DOI:
10.1080/17445760.2024.2352740

Document Version
Peer reviewed version

Sybil Attack Vulnerability Trilemma

Moritz Platt[a] and Daniel Platt[b,c] and Peter McBurney[a]

[a]King's College London, Faculty of Natural, Mathematical & Engineering Sciences, 30 Aldwych, London WC2B 4BG, UK; [b]Department of Mathematics, Imperial College London, Exhibition Road, London SW7 2BX, United Kingdom; [c]I-X Centre for AI In Science, Imperial College London, White City Campus, 84 Wood Lane, London W12 0BZ, United Kingdom

ARTICLE HISTORY
Compiled 4th May 2024

Abstract
Public and permissionless blockchain systems are challenged by Sybil attacks, in which attackers use multiple identities to gain control. Traditionally, such attacks are prevented by consensus mechanisms relying on resource expenditure. However, such mechanisms (e.g. proof of work) face criticism for being wasteful. To address this and other concerns, novel blockchain systems backed by new consensus mechanisms have recently emerged. We formalise three key characteristics pursued by these systems: permissionlessness, Sybil attack resistance, and freeness. We demonstrate that no blockchain protocol can simultaneously achieve all three characteristics within the paradigm established by our formalisation. Thus, a trilemma emerges for distributed ledger technology designers, who must balance these characteristics thoughtfully.

KEYWORDS
Blockchain; Consensus Mechanism; Sybil Attack

1. Introduction

Fault tolerance is crucial for both centralised and distributed computer systems, yet it is particularly vital for the latter: in distributed systems, reliable orchestration of shared computing resources over communication networks is essential [1], as all distributed systems may, at times, face physical or human-made faults of varying durations and extents [2]. Generally, such systems can withstand a maximum of $1/3$ faulty participants [3], a limit that is sufficient to allow the operation of common centrally governed systems in which the number of – potentially faulty – participants can be limited by preselection.

Blockchain technology introduced a new class of systems, secure decentralised systems, by allowing public and permissionless access and thus eliminating the need for a dominant operator. Due to this change in permissioning and other technological innovations, secure decentralised blockchain systems provided some novel benefits; namely, resistance to censorship, immutability, and pseudonymity. This led some to consider them suitable systems for democratic or participatory decision-making. However, with these benefits came vulnerabilities, particularly to 'Sybil attacks' [4] in which 'a single

CONTACT M. Platt. Email: moritz.platt@kcl.ac.uk

faulty entity [...] present[s] multiple identities [so] it can control a substantial fraction of the system' [4][1]. As the first large-scale system of its kind, Bitcoin [5] counteracted Sybil attacks by applying a proof of work (PoW) mechanism in which the likelihood of being selected as a system validator is proportional to the computational effort invested.

In response to challenges around energy demand [6], security [7], fairness [8], performance [9], and suitability for democratic processes [10] of PoW, numerous 'second generation' blockchain systems have been proposed [11]. *Permissionlessness*, i.e. 'free entry' [12], remained a central characteristic for these systems. *Sybil attack resistance* was equally important for such systems, even though this characteristic was often implied, as without it, permissionless systems cannot function effectively. A third characteristic many new blockchain systems strove for was *freeness*, i.e. the absence of an 'explicit monetary cost' [13, p. 1157] to participation.

While all three characteristics are desirable, it is unclear whether they are achievable: observations of existing blockchain systems, particularly around tendencies towards centralisation [14] and documented instances of Sybil attacks [15], cast doubt on the feasibility of a system embodying all three characteristics. This research gap is particularly relevant to designers of public blockchain systems, who need to develop protocols accordingly. We therefore set out to investigate the compatibility of permissionlessness, Sybil attack resistance, and freeness in blockchain systems. We do so by providing background on blockchain technology, with a particular focus on consensus mechanisms (see subsection 1.1). We then define a formal model of a blockchain system (see section 2) that culminates in an impossibility theorem (see subsection 2.2) and apply it to some real-world blockchain systems (see section 3). We close with avenues for future work (see section 4) and conclusions (see section 5). Examples from the blockchain space used in section 1, subsection 1.1, and section 3 are provided to illustrate practical applications of the trilemma for reader comprehension, without claiming comprehensive coverage of all aspects of these systems. We recognise that these examples may extend beyond immediate definitions and assumptions.

