BLOCKCHAIN TECHNOLOGY AND POLYCENTRIC GOVERNANCE

Primavera de Filippi, Morshed Mannan, Sofia Cossar, Tara Merk, Jamilya Kamalova

EUI ROBERT SCHUMAN CENTRE

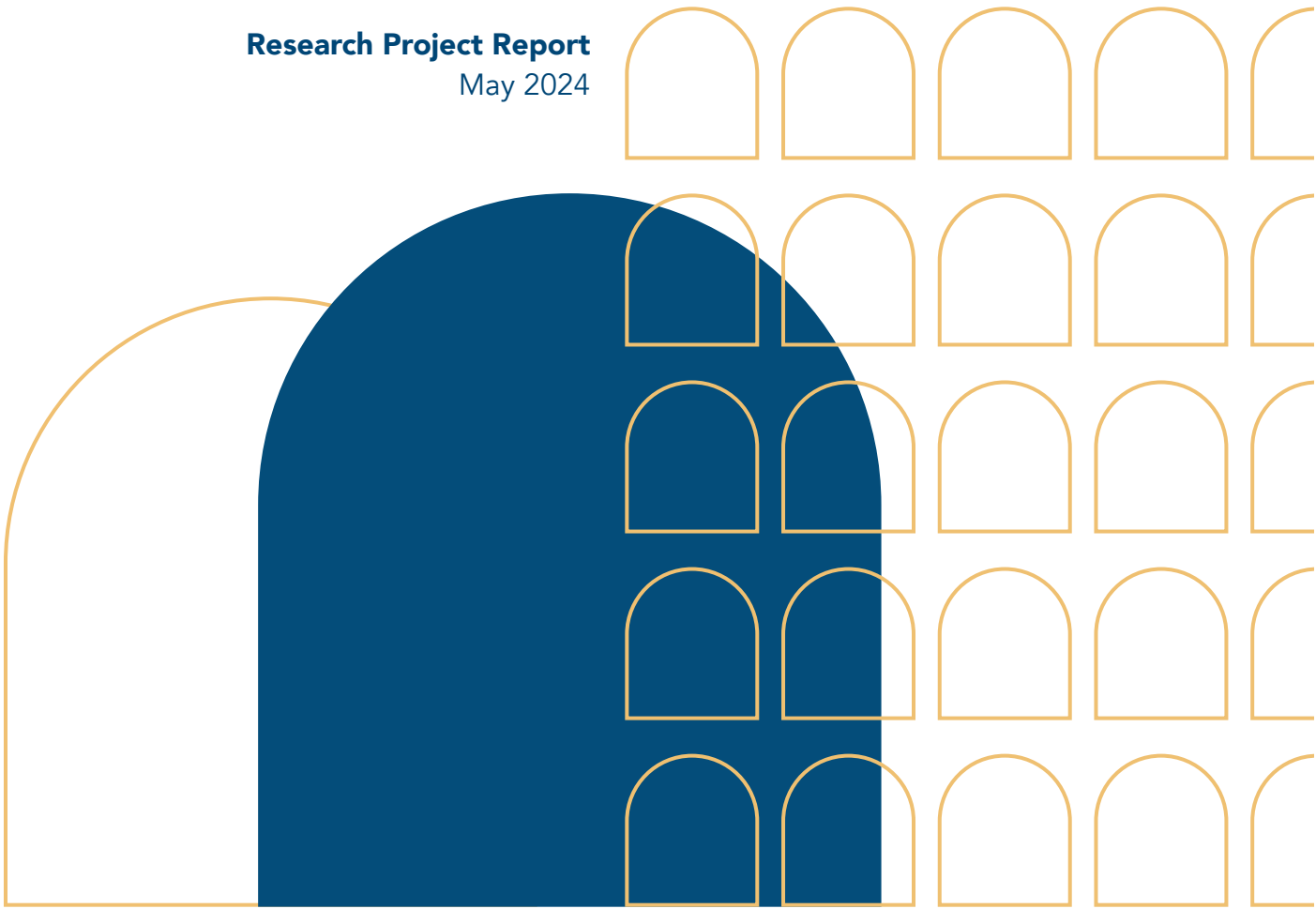
BLOCKCHAIN TECHNOLOGY AND POLYCENTRIC GOVERNANCE

Authors

Dr. Primavera de Filippi, Dr. Morshed Mannan, Sofia Cossar, Tara Merk, Jamilya Kamalova

Contributor Dr. Kelsie Nabben

Research Project Report
May 2024



Published by

European University Institute (EUI)

Via dei Roccettini 9, I-50014

San Domenico di Fiesole (FI)

Italy

This research is funded by the European Research Council under the European Union's Horizon 2020 Research and Innovation Programme (Grant Agreement No. 865856).

Table of Content

Executive Summary

Context: This report addresses the polycentric governance of blockchain systems, following conversations held from September 2022 until September 2023 by a reading group of blockchain practitioners and academics. The ERC-funded BlockchainGov project led the reading group. Since the publication of the Bitcoin whitepaper in 2008, blockchain technology has gained increasing popularity for being a "decentralized" ledger of transactions. Collectives of people have formed to discuss and decide on—to "govern"—the evolution of blockchain networks and blockchain-based applications, creating what we refer to as "blockchain systems." While much literature is dedicated to understanding the governance of blockchain systems, no substantial efforts have been made to apply the concept of "polycentricity" to blockchain governance. Polycentric governance systems are characterized by multiple autonomous decision-making centers with overlapping areas of responsibility, which both compete and cooperate within a common overarching system of commonly agreed-upon rules, spontaneously or deliberately generating a shared social order. A term initially presented by Michael Polanyi and famously further developed by Vincent and Elinor Ostrom, polycentricity allows us to understand blockchain systems' structure, process, and outcome.

Research questions and findings:

1. **Are blockchain systems polycentric?** Polycentricity in blockchain systems entails more than just "architectural decentralization." It involves evaluating the governance of the blockchain system both internally and externally from the perspectives of "insiders" and "outsiders" to the rules governing it. Recognizing polycentricity as a spectrum, the focus shifts from merely determining if a blockchain system is "polycentric" to assessing if it surpasses a specific threshold that distinguishes it from being "monocentric." Additionally, the nature of polycentricity within these systems is dynamic, subject to change over time, whether through deliberate design or unintended evolution.

2. **What significant challenges do blockchains face as polycentric systems?** Despite their non-centralized decision-making framework, polycentric blockchains are vulnerable to disruptions that can compromise their stability and integrity. Firstly, multiple independent decision-making centers, each driven by distinct and sometimes conflicting incentives, pose governance challenges, such as achieving consensus. Secondly, security breaches and hacks can precipitate critical "states of exception," during which the standard governance rules might be temporarily suspended in favor of more centralized interventions by certain actors, thus impacting the system's overall operation. Thirdly, these systems are not immune to systemic risks; a single decision-making center's failure or malfunction due to bankruptcy, fraud, or operational shortcomings can trigger cascading effects across the network.

3. **What makes a polycentric governance system legitimate?** Polycentric co-regulation, or regulation of the governance of blockchain systems by both "code" and "law," has been highlighted as the most efficient way of governing polycentric blockchain systems. Whether such a co-regulatory effort can be perceived as legitimate is a more nuanced question. The perception of blockchain systems as legitimate by insiders and outsiders is crucial to their survival and sustainability. Endogenously, legitimacy in polycentric systems hinges on the effective participation of all stakeholders impacted by decisions and the option for these parties to "exit" the system if desired. Exogenously, the legitimacy of a polycentric system is contingent upon its operations and outcomes not adversely affecting the broader

ecosystem to which it is connected. Simultaneously ensuring endogenous and exogenous legitimacy is challenging but not impossible. It requires a deep and continuous understanding of all stakeholders' expectations and the development of pragmatic regulatory frameworks that bring clarity but enough flexibility to allow for responsible technological innovation.

Case studies:

- **The Bitcoin scaling debate**, which took place between 2015 and 2017, illustrates the challenges that can arise in polycentric blockchain systems when interests within and between different decision-making centers become misaligned.

- **The DAO Hack**, occurring in 2016, is an example of a "state of exception" within the Ethereum network. After a hack into The DAO, community members voted in favor of a hard fork to reverse the transactions that led to the theft. Some members who disagreed fundamentally with the decision remained in the original blockchain ledger, now called Ethereum Classic.

- **The Terra/Luna collapse**, catalyzed in May 2022, presents an example of how the failure of a particular component in the DeFi ecosystem can have a cascading effect, impacting the broader cryptocurrency market. The failure led to the insolvency of numerous projects and inflicted significant financial losses on investors, amounting to billions of US dollars.

- **The downfall of FTX in November 2022**, a centralized cryptocurrency exchange, had ripple effects across the ecosystem, which attempted to self-regulate through informal norms and standards by doubling down—albeit temporarily—on their commitment to "decentralization."

- **The Ethereum Merge**, or the transition of the Ethereum network into Proof-of-Stake, finalized in September 2022, is a positive example of how the delicate balance between exogenous legitimacy and endogenous legitimacy can be struck.

- **The sanctions on Tornado Cash by the United States' OFAC in 2022** illustrate the challenges for blockchain systems in achieving exogenous legitimacy. Importantly, it highlights the risks individuals such as founders or software developers face in blockchain projects, showing how legal actions can still target them, which can profoundly affect the entire blockchain system.

Authors

Dr. Primavera De Filippi (CNRS/Harvard/EUI) is the director of the European Research Council (ERC)-funded BlockchainGov project. She is also a research director at the National Center of Scientific Research in Paris, a faculty associate at the Berkman-Klein Center for Internet & Society at Harvard, a visiting fellow at the European University Institute in Florence, a former member of the Global Future Council on Blockchain Technologies at the World Economic Forum, a founder and coordinator of the U.N. Internet Governance Forum's dynamic coalitions on Blockchain Technology (COALA).

Dr. Morshed Mannan (EUI) is a research member of the ERC's BlockchainGov project, a research fellow at the Robert Schuman Centre for Advanced Studies at the European University Institute in Florence, and a research affiliate of the Institute for the Cooperative Digital Economy at The New School. As a researcher, he is interested in blockchain and cooperative governance, platform cooperativism and "exit to community."

Sofia Cossar (CNRS) is a research member of the ERC's BlockchainGov project. She is also a Ph.D. candidate in legal theory and legal tech at Université Paris II and the National Center of Scientific Research in Paris.

Tara Merk (CNRS) is a research member of the ERC's BlockchainGov project. She is also a Ph.D. candidate in ethnography and social sciences at Université Paris II and the National Center of Scientific Research in Paris.

Jamilya Kamalova (CNRS) is a research member of the ERC's BlockchainGov project. She is also a Ph.D. candidate in legal theory and legal tech at the Université II and the National Center of Scientific Research in Paris and a researcher at the Kleros Cooperative.

Contributors

Dr. Kelsie Nabben (EUI) is a research member of the ERC's BlockchainGov project, undertaking a Max Weber postdoctoral Fellowship at EUI. She was a recipient of a PhD scholarship at the RMIT University Centre of Excellence for Automated Decision-Making & Society. As a researcher, she specializes in ethnographic methods to investigate the social outcomes of emerging technologies.

Preface

By Michel Bauwens

First of all, I must commend the BlockchainGov team for this quite extraordinary synthesis of knowledge, which combines vital empirical work with sound theorizing. This is a very valuable summary of what is known, and how that knowledge was cumulatively created through various authors and researchers.

Here is perhaps an added perspective concerning what the ultimate purpose of the blockchain might be.

Until the advent of open source and crypto infrastructures, the main paradigm of human societies was one of competition between 'closed' competing entities. I refer here to competitive endeavors of market and state institutions, which operate in peer polities but have no internal knowledge of each other. The exchange of value took place through either market pricing or hierarchical commands.

Open source was the first social technology to overcome this. It scaled the polycentricity of previously local commons, to the global scale, allowing the translocal mutual coordination of human labor through open holoptical[1] *ecosystems of collaboration and coordination. But open source was economically vulnerable as it required market interfacing and those involved in infrastructural work at the core of these ecosystems were often underfunded, leaving the terrain open for the involvement of large corporate entities.*

Not so with the second phase of the deployment of open source, community centric open systems that use the blockchain. In this case, through tokenization and other systems, we now have the second layer, that of the translocal mutual coordination of the financing of human labor. This is obviously a huge step, and we have here the beginning of 'fourth sector' organization, which permissionly coordinate, through commons-centric network formations, the previous organizational forms (i.e. profit, public and non-profit) while allowing distributed contributions outside the control of any single corporate entity, as this report illustrates.

So what is still missing, despite experimentations, is the coordination of actual production, namely blockchain-enabled coordinated supply chains, and real-time public ledgers for civic collective action. Vitalik Buterin has suggested that the next step for Ethereum would be the re-creation of a full digital stack, able to withstand the surveillance state and private corporate control, but I am suggesting, at the same time, a different tack: the building of interfaces between the crypto systems, with its DAOs, and the mutual provisioning systems of production and consumption, that are emerging in urban and rural bioregional zones. The mutualization of provisioning systems at local scale, would greatly benefit from its 'cosmo-localization' of its global cooperation, by interfacing through crypto.

1 "Holopticism"is a combination of Greek words holos (whole, holistic, all), optiké (vision), and tekhné (art, technique). Much like the way in which a fly uses its special eye to view the world in a multi-faceted manner, holopticism expresses the capacity for players in a given organization (or group) to perceive the emerging whole of that organization (or group) as if it were a unique entity, be it in a natural physical space or an online space (virtual)… A holoptical space is a space in which each participant gets a live perception of the 'Whole.' Each player, thanks to his/her experience and expertise, relates to this "Whole" in order to adjust his/her actions and coordinate them with others' moves. Therefore there is an unceasing round trip, a feedback loop that works like a mirror between the individual level and the collective one. *See* Collective Intelligence Research Institute, Definition of Holopticism: https://cir.institute/holopticism/

This for me would be the priority, i.e. 'Crypto for Real', adding material production coordination to what it is already capable of doing for labor and its financing.

Preamble

This report presents an overview of the discussions held by the "*Blockchain Technology and Polycentric Governance"* reading group and additional insights derived from research conducted by members of BlockchainGov. BlockchainGov is a 5-year long (2021-2026) project funded by the European Research Council through a €2M grant, operating at the Centre national de la recherche scientifique (CNRS) in Paris, France, and the European Union Institute in Florence, Italy.

This piece is one of a series of multidisciplinary writings investigating the governance of blockchain systems and specific assumptions about their decision-making structures, namely:

- Report on Blockchain Technology, Trust, and Confidence (De Filippi et al. 2022a), assessing the role of confidence and trust in blockchain systems;
- Report on Blockchain Technology and Legitimacy (De Filippi et al. 2022b), addressing the challenges of legitimacy in blockchain systems;
- Report on Blockchain Governance Practices (De Filippi et al. 2024), analyzing various blockchain communities' multifaceted blockchain governance models.

Building upon this work, we investigate the extent to which blockchain systems are "polycentric" governance systems. The reading group, from September 2022 to September 2023, gathered several blockchain scholars and practitioners with vast expertise in governance and polycentricity. This report applies the concept of *polycentric governance to blockchain systems*, both internally (i.e., "endogenously") and externally (i.e., "exogenously"), from a conceptual, empirical, and normative perspective. The term "polycentricity" was first coined by Hungarian-British polymath Michael Polanyi and subsequently popularized by the academic work of Elinor and Vincent Ostrom. Contrary to **monocentric systems**, which are ruled by a dominant and central authority, **polycentric systems** are characterized by multiple autonomous and interrelated decision-making centers that compete to influence the operations of a system (Aligica & Tarko 2012).

