Defining Blockchain Governance Principles: A Comprehensive Framework

Yue Liu, Qinghua Lu, Guangsheng Yu, Hye-Young Paik, Liming Zhu
Data61, CSIRO, Australia
University of New South Wales, Australia
yue.liu@data61.csiro.au, qinghua.lu@data61.csiro.au
saber.yu@data61.csiro.au, h.paik@unsw.edu.au, liming.zhu@data61.csiro.au

June 3, 2022

Abstract

Blockchain eliminates the need for trusted third-party intermediaries in business by enabling decentralised architecture design in software applications. However, the vulnerabilities in on-chain autonomous decision-makings and cumbersome off-chain coordination lead to serious concerns about blockchain's ability to behave in a trustworthy and efficient way. Blockchain governance has received considerable attention to support the decision-making process during the use and evolution of blockchain. Nevertheless, the conventional governance frameworks do not apply to blockchain due to its distributed architecture and decentralised decision process. These inherent features lead to the absence of a clear source of authority in blockchain ecosystem. Currently, there is a lack of systematic guidance on the governance of blockchain. Therefore, in this paper, we present a comprehensive blockchain governance framework, which elucidates an integrated view of the degree of decentralisation, decision rights, incentives, accountability, ecosystem, and legal and ethical responsibilities. The above aspects are formulated as six high-level principles for blockchain governance. We demonstrate a qualitative analysis of the proposed framework, including case studies on five extant blockchain platforms, and comparison with existing blockchain governance frameworks. The results show that our proposed framework is feasible and applicable in a real-world context.

blockchain, governance, decision right, accountability, incentive, ecosystem

1 Introduction

Blockchain is the technology behind Bitcoin [1], which is a decentralised data store that maintains all historical transactions of Bitcoin network. The concepts of blockchain have been generalised to distributed ledger systems that ensure distributed trust without the need for third-party intermediaries in business transactions [2]. A large number of projects have been conducted to explore how to re-architect application system. In particular, after the advent of smart contracts (i.e., computer programs run on blockchain), blockchain is explored as a general, decentralised computing and storage environment in which to build new applications and business models [3].

Despite the broad use of blockchain, there are serious concerns about whether the decisions directing a blockchain are made in a trustworthy and efficient manner. A few infamous incidents occurred in two of the world-renowned blockchain platforms, Ethereum and Bitcoin, raise the level of concerns. In 2016, within Ethereum, vulnerable code in smart contracts responsible for operating a DAO (Decentralised Autonomous Organisation) project was exploited by malicious attackers, which led to massive economic loss. After much debate, Ethereum conducted a hard fork to reverse the transactions in the DAO attack, and recover the stolen tokens worth over 60 million dollars [4]. Bitcoin also suffered a split of the platform after a lengthy debate over the block size (from August 2015 to January 2016) [5]. These incidents highlight the need for governance mechanisms that would orchestrate a clear decision-making process within the context of a decentralised system with different stakeholders. For instance, blockchain platforms need to be

updated to fix software bugs without causing a hard fork, or different stakeholders need to be coordinated effectively and efficiently to come to a consensus while still respecting the principle of decentralised decision-making processes.

Blockchain governance refers to structures and processes which ensure that the development and use of blockchain are compliant with legal regulations and ethical responsibilities [6]. This topic has received great attention as it is considered essential to improve the trustworthiness and efficiency of blockchain. Nonetheless, existing IT/data governance frameworks and standards can hardly be applied to blockchain, as there is no explicit declaration of a central source of authority within blockchain. Recently, there are some works that discuss governance structures for blockchain platforms, either focusing on customised governance methods in permissioned blockchain [7, 8], or investigating regulations about financial sectors [9, 10]. Some studies also propose governance frameworks for blockchain [8, 11, 12]. However, existing blockchain governance frameworks mainly discuss scattered governance mechanisms lacking stakeholders and process related linkages, which provide limited guidance to relevant stakeholders and the broader community who are interested in this topic.

Therefore, in this paper, we present a comprehensive blockchain governance framework that provides an integrated view of decentralisation level, decision rights, incentives, accountability, ecosystem, legal compliance and ethical responsibilities. The major contributions of this paper are as follows:

- We propose a blockchain governance framework that categorises the governance structures according to the decentralisation level of governed blockchains. The framework extensively covers the existing governance structures.

- The framework provides a systematic mapping of blockchain stakeholders and their respective decision rights, accountability, and incentives. This mapping can help inform stakeholders and the broader public about the authority, capability, and responsibility in blockchain governance.

- The framework extends governance to the blockchain ecosystem, which is comprised of four layers: data, platform, application, and community. We identify a set of governance mechanisms and associate each of them with the respective stage of each layer's lifecycle.

- The framework emphasises legal compliance and ethical responsibilities in blockchain governance. Using practical examples, we analyse the integration of existing regulations with the framework, and discuss the ethical responsibilities in blockchain governance.

We perform case studies on five well-known blockchain platforms: Bitcoin, Ethereum, Dash, Tezos, and Hyperledger Fabric. We apply our framework to these platforms to analyse how they implement governance, and examine whether our principles are considered in a real-world context. We distinguish similarities and differences across these platforms and identify current gaps. The results show that our framework is feasible and applicable. In addition, we compare the proposed framework with nine existing blockchain governance frameworks.

The remainder of this paper is organised as follows. The next section provides a literature review. Section 3 explains our research methodology. Section 4 presents our blockchain governance framework. Section 5 demonstrates the qualitative analysis of our proposed framework. Section 6 concludes the paper and outlines future work.

2 Related Work

We reviewed existing governance frameworks and standards, including IT governance [13, 14], data governance [15, 16], open-source software (OSS) governance [17, 18], platform ecosystem governance [19], and corporate governance [20]. IT governance focuses on how to align information technology with organisational goals in enterprises [13]. Data governance narrows down the subject of governance to data, specifically, how organisations evaluate, direct, and monitor the use of data [16]. OSS governance analyses how a group of volunteers contribute to the peer production of software [18]. Platform ecosystem governance provides platform-agnostic guidance on how decisions are made about a platform regarding environmental dynamics [19]. Corporate governance highlights code of conduct to retain the trust of clients [20].

We found that the decentralisation nature of blockchain differentiates its governance from existing governance frameworks with the absence of a clear source of authority. For instance, in both IT governance and corporate governance, there is a clear governance structure describing the allocation of responsibility, capability, and authority within an organisation. Policies and strategies are always decided by top executives, which embodies the centralisation of power. Further, governance is realised for the benefit of this particular organisation. Data, open-source software (OSS), and platform ecosystem governance have a similar situation in that they all involve multiple organisations, and there is a trusted entity acting as the agent between all relevant organisations.
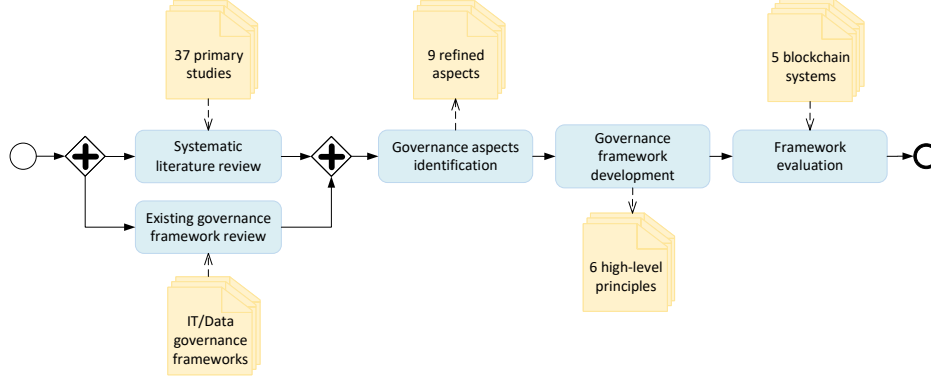
Figure 1: Overview of the research process.

Compared to the above frameworks, blockchain itself has intrinsic characteristics, such as consensus, incentives, transparency, and immutability, which could potentially create a situation where they conflict with human values (e.g. privacy, security), necessitating a trade-off analysis when implementing governance. In general, the decentralised environment gives more power to the community and highlights the notion of democracy. All on-chain transactions are under the algorithmic governance predefined by the blockchain project team, while other stakeholders can shift the direction of a blockchain via voting. Since there are no trusted third parties to coordinate the business relationships, the governance process may involve complex coordination among differential stakeholders. Consequently, reaching consensus from diverse intentions is considered the key point of blockchain governance. Besides, the codebase of blockchain is relatively static due to the immutable data structure design. Based on the above factors, any revision to the blockchain platform code or on-chain historical data will lead to a voting process for proposal acceptance and hard fork to update the on-chain protocol. Accordingly, the concepts of self-governance [21] and adaptive governance [22] are consistent with blockchain governance to satisfy the needs of decentralisation and inherent democracy spirit, and desires for risk management.

Further, there are nine studies that proposed governance frameworks for blockchain. Katina et al. [23] propose seven interrelated elements (philosophy, theory, axiology, methodology, axiomatic, method and applications) for further exploration of this topic. Allen and Berg [24] provide a descriptive framework to understand the exogenous and endogenous governance in blockchain. John and Pam [25] and Pelt et al. [11] both study the on-chain and off-chain development processes to realise governance. Beck et al. [8] formulate a blockchain governance framework that is centred on the three dimensions of decision rights, accountability, and incentives adopted from IT governance. Howell et al. [26] focus on the membership and transacting relationships. Werner et al. [27] develop a taxonomy of platform governance for blockchain. Hofman et al. [12] propose a high-level analytic framework, regarding six aspects (i.e. why, who, when, what, where, how) in the governance of blockchain. Tan et al. [28] analyse this research topic from the perspective of social sciences.