1.1. Background

As early as the 1960s, the foundations for distributed systems research were laid in the form of multiprocess networking theory [16]. It has since evolved into a robust field that focusses on improving system reliability by developing and integrating methods to detect, mask and recover from operational and design faults [17]. Contrary to blockchain technology, in early distributed systems, a *central* authority controlled the admission of participants through attribute-based access control mechanisms [18] and by encoding their permissions in policies [19].

1.1.1. Motivations for Decentralisation and Impact Beyond Finance

Blockchain systems, which are positioned as *decentralised* transactional technologies that can facilitate the censorship-resistant replication of pseudonymous data between distrusting peers, potentially even without human intervention [20], allow the preservation of system history without exposure to the risk of nation-state censorship or regulatory overreach [21]. They were, therefore, welcomed by those who wanted to evade governmental influence [22] and by those who sought a decentralised payment mechanism that contests traditional financial hierarchies [23]. Through cryptocurrencies, blockchain has gained widespread adoption, serving as the underlying technology

for both speculation [24] and payments [25]. Blockchain technology is commercially leveraged in trading platforms and payment applications for retail and institutional audiences [26]. Due to their decentralised and, therefore, difficult-to-regulate nature [27], blockchains, particularly when applied to permissionless cryptocurrencies, continue to attract criticism for their role in facilitating the financing of criminal activities [28,29]. The use of this technology, however, extends beyond the financial realm: some notable applications are evident in fields such as internet of things (particularly ad-hoc networks [30]), healthcare, energy, public services, artificial intelligence, and big data [31].

1.1.2. Blockchain Characteristics

Tai *et al.* [32] characterise blockchain systems as symmetric, admin-free, ledgered, and time-consensual. These key characteristics are useful to differentiate blockchain systems from prior, centrally governed, distributed systems. Most relevant for Sybil attacks is the *admin-free* property: it describes systems that possess 'no concept of a system administrator who is responsible for maintenance, infrastructure provisioning or access control' [32, p. 758]. Tai *et al.* [32, p. 758], furthermore, state that updates to a blockchain system happen 'on an individual basis [governed by] community consensus'. Although, as described earlier, such consensus was not necessary for previous distributed systems due to the availability of centralised controls, it becomes critical in open systems where these controls are absent. Therefore, it is evident that, for successful community consensus, the group forming the community must be known and that this group, by and large [33], must follow accepted rules to reach consensus.

Blockchain systems are commonly classified along the anonymity and trust continuums (see Table 1). From an anonymity perspective, they can be classified as public, displaying data openly, or private, with centrally enforced access controls. From a trust perspective, they are either permissioned, with pre-selected validators, or permissionless[2], if participation in the use, development, and governance of the system is possible without needing permission from an authority, simply by following publicly stated procedures [34].

Table 1. Tezel *et al.* [35, p. 549] categorise four archetypes of Blockchain architectures (adapted from Platt and McBurney [36]).

	Permissioned	Permissionless
Public	*i*	*ii*
Private	*iii*	*iv*

Therefore, the many permissioned blockchain systems (types *i* and *iii* in Table 1), in which only a limited and controlled group of participants can take part [37–39], are not of interest in the context of this study: we focus on permissionless systems (types *ii* and *iv* in Table 1), as only these are commonly threatened by Sybil attacks.

