance*)

Abstract: Trust is a key resource in financial transactions. Traditional financial institutions, and novel blockchain-based decentralized financial services (DeFi) rely on fundamentally different sources of trust and confidence. The former relies on heavy regulation, trusted intermediaries, clear rules (and restrictions) on market competition, and long standing informal expectations on what banks and other financial intermediaries are supposed to do or not to do. The latter rely on blockchain technology to provide confidence in the outcome of rules encoded in protocols and smart contracts. Their main promise is to create confidence in the way the blockchain architecture enforces rules, rather than to trust banks, regulators, markets. In this article, we compare the trust architectures surrounding these two financial systems. We provide a deeper analysis of how proposed regulation in the blockchain space affects the code- and confidence-based architectures which so far have underwrote DeFi. We argue that despite the solid safeguards and guarantees which code can offer, the confidence in DeFi is still very much dependent on more traditional trust-enhancing mechanisms, such as code governance, and anti-fraud regulation to address some of the issues which currently plague this domain, and which have no immediate, purely software-based solutions. What is more, given the risks of bugs or scams in the DeFi space, regulation and trusted intermediaries may need to play a more active role, in order for DeFi to gain the trust of the next generation of users.

Keywords:

Trust, trustworthiness, blockchain, decentralized finance, finance, institutional analysis, regulation

Acknowledgements:

This research is funded by the European Research Council (ERC) under the European Union's Horizon 2020 Research and Innovation Programme (Grant Agreements No. 759681 and No. 865856).
We would like to acknowledge the thoughtful comments of Judith Donath who kindly reviewed our paper prior to submission.

Conflict of Interest: None.

[1] Author order alphabetical, equal contributions.

Trust, confidence, and trustworthiness - an infrastructural approach

Trust is a wide ranging topic, which has enjoyed sustained attention in multiple disciplines, from cognitive psychology, anthropology (Coates, 2018), economics (Fukuyama, 1995; Zucker, 1985), via game theory or philosophy (O'Neill, 2002), to sociology (Luhmann, 2017; Giddens, 1990), history (Greif, 1989, 1994) or computer science (Danezis, 2014; Huurne et al., 2017; McKnight et al., 2002, 2011; Nickel, 2013). These different disciplines address different aspects of trust relationships. Psychology, game theory, and Human Computer Interaction focus on the trustor, and his/her capacity or willingness to trust. The main concerns of these studies is the following: What characteristics of the trustor help or inhibit the emergence of a trusting stance? Other disciplines, such as law, computer security, ethics or philosophy are often more concerned with the characteristics of a potential trustee, and his/her perceived and actual trustworthiness. The main questions in this domain address issues like the transparency, accountability, reliability, competence of a trustee, and the ways to improve these characteristics in a (human or non-human) counterparty. Finally, sociology, history, and cultural anthropology are looking at the social, economic, cultural, political, or institutional contexts in which trust relationships emerge (or not). Why is public trust higher in some countries than in others? How do communities (such as in ancient trade networks) keep track of reputation? What kind of institutional frameworks provide the necessary prerequisites for trusting relations?

For the purposes of this article we define trust as one's willingness to cooperate and interact with someone in face of the vulnerabilities and risks related to the actions of that party. Trust relations require the trustor to voluntarily engage into a position of vulnerability, because the agency of the trustee means that he or she is in the position to cause harm to the trustor. Trust is then the resource which helps the trustor cope with the uncertainty created by the agency of the trustee, and act with positive expectations about the future outcome of the interaction. Such a leap of faith depends on the individual characteristics of both the trustor and the trustee, as well as on the environment which is able to provide familiarity, safety nets, confidence or instruments of control for the trustor, and may thus contribute to increasing the perceived trustworthiness of the trustee. *Our focus in this article is on this trust environment: the conditions which facilitate engagement and cooperation in face of such risks.*

Most of the trust literature considers the trustee to be a human being, for reasons that agency is most clearly associated with individual human action. Institutional sociology, however, also considers trust in broader systems, such as the state; various institutions, such as the judiciary, the police, the press; or processes, such as the democratic process. More recently, trust questions have been raised vis-a-vis complex techno-social systems, such as Artificial Intelligence, digital platforms, or, as in our case, blockchain based systems. (Bodó 2020) This emerging interest in systemic trust is the result of the realisation that such systems do possess some form of agency, which cannot be exclusively attributed to particular individual humans who constitute such systems, but rather, to the rules, processes, design, governance, which define the socio-technical systems, their capacity to do good or harm, their reliability, predictability, their integrity, and accountability.

The trust in institutions, however, poses a difficult and complex challenge for the study of trust relationships, because institutions fulfill a double role: they provide the contextual framework to manage and facilitate the establishment of trust relationships, and, in doing so, they present themselves also as potential trustees. We define the formal and informal institutions in which trust relations are embedded as "*trust infrastructures"* whose role is to produce or maintain trust according to different logics. We distinguish, in particular, between three major typologies of trust infrastructures: interpersonal or communal trust networks; public trust infrastructures; and private trust producers. (Bodó 2021). These trust production infrastructures differ in their scope, mode of operation, governance, inclusion/exclusion rules, and the nature of trust they offer, but they all contribute to creating an environment in which trust-based interactions can emerge. *Communal trust production logics* produce trust by a group for the members of the group, defined by close interpersonal relationships, such as familial, professional relations, shared values, ideology, epistemic systems, shared past or experiences. *Public trust infrastructures* are predominantly provided by states to facilitate the co-existence and collaboration of individuals across the boundaries of communal trust networks. Incorporating larger, more heterogeneous populations they create institutions such as schools, public administration, media, to create the preconditions of trust (such as familiarity, security, predictability) and make them available to the public at large through public funding. *Private trust producers* offer conditions of trust only to those who specifically pay for it. Their business model is to charge a fee in exchange for trustworthiness signals and safeguards. Brands, banks, lawyers, credit rating agencies and other private enterprises belong to this last category. As we'll discuss it later in more detail, recent technological developments, such as AI, blockchains, and platforms also constitute private trust producers, which create conditions of trust-necessitating interactions, usually in exchange for a fee. It is increasingly apparent that these techno-social trust infrastructures themselves have their own agency, and so they can create vulnerability and risks for those who decide to engage with others through them. Trust infrastructures facilitate trust relations, but they also face questions of trust and trustworthiness themselves.

When it comes to various forms of relationships which involve risks, we distinguish between *trust* and *confidence*, as two closely related, but somewhat distinct logics that both contribute to establishing expectations about the future. In trust relations, the agency of the trustee is acknowledged by the trustor and is in the foreground of trust-related decisions, because the trustee can use this agency to potentially cause harm to the trustor. On the other hand, in a situation of confidence, agency considerations sink into the background (Keymolen 2016), because, for example, the agency of the trustee is limited, or because the expectations about the behaviour of the trustee have consolidated without the need to be questioned in each and every interaction. According to Luhmann (2017), in a situation of confidence, an individual will engage in a particular course of action without even considering the fact that things might not go as expected. There is no sentiment of risk or vulnerability towards a third party.

To illustrate the points we made so far, let us consider the following example. When visiting a doctor, one may trust one's doctor not only because of personal relationships, but also because one has confidence in the fact that she possesses the necessary skills to properly diagnose a disease and identify the most appropriate cure for it. The former is a relationship of interpersonal trust; whereas the latter is a relationship of confidence. Yet, one's confidence in the doctor's ability to identify the right cure for an illness is produced by one's trust in the health institutions that have conferred her the license to operate, as well as the confidence one holds in the broader system of science which has contributed to the elaboration of these cures. It also builds upon the trust one has in the systems of monitoring and enforcement which ensure that, if the conditions on which this confidence rests is violated, appropriate countermeasures will be taken (for example, with the revocation of the doctor's license). Accordingly, the personal relationship with the family doctor is embedded in communal trust infrastructures and produces trust vis-a-vis the doctor's intentions and personal abilities. The confidence in the professional excellence, benevolence, and integrity of the doctor is largely produced by public trust infrastructures: the medical education and the public health care system, which qualifies healthcare professionals. There are also private trust infrastructures at play: the predominantly private, market competition and profit-driven activities of pharmaceutical companies produce trust in their products and services through a predominantly private logic.

