SoK: Blockchain Governance

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

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

***Abstract*—Blockchain systems come with a promise of decentralization that, more often than not, stumbles 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 particularly 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, confidentiality, verifiability, accountability, sustainability, Pareto efficiency, suffrage 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 tradeoffs, something direly needed for blockchain platforms to operate effectively in the long term.

***Index Terms*—Blockchain, Governance, Decentralization**

I. Introduction

Following the founding of Bitcoin [1] 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 within their stakeholder community 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 stakeholder population 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 Etheurem and Ethereum Classic due to the the DAO debacle [2] and the split of the Bitcoin system 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 [3] for a notable such instance.

The above issues highlight the importance of sound blockchain governance, the ability of a blockchain platform stakeholders 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 [4], the Federal Election Commission's Voting Systems Standards [5] but also blockchain specific ones such as [6, 7, 8]. 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. The properties capture different aspects of important requirements for governance. The first has to do with the *Confidentiality* of the stakeholder input; 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 second property —*Verifiability*— asks for users to be able to verify their input has been taken into account in the output and that such output is correctly computed. These first two properties are in a sense "classical" security properties. Next we move to two properties that have to do with the incentives of the stakeholders. *Accountability* asks for stakeholders 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 stakeholders for providing meaningful input. We then move to a social choice consideration. *Pareto efficiency* asks that, given all stakeholders' preferences, the outcome of the governance process cannot be strictly improved vis-à-vis these preferences. The next property deals with participation eligibility; Decision making systems can produce legitimate outcomes provided they are inclusive — a property that we capture by different aspects of *Suffrage* suitably adapted to the blockchain setting. 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.

A. 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 II, where each governance property is defined. Pelt et al. [9] 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. [10] derive three key dimensions of blockchain governance to define an IT governance definition. De Filippi and McMullen [11] 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 blockchains. The work done by Hsieh et al. [12] and Allen and Berg [13] 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. [14] 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 [15] 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. [16] where the authors analyse delegated voting and conclude caution should be exercised when implementing such mechanisms).

II. 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 is a trade-off between satisfying too many and too few properties. 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 these system specific considerations, 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 platform.

Another important aspect of our property systematization is that we emphasize fundamental properties entirely decoupling them from any specific techniques, algorithms or mechanisms that facilitate 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,[1] 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.

We want to stress that satisfying all properties would not make a blockchain governance system *perfect*. There are many blockchains applications and each of them has different needs and use cases that would require community involvement. Some properties might be incompatible with each other. However, any design would have to at least *consider* how each property is addressed and ensure that the their choice is deliberate. As such, during the evaluation of different governance systems we will make sure that each property is judged *in context*, taking the goals of each system into account.

A. 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 1 (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. [17] and has been formally modeled in numerous subsequent works, e.g., see the model of Juels et al. [18]. 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 whitepaper provides an explanation about why *pseudonymity* [1] might be a good enough alternative.

[1] Such as Gitcoin quadratic funding, https://gitcoin.co/blog/gitcoin-grants-quadratic-funding-for-the-world/

Definition 2 (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 II-G. 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. [19] 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* [18, 20].

Definition 3. *A blockchain governance system is coercion-resistant 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 [18], 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).

B. Verifiability

To complement confidentiality, we need now 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 4 (End-to-End Verifiability)**.** *A blockchain governance system is verifiable if whenever a decision-making process takes place, participants are to 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 [21] 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 [22] 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 1 in particular) as well as coercion-resistance definition 3 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 [18] mentioned earlier, but also schemes such as the early work of Benaloh and Tuinstra [23], the Benaloh-challenge approach [24] that has influenced a lot of practical e-voting systems, see e.g., [25], or the hardware token based approach of [26]. This latter work also provides a comprehensive modeling of the concept of incoercibility that extends well beyond the setting of e-voting per se and can be immediately applicable to the blockchain setting as well.

C. 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. The investigation of such processes is the focus of Social Choice Theory [27], which is an entire field of study dedicated to them. One of its crowning early achievements is the famous Arrow's Impossibility Theorem (Arrow [28]), 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 $a_{i_1} \succ a_{i_2} \succ \ldots \succ a_{i_n}$. Combining the votes should lead to an outcome preference ordering $a_{j_1} \succ a_{j_2} \succ \ldots \succ a_{j_n}$ 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 [29], Satterthwaite [30]), 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., [31, 32]). These properties are tested assuming every voter truthfully reports their preferences.

Definition 5. *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 $a \succ b$. 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 $a \succ b$ 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 that 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 [33] 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 [34] 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.

D. Accountability

The quest for accountability in governance is not a recent pursuit, as it was clearly recognised by the ancient Egyptians and the ancient Greeks [35]. Since then, accountability as a concept has been split into multiple types and dimensions. For example, Grant and Keohane [36] outlines that accountability can take two general forms: vertical (where a party is accountable to other parties that are higher in a given hierarchy) and horizontal (where a party is accountable to other parties that are not higher or lower in a given hierarchy). Although *collective* accountability is often implicitly implied in coin-based voting, *individual* accountability is not. That is, if enough voters vote for a bad decision, the coin value of every voter declines whether or not they supported the decision. Individual accountability can take various forms, the most prominent of which is often referred to as 'skin in the game', where participants have an individual investment that will be directly affected by their individual actions.

Definition 6. *A blockchain governance system satisfies the property of accountability if whenever participants bring in a change, they are held individually responsible for it in a clearly defined way by the platform.*

Examples outside the blockchain space include the work done in Sacco et al. [37], where participants review publications and those having more 'skin in the game' (evaluating publications in which they will be marked as co-authors) have an increased individual interest in ensuring that a study's ambiguously reported methods and analyses are clarified prior to submission. Examples in the blockchain space include Polkadot's governance system [38], where voters who vote in favour of a proposal will have their stake locked until the proposal is 'enacted' or deployed.

E. Sustainability

Rational ignorance [39] is when actors refrain from acquiring knowledge when voting, or when delegating their vote, since 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 exceeds any potential benefits. Changes in blockchain governance rely on two main actors: those who develop and propose the changes, and those who decide on whether or not to adopt these changes. Contributions from both actors help the platform to adapt and evolve.

Definition 7 (Sustainable Development)**.** *A blockchain governance system sustains development if it incentivises, via monetary rewards or otherwise, participants who develop successful improvement proposals for the platform.*

Definition 8 (Sustainable Participation)**.** *A blockchain governance system sustains participation if it incentivises, via monetary rewards or otherwise, participants who participate in the decision-making process of the platform.*

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 [40]. Sustainability is different from accountability in both moral and practical terms. 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.

F. 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 most recent protocol (the Granada protocol) [41], 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 9. *A blockchain governance system satisfies liveness 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, which is a function of the urgency of the matter.*

Events like the DAO hack [2] 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 [38], which allows for emergency referenda 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.

G. Suffrage

In national or regional elections, it is often the case that the voting function implements a 'one person, one vote' rule. Different jurisdictions use different criteria in guaranteeing the right to vote to individuals, but the bottom line is that one person can only submit one vote. Although research is currently underway on proof-of-personhood systems [42], which verify that accounts correspond to unique individuals, the 'one person, one vote' rule is not applicable to most, if not any, current blockchain platforms. Instead, we often see that a minimum amount of stake or hashing power is required to guarantee a vote. We also see platforms where only the founders or core developers are guaranteed a vote. Guaranteeing decision-making rights only for the founders or the core-developers can disenfranchise the wider community of the platform. Therefore, we shall not include that as a form of suffrage.