Public and permissionless blockchains facilitate the recording and management of digital transactions independently of any centralized authority. In a prior report on the governance of blockchain networks (De Filippi et al. 2024), we explored **blockchain systems** as techno-social infrastructures. These systems blend core blockchain technology with a community of individuals and organizations involved in the development, maintenance, and operation of blockchain networks and the applications built upon them. Blockchain systems are constructed on various layers of a technological stack, encompassing blockchain networks, smart contracts, decentralized applications (DApps), and decentralized autonomous organizations (DAOs). The governance of blockchain systems encompasses a wide range of decision-making processes, covering areas from treasury management to software updates, among others. Key stakeholder groups in most blockchain systems include founding teams, software develop-

ers, token holders, investors, third-party organizations within the broader ecosystem, users, lawmakers, policymakers, and regulators. Each group influences the governance process to varying degrees, driven by diverse and sometimes conflicting interests.

Blockchain technology is often hailed for its **decentralizatio**n (Bodó & Giannopoulou 2019), a feature that signifies the distribution of control away from a central authority. While blockchains are **architecturally decentralized**, with copies of the ledger spread across numerous nodes in the network, the notion that they are **politically decentralized** requires careful examination (Buterin 2017, Srinivasan & Lee 2017). To assess the decentralization of blockchain systems, scholars and practitioners have devised various taxonomies, evaluating them across multiple dimensions (Sai et al. 2021, Karakostas et al. 2022). The governance of blockchain systems has attracted attention from several disciplines, including economics, game theory, sociology, and political science (De Filippi & Loveluck 2016, Reijers et al. 2016, De Filippi & Wright 2018, Alston 2019, Alston et al. 2021). However, the perspective of polycentric governance—a framework that considers multiple autonomous yet interrelated decision-making centers under an overarching rule set—has been seldom explored in blockchain governance research. Polycentric governance has been applied to diverse systems like the Internet and open-source software (Craig & Shackelford 2013, Shackelford et al. 2017, Mindel et al. 2018, Thussu 2021). Rozas et al. (2021) investigated its application in blockchain technology and governance, specifically within Commons-Based Peer Production (CBPP) communities. Alston et al. (2022) exploring the topic of change in blockchain systems through a polycentric lens. This report aims to bridge the gap in academic literature by **applying polycentric governance theory to the governance of the broader blockchain ecosystem.**

The reading group on *"Blockchain Technology and Polycentric Governance"* started with a series of research questions and preliminary hypotheses. These questions have facilitated the discussions and informed the draft of this report.

- **Q1: Are blockchains systems polycentric?**

  H1: Polycentricity in blockchain systems requires more than architectural decentralization.

  H2: Polycentricity in blockchain systems can be measured endogenously and exogenously, taking as a reference the "insiders" and "outsiders" of the overarching set of rules.

  H3: Polycentricity is a spectrum, not a binary, and a dynamic feature of blockchain systems.

- **Q2: What significant challenges do blockchains face as polycentric systems?**

  H1: Different and conflicting incentives can drive multiple decision-making centers to operate independently in a polycentric blockchain system. This risk can present challenges to gover nance, including difficulties in reaching consensus.

  H2: Security breaches and hacks affecting polycentric blockchain systems can lead to critical situations or "states of exception," where the usual decentralized governance model is temporarily overridden. In these scenarios, certain centralized actors or decision-making cen ters may intervene and make unilateral decisions affecting the system as a whole.

  H3: Polycentric blockchain systems may still be subject to systemic risks, where the failure or malfunction of one decision-making center, including bankruptcy, fraud, or significant operation al failure, can have cascading effects on others. Despite the decentralized nature of these sys-

tems, the interconnectedness of various nodes or decision centers can lead to problems in one area rapidly spreading to others.

- **Q3: What makes a polycentric blockchain system legitimate?**

  H1: Endogenously, or for a blockchain system to be considered legitimate by "insiders", it must at least ensure that those directly impacted by governance decisions can participate in the decision-making process. Additionally, it should provide all stakeholders with the ability to exit the system if they choose.

  H2: Exogenously, or for a blockchain system to be considered legitimate by "outsiders", it must at least ensure that its governance processes and outcomes do not purposefully harm the wider ecosystem within which it operates and interacts.

Led by BlockchainGov, a reading group was established to delve into specific research questions and hypotheses, attracting a broad spectrum of participants. This group ranged from blockchain practitioners eager to understand polycentric governance better to scholars and experts specialized in both blockchain governance and polycentric theory. Each meeting commenced with a designated discussant who dissected and presented the key aspects of the assigned readings. This approach not only facilitated targeted feedback and reflections from the author but also paved the way for an inclusive group dialogue. The gatherings wrapped up with reflections on how the literature informed the group's understanding of blockchain governance through a polycentric lens. This report aggregates the collective insights and knowledge derived from the reading group's sessions, alongside additional research conducted by BlockchainGov members and other pertinent scholars.

This report is structured in the following way. The introduction lays the groundwork by defining polycentricity and polycentric governance, alongside an introduction to blockchain technology. The first section, "Blockchain Systems as Polycentric Systems," examines how blockchain systems exhibit features of polycentric systems. The subsequent section, "Challenges in Polycentric Blockchain Systems," dives into the intricate challenges faced by these systems. It scrutinizes conflicts of interest, exceptional circumstances, and systemic risks, illustrating these concepts with real-world case studies such as the Bitcoin scaling debate, the The DAO hack, and the collapses of Luna/Terra and FTX. The third section, "Legitimacy in Polycentric Blockchain Systems," focuses on the notions of internal or "endogenous" legitimacy, highlighted by the Ethereum Merge case study, and external or "exogenous" legitimacy, as demonstrated by the situation of Tornado Cash following the US OFAC's sanctions. The conclusion encapsulates the main findings from the analysis and proposes directions for future research in the realm of blockchain systems.

Introduction

I. Understanding the Concept of "Polycentricity"

To delve into polycentric governance in blockchain systems, it is essential to get a clear understanding of *polycentricity*. This section aims to dissect the roots of the term, notably its development and popularization by scholars Vincent Ostrom and Elinor Ostrom. We will examine the fundamental characteristics of polycentricity, highlighting its context-dependent advantages and drawbacks. The focus will be on empirically identifying these traits and understanding their interrelationships. Furthermore, the discussion will emphasize that polycentricity exists along a spectrum, rather than being a simple binary concept, and will explore how polycentric governance evolves over time.

In a nutshell: *Polycentric governance systems are characterized by multiple autonomous decision-making centers with overlapping areas of responsibility, which both compete and cooperate within a common overarching system of commonly agreed-upon rules, spontaneously or deliberately generating a shared social order.*

The concept of 'polycentric governance,' developed across disciplines such as legal theory, economics, and political science, refers to the management of a social system where various decision-making centers operate independently but are interconnected within a framework of shared rules. This concept traces its roots to **Michael Polanyi**, a Hungarian-British polymath known for his contributions to physical chemistry and philosophy. In 1951, Polanyi laid the groundwork for 'polycentricity,' which has since significantly influenced the understanding of polycentric systems, especially in scientific communities and societal structures. Polanyi posited that multiple social systems, including **law, market, science, religion, and the arts, are inherently polycentric.** He argued that abstract ideals like justice, efficient resource distribution, objective truth, transcendental truth, and beauty drive these systems. According to Polanyi, these abstract ideals cannot be effectively imposed by a central authority on the members of a social system. He believed that centralized efforts to enforce these ideals are likely to fail due to inherent inefficiency or because such imposition is fundamentally undesirable. Polanyi's perspective suggests that, for instance, a religious body like the **Church** cannot genuinely change individuals' beliefs by imposing its version of 'transcendent truth' unless people choose to accept it. Similarly, centrally planning the optimal distribution of goods and services is challenging for a singular entity, lacking a comprehensive overview of every aspect within a community. Even when central imposition is feasible, it remains undesirable. For example, the pursuit of 'justice' is better achieved not by a single **court of law** but through the free interaction of multiple entities and agents, engaging in an ongoing dispute resolution process through trial and error and mutual adaptation. This approach allows for a more dynamic and responsive understanding of abstract ideals, aligning more closely with social systems' diverse and evolving nature (Aligica & Tarko 2012, p. 238-240).

Vincent and Elinor Ostrom, notable political economists, revitalized the concept of polycentricity by examining how complex social and economic systems could be structured to facilitate the efficient, sustainable, and accountable use of resources. They challenged the then-dominant belief that centralization was the most effective governance model. In their landmark study of American metropolitan governance in the 1960s, Vincent Ostrom, along with colleagues Charles Tiebout and Robert Warren, countered traditional public administration theories. They argued that local communities often possess the necessary knowledge and incentives to manage common resources sustainably. According to their

findings, **a system of multiple, overlapping private and public decision-making centers could outperform a single, centralized authority**. This is particularly true in scenarios where different services necessitate varying operational scales (Ostrom et al. 1961). In the subsequent decades, Vincent and Elinor Ostrom further developed polycentricity into a comprehensive social theory, underpinned by a series of innovative empirical studies. Elinor Ostrom's work on common-pool resources, which earned her a Nobel Memorial Prize, is a notable example. Her research highlighted the effective governance of these resources (Ostrom 1990, 1998, 2009). Additionally, they developed the Institutional Analysis and Development (IAD) framework, which offers a systematic approach to analyzing the governance of common resources. This body of work challenged existing paradigms and provided a new lens through which to view and understand the complexities of managing shared resources in diverse contexts.

After introducing the roots of the term polycentricity, scholars **Paul Aligica and Vlad Tarko** (2012) took a significant step in the **empirical application of polycentric governance principles** formulated by the Ostroms. They introduced a framework of three key attributes, each with specific indicators, to evaluate and understand polycentric systems. Their framework, detailed below, allows for a detailed analysis of whether a system is polycentric, its evolutionary trajectory, and its interactions with other polycentric systems:

1. Polycentric systems comprise **multiple decision-making centers**, which
(a) can actualize their unique perspectives practically,
(b) can make operational decisions independently from higher-level authorities or entities, and
(c) can have individual or shared goals.

2. Polycentric systems operate through an **overarching system of rules or institutional framework** characterized by
(a) a jurisdictional scope, which can be either territorial or non-territorial,
(b) a rule-making process involving either "insiders" or "outsiders,"
(c) decision-making methods, which could be grounded in consensus, individual decisions, or majority rule, and
(d) the correspondence between the established system of rules and the incentives for those governed by these rules.

3. Polycentric systems are not anarchic but rather **spontaneous orders** generated through the **evolutionary competition and cooperation** among the decision-making centers where
(a) the capacity to exit the system may be free or constrained,
(b) the criteria for entry into the system may be free entry, merit-based entry, or spontaneous entry, and
(c) the nature of the system's information flow may be public or private (Aligica & Tarko 2012 p. 256-257).

In summary, polycentric systems encompass a multifaceted network of interactions at various levels through power, incentives, rules, values, and individual mindsets (Aligica & Tarko 2012 p. 247).

Michael McGinnis, the former Director of the Ostrom Workshop, advanced the concept of polycentricity in 2016 by categorizing it into three distinct components: structure, process, and outcomes. According to McGinnis:

1. **Structure:** The architecture of a polycentric system is characterized by the presence of multiple autonomous decision-making centers, each with overlapping areas of responsibility. This structural aspect defines the basic framework within which the system operates.

2. **Process:** The functioning of a polycentric system is governed by the interactions between these decision-making centers. These interactions involve processes of mutual adjustment, which are influenced by competition and cooperation, as well as formal and informal relationships among the centers.

3. **Outcomes:** The results of polycentric governance manifest as emergent patterns in social order. These patterns can arise naturally or through coordinated efforts, maintaining the overarching set of rules while allowing for distinct subsystems to coexist. This emergent order optimizes efficiencies of scale at various levels, from local to global, while also supporting the self-governance capabilities of the individual centers.

McGinnis (2016) highlights that these three components are interrelated: the system's structure influences the processes, which determines the outcomes. However, he also notes that polycentric systems face inherent challenges. For instance, different groups within a polycentric system may experience varying costs for collective action, and successful groups can impose higher costs on others. The presence of multiple "veto points" can limit the scope for mutual adjustments. As systems grow more complex, the cost of participation increases, often favoring existing experts. This complexity can also hinder coordination for improvements across governance areas. Additionally, collective action dilemmas are particularly pronounced at higher levels of aggregation, and there is often no single objective uniformly pursued by all participants at every level. Due to these challenges, McGinnis argues that polycentric governance often needs to fully meet the ideal structural, procedural, and outcome-related criteria. Thus, measuring the degree of **polycentricity** in a given system is not a matter of a straightforward binary distinction but a **matter of degree**, reflecting the varied extent to which these criteria are met.

In the ongoing exploration of polycentricity, scholars have also focused on its normative aspects, particularly the debate over whether polycentric governance is generally preferable to monocentric governance. **Elizabeth Baldwin, Andreas Thiel, Michael McGinnis, and Elke Kellner** (2023) emphasize that while empirical studies show polycentric governance to be effective in certain situations, its efficacy varies. They highlight the need for more research to understand the conditions under which polycentric governance thrives or falters. The authors summarize findings from various studies, identifying several positive traits associated with polycentric governance. The **positive traits** of polycentricity include *adaptability* (the ability to tailor governance to local conditions), *learning and experimentation* (enhanced opportunities for innovation and knowledge acquisition), *resilience* (greater capacity to withstand external shocks), legitimacy (outcomes are often more accepted by the public), *collaboration* (easier identification of reliable partners), and *existence of diverse options* (accumulation of successful adjustments over time, offering a variety of choices). Conversely, the authors outline the cited **drawbacks** of polycentric governance, such as *transaction costs* (increased expenses in coordinating unified responses to significant challenges), *democratic accountability* (potential for reduced clarity in assigning responsibility), *exploitation risks* (opportunities for influential individuals to manipulate the system for personal gain), *exclusion of marginalized groups* (risks of overlooking non-institutionalized or disenfranchised communities unless they are intentionally integrated), *veto points and conflicts* (proliferation of stages

or positions within governance where a decision can be halted or lead to unresolved conflicts, impeding collective actions), *complexity* (high level of intricacy in how governance flows, maintaining the status quo), and *externalities and disputes* (increased chances of conflicts and externalities spreading across various forums).

Baldwin et al. (2023) also emphasize the importance of considering temporal and spatial dimensions to understand the effects of polycentric governance fully. They acknowledge that these **systems are dynamic and evolve over time**. To facilitate a more comprehensive analysis of polycentric governance, the authors propose a framework built upon four key factors:

1. **Contextual Conditions:** This factor focuses on the specific socio-ecological challenges that the polycentric governance system aims to address, as well as the broader governance environment in which it operates. It includes the characteristics of the actors and communities involved and the overarching institutions that allocate authority and decision-making power. Understanding the context helps identify how the governance system is positioned to meet its challenges and interact with existing structures.

2. **Operational Governance Arrangements:** This component examines the tangible governance structures within the polycentric system, including the number of decision-making centers, their respective scopes of authority, and the nature of governance processes. These processes can range from cooperative to competitive, conflictual, or hierarchical. Analyzing these arrangements provides insights into how the system functions and how power and responsibilities are distributed.

3. **Outcomes of Polycentric Governance:** This aspect evaluates the social, environmental, and governance impacts of the polycentric system. It also considers how participants perceive these outcomes. This dual focus on actual outcomes and perceptions is crucial for understanding the effectiveness and acceptance of the governance system among its stakeholders.

4. **Feedback Mechanisms:** This factor addresses how change occurs within polycentric systems over time, across different spaces, and through various jurisdictions. Change can be driven by bottom-up mechanisms (like individuals exercising their rights to voice opinions, resist changes by self-organizing, exit the blockchain system, and fork), top-down approaches (such as reforms and policy changes), or emerge organically from the outcomes of the governance itself. Understanding these feedback mechanisms is essential for comprehending how polycentric systems adapt and evolve (Baldwin et al. 2023).

In conclusion, from Polanyi's initial theory to more contemporary frameworks developed by Baldwin and other co-authors, the journey of the polycentricity concept reflects an ongoing, enriching dialogue among scholars from different disciplines. This evolution underscores the relevance of polycentricity in addressing the complexities of governance in a range of social, economic, and environmental systems, including those built upon novel technologies such as blockchain.