It is clear that these three logics of trust are somewhat independent, but nevertheless closely intertwined. Private trust production infrastructures are embedded in public ones regulating their activities, and providing services such as enforcement, public prosecution, and courts. Some trust institutions, such as scientific research are often hybrid: as some research is provided by public institutions, but it is also done by private ones. This means that the trust which emerges in the concrete situations is defined, albeit in each individual case to a different degree, by a mixture of these different logics. A patient's trust in a particular doctor suggesting a particular remedy may be a result of his/her personal relationship with the person, his/her degree of confidence in the health system, and his/her level of trust or distrust in the state, in experts, or science in general. The COVID epidemic highlighted the complex interplay between these different dimensions of trust and their relationship. With the fragmentation of epistemic, political, societal frameworks, one can now choose in which context one has more trust or confidence: in science advocating masks and vaccines, or maybe in religious, or libertarian opinion leaders, certain politicians, or some online influencers and moral entrepreneurs advocating horse-dewormer drugs and other non-conventional remedies. This choice of context is closely related to the trust or confidence one confers in other systems: in the state, in politicians, in science; or in domains more directly related to health care choices, such as in the professional capacity, goodwill, integrity of healthcare providers, and individual doctors.

In this contribution we'll try to disentangle the implications that separate contexts may have on both trust and confidence in the investment sector, by comparing the more traditional, trust-based and institutional environment, with the novel, trust-minimizing, blockchain based environment.

Trust *in* and trust *by* blockchain-based systems

Blockchain based systems have emerged in the context of the loss of trust in the global financial system after the 2008 financial crisis (Werbach 2018, p. 39). As we describe in more detail later, all three typologies of trust infrastructures which underwrote the financial system simultaneously failed: state bodies failed in their duties to monitor financial institutions and enforce financial regulations; private parties turned out to be unreliable, trying to maximize short-term profits at the expenses of long-term sustainability; and, as a result, peer trading networks froze up. In that context, blockchain systems emerged as a new financial infrastructure that operates outside and independently of these pre-existing logics, with new idiosyncratic relations that—allegedly—no longer require trust . As opposed to the traditional trust infrastructures in the financial systems, which are designed to produce more trust in the system, blockchain-based systems are described as *trustless* infrastructures—or *confidence machines* (De Filipi & al., 2020)— aimed at producing confidence rather than trust. Due to their global and decentralized nature, blockchain-based systems are largely disembedded from local social, economic, political, and legal contexts.. These systems are now mature enough to provide an alternative framework to some of the key functions of the global financial system (such as value transfer and investment); using an automated (and autonomous) technological infrastructure to replace some of its individual institutional constituents (such as banks, and other financial institutions) and the people who work there.

Yet, despite their characterization as a trustless technology, blockchain-based systems cannot entirely eradicate the need for trust, because these systems are ultimately developed and governed by human beings. Hence, design faults, bugs, and mistakes, but also incompetence, fraud, and criminal activities have highlighted the need for asking whether different implementations of these systems are to be trusted, and the potential costs of misplaced trust in them.

Rather than sticking to a narrow definition of trust (which might suggest that blockchain systems are 'trustless'), we need to acknowledge the fact that the trust environment around blockchain-based financial instruments is a highly complex one. It consists of several systems, with very different trust properties. To be sure, the technological design of many such systems is based on verifiably trust-minimizing design solutions, intended to eliminate the need for any trusted party responsible for the operations of the technical system. Yet, the human components of these systems, and the vulnerabilities they introduce, cannot be easily engineered away. Besides, crypto-assets and decentralized finance (DeFi) have gained enough prominence to warrant a flurry of regulatory activities—in the US, the EU, and elsewhere—with the goal of protecting both individual holders of crypto-assets and financial markets from risks not covered by other regulatory frameworks, such as consumer protection, and laws applying to financial service providers. In that context, the European Union justified its crypto market regulation proposal by stating that a "lack of an overall Union framework for crypto-assets can lead to a lack of users' confidence in those assets". (Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-Assets, and Amending Directive (EU) 2019/1937, 2020).

Given that blockchain innovation was fuelled by a general distrust in the state apparatus and in the financial system, it is important to ask whether such top-down regulation will be able to achieve its goal, increasing confidence in the decentralized crypto-economy, or on the contrary, whether the willingness, and ability of regulators to extend their powers to this domain will lead to a loss of confidence in such systems.

The answer to this question is far from being straightforward. As a general rule, for the first half of the history of blockchain based innovation, individual users' willingness to use blockchain-based systems, decentralized exchanges, crypto-tokens, Distributed Autonomous Organizations to invest their wealth or transact with each other was not directly linked to the existence of an applicable regulatory framework. Users engaged with these allegedly trustless systems largely because they had confidence in how these systems were designed from a technical and game-theoretical point of view; they believed that trust was largely irrelevant. Only recently it has become more apparent that the confidence in the technical design of these system ultimately depends on specific layers of trust in a multiplicity of actors, such as the developers responsible for coding the platforms, the miners in charge of maintaining the technical infrastructure, the market players capable of manipulating the value of the associated crypto-assets. As trust comes back into the picture, technology and game theory alone are no longer sufficient to ensure confidence in the proper operations of the system. The role of regulators (acting at the local, national and European level) also becomes more relevant, as they are in capacity to influence the activity of these actors, in ways that may both improve or reduce the confidence of these systems.[2]

In the remainder of this paper, we'll compare the trust logics of traditional finance with those of decentralized finance, to highlight the different types of trust and confidence relations that one must enter into when making an investment decision in the context of DeFI, as opposed to in the traditional financial systems. Through this comparison, we will demonstrate the impact of the contextual factors on the nature of confidence and trust relationships within, and across these environments.

Trust infrastructures in traditional and Decentralized Finance

A. Trust production in traditional finance

A financial investment can involve substantial risks, and can cause considerable amounts of financial and non-financial harm, therefore it often needs substantial amounts of trust on behalf of the investor. There are many ways the investor trustor can be disappointed by the many potential trustees in a transaction: the investment professional may steal the money, or they can lie about the risks and benefits of an investment opportunity[3]; the financial institution may act against the best interest of its clients[4]; or it simply may go bankrupt[5]; confidential financial information may get hacked or leaked, information asymmetries may favor some investors at the expense of others.

The traditional financial system relies on the interaction and proper functioning of a number of communal, public and private trust infrastructures to manage such risks by making them tangible, transparent, quantifiable and hopefully avoidable. In the following sections, we'll provide a brief schematic of the trust infrastructure in private investments as provided by the current banking system. The trust infrastructure consists of three major, institutional components: 1. Intra firm, control-based governance mechanisms;

[2] As a recent Europe-wide survey on the regulation of crypto-currencies suggests#, different countries have rather divergent views on who (the EU versus their national governments) they think is the most trustworthy agent to regulate the crypto domain, which seems to depend on their general attitudes towards EU financial institutions. (Walsh, 2021)

[3] See the Bernie Madoff case. (Yang & Kay, 2021)

[4] See Robin Hood stock trading app selling customer orders to Wall Street trading companies, and being fined for prioritizing the interests of the latter to the former.(Financial Industry Regulatory Authority, 2019)

[5] See, for example the Lehman Brothers Bankruptcy: (Wiggins et al., 2014)

2. Market based instruments, relying on transparency and insurance; and 3. public instruments, providing situational normality through regulation, and accountability through enforcement.

