SoK: Blockchain Governance

Aggelos Kiayias
University of Edinburgh, Input Output
Edinburgh, United Kingdom
aggelos.kiayias@ed.ac.uk

Philip Lazos
Input Output
London, United Kingdom
philip.lazos@iohk.io

ABSTRACT

Blockchain systems come with a promise of decentralization that, more often than not, stumble on a roadblock when key decisions about modifying the software codebase need to be made. In a setting where “code is law,” modifying the code can be a controversial process, frustrating to system stakeholders, and, most crucially, highly disruptive for the underlying systems. This is attested by the fact that both of the two major cryptocurrencies, Bitcoin and Ethereum, have undergone “hard forks” that resulted in the creation of alternative systems which divided engineering teams, computational resources, and duplicated digital assets creating confusion for the wider community and opportunities for fraudulent activities. The above events, and numerous other similar ones, underscore the importance of Blockchain governance, namely the set of processes that blockchain platforms utilize in order to perform decision-making and converge to a widely accepted direction for the system to evolve. While a rich topic of study in other areas, including social choice theory and electronic voting for public office elections, governance of blockchain platforms is lacking a well established set of methods and practices that are adopted industry wide. Instead, different systems adopt approaches of a variable level of sophistication and degree of integration within the platform and its functionality. This makes the topic of blockchain governance a fertile domain for a thorough systematization that we undertake in this work.

Our methodology starts by distilling a comprehensive array of properties for sound governance systems drawn from academic sources as well as grey literature of election systems and blockchain white papers. These are divided into seven categories, suffrage, Pareto efficiency, confidentiality, verifiability, accountability, sustainability and liveness that capture the whole spectrum of desiderata of governance systems. We interpret these properties in the context of blockchain platforms and proceed to classify ten blockchain systems whose governance processes are sufficiently well documented in system white papers, or it can be inferred by publicly available information and software. While all the identified properties are satisfied, even partially, by at least one system, we observe that there exists no system that satisfies most properties. Our work lays out a common foundation for assessing governance processes in blockchain systems and while it highlights shortcomings and deficiencies in currently deployed systems, it can also be a catalyst for improving these processes to the highest possible standard with appropriate trade-offs, something direly needed for blockchain platforms to operate effectively in the long term.

ACM Reference Format:
Aggelos Kiayias and Philip Lazos. 2022. SoK: Blockchain Governance. In 4th ACM Conference on Advances in Financial Technologies (AFT ’22), September 19–21, 2022, Cambridge, MA, USA. ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3558535.3559794

1 INTRODUCTION

Following the founding of Bitcoin [57] in 2009, cryptocurrencies and other blockchain platforms have tremendously risen in popularity. Unlike centralised organisations, which are governed by a select few, blockchain platforms operate in a decentralised fashion by the different actors in these platforms. The decentralised nature of blockchains has been essential to their appeal; however, it has also introduced new challenges. Blockchain platforms, like other organisations, try to adapt and adjust to their stakeholders’ needs and preferences. With different actors present whose preferences might not always align, governance problems arise and the risk of division between their community members increases.

Different governing mechanisms exist, depending on the platform. Off-chain governance is the most centralised of such mechanisms with the core developers or the most trusted contributors making most of the decisions. On-chain governance is achieved via on-chain voting mechanisms, which can be more transparent and inclusive than off-chain governance. In both of these mechanisms, community division can take place when a backward-incompatible update is adopted, where some stakeholders choose to stay on the original chain and others choose to upgrade to the updated chain, dividing the community into two. Alternatively, two or more competing updates may be proposed dividing the community about their potential merits. Eventually, consensus can fail and different segments of the community adopt the update that they believe to be the most beneficial.

In the most general sense, such deviations are known as hard forks and numerous examples of them have been observed in popular cryptocurrencies. Two notable examples are the split of the Ethereum chain to Ethereum and Ethereum Classic due to the the DAO debacle [1] and the split of the Bitcoin into Bitcoin and Bitcoin Cash over the debate around block size and the SegWit upgrade. Such divisions can fragment the community and its resources, and as a result reduce the overall value of the platform as well as its security. The latter consideration can be quite tangible as the reduced number of resources supporting a fork can lead to attacks. Such attacks are referred to as 51% attacks and have occurred on a number of occasions, e.g., see the case of Ethereum Classic [2] for a notable such instance.
The above issues highlight the importance of sound blockchain governance, the ability of a blockchain platform community members to express their will effectively regarding the future evolution of the platform as well as the best possible utilization of its resources. So this brings forth the question what characterizes proper governance in blockchain systems? This fundamental question motivates the systematization effort we undertake in this paper.

Our methodology is first to derive a set of properties, that are drawn from general governance principles and election theory and then interpret them to the blockchain governance setting. We use a variety of sources to ensure the comprehensiveness of our property list that include the Council of Europe technical standards for e-voting [3], the Federal Election Commission’s Voting Systems Standards [4], but also blockchain specific ones such as [5, 6, 56]. Given the set of properties, we then evaluate a wide array of blockchain platforms against those properties revealing each platform’s unique strengths and weaknesses.

We distill seven fundamental properties for blockchain governance, which capture different aspects of important requirements for governance. The first property deals with participation eligibility. Decision making systems can produce legitimate outcomes provided they are inclusive, a property we capture by different aspects of Suffrage adapted to the blockchain setting. Suffrage determines a set of “decision-makers” who are a subset of the community of a blockchain project. The second property has to do with the Confidentiality of the decision-makers’ inputs; it further specializes to Privacy, which asks for maintaining the input private while Coercion Resistance asks for the input to be free of any external influences. The third property, Verifiability, asks for decision-makers to be able to verify their input has been taken into account and the output is correctly computed. These last two properties are in a sense “classical” security properties. Next we move to two properties that have to do with the incentives of the decision-makers. Accountability asks for decision-makers to be held accountable for the input they provide to the system, while Sustainability asks whether appropriate incentives are provided for the system to evolve constructively and to the decision-makers for providing meaningful input. We then move to a social choice consideration. Pareto efficiency asks that, given all decision-makers’ preferences, the outcome of the governance process cannot be strictly improved vis-à-vis these preferences. Finally, the crucial ability of the system to produce outputs expediently is captured by Liveness.

Armed with the above comprehensive list of governance properties we investigate a number of popular blockchain platforms which provide some sort of governance functionality and we detail the way they satisfy (or fail to satisfy) each of the given properties. Our results dictate that while each of the properties is considered in the context of at least one system, there exists no platform that satisfies most of the properties.