Nevertheless, existing frameworks do not present an extensive view of blockchain governance. Consequently, they can only provide limited guidance to the community with scattered governance mechanisms. In this paper, we propose a comprehensive blockchain governance framework, which formulates nine core governance aspects into six high-level principles, to support a better governance process for the overall blockchain ecosystem.

3 Methodology

This section introduces the methodology of this study. As shown in Fig. 1, this study is conducted through mainly five steps. First, a systematic literature review (SLR) was performed following Kitchenham's guidelines [29] to understand state-of-the-art of blockchain governance. Secondly, we also reviewed extant governance frameworks and standards, to analyse the characteristics of blockchain governance. Afterwards, we identified six high-level governance principles, and proposed a new blockchain governance framework. Finally, we performed a qualitative analysis to confirm the feasibility and applicability of our proposed framework.

The SLR consists of four main steps: • keyword search, • selection based on predefined criteria, • backward and forward snowballing, and • data extraction and synthesis. We collected the literature from five reference databases: ACM Digital Library, IEEEXplore, ScienceDirect, SpringerLink, and Google Scholar. 1061 papers were retrieved, while after the removal of duplicates, and title/abstract screening, there were 75 papers in the initial selection set.

We then conducted a full-text screening, and scoped down to 27 papers as the tentative selection. Subsequently, the snowballing process identified 10 more papers, and the final selection set had 37 papers for data extraction, analysis, and synthesis. Table 1 illustrates our inclusion/exclusion criteria. The primary studies were analysed with six research questions (i.e. what, why, where, when, who, and how), which cover core aspects of blockchain governance [6]. The major findings of this SLR are as follows:

- Governance is applied for blockchain to address software qualities and human values such as adaptability, upgradability, security, and fairness. The ultimate goal of preserving these attributes is the prosperity of blockchain in various application scenarios by improving the trustworthiness of a blockchain platform.

- Blockchain governance can be split up into on-chain and off-chain regarding where governance methods are enforced. Specifically, on-chain governance aims at the operations and decisions for a blockchain platform itself and the stored data, while off-chain governance emphasises collaborations of the blockchain community in the real world.

- The community consists of different stakeholders who join a blockchain platform and hold the rights for governance issues. Major stakeholders include the project team, node operators, users, application providers, and regulators.

- Governance methods can be categorised into process mechanisms and product mechanisms. The former type supports blockchain development by determining meta-rules for governance, whilst the latter ones are coded as features and functionalities of blockchain to regulate the behaviour of stakeholders.

Table 1: Selection of Primary Studies in SLR.

Inclusion criteria	A paper that proposes a solution for the governance of blockchain.
	A paper that proposes principles or frameworks for developing governance of blockchain.
Exclusion criteria	Papers that focus on "governance through blockchain" instead of "governance of blockchain".
	Older version of a study that has a more comprehensive version.
	Papers that are not written in English.
	Papers that are not accessible.
	Survey, review and SLR papers. We do not conduct data extraction or synthesis from these studies as they are considered the related work of this literature review.

We reviewed extant governance frameworks and specifications, as discussed in Section 2. We included the literature of IT governance, data governance, and platform ecosystem governance adhering to a previous work of data governance for platform ecosystem process management [30], whilst OSS governance [5, 11] was selected based on the primary studies in our SLR. For corporate governance, VISA was selected as it is often compared to blockchain platforms regarding financial issues.

We identified nine core aspects of blockchain governance from the literature review, including decentralisation level, incentive, decision rights, accountability, stakeholder, ecosystem, lifecycle, legal compliance, and ethical responsibility. The identified aspects are then formulated into a blockchain governance framework, consisting of six high-level principles, as follows.

- Principle 1 elucidates different decentralisation levels of blockchains, which is extracted from the research question *"What is blockchain governance?"* in our SLR. The decentralisation level determines both the underlying infrastructure and governance structure of a blockchain.

- Principles 2-4 explore the mapping of incentive, decision rights, accountability and divergent stakeholders. The former three governance dimensions are extracted from the research question *"What is blockchain governance?"*, while blockchain stakeholders are identified in *"Who is involved in blockchain governance"*).

- Principle 5 extends governance to the overall blockchain ecosystem with elaborate governance mechanisms and their expected effects. This principle integrates four research questions from the SLR: *"Where is blockchain governance enforced?" "When is blockchain governance applied?" "How is blockchain governance designed?" "Why is blockchain governance adopted?"*

- Principle 6 is extracted from the research question *"Why is blockchain governance adopted?"* Legal and ethical responsibilities represent the essential guidelines for human behaviours in the blockchain ecosystem.

4

We demonstrate a qualitative analysis of the proposed framework. We apply the framework to five blockchain platforms as case studies, to confirm its feasibility and applicability. The selected blockchain platforms are Bitcoin, Ethereum, Dash, Tezos and Hyperledger Fabric. Bitcoin and Ethereum are included regarding their market values and active users, while Dash and Tezos blockchain are chosen because they have representative novel governance structures. Specifically, Dash introduces the concept of "masternodes", and Tezos enables smooth on-chain protocol replacement instead of hard fork. Hyperledger Fabric is a representative case of permissioned public blockchains. Data collection was performed on the official websites and documents of these five blockchains. We analysed the collected data using our framework design, to scrutinise the implementation of governance in different blockchain platforms. Afterwards, we compare nine existing blockchain governance frameworks with our framework, which are retrieved from our previous SLR [6] and continuing literature review. We use identified governance aspects as the comparison factors.

4 Blockchain Governance Framework

In this section, we present a framework to provide guidance for all relevant stakeholders, to support a better governance process, especially for practitioners as the discussion involves technical aspects of blockchain-based architectures and applications. The overview of our blockchain governance framework is illustrated in Fig. 2, which consists of six principles.

4.1 Principle 1: Consider the level of decentralisation

Blockchain platforms can be classified into three types to meet different requirements. Different types of blockchain may have a divergent focus on certain attributes, e.g., performance, flexibility. These types also reflect the different levels of decentralisation, and affect the governance structure regarding allocation of decision rights, accountability, and incentives. The essential classification criteria include permission of joining a blockchain, and the extent to which users are allowed to participate in the operation of a blockchain. They both lead to differences among three blockchain types, such as cost efficiency, performance, flexibility, etc. Hereby, "operation" denotes services a blockchain provides (e.g. generating and reading transactions), and contributions to the use of blockchain (e.g. the capability of installing a full node).

Permissioned private blockchain. Permissioned private blockchains have the lowest level of decentralisation among the three types. The access and operation of a permissioned private blockchain are both restricted to certain entities. This type of blockchain platform has an explicit single source of authority, and is deployed within an institute/organisation. Hence, there is a clear hierarchy structure between stakeholders in blockchain, which should align with the off-chain corporate structure. All involved individuals are identifiable and have fixed user privileges. Compared to the other two types, governance of permissioned private blockchains is more flexible and requires less effort to orchestrate decisions from different stakeholders, as every choice directing the blockchain is made by entities on the top of interior hierarchy.

Permissioned public blockchain. Permissioned public blockchains only require approval for participation, while operation-related rights are open to the participants. The applicable business context of this type of blockchain is usually a consortium of several organisations maintaining a cooperative relationship. Identity verification in permissioned public blockchains is similar to permissioned private ones. The governance structure is comprised of the hybrid of multiple authorities, each of which may make decisions for its own organisational benefits. Consequently, governance in this type of blockchain usually focuses on the coordination of involved authorities for collective goals.

Permissionless public blockchain. In permissionless public blockchains, the entries and operations are both open to entities, as there are no preset privileged stakeholders. Such openness, however, may result in higher complexity of governance in terms of two main aspects: 1) Since each individual is recognised via on-chain pseudonymous addresses without real-world identification, stakeholders may be unwilling to bear the responsibility of making decisions; 2) Stakeholders may need to go through a cumbersome negotiation process to reach an agreement, as everyone focuses more on personal interests, which may cause conflicts in decision-making processes. Consequently, permissionless public blockchains usually improve the governance participation rate by incentives, and exploit consensus mechanisms for decision finalisation.