Definition 10 (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.*

Definition 11 (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 12 (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 [43] 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 reflect proportionally stakeholder contributions to the platform. Analysis in quantifying decentralisation [44] on blockchain platforms, in terms of stake and hashing power, can provide insights into resultant power concentrations.

Ideally, participants would be guaranteed a decision-making right 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 13 (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 14 (Type 5: Universal Suffrage)**.** *A blockchain governance system satisfies this property if it guarantees decision-making rights to participants who have mining power or tokens in the platform as well as participants with positive contributions to the platform.*

It is important to note here that it is not our objective to outline specific mechanisms for governance. 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 all forms of investments and contributions of an actor 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 4 and 9 respectively. In the final election, if the first voter is richer they could purchase 100 votes, while the second 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.

Note that in evaluating individual platforms in Section III, we will ignore evaluating universal suffrage as it is implied by the other suffrage sub-properties.

III. Evaluations

In this section, we evaluate a number of popular platforms with respect to the properties outlined in Section II. 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 I.

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 as well. Finally we consider Compound, Uniswap and MakerDAO that use a governance token. 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, as they are actively developed and sometimes the documentation may lag behind the latest implementation. Typically, the platform's white paper would contain a very high level overview that is inadequate for our purposes. The exact details can sometimes be found on the websites of the respective blockchains, but more often than not 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.

A. Bitcoin

Bitcoin [1] is the most prominent blockchain platform and it is a proof-of-work, mostly off-chain governed blockchain. The Bitcoin Improvement Proposal (BIP) process [45] 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 fulfil 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 [46]. Maintainers and editors are often contributors who earnt 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 [46].

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 signalling mechanism introduced in [47].
- *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.

We now have an overview of the upgrades decision-making process in Bitcoin, which we will use to perform rough evaluations against the properties developed in Section II. It is important to note here that the Bitcoin decision-making mechanism is informal, at least with respect to other platforms. This results in rougher and less satisfying evaluations.

- **Confidentiality**:
  - **Secrecy**: Since the decision-making process among maintainers or reviewers is on public forums, an adversary might accurately guess each participant's input. Therefore, secrecy is *not* satisfied.
  - **Pseudonymity**: There are no defined requirements for participants to reveal their identities. Some choose to participate with their real identities and others do not. Therefore, pseudonymity is satisfied.
  - **Coercion-resistance**: Since the deliberation process among maintainers and others takes place on public

Platform	*Confidentiality*		*Verifiability*	*Pareto Efficiency*	*Accountability*	*Sustainability*		*Liveness*	*Suffrage*			
	Secrecy	*Coercion Resistance*				*Sustainable development*	*Sustainable participation*		*Identity-based*	*Token-based*	*Mining-based*	*Meritocratic*
Bitcoin	◔	○	◕	○	◔	○	○	◓	○	○	●	◓
Ethereum	◔	○	◕	○	○	○	○	◓	○	○	○	◓
Catalyst	◕	◔	◕	◓	◔	●	○	○	○	●	N	◔
Dash	◔	○	●	◓	○	●	●	○	○	●	○	○
Tezos	◔	○	●	◓	○	○	○	○	○	●	N	○
Polkadot	◔	○	●	●	●	○	●	●	○	●	N	◔
Decred	◔	○	●	◓	○	●	○	○	○	●	○	○
Compound	◔	○	●	◓	○	○	○	◓	○	●	○	◔
Uniswap	◔	○	●	◓	○	○	○	◓	○	●	○	◔
Maker DAO	◔	○	●	◕	○	○	○	●	○	●	○	○

TABLE I

OVERVIEW OF THE EVALUATIONS OF EACH PROPERTY AGAINST EACH OF THE CHOSEN PLATFORMS.

Every platfom might satisfy each property to a different degree. This is shown by a filled circle for robustly meeting the definition down to an empty circle if clear improvements are needed. The letter N is used if a property does not apply.

forums, an adversary might accurately guess each participant's input. Thus, coercion-resistance is *not* satisfied.

- **Verifiability**. The signaling mechanism used as a voting process for certain decisions is on-chain. However, even though the deliberation process takes place in public forums, the decision-making process remains informal, which makes it difficult to identify how inputs are incorporated from which parties and how they are tallied. However, such inputs can be traced through the public forums and any changes that are merged can be tracked on Github. Therefore, verifiability is *mostly* satisfied.
- **Pareto Efficiency**. Since the decision-making process is informal, there is no defined voting rule, which specifies how the inputs result in a final outcome. Therefore Pareto efficiency is *not* satisfied.
- **Accountability**. The platform does not define any way by which it can hold participants responsible or accountable for their individual actions. Therefore, accountability is *not* satisfied.
- **Sustainability**: *Sustainable Development*. There are no explicitly defined incentives for contributors to develop BIPs. Therefore, sustainable development is *not* satisfied.
- **Sustainability**: *Sustainable Participation*. There are no explicitly defined incentives for community members to participate in discussions or reviews throughout the BIP process. Therefore, sustainable participation is *not* satisfied.
- **Liveness**. Although no specific mention of inputs of urgency are provided by the platform, given the informality and flexibility of the BIP system, it is likely capable of taking inputs of urgency and acting on them in an amount of time that is a function of the urgency. Therefore, the platform *likely* satisfies liveness.
- **Suffrage**: Since miners are guaranteed to explicitly signal their approval or disapproval of soft-fork upgrades [47], 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. However, since meritocracy still does play a significant role in the process, we will conclude that meritocratic suffrage is *likely* satisfied.

B. *Ethereum*

Ethereum [48] is one of the most prominent second-generation blockchain platforms. It is a proof-of-work, off-chain governed blockchain. Similar to Bitcoin, Ethereum uses an Ethereum Improvement Proposal (EIP) process [49] as a mechanism for proposing and integration changes. Since the mechanism is almost identical to that of Bitcoin, we only highlight the properties in which their evaluations differ.

- **Suffrage**: *Mining-based*. Unlike Bitcoin, there is no existing mechanism in Ethereum by which miners are guaranteed a decision-making right on implementing proposals.

C. *Tezos*

Tezos [50] is a more-recent proof-of-stake, on-chain governed blockchain platform, which defines its governance process as 'self-ammending". The following overview of the Tezos governance process is of Tezos's current protocol: Granada [51]. In Tezos, to participate directly in the governance process, a participant is required to have at least $8,000$ tokens. A unit of $8,000$ tokens is called a *roll* and it equates to a single vote. In this case, the participant is called a *delegate*. Alternatively, to participate indirectly in the governance process, a participant can delegate whichever amount of tokens they have (which can be less than $8,000$) to an existing delegate.

The voting process is currently divided in five governance periods, each period spanning roughly two weeks or 20480 blocks (i.e. 5 cycles). Note that for proposals to be submitted in Tezos, they need to be compiled without errors so that at the end of the governance process the proposal can be adopted automatically. The following is a breakdown of the five governance periods:

1) **Proposal period**. Delegates can submit protocol amendment proposals using the proposals operation as long as the underlying codebase compiles with the change. Delegates then upvote their preferred proposal or proposals. The proposal with the most upvotes is selected. If there are no proposals, no proposals with upvotes of at least 5% of the possible votes, or a tie between proposals, a new proposal period starts.
2) **Testing-vote period**. Delegates can cast one vote to test or not the winning proposal using the ballot operation.
3) **Testing period**. A test chain is forked for the entire testing period to ensure a correct migration of the context.
4) **Promotion-vote period**. Delegates can cast one vote to promote or not the tested proposal using the ballot operation.
5) **Adoption period**. The adoption period serves as a buffer time for users to update their infrastructure to the new protocol. At the end of this period, the proposal is activated as the new protocol and a new proposal period starts. Here, the Tezos node software is aware that at the end of this period it needs to update to the new protocol, hence why the governance process is described as 'self-amending".