1.1 Related Work

As of the time of writing, there is yet to be a formal or rigorous coverage of good blockchain governance properties. However, the topic of blockchain governance has received coverage in multiple disciplines. Given their diversity, additional related work is also presented in context within each subsection of Section 2, where each governance property is defined. Pelt et al. [59] adapt the definition of OSS (open-source software) governance to blockchain governance; they then go on to derive six dimensions and three layers of blockchain governance from the literature to build a framework, which can be used as a starting point for discussion in new blockchain projects. Similarly Beck et al. [30] derive three key dimensions of blockchain governance to define an IT governance definition. De Filippi and McMullen [42] investigate the social and technical governance of Bitcoin, making a distinction between two coordination mechanisms: governance by the infrastructure (via the protocol) and governance of the infrastructure (by the community of developers and other stakeholders). Corporate governance has been drawn from in the literature to examine the governance of public blockchain systems. The work done by Hsieh et al. [49] and Allen and Berg [23] are such examples, where the authors of the latter work derive a definition of blockchain governance and make a distinction between endogenous and exogenous governance. Given the variety of actors and strategies in the decision-making processes in blockchain platforms, Khan et al. [51] view blockchain governance from the lens of IT governance and then analyse decision-making processes in the form of voting on a new blockchain improvement proposal, by using Nash equilibria to predict optimal governance strategies. Certain forms of blockchain governance, like traditional forms of governance, have the short-coming of participants not able to change their vote between two consecutive elections or votes. Venugopalan and Homoliak [68] address this shortcoming, among others, by introducing an always-on-voting (AoV): a repetitive blockchain-based voting framework that allows participants to continuously vote and change elected candidates or policies without having to wait for the next election. More specific analysis on certain aspects of blockchain decision-making processes also exist in the literature (e.g. Gersbach et al. [44] where the authors analyse delegated voting and conclude caution should be exercised when implementing such mechanisms).

2 BLOCKCHAIN GOVERNANCE PROPERTIES

One of the main contributions of our work is systematizing the properties pertinent to blockchain governance systems. We would like to stress that there is no single set that optimally captures every aspect. There are trade-offs between satisfying some properties to a high degree and others to a lesser degree. In addition, many current implementations do not have rigorously defined governance mechanisms for every use case and usually contain a mixture of formal on-chain features as well as informal off-chain ones. This is almost inevitable, as different blockchains are built for specific purposes and not all decision-making processes can be sufficiently captured by a smart contract or special purpose protocol logic. Others might still be centralized or transitioning to full decentralization. Irrespective of this, our property systematization focuses on first principles and is meaningful across the board, independently of the underlying set of mechanisms that are set in place to facilitate decision-making in each blockchain platform.

We can categorize the properties into four broad classes pictorially shown in Figure 1. The first class contains properties about the voting system that is used for decision-making. It will touch the issues of who is eligible to participate and what is the process.
that combines the inputs provided. The voting system enables us to argue about the governance process in an ideal, philosophical sense; questions such as who has the right to vote are relevant here. The remaining three classes deal with the way an ideal voting system can be implemented and touch three important domains: security which deals with cryptographic and cyber-security aspects, incentives which deals with game-theoretic and economics aspects, and timeliness which deals with issues of time and expediency. Within, the keywords Deliberation and Execution are greyed-out. These are not the focus of our systematization. The reasoning behind this will be explained below. Failures in the properties of these classes can have important repercussions for the legitimacy of the governance process. Even though the voting system might be acceptable in a ‘Platonic’ ideal sense, failures in the remaining properties can suggest that certain community members are disenfranchised because it is harder for them to participate, or they cannot express their will freely or even that they have no ability to properly form an opinion due to lack of proper incentivization. It is also worth adding that usability permeates these three implementation related classes, but it will be outside of scope of our systematization.

Figure 1: The partition map of governance properties.

An important aspect of our property systematization is that we emphasize fundamental properties entirely decoupling them from any specific techniques, algorithms or mechanisms that support them. To illustrate the point, a simple example is the distinction between the property of having privacy (or secrecy) and the cryptographic protocol techniques that may be used to achieve it. Another example is quadratic voting, which is a technique where additional votes can be ‘bought’ (using actual money, voting credit, etc.) but the cost scales quadratically with the number of votes. Even though it has received renewed interest in blockchain governance, particularly for participatory budgeting applications, it should be clear it is still just a mechanism, not a fundamental property per se; we revisit it in some more detail when we discuss Suffrage below as it is one of our basic properties that is most related.

Further to this point, whether a particular governance mechanism is on-chain, off-chain, uses a foundation etc. is a mechanism, not a property. These inner workings will not be part of our classification explicitly, unless they affect some fundamental property.

Definition 1. The community-members $C$ of a blockchain system are people that have direct interaction with it. This may be by providing resources in service of its security or consensus protocol, owning tokens, develop software etc.

--

5SoK: Blockchain Governance

AFT ’22, September 19–21, 2022, Cambridge, MA, USA

63
Definition 2. The decision-makers $D \subseteq C$ of a blockchain system are the people that participate in (any way) its governance.

Given these definitions, we establish the basic ways that community-members are granted voting rights in the blockchain space. The voting rights should more accurately be called voting weights, as it is very common to allocate a different number of votes across all community-members.

Definition 3 (Type 1: Identity-Based Suffrage). A blockchain governance system satisfies this property if it guarantees decision-making rights to participants who are able to prove their identities such that the votes correspond to unique individual humans.

Contrary to the usual notion of community-membership, identity alone is not (so far) a robust enough connection between users and blockchains. Also, there is no restriction against switching to different blockchains or having direct interactions with many of them. The following notions of suffrage are based on a more ‘quantifiable’ approach and typically assign voting power accordingly.

Definition 4 (Type 2: Token-Based Suffrage). A blockchain governance system satisfies this property if it guarantees decision-making rights to participants who have certain tokens in the platform or a minimum amount of tokens in the platform.

Definition 5 (Type 3: Mining-Based Suffrage). A blockchain governance system satisfies this property if it guarantees decision-making rights to participants who have a certain amount of hashing power in the platform (or other physical resource relevant to the platform, e.g., disk storage).

In the PoS setting, voting weight is often measured by an operator’s stake (or wealth). This can result in the following undesirable situations: (i) participants who may be more enthusiastic about the platform have lower voting weight than those who are less enthusiastic about the platform, and (ii) participants who may have contributed more to the platform may have lower voting weight than those who contributed less. Methods like quadratic voting [55] can help dampen the effects of stake-based voting weight (see below for an explanation), but it does not address the root of the problem: voting weight is ultimately based on wealth owned or even managed (e.g., centralized cryptocurrency exchanges may control a significant amount of stake that does not belong to them). Similar issues exist in the PoW setting, where hashing power may not proportionately reflect stakeholder contributions to the platform. Analysis in quantifying decentralization [7] on blockchain platforms, in terms of stake and hashing power, can provide insights into resultant power concentrations.

Remark (Governance Tokens). Often, tokens used to determine suffrage can have more than one use (e.g., native currency of a proof-of-stake system). However, particularly for the governance of smart contract based protocols, specific governance tokens can be used, who have no other direct functionality or value (such as paying for transaction fees or appearing as block rewards) other than enabling participation. Especially when these tokens are transferable, special care is needed to ensure that their supply, distribution and price accurately represents the community members who are more invested in the project. This was observed in the recent Beanstalk exploit, where an attacker used a flash loan to obtain a majority of governance tokens, passing his own malicious proposal and quickly implementing it. The voting mechanism worked well; but clearly, the voting weights did not accurately reflect the community. To avoid such attacks, other platforms such as Compound employ more fail-safes, such as a mandatory waiting period before enacting the election result.

