LIUC
Università Cattaneo

Università Cattaneo Working Papers

The governance of blockchains and systems based on distributed ledger technology

Carlo Gola
Valentina Cappa
Patrizio Fiorenza
Paolo Granata
Federica Laurino
Lorenzo Lesina
Francesco Lorizzo
Gabriele Marcelli

Numero 17 - 2024

Collana: Università Cattaneo Working Papers
ISSN: 2532-554X
Università Carlo Cattaneo - LIUC
Corso Matteotti 22, 21053 Castellanza (VA), Tel. 0331-572.282, email: biblio@liuc.it

The governance of blockchains and systems based on distributed ledger technology

Carlo Gola, Valentina Cappa*, Patrizio Fiorenza*, Paolo Granata*, Federica Laurino*, Lorenzo Lesina*, Francesco Lorizzo*, Gabriele Marcelli*

Abstract
This paper deals with the governance of systems based on distributed ledger technology (DLT). This technology enables the creation of a shared electronic archive accessible via the internet, in which information is stored in a secure and irreversible manner. The updating and management of the ledger takes place without resorting to a trusted third party. The absence of traditional organizational and governance structures makes DLT management complex. The work provides a conceptual framework to understand DLT technology and analyzes its governance, both for open (permissionless) systems and for those with limited access (permissioned). Different approaches are suggested for the application of governance rules, including for DLT with entirely algorithmic governance. The study describes the difference between management and governance tokens, having respectively administrative and property rights, which facilitate the direction and control of DLTs. Finally, the governance structure of two DLTs is described: Ethereum and Polkadot.

Keywords: Governance, open-source systems, Blockchains technology, distributed ledger technology, Crypto assets.

JEL Codes: G3, M4, D82, G14, G21, G28, M4, M15, O33

1. Introduction[1]

Blockchain technology allows the creation of a shared electronic archive accessible via the internet, in which information is securely and irreversibly stored and freely entered by network participants. The registry's updates, such as those related to economic transactions, occur in a decentralized manner without the need for a third-party intermediary as in traditional systems. This paper analyzes the governance of blockchains and, more broadly, of distributed ledger technology (DLT), covering both permissionless and permissioned types (see Box 1).

International bodies (IMF (2023), FSB (2022)) recommend appropriate governance structures and internal controls for the crypto ecosystem to ensure effective and prudent risk management. Achieving this goal is more feasible for permissioned DLTs, where

* Servizio Supervisione Intermediari Finanziari, Dipartimento Vigilanza Bancaria e Finanziaria, Banca d'Italia.
[1] The views expressed in this paper are those of the authors and do not necessarily reflect those of the Bank of Italy. The authors thank: Paolo Angelini, Fabio Bernasconi, Luigi Cannari, Roberto Parmeggiani, Andrea Pilati, Giuseppe Siani, Zorana Milicevic, for their helpful comments. Special thanks to Marco Bevilacqua, Oscar Borgogno, Federico D'Antoni, Marina La Fratta, and Carlo Lanfranchi for their valuable suggestions. This paper is a slightly revised version of the article in Italian: Gola, C., Cappa, V., Fiorenza, P., Granata, P., Laurino, F., Lesina, L., Lorizzo, L., Marcelli, G. (2023), *La governance delle blockchain e di sistemi basati sulla tecnologia dei registri distribuiti*, Questioni di Economia e Finanza (Occasional Papers), n. 773, giugno, Banca d'Italia.
No endorsement is made for the mentioned blockchains, which are only cited for illustrative purposes.

participants operate only if authorized and with well-defined roles, compared to permissionless DLTs, where adherence to governance rules can be problematic.[2] The paper discusses this issue and offers some policy proposals.

Box 1 – DLT: Technology, Accessibility, Governance
DLTs are specific computer architectures characterized as distributed systems composed of a network of computational nodes that cooperate to reach a common state in the form of a shared registry. Updates to the registry's state occur through so-called "consensus algorithms", which define the rules nodes must follow to make these updates. Blockchains are a specific subset of DLTs with two additional properties: (a) their registry is structured as blocks of transactions (the elementary units of state update), and (b) the blocks are linked using specific cryptographic functions that allow the registry to be updated only by adding data to the end without modifying previous blocks. DLTs are typically classified based on reading and writing profiles. Based on reading profiles and thus the ability to access and consult the information contained in the registry, DLTs are classified as public and private (the latter allowing only certain authorized nodes access). Based on writing profiles, DLTs are commonly distinguished between permissionless and permissioned according to the mode of participation in the consensus mechanism (in permissioned, only some of the nodes are authorized to participate in the consensus mechanism that allows updating the registry's state). The "ordinary" governance of the registry occurs as described above through automatisms coded in the consensus protocol that defines the rules for its update. However, when structural changes to these rules (upgrading significant software aspects) are necessary, the problem arises of how such "extraordinary" changes can be governed.

In recent years, banking and financial regulators have devoted considerable attention to crypto-assets, partly because DLTs enable the negotiation and transfer of ownership of traditional financial instruments or products. In 2022, the European Commission issued a legislative package on digital finance (the so-called Digital Finance Package) aimed at providing a regulatory framework for these technologies. Recently, the Basel Committee, tasked with defining prudential treatment criteria for banks holding crypto-assets, decided to evaluate whether permissionless DLTs can be considered as reliable as permissioned ones from a governance perspective.[3] This issue is also significant

[2] In particular, the FSB (2022) observed that: "Authorities should have the appropriate powers and tools, and adequate resources, to regulate, supervise, and oversee crypto-asset activities and markets, including crypto-asset issuers and service providers, as appropriate," Recommendation 1.
[3] BCBS (2022), p. 4.

because the basis of most decentralized finance (DeFi) initiatives is the permissionless Ethereum DLT.

This topic was addressed in the recent Communication from the Bank of Italy regarding decentralized technologies in finance and crypto-assets, observing that the technology "binds" the objective components (technical and organizational infrastructures and instruments) and subjective ones (various types of operators involved) of ecosystems into new products and services, a "synthetic" expression of each contribution. The relevance of the technological component and technology providers themselves establishes a sort of "algorithmic governance" that disrupts traditional governance schemes and must be taken into account.[4]

Analyzing the governance structure of permissioned DLTs is more straightforward as they apply explicit coordination processes among managers, akin to traditional corporate structures. In contrast, analyzing the governance structure of permissionless DLTs is more complex, where some processes can be regulated at various levels by algorithmic governance, also known as "on-chain". On-chain governance differs from "off-chain" governance in that it automates governance functions.

The balance between on-chain and off-chain governed processes is a peculiarity of the specific blockchain; this work examines two platforms with quite different models to exemplify the differences: Ethereum and Polkadot. Ethereum combines the native computer protocol (the main one from the project's start) with decision-making processes in the hands of identifiable physical or legal persons. These are responsible for "extraordinary" decisions related to the functioning of the DLT. Polkadot, on the other hand, aims to introduce all organizational and decision-making processes into the protocol itself. This mode can be classified as "entirely on-chain" or full algorithmic governance. It also includes bodies, technical committees, voting mechanisms, but enforcement is automated. Full algorithmic governance involves the inclusion of meta-rules capable of revising even the "constitutional" rules of the protocol itself, according to predefined modalities. Algorithmic governance (both partial and complete) is associated with the issuance of management and governance tokens that grant administrative and sometimes property voting rights to participants in the DLT management.

There are advantages and disadvantages to both approaches: to mention the main ones, off-chain processes are subject to opacity, moral hazard, and conflict of interest among

[4] See Banca d'Italia (2022), p. 7.

participants; the second (on-chain) are transparent and verifiable but necessarily more rigid and "incomplete" in the sense that they cannot – by definition – include decision-making processes not identifiable in advance. Moreover, decisions made by algorithmic governance systems could lead to undesirable and potentially uncontrollable automated effects. The on-chain approach must also demonstrate its ability to solve certain problems, such as post hoc correction of incorrectly entered transactions or responding to the need for a clear legal foundation, including the competent forum for resolving disputes.

Before proceeding, some clarifications are necessary: the scope of our analysis exclusively concerns governance processes related to the functioning of DLTs, thus excluding those related to services offered by third parties in support of crypto-assets, such as crypto-asset exchange platforms or the custody of such assets. Similarly, the work does not address the very relevant legal foundations of these decentralized technological infrastructures. An attempt in this direction has been made for decentralized autonomous organizations (DAOs) by Brummer and Seria (2022), seeking to identify a "legal wrapper" among existing legal forms in the United States, whether they are capital companies, even with limited liability, non-profit cooperatives, trust foundations, partnerships, joint ventures, or even non-legal entities like social clubs. None of the mentioned categories seem to satisfactorily accommodate these organizational forms, and it may be necessary to introduce a new category[5]. In this regard, as should become clear in the course of our discussion, particular attention must be paid to the role of randomization and governance tokens. The first aspect involves the random assignment of administrative control and delegation rights, a device used to avoid the concentration of powers and ensure (or try to ensure) implicit coordination among "atomistic" subjects; the second aspect concerns the need to align incentives towards a shared purpose through the use of digital representations of rights with market value that are transferable and negotiable. Many issues remain open, such as the nature of these rights and the ways in which they can be represented and protected. Finally, we emphasize that the work does not provide an analysis of the risks related to the management and control of this technology but only a preliminary conceptual framework for such further developments.

[5] On these aspects, see: Garrido et al. (2022); O. Borgogno (2022); UK Jurisdiction Taskforce (2019); The Law Society (2020), especially Chapter 8, "Blockchain Consortia." For an overview in the general categories of civil law and Italian financial law, with particular reference to crypto-assets, see C. Lanfranchi (2019).

The work is structured as follows: after describing the essential elements of traditional corporate governance (paragraph 2), it compares these aspects with the implicit or explicit government characteristics of both permissionless and permissioned DLTs (paragraph 3). Subsequently, the issue of regulatory intervention is discussed (when to intervene, how to calibrate the intervention, how to enforce it in the face of different DLT systems) (paragraph 4). Paragraph 5 provides some concluding remarks. The Appendix describes the governance systems of two permissionless DLTs that use, on-chain and off-chain governance processes; respectively, Ethereum and Polkadot.

2. Overview of Corporate Governance Principles

Corporate governance refers to a system of rules concerning the rights, organizational processes, and control mechanisms of management and leadership bodies to safeguard the interests of stakeholders and achieve the strategic objectives of a company. It should align incentives, establish responsibilities, monitor processes, and instill a set of values through a corporate culture. Historically, different governance models have emerged: more prescriptive in Continental Europe and based on general principles and self-governance in common law countries.[6] Often, the field has evolved following significant corporate crises. The approach based on general principles has the advantage of being adaptable to circumstances, including technological developments. In the United Kingdom, the entire subject was systematized in the Cadbury Report of 1992, later incorporated into the periodically updated Combined Code on Corporate Governance by the Financial Reporting Council. In the EU, the Commission played a significant role in creating a framework applicable in countries with different traditions and regulatory structures. In the banking and financial sector, these principles have been articulated with particular emphasis on sound and prudent management, the role of control bodies, and risk monitoring and mitigation.[7]

The OECD has developed principles that have become a benchmark on the subject. The aim has been to "promote long-term investment, financial stability, integrity, and ultimately the growth and inclusiveness of an economy". This is achieved "through an economic environment based on trust, transparency, and accountability".[8] The OECD

[6] See N. G. Maw et al. (1994); J.H. Farrar and B.M. Hannigan (1998), European Commission, "Green Paper. The EU framework on corporate governance," Brussels, April 5, 2012. See also: European Commission, Action Plan: European company law and corporate governance - a modern legal framework for more engaged shareholders and sustainable companies. COM(2012) 740 final. Strasbourg, December 12, 2012.