4.2 Principle 2: Provide stakeholders aligning incentives to achieve consensus

The second principle is to be addressed to a wide range of blockchain stakeholders. There are collective areas aligning diverse stakeholder objectives, giving incentives wide applicability. In blockchain governance, incentives are generalised to factors that may influence stakeholders' behaviours. The governance structure needs to provide incentive mechanisms to drive desirable behaviours (e.g., participation in governance), and resolve conflicts between stakeholders (e.g., finalising a decision), which usually end up with the finding of a Schelling point. In permissionless public blockchains,
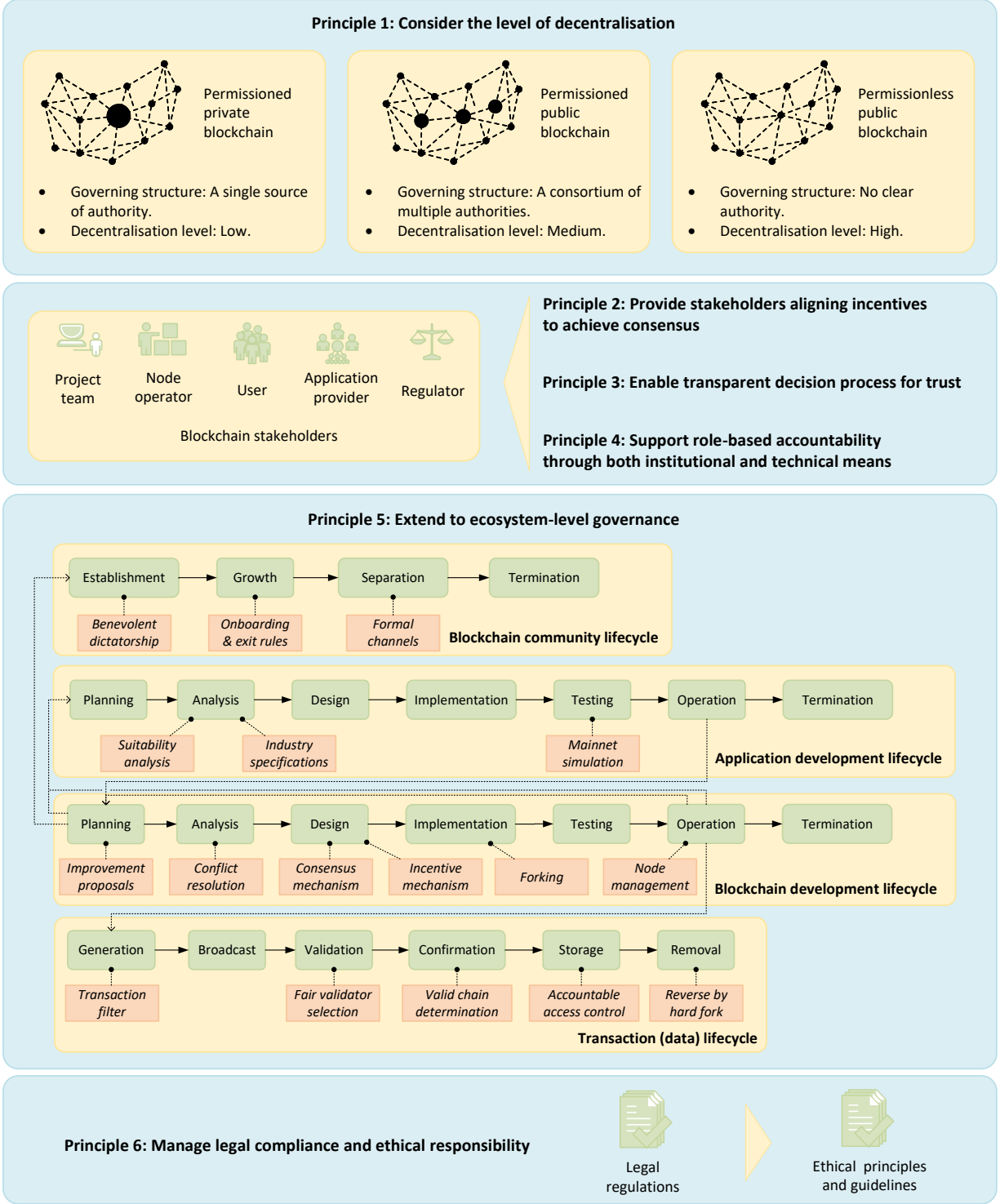
Figure 2: Blockchain governance framework.

incentive mechanisms may incorporate game theory to align different directions of blockchain governance. In this case, incentives are mostly rewarded on-chain, hence, can be traced by any other stakeholder. Meanwhile, incentives may be distributed off-chain according to institutional rules preset by the top executives in permissioned private blockchains, or based on commercial agreements among the multiple authorities in permissioned public blockchains.

Table 2: Distribution of 3 governance dimensions over blockchain stakeholders for Principles 2-4.

Stakeholders	Decision rights	Accountability	Incentives
Project team	Platform development: Blockchain infrastructure setting; Consensus mechanism; Incentive mechanism; Project management: Conflict resolution rules; Formal communication channel; Onboarding & exit rules; Risk management.	Institutional means: Real-world identity verification; Traceable code contributors; Standardised documentation; Technical means: Address-based on-chain identity; Ledger-enabled operation logs.	Increase of market values; Block rewards; Transaction fees; Service fees.
Node operator	Replica storage; Block validation; Improvement proposal voting; Forking (instance installation).	Technical means: Address-based on-chain identity; Ledger-enabled operation logs; Institutional means: Real-world identity verification.	Block rewards; Transaction fees.
User	Transaction submission; Improvement proposal voting.	Technical means: Address-based on-chain identity; Ledger-enabled operation logs; Institutional means: Real-world identity verification.	Achievement of personal goals: Personal investment; On-chain trading; Data storage.
Application provider	Blockchain adoption; Improvement proposal voting. Onboarding & exit rules.	Institutional means: Real-world identity verification; Commercial agreement.	Increase of market values; Service fees.
Regulator	Risk assessment & measurement: Regulatory policy; Audit trail.	Institutional means: Legal regulation; Real-world identity verification; Technical means: Address-based on-chain identity; Ledger-enabled operation logs.	Taxes and fees.

We conclude the incentives of different stakeholders in Table 2. In general, monetary incentives are straightforward to reward stakeholders in governance-related issues. The project team and application providers can benefit from the increase of market values (e.g., increase of cryptocurrency price), and service fees. Node operators receive block rewards and transaction fees according to predefined incentive mechanisms for their contributions to blockchain operation, while the project team may also obtain a certain proportion as compensation. Incentives of blockchain users mainly come from their intentions to use blockchain and applications, including personal investment, on-chain trading, and data storage. Finally, regulators collect taxes and charge for regulation services (e.g., audit).

4.3 Principle 3: Enable transparent decision process for trust

The decentralisation nature of blockchain drives the need for collective decisions on governance issues. Decision-makings rely on the authorities, responsibilities, and capabilities of relevant stakeholders. Notice that a stakeholder's role may change throughout the lifecycle of a blockchain, which implies the transition of decision rights. We summarised the decision rights of blockchain stakeholders in Table 2.

The project team of a blockchain mainly comprises developers and the foundation, for technical and monetary support respectively. Most governance-related decisions for a blockchain platform are made by developers. Specifically, developers' decisions determine a series of on-chain and off-chain meta-rules for both blockchain platforms and communities. On-chain decisions include the setting of blockchain infrastructure (e.g., block size and interval), and design of consensus and incentive mechanisms, which can regulate the behaviours of other stakeholders when using blockchain. Off-chain decisions refer to the implementation of code, establishment of conflict resolution rules, formal communication channel, and onboarding and exit rules for the whole community. In addition, blockchain governance should consider risks such as software bugs in coding, cyber attacks in operation, breach of commercial contracts,

etc. Risk management in blockchain is achieved by platform update and evolution, which the involves approval of improvement proposals, and implementation of new features, also known as forking.

Node operators hold either local full nodes to maintain all historical ledger contents, or light nodes with compressed information like block header. Meanwhile, an operator can become block validators, or special node operators who are granted rights to make improvement proposals for more contributions. As nodes are the fundamental elements to construct a blockchain, operators are the key roles to finalise forking by choosing and installing blockchain instances of a specific version.

Users interact with blockchain services via submitting transactions to achieve personal goals. When encountering an abnormal function/service, a user can report to the project team for improvements, while other users can then join the voting of proposed solutions.

Application providers have the right to choose which blockchain platform to be adopted in their existing workflow regarding business targets. They can contact the project team to exchange domain knowledge and requirements for blockchain adaptation, which may be raised in the form of an improvement proposal. Further, an application may have its own setting for onboarding and exit rules, which should be decided by providers.

Regulators mainly refer to governments and third-party auditors, who are responsible for ensuring the compliance of laws and ethics. The assessment and mitigation of corresponding risks rely on the enactment of regulatory policies and audit trails in blockchain ecosystem.

Ensuring the transparency of decision-making processes is critical in blockchain governance for stakeholders to oversee whether decisions are reasonable, accordingly, to gain trust from the whole community. When decisions are made on-chain, blockchain itself can record individuals' choices and the eventual outcome. This can usually be found in permissionless blockchains, where decision rights are allocated to different stakeholders for fairness and democracy in a highly decentralised environment. Off-chain decision-makings should be conducted in formal channels which are open to relevant stakeholders. Note that the clear source of authority may integrate multiple roles and corresponding decision rights into certain individuals in a permissioned context where significant decisions are usually made by blockchain deployers.

4.4   Principle 4: Establish role-based accountability through both institutional and technical means

Accountability in blockchain governance refers to the identifiability and answerability of stakeholders for their decisions. Accountability should be enforced in an explicit way to manifest the allocation of stakeholders' responsibilities and capabilities. Failure on this governance dimension may result in the abuse of power and eventually, the collapse of the entire blockchain system due to the risk of centralisation.

Accountability for blockchain governance can be established via both institutional and technical manners. Institutional accountability is applicable to conventional governance structures in a blockchain, which requires standardised documentation to report the off-chain accountability process. Technical implementation of accountability is embedded in the distributed ledger, providing evidence for on-chain accountability by recording both data and operations. In comparison with off-chain accountability, the on-chain process is still less mature and relies on how developers design the blockchain platform to reduce risks and uncertainties.