1. Intra firm instruments

The providers of financial services, mortgages, and investment opportunities are private entities, which face conflicting short term (profit) and long term (stability, growth, success) objectives. The short term goals would encourage businesses and employees to produce as much profit as they can even if it comes by dubious means: being dishonest about the risks and benefits of the investment they provide, lying about their own professional abilities, financial stability, and organizational capacity to manage the investments they receive. While fraudulent activity can be quite profitable in the short run, as countless fraudsters, snake-oil sellers, Ponzi scheme organizers can attest, they all end badly in the long run. To avoid such an outcome, respectable financial institutions have many tools at hand to make sure that individual employees and the organization as a whole can be trusted. These include clear internal rules that are enforced by multiple layers of management; employee remuneration systems which incentivise responsible behavior; compliance departments acting as internal watchdogs; and an independent board of directors that holds top management accountable to shareholders. While these instruments are predominantly private, as they only apply within the firm, they are prescribed by, thus embedded in public trust infrastructures.

The knowledge that an organization has solid internal mechanisms to secure the operations, supervise the employees and align the incentives of the management can increase the perceived trustworthiness of the organisation, and in turn create the conditions of trusting the products and services of that firm.

2. Market based instruments

Markets constitute an additional infrastructural layer which can contribute to increasing both trust and confidence in financial products. With regard to trust, the investment products offered by individual firms are competing on an open market, so that potential investors can compare them in terms of risks and profits. As such, markets, at least in their pure, theoretical form, provide both intrinsic and extrinsic trust producing mechanisms. The former assumes that market entities also compete in the trustworthiness dimension - they must factor trust in their offering, otherwise customers will walk away to a more trusty supplier[6]. The latter assumes that markets, through the price mechanism, are able to collectively and distributedly assess and reveal the risks associated with each traded commodity, thus providing

[6] The regulatory approach of the neoliberal economic order before 2008 was heavily based on this assumption. Alan Greenspan, the chairman of the Federal Reserve Board before the crisis, admitted that his approach to overseeing the financial markets was hands-off, because he believed in the self-regulating power of markets. Yet, this approach has serious limitations. In the subsequent congressional hearing he evaluated this approach as follows: "I made a mistake in presuming that the self-interest of organizations, specifically banks and others, were such that they were best capable of protecting their own shareholders and their equity in the firms. [,,,] So the problem here is something which looked to be a very solid edifice, and, indeed, a critical pillar to market competition and free markets, did break down. And I think that, as I said, shocked me. I still do not fully understand why it happened and, obviously, to the extent that I figure out where it happened and why, I will change my views. If the facts change, I will change." (The financial crisis and the role of federal regulators, 2008)

information on its corresponding trustworthiness.[7] Both of these mechanisms are supported by the activities of third party actors, such as credit rating agencies specialized on the individual and independent assessment of investment products, which they rate according to risk. Participants in the bond and stock markets also do their individual risk assessment and these get reflected in the cost of debt, and share price of the individual financial companies.

With regard to confidence, specialized financial instruments, such as the notorious credit default swaps, and other financial derivatives can serve as insurance against risk, and an insured risk induces confidence. Risk can also be commodified, and therefore efficiently allocated to those with the greater tolerance for risk and disappointment. In practice, this means that even if a financial product is revealed to be of a certain risk, that risk can be hedged. These trustworthiness signals and safeguards are predominantly produced by private actors, either through the individual services they provide, or through their market-coordinated activities. Such trust or confidence is offered for a fee, by these specialized trust producing agents. Again, both individual private trust producers, and markets in general are embedded in public trust infrastructures, and rely on internal, communal logics of trust production to demonstrate and safeguard the trustworthiness of these particular private logics.

3. Public (government-based) trust infrastructures

Another fundamental infrastructure that contributes to increasing trust in the financial sector are the public, state-provided infrastructures. These include comprehensive regulation that prescribes everything from the content of information investors have to have in relation to any investment opportunity offered on the market (called brochures), via capital requirements, to reporting obligations for publicly traded companies. Complex and multilayered institutional networks monitor the firms, and enforces the rules, including financial and market authorities, central banks, and supranational institutions, such as the IMF or the Basel Committee. The state investigates and prosecutes financial crimes, and resolves conflicts through the courts.

***

Taken together, these three types of infrastructures are attempting to improve the trustworthiness of financial service providers (along with their employees, and the products and services they provide) by strategically managing distrust (Sztompka 1999). Because none of the stakeholders can be trusted, it is necessary to create a system of oversight and accountability at all levels: the management watches the employees; the directors watch the managers; the markets and regulators the firms; the legislative and executive branches of the government watch the market; and the judicial branch watches the legislative and executive branches, etc. This is the paradox of institutional trust: individual actors are trusted because they are treated as untrustworthy, and there is a system of safeguards and guarantees designed to manage this distrust, with a series of “watchers watching the watchers” to create a circular system of accountability. Of course, this approach is not failproof: it creates additional layers of trusted actors in order to lower the chances of misbehavior by existing trustees—detecting misbehavior through monitoring, and assigning penalties while providing a safety net for the trustors if trust were nonetheless to be breached..

[7] This assumption has also been questioned in the wake of the 2008 crisis. Ben Barnake, the Chair of the US Federal Reserve during the crisis, has pointed out the detrimental role of credit rating agencies which provided an inaccurate or non-independent review of financial instruments. (*Statement by Ben S. Bernanke Chairman Board of Governors of the Federal Reserve System*, 2010)

This institutional approach is highly effective, but as the 2008 financial crisis has demonstrated, under certain circumstances, it can still break down. In particular, the forensic analysis of the events in 2008 highlighted the fact that too much confidence in markets, and the belief that the rational self-interest of individuals and financial firms would automatically lead to prudent behavior was unfounded. The public sector trust infrastructures—most prominently the legislative branch which relaxed rules separating investment and retail banking activities, and the oversight which the Fed was supposed, but failed to exercise —led to the systemic collapse of this trust infrastructure: the failure of a few led to a cascading failure of all trust producing mechanisms.

The production of trust through such institutional infrastructures is extremely costly. One experimental study (Davidson at al. 2018) estimated that a third of the US workforce in 2010 was occupied to produce systemic trust. The study estimated the percentage of time or effort spent on upholding trust in selected occupational categories, such as management, sciences, healthcare, sales, farming, etc. Though these percentages were established subjectively by the researchers, the study showed that trust production is an important economic activity. And, as the 2008 crisis has shown, the lack of trust is even more costly—as without it whole economic domains can shut down essentially overnight.

Trust infrastructures in Decentralized Finance

Decentralized finance (or DeFi) provides an alternative solution to the inefficiencies and mistrust in the financial system. As described above, the proper operation of the traditional financial system relies on the strategic management of distrust by institutions, using laws and regulations to ensure transparency and accountability (e.g. by requiring companies to engage in annual audits and reporting, or by prescribing the issuance of investor brochures). Yet, this model requires an additional infrastructure of trust to supervise the actors or intermediaries responsible for ensuring the proper application of these regulations (e.g. auditors and regulatory agencies), which must themselves be subject to a particular type of oversight. DeFi attempts at solving the problem of distrust through openness, transparency and verifiability: by promising that anyone can look at the code of the financial infrastructure (assuming that they understand the relevant programming language) in order to understand exactly how things are intended to operate. Instead of relying on intermediary third-parties, ie. fiduciary operators with their internal processes, DeFi applications operate in a decentralized manner, with rules encoded into the technical infrastructure of a blockchain network (De Filippi & Hassan 2018). Financial transactions are executed via smart contracts, in a secure and verifiable way, thereby eliminating the need for other forms of financial intermediaries or trusted third parties, such as custodians, escrows, or central clearing houses.