[7] In particular, see EBA (2021); BCBS (2015). For Italy, see Circular Banca d'Italia (285/2013 and subsequent updates (Supervisory provisions for banks), Part One, Title IV, Corporate governance, internal controls, and risk management, p. 274-472.

[8] See OECD (2015), p. 9

emphasizes that a corporate governance framework "typically includes elements related to legislation, regulation, self-regulatory arrangements, voluntary commitments, and business practices arising from specific circumstances, historical factors, or the traditions of various countries"; what matters - the OECD stresses - is the end result ("functional equivalence principle").[9] Governance aspects are also present in the recent European regulation allowing experimental issuance and trading of securities via DLT.[10]

2.1. On the Foundations of an Organizational and Governance Structure

Formally, a governance structure is an organizational system capable of making decisions based on a collective choice rule (a statute, a shared code, a protocol) and decisions formulated on the information accessible at a given moment by economic agents. As highlighted by Kennet Arrow (1974), since information transmission is resource-intensive, it is in principle more efficient to transmit all information to a single center rather than distribute it among all agents. Arrow also notes that the most radical alternative to central authority is "consensus".[11] He observes that spontaneous consensus would be efficient in an organization whose members have identical interests and information. However, if information is not easily and perfectly distributed, incentives might diverge. For example, some agents might be inclined to follow improper behaviors to the detriment of others if such behaviors (or their outcomes) are not fully observable; a problem known as the principal-agent problem.[12] Furthermore, if transaction costs are excessive, contracts are incomplete, or rationality is limited, allocative choices might be inefficient (O.D. Hart (1995); O. Williamson (1999)). Over the years, regulatory interventions have been introduced to limit such problems.

As complexity or functions increase, coordination and information costs rise in company or among agents. The organization allows for the exploitation of economies of scale or scope; it responds to the need to make the process efficient, reducing the level of decentralization. Internalizing production processes also reduces the risks of malicious behaviors by external parties, as internal controls within an organizational structure are easier, and the presence of shared interests is more likely. However, beyond a certain threshold, efficiency gains tend to decrease if distorting mechanisms prevail within the

[9] See OECD (2017), p. 11.

[10] Recently, the European Commission has issued a pilot regulation for distributed ledger technology-based market infrastructures, European Regulation 2022/858 (DLT Pilot regime). DLT operators (banks, financial intermediaries, market operators, other operators) must comply with traditional organizational, governance, investor protection, KYC/AML requirements. Similarly, the regulation on crypto-asset markets (MiCA Regulation) establishes rules whose enforcement would pass through a supervised entity (e.g., the crypto-asset service provider (CASP)).

[11] See K. Arrow (1974), pp. 49-50.

[12] For a review of the literature on the subject, see K. Arrow (1986). Also see: Jensen, M. C.; Murphy, K. J. (1990).

organizational system; efficiency gains can be obtained by externalizing certain functions or creating group configurations (P. Milgrom, J. Roberts (1992)). Thus, various trade-offs justify a more or less complex (more or less decentralized) organizational and corporate structure to minimize the productive and transactional costs arising from imperfect information, incomplete contracts, and opportunistic behaviors.

Operationally, it involves designing an organizational structure that binds the decision-making process based on certain criteria to identify and preserve the best solution for the collective set of agents (stakeholders) "in accordance with the public interest on a sustainable basis"[13]. If forms of coordination (e.g., hierarchical structures) among economic agents (or groups of economic agents) are possible, the governance system includes bodies with distinct functions (distribution of powers, responsibilities, control mechanisms)[14]. Note that ownership (capital share or voting rights) does not necessarily entail direct control of the initiative (managerial power); this usually occurs through a mechanism of delegation to directors (executive and independent) and requires a sufficiently high share (e.g., 50% +1) of votes or the ability to create voting coalitions to reach the required quorum for approving certain decisions. Therefore, within the enterprise, the organizational structure is based on more or less stringent mechanisms of mutual trust, delegation, and circularity of information. A balanced governance structure based on control and checks and balances between various bodies becomes essential. It must monitor both internal processes and those outsourced (in outsourcing or distributed in the network) if relevant.

2.2. A Definition of Corporate Governance for Distributed Registers

The traditional categories of corporate governance and organizational processes only partially fit the issue at hand. The governance of distributed registries has entirely novel characteristics, similar to those that are observable in collective governance systems like the "spontaneous" creation and management of open-source software (Markus L. M. (2007)[15]. Some authors have thus defined blockchain governance as follows: "a means

[13] See BCBS (2015), p. 3.

[14] The main bodies are: a governing body, responsible for evaluating and proposing strategic choices to be adopted; a decision-making body that expresses itself through a voting system; a management body, responsible for implementing decisions adopted in the best possible way; one or more independent monitoring and control bodies tasked with supervising compliance with governance rules established by the statute or dictated by an external authority to avoid conflicts of interest or improper behaviour.

[15] Software for which the original source code is freely available is defined as *open-source*.

to achieve direction, control, and coordination of stakeholders within the context of a given blockchain project in which they jointly contribute" [16] (van Pelt et al. 2020 p. 21).

While in the current version of most DLTs there are automated processes associated with traditional forms of coordination, some projects aim to develop DLTs where governance processes are fully automated (such as Polkadot). It should be noted, however, that regardless of the degree of decentralization, the governance of both types of DLT requires the presence of bodies (steering committees, technical and decision-making bodies) and tools (tokens with variously configured voting rights), not only to achieve orderly decision-making forms and respect the implicit rights of participants but also to ensure system efficiency ("scalable", to support significant volumes of transactions in limited times in a secure and flexible manner).

2.3. Ownership and Control

It's worth mentioning that in traditional corporate governance guidelines in the banking and financial sector (e.g., BCBS (2015); EBA (2021); ECB (2021a, 2021b)), the theme of the relationship between ownership and control (voting rights, relationship between shareholders and management, etc.) is usually not considered. The focus is on management mechanisms, the role and independence of bodies, risk monitoring and mitigation processes, etc. However, the former aspects are also relevant in an analysis of the governance criteria of a DLT, as they are closely connected with the mechanisms for achieving distributed consensus. Attention must also be paid to the token creation process, whether they incorporate particular rights in the management of the DLT, and whether voting coalitions or forms of concentration[17] in the exercise of such rights are possible (refer to Box 2 and paragraph 3.3). These aspects could configure the legal form of a de facto company, exposing participants to various risks, primarily to possible liability towards corporate obligations. Such liability would be unlimited, so participants would be responsible not only within the limits of the "share" contributed but also with their personal assets. There remains great uncertainty on these aspects, and they would require specific analysis starting from the legal foundations and solutions proposed by company law (O. Borgogno (2022)).[18] A comprehensive review is beyond the scope of

[16] The definition bears some similarities to that of Decentralized Autonomous Organizations (DAOs), where managerial and operational functions are encoded on-chain in DLTs in the form of smart contracts. See Hassan, S., De Filippi, P. (2021); Santana, C., Albareda, L. (2022).

[17] On these aspects, see: Schär, F., Nadler, M. (2022); Sultanik, E. et al., (2022).

[18] See N. G. Maw et al. (1994); J.H. Farrar and B.M. Hannigan (1998), European Commission, "Green Paper. The EU framework on corporate governance," Brussels, April 5, 2012. See also: European Commission, Action Plan: European company law and corporate governance - a modern legal framework for more engaged shareholders and sustainable companies. COM (2012) 740 final. Strasbourg, December 12, 2012.

this paper; some aspects will nevertheless be analysed here from a technological perspective: the role of nodes, the role of developers involved through various incentive mechanisms, the role of various advisory or technical committees present in some DLTs.[19] The intent is to provide elements useful for future reflection on the legal and regulatory profiles of these structures.

Box 2 – On Various Types of Tokens

In this work, we use the term token to indicate any digital representation of value (even created by the DLT itself) transferable via this technology. Most tokens are tradable through an exchange platform. There are three aspects to consider: the economic nature of the token and its predominant function (means of exchange, store of value, bet on its future value); financial characteristic (liquidity, volatility, negotiability); and legal nature (capacity to represent rights, promises, contractual obligations). If we use this last category as the driver, it is possible to classify tokens into two macro-classes depending on whether or not they incorporate rights for the holder.[20]

The first macro-class includes tokens without rights (real or financial) incorporated, except for the possession of the token itself; they are not representations of value with an asset and a liability that cancel each other out upon consolidation; they do not confer any rights on the user; they do not have generalized spending power by law, like a currency has. This class of tokens includes the so-called unbacked crypto assets (without a reserve of assets to support).

The second macro-class includes tokens that incorporate rights. They are: i) "tokenized" electronic money (where "tokenized" means traditional e-money transferable via DLT); ii) "tokenized" of central bank money; iii) "tokenized" financial instruments and products; iv) non-fungible tokens (NFTs): unique tokens representing ownership rights over goods such as artworks or themselves digital artworks; v) utility tokens: tokens aimed exclusively at guaranteeing the right to access a good or service provided by the DLT; some utility tokens are not transferable and therefore not tradable; vi) administrative and; v) governance tokens created by the protocol through smart contracts and assigned to those (e.g., developers) who provide a service aimed at “governing” the protocol; only governance tokens confer on the holder a specific right to the current or future potential pecuniary stream of income generated by the protocol. Administrative and Governance tokens can be assigned through various methods, including random allocation, and can confer different types of voting rights.

[19] Recently, the European Commission has issued a pilot regulation for distributed ledger technology-based market infrastructures (DLT Pilot Regime). DLT operators (banks, financial intermediaries, market operators, other operators) must comply with traditional organizational, governance, investor protection, KYC/AML requirements. Similarly, the regulation on crypto-asset markets (MiCA Regulation) establishes rules whose enforcement would pass through a supervised entity (e.g., the crypto-asset service provider (CASP)).

[20] On these aspects, see: C. Gola, et al., (2024). On the role of governance tokens, see IOSCO (2022).

3. Collective and Algorithmic Governance

This section aims to bridge traditional governance structures with decentralized organizational structures. Good governance, even if implicit in a spontaneously organized system, should clearly identify the role and operational modalities of all network participants, ensuring transparency, regulating incentive mechanisms to contain opportunistic or malicious behaviors, avoiding concentration of power that could hinder proper internal dialectics, and especially resolving conflicts among participants in an orderly manner. It should be capable of incorporating the laws of the jurisdictions where the DLT operates. A key point - to be highlighted later - is the distinction between collective governance functions of the DLT, operated among organized network subjects, and the so-called 'algorithmic governance' that automates certain functions. The former mainly concerns the allocation of powers and responsibilities; the latter deals with the enforcement of governance mechanisms through a computerized procedure. Proponents of complete algorithmic governance aim to achieve a fully automated governance system; however, even in the most advanced forms (as in the case of Polkadot presented here), it seems difficult to fully achieve this result, as is the case for any necessarily "incomplete" contractual form with respect to events originally not foreseen by the parties.

3.1. Blockchain as a System for Building Mutual Trust

In permissionless DLTs, especially those based on "Proof-of-Work", consensus emerges not so much from mechanisms of delegation and verification of compliance with traditional rules, but from automatisms and endogenous economic mechanisms that lead to a consensus among actors who do not directly communicate with each other and without prior need for mutual trust among stakeholders.

This process can be modeled as a dynamic equilibrium (Nash equilibrium), mathematically representable as a stochastic process that "dominates" other possible behaviors among agents who do not communicate with each other[21]. The equilibrium arises from the "consensus protocol," which allows various stakeholders, viewed as rational agents maximizing their utility, to achieve a common goal.