Accountability is also dependent on the decentralisation level of a blockchain. In permissioned blockchains, it is compulsory to conduct identity verification for entities to join the blockchain. Hence, it does not cost much effort to recognise accountable individuals for certain events or operations. By contrast, participants identify themselves via pseudonymous accounts in permissionless blockchains, which may increase the uncertainties of finding responsible entities and hence, hinder the accountability process.

As shown in Table 2, the accountability process of the project team, application provider, and regulator relies more on institutional means, while technical means are more important for node operator and user as they are usually identified via on-chain addresses. In general, institutional means of accountability enables an effective and efficient decision-making process where the source of authority is clear. Relevant stakeholders should be considerate when making governance decisions, otherwise, they could be criticised and punished immediately for their neglect of duty, which may further affect real-world business or individual reputation. For different stakeholders, institutional means may vary. For instance, the accountability of the project team relates to institutional means regarding the visibility and accessibility of source code development to monitor contributors. While for application providers, institutional means are dependent on their organisational code of conduct. However, technical means of accountability do not ensure such a rigorous decision-making process as the cost of violation may be low. A malicious node operator may attempt to forge and broadcast invalid blocks to the network. This can be traced by on-chain ledger logs to impose a fitting penalty such

as blacklisting the blockchain account. Nevertheless, the accountable entity can make more attacks over and over again via other blockchain accounts.

4.5 Principle 5: Support ecosystem-level governance

The governance of blockchain does not locate in merely the platform itself, but needs to support a broader environment of the overall ecosystem. Platform is the base of blockchain ecosystem, which includes underlying on-chain data, the superstructure of blockchain-based application systems, and the whole community comprising of different stakeholders. We illustrate the main phases in the lifecycle of each layer in Fig. 2.

Platform layer. Platform is both the base and target of governance structure for blockchain ecosystem. All governance-related design and tactics will eventually take effect in this layer. We adopt the software development process [31] to describe different phases of this layer.

During the initial planning and analysis stages of a blockchain platform, business context is taken into consideration to determine the blockchain type. Later in the design phase, the blockchain architecture with all on-chain self-governance features is constructed (e.g., consensus and incentive mechanisms), along with the distribution of stakeholders' decision rights, accountability, and incentives. When developing the platform, management of source code should be decided (e.g., open or closed source), while the testing environment needs to be separated from the mainnet to avoid influencing the actual business process. When a blockchain platform is officially in use, all on-chain issues need to adhere to established mechanisms of previous phases. Note that the management of nodes is specified in Principles 2-4 from the perspective of node operators.

If a blockchain platform needs updates or adjustments within a risk management process, the governance structure in permissioned blockchains can make quick responses such as forking or protocol replacement. In the case of permissionless blockchains, an improvement proposal is created, which starts a new epoch of development process from the planning phase. Such upgrades and evolutions require a series of formalised development procedures. An improvement proposal should be analysed by eligible stakeholders, with proper conflict resolution measures, usually voting, for its acceptance or rejection. The accepted ones are then codified and integrated into source code, and released as new versions via forking. This iteration of blockchain upgrades embodies an adaptive governance process to manage and mitigate risks in blockchain operation. Finally, blockchain platforms may be terminated for certain reasons. At this point, blockchain governance focuses on coordination among stakeholders about the transfer or redistribution of on-chain assets and resources, which requires explicit descriptions and explanations of decisions to guide the whole process.

Additionally, blockchain governance structures should define inter-system interoperation policies between different platforms regarding the decentralisation level. This will reflect in the data flow, integration of business process, and even adjustment of decision rights process. For instance, if two permissionless blockchain platforms have interoperations, the extent of visible and shared distributed ledger contents, transition of transaction format, and compatibility of on-chain programmability (i.e. smart contracts) should all be scrutinised.

Data layer. In blockchain, data governance is carried out along with the transaction lifecycle. When designing a blockchain platform, on-chain data governance is covered in the design phase, for instance, a standardised format to ensure transaction quality, access policies for security and privacy, and sharding technique for scalability. During the operation of a blockchain platform, transactions are generated and broadcast when users send data to blockchain. Insofar, a filter is utilised to automatically discard transactions that do not meet the unified requirements (e.g., transaction format, data contents). Transactions are then kept in nodes' local memory pool waiting for validation. After being validated and confirmed, data is then officially stored in blockchain. Hereby, confirmation can resolve conflicts that there may be several blocks generated at the same time, which requires subsequent blocks to confirm the workload of validation. The longest chain is viewed as the valid one. Note that pending transactions may be outdated and then automatically removed from the pool.

The emphasis on data governance during blockchain operation is placed on accountable access control of transactions. Capabilities of writing/reading data to/from blockchain, as well as validating transactions, are assigned to specific stakeholders considering the deployed blockchain type. For instance, in permissioned blockchains, validators are often appointed by authorities, while novel consensus mechanisms are designed and implemented to impartially elect the validator each round in permissionless blockchains. Changes of data states are logged by blockchain transactions, which enables an on-chain accountability process regarding all decentralisation levels. However, reading transparent data usually leaves no trace to blockchain history as no transaction is sent, which may hinder the identification of individuals. All on-chain operations should respect the rights of data subjects that illegal data need to be removed from blockchain by conducting a hard fork and reversing historical transactions. Finally, when a blockchain is terminated, all on-chain data will be destroyed under predefined guidance.

Application layer. Blockchain governance also covers the utilisation of blockchain as a component in software application systems. A blockchain-based application may have a close connection to the blockchain platform itself and consequently, its development process almost synchronises with the blockchain development process. This situation is usually found in blockchain-based decentralised finance (DeFi). Another situation is that when a blockchain platform is in operation, further investment is made to build up DApps over the platform. Application providers need to conduct suitability analysis regarding domain knowledge, and check whether adopting blockchain is compliant with industry standards and regulations during initial procedures. Afterwards, implementation and testing rely on the APIs and testnet provided by the blockchain project team. When operating the application, changes to industry regulations and specifications may generate new requirements. which in turn leads to upgrades of the underlying blockchain platform. Finally, an application may fail, and then needs to remove its data from blockchain and transfer resources based on the instructions of the project team or previous contractual agreements.

Community layer. The start of blockchain platform development indicates the establishment of corresponding off-chain community. In the early stages, the project team is considered the benevolent dictator as there are few other stakeholders. The project team can persuade them about certain decisions with its expertise. When a blockchain platform is officially in use, the community becomes larger with the participation of differential stakeholders, who will join the consequent decision-making processes. Along with the maturity of a blockchain platform, the off-chain community is gradually specialised and then divided into different groups regarding their roles and decision rights [32].

In particular, the project team and application providers may exist in the form of a company respectively. Accordingly, the internal governance of these organisations can refer to existing specifications. Another significant facet is the training of blockchain practitioners, which informs the capability development and growth in the future workforce. Ensuring they have adequate expertise, for the design and implementation of blockchain platforms and applications to avoid flaws, can gain more trust from other stakeholders. Further, blockchain governance highlights off-chain collaboration among different stakeholders. In permissioned blockchains, there is a systematic process to communicate in the constitutional hierarchy. By contrast, permissionless blockchains maintain explicit off-chain governance within the community, which implies the need for formal communication channels (e.g., maillist, online forum) to transparentise significant decision-makings (e.g., improvement proposal). Finally, termination of community is along with the collapse of blockchain platforms, where proper coordination of stakeholders is needed to rearrange off-chain resources and assets.

4.6 Principle 6: Manage legal compliance and ethical responsibility

The final principle ensures that all governance-related decisions and processes conform to existing legal regulations and ethical responsibilities. Law is usually considered to set the minimum standards of human behaviours. Ensuring legal compliance depends on where blockchain platforms and applications are launched and deployed, and how regulators (e.g. governmental institutions) enact policies to safeguard the blockchain development process and shape the whole ecosystem against risks and uncertainties. Examples include the regulation and standards in Australia in terms of digital identity, data provenance, and taxation [33]. The European Commission proposed new law on crypto-assets and plan blockchain regulatory sandbox [34]. In addition to blockchain-specific laws, other general regulations should also be considered, for instance, the General Data Protection Regulation (GDPR) specifies the "Right to Be Forgotten" [35] to protect personally identifiable information when managing on-chain data. Another issue is the review of data contents before a transaction is officially included in a block, to ensure data quality and avoid malicious information on-chain, such as child pornography. If such information is already stored on blockchain, a hard fork is required to reverse the transaction history.

Ethical responsibilities denote the maximum standards of human behaviours. Promote and encourage ethical principles and guidelines in blockchain governance can help uphold and protect human values, and the whole ecosystem will be more responsible and trustworthy. For instance, blockchain technology is usually criticised for energy-intensive platforms and applications, especially the ones applying the Proof of Work (PoW) consensus mechanism. Consequently, how to reduce energy consumption and benefit the environment is regarded as a significant governance topic. Other than environmental well-being, ethical responsibilities also involve consideration of human values from the perspective of software engineering, such as privacy, transparency, integrity, etc [36]. Embedding ethical responsibilities in blockchain governance is hard to guarantee, and requires the awareness of practitioners over such values and overall community culture.

5 Qualitative Analysis

In this section, we present a qualitative analysis of the proposed framework via case studies on extant blockchain platforms, and comparison with existing blockchain governance frameworks.