Instead of assuming that community-members would have an implied incentive to positively contribute to their respective blockchain’s governance, sometimes a more direct approach is taken. Participants are granted a decision-making right based on whether they have positively contributed to the platform. What defines a ‘positive’ contribution is not always clear cut and its definition is left to the platform’s community.

Definition 6 (Type 4: Meritocratic Suffrage). A blockchain governance system satisfies this property if it only guarantees decision-making rights to participants who have positively contributed to the platform.

Definition 7 (Type 5: Universal Suffrage). A blockchain governance system satisfies this property if it guarantees decision-making rights to participants who have positively contributed to the platform.

We reiterate that it is not our objective to outline specific mechanisms for translating community-membership to voting power. For example, we are not suggesting that an actor’s voting weight should be more influenced by previous contributions than by an actor’s stake in the platform. Instead, we are suggesting that it is important that all forms of investments and contributions of a community-member (which can be very different across different blockchains) should be considered when formulating voting weight.

In this context, a mechanism that has gained traction recently in the blockchain context is quadratic voting. In this mechanism, 1 vote would cost 1, but 2 votes would cost 4 and so on. Such a mechanism could achieve a better balance between the Token-Based Suffrage and Identity-Based Suffrage: having additional currency within the system does entail enhanced voting rights, but some balancing effect vis-à-vis the one-person one-vote rule seems appropriate. It also provides a more flexible way of expressing voter preferences. To see this, suppose that, in a governance system where votes can be exchanged for tokens, two voters believe that one vote in favour of this proposal, but in fact they bought more votes just for one another. The first voter is richer they could purchase 100 votes, while the second voter only buys 3. This would signal that the first voter is particularly enthusiastic about the platform, and they have positively contributed to the platform. What defines a ‘positive’ contribution is not always clear cut and its definition is left to the platform’s community.

We reiterate that it is not our objective to outline specific mechanisms for translating community-membership to voting power. For example, we are not suggesting that an actor’s voting weight should be more influenced by previous contributions than by an actor’s stake in the platform. Instead, we are suggesting that it is important that all forms of investments and contributions of a community-member (which can be very different across different blockchains) should be considered when formulating voting weight.

In this context, a mechanism that has gained traction recently in the blockchain context is quadratic voting. In this mechanism, 1 vote would cost 1, but 2 votes would cost 4 and so on. Such a mechanism could achieve a better balance between what Token-Based Suffrage and Identity-Based Suffrage: having additional currency within the system does entail enhanced voting rights, but some balancing effect vis-à-vis the one-person one-vote rule seems appropriate. It also provides a more flexible way of expressing voter preferences. To see this, suppose that, in a governance system where votes can be exchanged for tokens, two voters believe that one vote in favour of some proposal is worth 5 and 10 respectively. By this, we mean that the voters believe investing 1 coin for a vote, would yield a return on investment of 5 and 10 respectively. In the final election, if the first voter is richer they could purchase 100 votes, while the second voter only buys 3. This would signal that the first voter is particularly in favour of this proposal, but in fact they bought more votes just because they had a higher budget to spare. With quadratic voting, the first voter would acquire 2 votes: the next vote would cost 4, which is not seen as a profitable investment.

2.2 Pareto Efficiency

Any blockchain governance system will necessarily depend on a number of decision-making procedures: individual, competing preferences have to be collected and combined into specific actions. In this section we try to formalize how well the tools provided by blockchain allow the decision-makers (recall Definition 2) to reach their most favourable outcome. Ideally, the result would the same as...
one chosen by an omniscient algorithm that has collected all their private thoughts and magically chose the ‘perfect’ outcome. As we will see, even the notion of a ‘perfect’ outcome is hard to define (and under most definitions, does not always exist). We stress that this might be terrible for the community-members of the blockchain; in this section we only focus on how well the intentions of the decision-makers can be turned into actions. Aligning the intentions of the community-members and decision-makers is a question of suffrage (as well as Accountability, which we define in Section 2.5).

The investigation of such decision-making processes is the focus of Social Choice Theory [35], which is an entire field of study dedicated to them. One of its crowning early achievements is the famous Arrow’s Impossibility Theorem (Arrow [26]), on voting systems where participants rank the possible candidates. Specifically, given a set of alternatives $A = \{a_1, a_2, \ldots, a_n\}$, each voter $i$ submits an ordered vector of the form $a_{i1} > a_{i2} > \ldots > a_{in}$. Combining the votes should lead to an outcome preference ordering $a_{j1} > a_{j2} > \ldots > a_{jn}$ of the candidates that best represents the voters. Unfortunately Arrow’s Theorem states that the following natural properties cannot be satisfied at the same time:

- If every voter prefers candidate $X$ over $Y$, then $X$ is ranked higher than $Y$ in the final outcome. This property is often called unanimity.
- The order of $X$ and $Y$ in the final outcome depends only on the ordering of $X$ and $Y$ in each voters preference, irrespective of how all other candidates are ordered. This is called independence of irrelevant alternatives.
- There is no voter who has dictatorial control over the final outcome.

Variations of this result have been adapted in many voting settings, even in cases where the voting process does not have to reveal an entire ordering of outcomes (but only to select the ‘best’ one) or when voters have cardinal preferences (i.e. they can assign numerical preference values to each candidate). Note that almost all popular voting schemes (such as approval voting, where each voter selects a set of acceptable candidates) fall under these definitions. Perhaps the most famous of those impossibility results is the Gibbard-Satterthwaite Theorem (Gibbard [46], Satterthwaite [64]), roughly stating that any voting scenario with more than two candidates is either dictatorial, or subject to strategic voting (i.e., voters swaying the outcome by misreporting their actual preferences).

To deal with these impossibilities, the voting procedures used in practice are not required to be optimal in every scenario, but to satisfy certain weaker properties depending on the setting. One such mild property is Pareto efficiency (e.g., [54, 62]). These properties are tested assuming every voter truthfully reports their preferences.

Definition 8. A blockchain governance system is Pareto efficient if whenever a decision-making process is held, alternative $X$ cannot win if there exists another alternative $Y$ that is preferred by at least one participant and no participant prefers $X$ over $Y$.

A Pareto efficient governance system would never lead to an outcome that is clearly worse than another possible outcome. This property should typically be satisfied (at least when interpreted loosely, as some blockchain systems do not have an entirely rigorous governance model), unless there is good reason not to. Evaluating whether this property is satisfied can be tricky because a blockchain governance system contains many interacting components, with the final result seldom depending on a single vote. We make our best effort to fairly evaluate how likely it is that a Pareto efficient outcome is not selected and how much worse is the selected alternative.