Most DeFi protocols can be distinguished from traditional finance according to three core variables. First, they are **permissionless**: anyone can deploy a financial application without the need to request authorization from anyone, and—once deployed—the application can be accessed by anyone. This stands in contrast with traditional financial applications, which are highly regulated. Second, they are characterised by a significant degree of **capital inefficiency:** given that there are no gatekeepers to ensure against counterparty risk, DeFi protocols are heavily collateralised. This means that capital remains captive within these protocols, resulting in significant opportunity costs. These costs can however be remediated by the third key characteristic of DeFI: **composability**. To the extent that they rely on the same blockchain infrastructure as the settlement layer, different DeFI protocols can be easily interconnected to one another in order to implement complex financial instruments, e.g. using decentralized lending protocols to achieve leveraged positions from captive capital.

Hence, while both centralised and decentralised finance treat their constituents as untrustworthy, they deal with the problem of distrust in two radically opposite manners. Centralized finance relies on an extensive and multi-layered *trust* infrastructure to ensure the proper working of the system, by recreating trust through a complex system of regulation, competition, supervision and oversight. Decentralized finance also operates on the premise that no one is trustworthy, but instead of trying to re-establishing trust, it focuses instead on the implementation of a *confidence* infrastructure. The "trustless" nature of the blockchain infrastructure guarantees that every aspect of a DeFi protocol will operate precisely as stipulated by the code, thereby ultimately replacing trust with confidence (De Filippi & al., 2020). This is, however, based on the assumption that most people interacting with these systems do effectively believe (or trust) that the code will operate exactly as expected, leaving no room for any possible deviation or third-party intervention—which, as history has shown, is not always a valid assumption (Mehar & al., 2019). Hence, in order to properly understand how DeFi generates confidence, we also need to investigate its relationship to trust. This requires identifying who are the actors involved in the larger DeFi ecosysteme, and how they contribute to increasing or decreasing the overall reliability of the system, by intervening both at the trust and confidence level.

1. Blockchain and smart contracts infrastructure

All operations undertaken within a DeFi protocol are governed by the underlying blockchain protocols and smart contract code. These operations are both self-executing and deterministic, so that users can rest assured that, whenever a particular condition is fulfilled, the codified outcome will be triggered. These operations are also irreversible, meaning that once a transaction has been recorded on a blockchain, it cannot be modified and it becomes almost impossible to delete it without a coordinated action from the whole network. Finally, these transactions are publicly visible and verifiable by anyone who has access to the blockchain network. This means that no one can claim to have executed a transaction that does not appear on the blockchain, or—vice versa—not to have executed a transaction that has been recorded on the blockchain. These three features combined (guarantee of execution, irreversibility, and traceability) are intended to provide a high degree of confidence in the system, enabling people who do not trust each other to transact with one another without the need to rely on any centralized intermediary or trusted authority. The trust infrastructure of the traditional financial system is replaced by a set of technological guarantees which create confidence in the operations of a technological system.

However, it is worth noting that, while people might build strong expectations about the workings of a particular blockchain-based system, these expectations might not always nor necessarily coincide with what the system actually does. The theoretical safeguards of confidence suffer from a number of limitations. The intricacy of these systems can lead to significant complexity, both at the individual smart contract level[8], as well as at the level of this complex, interconnected system.[9] The transparency of the individual smart contract source code can provide some defence against bugs. But in practice, this safeguard is far from perfect: Zhou et al (2018) found that more than 77% solidity smart contracts, managing 31.6% of the transactions, and holding $3 B USD in value have not released public source codes. Even if transparent, a complex smart contract code may be difficult to understand and verify for users. Those who can read and understand the source may decide to personally study and verify the various constituents of a particular smart contract, thereby forming their expectations based on a first-hand familiarity with the system. Yet, bugs are easy to miss even in simple smart contracts, not to mention many DeFi applications rely on a complex network of smart contracts, implemented by different people, making it difficult for a single person to assess the exact working thereof. Those who do not understand the source code, or who have chosen not to personally engage in the analysis of the smart contract, must base their expectations of what that system does on a second-hand interaction, relying on the information provided by the developers of the system, third-parties describing the operations of a smart contract in a more human-understandable language (e.g. in a white paper, or youtube video), or professional code auditors. In recent years a multimillion dollar code audit industry emerged, whose sole role is to provide independent security audits for this sector. Yet, even such audited contracts have been hacked leading to hundreds of millions of dollars worth of losses for investors.[10] According to the research firm Elliptic, as of November 2021, "DeFi users and investors have suffered more than $12 billion in losses due to theft and fraud" (Elliptic Research, 2021).

Hence, confidence in DeFi protocols ultimately depends on trust in the external systems on which these protocols rely. The confidence in the technical design of a DeFI application is a function of investors' trust in the various actors responsible for the development, deployment and maintenance of the underlying technical infrastructure, as well as the multiplicity of parties involved in the DeFi ecosystem (such as code auditors, wallet and other infrastructure providers).

Moreover, one must not forget that the traditional financial system, through its own infrastructure of trust, provides additional guarantees that are not available in the context of DeFi. For example, banks have the power to revert a transaction which was held to be fraudulent, and governments will ensure that banks deposits are safe even if the institution goes bankrupt. All these important functions are key components of the trust infrastructure of traditional finance, which are—at least at the moment—not provided by the technological guarantees of DeFI. While it might be possible to implement these safeguards through technological means (e.g. alternative dispute resolution systems for reverting transactions, or private insurance schemes for hedging against bankruptcy), they are currently missing in a large majority of DeFi products. For instance, Nexus Mutual is currently one of the largest DeFi insurance companies, offering ways to manage risks in a variety of DeFi products, including failures in the protocol code, the economic design of the system, or the governance set-up or oracles. At the time of writing (December 2021) it has around ~700M USD worth of funds covered[11], yet, this represents less than 0.5% of the gross value locked in various DeFi protocols.[12]

[8] A case in point would be the so called parity bug, where a fault in a multisig wallets written by one of the inventors of Ethereums Solidity programming lanuage was exploited to lock more than half percent of the total EThereum supply at the time.(Parity Technologies 2017)

[9] Composability introduces the possibility of exploiting the interconnectedness of DeFi applications to extract value in ways that were not intended for (e.g. using flash-loans to drain funds from liquidity pools). See for example: (Coinbase, 2020; McDonald, 2020)

[10] For an updated list of DeFI hacks, see: https://cryptosec.info/defi-hacks/ and https://rekt.news/leaderboard/

[11] https://nexustracker.io/

[12] https://www.theblockcrypto.com/data/decentralized-finance/total-value-locked-tvl

2. Market dynamics

Confidence in the technological infrastructure of a blockchain-based system is a necessary yet insufficient condition to justify the adoption and use of a DeFi application. A sufficient amount of economic returns also need to be expected. DeFi protocols generally promise much higher returns on investment than traditional finance (with APY sometimes going as high as 3000%). Of course, as in every other financial product, high promised returns also come with comparably high risks. Indeed, while some forms of counterparty risk are significantly reduced as a result of automation and (over-)collateralization, new types of risks come into play with regard to the market, credit, and liquidity risk.

Market risks are typical in traditional finance, but are exacerbated in the context of DeFi, due to the high volatility of crypto-assets prices, which might lead to significant financial losses in a very short amount of time. In particular, fluctuations in the price of the crypto-assets deposited in a liquidity pool might lead to a potential loss (known as “impermanent loss”) whenever one of the crypto-assets involved in the transaction appreciates more than the other (Aigner & Dhaliwal 2021).