Governance principle		Bitcoin	Ethereum	Dash	Tezos	Hyperledger Fabric
Principle 1: Consider the level of decentralisation		Permissionless public	Permissionless public	Permissionless public	Permissionless public	Permissioned public
Principle 2: Provide stakeholders aligning incentives to achieve consensus	Project team	Contribution credits	Contribution compensations	Mining rewards	N/A	Deployment and maintenance fees
	Node operator	Mining rewards, banned account	Mining rewards	Mining rewards, Quorum system	Mining rewards, bonds	Business revenues
	User	Investment in Bitcoin token	Investment in Ether token	Investment in Dash token	Investment in Tezos token	Business revenues
	Application provider	N/A	N/A	N/A	N/A	Business revenues
	Regulator	Taxes	Audit fees	Taxes	N/A	Audit fees
Principle 3: Enable transparent decision process for trust	Project team	Blockchain platform, off-chain community	Blockchain platform, off-chain community	Blockchain platform, off-chain community	Blockchain platform, off-chain community	Blockchain platform, consultation with application providers
	Node operator	Blockchain replica, block validation	Blockchain replica, block validation	Blockchain replica, block validation, masternode	Blockchain replica, block validation	Blockchain replica, block validation
	User	On-chain service interaction	On-chain service interaction	On-chain service interaction	On-chain service interaction	On-chain service interaction
	Application provider	N/A	N/A	N/A	N/A	Blockchain adoption and deployment
	Regulator	Regulated financial system	Audit	Regulated financial system	DApp regulation	Audit
Principle 4: Establish role-based accountability through both institutional and technical means	Institutional means	Github commit history, institution structure	Github commit history, institution structure	Github commit history, institution structure	Github commit history, institution structure	Github commit history, sign-off statement, institution structure, identity verification
	Technical means	On-chain operation logs	On-chain operation logs	On-chain operation logs, Proof of Service	On-chain operation logs	On-chain operation logs
Principle 5: Support ecosystem-level governance	Data layer	Format check, multi-signature, CoinJoin, non-persistent memory, Merkle tree, Bloom filter	Format check, encryption, Merkle tree, Proof of Access, sharding, transaction reversal	Format check, transaction set	Format check, zero-knowledge proof	Endorsement policy, versioning check, private data collection
	Platform layer	Proof of Work, Bitcoin Improvement Proposal, hard fork	Proof of Work, Proof of State, Ethereum Improvement Proposal, carbonvote, hard fork, social contract	Proof of Work, governance message, Dash Improvement Proposal, masternode network	Proof of Stake, self-amendment	Pluggable consensus protocol, endorsement policy, code security scans, regular contributors meeting
	Application layer	Development tutorial, APIs, testnet	Development tutorial, APIs, testnet, regulatory mechanisms	Development tutorial, APIs, testnet	Development tutorial, APIs, testnet, DApp regulation	Development tutorial, APIs, testnet, multiple signatures, automated check, endorsement policy
	Community layer	Formal communication channel, benevolent dictator	Formal communication channel, benevolent dictator	Formal communication channel	Formal communication channel, benevolent dictator	Formal communication channel, Hyperledger Foundation Charter, code of conduct
Principle 6: Manage legal compliance and ethical responsibility	Legal compliance	Tax liability, restricted areas	Known scams	Banking Secrecy Act, Anti-Money Laundering, Know Your Customer regulations, known scams	DApp regulation	Data-sharing regulations, industry-specific regulations, intellectual property, commercial agreements, local and international law
	Ethical responsibility	Transparency, data privacy and integrity	Transparency, data privacy and integrity, environmental wellbeing	Transparency, data privacy and integrity	Transparency, data privacy and integrity	Data privacy and integrity, trust

Figure 3: Case study results. The framework is feasible as all principles are considered in real-world context, and applicable to different blockchain platforms.

5.1 Case Study

The purpose of case studies is to understand whether and how blockchain governance is implemented in a real-world context, while also confirming that our proposed framework is feasible and applicable. Specifically, feasibility refers to whether the principles in our framework solve blockchain governance problems, and applicability implies that the framework can be applied to different blockchain platforms to analyse their governance structures.

We selected five blockchain platforms for case studies: Bitcoin, Ethereum, Dash, Tezos, and Hyperledger Fabric. Bitcoin and Ethereum are the two most famous blockchain platforms around the globe, Dash and Tezos are included as they are representative of novel governance structures, whilst Hyperledger Fabric is selected as it provides a permissioned blockchain platform for a wide range of industry applications. We collected and analysed their implementation of governance from open official websites and documents (e.g., white paper, yellow paper). The rest of this section illustrates the results of case studies, which are summarised in Fig. 3.

Analysis of Principle 1. For the first principle, Bitcoin, Ethereum, Dash and Tezos are all permissionless public blockchains, and have a close connection to the DeFi field. In their white papers, the project team is the primary governing role to make decisions, whilst other stakeholders are also involved in governance issues, especially node operators. Hyperledger Fabric offers permissioned public blockchain solutions in enterprise contexts. Its project team only provides technical support to the underlying blockchain technology, while organisations that deploy Hyperledger Fabric instances are the authorities for governance-related decision-makings.

Analysis of Principle 2. In terms of providing incentives, the four permissionless platforms mainly discuss the investment income of users, and rewards to both node operators for their contributions to participate in the consensus mechanism, and the project team as funds for future development. However, there is a narrow discussion about

application providers' incentives from the perspective of governance. The following gives a detailed distribution of incentives in these blockchains.

In Bitcoin, software release notes of its official client, Bitcoin Core, record all contributors [37]. Transaction fees and mining rewards (i.e. new bitcoin tokens) are given to the corresponding validator (aka. miner) [1]. Node operators may be banned for a particular time period (by default 24 hours) if they send false information, as a waste of bandwidth and computing resources [38]. In Ethereum, a certain proportion of the total amount sold, which is about 60 million ethers, is distributed to compensate early contributors. Ethereum applies a similar incentive mechanism as Bitcoin: transaction fees and new ether tokens are both rewarded to validators [39]. In Dash, mining rewards are divided into three pieces: validators and masternodes get 45% respectively, while the remaining 10% is to fund improvement proposals [40]. Moreover, Dash implements a Quorum system in which a node will be deactivated after six violations [41]. In Tezos blockchain, both block validators and endorsers (who confirm a block via signature) are incentivised by mining rewards along with a bond. Validators can receive the bond after a security cycle (i.e. one year). The bond will be forfeited if violations in their blocks are found (e.g. double signing). Inactive Tezos addresses are not allowed to validate blocks or vote for improvement proposals until they are reactivated [42]. In addition, Bitcoin and Dash both mention taxes for regulators [43, 44], while Ethereum pays for audit services [45].

On the contrary, Hyperledger Fabric does not have a native cryptocurrency distribution, consequently, incentives in this blockchain platform refer to conventional business revenues. The project team are paid by application providers when IBM Cloud is utilised to deploy and maintain blockchain instances [46], and the team will pay for audit services [47]. Application providers, node operators and users of a Hyperledger Fabric instance belong to different organisations. These organisations establish business connections where blockchain is adopted. Hence, incentives of these stakeholders are based on institutional governance within a single organisation, or business agreements between multiple organisations.

Analysis of Principle 3. The analysis of decision rights is dominantly about the project team, node operators, users and regulators. First, the project team is in charge of the design, development, and management of both the blockchain platform and off-chain community. In particular, the Hyperledger fabric project team provides consultation of blockchain services to their clients (i.e., application providers) [48]. Secondly, node operators hold blockchain replicas locally, and block validators are responsible for the validation and confirmation of blocks. Dash introduces the concept of "masternodes", who provide services to ensure the availability of the Dash blockchain [41]. They are able to vote on governance and funding proposals. Thirdly, users submit transactions to use on-chains services. They can also participate in governance decision-makings. For instance, Ethereum users have cast votes for forking [49]. Finally, Bitcoin and Dash acknowledge that governments are making efforts to integrate blockchain platforms into formal and regulated financial systems [43, 44]. Ethereum and Hyperledger Fabric select third-party authorities to perform audits [45, 47]. Tezos mentions regulators for DApps [50]. All the above descriptions of decision rights and decision-making processes can be found on official websites and documents to gain the trust of existing and possible stakeholders. However, limited information is provided about how application providers are involved in governance decisions, except for Hyperledger Fabric. In Hyperledger Fabric, application providers are significant for deciding whether to adopt blockchain technology, and also maintaining an off-chain community. Especially, they need to consider the actual business problems, overall ecosystem, business and governance model, and also legal issues before deployment [51].

Analysis of Principle 4. All selected blockchain platforms utilise both institutional and technical means for the accountability process. Institutional means include commit history in Github to locate the exact contributor on a specific update, and internal governance within the project team, as they all provide the respective institution structure on official websites. Technical means mainly rely on blockchain addresses of participants, and operation logs in the transaction information. Particularly, Dash develops a Proof of Service scoring system to recognise the contributions of masternodes [52]. Nevertheless, in the four permissionless public blockchains, it is still hard to identify on-chain participants for real-world accountability. Further investigation is required to analyse trade-offs between accountability and privacy. While in Hyperledger Fabric, transacting entities are not anonymous, all involved organisations and their employees are identified by a Certificate Authority associated with each organisation [53].

Analysis of Principle 5. The results of Principle 5 are analysed regarding the four different layers as follows.

Data layer: When submitting transactions, all blockchain platforms filter transactions that any included field violating the standard format or required software version will result in errors, and neither be accepted, broadcast, nor validated. Bitcoin allows multi-signature feature that a transaction is sent with the approval of a set of users [54]. Further, it also enables "CoinJoin" which aggregates the operations of several users into a single transaction [38]. Ethereum specifies oracle services of sending data to blockchain [55].