Approval voting is of particular importance, as it is the most common voting mechanism used by the blockchains we evaluate. Given $n$ candidates, each voter can ‘approve’ as many as they want. The winner is the candidate which was approved by most voters, often combined with a threshold, such as also requiring approval from at least 20% of them. Notice that even though the voters might have ordinal or cardinal preferences, they can only submit a binary signal for each candidate. Starting with a simple example, suppose that 2 possible incompatible blockchain updates $a$ and $b$ are up for election. Furthermore, suppose that every voter prefers $a > b$. The outcome will be dictated by the threshold they chose when converting their ordinal preferences to an approval vote. Typically we would expect $a$ to win, but $b$ could win as well! Clearly, any truthful voter who approved $b$ would also approve $a$, since $a > b$ for every voter. However, some voters might chose not to approve either of them. In this case $b$ could win because of a tie. In fact, this is the only way an outcome of approval voting might not be Pareto efficient: if the winner is tied with the Pareto optimal candidate. This happened because the voters where completely uniformed about the preferences of each other and set their ‘approval threshold’ too high. The more information they have the less likely such an outcome becomes. A group of perfectly rational and informed voters would always produce a Pareto efficient outcome. In addition, it is important to keep in mind that there are two more ‘secret’ (implicit) options always available: to do nothing or to fork, which is to be avoided. When combined with a minimum approval threshold and some awareness on the part of the voters, the winner is most likely either Pareto efficient, a suboptimal yet highly popular alternative or a deadlock. Finally, strategic voting involves setting the threshold very high, which decreases the total number of votes and could lead to a deadlock, but is unlikely to result in a fork.

We briefly discuss an alternative voting system which uses the complete ordinal preference profile called instant-runoff (IRV) voting. It proceeds in turns:

- From every ballot, only the top preference is counted.
- If one candidate obtains a majority, they win.
- Otherwise, the least popular top preference is deleted from all ballots and the process repeats.

IRV is also not Pareto efficient as a good candidate might be deleted early, if they fail to win many first choice votes. It is however remarkably resistant to strategic voting [29] while retaining some properties that approval voting lacks, such as selecting the majority winner if one exists. This makes IRV particularly appealing when the community is asked to choose between alternatives in a non-binding way. The result can be further ratified by a referendum.

In some cases, IRV (and any voting system using ordinal preferences) might force the voters to inadvertently submit misleading information. For example, IRV assumes that the first and second place candidate on every ballot are separated by an equal amount, whereas some voters might be indifferent while others strongly in
favour of their first choice only. Approval voting sometimes gets around this issue by asking for even less information. Ordinal preferences can be easily elicited by an auction which is undesirable for an election. A better alternative is to use an ordinal voting mechanism such as majority judgment [28] or combine approval voting with token locking: voters who feel strongly about some candidate may lock their vote tokens for longer, indicating that this election is particularly important to them.

### 2.3 Confidentiality

One of the initial goals of Bitcoin, as well as arguably the first design consideration when implementing a voting system on which the governance system will be based, is the approach to privacy. While its definition is fairly intuitive, we make a distinction between secrecy and pseudonymity.

**Definition 9 (Type 1: Secrecy).** A blockchain governance system satisfies secrecy if whenever a decision-making process is held, an adversary cannot guess the input of any participant better than an adversarial algorithm whose only inputs are the overall tally and, if the adversary is a participant, the adversary’s input.

This definition follows from the early work of Benaloh, cf. [39] and has been formally modeled in numerous subsequent works, e.g., see the model of Juels et al. [50]. This is the strongest of the two notions and typically what would be required of an offline voting system (e.g., traditional elections in most countries). Often, true secrecy is difficult to accomplish in a decentralised setting or might be undesirable. For example, many blockchain combine on-chain governance with off-chain elements, such as discussions on forums. These discussions may be part of the formal governance model and could be combined with an off-chain poll, based on the on-chain distribution of voting power. In these cases there could be a benefit in using pseudonyms, keeping the real life identity safe but tying their public discourse with their actual vote. This is particularly relevant when the distribution of voting power distribution. Even though not explicitly mentioned by name, the Bitcoin white paper provides an explanation about why pseudonymity [57] might be a good enough alternative.

**Definition 10 (Type 2: Pseudonymity).** A blockchain governance system satisfies pseudonymity if no participant is required to reveal their real-life identity to participate in the decision-making processes.

The reason for the development of this notion is that blockchain systems are usually designed with the assumption that consensus is achieved only with regards to the shared ledger; it is impossible to keep track of any information outside of it. Therefore, the same techniques used to keep track of the distribution of wealth (e.g., publicly announcing and linking transactions together), can be used to provide voting rights to the people actually involved in the blockchain without requiring much additional work. This is further related to the notion of suffrage, which is defined in Section 2.1. For example, in Proof-of-Stake based cryptocurrencies like Cardano, voting rights for some applications are distributed based on the amount of stake held by each user, as outlined in the paper by Zhang et al. [70] describing the voting system used by the treasury system of that platform. In practical terms, as long as the cryptographic information required when first producing one’s online identity cannot be traced back to any real-life information, pseudonymity is satisfied. Privacy can be further strengthened, considering the notion of coercion-resistance [41, 50].

**Definition 11.** A blockchain governance system satisfies coercion-resistance if whenever a decision-making process is held, a participant can deceive the adversary into thinking that they have behaved as instructed, when the participant has in fact made an input according to their own intentions.

In a strict sense, this definition is arguably stronger than the guarantee provided by traditional elections: the voter should be able to deceive the adversary even about his participation, not just his vote. By definition, this exceeds the notion of privacy and requires at least one anonymous channel of communication. Such a scheme is described in [50], but tallying requires an amount of communication which is quadratic in the number of votes. As such, this property is typically too demanding to be fulfilled in a blockchain setting, for most applications. However, it can be partially satisfied (e.g., if a ballot is encrypted in a way such that the voter can verify its inclusion when it is cast, but it is impossible for him to reclaim it later, if asked to prove that they voted in some way — the fact that this only provides partial fulfillment of the property stems from the fact that if the participant’s device leaks the random coins, then the ciphertext can be demonstrated to encode the participant’s input).

### 2.4 Verifiability

To complement confidentiality, we now need a property that goes in the opposite direction, namely verifiability. This is a crucial property of every voting system, as it legitimises the election result. The widely accepted “golden standard” of verifiability is expressed below in the form of end-to-end verifiability.

**Definition 12 (End-to-End Verifiability).** A blockchain governance system is verifiable if whenever a decision-making process takes place, participants are able to verify their inputs were properly tallied and independent observers are able to verify that inputs from eligible participants were properly tallied.

Furthermore, Gharadaghy and Volkamer [45] split the definition of verifiability into two separate notions.

- **Individual Verifiability:** It is possible for the voter to audit that his/her vote has been properly created (in general encrypted), stored, and tallied.

- **Universal Verifiability:** Everyone can audit the fact that only votes from eligible voters are stored in a ballot box, and that all stored votes are properly tallied.

At a high level, a system satisfying both properties would be called end-to-end verifiable – but we refer to [40] for more details on the notion of verifiability as well as the subtleties that arise in defining the concept formally.