In the **proposal period**, approval voting is used. In the **testing-vote** and **promotion-vote** periods, the voting method is as follows:

- Each delegate can submit a single vote of a 'Yea", 'Nay" or 'Pass".
- If the participation reaches the current quorum and the proposal has a super-majority in favour, it goes through to the next stage.
  - The quorum is the participation threshold, it has maximum value of 0.7 and a minimum value of 0.2, and it changes after every vote.
  - A super-majority is when the number of 'Yea" votes is more than 80% of the number of 'Yea" votes and 'Nay" votes summed together.

Similar to the previously evaluated platforms, we perform the evaluations of the governance process in Tezos against the properties developed in Section II.

- **Confidentiality**:
  - **Secrecy**: The delegation mechanism requires the public key of each delegate to be recorded on the ballot, and all ballots are public. Therefore, secrecy is *not* satisfied.
  - **Pseudonymity**: Voters are not required to reveal their real-life identities to participate in the governance process; therefore pseudonymity is satisfied.
  - **Coercion-resistance**. Since delegate votes (rolls) are tied to their chosen pseudo-identities, coercion-resistance is *not* satisfied.
- **Verifiability**. Since the votes and final tally are all public, verifiability is, by definition, satisfied.
- **Pareto Efficiency**. 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 II-C, this effect is mild. In addition, the selected outcome is checked once again at the last step. Therefore, Pareto efficiency is *somewhat* satisfied.
- **Accountability**. Whether an operator is directly voting or delegating, the stake of each delegate is computed at the start of each voting period. This means that delegates can sell their stake before the adoption period ends and the proposal is activated. There are no accountability measures defined in Tezos. Therefore, accountability is *not* satisfied.
- **Sustainability**: *Sustainable Development*. There are no explicit or direct incentives given for developing successful proposals. Therefore, sustainable development is *not* satisfied.
- **Sustainability**: *Sustainable Participation*. There are no explicit or direct incentives given for participating in the governance process. Therefore, sustainable participation is *not* satisfied.
- **Liveness**. Given the lack of flexibility of the on-chain governance model, the Tezos governance system is incapable of taking inputs of urgency and responding to them in accordance to the severity of the issue. Although a Gitlab issue or a pull request could be initiated without going through the formal on-chain route, it is still not the officially documented, and certainly not the 'self-amending", way by which the system processes inputs. Therefore, liveness is *not* satisfied.
- **Suffrage**: Only token-holders are able to vote, with or without delegation. Therefore, token-based suffrage *is* satisfied.

D. Polkadot

Polkadot [38] is a proof-of-stake, *mostly-on-chain* governed blockchain platform. To make any changes to the network, *active* token holders and the *council* administrate a network upgrade decision. Whether the proposal is proposed by the public (token holders) or the council, it will go through a referendum to let all token-holders, weighted by stake, make the decision.

The council is an elected body of on-chain accounts that are intended to represent the passive stakeholders of Polkadot, currently consisting of 13 members [38]. The council has two major tasks in governance: (i) proposing referendums and (ii) vetoing dangerous or malicious referendums. The council implements what is called a *prime member* whose vote acts as the default for other members that fail to vote before the timeout. The prime member is chosen based on a Borda count [52]. With the existence of a prime member, it forces councillors to be explicit in their votes or have their vote counted for whatever is voted on by the prime.

Voting for councillors requires locking 5 DOT tokens (the native token of the platform) and takes on an approval voting approach. A token-holder can approve up to 16 different councillors and the vote will be equalised among the chosen group, with each council term lasting 7 days. The approval voting method used is the weighted Phragmén election algorithm (e.g. [53], where the candidates with most approvals are elected and, afterwards, a process is run that redistributes the vote amongst the elected set. This reduces the variance in the list of backing stake from the voters to the elected candidates in order to ensure that the minimum amount of tokens required to join the council is as high as possible. Running the Phragmén algorithm cannot be completed within the time limits of production of a single block. And waiting would jeopardise the constant block production time of the network. Therefore, as much computation as possible is moved to an off-chain worker, where validators can work on the problem without impacting block production time. An in-house refinement of Phragmén called Phragmms [54] could be used in the future.

A significant part of Polkadot's governance is the *technical committee*, which is composed of teams that have successfully implemented or specified either a *Polkadot runtime* or *Polkadot Host* [38]. These teams are added or removed from the technical committee via simple majority votes within the council. The technical committee can, along with the council, propose emergency referendums, which are fast-tracked for voting and implementation (e.g., for emergency bug fixes)

Besides electing councillors, token-holders get to vote in referendums. Each referendum has a specific proposal associated with it. Proposals can implement backward-compatible or backward-incompatible changes. Proposals can be submitted by token-holders, the council or the technical committee:

- For token-holders to submit a proposal, a minimum amount of tokens must be deposited. If another token-holder agrees with the proposal, they can also deposit the same amount of tokens in the proposal's support. The proposal with the highest amount of bonded support will be selected to be a referendum in the next voting cycle. The referendum, in this case, will have positive turnout bias. That is, the smaller the amount of stake voting, the larger the super-majority necessary for it to pass [38]. Specifically the proposal would pass if
$$\frac{\text{against}}{\sqrt{\text{turnout}}} < \frac{\text{approve}}{\sqrt{\text{electorate}}}.$$
- Proposals can only be submitted by the council through a majority or unanimously. In the case of a unanimous council, the referendum will have a negative turnout bias, that is, the smaller the amount of stake voting, the smaller the amount necessary for it to pass:
$$\frac{\text{against}}{\sqrt{\text{electorate}}} < \frac{\text{approve}}{\sqrt{\text{turnout}}}.$$
In the case of a majority, the referendum will be a majority-carries vote (51% of the votes is required to win).
- The technical committee can propose emergency referendums subject to approval from the council.

If a proposal passes in a referendum, then Polkadot's logic automatically schedules it for enactment: autonomous enactment. This is unlike other systems where miners or validators often have unilateral power to prevent protocol changes by refusing to upgrade software. Proposals submitted by the council or token-holders are enacted 28 days after the referendum, whereas ones submitted by the technical committee can be enacted immediately.

To vote, a token-holder generally must lock their tokens up for at least the enactment delay period beyond the end of the referendum. This is in order to ensure that some minimal economic buy-in exists and to dissuade vote selling. It is possible to vote without locking at all, but the vote is worth a small fraction of a normal vote. It is also possible to voluntarily lock for more than one enactment period, in which case, the weight of the vote increases proportionally. This mechanism exists to ensure that users with little stake but strong opinions can express their conviction in referendums.

- **Confidentiality**:
  - **Secrecy**: Votes on Polkadot, whether it's in electing councillors, internal council votes, or voting in referenda, are not documented to be private. Therefore, secrecy is *not* satisfied.
  - **Pseudonymity**: Participants are not required to reveal their real-life identities to participate in the decision-making process.Therefore pseudonymity *is* satisfied.
  - **Coercion-resistance**: Since secrecy is *not* satisfied, coercion-resistance is *not* satisfied by definition.
- **Verifiability**. Since the votes and final tally are all public, verifiability *is* satisfied.
- **Pareto Efficiency**. Council elections and referenda voting functions are Pareto efficient. However, veto-ing is not Pareto efficient where there is 100% consensus in a referendum. This is an extreme case however. The voters have the ability to lock their votes for an extended time, to signal the strength of their preferences. For all intents and purposes governance *is* Pareto efficient.
- **Accountability**. 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. Therefore, accountability *is* satisfied.
- **Sustainability**: There are no explicit or direct incentives/rewards given for participation or contribution.