Credit risks are also very common in traditional finance, and are one of the main justification for the establishment of trusted third parties (i.e. financial institutions) in charge of mediating these risks. In DeFi, over-collateralization is used as a form of credit risk management, intended to ensure that lenders will always be able to recoup their funds from the borrowers. However, in the context of specific market conditions, such as flash crashes, DeFi applications might rapidly become under-collateralised, thereby failing to eliminate credit risk (Perez & al., 2021).

Liquidity risk is more specific to DeFi, as it is related to the fact that many of the tokens used in the context of DeFi applications have a limited market cap and are generally not as liquid as traditional fiat currencies. This means that one cannot rely on the current market price of these tokens as an accurate indicator of the value they hold, since any attempt at rapidly selling these tokens on the open market would significantly decrease their value, as not enough buyers are willing to purchase them at the current price. Accordingly, assessing the potential gains that investors might obtain via different DeFi protocols is not as easy as looking at the corresponding APY. In order to secure their investments (and collaterals), DeFi users must ensure that they will be able to purchase or sell a sufficient amount of tokens at a reasonable price and in a sufficiently short time frame. As such, when making an investment, investors need to assess the liquidity of both the assets they could earn via the DeFI application, and the collaterals used as a security.

Hence, DeFi applications ultimately compete with one another for liquidity. Typically, a greater APY is provided by liquidity pools which are in need of greater liquidity, incentivizing investors to put more funds into the pool, in exchange for a higher return on investment. Yet, some of the tokens earned by investors from these liquidity pools are very niche and barely liquid, thus subject to significant market risk. Moreover, while some DeFi applications have been thoroughly audited by professional firms, others are just deployed as-is, without any security guarantees, and generally compensate for the security risk by offering extremely high APY. Market competition between DeFi applications could potentially help, yet performing a proper market analysis in the DeFi environment is a complex endeavour, which involves multiple factors of analysis, including security, transparency, return on investment, and all the associated market, credit, and liquidity risks. As a result, just like in the case of centralized finance, DeFi also relies on external actors such as comparators[13] and aggregators[14] in charge of comparing the risks and benefits of different DeFi protocols. Hence, in order for them to effectively increase the level of confidence in the system, they ultimately need to prove to be sufficiently trustworthy. Such trustworthiness, however, currently lacks independent guarantees.

3. Regulatory framework

Even though they rely on distributed infrastructures, DeFi protocols do not exist in a vacuum and are therefore not immune to external influence by regulators and other public authorities (De Filippi & al., 2021; Ferrari 2020). All major jurisdictions, such as China, the EU, or the US have been working towards extending their powers over the various intermediaries involved in the DeFi space, either by enacting new regulation, or by finding ways of enforcing existing ones. While they do not depend on any centralized intermediaries in order to ensure their operations, DeFi protocols nonetheless benefit from the services of third party operators (e.g. blockchain explorers, cryptocurrency exchanges, custodian wallets) that may themselves be subject to specific regulatory constraints. Whereas, in the context of traditional finance, regulation plays a crucial role in increasing confidence in the financial system, in the context of decentralized finance, regulation might lead to two very distinct and potentially diverging outcomes (De Filippi & Wright 2018). On the one hand, it may contribute to establishing a more trustworthy environment, by reducing the number of frauds and scams that are progressively taking over the space. On the other hand, regulation of DeFi, although impractical, may have the unintended effect to trigger a whack-a-mole game—similar to that which emerged in the peer-to-peer file sharing scene a two decades earlier (Patry, 2009) —where draconian regulations have spurred the development of more decentralized technological solutions designed to evade law enforcement.

Regulation can also upset the dynamics of innovation by raising the cost of compliance, leading to a potential concentration of players, and thus reducing the open and permissionless competition in the DeFi market. This centralization process may also change the trust calculus for some users, potentially reducing the use and adoption of specific DeFi protocols, and thus the liquidity of the associated assets.

Finally, it is important to note that even though DeFi is intended to maximize confidence through technological guarantees, one cannot assess the reliability of any DeFi protocol alone, without accounting for the broader ecosystem in which it operates. Indeed, DeFi rests upon a multi-layered infrastructure, with every layer building upon each other to create an open and interoperable system of interconnected building blocks. Because of the hierarchical dependencies between these layers, their security ultimately depends on that of the layers below. This means that if the underlying settlement layer (a.k.a. the blockchain) were compromised (by, for example, a 51% attack, or a sudden leap in quantum computing), all subsequent layers would be equally compromised. Hence, despite being less prone to failure due to breach of fiduciary obligations or counterparty risk, the DeFi nonetheless has to tackle a variety of other risks. The permissionless nature, along with the openness and composability of decentralized financial protocols might trigger a different set of trust issues, which could potentially result in considerable systemic risk.

[13] DeFI Score DeFi ((http://defiscore.io) provides a single, consistently comparable value for measuring DeFi platform risk, based on factors including smart contract, centralization and financial risk ; DeFi Pulse (https://defipulse.com/) has launched new safety ratings in alpha to enable users to compare the risks of on-chain protocols. However, the ratings system is still in development and does not factor in all risks, such as smart contract risks.

[14] The most popular Popular DeFi aggregators are 1inch, Matcha, and Paraswap, which leverages multiple different DEX and implements various buying and selling strategies to help users maximize profits, as well as mitigate high gas fees and DEX trading commissions.

The role and impact of regulation

As Ulrich Beck argues (1992), in modern societies where high-risk technologies are ubiquitous, the primary role of public policy is to distribute technology related risks and harms among various members of society. This is a complex exercise, as the harms and risks individuals face as consumers and citizens need to be balanced against the harms other stakeholders may suffer, and against communal interest, such as societal, economic, or ecological ones. In some cases substantial risks and harms can be identified in advance, such as the case with pharmaceuticals, or nuclear energy. In such cases technological innovation is subject to heavy regulation to make sure that the individual and social risks of innovation are properly understood before they reach the market. In other situations, such as digital or financial innovation, regulation usually responds to emerging risks after the innovation has been adopted and its risks have thus become more tangible. The role of regulation in these cases is to shift risks and harms from how the market has allocated them to how the policymaker sees them as socially, economically, culturally, or politically desirable and viable. Firms may put citizens' lives in danger by pollution, but regulation can shift the cost of pollution back from the citizen to the firm by stronger environmental rules. Some financial institutions may like to shift all risks to their clients, but central banks may also force them to take on more of such risk in the form of capital and liquidity requirements.

The post mortem analysis of the 2008 crisis has pointed out the failure of policymakers and regulators in both understanding the risks posed by subprime mortgage derivatives, and also removed many frameworks which could have forced financial institutions to internalize more of the risks of the financial products they bought and sold. Systemic risks were also weakly understood, and underestimated, which is a general problem with tightly coupled systems with non-linear, complex interactions (Perrow 1984).

The regulation of the blockchain space emerged as the economic relevance of the different activities in this domain started to materialize. In the first wave, regulatory activities were aimed at reducing legal uncertainty in front of innovation by creating blockchain innovation friendly legal environments through permissive rules, economic incentives, and regulatory sandboxes. The second wave of regulatory activities were prompted by number of factors: 1) growing number and complexity of DeFi products and services, which introduced a large number of potential points of failure in the ecosystem; 2) a rapid influx of easy-money-seeking lay users and capital, which shifted the demographics of the DeFi space from tech-savvy, risk tolerant early adopters towards technically less proficient, more vulnerable mainstream users; 3) a corresponding growth in the profitability of fraudulent activities. This has led, according to SEC Commissioner Caroline A. Crenshaw to inadequate internal controls; the victimization of individuals by malevolent actors; and *"information asymmetries which advantage rich investors and insiders at the expense of the smallest investors and those with the least access to information"* (Crenshaw 2021). This wave is characterized by the classification of various tokens according to existing financial regulation into various pre-existing asset classes, the enforcement of anti-money laundering and know your customer rules on certain intermediaries, tax rules on crypto-token assets, enforcing the same rules vis-a-vis blockchain based financial service providers as traditional financial services have to comply with.