In computing, the issue of achieving consensus among different actors traditionally concerned establishing how to reach a synchronization state (a "consensus") among a

[21] See Paul Apivat: https://paulapivat.medium.com/economics-games-and-proof-of-work-842d820f198c

discrete number of autonomous systems (nodes) with a certain degree of tolerance[22]. The challenge was to determine under what conditions the system could operate correctly, even in the presence of a certain number of nodes behaving anomalously (non-functioning or resulting from malicious behaviors). It has been shown that there are critical tolerance thresholds (e.g., 2/3 of the nodes operating correctly at any given time), above which the system continues to function correctly overall[23].

A novelty introduced by Bitcoin's blockchain with the Proof-of-Work[24] consensus mechanism was to demonstrate that it is possible – albeit probabilistically – to achieve a substantially similar result (i.e., consensus on a shared register) even in an open peer-to-peer system without requiring explicit communication among previously identified participants[25]. In DLTs that adopt Proof-of-Work consensus mechanisms, the consensus process is configured as a competition to solve a computationally costly cryptographic problem; corresponding to high energy and, consequently, economic expenditure, thereby disincentivizing improper behaviors as they would be unsustainable.

Interpreting the operation of this consensus model in terms of a process for solving the previously described governance problems, it can be said that it "collapses" functions attested at multiple operational levels (managerial and control) into a single process, that of reaching consensus on the state of the shared register.

The goal of uncoordinated cooperation among nodes not previously identified is achieved through an economic incentive awarded to nodes actively participating in the process (the so-called miners), resulting in the creation of new tokens awarded to nodes that win the competition to solve the aforementioned cryptographic problem. In Bitcoin, moreover, the total number of tokens that can be generated through this process is limited ex-ante by the protocol itself: tokens are thus perceived as objects with market value also due to their limited supply. The incentive system is therefore entirely based on the assumption that the token has value linked to its scarcity and that it will continue to have it in the future. Their fate is potentially precarious and is exclusively connected

[22] The issue is known in literature as the "Byzantine Generals Problem," and systems that, under specific conditions, exhibit tolerance to anomalous behaviour by a subset of nodes are defined as "Byzantine Fault Tolerant" (BFT).
[23] See Lamport, L., et al. (1982).
[24] This mechanism is also known as the "Nakamoto protocol," from the pseudonym with which the white paper describing Bitcoin was published: https://bitcoin.org/bitcoin.pdf.
[25] A *peer-to-peer* system is defined as a distributed computer system in which all nodes perform the same functions on a peer-to-peer basis. This system contrasts with *client-server* architectures, where some nodes assume a service provider role (the servers) and others the user role (the clients). The latter model is the most common in the implementation of distributed computer applications, while the former is historically known for its use in platforms for sharing and exchanging data.

to the fact that the reference token continues to be considered a worthy good of economic value by a sufficient number of individuals.

This system, based on imposing a computational cost, disincentivizes improper behaviors, making it extremely costly for any malicious participants to artificially multiply their role in the process of updating the shared register. Indeed, in the absence of a central entity verifying the participant's identity in the network, it would be possible to generate a large number of only apparently different digital identities at low cost, thereby acquiring disproportionate control over the network. This is how a coalition of nodes attributable to the same subject or group of subjects could control the entire system (*sybil attack*). The inclusion of a cost for participating in the consensus mechanism drastically reduces this possibility. On the contrary, Proof-of-Work consensus protocols are designed in such a way as to "align incentives" among nodes, meaning it is more advantageous to behave correctly rather than try to compromise the integrity of the network.

Box 3 – Incentive Mechanisms
The two main incentive mechanisms for participants in permissionless DLTs (such as Bitcoin's blockchain) are tokens generated by the protocol itself and fees paid by end-users in tokens to execute transactions. Users can increase this fee to expedite the validation process of their transaction, creating competition among users based on the price they are willing to pay to see it finalized in short times. When the maximum limit of tokens specified by the protocol is reached (in the case of Bitcoin, 21 million), the system would be incentivized only by fees. Regarding permissioned DLTs, characterized by an identifiable and limited set of nodes actively participating in the consensus mechanism, incentive schemes could in principle be freely designed, even using traditional remuneration systems based on the "effort" expended. Generally, incentive systems depend on the type of consensus protocol used and the associated voting and control mechanisms of the blockchain. For example, the creation of tokens with voting rights (governance tokens) has introduced a new type of incentive – described further in relation to the case studies presented.

The intertemporal equilibrium among nodes is thus achieved for any market value of the token, as Proof-of-Work protocols adaptively modify the difficulty of the cryptographic problem based on its solution time and therefore the relative computational cost to solve it. An increase in the price of tokens leads to the entry of new miners into the market, a more rapid creation of tokens, and therefore (by construction of the algorithm) an

increase in complexity[26]. All this, as mentioned, makes it very difficult to execute attacks aimed at attempting to modify already completed transactions or prevent the confirmation of new transactions[27].

3.2. Consensus Protocols and Voting Rights

As seen earlier, the creation of a token through the Proof-of-Work-based protocol is a fundamental element not only to remunerate the miners' activities but also to "align incentives" and create mutual trust. However, not all DLTs operate with Proof-of-Work-type consensus mechanisms; other types of algorithms are adopted for reasons of efficiency and reducing environmental impact[28]. Below we describe three alternative consensus protocol classes, aspects that also have implications for the governance of DLT: Proof-of-Stake (PoS), Pure Proof-of-Stake (PPoS), and Proof-of-Authority[29].

Proof-of-Stake (PoS) – Consensus algorithms within this category are adopted on the notion that, to update the ledger, nodes must demonstrate possession of a certain "stake". This stake, typically represented by a specified quantity of tokens, is immobilized within the protocol, akin to a security deposit. On one hand, the stake is a prerequisite for eligibility as validators, i.e., creators of new blockchain blocks (with mechanisms varying across algorithms); on the other, it represents the "risk capital" that incentivizes the node-validator to act appropriately (for example, preventing the same token from being spent twice (double spending)), and to actively participate in DLT management (for instance, to avoid network disconnections or service blocks). If a node behaves in a manner not conforming to the protocol's stipulations, it is penalized through the forfeiture of a portion of its deposit. Thus, while in PoW mechanisms the assurance of correct behavior derives from the demonstration of work performed (i.e. computational costs), in PoS mechanisms, it arises from a collateralization mechanism.

Pure Proof-of-Stake (PPoS) – This is a variant of the PoS mechanisms, adopted by the Algorand[30] blockchain, featuring additional intriguing characteristics, for instance, in terms of transaction finality guarantees (it is de facto forkless[31]) and, as claimed by the

[26] As observed in the Bitcoin white paper: "To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases," see Nakamoto (2008), p. 3.
[27] The problem of achieving this result through coalitions (mining pools) that coordinate a large number of nodes and are created to exploit economies of scale in the presence of high entry costs (increasingly expensive processors to solve the cryptographic puzzle) is different.
[28] On these aspects, reference is made to: C. Gola and J. Sedlmeir (2022); M. Javarone, et al. (2022).
[29] For the description of other consensus protocols, and their policy implications, see Bains, P. (2022).
[30] See Chen, J., Micali, S. (2019).
[31] The probability of a fork is 10^-18, essentially zero. In such a case, although formally the consensus mechanism is probabilistic, in substance and for all practical purposes, it can be considered deterministic.

project's proponents, is capable of resolving the so-called "blockchain trilemma"[32]. In this consensus algorithm, all blockchain users can potentially participate, without distinctions based on the role of nodes. The influence exerted by each node in selecting the new block of the chain is proportional to the number of tokens held (stake). For each block of transactions to be validated, a node is randomly and secretly chosen to propose a new block (leader node) and nodes with voting rights on the proposal (nodes forming the committee). All online blockchain nodes have the chance to be selected for the roles of leader and committee; however, the probability of being chosen and the weight of their vote are directly proportional to each one's stake. The system remains secure as long as the majority of tokens remain in the hands of “honest” users, who play by the rules established by the blockchain.

Proof-of-Authority (PoA) – The algorithms in this category presuppose the existence of special nodes that take on a coordination role (e.g., acting as "notaries"), effectively serving as trusted third parties. These nodes validate transactions through cryptographic signature mechanisms. Algorithms of the PoA type are essentially only usable in a restricted (permissioned) mode, as the ability to identify such nodes becomes an essential prerequisite. Moreover, unlike algorithms like PoS and PoW, PoA-based systems face scalability issues as the number of validator nodes increases[33]. This is because, in general, the number of messages that validator nodes must exchange to achieve consensus grows with the number of validators.

Box 4 – On Voting Rights, Participatory Mechanisms, and Concentration of power
There are various mechanisms for allocating tokens to nodes participating in the management of the blockchain, also based on the activities carried out. Voting mechanisms can be used both for the ordinary functioning of the DLT (e.g., transaction validation and updating of the shared registry) and for performing "extraordinary" activities (e.g., changing the technical parameters of the native protocol or even the consensus system). For this specific second

[32] The so-called "trilemma" asserts that it is very difficult for a blockchain to simultaneously achieve three objectives: security, scalability, and decentralization; the term was introduced by V. Buterin, one of the creators of the Ethereum blockchain. For example, PoW algorithms usually suffer from scalability problems on-chain. Conversely, blockchains based on traditional PoS consensus algorithms, which scale better than PoW algorithms, suffer from security issues (such as "nothing at stake" and "long-range" attacks, which involve attempts to rewrite the entire blockchain or part of it); these issues are mitigated through complex mechanisms of "punishment" of dishonest users. Finally, DLT technologies described as "Enterprise," usually permissioned, ensure the achievement of security and, to some extent, scalability objectives but do so at the expense of decentralization. In fact, in these technologies, it is common to introduce nodes with special coordination/validation roles that effectively constitute "trusted third parties."

[33] Crash Fault Tolerant (CFT) distributed computer systems can continue to function even if some of the nodes composing them stop responding, due to a malfunction or network issues. Byzantine Fault Tolerant (BFT) systems, in addition to being CFT, can continue to function correctly even if a subset of the nodes behaves incorrectly (which can occur due to malfunction, as a result of a cyber-attack, or due to a node's deliberate pursuit of its own interests to the detriment of others). In the case of blockchains/DLTs, CFT is usually not considered sufficient, and BFT consensus mechanisms are employed.

purpose, particular types of tokens have been introduced in some DLTs (known as governance tokens or voting right tokens).

The underlying logic of some DLT voting systems is to limit concentration, not only in the project launch phase but also over time, and to strengthen incentives - both through a reward and through a participatory mechanism (skin-in-the-game). This is achieved through various means, for example, the random allocation of voting rights[34]. Indeed, excessive concentration of voting rights[35] not only has obvious governance implications but also negatively affects the system's security. Another identified problem is the presence of a high number of voting rights holders who do not vote in decisions to manage changes to the protocol. They are the equivalent of "absentee" or passive shareholders in capital companies. Temporary delegation mechanisms assigned through random processes have been developed. It is also necessary to maintain the involvement of the subject participating in the system over time. This is achieved through security deposits, rewards in the form of tokens, which act as an incentive to provide intellectual or economic contributions, "loyalty rewards," and penalties for improper behavior.

Some possible approaches to voting systems includes:

- *One CPU one vote*: decision-making power is connected to the possession of hardware with high computational power; this principle underlies the PoW algorithm (mining).
- *One token one vote*: for example, in PoS, where decision-making power is linked to the number of owned tokens and deposited. In some systems, the vote can be repeated (multi-round voting) or "timed" (coin aging).
- *One head one vote*: all participants have the right to vote (possible only in permissioned systems).
- *Two stages cryptographically fair lottery*: (Random token – random committee).[36]
- *Pure lottery*: the right to vote is randomly distributed to a defined number of participants without constraints.
- *Lottery only for active nodes*: like the pure lottery, but the right can only be conferred to those who actively participate in the management of the DLT (e.g., developers).
- *Lottery with delegation*: the right to vote is randomly conferred to participants, who can in turn delegate a limited number of other nodes with particular skills. Over time, the delegate earns a reputation.