II. Understanding Blockchain Technology

According to Baldwin et al. (2023), the empirical studies of polycentric systems have significantly proliferated since the 2000s. Despite this growth, blockchain systems are rarely cited as examples of polycentric governance. In this section, we delve into blockchain technology's fundamental attributes and origins while also examining the inherent complexities of blockchain systems. This exploration will show why it is worth analyzing blockchain technology and blockchain systems through the lens of polycentric governance.

In a nutshell: *"Blockchain technology" represents a decentralized digital ledger of transactions. It securely records transactions across numerous computers, ensuring integrity and resistance to tampering, all without reliance on any central authority for its operation. "Blockchain systems" refer to the community of individuals and organizations involved in the development, management, and use of these blockchain networks and the applications built upon them.*

In essence, a **blockchain** operates as a distributed digital ledger, spread out across numerous computers, designed to prevent any single party from gaining total control over the network. While the technology comes in various forms, "**public and permissionless**" blockchains stand out for using cryptographic methods to guarantee that the data on the ledger is transparent, open to all, and secure against unauthorized changes. These networks are built to be censorship-resistant, meaning no single authority can control or restrict access to the network or its transactions. Furthermore, blockchains have a global reach, with nodes of the network spread across the globe, making them not bound by national borders.

The origin of blockchain technology is attributed to an individual or group under the pseudonym of Satoshi Nakamoto, who in 2008 introduced the groundbreaking concept via the whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto 2008). Nakamoto's implementation of the first blockchain was designed to function as the public ledger for all transactions occurring on the **Bitcoin** network. This innovation marked the beginning of a new era in digital transactions. Since this initial invention, blockchain technology has undergone extensive evolution, extending its utility well beyond the confines of digital currencies. A significant milestone in this evolution was the introduction of the **Ethereum** network in 2014, which enhanced blockchain's functionality by introducing **smart contracts.** These are self-executing contracts with the terms of the agreement directly written into code, which activate automatically when predetermined conditions are met. The advent of smart contracts led to the development of **decentralized applications (DApps)** and **decentralized autonomous organizations (DAOs)**, broadening blockchain's applicability. Currently, the versatility of blockchain is showcased through its myriad applications across diverse fields such as gaming, art, supply chain management, and identity verification, demonstrating its far-reaching impact.

Blockchain systems represent a sophisticated amalgamation of technology and social dynamics. They comprise the foundational blockchain technology and the network of individuals and organizations that develop, manage, and utilize it. A critical examination of how decision-making power is distributed is essential to evaluate how polycentric the governance of these intricate socio-technical systems is. In our interim report on blockchain governance practices (De Filippi et al. 2024), we undertook empirical research on 11 different blockchain networks. This research involved observing and analyzing the patterns of power distribution within these networks. From this comprehensive study, we gleaned insights that could be relevant to virtually any blockchain system, not only those around networks. These insights, detailed below, provide a nuanced understanding of the governance dynamics in these complex systems, offering a framework for assessing their polycentric nature.

1. **Layers of the Blockchain Tech Stack:** The technological stack or "tech stack" refers to the combination of technologies used to construct and operate a specific project. In blockchain technology, this stack consists of various layers, each playing a unique role. These layers include blockchain networks, DApps, and DAOs, with blockchain networks further subdivided into layer 0, layer 1, and layer 2.

- **Layer 0 Blockchains:** These provide the fundamental infrastructure for blockchain technology, serving as the bedrock upon which other layers are built.
- **Layer 1 Blockchains:** This layer consists of the blockchain protocol (which outlines the rules and procedures for data exchange, verification, and recording on the network) and the actual ledger that logs all transactions.
- **Layer 2 Blockchains:** Aimed at enhancing the efficiency and speed of transactions, layer 2 blockchains act as scaling solutions for layer 1 blockchains, addressing issues like network congestion and high transaction fees.
- **DApps:** These applications operate on a blockchain network rather than a centralized server or single computer. DApps represent a paradigm shift in application design and operation, utilizing blockchain's inherent security, transparency, and resilience benefits.
- **DAOs:** DAOs are collaborative groups functioning via the Internet with a specific objective. They use smart contracts on blockchain networks and blockchain-based assets such as tokens and cryptocurrencies to manage governance processes.

Each layer of the tech stack can form *distinct yet interconnected blockchain systems*. The governance of the blockchain systems at the bottom affects the governance of the systems that are built on top. Naturally, members of blockchain systems at the top of the stack have incentives to participate in some governance decisions of blockchain systems at the bottom.

2. **Governance Areas:** The governance of blockchain systems is shaped not only by their placement within the technological stack but also by the specific nature and type of decisions that need to be made. Across most blockchain systems, there are common decision-making areas that include:

- **Software Updates:** These decisions involve updates or modifications to the software components that the blockchain relies on.
- **Monetary Policy:** This area covers the issuance, distribution, and management of a cryptocurrency or token utilized by the blockchain system.
- **Treasury Allocation:** Governance in this area concerns how to save, spend, or invest funds pooled together within the blockchain system.
- **Rewards to Contributors:** This involves establishing policies and practices to acknowledge and reward the contributions made by community members.
- **Standards and Interoperability**: These decisions focus on processes that enable the integration of the blockchain system with other platforms and projects within the broader blockchain ecosystem.
- **Security Measures and Breaches**: This area usually involves exceptional governance processes or mechanisms, distinct from the standard governance areas, to address security-related issues.

- **Secondary Rules**: These are meta-rules that govern how to create, amend, and repeal other governance rules within the system.

Additionally, for systems built around blockchain networks, a critical governance area is:

- **Block Production:** This involves decisions on how new blocks of transactions are added to the ledger, guided by a predefined consensus algorithm.

Each of these governance areas plays a crucial role in the effective functioning of blockchain systems, influencing everything from daily operations to long-term strategic direction. Understanding these areas is essential for comprehending the complex governance landscape of blockchain technology.

3. Stakeholders: In the governance of blockchain systems, various stakeholder groups play pivotal roles, engaging directly or indirectly in one or more governance areas. These groups encompass a diverse range of participants, including:

- **Founders and Founding Teams:** Individuals or groups who initiate and develop the blockchain project.
- **Software Developers:** Professionals responsible for building and maintaining blockchain technology and its applications.
- **Organizations from the Broader Ecosystem:** Entities that are either integrated with or competed with the referenced blockchain system. These might be other blockchain projects or businesses leveraging blockchain technology.
- **Investors:** Individuals or entities that provide capital for the development and expansion of the blockchain system.
- **Token Holders:** People who own cryptocurrencies or tokens associated with the blockchain, often having voting rights or other forms of influence in the system.
- **Users:** End-users who interact with the blockchain system, either through transactions, applications, or other forms of engagement.
- **Policy Makers, Lawmakers, and Regulators:** Governmental and regulatory bodies that influence the legal and operational framework within which blockchain systems operate.

It is important to note that overlap often exists within these stakeholder groups. For instance, core software developers may also be investors in the blockchain project. Each group behaves according to their own financial and non-financial incentives, which can sometimes lead to challenges in coordination and alignment of interests. Recognizing and understanding the diverse motivations and potential conflicts among these stakeholders is crucial for effective governance in blockchain systems.

4. Governance Mechanisms: Blockchain systems employ a variety of governance mechanisms to regulate themselves. These mechanisms can be split into on-chain and off-chain.

- **On-chain Governance Mechanisms:** Also referred to as “governance by the infrastructure,” these mechanisms are embedded directly within the blockchain’s code, making them transparent and relatively resistant to change. Key examples include:

○ *Ex-ante rules and processes:* Consensus algorithms used for block production in blockchain networks.

○ *Ex-post rules and processes:* On-chain signaling and voting systems designed for amending existing governance rules.

● **Off-chain Governance Mechanisms:** Also known as “governance of the infrastructure,” these mechanisms involve decision-making processes that are not directly recorded on the blockchain. This approach offers more flexibility but often lacks the transparency of on-chain mechanisms. They include:

○ *Community-driven mechanisms:* In-person meetings, online forums, and off-chain voting, where the blockchain community collaborates and makes decisions in a more traditional, less technologically tethered manner.

○ *External party-driven mechanisms:* Laws, regulations from governmental agencies, and technology standards set by non-blockchain tech firms. These mechanisms influence blockchain governance from *outside* the blockchain community.

As noted by De Filippi and McMullen (2018), the choice between on-chain and off-chain governance mechanisms depends on the specific needs and context of the blockchain system, balancing transparency, flexibility, and responsiveness to internal and external influences.

The following example helps to illustrate the points above. Updates to the ledger in blockchain networks such as Bitcoin and Ethereum are done when the **nodes** reach consensus on the updated state via a decentralized “consensus algorithm” such as Proof of Work (PoW) for Bitcoin and Proof of Stake (PoS) for Ethereum. Consensus algorithms rely on game theoretic models to incentivize honest behavior and not propagating malicious transactions to the network by offering financial or “block” rewards for updating the ledger honestly and financial sanctions such as “slashing” within PoS networks for malicious or non-conformist behavior. The nodes that validate new transactions which are added to the ledger are referred to as **miners** (in PoW) and **stakers or validators** (in PoS). The **protocol** of public blockchain systems is often maintained and updated by **software developers** through open-source code repositories hosted on various platforms such as GitHub. While there are different software implementations that nodes need to run to interact with the blockchain network, core implementations typically emerge, such as Bitcoin Core in the Bitcoin network and Geth in the Ethereum network. Most blockchain systems, including Bitcoin and Ethereum, have processes in place for the community to discuss governance decisions, including updates to rules at the protocol and client implementation level. Examples of these processes are Bitcoin Improvement Proposals (BIP) and Ethereum Improvement Proposals (EIP), as defined in BIP-0001, BIP-002, and EIP-1, respectively. Even when these discussions are open for enthusiasts to participate, known and active **founders and founding teams**, such as in the case of Ethereum’s co-founder Vitalik Buterin, retain a considerable influence over the direction and outcome of the discussions. Running a node is usually unnecessary to use the blockchain network for transactions. Instead, **users** rely on so-called “light clients,” which connect to various nodes to read the state of the blockchain and propagate transactions across the network. To buy cryptocurrencies, users often turn to **cryptocurrency exchanges**, which enable trading fiat money, such as US dollars and Euros, for cryptocurrencies in exchange for a fee. In addition to cryptocurrency transactions, some blockchains, like Ethereum, allow for the automated execution of code, called **smart contracts**, which are the bedrock of **DApps**. DApps are built by **entrepreneurs** who sometimes rely on the money of outside **investors** who

might exert influence on their evolution. At the time of writing, the most popular DApps on Ethereum belong to the space of Decentralized Finance (DeFi), Non-fungible tokens (NFTs), and the governance of **DAOs**. **Token holders**, meaning individuals and entities holding the token or cryptocurrency used in a particular blockchain network, DApp or DAO, can also exert influence by, for example, voting on-chain. Together, they command vast resources and are backed by a large Ethereum community. The action space of each stakeholder group is, in turn, mediated by the **regulation efforts** from agents of various state and international organizations claiming to have jurisdiction over the operations related to blockchain systems.

III. Blockchain Systems as Polycentric Systems

The introduction of this report laid the groundwork for understanding polycentric governance, simultaneously highlighting the complex nature of blockchain systems. This section will address our **first research question: Are blockchain systems "polycentric"?** The response to this question is multifaceted. First, it is essential to recognize that while blockchain technology stores data in a decentralized manner, such "architectural decentralization" does not automatically equate to polycentricity. Second, the presence of polycentricity in blockchain systems can be identified both internally (endogenously) and externally (exogenously), depending on the perspectives of those within ("insiders") and outside ("outsiders") the system's overarching rules. Third, considering that polycentricity varies in extent, a more pragmatic approach is determining if blockchain systems fulfill specific criteria that set them apart from being purely monocentric. Lastly, the degree of polycentricity in blockchain systems is not static; these systems can evolve to become more or less polycentric over time through deliberate design or natural progression.

In a nutshell: *Simply being "architecturally decentralized" does not make blockchain systems "polycentric." While polycentricity is a matter of degree, all blockchain systems meet the essential criteria to be considered non-monocentric. Moreover, polycentricity in blockchain systems can be measured endogenously and exogenously by distinguishing between "insiders" and "outsiders" within the governing rules. Over time, the level of polycentricity in a blockchain system may change, whether by design or chance.*

A. Decentralization versus Polycentricity

Undoubtedly, **"decentralization"** stands out as a critical technical characteristic and a core value celebrated by many proponents of blockchain technology, often touted as a revolutionary aspect (Bodó & Giannopoulou, 2019). However, the definition of decentralization, along with its measurement and application in different blockchain systems, remains a subject of debate. Vitalik Buterin famously differentiated between **"architectural decentralization"** and **"political decentralization"** in blockchain systems (Buterin 2017). Architectural decentralization, sometimes termed "disintermediation" (Swan 2015), refers to the distribution of ledger data across multiple nodes rather than a single server, forming the technical cornerstone of blockchain technology. However, the question of political decentralization in blockchain systems is more complex. Various methodologies, from the Nakamoto Coefficient (Srinivasan & Lee 2017) to recent comprehensive taxonomies (Sai et al. 2021; Karakostas et al. 2022), have

been employed by practitioners and academics to explore the distribution of political power within blockchain systems. This analysis necessitates thoroughly examining the **intricate web of governance areas, stakeholders, and mechanisms within these systems.**

Moreover, while related, the concepts of "decentralization" and "polycentricity" have **distinct meanings** in the context of governance and organizational frameworks. These concepts are spectrums rather than binary states addressing the distribution of power and authority. **Decentralization** primarily concerns the **structural** dimension of governance, referring to the delegation of authority from a central body to various subordinate entities or levels. It highlights the power shift away from a singular locus but does not inherently ensure a multiplicity of independent decision-making entities. **Polycentricity**, as elucidated by McGuinnis (2016), represents a more expansive notion encompassing **structure, process, and outcome**. It is characterized by multiple and independent decision-making centers, each operating within a collective framework of rules. This structure facilitates a dynamic and evolving social order where these centers interact, collaborate, and sometimes compete. In a polycentric system, governance is not just decentralized but also diversified across multiple autonomous yet interrelated nodes.

B. Endogenous and Exogenous Polycentricity

Exploring the internal and external aspects of polycentricity in blockchain systems requires a deep dive into the concept of **"boundaries,"** essential for distinguishing between insiders and outsiders within these frameworks. Within polycentric and blockchain systems, boundaries are defined by the overarching system of rules. As Aligica and Tarko articulate (2012, p. 257), **insiders** are subject to the system's rules, rights, and obligations. In contrast, **outsiders** are not bound by these rules, either by their own choice or due to limitations or external constraints that preclude their participation as insiders. From this perspective, **endogenous governance** refers to the mechanisms and decisions that occur within the boundaries of the blockchain system, as defined by its rules. It encompasses the internal operations and policies directly controlled and influenced by the system's participants – the insiders. In contrast, **exogenous governance** pertains to external factors and influences that impact the blockchain system but originate outside its established boundaries. Exogenous governance can encompass regulatory decisions, market dynamics, technological advancements, and broader socio-political factors shaped by outsiders. While insiders of the blockchain system might not directly control external factors, external factors still affect the system's operations.

When considering a specific blockchain system, such as the **Ethereum network**, the distinction between its endogenous and exogenous governance is contingent upon the Ethereum overarching rule system, which defines roles and incentives.

- **Endogenous Governance:** Internally, Ethereum's governance relies on its on-chain rules, such as the Ethereum protocol and smart contracts code. Alongside these are off-chain rules, which include formal structures like Ethereum Improvement Proposals (EIPs) and informal practices, such as ad hoc online meetings among software developers. Collectively, these rules and practices form what is often referred to as the "constitution" of the blockchain system (Mannan et al. forthcoming, Zargham et al. 2023, and Alston et al. 2021).