Intuitively, satisfying privacy (and Definition 9 in particular) as well as coercion-resistance definition 11 should make verifiability more difficult to achieve. After all, these two limit the amount of information that a third-party could elicit by observing the blockchain. Despite this, it is indeed possible to achieve both to a certain adequate level. As exemplary schemes we can point to the work of
whether or not to adopt these changes. Contributions from both ac-
ceptors help the platform to adapt and evolve and need to be rewarded.

Definition 15 (Sustainable Participation). A blockchain govern-
ance system sustains participation if it incentivises, via monetary
rewards or otherwise, participants who participate in the decision-
making process of the platform.

Remark. Sustainability is different from accountability in both
moral and practical terms. Contrary to the definition of Accountability,
Sustainability rewards development or participation with no regard to
its outcome (ideally, before the respective agents have to perform the
work or incur any costs). Accountability relates to possible penalties
applied afterwards, once the effects of a particular change are apparent.
For example, rewarding users just for voting would somewhat enable
sustainable participation, but would not qualify for accountability.
On the contrary, penalizing voters who approved a malicious proposal,
without ever rewarding anyone, would only meet the definition of
accountability.

The idea behind having participation and development incentives in place is to help justify the cost of engagement, which can lead to higher voter participation or more contributions to the platform. These incentives can take various forms, from monetary incentives to reputation- or merit-based incentives [71]. However, Sustainable Participation could be a double edged sword if applied carelessly (e.g., [58, 65]. A monetary reward that is too small might convert a moral decision into a financial one, paradoxically decreasing participation. While in general increased participation also leads to an increase in information acquisition from the voters, it is certainly more beneficial to have a smaller set of participants that have done their due diligence and vote as honestly as possible, than a larger group of disinterested individuals who cast votes at random just to collect rewards.

2.7 Liveness

In formal, on-chain governed platforms, the process for proposing and adopting changes is often constrained by fixed-length time periods. An example of this is Tezos’s Granada protocol [9], where a proposal has to go through five governance cycles (each lasting roughly two weeks) in order to be adopted. In such platforms, an unforeseen event that requires urgent action will not be resolved promptly through the platform’s governance process. Therefore, a blockchain governance system must not only be able to process regular changes, but also urgent ones.

Definition 16. A blockchain governance system satisfies liven-
ess if it is capable of incorporating an input of urgency from the
stakeholders and then being capable of acting on it in the sense that
if an issue is deemed to be urgent according to some function, then
the decision making procedure is capable of terminating within a
reasonable amount of time, as a function of the urgency of the matter.

This definition includes having some protection against denial of
service attacks, that would prohibit governance mechanisms from
terminating in time. All systems evaluated in this work are safe, at
least from a high level standpoint, ignoring implementation details.

Events like the DAO hack [1] have shown the need for blockchain
governance systems to be able to accommodate inputs of urgency and
act on them within a suitable amount of time. An example of blockchain governance system with liveness measures is Polkadot
[8], which allows for emergency referendums to be initiated by
an assigned technical committee. Others, such as MakerDAO, implement an emergency shutdown functionality: since it is running on Ethereum, in an emergency the smart contact can suspend its normal operation and return the invested assets to their owners.

3 EVALUATIONS

In this section, we evaluate a number of popular platforms with respect to the properties outlined in Section 2. The platforms below were chosen such that they present an overview of current approaches. An overall view of the evaluations can be found in Table 1. We start with Bitcoin and Ethereum, two of the oldest and most influential blockchains. These two use proof-of-work for consensus and rely mostly on their developers for governance, who maintain a connection with the community but ultimately have control over the direction of the platform. Continuing, we consider Tezos, Polkadot and Decred. The first two use proof-of-stake, while Decred takes a hybrid approach. In particular, whereas Tezos and Decred favour “direct” democracy, Polkadot uses a council as well, representing two fundamentally different approaches to managing how voters express their preferences and interact with the governance process. 

Next, we study Project Catalyst and Dash, which incorporate a treasury in their decision making, meaning that the result of the voting process needs to respect a budget. Finally we consider Compound, Uniswap and MakerDAO that use a governance token approach. In the case of Compound and Uniswap this token is purely used for voting, while for MakerDAO it also supports the normal operation of the Maker protocol.

Gathering all the necessary information about every governance system is not always easy: typically, the platform’s white paper would contain a very high level overview. Moore details can sometimes be found on the websites of the respective blockchains, but often the complete picture can only be acquired by interacting with a wallet, voting app or forum. Keeping that in mind, we have made our best efforts to cite the relevant sources.

Remark. Due to size constraints, in the main text we include only a high level evaluation of some of the governance protocols. A more in-depth, up-to-date study, along with a point-to-point comparison with respect to each property can be found in the full version of this paper [52].

3.1 Bitcoin

Bitcoin [57] is the most prominent blockchain platform and it is a proof-of-work, mostly off-chain governed blockchain. The Bitcoin Improvement Proposal (BIP) process [10] is Bitcoin’s primary mechanism for ‘proposing new features, for collecting community input on an issue, and for documenting design decisions’. An individual or a group who wishes to submit a BIP is responsible for collecting community feedback on both the initial idea and the BIP before submitting it to the Bitcoin mailing list for review. Following discussions, the proposal is submitted to the BIP repository as a pull request, where a BIP editor will appropriately label it. BIP editors fulfill administrative and editorial responsibilities. There are repository ‘maintainers’ who are responsible for merging pull requests, as well as a ‘lead maintainer’ who is responsible for the release cycle as well as overall merging, moderation and appointment of maintainers [11]. Maintainers and editors are often contributors who earn the community’s trust over time. A peer review process takes place, which is expressed by comments in the pull request. Whether a pull request is merged into Bitcoin Core rests with the project merge maintainers and ultimately the project lead. Maintainers will take into consideration if a patch is in line with the general principles of the project; meets the minimum standards for inclusion; and will judge the general consensus of contributors [11].

There are stages through which a BIP can progress, including ‘Rejected’ and ‘Final’. In progressing to a status of ‘Final’, there are two paths:

- **Soft-fork BIP**: A soft-fork upgrade often requires a 95% miner super-majority. This is done via an on-chain signaling mechanism introduced in [12].
- **Hard-fork BIP**: A hard-fork upgrade requires adoption from the entire ‘Bitcoin economy’, which has to be expressed by the usage of the upgraded software.

**Evaluation.** It is important to note here that the Bitcoin decision-making mechanism is informal, at least with respect to other platforms. Clearly, the on-chain aspects of Bitcoin’s governance satisfy pseudonymity, but not secrecy or coercion resistance as no ‘votes’ are even encrypted. The same is true for its off-chain component. This has the advantage that the system is mostly verifiable, even though having part of the deliberation take place in public forums is harder to track and could be an impermanent storage solution. Since the decision-making process is informal, without clearly defined structure or voting rules, Pareto Efficiency (to any degree) cannot be guaranteed. Sustainability and Accountability fail for the same reason, as there are no defined rules for either. Liveness is arguably partially satisfied, given the informality and flexibility of the BIP system. Since miners are guaranteed to explicitly signal their approval or disapproval of soft-fork upgrades [12], mining-based suffrage is satisfied. Although those with previous positive contributions and relevant expertise are able to provide substantial inputs in the decision-making process, there is no explicit guarantee of their decision-making rights due to the informality of the process. Despite this, we conclude that meritocratic suffrage is likely satisfied.