Therefore, *neither* sustainable development or sustainable participation are satisfied.

- **Liveness**. The Polkadot governance mechanism is capable of taking in inputs of urgency (i.e. emergency referenda) 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. Therefore, liveness *is* satisfied.
- **Suffrage**: 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 referenda) 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. Therefore, meritocratic suffrage is only *slightly* satisfied.

E. Decred

Decred is a hybrid proof-of-work and proof-of-stake system that is mostly on-chain governed [55]. Such a hybrid implementation results in three main types of stakeholders: miners, voters and regular users. All three participate pseudo-anonymously. To have decision-making powers (in governance and block-validation), participants need to have 'tickets', which are bought or acquired through time-locking DCR (the native token of the platform). We will not go through the details of a ticket lifecycle, but the process is thoroughly outlined in [55]. Each block contains 5 pseudo-randomly sampled tickets (i.e. 5 votes).

Proposals can be handled either by an on-chain or off-chain procedure. Specifically, proposals regarding high level issues or that require funds from the Decred Treasury are handled off-chain. They first appear in Politeia, the system's deliberation platform, to be discussed throughout the community. Admins of the platform can flag spam proposals or comments. When a proposal owner decides to put their proposal for a vote, the admins of the platform can then trigger the start of off-chain voting. A snapshot of the currently bought tickets takes place 256 blocks before the start of voting. Then, the ticket-voting interval of 2,016 blocks (approximately 1 week) formally begins, which means 10,080 pseudo-randomly sampled tickets have the opportunity to vote. Voting on Politeia is not recorded on chain, but it is still backed by cryptographic techniques which prevent Sybil attacks and unfair censorship. When the ticket-voting period ends, the proposal is formally approved or rejected. There is a quorum requirement for a vote to be considered valid: 20% of the eligible tickets must vote 'Yes' or 'No'. The threshold for a proposal to be approved is 60% 'Yes' votes. When a proposal with a budget and deliverables is approved, work can begin. The proposal owner can submit claims against the budget as deliverables are completed.

The on-chain type of proposals is also called Decred Change Proposal (DCP) [56], which are about updating the consensus mechanism. With a DCP, the proposed node software must be developed and released. The new code will lie dormant until the change has been voted upon and accepted by the proof-of-stake voters. Each voting interval lasts for 8,064 blocks, which makes the maximum number of votes 40,320. A ticket can vote to accept the rule change, to reject it or to abstain (the default choice). Every vote has a quorum requirement of 10%. This means that at least 10% of all votes cast must be non-abstain for the result to be considered valid. If all non-abstaining votes fail to meet a 75% Yes or No majority threshold, the agenda vote remains active for next voting period. If 75% of all non-abstaining votes accept the proposal, the agenda is considered locked in and the consensus changes will activate 8,064 blocks (4 weeks) after the vote passed. If 75% of all non-abstaining votes reject the proposal, the agenda fails and the consensus changes will never activate. If an agenda reaches its expiration before ever reaching a 75% majority vote, the agenda expires and the consensus changes will never activate. After a ticket has voted, missed, or expired, the funds cannot be released for another 256 blocks.

If the quorum requirement is met, and more than 75% of the votes are in favour of activating the new consensus rules, then a 'lock-in' period begins of 8,064 blocks. During this period, all participants in the Decred network must upgrade their software to the latest version. All full nodes participating in the network will automatically activate the new rules on the first block after this period, so any nodes still running the old software will no longer be able to participate. Throughout the process, it is possible to verify the voting preference of a ticket.

With this brief overview in mind, we can now perform evaluations of Decred's governance against our proeprties.

- **Confidentiality**:
  - **Secrecy**: There are no explicit secrecy guarantees in the voting process. Therefore, secrecy is *not* satisfied.
  - **Pseudonymity**: Participants (miners, voters, and regular users) are not required to reveal their real-life identities to participate in the decision-making process. Therefore pseudonymity *is* satisfied.
  - **Coercion-resistance**: Since secrecy is NOT satisfied, coercion-resistance is *not* satisfied by definition.
- **Verifiability**. Since the votes and final tally are all public, verifiability *is* satisfied.
- **Pareto Efficiency**. If a proposal vote occurs with a quorum of less than 10%, the proposal will not pass, even when it receives one or more approval votes. Furthermore, given the role of Politeia, it is unlikely that a truly controversial proposal will pass. Therefore, the most likely 'suboptimal' outcome is not selecting any proposal, when one might have had some support. Therefore, Pareto efficiency is *somewhat* satisfied.
- **Accountability**. Although funds from the ticket cannot be released until 256 blocks after voting, the changes to the consensus rules are not applied until after 8,064 blocks. This implies that if a voter or a group of voters voted in a malicious proposal, they can withdraw their locked funds before the proposal is enacted. Therefore, accountability is *not* satisfied.

- **Sustainability**: *Sustainable Development*. Although there is no explicit incentive or reward given to the proposing group or individual, it is the responsibility of the proposer to request the amount which represents the value of their work. Therefore, sustainable development *is* satisfied.
- **Sustainability**: *Sustainable Participation*. Although voters can gain rewards from their tickets via validating blocks as part of the consensus protocol [55], there are no explicit additional incentives for voting (or participating in the governance process). Therefore, sustainable participation is *not* satisfied.
- **Liveness**. Given the lack of flexibility of the on-chain governance model, it is incapable of taking inputs of urgency and responding to them in accordance to the severity of the issue. Therefore, liveness is *not* satisfied.
- **Suffrage**. Since voting eligibility depends on only buying proof-of-stake tickets, token-based suffrage *is* satisfied.

F. Compound

Compound [57] is a protocol running on the Ethereum blockchain that establishes money markets. These are collections of Ethereum assets (e.g. Ether, ERC-20 stablecoins, coins like DAI or ERC-20 utility coins such as Augur) that users can supply and borrow. These assets have algorithmically defined interest rates, dependent on supply and demand, that users collect or pay when supplying and borrowing respectively. Users can borrow depending on the value of the underlying asset they have as collateral and repay at any rate they want, paying the accrued interest. This provides the ability to quickly switch between tokens without putting trust in a centralized authority.

Governance in Compound is fuelled by an ERC-20 compatible token called COMP [58]. The maximum number of COMP tokens is capped at 10000000. About 4200000 of them are distributed to the community at a rate of 2312 per day. Of those, a fixed fraction of these tokens is allocated to every market on Compound, half of which goes to suppliers and the other half to borrowers and subsequently allocated proportionately within each group. Additionally, 2400000 tokens belong to the Compound Labs Inc. shareholders, 2200000 are allocated over 4 years to the Compound team (with an additional 320000 reserver for future members) and finally 775000 are reserved for the community.

In addition to exchanging their tokens, holders of COMP can also use them to delegate voting power and create *government* proposals. COMP tokens can be delegated to other addresses at rate of 1 vote per token, or delegated to oneself for a direct vote. A government proposal can then be created by any address holding at least 65000 COMP. On top of that, any address with 100 COMP can create an *autonomous* proposal, which in turn can become a government proposal once that address receives 65000 COMP or more in delegation. A government proposal is an executable piece of code, which could update some parameter (e.g. the rate at which COMP tokens are distributed), create a new money market or provide additional functionality to the Compound smart contracts. A single address cannot issue multiple proposals in parallel.