- **Exogenous Governance:** Externally, Ethereum's governance is influenced by different types of off-chain factors. These include national and international laws and policies aimed at overseeing blockchain technology, including measures implemented by entities such as the United States Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC). Market dynamics,

notably the supply and demand fluctuations of Ethereum's native cryptocurrency ($ETH) in relation to alternative ones such as like Bitcoin ($BTC), Solana ($SOL), or Avalanche ($AVAX), play a significant role as well. Furthermore, the governance mechanisms, both on-chain and off-chain, of rival blockchain initiatives providing analogous services or targeting similar user bases, also impact Ethereum's governance landscape (Alston et al. 2021).

- **Insiders and outsiders roles:** Within this governance framework, stakeholders, including founders, software developers, validators, nodes, investors, token holders, and users are categorized as the "insiders" of the Ethereum blockchain system. Conversely, entities not directly integrated into the Ethereum network, such as competing blockchain organizations, as well as policymakers, lawmakers, and regulators, are considered "outsiders." Insiders and outsiders are not fixed individual identities but roles played within and around the (blockchain) polycentric system (Aligica & Tarko 2012, p. 254). An individual can occupy multiple roles simultaneously. For example, a person can *technically* be a "core" Ethereum software developer and a U.S. policymaker, barring any legal restrictions due to possible conflicts of interest.

Blockchain systems exhibit unique aspects regarding the nature and meaning of boundaries, distinguishing them from more traditional polycentric systems:

- **Entry and Exit in Blockchain Systems:** In polycentric systems, entry into the system can be open, merit-based, or spontaneous, whereas exit may be unrestricted or constrained (Aligica & Tarko 2012, p. 257). However, when it comes to public and permissionless blockchain systems, entry and exit are typically free but not without cost. The principle of "permissionlessness," a fundamental technical and value among some blockchain advocates, refers to the ability to participate in using, developing, and governing a system without requiring authorization from a central entity, by adhering to publicly established procedures (Nabben and Zargham 2022). This freedom in decision-making enables individuals and entities to navigate into and out of blockchain systems as they wish, without the need for external authorization or coercion. Our report on blockchain and legitimacy (De Filippi et al. 2022) contextualizes permissionlessness in blockchain systems within Albert Hirschman's framework of "Exit, Voice, and Loyalty." Hirschman (1970) posited that individuals facing organizational decline had the choice to either exit (leave the organization) or voice (express dissatisfaction), where loyalty—or a sense of belonging—may decrease the likelihood of choosing to exit. Blockchain systems, in contrast to more centralized entities like nation-states or conventional corporations, tend to have lower entry and exit barriers, thereby facilitating stakeholders' ability to depart for or join other systems with relative ease.

- **Outsiders' Influence in Blockchain Systems:** In polycentric systems, outsiders sometimes hold specific rights that are not available to insiders, such as the authority and capacity to offer formal dispute resolution services (Aligica & Tarko 2012, p. 255; Carlisle & Grugby 2017). However, outsiders frequently face difficulties in enforcing rules and regulations within blockchain systems. This difficulty is mainly due to the unique characteristics of blockchain technology, which introduce two principal obstacles to external regulation and enforcement: identifying the relevant legal framework and effectively implementing these laws (Alston et al. 2021). Firstly, identifying the applicable legal jurisdiction for blockchain-related activities can be problematic. Given the decentralized nature of blockchain, multiple states might assert jurisdiction based on the domicile of blockchain "insiders," yet confirming such presence or operational bases proves challenging. The ongoing discourse regarding classifying cryptocurrencies—as currencies, securities, or commodities—further complicates establishing a precise legal

framework for crypto-related enterprises and transactions. Secondly, even when the applicable legal parameters are clear, external entities cannot unilaterally interrupt the operation of blockchain protocols or smart contracts. This limitation has led to viewing blockchain technology as “alegal” or somewhat beyond conventional legal boundaries. The legal challenges presented by blockchain can be:

- **Spatial:** Allowing stakeholders to collaborate across state borders despite legal constraints.
- **Temporal:** The immutability of transactions and self-executing rules via smart contracts alters the traditional sequence of legal actions.
- **Material:** Enabling transactions with otherwise sanctioned individuals or organizations.
- **Subjective:** Challenging the determination of legal status for insiders due to the pseudonymous nature of blockchain transactions (De Filippi et al. 2022c).

Despite these complexities, policymakers and regulators retain significant influence in blockchain systems. While they may not be able to directly “stop” the operations of a blockchain protocol or smart contract, they can impose sanctions on individuals and entities they consider to be associated with these systems. This dynamic highlights the nuanced and multifaceted nature of regulatory power in blockchain technology.

C. Non-Monocentricity Threshold

Because polycentricity exists on a spectrum, rather than labeling blockchain systems as endogenously and exogenously polycentric, it is better to test whether they meet a minimum criteria to label them non-monocentric. This exercise involves assessing attributes and indicators. Attributes represent broader conceptual understandings, while indicators provide empirical means to operationalize these attributes.

As we briefed in the introduction, a system is considered non-monocentric if it fulfills the following criteria:

1. **Multiple Decision-Making Centers:** The system must have more than one center where decisions are made independently.
    a. **Active Decision-Making:** The decision-making centers must actively exercise or implement different opinions and preferences.
    b. **Autonomy from Outsiders:** The decision-making centers need to be able to make operational decisions autonomously from the higher level or without direct influence from external entities, including those that might enforce rules.
2. **Unified Rule Set:** Despite the autonomy of various centers, there should be a coherent and overarching set of rules that applies across the entire system.
    a. **Rule Set Utility and Transparency:** The rules of the overarching rule set need to be deemed useful by the agents subject to them, and the repercussions of non-compliance should be clear and understandable.
3. **Spontaneous Social Order:** The system should exhibit a social order that emerges spontaneously through coordination or competition among the various decision-making centers (Aligica & Tarko 2012, p. 255-256).

Attributes of Blockchain Systems

1. **Multiple Decision-Making Center:** Governance in blockchain systems is not centralized but dispersed across various stakeholder groups, including both insiders (such as developers, miners, and users) and outsiders (like competitors and regulators).

2. **Unified Rule Set:** Blockchain systems operate according to a mix of on-chain rules (coded into the blockchain) and off-chain rules (not coded into the blockchain). Off-chain rules originate within the blockchain community and in external and interrelated systems, including other blockchain systems, legal frameworks, and market dynamics.

3. **Spontaneous Order:** Rather than being chaotically disorganized, blockchain systems organically develop a structured order through the interaction of their various decision-making bodies. This order emerges from competition and cooperation among stakeholders, facilitated by relatively open (yet not costless) entry and exit conditions and the availability of governance information to the public.

Indicators in Blockchain Systems

1.a. Active Decision-Making: Stakeholders are empowered to actively participate in governance decisions, typically by expressing their opinions publicly or voting (voice), including actively resisting changes from within the system (self-organizing). They can also opt to leave for a competing system (exit) or initiate a blockchain hard fork (exit-and-voice).

1.b. Autonomy from Outsiders: Insiders, including founders, developers, and users, retain a significant degree of autonomy over their decision-making processes, even when facing external pressures such as regulatory scrutiny.

2.a. Rule Set Utility and Transparency:

- The feasibility of exiting a blockchain system incentivizes the creation of on-chain and off-chain rules that stakeholders view as beneficial.

- The repercussions of breaching the system's rules are usually clear and transparent. Given the decentralized nature of blockchain systems, punitive measures for rule violations differ from those in more traditional entities. They may involve economic losses (such as a decrease in asset value or exclusion from financial rewards) or social penalties (like a loss of reputation or trust within the community).

In conclusion, public and permissionless blockchain systems satisfy the basic criteria to classify as non-monocentric. Below, we will further explore the importance of these three indicators in the governance of blockchain systems.

Endogenous Governance: Active Decision-Making and Rule Set Utility and Transparency

The **capacity to exercise dissent** and the **utility and transparency of the overarching rules** can be exemplified by looking into the **endogenous governance** of a blockchain system. For example, in a blockchain network like Ethereum, anyone can suggest protocol improvements using an Ethereum Improvement Proposal (EIP). To successfully implement these EIPs, they need the backing of either miner (as in the older Ethereum 1.0, which used Proof-of-Work) or validators (in the newer Ethereum 2.0, which employs Proof-of-Stake) who choose whether or not to run the updated software. Maintaining the network's size partly depends on most nodes expressing support for the EIP by remaining in the

Ethereum network rather than leaving it. The ability for nodes to "exit" underscores the importance of the community perceiving the rule system as beneficial. Founders and teams behind DApps on Ethereum can continue on the updated Ethereum network or shift their operations to a different blockchain, like Solana. Centralized exchanges (CEXs) and decentralized exchanges (DEXs) hold the authority to define the terms for cryptocurrency and token transactions. Transactions may involve Ethereum's native token, Ether. Some DAOs manage the governance of some DApps, where token holders usually possess voting rights proportional to their token holdings. In cases where token holders disagree with governance decisions within a DAO, they have options beyond just voting against proposals. Sometimes, they can also choose to "ragequit" by withdrawing their stake and discontinuing participation. Ultimately, users can select which blockchain networks, DApps, and DAOs to engage. Given the blockchain community's strong commitment to open-source technology, options such as abandoning a blockchain system (exiting) or creating a replica of the system via hard forking (exiting-and-voicing) are always on the table as governance strategies. However, the costs of these actions can vary (Atik & Gerro 2018). The example illustrates that blockchain systems are governed by multiple autonomous decision-making entities, each with intersecting realms of authority. This dynamic of different centers of power overlapping has been a subject of interest in past studies (De Filippi & Loveluck 2016; Musiani et al. 2017; Böhme et al. 2015). Furthermore, each group within the system holds discretionary authority over their "constituency." The extent to which stakeholders perceive the overarching rules as convenient plays a vital role in cultivating loyalty toward the system.

Exogenous Polycentricity: Autonomy from Outsiders

The **autonomy in operational decision-making**, especially apart from **outsiders rule enforcers**, gains marked significance within the sphere of **exogenous governance**. A notable example is the recent regulatory measures implemented in the United States by bodies like the SEC and the CFTC. The SEC, in particular, is recognized for its "regulation by enforcement" approach. This strategy primarily relies on enforcement actions as the primary tool to assert regulatory authority and control over the blockchain and digital asset sector (Ubell et al. 2023). In the fiscal year 2023 alone, the SEC executed 784 enforcement actions, secured orders for almost $5 billion in financial remedies, and redistributed nearly $1 billion to investors who suffered losses (US SEC 2023b). Investigations and enforcement measures have significantly impacted CEXs, including well-known names like Binance, Bittrex, Celsius, Coinbase, FTX, Genesis/Gemini, and Kraken. Beyond CEXs, the SEC has been decisively pushing for the application of securities law to DEXs, mirroring the regulatory framework used for traditional securities exchanges. Examples include the SEC's decision in July 2023 to prolong the commentary period for its proposal to revise the Securities Exchange Act of 1934 (US SEC 2023a), as well as the announcement in February 2024 of a new rule to include certain participants as market "dealers" (US SEC 2024). This move is particularly significant against the backdrop of blockchain technology's "alegal by design" ethos, which complicates the regulation of both CEXs and DEXs. Decision-making centers within blockchain systems often have a level of autonomy that renders them relatively impervious to direct regulatory pressures. For instance, even if access to DApps is restricted via traditional web interfaces, their foundational smart contracts might continue to operate unabated on the InterPlanetary File System (IPFS). Yet, the year 2023 witnessed enforcement actions effectively disrupting operations within both the centralized finance (CEFI) and decentralized finance (DEFI) ecosystems. Strategies such as legal pursuits against DApp founding teams and instilling a sense of uncertainty among users have proven impactful. This scenario has led experts like Ostercamp (2021) to argue that while enforcing regulations without the blockchain and crypto industry's cooperation may prove challenging, a regulatory stance that solely leans on code while disregarding established legal frameworks is not viable.

D. Evolution of Polycentricity

Public and permissionless blockchain systems are non-monocentric because they meet a minimum set of requisites. However, the precise form of their polycentric governance evolves, influenced by various factors, as Baldwin et al. (2023) have outlined. We can observe this evolution through external or **contextual shifts,** such as presidential elections in the United States. The stance of a new administration toward blockchain technology can profoundly affect **how these systems operate**, potentially leading to adjustments in their **governance structures** (for example, by increasing the diversity and number of decision-making entities) and **processes** (such as the formalization of "rules on how to make rules"). New operational arrangements can impact external **social, environmental, and governance spheres.** With a greater variety of decision-making bodies, there is an opportunity for a broader spectrum of stakeholders, including those previously marginalized, to participate in governance. These changes could result in a blockchain ecosystem that is both more inclusive and diverse. Regulatory changes under a new administration could also encourage the adoption of greener technologies within these systems, such as a shift from energy-intensive Proof-of-Work to more sustainable Proof-of-Stake consensus mechanisms. Furthermore, introducing new governance structures and processes can make blockchain systems more attuned to the needs and preferences of their communities, ensuring a closer match between what users expect and what the systems deliver. These adjustments can positively affect **stakeholders' views**, potentially increasing the system's **perceived legitimacy.** The social, environmental, and governance outcomes can, in turn, **feed back** into the system, influencing future contextual conditions and operational arrangements in a cyclical pattern. For instance, favorable results may motivate advocates within the blockchain community to push for even more participatory and transparent governance structures. Simultaneously, these outcomes could lead legislators, policymakers, and regulators to develop regulatory frameworks more conducive to technological innovation, thus creating a nurturing environment for blockchain systems' ongoing development and evolution.

IV. CHALLENGES OF POLYCENTRIC BLOCKCHAIN SYSTEMS

The governance frameworks of polycentric blockchain systems adapt and transform in response to various external pressures. These outside forces can significantly shape the fundamental attributes and metrics that underscore the non-monocentric essence of these systems. In this section, we will address our **second research question: What significant challenges do blockchains face as polycentric systems?** We will explore three key challenges: misaligned interests, exceptional circumstances, and systemic risks. We will illuminate these challenges through a series of case studies: the Bitcoin scaling debate, The DAO Hack, the Terra/Luna stablecoin collapse, and the FTX cryptocurrency exchange downfall.

A. Interest Misalignment

In a nutshell: *Interest misalignment can refer to interests within a decision-making center, between decision-making centers or concerning the higher ideal driving the overall blockchain system. The Bitcoin scaling debate, which took place between 2015 and 2017, illustrates the challenges that can arise in polycentric blockchain systems when interests within and between different decision-making centers become misaligned.*

As described in the introduction, Polanyi first recognized polycentricity in systems such as the law or science, where independent decision-making centers compete, cooperate, and coexist to form a higher-level order driven by ideals such as justice or truth (Polanyi 1951). Consequently, in the context of polycentricity, interest misalignment characterizes a multi-level phenomenon that can refer to **interests within a decision-making center, between decision-making centers, or concerning the higher ideal driving the overall system**. Interest misalignment at different levels can lead to different challenges in the polycentric system as a whole. Firstly, interests of people within a specific decision-making center may become misaligned, hindering the progress within this specific center. Differences may be reconciled by forming a new, competing decision-making center or the old decision-making center seizing to exist. These potential scenarios illustrate the“free” or voluntary exit indicator mentioned by Aligica & Tarko (2012). In both cases, internal misalignment in one decision-making center can affect the work of other decision-making centers within the system and, thus, the system as a whole. Secondly, interest misalignment between different centers of decision-making may spur a process of cooperation, competition, and mutual adaptation between different decision-making centers (McGinnis 2016). In this sense, interest misalignment between different decision-making centers is not necessarily harmful in polycentric systems. However, it can also be understood as the driver of its ongoing evolution. Finally, polycentric systems require alignment across stakeholder groups on the higher goals or ideals they are pursuing, such as truth in science or justice in law. If and when this higher-level alignment breaks down, it poses a significant challenge to the polycentric system as its raison d’être is undermined. The following section describes the Bitcoin Scaling debate during which interest misalignment occurred at all three levels within the polycentric blockchain system of the Bitcoin network.