3.2 Ethereum

Ethereum [13] is one of the most significant second-generation blockchain platforms. Starting as proof-of-work and transitioning on 15 September 2022 to proof-of-stake (PoS) it is governed off-chain, using the Ethereum Improvement Proposal (EIP) process [14] as a mechanism for proposing and integration changes. It is almost identical to that of Bitcoin, without giving miners the option to signal their preferences on-chain.

3.3 Tezos

Tezos [15] is a proof-of-stake, on-chain governed blockchain platform, which defines its governance process as ‘self-amending’. Contrary to Bitcoin or Ethereum, participating in governance is based on stake. Specifically, Bakers (also known as delegates) need to have at least 8,000 XTZ (called a roll) and the infrastructure to run a Tezos node in order to gain both block producing and voting privileges. Community members who have fewer than 8,000 XTZ or
Table 1: Overview of the evaluations of each property against each of the chosen platforms. Every platform might satisfy each property to a different degree, shown by appropriately filling each circle.

| Platform  | Suffrage | Pareto Efficiency | Confidentiality | Verifiability | Accountability | Sustainability | Liveness |
|-----------|----------|-------------------|-----------------|---------------|----------------|-----------------|----------|
| Bitcoin   | O        | O                 | O               | O             | O              | O               | O        |
| Ethereum  | O        | O                 | O               | O             | O              | O               | O        |
| Catalyst  | O        | O                 | O               | O             | O              | O               | O        |
| Dash      | O        | O                 | O               | O             | O              | O               | O        |
| Tezos     | O        | O                 | O               | O             | O              | O               | O        |
| Polkadot  | O        | O                 | O               | O             | O              | O               | O        |
| Decred    | O        | O                 | O               | O             | O              | O               | O        |
| Compound  | O        | O                 | O               | O             | O              | O               | O        |
| Uniswap   | O        | O                 | O               | O             | O              | O               | O        |
| Maker DAO | O        | O                 | O               | O             | O              | O               | O        |

Evaluation. As with Bitcoin, Tezos only satisfies Pseudonymity, but is completely verifiable. Pareto Efficiency is more nuanced. If a proposal receives less than 5% of the upvotes or is tied with another proposal, no proposal will pass, even though operators could have voted for some proposals. However, given the properties of approval voting outlined in Section 2.2, this effect is mild. In addition, the selected outcome is checked once again at the last step. Pareto efficiency could be further hampered under the assumption that the proposals appearing in a single voting period are too many or too technical to evaluate in the allotted time, before the vote. This could make voters inadvertently split their votes and abstain on many proposals, either leading to a deadlock or too many whales. A quorum between 0.2 and 0.7 of the total stake need to be reached, and the proposal is implemented if an 80% supermajority of 'Yea' is reached.

Polkadot [8] is a proof-of-stake, mostly-on-chain governed blockchain platform with a number interesting additions, including an elected council and a technical council. Voters require at least 5 DOT to participate in governance and their voting power is based on stake. At a glance, the voters elect councilors, directly vote on referendums and submit proposals. The councilors then have the power to veto dangerous proposals, elect the technical committee, submit proposal of their own for approval by the voters and also control the treasury. The technical council can submit emergency referendums, that are implemented immediately if approved.

More specifically, the council consists of 13 members with 7 day tenures. They are elected using an approval voting based method, the weighted Phragmén election algorithm (e.g. [36]). An in-house refinement of Phragmén called Phragmims [38] could be used in the future. During a referendum election, an adaptive quorum is used, requiring a different majority and turnout based on how the referendum was created (e.g. by the community or a weak council majority). A successful referendum enters a 28 day waiting period before enactment, unless it is an emergency. Typically, the voters cast are locked for these 28 days. However, the voters can increase their voting power by voluntarily locking them for longer (or decrease it by not locking at all). The treasury is controlled by the council, which decides whether to allocate funds to proposals that ask for them based on current supply.

Evaluation. Only Pseudonymity and Verifiability are satisfied. The council elections and referendums are Pareto efficient. In addition, the voters can signal the strength of their preferences by locking their votes for an extended time. Voting in favour of a proposal requires funds to be locked in until the proposal is enacted.
The documented rationale behind this is to hold voters responsible for a proposal that they vote for, satisfying accountability and further reinforcing Pareto Efficiency. However, Polkadot have deliberately chosen against monetary rewards for voters, for justified reasons (as detailed in Section 2.6). However, council members should probably receive some direct compensation. Even though their tenure is short, they hold a lot of power and should have the ability to devote themselves full time. The Polkadot governance mechanism is capable of taking in inputs of urgency (i.e. emergency referendums) and acting on it if deemed urgent by the council, all whilst being able to terminate within an amount of time proportional to the urgency. Token-based suffrage is satisfied since only token holders are allowed to vote. The council adds teams to the technical committee (which is able to propose emergency referendums) based on their positive technical contributions and expertise. However, those teams are chosen by council members only and a positive contribution does not equate to a guarantee of an input in a decision-making process.

3.5 Decred
Decred is a hybrid proof-of-work and proof-of-stake system that is mostly on-chain governed [16]. Voters can participate in governance by locking enough DCR, which is the native token of Decred. This provides them with tickets which supplement the consensus protocol and can also be used for voting. High level issues that require funds from the Decred Treasury are handled off-chain, in Politeia. This deliberation results in an election which is cryptographically coupled to a snapshot of the chain. A 20% quorum is needed, with over 60% of the votes being in favour. The on-chain component is the Decred Change Proposal (DCP) [17], through which the consensus mechanism is updated. This requires a 10% quorum and 75% majority of approval. Failing to meet the quorum, the election will be repeated in the next cycle. If it is successful, a ‘lock-in’ period begins, after which all nodes should update their software.

Evaluation The votes are not encrypted, therefore only pseudonymity and verifiability are satisfied. Pareto efficiency is somewhat satisfied: there are similar issues as Tezos, but the added role of Politeia could improve the outcome. Sustainable development is satisfied (somewhat informally) but there are no specific rewards for participating in governance. Voters receive rewards, but these have to do with their role in the hybrid consensus protocol. Accountability could be improved, as the token locking required for voting is shorter than the timelock for successful proposals.

3.6 Compound
Compound [18] is a protocol running on the Ethereum blockchain that establishes money markets. Governance in Compound is fueled by an ERC-20 compatible token called COMP [19]. These governance tokens are distributed to the community through various channels: some are allocated to users based on their invested assets, others to Compound Labs Inc. shareholders and employees, etc. Holding COMP allows users to vote, delegate to others and create proposals, which are executable pieces of code. Once submitted, these proposals enter a two day review period, following a three day election. A proposal is successful if a majority is in favour and a quorum is reached. After that, the proposal is locked for two days before implementation, for security. Finally, the Pause Guardian (controlled by a community appointed multi-signature) can suspend most functionalities of Compound at any time.