[34] It has been observed that the use of random allocation of voting rights finds an interesting analogy in some solutions adopted in social choice theory to aggregate preferences, recently revitalized by *computational social choice*, see D. Grossi (2022).

[35] For some data on the concentration of governance token ownership, see FSB (2023), table 1, p. 13.

[36] The “Pure Proof-of-Stake” is a two-phase process: in the first phase, a single token is randomly selected, and its owner is the user who proposes the next block; in the second phase, a given (1000) number of tokens are selected among all tokens currently in the system; the owners of such tokens are selected to be part of a ‘committee’ which approves the block proposed by the first user. Therefore, to belong to the committee, one of the coins owned the active node must win a cryptographically fair lottery. See Micali (2019).

3.3. Off-chain and On-chain (algorithmic) governance

In this section, we will show how some DLT rules are incorporated into the native code (*on-chain*) and, in this way, limit the problems of informational asymmetries (principal-agent problem) through automated systems, while other functions or processes are realized outside of the native protocol (*off-chain*) and sometimes rely on traditional corporate governance safeguards, such as technical committees or coordination bodies among participants.

The overall picture is further complicated by the existence of multi-level approaches, where in some DLTs (second-level blockchains or 'Layer 2', sidechains) it is possible to outsource some processes, which are themselves automated, but often based on different governance/consensus systems[37]. We will briefly delve into these aspects, limiting our analysis to permissionless DLTs, as permissioned ones are governable through traditional corporate management and control systems[38].

Most permissionless DLTs, such as Bitcoin or Ethereum, do not have pre-defined coding features to allow their updating (upgrading). Therefore, when the need arises to improve their security or efficiency, they must face a decision-making process that, in the absence of a structured governance system, can be long and complex. This process, not being provided for by the native protocol, is carried out off-chain[39] (see Box 5). If an agreement is reached, and therefore the majority of the nodes update their software to the new proposed version of the protocol, the update becomes de facto the new version of the native protocol. If a part of the community disagrees with the proposal and consequently decides not to update the version of the software used as a client, a split (hard fork) of the protocol occurs and the shared registry, which from that point onwards will follow distinct evolutions for each of the 'branches' created by the bifurcation[40]. If, on the other hand, the introduced change is backward-compatible, it is referred to as a soft fork: in this case, nodes that do not update the protocol can continue to participate in the

[37] These are functionalities that can be different from those managed in the base protocol, such as layers that manage smart contracts to carry out token exchange activities, lending of crypto-assets, or others. In fact, these systems externalize transaction validation, executing them at level 2 and recording them at level 1. Simplifying, it can be said that level 2 functions "inherit" security characteristics from the underlying level 1. For a description of these additional articulations or "layers" of DLT, see Schär, F. (2021) and IOSCO (2022).

[38] In recent years, numerous contributions have been produced on these aspects, for example: Accenture (2019); Allen, D. W. E., Berg, C. (2020); ASTRI (2016), Hofman, D., et al. (2021); Liu, Y., et al. (2022); Naudts, E., et al. (2022); van Pelt, R. et al. (2020); Wang S. et al. (2019).

[39] See Ehrsam, F. (2017).

[40] Examples of hard forks include those that occurred in the Bitcoin environment with the creation of the "Bitcoin Cash" blockchain, or in the Ethereum environment with the creation of the "Ethereum Classic" and, more recently, "Ethereum PoW" blockchains.

network, although they may not have access to the new functionalities introduced by the update[41].

Box 5 – On-chain, Off-chain, and Mixed Processes

On-chain Governance Processes – These are defined as governance processes written in the native protocol of the DLT. These processes, which could be characterized as complete algorithmic governance, can modify the rules of the native protocol according to predefined forms and methods. In this context, rules related to voting mechanisms, block or transaction sizes, interface modes (API/RPC), for example, could be decided and directly inscribed into the protocol. The decision-making process is embedded directly within the source code of the protocol. Various mechanisms guiding the process or aggregating participant preferences can be introduced, along with non-modifiable technical (e.g., base code language) or managerial constraints (similar to non-modifiable substantive rules of a statute). Advisory bodies, committees, spontaneous aggregation groups may exist, but final decisions occur through referendums open to network participants, following predetermined and unalterable modes established by the blockchain. It is worth noting that, based on our knowledge, a DLT with entirely on-chain governance has not yet been developed. However, there are advanced development projects aiming to eliminate any off-chain phases, seeking to develop complete algorithmic governance.

Off-chain and Mixed Governance Processes – These processes are not directly written into the native protocol of the DLT but involve organizational or decision-making functions performed externally. Similar to the previous case, there may be technical bodies or committees, but decisions take place off-chain through a traditional organizational structure. Understanding these decision-making processes, power and responsibility allocations, delegation mechanisms, etc., is crucial for evaluating the governance of a DLT. It is at the off-chain level that opacity, fragility, distortions (such as excessive concentration of power) can nest, as this operational mode does not guarantee the transparency levels of fully automated on-chain processes. It is, of course, a "transparency" that depends on the technical and material ability to verify and understand such publicly accessible content. Clearly defined and structured off-chain processes have the advantage of leveraging traditional corporate governance safeguards, including responsibility attribution and accountability.

In reality, at the current state, most DLTs have a mixed configuration, with some processes fully automated on the blockchain and others occurring outside it, through more or less formalized coordination among network participants. Of the two case studies described in the

[41] Examples of soft forks include upgrades to the Bitcoin protocol known as "SegWit" and "Taproot," which, although introducing innovations to the protocol - for example, in terms of scalability features or cryptographic signature technologies - did not produce a fork of the shared ledger upon their introduction.

appendix, Ethereum has a strong off-chain component, while Polkadot operates predominantly on-chain[42].

Off-chain procedures involve various decision-making and coordination mechanisms, both formal (through decision-making and control structures established by the initiative's founders) and informal (for example, through blogs, social networks, or other forums formed among network participants)[43]. These decision-making processes can be lengthy and lead to suboptimal results; they are often open to the community, but final decisions may be made opaquely or in a top-down manner. The threat of a fork (hard-fork) establishes a certain discipline that encourages network members to find a less traumatic solution. In fact, when these events occur, ex-ante uncertainty and ex-post transactional and adaptation costs are incurred.

From the perspective of corporate governance, the implications of different types of updates are evident. In cases where the changes to be made have modest impacts, resulting in a soft fork, it is easier for consensus to be found among users. Conversely, in the case of radical changes, with a potentially strong economic impact resulting in the loss of value of "installed capital" (e.g., hardware devices used to participate in the DLT) or requiring new investments, reaching consensus on the update can be problematic. The problem is even more relevant in the case of changes following the identification of computer vulnerabilities, which would require rapid intervention times.

To overcome the limitations of the above-described governance systems, two approaches can be identified: a) the community could organize with more structured and balanced governance functions, adhering to traditional role separation criteria to avoid conflicts of interest, moral hazard, and concentration of power; b) further expand the scope of on-chain algorithmic governance, incorporating additional decision-making automatisms into the protocol that establish a self-governing system, including "endogenous" rules that allow modification of the native protocol (so-called upgradable blockchain - see M. Ciampi, et al. 2020).

Some DLTs are following this second path (e.g., Polkadot, Tezos, Internet Computer (ICP)), although for now, they are still in a hybrid form between the two models. The debate is open and involves, on one side, supporters of a fully on-chain model, based

[42] For a position in favor of the mixed approach with a strong off-chain component, see the posts by the founder of Ethereum, V. Buterin (2017, 2021).
[43] For example, for Bitcoin, there is BIP, and for Ethereum, there is EIP (https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals and https://ethereum.org/en/eips/).

solely on algorithmic governance that includes the ability to upgrade the blockchain; on the other side, doubts persist among those who emphasize the emergence of numerous complexities and unsolvable trade-offs in a satisfactory manner.

Fully on-chain governance structures usually follow a predetermined decision-making process in a sequential path inscribed in the algorithm. For example: i) submission of change proposals; ii) provisional acceptance of the proposals; iii) creation of a parallel blockchain to test the proposals; iv) incorporation of the proposals once the experimentation phase is passed; v) allocation of rewards (in the form of tokens) to the entity (or persons) participating in the system. To avoid power concentration, the system usually imposes limits on this last step.

The same procedure is followed in off-chain operating DLTs, but with a fundamental difference: if governance is fully algorithmic, the entire process takes place directly on-chain by default, transparently and bindingly ex-ante (and, as such, easily accessible to an external auditor). Like all "constitutional" rules, they should not only indicate through which procedures and voting mechanisms it is possible to modify the native protocol, but also impose constraints on such changes to preserve its fundamental principles. For example, a DLT could establish governance rules allowing a transition from a Proof-of-Work-based protocol to a Proof-of-Stake-based one while simultaneously ensuring compliance with pre-established participation requirements.

4. When Regulatory Intervention is Necessary

In general, regulators should adhere to the principle of technological neutrality to avoid interfering with the autonomous developments of the market (OECD 2022). However, we acknowledge that regulatory action is justified by the need to promote an efficient allocation of resources, especially in cases where the market cannot achieve this condition spontaneously through free competition among economic agents. Efficiency is maintained if there are no market failures[44]. These can occur in both permissioned DLTs - effectively falling within traditional governance systems - and in permissionless ones, which are not free from corporate governance issues, such as due to the concentration

[44] These can arise from: i) informational asymmetries (which can favour situations of moral hazard or dishonest behaviour, for example, by some parties (the "agents") towards the promoter of the initiative (the "principal")); ii) exploitation of dominant positions, also through excessive concentration, entry barriers, poor interoperability, or other aspects that limit market contestability, such as - in our context - the presence of few mining pools; iii) creation of negative externalities (in the form of financial contagion, negative environmental impact, infringement of certain rights). Aspects not attributable to the principle of Pareto efficiency should also be considered, such as, for example, the protection of privacy, inclusiveness, or the need to protect individuals and society as a whole from risks that are "unacceptable" from an ethical point of view (aspects considered, for example, in the European proposal regulation on artificial intelligence (Artificial Intelligence Act)).

of voting rights. Regulatory intervention should be calibrated based on risks potentially not mitigated by the market. The rules should be applied in non-traditional ways, understanding the inherent difficulties in doing so in a decentralized environment. We will explore these aspects, including the role of transparency through the so-called white paper that usually accompanies DLTs projects. This aspect is crucial, especially in a context where it is necessary to inform the market about the characteristics of this new technology.

4.1. Transparency and the Role of the White Paper

The analysis of standards that should be respected for good DLT management is not within the scope of this work. We limit ourselves to highlighting the aspects that the initiative's promoter should outline in the white paper (WP) during the project's launch[45].

The WP should first describe the purposes of the DLT, the underlying strategy, its economic sustainability, and, in a non-technical manner, the main aspects of the "consensus protocol" on which the creation of tokens, the role of nodes, incentive mechanisms, and the voting system depend.

In more detail, the WP should indicate whether the DLT is permissionless or permissioned, public or private; whether it intends to follow a predominantly equalitarian or "capitalistic" approach, where entities holding a larger number of tokens have the opportunity to decide on the DLT's strategic choices. The WP should specify if stakeholders can operate collectively or individually (through bodies, committees, coalitions, both on-chain and off-chain). If the DLT "creates" tokens, the WP should distinguish whether they include rights, such as access rights to the "extraordinary" management of the blockchain (changes to the parameters of the native protocol or its operation), or only rights to "ordinary" management (transaction validation, backward-compatible updates); it should clarify how tokens are allocated to participants, for example, randomly, based on computing power (CPU) used, as a result of a commitment (collateral deposit), or active contribution to writing the protocol. If the DLT envisions a de facto partnership among an identifiable number of participants, it should clarify the social nature and the jurisdiction of belonging to provide legal certainty to the initiative and protect stakeholders. In this case, as indicated by OECD principles (2015, 2017), the three fundamental aspects of corporate governance should be analytically

[45] Reference is made to the document that usually accompanies the launch of a DLT, such as the well-known Nakamoto WP (2008).

addressed: ownership and control structure and concentration; control tools; exercise of control.