The Bitcoin Scaling Debate

The Bitcoin Scaling Debate describes a period between 2015 and 2017 during which the Bitcoin community engaged in a polarizing discussion on how best to scale the transaction throughput on the Bit-

coin network. During this time, and as the use of the Bitcoin network increased, the size of individual blocks (limited to 1MB) began to significantly saturate the number of transactions the network could process at any given time. In July 2015, several Bitcoin developers submitted the **Bitcoin Improvement Proposal (BIP) 101** that advocated for increasing the size of Bitcoin blocks to more than 1MB, thus allowing the network to verify more transactions in each block. This proposal required the implementation of a backward incompatible hard fork, demanding significant off-chain coordination and support across various stakeholder groups involved in Bitcoin's polycentric governance. Those advocating for bigger blocks, perceived Bitcoin as digital cash, which, in order to compete with other solutions such as Visa and PayPal, would need to make various tradeoffs to enable high levels of scalability, throughput, and speed. Several other Bitcoin developers contested that this proposal would require unacceptable tradeoffs on other core characteristics, such as political decentralization and censorship resistance. Bigger blocks would require more professionalized resources and capacity, thus further excluding regular users from becoming miners or validators. For them, it was paramount to maintain Bitcoin's capacity as a store of value akin to digital gold, preserving its original design and reducing the need for off-chain coordination. Scaling Bitcoin by increasing the block size in the protocol's code was not a solution. Instead, they proposed scaling Bitcoin by implementing **SegWit** (formally proposed in **BIP 141**) via a soft fork. This technical upgrade could free up space within the 1MB blocks, de facto increasing the number of transactions that could be verified per block without requiring a hard fork to implement the change. The Bitcoin Scaling debate ended with a network split, with the Bitcoin Cash hard-fork on the one hand, which increased the blocksize, and the original Bitcoin blockchain on the other hand, incorporating the SegWit proposal in August 2017.

The case illustrates the challenges that can arise in polycentric blockchain systems when interests within and between different decision-making centers become misaligned. While the issue of scaling Bitcoin triggered the broader debate, it ultimately resulted in a critical discussion on how much power each of the decision-making centers within Bitcoin holds and should hold. The outcome of the Bitcoin Scaling Debate suggests that **neither developers, miners, nor users are in sole control of Bitcoin's overarching polycentric order**—at least the part technically enshrined in the Bitcoin protocol. Furthermore, the Bitcoin Cash hard fork presents an interesting case of permissionless exit from one polycentric system to create an alternative network, using forking to resolve interest misalignment (Brekke et al. 2021).

B. States of Exception

In a nutshell: *A state of exception is a situation where the law is suspended or overridden by the sovereign power. The DAO Hack, which took place in 2016, is an example of a "state of exception" within the Ethereum network. After a hack into The DAO, community members voted in favor of a hard fork to reverse the transactions that led to the theft, an action seen by some as a violation of the tenet of immutability. Some community members who fundamentally disagreed with the decision remained in the original blockchain ledger, now referred to as Ethereum Classic.*

The concept of "state of exception" in legal and political theory is most prominently associated with the work of **Carl Schmitt,** a German legal and political theorist. Schmitt introduced and extensively discussed this concept in his 1922 book, "Political Theology" (Schmitt 2014). The author defined the "**state of exception**" as a situation where the sovereign power suspends or overrides the law. In such a state, the sovereign can transcend the rule of law, particularly in times of crisis or perceived existential threats. The idea that the "sovereign is he who decides on the exception is central to Schmitt's concept." This

tenet meant that the ultimate power in a political system was the ability to decide when the "ordinary" legal order could be disregarded. The concept of "state of exception" has been further explored and critiqued by other scholars, most notably **Giorgio Agamben**, an Italian philosopher who expanded on Schmitt's ideas in his own work, critically examining the implications of such a state for civil liberties and the rule of law. Agamben's exploration (2005) delves into how states of exception have been historically used to suspend constitutional rights and justify authoritarian measures.

While the concept of "state of exception" was developed with monocentric nation-states in mind, which operate through coercive, centralized authorities that monopolize violence, it certainly can apply to polycentric governance as well. In this case, a "state of exception" poses significant direct challenges to two of the core attributes of polycentricity presented by Aligica and Tarko (2012). Firstly, it would partly or totally suspend the institutional framework that encompasses polycentric systems. Secondly, it would reduce the relative autonomy of the multiple decision-making centers by having a central authority decide on the "exception." However, as we further explore based on the example of The DAO Hack presented below, blockchain systems offer unique technological guarantees to the challenges of the "state of exception"—the possibility of *exiting* or *forking.*

The DAO Hack

The DAO was a decentralized autonomous organization governed through open-source smart contracts running on Ethereum designed to operate as a **venture capital fund without a typical management structure or board of directors**. Instead, decisions were to be made by its investors through a voting process. The DAO did not directly possess investor funds. Instead, investors held DAO tokens, granting them voting rights on prospective projects. Investors also had the option to withdraw their funds before casting their first vote. The DAO was launched in **April 2016** and quickly became a massive crowdfunding success, raising over **$150 million worth of Ether**, around 14% of all Ether in circulation at the time, from thousands of investors (DuPont 2017).

In June 2016, an unknown attacker exploited a vulnerability in The DAO's smart contract code. This vulnerability was related to the way Ethereum smart contracts handled recursive calls. The attacker was able to repeatedly withdraw Ether from The DAO into a "Child DAO" that they controlled. They did this by requesting to withdraw Ether before the transaction was completed, making the contract repeat the withdrawal multiple times. Approximately 3.6 million Ether, which was valued at around $50 million at the time, were drained by the hacker.

When the Ethereum community learned of the attack through an urgent Reddit post (thehighfiveghost 2016), they quickly gathered in a private Slack channel to devise response strategies. In the meantime, on June 18, a communication was shared, purportedly from the attacker, which stated: "I am disappointed by those who are characterizing the use of this intentional feature as 'theft'. I am making use of this explicitly coded feature as per the smart contract terms and my law firm has advised me that my action is fully compliant with United States criminal and tort law" (The Attacker 2016). The message argued that the diverted funds should be considered a 'reward' for highlighting the system's flaw, thus adhering to the **'code is law'** principle. 'Code is law' is a phrase coined by Laurence Lessig (1999) to reference a type of regulation in which private entities can instill their own values into technological creations, thereby influencing and limiting our behaviors. In the blockchain ecosystem, it is used to describe that the code underpinning blockchain protocols and smart contract should be the definitive set of rules governing transactions or interactions (De Filippi & Hassan 2016). This ethos promotes blockchain's tech-

nical features and values of **immutability** and **autonomy**: once deployed, the code (and thus the rules) cannot be easily altered, emphasizing these digital systems' permanence and self-enforcing nature.

As reported by a variety of sources (Buterin 2016, Higgings 2016, Mehar et al. 2017), the Ethereum community embarked on one of its most crucial debates to decide how to resolve the crisis in a way that would minimize the damages to the investors and maintain the integrity of the Ethereum network. The first action was to convince major cryptocurrency exchanges to stop trading The DAO's specific tokens. Following that, the community explored a variety of options. One of the initial proposals was to implement a **soft fork**, or a backward-compatible upgrade to the blockchain, which would blacklist the transactions involving the stolen Ether, effectively freezing the funds in the attacker's account. This option would have prevented the attacker from withdrawing the stolen Ether but would not have recovered the funds. The more drastic option was a **hard fork,** a backward-incompatible upgrade to the blockchain. The proposed hard fork aimed to reverse the transactions that led to the theft, returning the stolen Ether to the original The DAO investors. This option was controversial because it went against the immutability principle that some consider central to blockchain technology. However, it was seen as a way to fully reverse the damage the attacker caused. Another option was to **do nothing** and accept the hack as a lesson in the risks and importance of security in smart contract development. This approach would uphold the principle of immutability but at the cost of significant financial loss for The DAO investors and potential damage to the credibility of the Ethereum platform. Some members of the community suggested taking **legal action** against the attacker. However, the anonymous nature of blockchain transactions and the decentralized structure of The DAO made it challenging to identify the attacker and enforce said legal action. Finally, a group of white hat hackers began using the same vulnerability to drain the remaining Ether from The DAO into a separate secure account to protect it from the attacker. This approach was a form of **self-help**, leading to the white hats to secure the remaining 8 million Ether. However, there was a catch: neither the attacker nor the white hats could access the funds in the "Child DAO" until 27 days had elapsed since the split. The DAO's smart contract included a security mechanism that 'locked' the funds in the new DAO for about 27 days.

In **July 2016,** the Ethereum community voted to decide on the course of action to respond to The DAO hack. The community used a voting mechanism called **carbonvote** to gauge the opinion on whether to proceed with a hard fork to reverse the transactions resulting from the hack. Carbonvote was a simple, web-based platform that allowed Ethereum users to signal their preference by sending a 0 ETH transaction (a "vote") from an Ether account. Ethereum holders sent these 0 ETH transactions to specific Ethereum addresses that represented *yes* or *no* to the hard fork. Approximately 85% of the participating Ethereum addresses voted for the hard fork. The vote led to the emergence of a separate blockchain called Ethereum Classic (ETC), which rejected the decision to reverse the attacker's transactions and thus maintained the original Ethereum blockchain until the hack.

The split of the Ethereum community reflected a clash of visions between immutability on the one side and pragmatism on the other side. The **Ethereum Classic** community saw the handling of the "state of exception" as an introduction to "risks of centralization" (Ethereum Classic 2016). To date, its website invokes the mantra of "code is law" and "decentralism." Another important aspect of The DAO hack is that it attracted the attention of "outsiders," such as the United States' Security and Exchange Commission (SEC). Its Enforcement Division inquired whether associated entities and individuals had "violated federal securities laws with unregistered offers and sales of DAO Tokens in exchange for 'Ether,' a virtual currency" (US SEC 2017).

In our previous academic work (De Filippi et al. forthcoming), we explored how the resolution of The DAO hack diverged from traditional "states of exception" encountered in other systems. Unlike the inhabitants of nation-states, individuals who disagreed with the majority's decision in the blockchain context had the tangible option to continue on the original Ethereum blockchain or migrate to an alternative blockchain network. This capacity to operationalize dissent by choosing a different path highlights a unique aspect of blockchain systems. Consequently, even though the foundational principles of non-monocentricity might have been momentarily put to the test, the community within the blockchain system leveraged available tools to navigate and potentially overcome these challenges.

C. Systemic Risks

In a nutshell: *Systemic risk refers to the potential for a widespread collapse within an ecosystem, triggered by the failure of a single component, which then has far-reaching consequences across the entire system. The collapse of the Terra/Luna stablecoin in 2022 affected the DeFi ecosystem as a whole. Likewise, the downfall of FTX, a centralized cryptocurrency exchange, had ripple effects across the ecosystem, which attempted to self-regulate through informal norms and standards by doubling down—albeit temporarily—on their commitment to "decentralization."*

Systemic risks can be defined as the potential for an ecosystemic collapse triggered by the failure of a single component, with significant repercussions across the ecosystem as a whole. Kaufman (1996) noted that systemic risk escalates with the degree of interconnectedness among all participants in the system. In financial markets, this interconnectedness means that an initial shock in one institution can be passed on to other institutions, causing a domino effect that can impact the whole market (Kaufman & Scott 2003). Factors such as high leverage, information asymmetry, lack of relevant information, and questionable accounting procedures make it particularly challenging to distinguish between solvent and insolvent entities in the financial market before a crisis occurs (Kaufman & Scott 2003). In the context of polycentric blockchain systems, autonomous yet interconnected decision-making centers alongside a lack of regulatory clarity can intensify the threat of systemic risk. In this section, we describe the collapse of the Terra/Luna stablecoin, and the downfall of the FTX cryptocurrency exchange to illustrate how polycentric governance systems, if not adequately governed, can be exposed to systemic risk.

Terra/Luna

The **Terra/Luna** collapse presents an example of how the failure of a particular component in the DeFi ecosystem can have a cascading effect, impacting the broader cryptocurrency market. The failure led to the insolvency of numerous projects and inflicted significant financial losses on investors, amounting to billions of US dollars.

In 2018, **Kwon Do-hyung**, a South Korean businessman, co-founded Terraform Labs, a company focused on the development of a stablecoin (Terra) that used a secondary cryptocurrency (Luna) as a governance token (Kereiakes et al. 2019). **TerraUSD/UST was a stablecoin pegged to the U.S. dollar**. Like other algorithmic stablecoins in the DeFi ecosystem, TerraUSD was not backed by fiat assets. Instead, it relied on the Luna governance token to absorb volatility by facilitating the swap between Terra and Luna at Terra's target exchange rate (Kereiakes et al. 2019). As the market value of Terra and Luna were highly dependent on each other, the inefficiencies of either one meant a considerable risk

to the entire Terra/Luna ecosystem, eventually leading to its rapid collapse. **In May 2022, right before Terra UST lost its peg to USD**, UST reached its peak market capitalization by surpassing $18 billion. Being the third largest stablecoin at the time, the depegging event triggered immediate investor panic, leading to a surge in UST withdrawal and swap activities, with almost no market demand for the Luna cryptocurrency. Multiple factors may have been responsible for the crash. In addition to the algorithmic stablecoin design vulnerabilities and allegations of a coordinated attack targeting the Terra ecosystem, it was concluded by several sources that the Anchor Protocol funds outflow put increased pressure that eventually broke the UST peg (Barthere et al. 2022).

Anchor was introduced in 2020 as a **savings protocol** on the Terra blockchain (Platias et al. 2020). It quickly became one of Terra's most popular projects, offering nearly 20% annual percentage yield (APY) for UST deposits. The introduction of Anchor resulted in the increase of the circulating UST in the market, along with a rising number of lenders and a relatively small number of borrowers, which is believed to have caused the reserves to decrease over time. By April 2022, more than 72% of all USTs were deposited in Anchor, which underlined the critical state of UST's dependency on Anchor's success (Kelly 2022). On-chain analysis performed by the Nansen research team showed that a few players moved the funds out of the Anchor protocol prior to the depeg. Specifically, from 7-10 May 2022, the top 20 addresses collectively withdrew 2 billion UST from Anchor through a total of 5,051 transactions (Barthere et al. 2022). Whether the substantial unstacking and selling were a reaction to market volatility, vulnerability exploits, or a deliberate attack is a subject of ongoing debate.

Even the **Luna Foundation Guard (LFG)**, established in February 2022 to support and uphold the UST peg, proved unsuccessful in mitigating the consequences of the market crash. The whole Terra ecosystem suffered from a liquidity crisis where the entire value of Luna could not balance out the value of UST. The efforts to defend the depeg involved liquidating reserves totaling billions of US dollars in various cryptocurrencies such as BTC, BNB, and USDT. However, those efforts were unsuccessful and may have contributed to a subsequent decline in the broader DeFi ecosystem, negatively affecting projects like Alameda Research, a quantitative cryptocurrency trading firm closely linked to the FTX crypto exchange.

FTX

FTX was a cryptocurrency exchange and trading platform headquartered in the Bahamas and founded by Sam Bankman-Fried in 2019, following the (seemingly) successful launch of his other major venture, Alameda Research, a quantitative cryptocurrency trading firm two years previously. The two ventures had always been closely intertwined, with Alameda incubating FTX at its early stages and using the exchange subsequently, thus providing the platform with liquidity and ensuring that FTX could fulfill its role as a market maker from its outset. After the incubation phase, the two companies were to be operated independently of each other, a legal requirement to hedge against insider trading and other collusion dynamics.