After generation, transactions are kept in a pending pool for validation. Bitcoin states that Bitcoin Core clients keep pending transactions in non-persistent memory [38]. If a node is shut down, the memory pool will be lost. While in Dash, masternodes are randomly selected to relay the inputs, outputs and signatures of transaction sets [41]. A

transaction set collects multiple transactions of the same user, but the selected masternode does not know the exact on-chain identity. In a Hyperledger Fabric instance, a transaction needs to be endorsed by appointed nodes before the ordering service node packages transactions into blocks [53].

After validation, full node operators take the responsibility of storing the whole transaction history, while light nodes provide auxiliary transaction verification services by recording only block headers. Bitcoin implements Merkle tree and Bloom filter to test the membership of elements [38], which can achieve data compression in light nodes. Ethereum also splits desired data into blocks with encryption techniques, and then builds up a Merkle tree [39]. Arweave's Proof of Access is applied to test whether a node maintains both the most recent and randomly past block [55]. Tezos utilises indexers to achieve a quick fetch of blockchain data [56]. In addition, the current upgrade of Ethereum will create new chains as shards for data storage and improve transaction throughput [57]. Tezos is investigating zero-knowledge proof to ensure data privacy [58]. Hyperledger Fabric allows users to send private data, where original contents are transferred during the endorsement process, and the respective hash values are stored in blocks [53]. When data is stored in blocks, the accessibility is set via on-chain smart contracts. Nevertheless, the removal of on-chain data is not explicitly covered, except that Ethereum mentioned a hard fork was conducted to solve the DAO attack, which reversed transactions within a specific time period [59].

Platform layer: The critical difference of governance in planning, analysis and design phases is embodied in the choice of consensus mechanisms. Currently, Bitcoin, Ethereum and Dash all implement Proof of Work, while Tezos deploys Proof of Stake (PoS). However, Ethereum is undergoing an upgrade from PoW to PoS. Tezos validators need to hold a minimum of 8000 XTZ tokens [60] while Ethereum's future PoS requires 32 ETH tokens [57]. Although the validator selection in Dash relies on PoW, becoming a masternode has a PoS-style demand for holding at least 1000 Dash tokens [52]. Hyperledger Fabric supports pluggable consensus protocols which can be customised according to application providers' requirements [53]. Raft is recommended by the Hyperledger Fabric project team where a "leader and follower" scheme is implemented. Note that block validators (aka. ordering service nodes) in Fabric instances are assigned by authorities instead of competed as in permissionless blockchains. In terms of platform implementation, Github is commonly leveraged to manage source code in these platforms, which can provide commit history to assist the off-chain accountability process.

Upgrading blockchain platforms require a complete process of submitting improvement proposal, analysis and conflict resolution via voting, and implementation of code. Ethereum adopts "Carbonvote", which means stakeholders' votes are calculated according to their owned ether tokens [49]. In Dash, specific on-chain governance messages contain the proposals and corresponding votes. The acceptance of a proposal needs the approval of at least 10% of the masternode network [61]. Improvements in Tezos are grouped into five periods: proposal, exploration vote, cooldown, promotion vote, and adoption, each phase lasts for about 14 days [62]. When releasing updated code, accepted proposals are implemented via a hard fork in Bitcoin and Ethereum as they are less flexible, while the other two permissionless platforms have smoother transitions between different versions. Dash integrates updated code into the current platform but does not immediately active new features, until more than 80% of participants update their clients [61]. Tezos's on-chain protocol has two parameters for version control, which can conveniently enable accepted proposals [42]. Upgrades in Hyperledger Fabric need to contemplate both each deployed instance and the overall platform. If an application provider intends to change the settings of a Fabric instance, it needs to generate a new configuration file, which requires signatures from other organisations in the same instance [53]. For upgrading the overall Hyperledger Fabric platform, regular issues such as bug fixes and documentation improvements are accomplished via the normal GitHub pull request workflow, while major upgrades require consensus from the broader community [63]. As Hyperledger Fabric does not implement an inherent token distribution or universal blockchain instance, such decisions are finalised via off-chain approaches. For instance, contributors meetings are held to plan and review release progress, and discuss future directions [53].

Regarding the termination of blockchain, Ethereum proposes the concept of "social contract", in which entities with a certain quantity of ethers can develop a candidate version of Ethereum [39]. The Hyperledger Foundation specifies a project's lifecycle, which includes "deprecated" and "end of life" [64]. Project maintainers should cast vote(s) on the deprecation proposal, and the Hyperledger Technical Steering Committee determines whether to stop supporting a project.

Application layer: The intrinsic DeFi background fertilises cryptocurrency-related applications with different client software and exchanges in permissionless public blockchains. In addition, diverse DApps are built up based on all selected platforms. They all provide tutorials and APIs for DApp development to practitioners. Testnet can be deployed to run new functionalities, avoiding negative influences on real-world business processes. In particular, Ethereum notes that it does not attempt to limit its use in particular fields, while regulatory mechanisms should be designed to prevent harm [39]. Hyperledger Fabric enables a smart-contract level endorsement policy, which specifies nodes from certain organisations need to validate transactions related to particular smart contracts [53].

Community layer: There are no specific onboarding or exit rules for permissionless blockchains, anyone can join or leave at any moment. The separation of community is based on stakeholders' different expertise and spotlights on the blockchain platform or applications. Every platform provides formal communication channels, such as online blogs, discussion forums (e.g., Stack Overflow) and social media, and also offline workshops and meetings. Regarding Hyperledger Fabric instances, each organisation has its own structure for governance and management of employees. In the Hyperledger project team, there are clear instructions on how to participate and contribute to the project [53] and code of conduct [65]. In addition, we also note that Bitcoin, Ethereum, and Tezos all have their own *benevolent dictator(s)* who have dominant decision rights on governance issues. In Bitcoin, Satoshi Nakamoto was regarded as the benevolent dictator of the Bitcoin ecosystem before his/her retirement [66], while the co-founder of Ethereum, Vitalik Buterin, is still active in governance-related issues in the Ethereum ecosystem[1]. In Tezos, the foundation has a veto power for the first 12 months as a security measure [42].

Analysis of Principle 6. Legal compliance and ethical responsibilities are heavily reliant upon the culture where a blockchain platform is deployed. Bitcoin mentions tax liability [43] for individual incomes, and also lists that Bitcoin is now prohibited or restricted in certain areas [67]. Ethereum discusses common scams to prevent serious risks [68]. Dash provides detailed clues about the conformation of Banking Secrecy Act, Anti-Money Laundering, and Know Your Customer regulations, and lists known scams, fake wallets and Ponzi or pyramid schemes on the platform [44]. Tezos specifies that a DApp "CoinHouse" is under the highest legal standards in French law [50]. Hyperledger Fabric suggests that application providers should contemplate legal issues, including data-sharing regulations, industry-specific regulations, intellectual property, commercial agreements, and local and international law, before adopting blockchain in their business models [51]. Specifically, Pal [69] and Smith [70] both discussed GDPR and Hyperledger Fabric. In addition, the Linux Foundation behind Hyperledger Fabric specifies that their Antitrust Policy complies with all applicable state and federal antitrust and trade regulation laws [71].

Ethical responsibilities found in these blockchain platforms mainly refer to transparency, data privacy, and integrity. Transparency and data integrity are achieved by the decentralisation level of permissionless public blockchains. On the other hand, data privacy is preserved by access control policies over the data layer. Note that Ethereum now is undergoing a vital upgrade which includes the replacement of Proof of Work with Proof of Stake, this change will enormously reduce the energy consumption and improve the sustainability of Ethereum [57]. In addition, Hyperledger Fabric highlights the need for trust as all involving stakeholders are identified.

Summary. The case studies show that our proposed framework is applicable in real-world blockchain governance. All six high-level principles can be found in the five blockchain platforms. In addition, the case studies also reveal the similarities and differences across selected platforms, as well as some findings to improve their governance as follows.

First, the major difference between these blockchains is how to distribute incentives and deployed consensus protocols. PoW and PoS are commonly applied, as they can choose validators who are regarded as having more contributions (either computation power or holding tokens), and hence should be granted more decision rights. The choice of consensus mechanisms is also dependent on the decentralisation level. For instance, Proof of Authority is suitable for the low decentralisation level while Proof of Elapsed Time can achieve a random selection of validators and build a highly decentralised environment. In addition, as permissionless public blockchains provide universal blockchain instances, their project teams are significant when arranging consensus and incentives. Consequently, the deviation of incentives reflects how the project team value the contribution of stakeholders in permissionless blockchains. In the selected four cases, their incentive mechanisms all involve a game theory to attract block validators, and preserve the fund for future development. From the perspective of DeFi, it is also leveraged to mint new tokens into the market. Incentives in permissioned public blockchains may rely on conventional business models, as they are usually adopted in various application scenarios where there is no inherent token distribution. In the case of Hyperledger Fabric, the project team is more like a service provider. All stakeholders are closely connected by business agreements.