Regarding technical aspects, the WP could consider governance criteria for DLTs recently developed by the International Organization for Standardization (ISO)[46]. These should be integrated by adapting the Basel Committee's guidelines on bank governance (BCBS 2015). In particular, the following aspects should be analytically covered[47]:

- Consensus protocol used and governance implications: ISO P3;
- Stakeholders (nodes; full nodes): identification, concentration: OECD-1; ISO-P1; BCBS-2 and 3;
- Upgrading the native protocol (on-chain and off-chain) and conflict resolution (without hard forking);
- Types of generated and exchanged tokens (with or without embedded administrative or proprietary rights):
- Control exercise through participation in bodies and voting on-chain and off-chain;
- DLT management, both on-chain and off-chain: ISO P2; BCBS-4 and 5;
- Transparency and degree of openness (public and private DLTs): ISO-P4; BCBS-12;
- Incentive mechanisms (token allocation, fees, penalties): ISO-P5; BCBS-10;
- Risk management, privacy, and integrity of the DLT: ISO P7 and P8; BCBS- 6, 7, 8;
- Compliance and auditing functions (explicit or through market discipline): BCBS- 9, 10

4.2. Governance Requirements Based on Performed Activities

A fundamental component of good governance involves identifying, monitoring, and managing risks. This depends on its use. It is important to note that DLT can be used for a wide variety of functions. In the banking and financial sector, this ranges from managing a shared ledger, creating and distributing an unbacked token (without embedded rights), transferring traditional digital assets to a full-fledged payment system.

[46] See ISO (2022).
[47] Alongside each aspect to be considered, the number of the applicable principle is indicated.

Each of these functions corresponds to a different set of risky events and negative impacts on the system. It is therefore necessary to establish a functional relationship (mapping) between activities carried out through DLT, the risks it can generate, and their respective impacts. Here, we propose a logical framework that can be easily developed by adopting conventional risk monitoring and management tools.

Table 1 - Activities Supported by DLT and Related Risks[48]
(Activities and associated risks)

A1	Creation of a shared register (e.g., for supervisory purposes)	R1 = information corruption
A2	Creation of a token without embedded rights	R2 = technological vulnerabilities
A3	Creation of a token with embedded rights (e.g., NFT)	R3 = ambiguous definition of rights
A4	Transfer of token avoiding soft or hard forks	R4 = duplication of ownership
A5	Exchange and custody of crypto-assets	R5 = pour consumers or investors protection
A6	Operation of a trading and settlement system for a financial instrument	R6 = market integrity failure
A7	Transfer of "tokenized" electronic money	R7 = lack of proper banking or financial license
A8	Brokerage activities based on "tokenized" instruments (collateral, loans, derivatives, etc.)	R8 = poor collateralization
	…	
An	Other activities	Rn = other type of risks

Through this mapping, regulators could impose progressively stringent rules based on the impact of these risks. The required requirements could range from simple constraints on computer robustness, compliance with privacy criteria, adherence to anti-money laundering and combating the financing of terrorism (AML/CFT) regulations, to more pervasive rules, such as for DLT protocols supporting a stablecoin with monetary

[48] For a list of use cases and their frequency, see: Deloitte (2021), p. 18.

functions. Table 1 illustrates a mapping between given activities A1, A2, ...An, and the corresponding risks R1, R2, …Rn that would be generated by the malfunctioning of the DLT (the examples of risks provided in Table 1 are purely illustrative). The analysis of processes aimed at identifying, monitoring, and mitigating DLT risks is not within the scope of this work. Our goal is to demonstrate how these processes can be embedded in an appropriate governance structure.

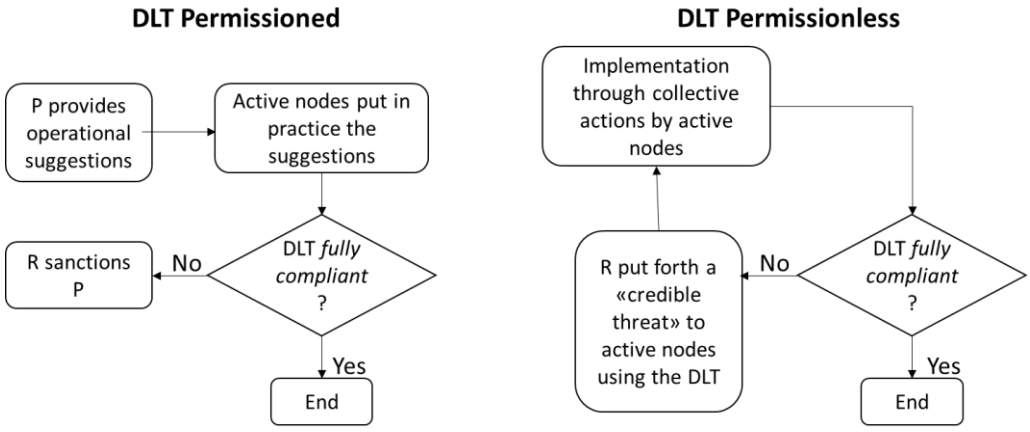
4.3. On the Issue of the Entry Point

Once the governance requirements that a DLT should adhere to have been identified, the following question arises: how can the regulator enforce these requirements on a decentralized or partially decentralized structure like a DLT? While in permissioned DLTs, it is possible to establish interaction between identifiable entities (individual persons or legal entities) and the regulator, such interaction is not feasible in the usual ways when facing an indefinite and anonymous or pseudo-anonymous set of actors (nodes) collectively "governing" the blockchain, as is the case in permissionless DLTs. In these cases, the literature on the subject seems to rely on forms of indirect enforcement[49]. These take the form of an iterative process between the observable object (the blockchain) and the entity (or entities) tasked with assessing whether the DLT adheres to certain principles or rules. In following this approach, reference could be made to the OECD *functional equivalence principle* (OECD, 2017), which aims to evaluate the end result of a governance process, where substance prevails over form. Let's explore these aspects in more detail.

Permissioned DLTs - Figure 1 stylizes the two situations: in the traditional approach (applicable to permissioned DLTs), the initiator of the project (which we call P and could also be represented by a group of consortium members) provides a series of strategic indications to a set of agents (or operational nodes) that, in more or less hierarchical ways, fulfill certain functions (such as proposing improvements to the system's security) and are responsible for the initiative. These functions or processes, once incorporated into the DLT, are observable by the regulator, an auditor from a market self-regulatory body, or the DLT user (for example, a bank manager delegated to monitoring). We refer to these entities as R. If the DLT does not comply with certain rules or principles, R can take action against P if it is not fully compliant.

[49] See, for example, Y. Liu et al. (2022); ISO (2022).

Figure 1 - Enforcement of Governance Rule



The governance rules to be followed should be calibrated based on the mapping described earlier, depending on the type of activity performed. In case the principles of governance required for a DLT used for a specific activity (e.g., transferring "tokenized" bonds) are not adhered to, R can act through direct supervision of the DLT's managers or group of managers. This would assimilate it to a market IT infrastructure (as in other areas, such as payment systems). R could establish that a certain infrastructure cannot be used to perform certain functions.

Permissionless DLTs - Let's now describe the methods of implementing good governance for a permissionless DLT. In this case, in the absence of a clearly identifiable subject, the only viable option seems to be an indirect action aimed at achieving a "state" for the DLT consistent with the criteria deemed satisfactory by R. In this case, R can act on the users of the DLT by discouraging its use if it does not meet certain criteria.

The improvement, only gradual and tendential, towards characteristics acceptable to the regulator would occur through the process illustrated on the right side of Figure 1. This approach is consistent with the typical operation of open-source systems and many permissionless DLTs (see the case of Ethereum in the Appendix). Moreover, this process does not seem far from what is referred to in law as "participatory regulation" (although in a traditional context, it occurs in a structured way through consultation procedures). The collective action of agents participating in the network should implement the necessary corrections, if consistent with the economic benefits of the majority. The process would, in principle, allow adaptation even in the event of a possible change in the rules and activities supported by the DLT.

In this process, the ability of R to implement "credible threats" becomes crucial to incentivize DLT users to adhere to desirable standards[50]. A threat is credible if the regulator demonstrates to have the expertise to evaluate the correct, albeit indirect, application of the rules imposed on that class of DLT and can show that it has tools for indirect enforcement. The mere threat could induce network participants, even without explicit coordination, to converge towards a solution consistent with R's rules, in the interest of all stakeholders. It is plausible to think that the threat of "migration" by many users to a more rule-abiding DLT could lead the community collectively managing that DLT towards protocols that apply the desired standards. For example, it was the international community's pressure on the negative environmental effects of PoW that induced Ethereum's ecological transition, even at the cost of significant "adjustment costs."

Table 2 shows the interfaces (the entry point) for applying governance rules, both directly and indirectly (through supervised intermediaries or other entities). If the individual intermediary or a group of supervised intermediaries (e.g., in the form of a consortium) are themselves the managers of the DLT, and it is permissioned, then it is possible to act directly (columns A and B)[51]. If intermediaries use identifiable third-party services (column C), competent authorities could have certain supervisory powers. Several banking authorities[52] have powers of informative and inspection supervision, as well as limited sanctioning powers and intervention on suppliers that provide outsourced activities for supervised intermediaries, as they must comply with criteria for sound and prudent management. The new European legislation on digital operational resilience (DORA) strengthens oversight over suppliers of supervised intermediaries, introducing both specific requirements for ICT risks, including those of third parties, and a direct surveillance regime for critical third-party ICT.

There is currently no enforcement method for permissionless DLTs, although a mixed surveillance approach (individual and consortial) could be applied to permissionless DLTs with a significant off-chain component (column D)[53]. Regarding permissionless DLTs with entirely algorithmic governance (on-chain), the only viable option would be

[50] For this concept, typical of game theory, see the classic contribution by C. Schelling (1960), chapter 8.
[51] See CPMI-IOSCO (2022) with reference to stablecoins. On the management of a DLT for a market infrastructure, see E. Naudts et al. (2022), pp. 11-13.
[52] See also EBA (2019); ESMA (2021).
[53] It should be noted that recently the European Commission, in the proposal for a regulation on the use and fair access to data (Data Act Regulation), after defining smart contracts, regulates their requirements (robustness, blockability, auditability, etc.); these requirements, in the Commission's proposal, should be met either by the provider of the applications that use the smart contract or, in its absence, by the person (in our interpretation, a node of a DLT) whose commercial, entrepreneurial, or professional activity involves the implementation of smart contracts for other parties in the context of a data provision agreement. (Data Act, art. 30).

the previously described indirect enforcement (column E). This is, of course, only an iterative and long-term enforcement process. The legal problem of the possibilities of reaction of the subject who considers themselves prejudiced by the operation of the protocol remains unresolved; an aspect, as emphasized at the beginning, that is beyond the scope of this work.