Both firms grew steadily, with FTX raising over $1.8 billion in capital, according to Crunchbase data, at a valuation of $32 billion before their demise in November 2022. The trouble started after CoinDesk, a cryptocurrency news outlet, published an article citing a leaked Alameda balance sheet, which showed that the company was heavily indebted to FTX and much of its collateral was held in FTT, the FTX native tokens issued by the exchange itself. Responding to the article, Changpeng **"CZ" Zhao announced that he would sell the remainder of his substantial FTT holdings.** CZ was the founder and (by then) the CEO of Binance, the world's largest cryptocurrency exchange at the time of writing, and an early

investor in FTX. The interactions following this Tweet led the price of the FTT token to drop by over 90%, from about USD26 at the beginning of November to around USD2 on 9 November. Despite repeated reassurances and attempts by both Bankman-Fried and Alameda CEO Ellison that they would be able to raise the capital required to cover the liquidity gap, **Alameda filed for Chapter 11 bankruptcy on 10 November, followed by FTX on 11 November**, which comprised 136 separate entities and including FTX US, which had until then been heralded as being fully solvent (Keoun 2022).

Subsequently, ongoing court proceedings revealed Alameda had borrowed significant customer funds from FTX against predominantly FTT-based collateral and used them to invest in the market, which rapidly turned down following the collapse of Terra/Luna, leaving Alameda unable to service its debt and FTX subsequently unable to payout customer funds (Koo et al. 2022). Beyond the plainly **illegal and irresponsible management of customer funds**, competitive market forces (Alston et al. 2021) ultimately contributed to the collapse of FTX.

From the perspective of polycentricity, observing how other **autonomous units within the ecosystem began to rapidly adapt their practices** in response to the FTX collapse to self-regulate the space through informal norms and standards is interesting. Actors in the blockchain space also started doubling down on "decentralization" as an overarching value guiding the ecosystem (Aligica & Tarko 2012). New norms and standards emerged, at least for a time, in the form of other centralized exchanges beginning to publish proof of reserves (Asmakov 2022) following the FTX debacle. The value of decentralization was tangibly re-emphasized by users withdrawing their holdings to self-custody wallets and moving to decentralized alternatives, causing a run on *de facto* crypto banks (Bambrough 2022). At the same time, the Ethereum community started accelerating efforts on Account Abstraction. This technical upgrade improves the user experience of using non-custodial wallets, making it more competitive to hold funds on centralized exchanges (Crypto.com 2023). Finally, the FTX case also illustrates the effects of the outsider's governance forces overseeing the blockchain industry, as the ecosystem now faces increased regulatory scrutiny, with SEC activity increasing by almost 200% in the six months following the FTX collapse (Coghlan 2023).

V. Legitimacy in Polycentric Blockchain Systems

Another factor influencing the governance evolution of blockchain polycentric systems is legitimacy. This section addresses our **third research question: What makes a polycentric governance system legitimate?** As discussed in our report on blockchain technology and legitimacy (De Filippi et al. 2022b), speaking of legitimacy inevitably requires referring to Max Weber's work, according to which "legitimacy" refers to the acceptance of a system exercising authority or power over those subject to it (Weber 1964). While Weber focused on legitimacy in predominantly single-authority systems like nation-states, Julia Black (2008) explains why individuals within a polycentric system might accept it, whether due to moral alignment, the system serving their interests or goals, or a belief in its inevitability. In the case of blockchain polycentric systems, achieving both endogenous and exogenous legitimacy may require compromises, as efforts to strengthen one can sometimes undermine the other. Through the examples of The Ethereum Merge and Tornado Cash, we delve into how polycentric blockchain systems navigate the intricate balance between internal and external legitimacy.

A. Polycentric Co-regulation

In a nutshell: *Polycentric co-regulation is an effort undertaken by public and private actors, or by "code" and "law," to regulate a blockchain system. While this strategy may be the most "efficient," it is unclear whether it would be perceived as legitimate by "insiders" or "outsiders."*

During the reading group sessions on blockchain and polycentricity, we learned that, for some authors, **polycentric co-regulation** between public and private actors offers the **most efficient** way of governing polycentric blockchain systems (Ostercamp 2021). However, whether such a co-regulatory effort would be perceived as *legitimate* is a more complex question. According to Ostercamp, if **"legitimacy" is grounded in the perception of "fairness" or "acceptance" of the actions of an organization by those who are subject to them,** the legitimacy of co-regulatory efforts will be determined by how the public and private actors involved perceive the legitimacy of each other's actions. For co-regulation to work, certain actions of private actors have to be accepted by public actors as being legitimate, and certain actions of public actors have to be accepted by private actors as being legitimate.

However, there is no guarantee that such perceptions of legitimacy will exist. **Firstly, balancing "insiders" and "outsiders" expectations is challenging.** On the one hand, a community of users, developers, and other participants of a blockchain system may consider the extraterritorial application of state laws to persons or activities outside of a state's jurisdiction to be illegitimate. In such circumstances, there is no "consent of the governed" (Greene 2016) and state law may impose unjust or impractical outcomes. Blockchain systems that adhere to such state laws would consequently have **low endogenous legitimacy** as the system is not acting in the interests of network participants. On the other hand, the state may consider the regulation of DeFi via smart contract code to lack legitimacy since it confers rule-making authority to software developers who do not have a public democratic mandate, and code-based regulation may not necessarily respond to "socially desirable" public interests (Ostercamp 2021, p. 34). Thus, a blockchain system that adheres to a code-is-law rule system would have **low exogenous legitimacy** as the system does not accommodate interests beyond those of network participants.

Secondly, the expectations of "insiders" and "outsiders" regarding blockchain systems are not uniform. As we touched upon with the concept of blockchain *alegality*, external figures such as policymakers, lawmakers, and regulators often have differing views on how state law applies to blockchain

systems, including questions of jurisdiction and the relevant legal framework. Similarly, within the blockchain community itself, perspectives on the principle of "code is law" vary significantly, a divergence highlighted by the aftermath of The DAO Hack and the resulting split in the Ethereum community. While some members of the community may be open to engaging with the wider legal and regulatory landscape, others may show considerable resistance. When the decision-making entities within a blockchain system choose to adhere to legal and regulatory standards, it may prompt those who disagree to "exit" or initiate a "fork" of the community.

However, legitimate efforts of polycentric co-regulation are not impossible. For blockchain systems to be recognized as legitimate by both insiders and outsiders, a sustained and in-depth grasp of the expectations of all stakeholders is essential. Additionally, the creation of pragmatic regulatory frameworks that offer clear guidelines while maintaining sufficient flexibility is crucial. This approach ensures that there is room for responsible technological innovation.

B. Endogenous Legitimacy

In a nutshell*: Insiders have expectations about how blockchain systems should legitimately operate. When these expectations are not met, the endogenous legitimacy of a blockchain system usually suffers. For this reason, at a minimum, the blockchain system must ensure that those directly impacted by governance decisions can participate in the decision-making process. Additionally, it should provide all stakeholders with the ability to exit the system if they choose. The Ethereum Merge is a positive example of how the delicate balance between exogenous legitimacy and endogenous legitimacy can be struck.*

As we have explained elsewhere (De Filippi et al. 2022b), **endogenous legitimacy is crucial to blockchain systems** as it helps organically retain network participants within a blockchain system. The perception of endogenous legitimacy increases loyalty and deters participants from exiting or forking the original blockchain system. As a consequence, endogenous legitimacy has an important function in generating network effects and ensuring the long term viability of the system. Drawing from Julia Black's insights (2008), members might view a blockchain polycentric system as legitimate if it aligns with their interests or moral values. Simply put, **when these systems fulfill members' expectations, they are more likely to be regarded as legitimate**. Conversely, failing to meet these expectations can erode participants' confidence in the blockchain (De Filippi et al. 2020), thereby endangering its endogenous legitimacy.

In (De Filippi et al. (forthcoming) we explored the origins and some examples of the most important expectations held by members of blockchain systems about how such systems should legitimately operate:

1. Some of these expectations stem from the **core technical properties of public permissionless blockchain systems:**

- **Transparency:** As transparent systems, all network participants expect to know the network's protocol and consensus algorithms, and be able to read certain data about transactions.

- **Pseudonymity:** While certain data is public, there is an expectation that participation in the network will be pseudonymous, as a public/private key pair and public blockchain address is only necessary to execute transactions. With all the transactions being cryptographically signed with a

private key, network participants can be confident that the holder of a private key has executed a transaction—unless they can later prove they have been coerced in some way.

- **Resilience and tamper-resistance:** As an append-only ledger, it is expected that data on the blockchain will only be added and never be retrospectively edited or modified. If there is an (illegitimate) attempt to modify recorded transactions in this way, then all the nodes maintaining the network will become aware of such an attempt. Shutting down one or more nodes will not disable the entire network, as copies of the ledger are maintained by all nodes, making it possible to replicate the network from any one node.

- **Permissionlessness:** As permissionless systems, not only can anyone buy crypto-assets, anyone can become a miner, validator, and developer in these systems without requiring any person's permission, provided they meet certain common technical or economic requirements.

- **Active consent:** A corollary to permissionless entry (and exit) is the inability of network participants to technically coerce another. Developers cannot coerce nodes to accept upgrades to a blockchain protocol, as the implementation of such upgrades require their active consent. It is, instead, possible for some network participants to decide to fork the underlying blockchain protocol, as we mentioned happened after The DAO attack. Conversely, with the developers of major public, permissionless blockchain networks being a fluctuating group of individuals, some of whom are difficult to identify, coercion by network participants is unlikely to be effective.

2. Another source of expectations is the **writings of influential insiders** in the blockchain space such as Ethereum co-founder Vitalik Buterin, which usually reflect an ideological commitment to negative liberty (Berlin 1969):

- **Credible neutrality:** One example is Buterin's argument that blockchain systems should be credibly neutral mechanisms, which means that it should not appear that the mechanism discriminates for or against anyone (Buterin 2020).

However, **a system that is endogenously legitimate may be perceived as having low exogenous legitimacy**, as they do not meet the expectations of external actors such as national governments. A prominent illustration of this in the blockchain space is the environmental footprint of public, permissionless blockchain networks like Bitcoin and Ethereum, which has created a negative public image of these networks. The Ethereum Merge, finalized on 15 September 2022, was in part a response to this image and ushered in a drastically less energy intensive 'Ethereum 2.0'. It is also a positive example of how the delicate balance between exogenous legitimacy and endogenous legitimacy can be struck.

The Ethereum Merge

The history of **Ethereum 2.0** is almost as old as Ethereum itself. As Buterin mentioned during a viewing party in the leadup to The Merge being executed (Fortis 2022), the plan of transitioning from a computationally- and resource-intensive PoW to a PoS system had been "the dream" from as early as January 2014. In a blog post on 15 January 2014, **Buterin had identified two major advantages of PoS over PoW:** it would remove the need to perform "useless calculations to secure the network" and, relatedly, would obviate the need for miners to operate specialized hardware, which could potentially concentrate mining power in the hands of wealthy parties that can afford to accumulate mining equipment (Buterin 2014). In short, according to Buterin, PoS could reduce the environmental footprint of Ethereum and diminish the risk that the network would be subject to plutocratic governance. PoS would replace network security gained through the burning of energy by security gained through people wishing to avoid significant economic losses (Buterin 2016).

However, the challenge laid in designing a PoS protocol for Ethereum. This was as much a challenge of designing incentives as it was a technical challenge. For instance, there was a risk that a validator in a PoS system selfishly validates transactions on both an original and forked blockchain, thereby compromising the primary way in which a "legitimate blockchain" is determined (Buterin 2014). This risk existed because nothing was actually at stake in early experiments with PoS systems. As a result, Buterin and, later, Vlad Zamfir conceived of 'slashing' mechanisms in which validators in PoS systems would be penalized for bad behavior. This would involve validating nodes paying a "security deposit" to be able to have the right to block produce and earn returns, while losing said deposit if the rules of the system were infringed (Zamfir 2016a). To take another related example, there was a risk that nodes could simply be bribed to hand over their private keys to an attacker, allowing the attacker to eventually "take control of the blockchain" and "create 'fake histories' at will" (Zamfir, 2016b). Zamfir suggested that this challenge could be tackled by only accepting messages about the state of the network from nodes that *maintained* deposits at the time the message was sent. In the following years, Buterin, Zamfir, and others continued to discuss how to reinforce the security of PoS protocols, such as preventing bad actors' efforts to revert the finality of Ethereum transactions, and incentivize good behavior by network participants (Buterin 2018; Buterin & Griffith 2017). These and other technical challenges continued to be discussed and researched over the years, with updates provided on social media, blogs, and other online resources.

As the Ethereum network's popularity surged, **voices from outside the immediate blockchain community,** including environmental NGOs, policymakers, academic, and financial institutions, **started voicing concerns about the energy consumption of cryptocurrencies**, especially Bitcoin and Ethereum (Neumueller 2022, 2023). The central worry was that, amid escalating climate change, the PoW consensus mechanism Ethereum previously utilized consumed as much energy as countries the size of Finland, contributing minimally to the economy. In contrast, some defended PoW mining's environmental impact, arguing it encourages the shift to renewable energy, aids in balancing electricity grids, and minimizes energy wastage (Rennie 2023). Nonetheless, the intense public scrutiny on PoW mining's energy use significantly influenced the blockchain community's perception, leading to a notable increase in discussions about the benefits of PoS, particularly its potential for reducing carbon and environmental footprints, in subsequent analyses of the PoS consensus mechanism.

To test whether their PoS consensus protocol worked and was secure, **in December 2020 the 'Beacon chain' was launched** in parallel to the Ethereum main chain, which continued to operate using PoW

consensus. This allowed the testing of whether this new protocol could maintain consensus about its own state without vulnerabilities and downtime, while the PoW consensus system of the Ethereum main chain continued to process and secure transactions. **The Merge was finally executed on 15 September 2022**. The consensus clients of the Beacon chain replaced the main chain as the consensus layer, while the original clients formed the execution layer with both layers being able to communicate with one another (Ethereum 2023). PoW mining was discontinued, but all the Ethereum transaction history was preserved.

The Merge can be seen as an attempt to address this public concern in a manner that does not diminish endogenous legitimacy and comports with the polycentric nature of blockchain networks. This was achieved due to multiple procedural considerations being taken into account:

1. Firstly, the plan to eventually transition to PoS had been **announced at an early stage**, so network participants knew that this was part of the roadmap from the time they joined the network

2. Secondly, the PoS protocol was **carefully tested over a period of time.**

3. Thirdly, the transition **didn't lead to network downtime**, thereby not disturbing network participants.

4. Fourthly, the implementation of The Merge **required the thousands of nodes to actively and voluntarily agree to upgrade their clients**, for instance, by running both a consensus client and an execution client. In other words, nodes could not be directly coerced into accepting these upgrades by developers or other third parties. As always, it was possible for a fork to take place, and immediately prior to The Merge, a prominent Chinese Ethereum miner did try to organize a fork that would retain proof-of-work consensus (Lutz 2022). It was also possible for network participants to leave Ethereum, with the ETC Cooperative, the organization supporting the development of Ethereum Classic, reporting a surge of interest in the proof-of-work based Ethereum Classic in the leadup to The Merge (Munster 2022).

5. Finally, **expectations were managed**. The energy usage of Ethereum was indeed dramatically reduced (Neumeuller 2023)—the Ethereum Foundation estimates by 99.95%—but no commitments were made that, for example, transactions would become faster as a result of The Merge.

The fact that The Merge did not lead to a mass exodus of participants from the network, nor lead to the complete collapse of the value of Ether, indicates that **this process was broadly considered to be endogenously legitimate.** The existence of the factors described above confirms that it is possible for polycentric governance in blockchain systems to be endogenously legitimate provided there are opportunities to effectively participate in governance and exit from the system. Importantly, the example of the Ethereum Merge offered lessons for polycentric co-regulation. It demonstrated how external actors can shape social norms, for example, about contributing to environmental harm, in a manner that leads to a change in the technical architecture of the blockchain system so that public policy concerns are addressed, but without imposing inefficacious or punitive regulations or compromising the endogenous legitimacy of the system (De Filippi et. al 2024).