Evaluation Every step of the governance process is performed by interacting with smart contracts on Ethereum, without any further cryptographic techniques, satisfying pseudonymity and verifiability. Once a proposal enters the voting phase, the voters only have two options: yes or no, which is clearly Pareto Efficient. If there are multiple incompatible options (e.g., values of a specific parameter), these proposals would have to be dealt with sequentially: the actual order could bias voters, which complicates their decisions and leaks information. Therefore, Pareto Efficiency is somewhat satisfied (e.g., between two highly popular proposal, the slightly less popular one might win if it is up for election first and then the users might be less eager to implement another change). Once a proposal is executed, its creator and voters are completely independent from its future and there are no rewards associated with the process. Therefore, neither availability or sustainability are satisfied. The total time between creating a government proposal and voting for it takes 7 days, 2 of which are hard-coded into the Timelock. This window for immediate action is only open right after a vote, but adding the Pause Guardian, liveness is satisfied. Since voting eligibility depends only on having COMP tokens, which can be exchanged and are initially distributed to addresses with assets on Compound, token-based suffrage is satisfied. Some COMP tokens are distributed or reserved for members of the Compound team. Therefore, meritocratic suffrage is slightly satisfied.

3.7 Maker DAO
Maker DAO [20] is a decentralized organization running on Ethereum and based on the Maker Protocol. One of its features is using a two-token system, with DAI, which is a stablecoin pegged to the U.S. dollar, and MKR as the governance token. MKR also serves an additional purpose: to support DAI’s peg. The governance system employs both on and off-chain elements. The off-chain component takes place at the Maker DAO forum, where users can create Forum Signal Threads, which are followed by a poll. Each forum user has a single vote, irrespective of MKR. These are further ratified on-chain by Governance Polls, which employ instant-runoff voting, weighted by the MKR of each voter. Finally, changes to the protocol (which are pieces of executable code) are enacted by Executive Votes. These follow a continuous approval vote system, with the most approved Vote at any given time being the actual implementation. For security reasons, these changes happen after a 24 hour waiting period and there is also an emergency shutdown functionality, triggered if the community locks enough MKR.

Evaluation. As there is no vote encryption, only pseudonymity and verifiability are satisfied. Pareto Efficiency is improved compared to other designs by using instant-runoff voting to handle competing proposals, thus giving voter a richer action space to declare their preferences accurately. Suffrage is also improved, as there is a clear connection between MKR tokens and the overall functionality of Maker DAO, further coupling its value to some actual generated utility.
**Remark.** Project Catalyst and Dash include a treasury. Funds are collected during the normal blockchain operation and allocated to fund its development and other projects. The voter preferences are more complicated, since each proposal needs to be weighed against its budget and the opportunity cost of funding it. Decred also includes a treasury, but proposals are first debated off-chain, rather than set to compete on-chain for some portion the budget available in one round of funding. The final vote is on-chain, but only to confirm proposals that already have off-chain support.

### 3.8 Project Catalyst

Project Catalyst [21] is the on-chain treasury governance system used by the Cardano blockchain, which is proof-of-stake. Governance takes place in twelve week periods called funds and involves a number of additional agents, on top of the usual voters, whose voting power and eligibility is dependent on stake ownership. At the beginning of the fund, community generated proposals (which include a corresponding budget) are submitted. These are then reviewed by Community Advisors (CA’s) and these reviews are further checked for their quality by veteran Community Advisors (vCA’s), both of which are rewarded for their efforts. Given these evaluations, an approval voting based mechanism [70] is used. The proposal whose ‘yes’ votes minus the ‘no’ votes are more than 5% of the total votes received is eligible for funding. These eligible proposals are then sorted according to their approval. If the available funds are not enough to cover some proposal, it is skipped and a less popular (but cheaper one) could take its place. In addition, there is the Catalyst Circle [22], an elected group of representatives that oversees Catalyst and a delegated voting system is proposed for future iterations.

**Evaluation.** Everyone participates in Project Catalyst using their wallet address. Voters submit encrypted ballots (padded with some randomness), using the public key issued by a committee, which tallies the votes and decrypts the result. If the voter address is linked to a real identity, the only information available is that this particular person voted, keeping the contents secret. The ballot itself cannot be decrypted by the voter and if the random padding is not kept, it is impossible even for the voter to convince anyone of the way they voted. The result of the vote can be independently verified and long as the voter saved the random padding, they can verify that their particular vote was counted. Therefore, there is a (somewhat contrived) sequence of events after which a voter would be unable to check that their ballot has been added.

In some cases, proposals with fewer votes will be prioritised for their lower budgets. For example, if the total fund is 100 and the three winning proposals have budget 1, 50 and 50 (in order of popularity) the last proposal will not receive funding, even though every voter might prefer funding the two 50 proposals. Additionally, each voter could submit an uninformative ‘no’ vote to many proposals, in order to maximize the winning chance of their favourite. A potential mitigation would be to use techniques from Participatory Budgeting [31] and Distortion [25], which use a small amount of ordinal information (e.g., asking voters to compare between 2 proposals or to list their most favourite one) to improve the quality of the outcome. Overall, Pareto Efficiency is somewhat satisfied.

There are no explicit, on or off-chain, penalties. Proposers need to submit progress reports about their projects to keep receiving funding and community advisors can be penalized for poor reviews or absence. As these are centralized or community-driven without clearly described mechanisms, accountability is mostly not satisfied. Although there is no explicit reward given to the proposer, it is her responsibility to request the amount which cover the cost of her work. All other parties are rewarded for participating in the governance process and to an extent receive larger rewards for additional effort. Each Project Catalyst Fund follows a 12 week timeline. Liveness is not satisfied: even though the funds can be released in accordance with each proposal’s progress, there is no mechanism to take urgent action. Voting rights depend only on having at least 500 ADA. There are no guaranteed voting rights based on previous positive contributions, however, community advisors can affect the outcome of the votes through their reviews.

### 4 CHALLENGES & RESEARCH DIRECTIONS

It should be clear from our exposition so far that the blockchain governance space is still rife with challenges and open questions. We summarize in this section a number of them to motivate future research in the area.

I. Tradeoffs between Privacy vs. Verifiability and Suffrage. The tension between verifiability and privacy stems from requirements such as universal verifiability which mandates tracing each decision back to the inputs of decision-makers as determined by suffrage. The higher degree of privacy that is required, the more difficult it is to ensure verifiability; as a simple example from classical elections, if the electoral roll remains private, then it is difficult for an external observer to verify whether the correct set of decision-makers has participated. This also creates a tension with suffrage as types of suffrage that maximize inclusion, for the sake of verifiability, might have to expose a larger set of community-members that otherwise would have remained private. Technically reconciling these properties is highly non-trivial, especially if privacy aspects such as coercion resilience are desired.