Meanwhile, while DeFi relies on the technological guarantees provided by blockchain technology to reduce counterparty risk (i.e. by restraining the agency of third parties interacting on a blockchain-based system), it remains nonetheless necessary to identify ways to address the risks specific to such trust minimizing systems, and DeFi in particular. Carter and Jeng (2021) identified five major risks factors in relation to DeFi: technical risks, comprising the operational risks of blockchains, smart contract vulnerabilities, and scalability challenges; risks related to the governance of the technology, and risks stemming from DeFi's interconnections with the traditional financial system. These different types of risks require different solutions. At the moment, the technical risks are only addressed through voluntary, market based logics: open sourcing the code pushes responsibility and the corresponding risk to the user. Code audits are voluntary, and since this is a nascent field, mistakes in the audit are possible. Product liability rules of software, or more general consumer protection rules may offer alternative venues in case of defective or fraudulent smart contracts (Cabral 2020, Prince 1980, Rustad & Koenig 2005). To address the risks related to the governance of the technology requires us to establish stronger links between what can be an open source software running on a decentralized computer network, and those legal entities, which deploy and operate such software to provide financial services, and which benefit financially from their operation. In other words, while the software may be decentralized, there is often a rather centralized, well-identifiable entity behind it, and there is no reason to apply to them different rules than the ones which apply to other financial service providers. At the moment, the technical risks are only addressed through voluntary, market based logics: open sourcing the code pushes responsibility and the corresponding risk to the user. Code audits are voluntary, and since this is a nascent field, mistakes in the audit are possible. Product liability rules of software, or more general consumer protection rules may offer alternative venues in case of defective or fraudulent smart contracts (Cabral 2020, Prince 1980, Rustad & Koenig 2005). To address the risks related to the governance of the technology requires us to establish stronger links between what can be an open source software running on a decentralized computer network, and those legal entities, which play a central role in their development, and which benefit financially from their operation. In other words, while the software may be decentralized, there is often a rather centralized, well-identifiable entity behind it, and there is no reason to apply to them different rules than the ones which apply to other financial service providers. Ensuring a stable and solid connection between DeFi and the traditional financial system is one of the main goals of emerging regulations, whereas market competition provides a means to discriminate against projects with subpar governance. The technical risks are more difficult to address as the immutability and tamper-resistance of blockchain based systems may limit the technological accountability of these systems. Attempts at reducing the impact of bugs or exploits in blockchain applications have triggered innovative responses by the developer community, such as introducing means of making smart contracts pausable (Claburn, 2021), introducing code audits and bug hunts (Khatri, 2020). Sometimes, however, the only way to remediate harm would require compromising on some of the fundamental promises of blockchain technology, such as immutability, and intervene at the protocol level in order to modify the code of the problematic smart contract (Reijers & al, 2021). In addition, efforts are often made to identify perpetrators through vigilante blockchain and digital forensics,[15] or by referring cases to traditional public trust institutions (e.g. the judicial and executive branch of the government) (Goodin, 2021, MonoX Team, 2021). Despite such efforts, the pseudonymity inherent in the design of many blockchain-based systems limits the effectiveness of such efforts. Several attempts have also been made to retrieve funds by non-technical means, by relying on alternative approaches such as social engineering (Baker, 2020), or through the offering of monetary bounties to incentivize the attacker(s) to return the funds (Chipolina, 2021).

[15] https://www.blocknative.com/blog/mempool-forensics

The understanding of market risks is also more differentiated than before. On the one hand, it is probably well understood and acknowledged by at least some members of the DeFI community, that crypto assets with no links to real-world fundamentals are highly speculative assets, with correspondingly high risks. On the other hand, there is a growing intolerance of clearly fraudulent so-called pump-and-dump activities. While the perpetrators of such schemes often remain unknown, they often enlist social media influencers and opinion leaders in order to generate hype. As Elon Musk learned the hard way, the resentment of defrauded users against these influencers might dissuade them from expressing support for blockchain-projects which they are not sure about. This means that influencers will necessarily have to be more prodent in advertising sketchy projects, especially if they want to keep their reputation intact, and also avoid possible legal liabilities.[16]

Finally, while some parts of the DeFi ecosystem are largely unregulated, and may also prove hard to regulate, other, key parts of the infrastructure are not only heavily centralized, but also increasingly strictly and effectively regulated. These facts may be a curse or a blessing in disguise for the unregulated section of DeFi. Know Your Consumer (KYC), Anti Money Laundering (AML) and Counter-Terrorist Financing (CTF) rules which apply to fiat exchanges also apply in the context of DeFi, potentially cutting off some of the illicit money flowing into the ecosystem.

Conclusion

The blockchain and DeFi space is in the midst of transformational change as it is gaining more mainstream adoption. The rapid pace of technological innovation prompted changes in the typology of actors inhabiting this space, how it is governed, and how trust is being produced within it. The early adopters of DeFi accepted the risks of bugs, fraud, and extreme volatility as an inherent part of the system. But the hype, and the prospects of astronomical profits that came along with it, attracted a different crowd into the DeFi space, with a different attitude with regard to the tolerance of risks, harms, and expectations regarding safety and security. This new crowd includes technically less capable developers, soldiers of fortune, naive retail investors, meme-mesmerized kids, gamblers, as well as serious, high profile investors, and other stakeholders, such as stablecoin providers, with non-trivial legal obligations and regulatory scrutiny. Although they came later, these new types of investors have already outnumbered the early adopters, and are progressively changing the general expectations about the way trust is to be produced and maintained in the space.

The trust infrastructures which were well aligned with the expertise and politics of the early adopters may prove inadequate for the latter type of crowd. The enormous amounts of money which flooded the DeFi space attracted all kinds of predators who try to find exploits in both the technical and the social dimensions of this emerging techno-social system. Today, the DeFi space has little to offer beyond high-risk high-yield value proposition, and seems to be incapable of reducing fraud and bug related risks on its

[16] A number of celebrities such as Kim Kardashian, boxer Floyd Mayweather, and former NBA star Paul Pierce are being sued by crypto investors in a the U.S. District Court of the Central District of California for alleged pump and dump activity. "Defendants touted the prospects of the company and the ability for investors to make significant returns due to the favorable 'tokenomics' of the EMAX Tokens,"

own. This is what motivated governmental intervention in order to protect the interests of both existing DeFi users, and new potential users who would be otherwise reluctant to engage with these platforms.

However, the use of regulation as a means to minimize or redistribute risk amongst stakeholders only works in a context where people's trust is not misplaced in the newly established trust infrastructure imposed by the law, along with all the relevant intermediaries and trusted authorities that come with it. In times when the public trust infrastructures provided by the government (including central banks, the court system, and the various regulatory authorities such as the SEC or the CFTC in the U.S.) are often distrusted by citizens —especially in the wake of the 2008 crisis —, the denizens of the blockchain and DeFi ecosystem retreated to an allegedly "trustless" technology (Saiedi & al, 2020; Auer & Tercero-Lucas 2021). And yet, despite its promises, DeFi relies on multiple layers of trust and new intermediary operators that might jeopardize the technological guarantees that the system is intended to provide. If, by virtue of technical bugs, commercial scams and frauds, a large portion of DeFi platforms regularly end up with a series of meltdowns which wipe out investments and savings with the same efficiency as the 2008 crisis, users who put their money in the system may want to find new ways to trust such systems. Besides, even though many of the components of the DeFi ecosystem may successfully evade regulation, some of the key players in the system (such as fiat exchanges, stablecoin providers with fiat assets in the bank, key management service providers for multisig transactions, as well as any other entity with a real world legal presence inescapably remain under the purview of regulators (Carter & Jeng, 2021).