C. Exogenous Legitimacy

In a nutshell: Outsiders also have expectations about how blockchain systems should legitimately operate. When these expectations are not met, the exogenous legitimacy of a blockchain system suffers. These expectations may involve compliance with existing legal and regulatory frameworks. However, given the nascent and "alegal" nature of blockchains, this is no easy task. For this reason, at a minimum, blockchain systems should ensure that their governance processes and outcomes do not purposefully harm the wider ecosystem. The Tornado Cash case exemplifies the struggle to strike a balance between endogenous legitimacy and exogenous legitimacy.

In our study of blockchain and legitimacy (De Filippi et al. 2022b), we mentioned existing literature on the **exogenous legitimacy of blockchain systems** (Vilet 2019, Rosati et al. 2021, Dimitropoulos 2022, Reinsberg 2021). These writings seem to indicate that exogenous legitimacy **also depends on whether expectations are met**. Following Black's (2008) analysis, expectations generally involve the blockchain system serving external interests or functioning in a perceived correct manner. **Pragmatic views** on external legitimacy may emerge when, for example, blockchain systems enhance the operational efficiency and transparency of public and private organizations. Conversely, **moral or normative** views are based on the system's adherence to legal and regulatory standards. Yet, as highlighted across this report, ensuring compliance with these standards poses a significant challenge due to blockchain's inherent design features. To maintain a baseline of moral or normative legitimacy from an external viewpoint, it is essential that the blockchain system **avoids producing negative impacts on the broader ecosystem**.

Interestingly, the very attributes that may grant a blockchain system endogenous legitimacy, such as autonomy or immutability, may at times conflict with the criteria for exogenous legitimacy. The case of Tornado Cash, penalized by the United States' Treasury's Office of Foreign Assets Control (OFAC), illustrates the delicate balance between legitimacy perceptions of "insiders" and "outsiders," showcasing the nuanced interplay between satisfying internal community values and external societal expectations.

Tornado Cash

Initially released in 2019, **Tornado Cash** is a collection of open source smart contracts on Ethereum that provides privacy for cryptocurrency transactions. It operates by breaking the on-chain link between a sender's and a recipient's addresses. To do so, Tornado Cash allows users to send cryptocurrency to a smart contract *from one address* and withdraw *to another address* after mixing the users deposits (Chainalysis 2023). In this way, the public link between the deposit and withdrawal addresses is obfuscated, without the user ever losing control over their cryptocurrency.

Tornado Cash became quite popular among users seeking privacy for their Ethereum and other cryptocurrency transactions, particularly those who valued anonymity for legitimate personal or business reasons, as well as those concerned about the public nature of blockchain transactions. At its peak, its transaction volume reached USD 2.8 billion (Malwa 2023). Popularity was not just limited to individuals seeking privacy; it also attracted attention from various entities and developers interested in the broader applications of privacy-preserving technologies within the blockchain ecosystem. For example, Tornado Cash's innovative use of cryptographic proofs (such as zero-knowledge proofs) to enable privacy without sacrificing the security and integrity of transactions was a significant contribution to the field of blockchain technology.

Popularity also came with controversies. As one might expect, this service can be used for both legal privacy-preserving purposes and illegal purposes. Soon enough, Tornado Cash was subject to regulatory scrutiny for allegations of it being used for money laundering and terrorist financing (Wade et al. 2022). **In August 2022, the US Treasury's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash.** The initial and subsequent sanction notices (US DOT 2022a, 2022b) explicitly mention the use of Tornado Cash by a collective of North Korean hackers for laundering proceeds from their hacks of US-based crypto-firms and for assisting sanctioned North Korean governmental entities. This sanction was introduced despite Tornado Cash's own **efforts to add a third-party tool** that would block crypto-wallets tied to individuals and entities that had been sanctioned by OFAC from accessing the front-end of the Tornado Cash dApp (Gkritsi 2023). The smart contracts, nonetheless, were still accessible by sanctioned entities and individuals through the InterPlanetary File System (IPFS).

Soon after the sanctions were announced, **Tornado Cash developers 'went dark' or ceased public activity**, and the platform's interface went down, although the smart contracts were still accessible and the system continued to be used. Following the sanctions, Flashbots—one of the most popular Ethereum clients—enabled the filtering of transactions linked to Tornado Cash's sanctioned addresses. Consequently, **over half of Ethereum's block producers started to block Tornado Cash transactions**, regardless of their own exemption from OFAC sanctions (Carreras 2022). Most significantly, on 10 August 2022, **one of the Tornado Cash software developers was arrested in the Netherlands** and was indicted by the Dutch Public Prosecutor for allegedly writing code for software that facilitates money laundering (FIOS 2022).

The US OFAC sanctions targeted Ethereum smart contracts, sparking a significant debate within the blockchain ecosystem about privacy, free speech, and the extent of regulatory oversight. Some argued that sanctioning smart contracts exceeded the power granted to the Treasury Department, given that it could only impose sanctions on individuals, not software. They also alluded that the sanctions were an attack on the First Amendment of the US Constitution, particularly the right to freedom of speech, by highlighting legal precedents that recognized computer code as a type of language and software as a form of expression (Opsahl 2022, Reynolds 2023b). Others disagreed with the argument that the sanctions were indeed restraining free speech and saw the measures taken as necessary: *"Researchers are not prohibited from copying, posting, 'discussing, teaching about, or including open-source code in written publications, such as textbooks.' (...) OFAC's actions are aimed at preventing persons from using software applications that undercut one of the most basic functions of government: regulating activities that it deems endangers national security"* (Farrell and Schneier 2022).

An important architectural feature of the project is that the **Tornado Cash system was intentionally designed to be polycentric and its smart contracts were purposefully immutable and unstoppable.** As the Tornado Cash team explained on 20 May 2020, the aim was to live "by the precepts that code is law" (Tornado Cash 2020a). In January 2022, Tornado Cash co-founder Roman Semenov told CoinDesk: *"There is not much we can do in terms of helping investigations because the team doesn't have much control over the protocol"* (Reynolds 2022a). This meant that, once deployed, the smart contracts cannot be altered or controlled by any single entity, including the development team or participants in Tornado Cash's decentralized autonomous organization (DAO), which governs the Tornado Cash protocol. The Tornado Cash DAO was created to allow for certain aspects of the Tornado Cash protocol to evolve through decision-making by the DAO's members, while nonetheless preserving the immutability of the smart contracts that pool and redistribute the cryptocurrencies (Tornado Cash 2020b).

The Tornado Cash case study illustrates many crucial aspects of the governance of blockchain polycentric systems:

1. Firstly, despite the operational autonomy of smart contracts, **the enforcement of sanctions against Tornado Cash shows the impact of legal and regulatory pressures on blockchain polycentric networks.**

- The detention of one of the Tornado Cash software developers exposed the limitations of deeming blockchain technology "alegal," since individuals involved in blockchain projects can still be targeted by legal actions, even when smart contracts cannot be unilaterally "stopped."

- The reaction of other interconnected blockchain systems such as Flashbots and the Ethereum network block producers show a different aspect of systemic risks. The impact of regulatory enforcement can, indeed, also spread out across the blockchain ecosystem beyond the targeted entities.

2. Secondly, it shows **how a blockchain polycentric system that may enjoy endogenous legitimacy can still face inherent challenges in achieving exogenous legitimacy**.

- For "insiders" that valued precepts such as "code is law" and privacy-preserving technologies, Tornado Cash was likely to meet their expectations and thus be perceived as endogenously legitimate.

- However, some "outsiders" saw those same architectural features as catalysts of negative externalities, such as threatening US national security by facilitating money laundering and financing of terrorist activities.

Together, these aspects underscore the ongoing struggle to strike a balance between the need to abide by the principles and ideologies of blockchain systems in order to achieve endogenous legitimacy, and the need to comply with external regulatory pressures in order to enjoy exogenous legitimacy.

CONCLUSION

This report addresses the polycentric governance of blockchain systems, following conversations held from September 2022 until September 2023 by a reading group of blockchain practitioners and academics. The ERC-funded BlockchainGov project led the reading group. Since the publication of the Bitcoin whitepaper in 2008, blockchain technology has gained increasing popularity for being a "decentralized" ledger of transactions. Collectives of people have formed to discuss and decide on—to "govern"—the evolution of blockchain networks and blockchain-based applications, creating what we refer to as "blockchain systems." While much literature is dedicated to understanding the governance of blockchain systems, no substantial efforts have been made to apply the concept of "polycentricity" to blockchain governance. Polycentric governance systems are characterized by multiple autonomous decision-making centers with overlapping areas of responsibility, which both compete and cooperate within a common overarching system of commonly agreed-upon rules, spontaneously or deliberately generating a shared social order. A term initially presented by Michael Polanyi and famously further developed by Vincent and Elinor Ostrom, polycentricity allows us to understand blockchain systems' structure, process, and outcome.

Throughout this report, we came to the following conclusions:

1. Nature of blockchain systems: Polycentricity in blockchain systems entails more than just "architectural decentralization." It involves evaluating the governance of the blockchain system both internally and externally from the perspectives of "insiders" and "outsiders" to the rules governing it. By recognizing polycentricity as a spectrum, the focus shifts from merely determining if a blockchain system is "polycentric" to assessing if it surpasses a specific threshold that distinguishes it from being "monocentric." Additionally, the nature of polycentricity within these systems is dynamic and subject to change over time, whether through deliberate design or unintended evolution.

2. Challenges: Despite their non-centralized decision-making framework, polycentric blockchains are vulnerable to disruptions that can compromise their stability and integrity. Firstly, the presence of multiple independent decision-making centers, each driven by distinct and sometimes *conflicting incentives*, poses governance challenges, such as achieving consensus. Secondly, *security breaches and hacks* can precipitate critical "states of exception," during which the standard governance rules might be temporarily suspended in favor of more centralized interventions by certain actors, thus impacting the system's overall operation. Thirdly, these systems are not immune to *systemic risks*; the failure or malfunction of a single decision-making center, due to issues like bankruptcy, fraud, or operational failures, can trigger cascading effects across the network.

3. Legitimacy: The perception of blockchain systems as legitimate by insiders (endogenously) and outsiders (exogenously) is crucial to their survival and sustainability. Simultaneously ensuring endogenous and exogenous legitimacy is challenging, but not impossible. It requires a deeper and continuous understanding of all stakeholders' expectations and the development of pragmatic regulatory frameworks open to responsible innovation. Endogenous legitimacy in polycentric systems hinges on the effective participation of all stakeholders impacted by decisions and the option for these parties to exit the system if desired. This underscores the importance of inclusivity and autonomy within the system, ensuring that all voices are heard and considered in decision-making processes. Exogenously, the legitimacy of a polycentric system is contingent upon its operations and outcomes not adversely affecting the wider ecosystem to which it is connected. This external perspective of legitimacy emphasizes the responsibility of the polycentric system to operate in a manner that is harmonious and sustainable, avoiding negative repercussions on the broader environment and communities it interacts with.

Blockchain technology has made possible novel configurations of governance, opening the door to new opportunities and challenges in collective action and decision-making. We strongly advocate for further research into the governance of blockchain systems, focusing not only on descriptive analyses of how trust, confidence, and legitimacy are cultivated within these communities but also on prescribing best governance practices. Such research should aim to offer actionable insights and frameworks that can guide blockchain communities in sustainably governing themselves. By identifying and promoting effective governance mechanisms, we can help ensure that blockchain ecosystems are able to navigate the complex challenges they face, fostering environments where trust and legitimacy are enhanced, and thereby securing their long-term viability and success. This endeavor is crucial for the advancement and widespread adoption of blockchain technology, as well-designed governance models can significantly contribute to the resilience and efficacy of these polycentric systems.

References

Agamben, G. (2005). State of exception. University of Chicago Press. https://press.uchicago.edu/ucp/books/book/chicago/S/bo3534874.html

Aligica, P. D., & Tarko, V. (2012). Polycentricity: from Polanyi to Ostrom, and beyond. Governance, 25(2), 237-262. https://doi.org/10.1111/j.1468-0491.2011.01550.x

Alston, E., Law, W., Murtazashvili, I., & Weiss, M. (2021). Can permissionless blockchains avoid governance and the law?. Notre Dame J. on Emerging Tech., 2, 1.

Alston, E., Law, W., Murtazashvili, I., & Weiss, M. (2022). Blockchain networks as constitutional and competitive polycentric orders. Journal of Institutional Economics, 18(5), 707-723.

Alston, E. (2019). Constitutions and blockchains: Competitive governance of fundamental rule sets. Case W. Res. JL Tech. & Internet, 11, 131.

Asmakov, D. A. (2022, December 20). What Are Proof of Reserves And Why Do They Matter? Retrieved January 26, 2023, from Decrypt website: https://decrypt.co/resources/what-are-proof-reserves-why-do-they-matter

Atik, J., & Gerro, G. (2018). Hard forks on the Bitcoin blockchain: reversible exit, continuing voice. SSRN.

Bambrough, B. (2022, December 13). Move Your Funds 'Immediately'—Serious $2.2 Billion Crypto Warning Issued After Sudden Bitcoin And Ethereum Rival Price Crash. Retrieved January 26, 2023, from Forbes website: https://www.forbes.com/sites/billybambrough/2022/12/13/move-your-funds-immediately-serious-22-billion-crypto-warning-issued-after-sudden-bitcoin-and-ethereum-rival-price-crash/

Barthere, A., Baraki, B., Grushyn, P., Ho, J., Choe, L., Li Khoo, Y., & Yi Lim, X. (2022). On-Chain Forensics: Demystifying TerraUSD De-peg| Nansen.

Berlin, I. (1969). "Two Concepts of Liberty," in Four Essays on Liberty. Oxford University Press.

Black, J. (2008). Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. Regulation & governance, 2(2), 137-164

Bodó, B., & Giannopoulou, A. (2019). The logics of technology decentralization-The case of distributed ledger technologies. SSRN.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of economic Perspectives, 29(2), 213-238.

Brandlitic (Learn With Whiteboard). (2022, April 13). What is Blockchain Layer 0, 1, 2, 3 Explained | Layers of Blockchain Architecture [Video]. YouTube. Retrieved December 4, 2022, from https://www.youtube.com/watch?v=qniz6h2fYuc&ab_channel=LearnwithWhiteboard

Brekke, J. K., Beecroft, K., & Pick, F. (2021). The dissensus protocol: Governing differences in online peer communities. Frontiers in Human Dynamics, 3, 641731.

Buterin, V. (2014, January 15.) Slasher: A Punitive Proof-of-Stake Algorithm. Ethereum Foundation Blog https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm.

Buterin, V. (2016, June 17). CRITICAL UPDATE Re: DAO vulnerability | Ethereum Foundation blog. Ethereum Foundation Blog. Retrieved February 19, 2024, from https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability

Buterin, V. (2017, February 6). The Meaning of Decentralization. Medium. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

Buterin, V. (2018). “Today I am going to make a tweet storm…” https://twitter.com/VitalikButerin/status/1029900695925706753

Buterin, V. (2020, January 3). Credible Neutrality as a Guiding Principle. Nakamoto. https://nakamoto.com/credible-neutrality/

Buterin, V. and Griffith, V. (2017). Casper the Friendly Finality Gidget. https://arxiv.org/pdf/1710.09437.pdf.

Carlisle, K., & Gruby, R. L. (2019). Polycentric systems of governance: A theoretical model for the commons. Policy Studies Journal, 47(4), 927-952.