Table 2 - Entities, forms of corporate governance, and possible entry points

	DLT permissioned			**DLT permissionless**	
	A – Single Intermediary	B – Market infrastructure (MFI)	C- Third parties ITC	D – *Off-chain*	E – *On-chain*
Corporate governance	Traditional	Traditional	Traditional	Mix (algorithmic + Corporate governance bodies)	Full algorithmic
'Entry point'	Single entity	Single entity or group of entities	Indirect	Indirect	Indirect (via market discipline)
Relevant regulation or Guidelines	OCSE (2015) BCBS (2015) DORA (2022) DLT Pilot (2022) MiCAR (2023)	OCSE (2015); CPMI-IOSCO (2022); ECB (2021a); ECB 2021b)	OCSE (2015) DORA (2022) DLT Pilot (2022) if "systemic" MiCAR (2023)	OCSE (2015)	OCSE (2015)

4.4. On the Limits of a Decentralized Governance System

Blockchain technology is evolving to improve efficiency and flexibility of use. To achieve this, it is introducing more structured forms of governance, although still in the preliminary

stage. Two paths have been followed, still widely debated among experts[54]: the first (followed for example by Ethereum) involves adopting elements of traditional corporate governance developed through bodies or functions external to the electronic protocol (off-chain); the second (followed for example by Polkadot), more ambitious, aims to develop a complete algorithmic governance. This includes meta-rules aimed at reviewing, according to predefined methods, even the "constitutional" rules of the protocol, seeking to eliminate the need for external governance structures. However, three aspects limit this approach.

The first relates to the impossibility of modifying the native code in ways incompatible with the rules that the code (the "constitution") establishes as unchangeable. Like all contracts, they can be incomplete in the event of unforeseen circumstances ex-ante. The second aspect concerns situations that require flexibility or difficult interpretation, associated, for example, with a “criterion of fairness” that is not easily defined. The third aspect would be the difficulty of having a purely automated system that preserves incentive mechanisms in every circumstance, avoiding forks. These can create triggers or automatisms with systemic effects that are difficult to control. If the impact of such rare events were particularly high considering the activity carried out by a specific DLT, a precautionary approach based on traditional governance forms would be preferable. At the current state of technology, it seems appropriate to entrust complex market infrastructures only to DLTs supported by historically established and long-tested governance structures. These would be able to implement known risk detection, monitoring, and mitigation systems.

5. Conclusions

The work shows that DLTs that are predominantly based on on-chain processes reduce informational asymmetries, thereby addressing most of principal-agent issues. However, they face difficulties in adopting traditional corporate governance safeguards. DLTs based mainly on off-chain processes are more exposed to principal-agent issues, but traditional safeguards can be applied to mitigate risks and improve governance processes. In the world of DLTs, a phenomenon similar to what happened in the evolution of open-source systems in the early 2000s is observed: from "spontaneous" governance structures, aimed at developing and improving software openly and collaboratively, there has been a shift towards more structured forms, essential to

[54] See interventions by V. Buterin (2017, 2021).

facilitate collective decisions and overcome potential conflicts among participants (P.B. De Laat, 2007). There is a growing awareness of these issues, and different solutions are being experimented with. Some DLTs are moving towards hybrid forms, complementing algorithmic governance with external structures of more traditional corporate governance; others aspire to entirely incorporate these processes into the computer protocol. Advocates of the approach based on complete algorithmic governance intend to realize the idea of creating an open, egalitarian structure organized in a network. In both models, to avoid excessive concentration of powers and roles, the expedient of randomizing the assignment of managerial roles and voting rights has been used (a method also widely explored in social choice theory).

The outcome of these developments is difficult to predict, but it is certain – as in the field of artificial intelligence – that this technology opens up new and unavoidable scenarios for the operation of the economic system.

Based on the analysis carried out, the work suggests different approaches for enforcing the most appropriate corporate governance rules for each type of DLT[55]. With particular reference to on-chain processes, as there is no direct interface for a regulator or an external auditor to perform enforcement activities (the so-called entry point problem) indirect action can be taken through two mutually reinforcing channels:

i) Through market discipline, achieved via interaction with the active community within such systems; this is a typical approach of many open-source structures, whose operations are detailed, including two case studies (Ethereum and Polkadot). The collective action of network participants and the presence of endogenous incentive mechanisms could lead to improvements in system governance;

ii) By requiring entities active in regulated sectors using a DLT to rely only on systems capable of meeting satisfactory governance criteria. These criteria would be calibrated based on the activities supported by a given DLT. The work illustrates the application of a flexible criterion based on governing rules according to the impact generated by potential negative events.

What emerges from the work is that DLTs based on a decentralized decision-making system, even entirely automated, need a clear, well-balanced, and robust governance structure if they intend to meet efficiency, scalability, flexibility, and security

[55] A methodology for describing and comparing DLTs with different technological, functional, and governance configurations is provided by: Gola, C., Fiorenza, P., Laurino, F., Lesina, L. (2024).

requirements. In pursuing this balance, the well-established experience from the developments in corporate governance, legal foundations, and economic theory is certainly helpful, as these fields have long addressed numerous aspects useful in this context. On the other hand, the paradigm shift introduced by this technology requires a revision of some consolidated categories in the aforementioned disciplines. It is also necessary for traditional economic actors, including policymakers, to have an in-depth understanding of these technological developments.

Appendix: Two Case Studies: Ethereum and Polkadot[56]

Throughout the text, Ethereum and Polkadot have been mentioned several times. The reasons for selecting these two DLTs are as follows: Ethereum is the second most widely used network globally[57] after Bitcoin, and it has been chosen because its governance model involves a balance between on-chain and off-chain processes, similar to numerous other blockchains. Polkadot represents an example of a blockchain aiming to achieve fully algorithmic governance.

A1 - Ethereum

Ethereum is an open-source computing project launched in 2015 by a Russian/Canadian computer scientist, Vitalik Buterin, with the goal of using blockchain technology for a broader range of purposes than initially envisioned by Nakamoto's protocol. The idea was to design a permissionless DLT, not only public (open for both writing and reading) but also flexible and fully programmable[58]. Ethereum provides the foundation for implementing binding programs for parties based on predefined procedures (smart contracts).

The Ethereum protocol and activities:

- Maintains a distributed ledger of transactions. This ledger is public, containing transactions related to the native token as well as transactions of tokens implemented on the Ethereum platform through smart contracts.
- Creates a token, called Ether (symbol ETH), which: 1) allows participation in the system's governance, granting the ability to validate transactions, subject to a stake deposit (or staking) of at least 32 ETH; 2) can be used to pay transaction fees on the ETH network or to execute smart contracts on the Ethereum blockchain. The latter enables developers to create on-chain crypto-assets, especially in the decentralized finance (DeFi) sector.
- Allows the creation of entities governed by computer code (Decentralized Autonomous Organizations, DAOs), also through the use of smart contracts.

[56] For a more in-depth analysis of these two DLTs, see: Gola, C. et al. (2023).
[57] For updated statistics, reference can be made, for example, to https://coinmarketcap.com/.
[58] To this end, a model of a distributed virtual machine among all participating nodes in the network has been created, called the "Ethereum Virtual Machine" (EVM); to develop code for this virtual machine, specific programming languages (Solidity and Vyper) have been developed. Among the most representative members of the developer group that created Ethereum, a prominent role is played by Vitalik Buterin, who is still one of the main leaders in the evolution of Ethereum, and by Gavin Wood, who conceived the Solidity programming language, and who subsequently promoted the development of the Polkadot blockchain.

Degree of Decentralization

Determining the degree of decentralization of Ethereum is currently quite challenging, partly due to the recent transition of the protocol from the Proof-of-Work (PoW) consensus mechanism to Proof-of-Stake (PoS). Before the transition to PoS, block validation on the Ethereum blockchain occurred through mining, a competitive process that required each participating node to consume a significant amount of electricity. This process also necessitated the use of increasingly powerful and expensive processors. The pursuit of economies of scale led to the creation of so-called mining pools. Within the Ethereum network, there was a pressing need to promote a transition to a less concentrated consensus protocol, especially one with a lower environmental impact. For years, the Ethereum community had been working on this transition in a secure, shared, and governance-wise robust manner.

The Transition from PoW to PoS

On September 15, 2022, the Ethereum blockchain transitioned from the PoW consensus mechanism to a PoS consensus[59], merging Ethereum Mainnet (the main blockchain) with the PoS Beacon Chain (a chain built specifically for the transition from PoW to PoS). This fusion significantly reduced the energy consumption of the Ethereum network, addressing a long-standing criticism. The introduction of the PoS consensus mechanism, according to the network developers, is part of a broader project aimed at increasing the efficiency, security, and scalability of the network.

PoS-based Governance of Ethereum

The new PoS algorithm of Ethereum employs a process that randomly selects nodes from the active network as "validators" for a brief period. This selection occurs through a random process, similar to a lottery. Unlike the PoW mechanism, this algorithm does not require specific computational power, significantly limiting energy consumption and preventing the concentration of validation power in a few nodes. In PoS systems, adding new blocks to the blockchain is called "forging" instead of mining; nodes participating in the forging process must deposit (stake) a minimum of 32 ETH in a public address on the network. While it's possible to deposit more ETH than the minimum required, doing so does not increase the likelihood of a node being selected as a block validator. This

[59] The upgrade process, rather complex, took several years to solve technological problems and, above all, to find agreement among the majority of network participants. It involved first creating a separate network, called the "Beacon Chain," with a PoS consensus mechanism; subsequently, the main Ethereum network ("mainnet") was unified with the Beacon Chain. The unification of the two networks allowed, in very simplified terms, to resume the state of the first and the consensus mechanism of the second.

measure is designed to mitigate concentration of the transaction validation process among a few entities holding significant amounts of ETH.

Every 12 seconds, a node with at least 32 ETH at stake is randomly chosen to validate a block, which is then broadcast to the rest of the network with its "digital signature." The transactions in this block are re-verified by a group of randomly selected validators tasked with providing a final "vote" on their validity. Blocks deemed correct by the majority are added to the blockchain, while others are discarded. As each block has a verifiable proponent, any malicious or fraudulent behavior by the proponent is discouraged through a punitive mechanism that can lead to the exclusion of the validator from the network (slashing), resulting in the loss of the staked ETH.

Governance

Despite being a public permissionless protocol, Ethereum's governance structure is complex. While the consensus mechanism described above is entirely managed on-chain, key governance decisions regarding protocol development and changes are handled off-chain, involving a plurality of stakeholders with different roles. The process begins with the publication of Ethereum Improvement Proposals (EIPs[60]) on the web, which can be proposed by any participant in the Ethereum community[61]. The proposed EIPs are then discussed on public forums[62] by network participants, but final decisions on which EIPs to implement and when are made by the core developer team off-chain. This is because there is no defined procedure for handling controversial proposals and conflicts among the various stakeholders affected by the implementation of a specific EIP.

Ethereum Foundation

Ethereum Foundation is a non-profit institution chaired by its founder, Vitalik Buterin. The Foundation does not own the intellectual property of the Ethereum software, nor does it directly control it. The foundation's purpose is to support the information technology infrastructure in its routine maintenance and potential structural improvements (upgrades) for the benefit of the user community. The Foundation includes programmers, companies, and entrepreneurs who may hold shares of the tokens issued by the protocol. The majority of blockchain projects, not just in DeFi but also for other purposes,

[60] EIPs are technical standards for preparing proposals concerning protocol changes such as the implementation of new processes and functionalities.
[61] The community consists of all ETH holders. However, given the high technical level required to submit a well-crafted EIP, usually, a large portion of EIP authors are application or protocol developers.
[62] Ethereum Magicians Forum, https://ethereum-magicians.org/.

use Ethereum as the foundational infrastructure of an entire ecosystem. The Foundation allocates financial resources, denominated in ETH, through decision-making procedures that are not easily identified, determining which projects are more deserving.

Core Developers

Changes to the native protocol occur through the interaction between the developer community proposing changes and a small set of core developers (which includes Vitalik Buterin). The core developers' group, consisting of over 200 members, meets monthly. The process described above occurs off-chain, meaning it does not involve an automatic and binding integration of new procedures into the native protocol. In the past, under the PoW-based regime, a majority of the computational power of full nodes (validator nodes) was required for this, and they needed to agree before, during, and after the protocol upgrading process. If there was no agreement, it resulted in a duplication of the blockchain, creating a new token. With the transition from PoW to PoS for making changes to the native protocol, the majority of staked tokens by validators is now required instead of computational power.