The governance process is controlled by two smart contracts: Governor Bravo and Timelock. Once a government proposal is created, it is put into a two day review period, followed by an election lasting 3 days. COMP holders can vote for or against the proposal, which passes if the majority was in favour *and* it received more than 400000 votes in total. After that, it is put in Timelock for a mandatory 2 day waiting period, before it is executed. At any point prior to execution, the creator of the proposal (or any address if the creator has fewer than 650000 COMP) can cancel the process.

With this brief overview in mind, we can now perform evaluations of Compound's governance against our set of properties.

- **Confidentiality**:
  - **Secrecy**: Every step of the governance process, such as proposing, voting or delegating is on-chain, by interacting with smart contracts on Ethereum. This done through possibly pseudonymous addresses and is public and unencrypted. Therefore secrecy is *not* satisfied.
  - **Pseudonymity**: Users participate using their Ethereum address, therefore pseudonymity *is* satisfied.
  - **Coercion-resistance**: Since secrecy is NOT satisfied, coercion-resistance is *not* satisfied by definition.
- **Verifiability**. Since the votes and final tally are all public, verifiability *is* satisfied.
- **Pareto Efficiency**. Once a proposal enters the voting phase, the voters only have two options: yes or no. This is clearly Pareto efficient and aligned with their incentives. Things get more tricky once there are multiple incompatible options (e.g., values of a specific parameter). In this case the 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).
- **Accountability**. Once a proposal is executed, its creator and voters are completely independent from its future. Therefore, accountability is *not* satisfied.
- **Sustainability**: *Sustainable Development*. There is no mechanism to reward development efforts: the proposal should already be complete and executable. Therefore, sustainable development is *not* satisfied.
- **Sustainability**: *Sustainable Participation*. Although COMP tokens have an value and can be traded, there are no additional reward for voting or creating a government proposal. Therefore, sustainable participation is *not* satisfied.
- **Liveness**. 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 is reasonable: in addition, if an exploit is found while in Timelock, the proposer can cancel it. Failing to do so, the users of Compound have some time to either move their assets or fork. However, this window for immediate action is only open right after a vote. Therefore, liveness is *somewhat* satisfied.

- **Suffrage**. 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.

G. *Uniswap*

We briefly sketch Uniswap [59] governance, which combines off and on-chain components. The on-chain part of its governance system is almost identical to Compound section III-F, using the UNI token instead, which is minted and distributed similar to COMP. However, UNI can also be used to empower on-chain processes, which precede the on-chain votes. Interestingly, the current distribution of UNI tokens is used to weigh voting power in the off-chain processes as well.

The off-chain discourse takes place on the Uniswap governance forum, where 2 types of posts have particular significance. The first is the Temperature Check, whose goal is to gauge interest in changing the status quo. After 3 days there is a poll, where users have vote according to the amount of UNI they hold on-chain. If a majority is reached and more than 25000 UNI voted yes, a Consensus Check is created on the same forum. During the 5 day duration of the Consensus Check, a proposal needs to be fleshed out. In the end, a second poll is brought before the users, this time possibly containing many alternatives. As long as the highest ranked alternative receives more than 50000 UNI, an on-chain Governance Proposal is created and handled in the same way as in Compound, using the Governor Bravo smart contract.

To summarize, the evaluations of Uniswap and Compound are identical, but perhaps the governance process of Uniswap ensures that voters are better informed about upcoming proposals.

H. *Maker DAO*

Maker DAO [60] is a decentralized organization running on Ethereum and based on the Maker Protocol. It employs a two-token system, using Dai and MKR, both of which are ERC-20 compatible. The first, DAI, is a collateral-backed stablecoin which is soft-pegged to the U.S. dollar and is collateralized by a *mix* of other cryptocurrencies. The second, MKR, is a governance token is used by stakeholders to maintain the system and manage Dai. However, in addition to the previous governance token models, MKR, which is *not* a stablecoin, is also used to control the price of Dai, by creating favourable exchange rates between the two coins, depending on Dai supply and demand. In particular, 1000000 MKR were originally minted. The total supply is then kept as close to this number as possible, by burning or minting new tokens in exchange for Dai.

The governance model employed [61] combines some of the features of Compound (such as on-chain voting for some issues, executable proposals and a mandatory waiting period) and some off-chain features of Uniswap (such as forum discussions). Note that the two components are *not* officially coupled. The off-chain component takes place at the Maker DAO forum, which is public. In addition to usual forum posts, users can (and are encouraged to) create a *Forum Signal Thread*. The purpose is to get community feedback on some issue, possible on-chain proposals or generally any potential improvement to Maker DAO. At the end, the Forum Signal Thread is followed by a poll, where users vote pseudonymously. Every user has *one* vote, irrespective on the amount of MKR they may have. The intended function is that the discussion and poll results will inform the choices of an upcoming *on-chain* governance action.

There are two on-chain processes facilitated by smart contracts: *Governance Polls* and *Executive Votes*. The aim of Governance Polls is to ratify Forum Signal Threads, formally gauge consensus about important topics and select one of many alternative designs before an Executive Vote. The Governance Poll could contain multiple options and holders of MKR vote using instant-runoff. Governance Polls usually stay open for 3 to 7 days. The results of Governance Polls can then be turned into Executive Votes, although both processes could be initiated by any Ethereum address at any point. However, only Governance Facilitators can link specific Governance Polls and Executive Votes in the official forum.

The Executive Vote is the only way to enact changes on the smart contracts supporting of Maker DAO. Indeed, an Executive Vote should contain instructions to amend their code with the proposed set of changes. Executive Votes are selected via *continuous* approval voting, typically without having a fixed voting window. Specifically, holders of MKR can change their vote at any time and the Executive Vote with the highest approval would win. However, once an Executive Vote that was implemented loses to another one, it is deactivated and the only way to revert to the previous status is through a new vote. Once a new Executive Vote wins, the Governance Security Module imposes a 24 hour waiting period, during which the vote can be reversed.

Maker DAO also makes use of Emergency Shutdown. At any point if a total of 50000 MKR are deposited into the Emergency Shutdown Module, an Emergency Shutdown is triggered. These coins are immediately burned and the Maker Protocol is shut down. Then, collateral supporting Dai (as well as the coins themselves) are returned to their owners. For various reasons, Dai takes lower priority than collateral and could be exchanged for less than 1$ per Dai.