The regulation of DeFI might thus have divergent implications on the perceived trustworthiness of DeFi applications, depending on corresponding preferences and risk profiles of the user base. Those who already trust the public trust infrastructure provided by the state (as most users involved in the traditional financial system do) might feel more comfortable to engage in DeFi because of the greater sense of security and protection that regulation might provide to them—i.e. in terms of knowing that they will be at least partially protected against the risks of frauds, scams, bugs, hacks or other technological failures. Those who do not consider the public trust infrastructure as sufficiently trustworthy (as hinted by a significant portion of existing DeFi users) might instead be discouraged by the appearance of the state and its institutions. Indeed, by shifting risks away from a low agency, confidence-based technological system, towards a more institutional trust-based system, regulation might be perceived—at least by some—as possibly (re-)introducing the same old risks into a system which was built precisely to eliminate such risks.

Ensuring that regulation has a net positive impact on the adoption of DeFi would require that any new intermediary operator or supervisory authority that is brought to intervene into the DeFi ecosystem be regarded as a trusted authority by current and potential users. This means that the risks that come with the introduction of any new regulatory or supervisory authority must be regarded as an acceptable compromise or trade-off, where the added benefits of increased agency and intervention by a third party (and the associated counterparty risk) more than compensate for the technological risk associated with the current model of DeFi.

At the same time, one potential outcome of regulation might be that those who do not want to rely on the public trust infrastructure will be incentivized to develop new DeFi applications that make it more difficult for regulators to influence the operation of these systems. The evolution of P2P file sharing software in the early 2000's has already shown that regulatory intervention can lead to the deployment of increasingly decentralized applications, which are not easily regulatable. Incentives for developing such applications can be political or ideological, especially for those who believe that the immutability and tamper-resistance of the underlying blockchain infrastructure is more important than the risk inherent into the technological fabric of these systems (as regards social, economic, and regulatory risks). Other incentives may be clearly economical: if more money can be made in the unregulated space than in the regulated one, some will have ample reasons to build new decentralized systems, specifically designed to escape from the infrastructure of trust established by the law.

This is the case, for instance, of decentralized exchanges like Uniswap or Sushiswap, or privacy coins like Tornado-cash, aimed at establishing a decentralized ecosystem of blockchain-based applications which, by virtue of their decentralized and pseudonymous/anonymous characteristics, cannot be easily regulated or influenced by governmental interventions. Indeed, since the way these systems operate in the back-end is governed by the rules of the underlying blockchain protocol, regulators have only indirect power over them, by for example putting pressure on the developers or the maintainer of these systems, or on those supporting their use with specific interfaces (*i.e.* front-end web apps). The efficiency of such an indirect approach is expected to be increasingly often tested in court. (Tokar, 2022)

The blockchain and Defi communities proclaimed their independence from the powers that be just like John Perry Barlow did a quarter of a century earlier with the *Declaration of Independence of Cyberspace* (1996). Early Internet advocates were eager to create a new social, economical and political space, where the rules are defined by the denizens of that space, rather than by governments and corporations. This created the conditions for playful experimentation and open-ended innovation, driven by the fruitful blossoming of ideas, new approaches, and creativity. The advent of blockchain technologies and DeFi is reminiscent of the early internet days, with one notable difference, though: while the early Internet was everything but financial, the blockchain ecosystem cannot be non-financial. This is an important difference because, even more than the Internet, in the context of a hyper-financialized ecosystem like DeFi, where billions of dollars worth of crypto-assets circulate daily, trust becomes a crucial and indispensable resource.

The blockchain ecosystem is trying to obviate this need for trust by building “trustless” systems, where trust does not rely on any third party operator, but rests solely in the technological infrastructure. Yet, recent developments in DeFi suggest that such a solution might not be ultimately viable. In order to facilitate the mainstream adoption of DeFi, the trust infrastructure it relies upon needs to account for both on-chain and off-chain mechanisms. In particular, one needs to account for the various social institutions that operate off-chain, such as traditional laws and regulations, but also social norms, community rules, and the multiple accountability mechanisms that exist to address the countless ways in which things could go wrong in a system where the stakes are so high. Unless DeFi identifies new means to allow for conflict resolution, and for the remedification of undesirable transactions (e.g. through specific insurance schemes), it will remain a niche market, mostly populated by investors and speculators with a high-risk profile. Overall, theDeFi experiment cannot be held to be either a success or a failure; it is an on-going experiment that helps us explore new technological infrastructures of trust, their strengths and their limitations.

References

Aigner, A. A., & Dhaliwal, G. (2021). UNISWAP: Impermanent Loss and Risk Profile of a Liquidity Provider. *ArXiv:2106.14404 [q-Fin]*. https://doi.org/10.13140/RG.2.2.32419.58400/6

Auer, R., & Tercero-Lucas, D. (2021). *Distrust or speculation? The socioeconomic drivers of US cryptocurrency investments*.

Baker, P. (2020, September 14). *DeFi Lender bZx Reclaims $8M Stolen in Sunday's Attack*. CoinDesk. https://www.coindesk.com/markets/2020/09/14/defi-lender-bzx-reclaims-8m-stolen-in-sundays-attack/

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. *Eff.Org*, *January 18, 2011*. https://projects.eff.org/~barlow/Declaration-Final.html

Beck, U. (1992). *Risk society: Towards a new modernity*. Sage Publications.

Bodó, B. (2020). Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*, 146144482093992. https://doi.org/10.1177/1461444820939922

Bodó, B. (2021). *The commodification of trust* (SSRN Scholarly Paper ID 3843707). Social Science Research Network. https://doi.org/10.2139/ssrn.3843707

Cabral, T. S. (2020). Liability and artificial intelligence in the EU: Assessing the adequacy of the current Product Liability Directive. *Maastricht Journal of European and Comparative Law*, *27*(5), 615-635.

Carter, N., & Jeng, L. (2021). DeFi Protocol Risks: The Paradox of DeFi. In B. Coen & D. R. Maurice (Eds.), *Regtech, Suptech and Beyond: Innovation in Financial Services*. Risk Books. https://doi.org/10.2139/ssrn.3866699

Chipolina, S. (2021, August 13). *Poly Network Hacker Returns All Stolen Ethereum Assets*. Decrypt. https://decrypt.co/78442/poly-network-hacker-returns-all-funds

Claburn, T. (2021). *BadgerDAO DeFi defunded as hackers apparently nab millions in crypto tokens*. The Register. https://www.theregister.com/2021/12/02/badgerdao_coin_theft/

Coates, J. (2018). Trust and the Other: Recent directions in Anthropology. *Social Anthropology*, 1469-8676.12596. https://doi.org/10.1111/1469-8676.12596

Coinbase. (2020, September 4). *Around the Block #3: BZx attack update, DeFi vulnerabilities, and the state of debit cards in…*. Medium. https://blog.coinbase.com/around-the-block-analysis-on-the-bzx-attack-defi-vulnerabilities-the-state-of-debit-cards-in-1289f7f77137

Crenshaw, C. A. (2021). Statement on DeFi Risks, Regulations, and Opportunities. *The International Journal of Blockchain Law*, *1*(1). https://www.sec.gov/news/statement/crenshaw-defi-20211109

Danezis, G. (2014). Trust as a Methodological Tool in Security Engineering. In R. H. R. Harper (Ed.), *Trust, Computing, and Society* (pp. 68–92). Cambridge University Press. https://doi.org/10.1017/CBO9781139828567.007

Davidson, S., Novak, M., & Potts, J. (2018). The Cost of Trust: A Pilot Study. *The Journal of the British Blockchain Association*, *1*(2), 1–7. https://doi.org/10.31585/jbba-1-2-(5)2018

De Filippi, P., & Wright, A. (2018). Blockchain and the Law. Harvard University Press

De Filippi, P., & Hassan, S. (2018). Blockchain technology as a regulatory technology: From code is law to law is code. arXiv preprint arXiv:1801.02507.