Carreras, T. (2022, October 14). 51% of Ethereum Blocks Can Now Be Censored. It’s Time for Flashbots to Shut Down. Crypto Briefing. https://cryptobriefing.com/51-of-ethereum-blocks-can-now-be-censored-its-time-for-flashbots-to-shut-down/

Chainalysis. (2023, October 31). Understanding Tornado cash, its sanctions implications, and key compliance questions. Retrieved February 13, 2024, from https://www.chainalysis.com/blog/tornado-cash-sanctions-challenges/

Coghlan, J. (2024, February 2). FTX’s $400M hack linked to SIM-swap attack, feds charge 3. Cointelegraph. https://cointelegraph.com/news/crypto-exchange-ftx-400m-hack-sim-swap-attack

Craig, A. N., & Shackelford, S. J. (2013). Hacking the planet, the Dalai Lama, and you: managing technical vulnerabilities in the Internet through polycentric governance. Fordham Intell. Prop. Media & Ent. LJ, 24, 381.

Crypto.com. (2023, December 18). A guide to Ethereum’s ERC-4337 standard and account abstraction | Crypto.com. Retrieved February 19, 2024, from https://crypto.com/university/ethereum-erc-4337-standard-account-abstraction#:~:text=The%20ERC%2D4337%20token%20standard,private%20keys%20in%20each%20transaction.

Davidson, S., De Filippi, P., & Potts, J. (2016). Economics of blockchain. Available at SSRN 2744751.

Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. Journal of Institutional Economics, 14(4), 639–658. https://doi.org/10.1017/S1744137417000200

De, N. (2022, November 14). FTX’s Failure Is Sparking a Massive Regulatory Response. Retrieved January 26, 2023, from https://www.coindesk.com/policy/2022/11/14/ftxs-failure-is-sparking-a-massive-regulatory-response/

De Filippi, P., & Loveluck, B. (2016). The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure. Internet policy review, 5(4).

De Filippi, P., & McMullen, G. (2018). Governance of blockchain systems: Governance of and by Distributed Infrastructure (Doctoral dissertation, Blockchain Research Institute and COALA).

De Filippi, P., Cossar, S., Mannan, M., Nabben, K., Merk, T., Kamalova, J. (2024). Interim Report on Blockchain Governance Practices. Project Liberty, forthcoming. Retrieved February 16, 2024, from https://www.projectlibertyfoundation.io/news/decentralized-future-requires-robust-governance-models

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. (2022c). The alegality of blockchain technology. Policy and

Society, 41(3), 358-372.

De Filippi, P., Mannan, M., Henderson, J., Merk, T., Cossar, S., Nabben, K. A. (2022b). Report on blockchain technology & legitimacy, Research Project Report. Cadmus, EUI Research Repository. https://hdl.handle.net/1814/75167

De Filippi, P., Mannan, M., Reijers, W., Berman, P., & Henderson, J. (2022a). Blockchain Technology, Trust & Confidence. Reinterpreting Trust in a Trustless system?. Zenodo. https://doi.org/10.5281/zenodo.6516991

De Filippi, P., Wessel, R., Mannan, M. (forthcoming) Blockchain Governance, MIT Press.

De Filippi, P. & Hassan, S. (2016). Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. First Monday Vol 21, N. 12, special issue on 'Reclaiming the Internet with distributed architectures.

De Filippi, P. & Wright, A., (2018). Blockchain and the law: the rule of code. Harvard University Press.

Dimitropoulos, G. (2022). The use of blockchain by international organizations: effectiveness and legitimacy. Policy and Society.

DuPont, Q. (2017). Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization. In Bitcoin and beyond (pp. 157-177). Routledge.

Dutch Fiscal Information and Investigation Service. (2022, August 12). Arrest of suspected developer of Tornado Cash. FIOD. Retrieved February 14, 2024, from https://www.fiod.nl/arrest-of-suspected-developer-of-tornado-cash/#:~:text=On%20Wednesday%2010%20August%2C%20the,arrests%20are%20not%20ruled%20out.

Ethereum. (2023). The Merge. https://ethereum.org/en/roadmap/merge/

Farrell, H., & Schneier, B. (2022, October 13). Tornado Cash is Not Free Speech. It's a Golem. Lawfare. Retrieved February 26, 2024, from https://www.lawfaremedia.org/article/tornado-cash-not-free-speech-its-golem

Fortis, S. (2022). "Ethereum co-founder Vitalik Buterin celebrates the Merge: 'Dream for years'" Coindesk, Retrieved December 25, 2023, from https://cointelegraph.com/news/ethereum-co-founder-vitalik-buterin-celebrates-the-merge-dream-for-years.

Gkritsi, E. (2023, May 11). Tornado Cash Adds Chainalysis Tool for Blocking OFAC-Sanctioned Wallets From Dapp. CoinDesk. Retrieved February 13, 2024, from https://www.coindesk.com/tech/2022/04/15/tornado-cash-adds-chainalysis-tool-for-blocking-ofac-sanctioned-wallets-from-dapp/ (Original work published 2022)

Greene, A. R. (2016). Consent and political legitimacy. Oxford studies in political philosophy, 2, 71-97.

Higgins, S. (2021, September 11). Ethereum developers launch White Hat Counter-Attack on the DAO. CoinDesk. https://www.coindesk.com/markets/2016/06/21/ethereum-developers-launch-white-hat-counter-attack-on-the-dao/

Karakostas, D., Kiayias, A., & Ovezik, C. (2022). SoK: A Stratified Approach to Blockchain Decentralization. arXiv preprint arXiv:2211.01291

Kaufman, G. G., & Scott, K. E. (2003). What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It? The Independent Review, 7(3), 371–391. http://www.jstor.org/stable/24562449

Kaufman, George. (1996). Bank failures, systemic risk, and bank regulation. Cato Journal. 16.

Kelly, L. J. (2022, April 30). We need to talk about Terra's anchor. Decrypt. https://decrypt.co/98482/

we-need-to-talk-about-terras-anchor

Keoun, S. D. Y. and B. (2022, November 12). The Epic Collapse of Sam Bankman-Fried's FTX Exchange: A Crypto Markets Timeline. Coindesk, Retrieved November 18, 2022, from https://www.coindesk.com/markets/2022/11/12/the-epic-collapse-of-sam-bankman-frieds-ftx-exchange-a-crypto-markets-timeline/

Kereiakes, E., Do Kwon, M. D. M., & Platias, N. (2019). Terra money: Stability and adoption. White Paper, Apr.

Koo, J. L., Choe, L., Chia, D., Leow, S., & Polk, N. (2022, November 17). Blockchain Analysis: The Collapse of Alameda and FTX. Retrieved January 26, 2023, from https://www.nansen.ai/research/blockchain-analysis-the-collapse-of-alameda-and-ftx

Lessig, L. (2009). Code and Other Laws of Cyberspace. Basic Books. ISBN: 0-465-03912-X

Lutz, S. (2022). Prominent Chinese Ethereum Miner Wants to Resist Merge, Create Fork. Decrypt https://decrypt.co/106409/prominent-chinese-ethereum-miner-wants-to-resist-merge-create-fork.

Malwa, S. (2023, October 12). Tornado Cash Trading Volumes Nosedived 90% After U.S. Sanctions. CoinDesk. Retrieved February 26, 2024, from https://www.coindesk.com/policy/2023/10/11/tornado-cash-trading-volumes-nosedived-90-after-us-sanctions/

Mannan, M., De Filippi, P., Reijers, W. (forthcoming). Blockchain Constitutionalism.

McGinnis, M. D. (2016). Polycentric Governance in Theory and Practice: Dimensions of Aspiration and Practical Limitations [SSRN Scholarly Paper]. https://doi.org/10.2139/ssrn.3812455

Mehar, M., Shier, C., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H. M., & Laskowski, M. (2017). Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. Journal of Cases on Information Technology, 21(1), 19-32. https://doi.org/10.2139/ssrn.3014782

Mindel, V., Mathiassen, L., & Rai, A. (2018). The sustainability of polycentric information commons. MIS Quarterly, 42(2), 607-632.

Munster, B. (2022, September 23). 'Was the Ethereum Merge a Mistake?' Decrypt. https://decrypt.co/110426/was-ethereum-merge-mistake/

Musiani, F., Mallard, A., & Méadel, C. (2017). Governing what wasn't meant to be governed: A controversy-based approach to the study of Bitcoin governance. In Bitcoin and beyond (pp. 133-156). Routledge.

Nabben, K., & Zargham, M. (2022). Permissionlessness. Internet Policy Review, 11(2), 1-10.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized business review.

Neumueller, A. (2022). 'A deep dive into Bitcoin's environmental impact' University of Cambridge Judge Business School. https://www.jbs.cam.ac.uk/2022/a-deep-dive-into-bitcoins-environmental-impact/

Neumueller, A. (2023). 'Ethereum's climate impact: a contemporary and historical perspective.' University of Cambridge Judge Business School. https://www.jbs.cam.ac.uk/2023/ethereums-climate-impact-a-contemporary-and-historical-perspective/

Opsahl, K. (2022, August 22). Code, speech, and the Tornado cash mixer. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2022/08/code-speech-and-tornado-cash-mixer

Ostercamp, P. (2021). From 'Code is Law'to 'Code and Law': Polycentric Co-Regulation in Decentralised Finance (DeFi). Available at SSRN 4134259.

Ostrom, E. (1990). Governing the commons: The evolution of institutions for collective action. Cambridge university press.

Ostrom, E. (1998). The comparative study of public economies. The American Economist, 42(1), 3-17.

Ostrom, E. (2009). Understanding institutional diversity. Princeton university press.

Ostrom, V., Tiebout, C. M., & Warren, R. (1961). The organization of government in metropolitan areas: a theoretical inquiry. American political science review, 55(4), 831-842

Platias, N., Lee, E. J., & Maggio, M. (2020). Anchor: Gold Standard for Passive Income on the Blockchain.

Polanyi, M. (1951). The Logic of Liberty. Chicago, IL: University of Chicago Press.

Reijers, W., O'Brolcháin, F., & Haynes, P. (2016). Governance in blockchain technologies & social contract theories. Ledger, 1, 134-151.

Reinsberg, B. (2021). Fully-automated liberalism? Blockchain technology and international cooperation in an anarchic world. International Theory, 13(2), 287-313.

Rennie, E. (2023, January 31). "Climate change and the legitimacy of Bitcoin" https://dx.doi.org/10.2139/ssrn.3961105.

Reynolds, S. (2023a, May 12). Tornado Cash Co-Founder Says the Mixer Protocol Is Unstoppable. CoinDesk. Retrieved February 26, 2024, from https://www.coindesk.com/tech/2022/01/25/tornado-cash-co-founder-says-the-mixer-protocol-is-unstoppable/

Reynolds, S. (2023b, May 25). Lawyers Challenging U.S. Tornado Cash Sanctions Say Free Speech Is at Stake. CoinDesk. Retrieved February 26, 2024, from https://www.coindesk.com/policy/2023/05/25/lawyers-challenging-us-tornado-cash-sanctions-say-free-speech-is-at-stake/

Rosati, P., Lynn, T., & Fox, G. (2021). Blockchain: A Technology in Search of Legitimacy. In Blockchain Technology and Innovations in Business Processes (pp. 17-32). Springer, Singapore.

Rozas, D., Tenorio-Fornés, A., Díaz-Molina, S., & Hassan, S. (2021). When ostrom meets blockchain: exploring the potentials of blockchain for commons governance. Sage Open, 11(1), 21582440211002526.

Sai, A. R., Buckley, J., Fitzgerald, B., & Le Gear, A. (2021). Taxonomy of centralization in public blockchain systems: A systematic literature review. Information Processing & Management, 58(4), 102584.

Schmitt, C. (2014). Political theology II: The myth of the closure of any political theology. John Wiley & Sons. [Originally published in 1922].

Shackelford, S. J., Raymond, A., Charoen, D., Balakrishnan, R., Dixit, P., Gjonaj, J., & Kavi, R. (2017). When toasters attack: A polycentric approach to enhancing the security of things. U. Ill. L. Rev., 415.

Srinivasan, B. S., & Lee, L. (2017). Quantifying decentralization. news. earn. com. https://news.earn.com/quantifying-decentralization-e39db233c28e

Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.

Swartz, L. (2018). What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology, Cultural Studies, 32:4, 623-650, DOI: 10.1080/09502386.2017.1416420

Teubner, G. (2012). Constitutional Fragments: Societal Constitutionalism and Globalization. Oxford University Press.

The Attacker. (2016, June 17). Letter from DAO attacker. Pastebin. Retrieved February 19, 2024, from

https://pastebin.com/CcGUBgDG

thehighfiveghost. (2016, June 17). Critical Update RE: DAO vulnerability [Online forum post]. Reddit. Retrieved February 12, 2024, from https://www.reddit.com/r/ethereum/comments/4oiqj7/critical_update_re_dao_vulnerability/

Thussu, D. (2021). Transcultural Communication for a Polycentric World. Journal of Transcultural Communication, 1(1), 20-36.

Tornado Cash. (2020a, May 21). Tornado.cash is finally trustless! Medium. Retrieved February 13, 2024, from https://tornado-cash.medium.com/tornado-cash-is-finally-trustless-a6e119c1d1c2

Tornado Cash. (2020b, December 18). Tornado.Cash Governance proposal. Medium. Retrieved February 13, 2024, from https://tornado-cash.medium.com/tornado-cash-governance-proposal-a55c5c7d0703

Ubell, K., Chang, M., & Fovent, A. B. (2023, May 31). “Regulation by enforcement” in the digital asset industry: a lagging response to stale facts. Goodwin. Retrieved February 16, 2024, from https://www.goodwinlaw.com/en/insights/publications/2023/05/insights-otherindustries-dcb-regulation-by-enforcement

United States Department of the Treasury. (2022a, August 8). U.S. Treasury sanctions notorious virtual currency mixer tornado cash. U.S. Department of The Treasury. Retrieved February 13, 2024, from https://home.treasury.gov/news/press-releases/jy0916

United States Department of the Treasury. (2022b, November 8). Treasury designates DPRK weapons representatives. U.S. Department of The Treasury. Retrieved February 13, 2024, from https://home.treasury.gov/news/press-releases/jy1087

United States Securities and Exchange Commission. (2017, July 25). SEC issues investigative report concluding DAO tokens, a digital asset, were securities. SEC.gov. Retrieved February 19, 2024, from https://www.sec.gov/news/press-release/2017-131

United States Securities and Exchange Commission. (2023a, April 14). SEC Reopens Comment Period for Proposed Amendments to Exchange Act Rule 3b-16 and Provides Supplemental Information. SEC.gov. Retrieved February 16, 2024, from https://www.sec.gov/news/press-release/2023-77

United States Securities and Exchange Commission. (2023b, November 14). SEC Announces Enforcement Results for Fiscal Year 2023. SEC.gov. Retrieved February 16, 2024, from https://www.sec.gov/news/press-release/2023-234

United States Securities and Exchange Commission. (2024, February 6). SEC adopts rules to include certain significant market participants as “Dealers” or “Government securities dealers.” SEC.gov. Retrieved February 16, 2024, from https://www.sec.gov/news/press-release/2024-14

Vliet, R. V. (2019). Legitimizing the Blockchain Industry. An assessment of the blockchain industry’s current state of affairs.

Wade, A., Lewellen, M., & Van Valkenburgh, P. (2022, August 25). How does Tornado Cash work? Coin Center. Retrieved February 13, 2024, from https://www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work/

Weber, M. (1964). The Theory of Social and Economic Organization, New York: Free Press.

Zamfir, V. (2016a). The History of Casper - Part 1. Medium. https://medium.com/@Vlad_Zamfir/the-history-of-casper-part-1-59233819c9a9.

Zamfir, V. (2016b). The History of Casper - Part 2. Ethereum Foundation Blog. https://blog.ethereum.

org/2016/12/07/history-casper-chapter-2

Zargham, M. Alston, E., Nabben, K. & Ben-Meir, I. (2023, April 20). What constitutes a constitution? - BlockScience - Medium. Medium. https://medium.com/block-science/what-constitutes-a-constitution-2034d3550df4

Research Project Report
May 2024

ISBN:978-92-9466-551-5
doi:10.2870/049527
QM-09-24-368-EN-N