- **Confidentiality**:
  - **Secrecy**: Every step of the governance process, such as proposing, voting or delegating is on-chain, by interacting with smart contracts on Ethereum. This

done through possibly pseudonymous addresses and is public and unencrypted. Therefore secrecy is *not* satisfied.
  - **Pseudonymity**: Users participate using their Ethereum address. Therefore, pseudonymity *is* satisfied.
  - **Coercion-resistance**: Since secrecy is NOT satisfied, coercion-resistance is *not* satisfied by definition.
- **Verifiability**. Since the votes and final tally are all public, verifiability *is* satisfied.
- **Pareto Efficiency**. For Executive Votes, the voters only have two options: to vote yes or no. Even though these do not have to follow Governance Polls, the ranked-choice, instant runoff voting mechanism used there gives the voters the option to choose between multiple alternatives, avoiding the possibility of a sequential vote (e.g., as could happen in Compound). Therefore, Pareto Efficiency is *mostly* satisfied.
- **Accountability**. Once a proposal is executed, its creator and voters are completely independent from its future. Therefore, accountability is *not* satisfied.
- **Sustainability**: *Sustainable Development*. There is no mechanism to reward development efforts: the proposal should already be complete and executable. Therefore, sustainable development is *not* satisfied.
- **Sustainability**: *Sustainable Participation*. MKR are crucial for Maker DAO as they help maintain the peg with Dai. However, the extra energy spent on deciding what to vote on is not explicitly compensated. Therefore, sustainable participation is *not* satisfied.
- **Liveness**. An Executive Vote can be implemented in 24 hours, once it receives enough votes. This gives both the ability to quickly prevent a bad proposal and relatively quickly enact a better one. In addition, there is also an Emergency Shutdown functionality. Therefore, liveness *is* satisfied.
- **Suffrage**. Since voting eligibility is only guaranteed to MKR token holders, token-based suffrage *is* satisfied.

Treasury Systems

Project Catalyst and Dash also include a *treasury*, which complicates the voting process. Funds are periodically collected by the normal blockchain operation and allocated to fund its development and undertake projects *whose results may take months to materialize*. In addition, at every funding round more than one proposal may be selected, as long as their total cost does not exceed a budget. As such, the voters need additional flexibility to signal their preferences. Specifically, they not only need to consider if a proposal is good in isolation, but they need to compare it with its budget and think about the opportunity cost of funding it. This is closely related to the field of *Participatory Budgeting* (e.g., [62, 63, 64]).

I. Project Catalyst

Project Catalyst [65] is the on-chain governance system used by the Cardano blockchain. The role of Project Catalyst is to provide a mechanism through which users can collectively decide how Cardano's treasury funds should be allocated.

Governance in Project Catalyst occurs in 12 week intervals, called *Funds*. There are 4 primary types of agents participating: proposers, voters, Community Advisors (CA's) and Veteran Community Advisors (vCA's). Additionally, people can participate by referring projects to be funded and designing challenges that need to be addressed. At the beginning of each fund a set of challenges is issued, either by users of Cardano or the Project Catalyst team. Then, the proposers offer proposals, which may, but are not required to, address a specific challenge. The proposals should contain a detailed set of goals, along with a specific plan to achieve them and a required budget. Then, the community advisors write reviews for any proposal they chose to, focusing on impact, implementability and auditability. These reviews are then reviewed again by the veteran community advisors and are assigned a grade that can be 'Excellent', 'Good' or 'Filtered Out', the last reserved for particularly uninformative reviews. Having all this information, the voters can vote 'Yes', 'No' or 'Abstain' for as many proposals as they want. Each vote has weight proportional to the users stake in ADA, which is the currency used by Cardano. Project Catalyst implements *fuzzy threshold voting* [19]. Voters express a 'Yes', 'No' or 'Abstain' opinion for each proposal. A proposal passes if the number of 'Yes' votes minus the number of 'No' votes is at least 5% of the total votes it received. The winning proposals are awarded their funds in the order of the margin by which they are passing, until either the entire budget is allocated or no more passing proposals exist. If a proposal has passed the voting threshold but insufficient funds remain to pay the full amount requested, it will not receive partial funding. Instead, any smaller proposals which have also passed the threshold that will fit in the budget will be funded, even if they have lower net approval than the larger proposal.

All agents involved in Project Catalyst are rewarded in some capacity. At every Fund each reward pool corresponds to a set percentage of the total. As a concrete example we will examine Fund7, which had total budget of $8000000 in ADA. This amount was further broken down as follows:

- $80\% \rightarrow$ $6400000 for funding proposals
- $13\% \rightarrow$ $1040000 for voting rewards.
- $4\% \rightarrow$ $320000 for community advisors
- $1\% \rightarrow$ $80000 for veteran Community Advisors.
- $1\% \rightarrow$ $80000 for referral rewards.
- $1\% \rightarrow$ $80000 for challenge teams rewards.

Any user with more than 500 ADA can become a voter. This is measured by a snapshot of the stake distribution taken before the election, but the funds are not locked. Each voter receives voter rewards proportional to their stake. Community advisors receive rewards relative to the quality of the reviews, but also depending on how many other reviews were written for the proposals they reviewed. An 'Excellent' review provides 3 times the reward of a 'Good' review and each proposal has rewards for 2 'Excellent' and 3 'Good' reviews. If these rewards are not enough to cover the reviews, a lottery is used. Veteran community advisors are rewarded equally, provided they reviewed a minimum number of reviews. Proposers are not rewarded explicitly, but can manage the funds received by their proposal and have to periodically submit progress reports to the community. The performance of community advisors and veteran community advisors is recorded, but there is no currently defined on-chain mechanism for a voter to become either of those. The promotion from voter (or proposer) to community advisor to veteran is centralized.

- **Confidentiality**:
  - **Secrecy**: Everyone participates in Project Catalyst using their wallet address. Proposers, community advisors and veteran community advisors participate publicly. Voters submit *encrypted* ballots (padded with some randomness), using the public key issued by a committee. Then, these votes are tallied and the result is decrypted by the committee, if a majority of its members agrees. Furthermore, if the wallet address is linked to a real identity, the only information available is that this particular person voted, but the actual vote is still secret. Therefore the vote is *mostly* secret.
  - **Pseudonymity**: Voters participate with their wallet address, therefore pseudonymity *is* satisfied.
  - **Coercion-resistance**: The system is somewhat coercion resistant. The ballot itself cannot be decrypted by the voter. Additionally, if the random padding is not kept, it is impossible even for the voter to convince anyone of the way they voted.
- **Verifiability**. The result of the vote can be independently verified. In addition, as long as a voter saved the random padding, they can verify that their particular vote was counted. Without the padding this is impossible, as the votes *cannot* be decrypted. Therefore, there is a (somewhat contrived) sequence of events after which a voter would be unable to check that their ballot has been added. As such, verifiability is only *mostly* satisfied.
- **Pareto Efficiency**. In some cases, proposals with less approvals 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. This could happen even if the most preferable outcome for every voter is to fund both cost 50 proposals. Additionally, there is an incentive for each voter to submit an uninformative 'no' vote to many proposals, in order to maximize the winning chance of their favourites. A potential mitigation would be to use techniques from Participatory Budgeting [63] and Distortion [66], 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. In total, Pareto Efficiency is only *somewhat* satisfied.
- **Accountability**. There are no explicit, on or off-chain, penalties. Proposers need to submit periodic progress reports about their projects to keep receiving funding. Similarly, community advisors and veteran community advisors can be penalized for poor reviews or absence. As these are either centralized or community-driven without clearly described mechanisms, accountability is mostly *not* satisfied.
- **Sustainability**: *Sustainable Development*. Although there is no explicit incentive or reward given to the proposing group or individual, it is the responsibility of the proposer to request the amount which represents the value of their work. Therefore, sustainable development *is* satisfied.
- **Sustainability**: *Sustainable Participation*. Since all parties are rewarded for participating in the governance process and to an extent receive larger rewards for additional effort (e.g. community advisors and review quality), sustainable participation *is* satisfied.
- **Liveness**. Project Catalyst is primarily used for allocating treasury funds and each Fund follows a 12 week timeline. As such, liveness is *not* satisfied: even though the funds can be released in accordance with each proposal's progress, there is no direct mechanism to take urgent action. However, liveness is arguably not required for its purposes.
- **Suffrage**. Since voting eligibility depends on only having at least 500 ADA, token-based suffrage *is* satisfied. There are no guaranteed voting rights based on previous positive contributions. However, community advisors and veteran community advisors can affect the outcome of the votes through their reviews. Meritocratic suffrage is *slightly* satisfied.