II. Proofs of Personhood, Identity-based suffrage and tradeoffs with Privacy. While there is wide agreement that individual users should have equal weight in decision-making (something advocated in the context of election reform for centuries, cf. [48]), achieving this type of suffrage is particularly challenging in the context of decentralized systems. Even though some initial work is undertaken in this direction e.g., [66], and there are also connections with other concepts in cyber-security such as CAPTCHAs [69], nevertheless the problem of achieving a satisfactory level of identity-based suffrage in the context of blockchain governance is still wide open. This challenge should be also considered from the lens of privacy, since in many cases of such proofs, community-members would have to reveal personally identifiable information to other actors something that comes inevitably with privacy implications.

III. Meritocratic suffrage and tradeoffs with privacy. The challenge in the context of meritocratic suffrage is in two levels, first, in quantifying what type of merit itself should warrant participation to decision-making. The second level is recording reliably the relevant actions of community-members in the system so that it can be acted upon during the decision-making process. Finally, as in the
case of proofs of personhood, there can be privacy implications. Some early works in this direction show that privacy and merit may be reconciled, see, e.g., the signatures of reputation primitive [34] but still, significantly more work is required to fully tackle the full spectrum of possible ways to express and act on merit.

IV. Exchanges, venture capital investors and token-based suffrage. In the setting of token-based suffrage, an important consideration is the fact that token-holders may choose custody solutions for their tokens (e.g., reducing risks regarding loss of keys, or the ability to access services or rewards provided by custody operators). While among some cryptocurrency users this is frowned upon (the tenet “not your keys, not your coins” is frequently repeated in social media) there is a large number of users that prefer to keep their digital assets in third party providers’ systems.2 This results in entities with inflated leverage in a token-based system that in some cases can control a very significant portion of the token supply. A related issue is the presence of venture capital firms that are early investors in some platforms and receive a large amount of tokens at preferential prices in exchange for funding initial development efforts. This similarly may result in increased leverage which can be perceived as unfair by other community-members.

V. Rational ignorance and inaction. Rational ignorance [67] is when decision-makers refrain from acquiring the knowledge required of meaningful input when voting, or when delegating their vote, due to the fact that the cost of acquiring that knowledge exceeds any expected potential benefits. A similar argument can be applied to developing improvement proposals, where inaction can be more rational than action if the cost of development (or even the act of preparing a proposal) exceeds any potential benefits. These issues pertain to the property of sustainability which so far lacks a comprehensive theoretical framework in the context of blockchain governance. For some recent work in this direction see [60, 61].

VI. Tradeoffs between accountability and utility. Recall that making decision-makers accountable suggests some degree of “skin-in-the-game” on their side and the natural way to achieve this implies some form of restriction of the functionality that is offered to them. As a result, the immediate utility that decision makers can extract from the platform is reduced — recall the example of “token lockup” for the duration of a certain decision making process. The main challenge in this setting is to model and quantify the relevant aspect of this utility reduction and mapping the spectrum of possible options so that the right balance between accountability and utility can be determined on a case by case basis.

VII. Tradeoffs between Liveness vs. Pareto Efficiency and Suffrage. As discussed in the context of liveness, expedient decision-making is highly desirable. Unfortunately high expediency can come at odds with Pareto efficiency: if decision-makers have preferences which are not recorded due to the system not giving them enough time to react, Pareto efficiency could be affected (notice that abstaining can be also a preference, but there is a distinction between having an actual preference and missing the deadline to provide it). Liveness can also exhibit a similar tradeoff with suffrage: the more exclusive the suffrage mapping from community-members to

decision-makers is, the higher the expediency of the system may become - but this of course comes at the expense of the system being less inclusive. Striking the right balance between these properties is another question on which future research should focus.

5 CONCLUSION

In this work we focused on systematizing the core properties of blockchain governance. We took a first principles approach and derived seven fundamental properties using which we analyzed a number of widely used blockchain platforms. There are also other platforms that we attempted to cover, but these were either too poorly documented or were yet to implement governance mechanisms. We consider our work to be a comprehensive coverage of popular blockchain systems at the time of writing.

The main outcome of the systematization effort, as illustrated in Table 1, is that in many ways all current blockchain platforms either have deficiencies in their governance processes or allow significant room for improvement. It is worth reiterating that achieving all stated properties to the highest possible degree is impossible due to their conflicting nature and as a result it is inevitable that platforms must decide on appropriate tradeoffs between the various properties that are the most suitable for each particular setting. Arguably, without effective governance processes, blockchain technology will fail to reach its full potential. For one thing, software engineering practice has shown that software updates, extensions and patches are a necessity in the lifecycle of computer systems and as a result, without proper governance, blockchain systems will fail to adapt to unanticipated use cases and mitigate software bug vulnerabilities that are inevitably discovered in any system.

REFERENCES

[1] Divisions of Corporation Finance and Enforcement. Statement by the Divisions of Corporation Finance and Enforcement on the Report of Investigation on the DAO. Investigation report. July 2017. URL: https://www.sec.gov/litigation/investreport/34-81077.pdf.
[2] Almost $500,000 in Ethereum Classic coin stolen by forking its blockchain, Dan Goodin, 1/8, 2019, Ars technica.
[3] Legal operational and technical standards for e-voting, Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum, Council of Europe publishing, 2004. http://www.euds.eu/library/CoE_Recommendation%20on%20legal%20operational%20and%20Technical%20standards%20for%20elections%20voting_2004_EN.pdf.
[4] Voting System Standards Volume I, Federal Election Commission, USA. April 2002. https://www.eac.gov/sites/default/files/eac_assets/1/28/Voting_System_Standards_Volume_1.pdf.
[5] V. Buterin. Moving beyond coin voting governance, August, 2021. Accessed on: October 1, 2021. Available: https://vitalik.ca/general/2021/08/16/voting1.html.
[6] Wharton Cryptogovernance Workshop. Accessed on: October 19, 2021. Available: https://cryptogov.net.
[7] B. S. Srinivasan and L. Lee. Quantifying Decentralization, news.earn.com, July, 28, 2017. Accessed on: October 3, 2021. Available: https://news.earn.com/quantifying-decentralization-e39db238c29c.
[8] D. Salman, Governance, Polkadot Wiki, September 17, 2021. Accessed on: October 3, 2021. Available: https://wiki.polkadot.network/docs/learn-governance.
[9] Tezos Foundation, The Voting Process, Tezos Documentation, July 16, 2021. Accessed on: October 2, 2021. Available: https://gitlab.com/tezos/tezos/-/blob/master/docs/010/voting.rst.
[10] L. Dashjr, BIP Process, github.com, February, 4, 2016. Accessed on: October 14, 2021. Available: https://github.com/bitcoin/bips/bip-master/bip-0002.medialink.
[11] J. Schnelli et al., Contributing to Bitcoin Core , github.com, September, 26, 2015. Accessed on: October 14, 2021. Available: https://github.com/bitcoin/bitcoin/blob/master/CONTRIBUTING.md.
[12] P. Wulle, P. Todd, G. Maxwell, and R. Russell, Version bits with timeout and delay, github.com, October, 4, 2015. Accessed on: October 14, 2021. Available: https://github.com/bitcoin/bips/bip-master/bip-0009.medialink.