Secondly, regarding the three governance dimensions (i.e., incentive, decision rights, and accountability), there is a lack of discussion on how application providers make governance-related decisions, and what incentives drive their behaviours in the four permissionless public blockchains. A possible reason is that these platforms intend to promote the development of decentralized autonomous applications and organisations where human interference is minimised to achieve on-chain autonomy. On the contrary, the significance of application providers is highlighted in permissioned blockchains, as they are the ones to decide whether to deploy a blockchain instance. In addition, there are different settings for node operators. For example, Dash specifies "masternodes" as the on-chain committee dealing with governance issues like voting on improvement proposals. This may facilitate the future design of more special roles with certain rights to finalise governance decisions (e.g., transaction visibility). While in a permissioned public blockchain instance, on-chain roles are usually matched to corresponding off-chain positions. Further, different from mandatory identity verification in permissioned public blockchains like Hyperledger Fabric, permissionless public blockchains

---

[1]Vitalik Buterin's website: `https://vitalik.ca/index.html`

have an inherent weakness for on-chain accountability that individuals are hard to identify, which implies the low cost of violations. This requires investigation of digital identity, for instance, self-sovereign identity is a blockchain-based application, which may in turn help on-chain identification.

Thirdly, all lifecycle phases of each ecosystem layer are covered except for the termination phase in several selected cases. This may indicate the project teams' confidence that they can survive in the competitive market to some extent. We suggest a full development process, which considers the termination phase, can help enable a complete governance-driven architecture design. For example, data handling and transaction management require proper on-chain data removal mechanisms that respect data subjects' rights and comply with related regulations like GDPR.

The third remark further leads to our final finding that although blockchain-related legal compliance and ethical responsibilities are still under investigation, these platforms do provide related discussions and analysis. Future studies can be conducted to raise general awareness, and further integrate it with current blockchain governance methods. For instance, filters can be applied to examine data contents instead of merely transaction format, to prevent malicious information from being fed to blockchain.

Through the case studies, it is observed that the proposed framework can satisfy feasibility and applicability. For feasibility, we confirmed that the six principles in our framework are addressed and considered in a real-world context. In terms of applicability, we demonstrated how the proposed framework is applied to different blockchain platforms to scrutinise their governance structures. The results helped identify current gaps and limitations based on selected platforms.

Hereby, we summarise several research directions to guide practitioners in the implementation of blockchain governance. Future study is required to translate the high-level principles into actionable mechanisms and patterns, explore the effects of architectural decisions on governance, and analyse corresponding trade-offs from the perspective of software engineering. For instance, design patterns can be extracted from extant blockchain platforms by scrutinising reusable governance solutions.

Table 3: Comparison results of existing frameworks for blockchain governance.

Governance aspects	Katina et al. [23]	Allen and Berg [24]	John and Pam [25]	Pelt et al. [11]	Beck et al. [8]	Howell et al. [26]	Werner et al. [27]	Hofman et al. [12]	Tan et al. [28]	Our framework
Decentralisation level	×	○	×	●	●	●	●	●	●	●
Stakeholders	○	●	○	●	●	●	●	●	●	●
Incentives	×	○	○	●	●	○	●	●	○	●
Decision rights	○	○	×	●	●	●	●	●	○	●
Accountability	○	×	○	●	●	○	○	●	●	●
Ecosystem	○	○	○	○	○	○	○	○	○	●
Lifecycle	○	○	○	○	○	○	×	○	○	●
Legal regulations	○	●	○	○	○	●	×	●	●	●
Ethical responsibilities	×	×	○	×	×	×	×	○	○	●

● Covered　　○ Partially Covered　　× Not Covered

5.2 Comparison

We compared our proposed framework with existing governance frameworks for blockchain platforms. We used the identified governance aspects as comparison factors to evaluate different concerns of compared frameworks. "Sufficiency" is used to examine whether the aspects are considered in the frameworks. A result is determined as "not covered" (×), "partially covered" (○), or "covered" (●). The comparison results are illustrated in Table 3.

First, most compared frameworks involve consideration of decentralisation levels when either designing their frameworks or conducting evaluations as our framework. Nevertheless, [24] limits its investigation to permissionless public blockchains, while [23] and [25] do not explicitly mention specific blockchain types. Existing frameworks highlight that the decentralisation levels are significant for governance structures, we further discuss how this aspect affects the

following governance aspects in our work. For instance, we explain how incentives, decision rights, and accountability may be various in different blockchain types.

Secondly, existing frameworks are marked as "covered" for stakeholders in blockchain governance, if at least two types of stakeholders are considered. Most existing frameworks place emphasis on the project team, node operator, and user, while analysis of application provider and regulator is limited. Notably, [24] covers the same stakeholders as our framework. [8, 11, 28] adopt decision rights, accountability and incentives from IT governance. In particular, [8] and [11] define multiple research questions regarding the three governance dimensions for further theoretical work. Compared to them, our framework illustrates a comprehensive mapping between five groups of stakeholders to the three governance dimensions of incentives, decision rights, and accountability. This mapping can help the broader community comprehend the authority, capability, and responsibility of different stakeholders for blockchain governance.

Further, most compared frameworks are marked as "partially covered" for both ecosystem and lifecycle aspects. For the blockchain ecosystem, existing frameworks discuss the separation of on-chain and off-chain governance [11, 24], or focus on either side. In this paper, our framework provides a more extensive blockchain ecosystem with four refined layers (i.e., data, platform, application, and community), and discusses how governance can be implemented in each layer. Regarding when to implement blockchain governance, existing frameworks roughly divide the phases into exogenous and endogenous governance [24, 26]. In the proposed framework, the governance process is elaborated in terms of each identified ecosystem layer. In particular, we adopt the software development lifecycle to describe the governance process of platform and application layers. Our framework specifies multiple constructive governance mechanisms regarding different lifecycle phases.

Finally, extant frameworks lack concrete instances of legal conformation. In our framework, *Principle 6* is provided as a high-level guidance with discussion and multiple examples of both legal compliance and broader ethical responsibility.

It is observed in the comparison that there are significant gaps between compared frameworks and our proposed framework. This highlights the need for our framework again.

6 Conclusion

In this paper, we proposed six blockchain governance principles, and built a comprehensive framework to support better governance processes in blockchain and blockchain-based applications. The governance framework considers the level of decentralisation in different blockchain types, allocation of incentives, decision rights and accountability of stakeholders. Further, the proposed framework extends governance to the blockchain ecosystem, and highlights both legal compliance and ethical responsibilities in blockchain governance. We elucidated how governance is implemented for five blockchain platforms through case studies, identifying current gaps and limitations. Their open websites and documents confirm the feasibility and applicability of our proposed framework. Blockchain governance is an arduous and ongoing topic, and there is a continuing need of providing considered guidelines for the design and implementation of blockchain and applications. In the future, we plan to propose a design pattern catalogue, and explore architectural decisions for blockchain governance.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoinsv.io/bitcoin, 2008, accessed 30-January-2022.

[2] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, p. 464, 2016.

[3] A. Bratanova *et al.*, "Blockchain 2030: A look at the future of blockchain in Australia," Data61, CSIRO, Brisbane, Australia, Tech. Rep., Apr. 2019. [Online]. Available: https://www.researchgate.net/publication/332298704_Blockchain_2030_A_Look_at_the_Future_of_Blockchain_in_Australia

[4] N. Atzei, M. Bartoletti, and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts (SoK)," in *Principles of Security and Trust*, M. Maffei and M. Ryan, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017, pp. 164–186.

[5] P. De Filippi and B. Loveluck, "The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure," *Internet Policy Review*, vol. 5, no. 4, 2016.

[6] Y. Liu, Q. Lu, L. Zhu, H.-Y. Paik, and M. Staples, "A systematic literature review on blockchain governance," *arXiv preprint arXiv:2105.05460*, 2021.

[7] Z. Bao, K. Wang, and W. Zhang, "An auditable and secure model for permissioned blockchain," in *Proceedings of the 2019 International Electronics Communication Conference*, ser. IECC '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 139–145. [Online]. Available: https://doi.org/10.1145/3343147.3343170

[8] R. Beck, C. Müller-Bloch, and J. L. King, "Governance in the blockchain economy: A framework and research agenda," *Journal of the Association for Information Systems*, vol. 19, no. 10, p. 1, 2018.

[9] H. Nabilou, "Bitcoin governance as a decentralized financial market infrastructure," *Available at SSRN*, 2020. [Online]. Available: https://ssrn.com/abstract=3555042

[10] P. Paech, "The governance of blockchain financial networks," *The Modern Law Review*, vol. 80, no. 6, pp. 1073–1110, 2017.

[11] R. van Pelt, S. Jansen, D. Baars, and S. Overbeek, "Defining blockchain governance: A framework for analysis and comparison," *Information Systems Management*, vol. 38, no. 1, pp. 21–41, 2021.

[12] D. Hofman, Q. DuPont, A. Walch, and I. Beschastnikh, "Blockchain governance: De facto (x) or designed?" in *Building Decentralized Trust*. Springer, 2021, pp. 21–33.

[13] P. Weill and J. W. Ross, "IT governance on one page," *Available at SSRN 664612*, 2004. [Online]. Available: https://ssrn.com/abstract=664612

[14] S. Cobit, "A business framework for the governance and management of enterprise IT," *Rolling Meadows*, 2012.

[15] C. Ballard, J. Baldwin, A. Baryudin, G. Brunell, C. Giardina, M. Haber, E. A. O'neill, S. Shah *et al.*, *IBM information governance solutions*. IBM Redbooks, 2014.