J. Dash

Like Bitcoin, Dash [67] uses a proof-of-work consensus mechanism. However, Dash's approach to governance takes a formal, on-chain form. The Dash Governance System (DGS) uses a 'budget and masternode voting system' to govern and fund the underlying blockchain's development and maintenance. Masternodes are nodes that can place at least a $1,000$ DASH, the platform's native token, as a collateral to participate in the governance process. Each masternode has a single, public, approval-vote expressing which improvement proposals the masternode approves of. In each voting cycle (which is roughly a month long), project proposals are submitted and then voted on. Even though anyone can submit a proposal, doing so comes at a cost of 5 DASH to ensure that only serious proposals are voted on.

The DGS implements a system very similar to Project Catalyst with one difference: A proposal is eligible for funding if the number of 'Yes' votes minus the number of 'No' votes is at least 10% of the *total* masternode count. Additionally, if there are two proposals with the same approval, then the one with a larger proposal transaction hash is ranked higher. The treasury is funded through various channels. When new blocks are mined, 45% of the block reward is reserved for the miner, 10% for the budget and 45% for the masternodes' reward. We now perform evaluations of the DGS against the properties developed in Section II.

- **Confidentiality**:
  - **Secrecy**: Since the masternodes vote publicly, the DGS does *not* satisfy secrecy.
  - **Pseudonymity**: Masternodes are not required to reveal their real-life identities to participate in the governance process; therefore pseudonymity is satisfied.
  - **Coercion-resistance**: Since masternode votes are tied to their chosen pseudo-identities, coercion-resistance is *not* satisfied.
- **Verifiability**. Since the votes and final tally are all public, verifiability is, by definition, satisfied.
- **Pareto Efficiency**. As with Project Catalyst, Pareto Efficiency is only *somewhat* satisfied.
- **Accountability**. Although masternodes are required to lock 1000 DASH to vote, if a group of masternodes vote in a malicious proposal, they will face no negative consequences and will be able to unlock their funds before the malicious proposal is enacted. Therefore, accountability is *not* satisfied.
- **Sustainability**: *Sustainable Development*. Although there is no explicit incentive or reward given to the proposing group or individual, it is the responsibility of the proposer to request the amount which represents the value of their work. Therefore, sustainable development *is* satisfied.
- **Sustainability**: *Sustainable Participation*. Since 45% of the mining reward is kept as a reward for masternodes for their participation in the governance process. Therefore, sustainable participation is satisfied.
- **Liveness**. Given the lack of flexibility of the on-chain governance model, the DGS is incapable of taking inputs of urgency and responding to them in accordance to the severity of the issue. Although a Github issue or a pull request could be initiated without going through the formal on-chain route, it is still not the officially defined way by which the system processes inputs. Therefore, liveness is *not* satisfied.
- **Suffrage**. Since voting eligibility depends on only having at least 1000 DASH, token-based suffrage is satisfied.

IV. Conclusion

In this systematization work we focused on documenting a comprehensive list of 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. It is worth saying that there are also other platforms that we have attempted to cover, but these were either too poorly documented or were yet to implement governance mechanisms, thus we consider the list a comprehensive coverage of popular blockchain systems at the time of writing.

The main outcome of the systematization effort, as illustrated in table I, is that in many ways all current blockchain platforms either have significant deficiencies in their governance processes or they allow significant room for improvement. It is worth also 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.

V. Acknowledgements

We would like to thank Yussef Soudan for his extensive research and participation in many meetings during the earlier stages of this work. Additionally, we thank Roman Oliynykov for providing many details and insights regarding the evaluation of Project Catalyst.

References

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] Divisions of Corporation Finance and Enforcemen. 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/34-81207.pdf.

[3] Almost $500,000 in Ethereum Classic coin stolen by forking its blockchain, Dan Goodin, 1/8/2019, Arstechnica.

[4] 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.eods.eu/library/CoE_Recommentaion%20on%20Legal,%20Operational%20and%20Technical%20Standards%20for%20E-voting_2004_EN.pdf.

[5] 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_I.pdf.

[6] V. Buterin, Moving beyond coin voting governance, August, 2021. Accessed on: October 1, 2021. Available: https://vitalik.ca/general/2021/08/16/voting3.html.

[7] 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.

[8] Wharton Cryptogovernance Workshop. Accessed on: October 19, 2021. Available: https://cryptogov.net.

[9] R. v. 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.

[10] 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.

[11] P. De Filippi and G. McMullen, "Governance of blockchain systems: Governance of and by distributed infrastructure," 2018.

[12] Y.-Y. Hsieh, J.-P. J. Vergne, and S. Wang, "The internal and external governance of blockchain-based organizations: Evidence from cryptocurrencies," pp. 48–68, 2017.

[13] D. W. Allen and C. Berg, "Blockchain governance: What we can learn from the economics of corporate governance," *Allen, DWE and Berg, C (Forthcoming)'Blockchain Governance: What can we Learn from the Economics of Corporate Governance*, 2020.

[14] N. Khan, T. Ahmad, A. Patel, and R. State, "Blockchain governance: An overview and prediction of optimal strategies using nash equilibrium," *arXiv preprint arXiv:2003.09241*, 2020.

[15] S. Venugopalan and I. Homoliak, "Always on voting: A framework for repetitive voting on the blockchain," *arXiv preprint arXiv:2107.10571*, 2021.

[16] H. Gersbach, A. Mamageishvili, and M. Schneider, "Vote delegation and misbehavior," *arXiv preprint arXiv:2102.08823*, 2021.

[17] J. D. Cohen and M. J. Fischer, "A robust and verifiable cryptographically secure election scheme (extended abstract)," in *26th Annual Symposium on Foundations of Computer Science, Portland, Oregon, USA, 21-23 October 1985*. IEEE Computer Society, 1985, pp. 372–382. [Online]. Available: https://doi.org/10.1109/SFCS.1985.2

[18] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in *Towards Trustworthy Elections*. Springer, 2010, pp. 37–63.

[19] B. Zhang, R. Oliynykov, and H. Balogun, "A treasury system for cryptocurrencies: Enabling better collaborative intelligence," in *The Network and Distributed System Security Symposium 2019*, 2019.

[20] E. Cuvelier, O. Pereira, and T. Peters, "Election verifiability or ballot privacy: Do we need to choose?" in *European Symposium on Research in Computer Security*. Springer, 2013, pp. 481–498.

[21] R. Gharadaghy and M. Volkamer, "Verifiability in electronic voting-explanations for non security experts," in *4th International Conference on Electronic Voting 2010*. Gesellschaft für Informatik eV, 2010.

[22] V. Cortier, D. Galindo, R. Küsters, J. Mueller, and T. Truderung, "Sok: Verifiability notions for e-voting protocols," in *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016, pp. 779–798.