Ethereum Classic

As mentioned earlier, in case of disagreement among the validator community (formerly miners) regarding some aspect of Ethereum's code, there is a possibility that the community, and consequently the blockchain, forks, as has happened in the past. The current Ethereum blockchain originated from a fork and does not contain the unchanged history of the network itself, which remains in the blockchain now known as Ethereum Classic. In 2016, the Ethereum foundation, following a hack of a third-party project (resulting in a loss of €50 million equivalent in ETH), created a new version of the main blockchain with a state change that effectively fixed the damage. However, a minority part of the community of miners (and users) decided to consider the state change illegitimate, advocating the concept of "The code is law," and continued participating in the original Ethereum network, renamed Ethereum Classic.

A2 - Polkadot

Polkadot is a system that enables various blockchains, based on different consensus protocols (e.g., PoW, PoS, PoA, both public and private), to communicate securely and reliably. It aims to create a global market infrastructure that makes different types of blockchains or DLTs compatible (interoperable) with each other.

The Polkadot system is built upon a main blockchain, called the Relay Chain, created by the initiative's promoters, and secondary blockchains, known as Parachains, which integrate with the main chain. The Relay Chain is designed to coordinate an entire ecosystem where numerous blockchains, created by various developer groups, connect to the Polkadot system. The Parachains connected to the Relay Chain share the same level of security. If, for any reason, the Relay Chain were to discard a transaction or any other type of shared ledger update, all connected Parachains would also be required to discard it. This makes the entire Polkadot ecosystem coherent in its parts.

The Polkadot protocol and activites:

- Holds a distributed ledger of transactions. This ledger is public and contains transactions from various Parachains that are part of the Polkadot protocol. Any full node in the system can temporarily apply to contribute to writing blocks on the ledger.
- Creates a token called DOT, which: 1) allows participation in system governance, providing the ability to nominate or vote for validators; 2) can be used as a stake to operate within the system; 3) enables the addition of new Parachains to the system.
- Provides crowdfunding services for Parachains that cannot afford a slot within the protocol.
- Offers custody services (wallet).
- Allows the transfer of tokens between different Parachains, between Parachains and the Relay Chain, and even from external blockchains through special applications called bridges.

The Polkadot system relies on a set of stakeholders and governance bodies with distinct functions: there are "validators," "nominators" (who support validators in a fairly distributed manner), "collectors" (who collect blocks from Parachains to be included in the main protocol), and "fishermen" tasked with intercepting and penalizing nodes that behave incorrectly. There are also algorithmic bodies that give structure to the entire process: the Referendum, the Council, and the Technical Committee. The system, still evolving, aims to create a balanced and fully automated system, eliminating the need for

bodies presided over by individuals or entities with privileged roles, thanks to the role played by the referendum.

Degree of Decentralization

Polkadot is a permissionless public DLT characterized by a high level of decentralization, mainly derived from the introduction of a protocol called Nominated Proof of Stake (NPoS). The goal of this protocol is the periodic election of a defined number of validators from an indefinite number of possible candidates, responsible for recording new transactions on the Relay Chain, including those from various Parachains within the Polkadot protocol.

Nominated Proof of Stake (NPoS):

Validators are nodes temporarily tasked with block production on the Relay Chain, including transactions made on the various Parachains, which are also part of the protocol. Any node with the technological infrastructure to continuously perform the functions required by the Relay Chain can apply as a validator. To apply, validators lock a certain amount of DOT, which will be returned at the end of their operation unless there are misconducts, along with a reward for the work done. The activity of a validator lasts about 24 hours (called an "era"), after which a new election takes place.

Nominators are nodes that participate in the election of validators by financially supporting a set of candidates through a collateral deposit of a certain amount of DOT. This deposit is then divided among the selected candidates by the nominator and added to the candidates' initial deposit. If the selected validators by the nominator are successfully elected and produce at least one block, a portion of the validators' reward goes to the nominator, proportional to the amount of DOT deposited by them. If one of the validators misbehaves, their deposited DOT is seized, and the same principle applies to the nominators who supported them. Therefore, nominators are incentivized to choose validator candidates based on the amount of stake they support, the candidates' past performance (indicators of their honesty), and the fees charged by the validator.

The system described above is implemented by an algorithm called Phragmén's Sequential, whose ultimate goal is to maximize the number of tokens locked by validators, ensuring the highest possible level of stake equal distribution. This would guarantee decentralization and security: decentralization because the election algorithm ensures that even minorities (validators supported by few nominators) are proportionally represented if associated with a sufficient amount of tokens; security because, with the

maximization of the minimum deposit, each validator is supported by a large amount of DOT, making the election of a malicious validator involve a significant investment of DOT (which risks being lost).

Another element favouring the decentralization of the system is that the rewards received by validators when they record a block on the Relay Chain are independent of the amount of DOT staked to support the validator. This means that nominators of popular validators receive a lower reward (as it has to be distributed among more supporters), incentivizing them not to always vote for the same validator (which would lead to centralization, as in the case of mining pools) but to sufficiently diversify their votes.

Coordination between Relay Chain and Parachains:

As described earlier, the role of validators is to validate blocks on the Relay Chain containing transactions made on individual Parachains. Since validators do not have a synchronized database of all Parachains (as that would be too burdensome), they rely on collector nodes to create blocks for Parachains. Validators control and are responsible for the correct state transitions of the Parachain; this responsibility is randomly assigned and changes every time a new block is created. Multiple validators are generally responsible for the same Parachain.

Collectors:

The system also includes the figure of collectors responsible for the operation of all various Parachains. They collect transactions made on Parachains by users and produce proofs of state transition—meaning, through a specific algorithm, proof that the new block is consistent with the previous block, regarding the same Parachain—for Relay Chain validators. In other words, collectors aggregate Parachain transactions into "Parachain block candidates" and produce proofs of consistency with previously validated blocks so that Relay Chain validators can insert the blocks into the Relay Chain. Collectors operate as full nodes for both the Relay Chain and the specific Parachain to which they are connected; this means they retain all the information needed to create new blocks and perform transactions similarly to miners operating on PoW-based blockchains. Unlike validators, collectors are not tasked with ensuring security for the network. If a Parachain block is not valid, it will be rejected by validators.

Fisher Nodes:

Represent an additional security measure in the system. Their role is to identify validators behaving incorrectly. Fisher nodes are complete nodes of Parachains, but unlike

validators, they play a different role in the Polkadot network. Instead of packaging state transitions and producing subsequent blocks for Parachains, fisher nodes observe the entire process and ensure that invalid state transitions are not included. Currently, the figure of the fisher node has not been made operational in the Polkadot network, although it has been envisaged in the overall design of the infrastructure.

Creation and Finalization of Relay Chain Blocks:

The consensus mechanism of the Polkadot protocol governs the creation and finalization of blocks on the Relay Chain. Finalization can generally be of two types: probabilistic or deterministic. With probabilistic finalization, each node knows that a block is finalized with a certain probability, as in the case of Bitcoin. As time passes and the chain grows, the chances that a block created in the past may become invalid decrease (it would be too costly to go back and change the system's history). However, there is never 100% certainty. With deterministic finalization, once a block is finalized, that state becomes permanent and cannot be changed. The drawback in this case is that the process of creating new blocks could become very slow: one must wait for the complete finalization of the previous block before adding a new one (since it is irreversible). In Polkadot, the goal is to leverage the advantages of both types of finalization: the agility and speed of the probabilistic approach and the facilitation of communication with blockchains outside the Relay Chain of the deterministic approach. To achieve this, the processes of block creation and finalization are separated and independent of each other: the first is called Blind Assignment for Blockchain Extension (BABE), and the second is GHOST-based Recursive Ancestor Deriving Prefix Agreement (GRANDPA).

BABE Process:

Each "era" (the period of validity in office for a validator) is divided into "epochs," and each epoch is divided into multiple time windows (slots); each slot corresponds to the creation of a block. At the beginning of the era, validators are randomly assigned a slot. Multiple validators can operate in the same slot. When it's their turn, the validator creates the block and adds it to the longest chain that contains the last block finalized with the GRANDPA algorithm. It is observed that the last finalized block often does not coincide with the last created block. Other blocks created in the same epoch but in previous slots may not have been finalized yet, leading to the possibility of forks due to multiple validators responsible for the same slot creating different blocks simultaneously.

GRANDPA Process:

The GRANDPA process allows validators to decide which of the blockchains created with BABE will be finalized. When a chain reaches 2/3 of the votes, it and all its not yet finalized blocks become part of the Relay Chain. For the protocol to function, it is essential that the number of validators is limited and predetermined. The finalization relies on the fundamental assumption that at least 2/3 of validators are honest. In this sense, this DLT can be classified as having a deterministic finalization process.

Governance Mechanisms:

After clarifying the essential elements of the Polkadot DLT, its governance can be studied. It is important to note that the algorithmic governance system is still in development, with the perspective of functioning fully automated using only Referendum, aiming to prevent any entity or coalition from controlling the network. Currently, the main governance tools of Polkadot are the Referendum, the Council, and the Technical Committee.

Referendum:

One of the most complex issues in DLTs is defining a governance system capable of managing updates or structural changes to the computer protocol. In Polkadot, any modification to the base protocol (Relay Chain) must be approved through a voting process (referendum) based on the stake weight of participants. In this fully public structure, anyone with a computer can participate by purchasing a certain number of tokens (DOT) generated by the DLT. Each referendum is associated with a specific proposal to change part of the Relay Chain code, and the possible responses to referendums are always binary: "yes," "no," or abstention. Referendums can be activated in different ways: through a public proposal, a proposal by the Council, or an "emergency" proposal by the Technical Committee, with pre-approval from the Council. There is a referendum every 30 days (except for emergency proposals, where exceptions can be made). The proposal to be discussed is alternately chosen from the Council's proposal list or the public proposal list (the one with the most support).

Each referendum has an implementation period, counted from the end of the referendum to the implementation of proposed changes (assuming the referendum proposal is approved). The time periods, in reference to the referendum, are divided into two types: the voting cycle and the proposal cycle. During each proposal cycle, anyone can propose a referendum by "locking" a certain amount of DOT tokens. If another network participant agrees with the deposited proposal, they can join by "locking" DOT tokens alongside

those locked by the proponent. At the end of the proposal cycle, referendums to be voted on are selected, choosing those with the most locked DOT tokens.

Any network user with DOT tokens can vote in a referendum by depositing them for a certain period. The weight of the vote is determined by the following mathematical formula: Vote weight = (number of locked DOT)*(number of months locked). This way, participants with fewer DOT tokens can influence the referendum vote more than those with more DOT tokens by locking their tokens for a longer period.

Council:

The Council, currently consisting of 13 members elected at regular intervals among DOT holders63, performs various governance functions. These include proposing referendums beneficial to the community, eliminating harmful or useless referendums, and electing the technical committee. Additionally, the Council has the authority to use funds from a treasury exclusively denominated in DOT, locked in the Relay Chain and not accessible at its discretion. The fund is fuelled in part by transaction fees and in part by "sanctions" resulting from illicit behavior. To propose a new referendum, the majority of the Council must be in favour. A Council member can exercise the right of veto only once if the referendum proposal is resubmitted.

Depending on the percentage of Council members in favour of the referendum proposal, different counting schemes can be activated. In particular, Council motions that pass with a 3/5 majority (60%)—without reaching unanimity—will transform into a public referendum with a simple majority counting scheme. If all Council members vote in favour of a motion to be transformed into a referendum, a counting scheme will be adopted where it is mathematically more difficult to reject the proposal.