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society, 62, 101284.

De Filippi, P., Mannan, M., & Reijers, W. (2021). The Alegality of Blockchain Technology. *Policy and Society*, *Cambridge University Press*.

Elliptic Research. (2021). *DeFi: Risk, Regulation, and the Rise of DeCrime* (2022 Elliptic Report). Elliptic. https://www.elliptic.co/resources/defi-risk-regulation-and-the-rise-of-decrime

Ferrari, V. (2020). The regulation of crypto-assets in the EU - Investment and payment tokens under the radar. *Maastricht Journal of European and Comparative Law*, *27*(3), 325-342. https://doi.org/10.1177/1023263X2091153

Financial Industry Regulatory Authority. (2019). *FINRA Fines Robinhood Financial, LLC $1.25 Million for Best Execution Violations*. Finra.Org. https://www.finra.org/media-center/newsreleases/2019/finra-fines-robinhood-financial-llc-125-million-best-execution

Fukuyama, F. (1995). *Trust: The social virtues and the creation of prosperity*. Free press.

Giddens, A. (1990). *The consequences of modernity*. Polity Press.

Goodin, D. (2021, December 1). *Really stupid "smart contract" bug let hackers steal $31 million in digital coin*. Ars Technica. https://arstechnica.com/information-technology/2021/12/hackers-drain-31-million-from-cryptocurrency-service-monox-finance/

Greif, A. (1994). On the Political Foundations of the Late Medieval Commercial Revolution: Genoa During the Twelfth and Thirteenth Centuries. *The Journal of Economic History*, *54*(2), 271–287. https://doi.org/10.1017/S0022050700014479

Huurne, M. ter, Ronteltap, A., Corten, R., & Buskens, V. (2017). Antecedents of trust in the sharing economy: A systematic review. *Journal of Consumer Behaviour*, *16*(6), 485–498. https://doi.org/10.1002/cb.1667

Keymolen, E. L. O. (2016). *Trust on the line: A philosophical exploration of trust in the networked era* [Erasmus University Rotterdam]. hdl.handle.net/1765/93210

Khatri, Y. (2020). *DEX protocol Bancor suffered security vulnerability, migrated $455K worth of user funds*. The Block.

https://www.theblockcrypto.com/post/68791/dex-protocol-bancor-suffered-security-vulnerability-migrated-455k-worth-of-user-funds

Konnath, H. (2022). *Floyd Mayweather, Kim Kardashian Sued Over Crypto Promos—Law360*. Law360. https://www.law360.com/articles/1453678/floyd-mayweather-kim-kardashian-sued-over-crypto-promos

Luhmann, N. (2017). *Trust and power*. Polity.

Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., ... & Laskowski, M. (2019). Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack. *Journal of Cases on Information Technology (JCIT)*, *21*(1), 19-32.

McDonald, M. (2020, June 29). Incident with non-standard ERC20 deflationary tokens. *Balancer Protocol*. https://medium.com/balancer-protocol/incident-with-non-standard-erc20-deflationary-tokens-95a0f6d46dea

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems*, *2*(2), 12:1-12:25. https://doi.org/10.1145/1985347.1985353

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research*, *13*(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

MonoX Team. (2021, December 1). Exploit: Post Mortem. *MonoX*. https://medium.com/monoswap/exploit-post-mortem-33921a779b43

Nickel, P. J. (2013). Trust in Technological Systems. In M. J. de Vries, S. O. Hansson, & A. W. M. Meijers (Eds.), *Norms in Technology* (Vol. 9, pp. 223–238). Springer Netherlands. https://doi.org/10.1007/978-94-007-5243-6

O'Neill, O. (2002). *Autonomy and trust in bioethics*. Cambridge University Press.

Parity Technologies. (2017). *A Postmortem on the Parity Multi-Sig Library Self-Destruct*. Parity.Io. https://www.parity.io

Patry, W. F. (2009). *Moral panics and the copyright wars*. Oxford University Press.

Perez, D., Werner, S. M., Xu, J., & Livshits, B. (2021). Liquidations: DeFi on a Knife-edge. *International Conference on Financial Cryptography and Data Security*, 457–476.

Perrow, C. (2011). *Normal accidents*. Princeton university press.

Prince, J. (1980). Negligence: liability for defective software. Okla. L. Rev., 33, 848.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, no. COM/2020/593 final (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., Cubillos Vélez, A., & Orgad, L. (2021). Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies. *Topoi*, *40*(4), 821–831. https://doi.org/10.1007/s11245-018-9626-5

Rustad, M. L., & Koenig, T. H. (2005). The tort of negligent enablement of cybercrime. *Berkeley Tech. LJ*, *20*, 1553.

Saiedi, E., Broström, A., & Ruiz, F. (2021). Global drivers of cryptocurrency infrastructure adoption. *Small Business Economics*, *57*(1), 353–406.

Statement by Ben S. Bernanke Chairman Board of Governors of the Federal Reserve System, (2010). https://www.federalreserve.gov/newsevents/testimony/bernanke20100902a.pdf

Sztompka, P. (1999). *Trust: A sociological theory*. Cambridge University Press.

The financial crisis and the role of federal regulators, Serial no. 110-209, House of Representatives, 110th Congress, Second session (2008). https://www.govinfo.gov/content/pkg/CHRG-110hhrg55764/html/CHRG-110hhrg55764.htm

Tokar, D. (2022, January 13). Crypto-Savings Lawsuit Puts Principles of DeFi to the Test. *Wall Street Journal*. https://www.wsj.com/articles/crypto-savings-lawsuit-puts-principles-of-defi-to-the-test-11642069806

Walsh, D. (2021, September 1). *Europeans don't want the EU to regulate cryptos, Euronews poll finds*. Euronews. https://www.euronews.com/next/2021/09/01/majority-of-europeans-want-their-countries-to-regulate-crypto-not-the-eu-exclusive-euronew

Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. Mit Press.

Wiggins, R. Z., Piontek, T., & Metrick, A. (2014). *The Lehman Brothers Bankruptcy A: Overview* (No. 2014-3a-v1; Yale Program on Financial Stability Case Study). Yale University.

Yang, S., & Kay, G. (2021). *Bernie Madoff died in prison after carrying out the largest Ponzi scheme in history – here's how it worked*. Business Insider. https://www.businessinsider.com/how-bernie-madoffs-ponzi-scheme-worked-2014-7

Zhou, Y., Kumar, D., Bakshi, S., Mason, J., Miller, A., & Bailey, M. (2018). Erays: Reverse engineering ethereum's opaque smart contracts. *Proceedings of the 27th USENIX Security Symposium (USENIX Security 18)*, 1371–1385.

Zucker, L. G. (1985). Production of Trust: Institutional Sources of Economic Structure, 1840 to 1920. In L. L. Cummings & B. Staw (Eds.), *Research in Organizational Behavior*. JAI Press.