[23] J. C. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections (extended abstract)," in *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing, 23-25 May 1994, Montréal, Québec, Canada*, F. T. Leighton and M. T. Goodrich, Eds. ACM, 1994, pp. 544–553. [Online]. Available: https://doi.org/10.1145/195058.195407

[24] J. Benaloh, "Simple verifiable elections," in *2006 USENIX/ACCURATE Electronic Voting Technology Workshop, EVT'06, Vancouver, BC, Canada, August 1, 2006*, D. S. Wallach and R. L. Rivest, Eds. USENIX Association, 2006. [Online]. Available: https://www.usenix.org/conference/evt-06/simple-verifiable-elections

[25] A. Kiayias, T. Zacharias, and B. Zhang, "Ceremonies for end-to-end verifiable elections," in *Public-Key Cryptography - PKC 2017 - 20th IACR International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, The Netherlands, March 28-31, 2017, Proceedings, Part II*, ser. Lecture Notes in Computer Science, S. Fehr, Ed., vol. 10175. Springer, 2017, pp. 305–334. [Online]. Available: https://doi.org/10.1007/978-3-662-54388-7_11

[26] J. Alwen, R. Ostrovsky, H. Zhou, and V. Zikas, "Incoercible multi-party computation and universally composable receipt-free voting," in *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, ser. Lecture Notes in Computer Science, R. Gennaro and M. Robshaw, Eds., vol. 9216. Springer, 2015, pp. 763–780. [Online]. Available: https://doi.org/10.1007/978-3-662-48000-7_37

[27] F. Brandt, V. Conitzer, and U. Endriss, "Computational social choice," *Multiagent systems*, pp. 213–283, 2012.

[28] K. J. Arrow, "A difficulty in the concept of social welfare," *Journal of political economy*, vol. 58, no. 4, pp. 328–346, 1950.

[29] A. Gibbard, "Manipulation of voting schemes: a general result," *Econometrica: journal of the Econometric Society*, pp. 587–601, 1973.

[30] M. A. Satterthwaite, "Strategy-proofness and arrow's conditions: Existence and correspondence theorems for voting procedures and social welfare functions," *Journal of economic theory*, vol. 10, no. 2, pp. 187–217, 1975.

[31] R. L. Rivest and E. Shen, "An optimal single-winner preferential voting system based on game theory," in *Proc. of 3rd International Workshop on Computational Social Choice*. Citeseer, 2010, pp. 399–410.

[32] B. Kluiving, A. de Vries, P. Vrijbergen, A. Boixel, and U. Endriss, "Analysing irresolute multiwinner voting rules with approval ballots via sat solving," in *ECAI 2020*. IOS Press, 2020, pp. 131–138.

[33] J. J. Bartholdi and J. B. Orlin, "Single transferable vote resists strategic voting," *Social Choice and Welfare*, vol. 8, no. 4, pp. 341–354, 1991.

[34] M. Balinski and R. Laraki, "Majority judgment," *Cambridge/Mass*, 2011.

[35] C. A. Dykstra, "The quest for responsibility," *American Political Science Review*, vol. 33, no. 1, p. 1–25, 1939.

[36] R. W. Grant and R. O. Keohane, "Accountability and abuses of power in world politics," *American political science review*, vol. 99, no. 1, pp. 29–43, 2005.
[37] D. F. Sacco, S. V. Bruton, M. Brown, and M. M. Medlin, "Skin in the game: Personal accountability and journal peer review," *Journal of Empirical Research on Human Research Ethics*, vol. 15, no. 4, pp. 330–338, 2020, pMID: 32425095. [Online]. Available: https://doi.org/10.1177/1556264620922651
[38] D. Salman, Governance, Polkadot Wiki, September 17, 2021. Accessed on: October 1, 2021. Available: https://wiki.polkadot.network/docs/learn-governance.
[39] B. R. Taylor, "The psychological foundations of rational ignorance: biased heuristics and decision costs," *Constitutional Political Economy*, vol. 31, no. 1, pp. 70–88, 2020.
[40] Y. Zhang and M. van der Schaar, "Reputation-based incentive protocols in crowdsourcing applications," in *2012 Proceedings IEEE INFOCOM*, 2012, pp. 2140–2148.
[41] 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.
[42] D. Siddarth, S. Ivliev, S. Siri, and P. Berman, "Who watches the watchmen? a review of subjective approaches for sybil-resistance in proof of personhood protocols," *Frontiers in Blockchain*, vol. 3, p. 46, 2020.
[43] S. P. Lalley and E. G. Weyl, "Quadratic voting: How mechanism design can radicalize democracy," vol. 108, pp. 33–37, 2018.
[44] 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-e39db233c28e.
[45] L. Dashjr, BIP Process, github.com, February, 4, 2016. Accessed on: October 14, 2021. Available: https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki.
[46] 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.
[47] P. Wuille, 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/blob/master/bip-0009.mediawiki.
[48] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform", github.com, 2013. Accessed on: November 15, 2021. Available: https://ethereum.org/en/whitepaper/.
[49] M. Becze, H. Jameson, et al., "EIP-1: EIP Purpose and Guidelines," Ethereum Improvement Proposals, no. 1, October 2015. Accessed on: November 15, 2021. [Online serial]. Available: https://eips.ethereum.org/EIPS/eip-1.
[50] "*Tezos Docs*", September 9, 2016. Accessed on: October 23, 2021. Available: https://gitlab.com/tezos/tezos/-/tree/master/docs.
[51] "Protocol Granada", January 24, 2021. Accessed on: October 23, 2021. Available: https://gitlab.com/tezos/tezos/-/commits/master/docs/protocols/010_granada.rst.
[52] P. Emerson, "The original borda count and partial voting," *Social Choice and Welfare*, vol. 40, 02 2013.
[53] M. Brill, R. Freeman, S. Janson, and M. Lackner, "Phragmén's voting methods and justified representation," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 31, no. 1, 2017.
[54] A. Cevallos and A. Stewart, "A verifiably secure and proportional committee election rule," in *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, 2021, pp. 29–42.
[55] "Decred Documentation", April 26, 2016. Accessed on: November 16, 2021. Available: https://github.com/decred/dcrdocs.
[56] "Decred Change Proposals", May 6, 2017. Accessed on: November 21, 2021. Available: https://github.com/decred/dcps.
[57] R. Leshner, G. Hayes, "Compound: The Money Market Protocol", compound.finance, 2019. Accessed on: November 16, 2021. Available: https://compound.finance/documents/Compound.Whitepaper.pdf.
[58] Coinbase Statistics on COMP, Accessed on: December 1, 2021. Available: https://coinmarketcap.com/currencies/compound/.
[59] H. Adams, N. Zinsmeister, M. Salem, R. Keefer, D. Robinson, "Uniswap v3 Core", 2021. Accessed on: November 16, 2021. Available: https://uniswap.org/whitepaper-v3.pdf.
[60] The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System. Accessed on: November 16, 2021. Available: https://makerdao.com/en/whitepaper.
[61] Maker Governance. Accessed on: October 18, 2021. Available: https://vote.makerdao.com/.
[62] H. Aziz and N. Shah, "Participatory budgeting: Models and approaches," 2020.
[63] G. Benade, S. Nath, A. D. Procaccia, and N. Shah, "Preference elicitation for participatory budgeting," *Management Science*, vol. 67, no. 5, pp. 2813–2827, 2021.
[64] V. Buterin, Z. Hitzig, and E. G. Weyl, "A flexible design for funding public goods," *Management Science*, vol. 65, no. 11, pp. 5171–5187, 2019.
[65] Project Catalyst Community website. Accessed on: December 15, 2021. Available: https://cardanocataly.st.
[66] E. Anshelevich, A. Filos-Ratsikas, N. Shah, and A. A. Voudouris, "Distortion in social choice problems: The first 15 years and beyond," *arXiv preprint arXiv:2103.00911*, 2021.
[67] "*Dash Docs*", February 13, 2018. Accessed on: October 17, 2021. Available: https://github.com/dashpay/docs.