[16] "Information technology – governance of IT – governance of data – part 1: Application of ISO/IEC 38500 to the governance of data," International Organization for Standardization, Standard ISO/IEC 38505-1:2017, 2017. [Online]. Available: https://www.iso.org/standard/56639.html

[17] S. O'mahony and F. Ferraro, "The emergence of governance in an open source community," *Academy of Management Journal*, vol. 50, no. 5, pp. 1079–1106, 2007.

[18] P. B. De Laat, "Governance of open source software: state of the art," *Journal of Management & Governance*, vol. 11, no. 2, pp. 165–177, 2007.

[19] A. Tiwana, B. Konsynski, and A. Bush, "Platform evolution: coevolution of platform architecture, governance, and environmental dynamics (research commentary)," *Information Systems Research*, vol. 21, no. 4, pp. 675–687, 2010.

[20] V. Inc., "Corporate governance guidelines," https://investor.visa.com/corporate-governance/, 2020, accessed 10-July-2021.

[21] E. Ostrom, *Understanding institutional diversity*. Princeton university press, 2009.

[22] P. Olsson, L. H. Gunderson, S. R. Carpenter, P. Ryan, L. Lebel, C. Folke, and C. S. Holling, "Shooting the rapids: navigating transitions to adaptive governance of social-ecological systems," *Ecology and society*, vol. 11, no. 1, 2006.

[23] P. F. Katina, C. B. Keating, J. A. Sisti, and A. V. Gheorghe, "Blockchain governance," *International Journal of Critical Infrastructures*, vol. 15, no. 2, pp. 121–135, 2019.

[24] D. W. Allen and C. Berg, "Blockchain governance: What we can learn from the economics of corporate governance," *The Journal of the British Blockchain Association*, 2020.

[25] John, Thomas and Pam, Mantri, "Complex adaptive blockchain governance," *MATEC Web Conf.*, vol. 223, p. 01010, 2018. [Online]. Available: https://doi.org/10.1051/matecconf/201822301010

[26] B. E. Howell, P. H. Potgieter, and B. M. Sadowski, "Governance of Blockchain and Distributed Ledger Technology Projects," International Telecommunications Society (ITS), 2nd Europe – Middle East – North African Regional ITS Conference, Aswan 2019: Leveraging Technologies For Growth 201737, 2019. [Online]. Available: https://ideas.repec.org/p/zbw/itsm19/201737.html

[27] J. Werner, S. Frost, and R. Zarnekow, "Towards a taxonomy for governance mechanisms of blockchain-based platforms," *Proceedings of the 28th European Conference on Information Systems (ECIS), An Online AIS Conference*, June 2020. [Online]. Available: https://aisel.aisnet.org/ecis2020_rp/26

[28] E. Tan, S. Mahula, and J. Crompvoets, "Blockchain governance in the public sector: A conceptual framework for public management," *Government Information Quarterly*, p. 101625, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0740624X21000617

[29] B. A. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Tech. Rep., 2007.

[30] S. U. Lee, L. Zhu, and R. Jeffery, "A data governance framework for platform ecosystem process management," in *Business Process Management Forum*, M. Weske, M. Montali, I. Weber, and J. vom Brocke, Eds. Cham: Springer International Publishing, 2018, pp. 211–227.

[31] "Systems and software engineering – Software life cycle processes," International Organization for Standardization, Standard ISO/IEC/IEEE 12207:2017, 2017. [Online]. Available: https://www.iso.org/standard/63712.html

[32] O. E. Williamson, *Economic organization: firms, markets and policy control*. New York University Press New York, 1986.

[33] E. R. Australian Government Department of Industry, Science. National blockchain roadmap: Regulation and standards. https://www.industry.gov.au/data-and-publications/national-blockchain-roadmap/regulation-and-standards. Accessed 30-January-2022.

[34] E. Commission, "Legal and regulatory framework for blockchain," https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain, accessed 30-January-2022.

[35] P. Voigt and A. Von dem Bussche, "The EU general data protection regulation (GDPR)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, p. 3152676, 2017.

[36] W. Hussain, H. Perera, J. Whittle, A. Nurwidyantoro, R. Hoda, R. A. Shams, and G. Oliver, "Human values in software engineering: Contrasting case studies of practice," *IEEE Transactions on Software Engineering*, pp. 1–1, 2020.

[37] BitcoinCore, "Bitcoincore - about," https://bitcoincore.org/en/about/, accessed 30-January-2022.

[38] Bitcoin, "Developer guides," https://developer.bitcoin.org/devguide/, accessed 30-January-2022.

[39] Ethereum, "Ethereum whitepaper," https://ethereum.org/en/whitepaper/, accessed 30-January-2022.

[40] Dash Core, "Dash core developer documentation," https://dashcore.readme.io/docs, accessed 30-January-2022.

[41] Dash, "Dash whitepaper," https://github.com/dashpay/dash/wiki/Whitepaper, accessed 30-January-2022.

[42] Tezos, "Tezos whitepaper," https://wiki.tezosagora.org/whitepaper, accessed 30-January-2022.

[43] Bitcoin, "Frequently asked questions," https://bitcoin.org/en/faq, accessed 30-January-2022.

[44] Dash, "Dash legal," https://docs.dash.org/en/0.12.3/legal.html/, accessed 30-January-2022.

[45] H. Jameson, "Progpow audit: Goals & expectations," https://medium.com/ethereum-cat-herders/progpow-audit-goals-expectations-75bb902a1f01, accessed 30-January-2022.

[46] IBM Cloud, "IBM blockchain platform: Pricing," https://www.ibm.com/cloud/blockchain-platform/pricing, accessed 30-January-2022.

[47] Hyperledger Fabric, "Hyperledger Fabric audits," https://wiki.hyperledger.org/display/fabric/Audits, 2021, accessed 30-January-2022.

[48] IBM Cloud, "IBM blockchain services and consulting," https://www.ibm.com/blockchain/services, accessed 30-January-2022.

[49] Ethereum, "Introduction to Ethereum governance," https://ethereum.org/en/governance/, accessed 30-January-2022.

[50] Tezos, "Tezos corporate baking," https://wiki.tezosagora.org/learn/uses-of-tezos/corporate-baking, accessed 30-January-2022.

[51] A. Banda, M. Hamilton, E. Lowry, and J. Widdifield, "The founder's handbook: An introduction to building a blockchain solution," https://www.ibm.com/downloads/cas/GZPPMWM5, 2020, accessed 30-January-2022.

[52] Dash, "Dash platform developer documentation," https://dashplatform.readme.io/, accessed 30-January-2022.

[53] Hyperledger Fabric, "A blockchain platform for the enterprise," https://hyperledger-fabric.readthedocs.io/en/latest/index.html, 2020, accessed 30-January-2022.

[54] Bitcoin, "Bitcoin for businesses," https://bitcoin.org/en/bitcoin-for-businesses, accessed 30-January-2022.

[55] Ethereum, "Ethereum development documentation," https://ethereum.org/en/developers/docs/, accessed 30-January-2022.

[56] Tezos, "Blockchain indexers," https://wiki.tezosagora.org/build/blockchain-indexers, accessed 30-January-2022.

[57] Ethereum, "Upgrading Ethereum to radical new heights," https://ethereum.org/en/upgrades/, accessed 30-January-2022.

[58] Tezos, "Tezos privacy," https://wiki.tezosagora.org/learn/futuredevelopments/privacy, accessed 30-January-2022.

[59] Ethereum, "The history of Ethereum," https://ethereum.org/en/history/, accessed 30-January-2022.

[60] Tezos, "Tezos baking," https://wiki.tezosagora.org/learn/baking, accessed 30-January-2022.

[61] Dash, "Dash features," https://docs.dash.org/en/stable/introduction/features.html, accessed 30-January-2022.

[62] Tezos, "Tezos governance," https://wiki.tezosagora.org/learn/governance, accessed 30-January-2022.

[63] D. E. M. B. W. Kostas Christidis, Christopher Ferris, "Hyperledger Fabric RFCs process," https://github.com/hyperledger/fabric-rfcs/blob/main/README.md, 2020, accessed 30-January-2022.

[64] Hyperledger Foundation, "Project lifecycle," https://tsc.hyperledger.org/project-lifecycle.html, accessed 30-January-2022.

[65] The Linux Foundation, "Hyperledger foundation charter," https://www.hyperledger.org/about/charter, 2021, accessed 30-January-2022.

[66] Bitcoin WiKi, "Satoshi Nakamoto," https://en.bitcoin.it/wiki/Satoshi_Nakamoto, accessed 30-January-2022.

[67] Wikipedia, "Legality of cryptocurrency by country or territory," https://en.wikipedia.org/wiki/Legality_of_cryptocurrency_by_country_or_territory, accessed 30-January-2022.

[68] Ethereum, "Ethereum security and scam prevention," https://ethereum.org/en/security/, 2022, accessed 30-January-2022.

[69] G. Pal, "The GDPR blockchain blind-spot: Regulating data and everything else," https://www.ibm.com/blogs/blockchain/2018/06/the-gdpr-blockchain-blind-spot-regulating-data-and-everything-else/, 2018, accessed 30-January-2022.

[70] S. S. Smith, "Blockchain, the GDPR and what accounting professionals need to know," https://www.ibm.com/blogs/blockchain/2018/05/blockchain-the-gdpr-and-what-accounting-professionals-need-to-know/, 2018, accessed 30-January-2022.

[71] The Linux Foundation, "Antitrust policy," https://www.linuxfoundation.org/antitrust-policy/, 2007, accessed 30-January-2022.