Technical Committee:

The Technical Committee is composed of members elected by the Council. Its purpose is to discover technical issues within the system (including security issues) and propose emergency referendums. Any team that has successfully implemented at least a part of the Polkadot protocol can apply to be part of the committee. These teams can be added or removed from the committee with a majority vote from the Council. An emergency proposal to go to referendum needs approval from at least 3/4 of the Council and at least

[63] Any DOT holder node can run for Council membership, and the election is conducted in the same way as that of validators, i.e., it takes place on-chain, and users vote.

2/3 of the Committee. The referendum in this case is much faster, with practically no waiting time between the result and the start of the implementation of the change.

References

Accenture (2019). Governing DLT Networks. Distributed Ledger Technology Governance for Permissioned Networks.

Allen D. W. E., Berg C. (2020). Blockchain Governance: what we can learn from the Economics of Corporate governance. The JBBA, Volume 3, Issue 1.

Arrow K. J. (1974). The limits of the organization, W.W. Norton and Company NY - London.

Arrow K. J. (1986). Agency and the market. In: K. J. Arrow e M.D. Intrilligator (ed.), Handbook of Mathematical Economics, Volume 3, Chapter 23, pp. 1183-1195.

ASTRI (2016). Whitepaper on Distributed Ledger Technology. Hong Kong Applied Science and Technology Research Institute and Hong Kong Monetary Authority.

Bains P. (2022). Blockchain Consensus Mechanisms: A Primer for Supervisors. Fintech Notes, 3, International Monetary Fund.

Banca d'Italia (2022). Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività. Roma.

BCBS (2015). Guidelines - Corporate governance principles for banks.

BCBS (2022), Prudential treatement of cryptoasset exposures.

Borgogno O. (2022), Marking decentralized autonomous organizations (DAOs) fit for a legal life: mind the gap. Questioni di Economia e Finanza, 718, Banca d'Italia.

Brummer C. J., Seira R. (2022). Legal Wrappers and DAOs.
SSRN: https://ssrn.com/abstract=4123737 or http://dx.doi.org/10.2139/ssrn.4123737 .

Buterin V. (2017). Notes on Blockchain Governance. https://vitalik.ca .

Buterin V. (2021), Moving beyond coin voting governance, https://vitalik.ca .

Chen J., Micali S. (2019). Algorand: A secure and efficient distributed ledger. Theor. Comput. Sci., 777.

Ciampi M. *et al.* (2020). Updatable blockchain. Computer Security - ESORICS 2020, Lecture Notes in Computer Science, vol. 12309, Springer-Verlag, pp. 590-609.

CPMI – IOSCO (2022). Application of the Principles for Financial Market Infrastructures to stablecoins arrangements.

De Laat P. B. (2007). Governance of open source software: State of the Art. Journal of Management and Governance, 11(2), 165-177.

Deloitte (2021). Global Blockchain Survey.

EBA (2019). Orientamenti in materia di esternalizzazione.

EBA (2021). Guidelines on internal governance.

ECB (2021a). Eurosystem assessment methodology for electronic payment instruments, schemes and arrangements.

ECB (2021b). Response to the public consultation on the European oversight framework package for electronic payment instruments, schemes and arrangements.

ESMA (2021). Orientamenti in materia di esternalizzazione a fornitori di servizi cloud.

EU Commission (2020). DORA. Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014.

EU Commission (2022). Data Act. Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data. Brussels, 23.2.2022 COM(2022) 68 final 2022/0047 (COD).

EU Commission (2022). DLT Pilot regime. Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology (EU) 2022/858

EU Commission (2022), *MiCA*, Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937.

Ehrsam F. (2017). Blockchain Governance: Programming Our Future. Mimeo.

Farrar J.H., Hannigan B.M. (1998). Farrar's Company Law. Butterworth, London, fourth edition.

FMI (2023). Elements of Effective Policies for Crypto Assets. gennaio.

FSB (2022), Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets Consultative document, ottobre.

FSB (2023). The financial stability risks of decentralised finance. febbraio. Garrido, J., Liu, Y., Sommer,J, Viancha, S. (2022), Keeping Pace with Change: Fintech and the Evolution of Commercial Law, IMF Fintech Notes 2022/01.

Gola C. *et al.* (2024), Using switching circuits to classify and assess blockchains and crypto-assets. Risk Management Magazine, forthcoming.

Gola C., Caponera A. (2019). Policy issues on crypto-assets. LIUC Papers in Economics, Cattaneo University.

Gola C. *et al.* (2023). La governance delle blockchain e di sistemi basati sulla tecnologia dei registri distribuiti. Questioni di Economia e Finanza (Occasional Papers), 773, giugno, Banca d'Italia.

Gola C., Sedlmeir J. (2022). Addressing the Sustainability of Distributed Ledger Technology. Questioni di Economia e Finanza (Occasional Papers), n. 670, Banca d'Italia.

Grossi D. (2022). Social Choice Around the Block: On the Computational Social Choice of Blockchain. Cornell University.

Hart O. D. (1995), Firms, Contracts, and Financial Structure. Clarendon Press, Oxford.

Hassan S., De Filippi P. (2021). Decentralized Autonomous Organization. Internet Policy Review, Alexander von Humboldt Institute for Internet and Society, Berlin,10(2), 1-10.

Hofman D. *et al.* (2021). Blockchain Governance: De Facto (x)or Designed?. in Lemieux, V.L., Feng, C. (eds.), Building Decentralized Trust, Chapter 2.

IOSCO (2022). IOSCO Decentralized Finance Report. marzo.

ISO – Technical specifications (2022). Blockchain and Distributed Ledger Technologies. Guidelines for Governance, TS/23635, febbraio.

Javarone M. *et al.* (2022). Evolutionary Dynamics of Sustainable Blockchain. Royal Society Open Science, Proceedings.

Jensen M. J., Murphy K.J. (1990). Performance Pay and Top-Management Incentives. Journal of Political Economy, 98, 225-264.

Lamport L., Shostak R., Pease M. (1982). The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4(3), 382-401.

Lanfranchi C. (2019). Profili giuridici delle valute virtuali. Ciberspazio e Diritto. 20(62).

Liu Y. *et al.* (2022). Defining Blockchain Governance Principles: A Comprehensive Framework. University of New South Wales, Australia.

Markus L. M. (2007). The governance of free/open source software projects: monolithic, multidimensional, or configurational?. Journal of Manage Governance, 11, 151–163.

Maw N.G. Lord Lane of Horsell, Craig-Cooper M. (1994). Maw on Corporate governance. Dartmouth Publishing Company, Brookfield, Vermont, USA.

Micali S. (2019). Algorand's Core Technology (in a nutshell). April: https://medium.com/algorand/algorands-core-technology-in-a-nutshell-e2b824e03c77 .

Milgrom P., Roberts J. (1992). Economics, Organization and Management. Prentice Hall, Inc. New Jersey, USA.

Nakamoto S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. white paper.

Naudts E. *et al.* (2022). Governance in systems based on distributed ledger technology (DLT): A comparative study. AFM.

OCSE (2015). G20/OECD Principles of Corporate governance. OECD Publishing, Parigi.

OCSE (2017). Methodology for Assessing the Implementation of the G20/OECD Principles of

Corporate governance. OECD Report to the G20 Finance Ministers and Central Bank Governors, Parigi.

OCSE (2022). Why Decentralised Finance (DeFi) Matters and the Policy Implications. Parigi.

Santana C., Albareda L. (2022). Blockchain and the emergence of Decentralized Autonomous Organizations (DAOs): An integrative model and research agenda. Technological Forecasting & Social Change, 182, 121806.

Schär F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Federal Reserve Bank of St. Louis Review, 103(2), 153-74.

Schär F., Nadler M. (2022). Decentralized Finance, Centralized Ownership? An Iterative Mapping Process to Measure Protocol Token Distribution. Journal of Blockchain Research, 1, 29–36.

Schelling T. C. (1960). The strategy of conflict. Harvard University, Cambridge, Massachusetts, USA.

Sultanik E. *et al.* (2022). Are Blockchain Decentralized? Unintended Centralities in Distributed Ledgers. Trail of Bits.

The Law Society (2020). Blockchain: Legal & Regulatory Guidance. Tech London Advocates, Blockchain Legal and Regulatory.

UK Jurisdiction Taskforce (2019). Legal statement on crypto-assets and smart contracts. The LawTech Delivery Panel.

van Pelt R. *et al.* (2020). Defining Blockchain Governance: A Framework for Analysis and Comparison. Information Systems Management, 38(1), 21-41.

Wang S., *et al.* (2019). Decentralized Autonomous Organizations: Concept, Model, and Applications. IEEE Transactions on Computational Social Systems, 6(5).

Williamson O. (1999). The Mechanism of Governance. Oxford University Press.

Biographical note

Carlo Gola
He obtained his degree in Economics from Modena University and an M.Phil in Economics from the University of Oxford. After working as an economist at IRS (Institute for Social Research in Milan) for a few years, he joined the Bank of Italy as a senior economist. He then served as Deputy Representative of the Bank of Italy in London and later as Senior Advisor to the Italian Executive Director at the IMF. He has actively participated in several international work-streams, including FSB, EBA, ESRB, Joint Forum, and the EU Council during the Italian Presidency semester. He is the author of several articles and a book on the UK banking system.

Valentina Cappa
Graduated with honors in Law from the University of Florence in 2003. In 2009 she obtained an LLM (Master of Law) in International and EU Law from PennState University (USA). Admitted to the Italian Bar, she has worked as an in-house lawyer in Italy and Denmark. In 2016 she joined the Bank of Italy, in the Directorate General for Financial Supervision and Regulation, focusing on outsourcing, crypto-assets and operational risk.

Patrizio Fiorenza
Graduated in Bachelor's Mathematics and Specialist Statistics, he was successful/eligible in three public competitions, for all of which he was followed up on his recruitment. After working as an inspector for IVASS, he is currently employed at the Bank of Italy. His specialist skills include decentralized finance, non-life actuarial technology, statistics (in particular time series analysis), number theory, general mathematics.

Paolo Granata
Paolo Granata currently works in the Financial Supervision Directorate of the Bank of Italy. He is alternate member of the “crypo-assets workstream” of the BCBS and participates in several task forces and working groups focused on the crypto-assets market and the impacts of decentralized finance on supervised intermediaries. He is the author of a research paper on the governance of DLTs. Before joining the Bank of Italy, he worked for several years for an Italian banking group as a Senior Internal Auditor. He graduated with honors in International Relations at the University of Rome (“Roma Tre”).

Federica Laurino
She holds an MSc in Mathematics from the University of Salerno and a PhD in Mathematical Models and Methods in Engineering from Polytechnic University of Milan. With experience gained from a traineeship at the European Central Bank, she currently works in financial supervision at Bank of Italy, focusing on outsourcee and third-party supervision.

Lorenzo Lesina
Lorenzo Lesina currently works as an Expert in the Financial Supervision Directorate of the Bank of Italy. He participates in task forces and working groups focused on the crypto-assets market and decentralized finance. He is the author of two research papers on the governance of distributed ledgers published in the QF series by the Bank of Italy). Before joining the Bank of Italy, he worked in Mergers and Acquisitions sector. He graduated with honors in Corporate Finance from Luiss University.

Francesco Lorizzo
Graduated with honours in Electrical and Computer Engineering at Politecnico di Torino and University of Illinois, Chicago. He is currently an IT Enterprise Architect in Bank of Italy, involved in Artificial Intelligence and Distributed Ledger Technologies projects. Former manager at Deloitte, with expertise on IT governance, cybersecurity and risk management.

Gabriele Marcelli
Gabriele Marcelli is an IT architect with over 15 years of experience in the design and implementation of enterprise systems in the energy and financial sectors. At Banca d’Italia, after working as a project manager for several years, he now works on digital innovation in the financial sector, focusing on DLTs, Digital Currencies, CBDC and payment systems. He is co-author of several papers on these topics.

LIUC
Università Cattaneo