1.1.3. Sybil Attack Resistance

All distributed systems, but particularly permissionless systems, face the consensus problem: 'a problem in distributed computing wherein nodes within the system must reach an agreement given the presence of faulty processes or deceptive nodes' [40, p. 1545]. Malicious participants may worsen this problem via Sybil attacks, where

large numbers of bogus processes are created to overpower genuine ones. Under the assumption that the number of malicious processes executed by an attacker is not limited, achieving consensus in systems under Sybil attacks is not possible using simple voting-based techniques [41–43]. Specifically leader-based mechanisms, such as Practical Byzantine fault tolerance [44] or Raft [45], while well suited to centrally managed distributed systems, are ineffective in public and permissionless systems, where an attacker can create arbitrary processes. There are many models to reach agreements in the presence of Sybil attacks [36], with PoW being the most popular.

1.1.3.1. Proof of Work. Bitcoin [5] introduced PoW, a mechanism that fundamentally employs an 'efficiently verifiable, but parameterisably expensive to compute' [46], cryptographic puzzle to prevent Sybil attacks. Solving this puzzle entitles the solver to carry forward the system log as a validator and grants them a cryptocurrency reward that is automatically distributed. This ensures that those investing significant computational effort are selected as validators, irrespective of the total number of candidates, thereby making Sybil attacks ineffective. Furthermore, the underlying reward mechanism ensures the anonymity of system validators in data replication, while simultaneously disincentivising them from consolidating [47]. This approach to consensus and data replication has been remarkably effective for maintaining system stability but requires the expenditure of large amounts of electricity [6] and is thus facing resistance [48].

1.1.3.2. Alternative Consensus Mechanisms. Consequently, alternative blockchain systems have been introduced. These often employ less resource-consumptive [49] consensus mechanisms [36], thereby lending themselves to sustainable innovation [50]. Some of these novel systems make participation free by relying on reputation systems to determine the probability of being selected as a system validator [51]. Although these novel systems have demonstrated the ability to withstand small-scale Sybil attacks [42], there are doubts about their resistance to Sybil attacks in fully permissionless contexts [36]. We aim to address such doubts with this work.

1.1.4. Consensus Mechanisms as Votes on System State

Both proof of resources and majority voting can be considered forms of votes on the canonical state of a decentralised system. For example, a simple PoW scheme, like the one used by Bitcoin, can be considered a probabilistic weighted voting scheme: in it, the voting power of a participant aligns with how much computational effort they invest into solving the PoW puzzle. A miner contributing $1/10$ of the system-wide computational effort for solving a given PoW puzzle would be selected as a block proposer with an approximate likelihood of 10 %. Likewise, in a simple proof of authority scheme based on random miner selection, the likelihood of being selected as a block proposer for a system with 10 participants is 10 %.

The concept of *blocks* is central to drawing parallels between blockchain consensus and voting. Blocks are compiled by miners, who gather transactions over time. Blocks, furthermore, group 'a set of transactions [and are] used as the unit of consensus' [32, p. 759] in blockchain systems. Since the system state of a blockchain is built up by monotonically chaining such blocks: every instance of a block proposal that is subject to a vote contributes to the overall system state, and thus to the decision on the version of events that is to be considered canonical. Therefore, even if common consensus

protocols do not purposively implement democratic principles, the mechanisms they apply to derive system state may show strong similarities with voting processes.

1.1.5. Consensus and Social Choice Theory

Based on the realisation presented in the previous section, it can be shown that findings concerning collective decision-making relate to blockchain consensus mechanisms: in particular, questions of social choice theory and blockchain consensus have an overlap. For example, Arrow's impossibility theorem [52] and the Gibbard–Satterthwaite theorem [53,54] can be applied to blockchain consensus to analyse how non-objective miners behave when they seek to advance a non-canonical version of the system's history.

1.2. Context

Many researchers have discussed blockchain systems as foundations for democratic self-governance [10,55–58], some emphasising their suitability for democratic or participatory decision-making [59]. Indeed, it appears reasonable to assume that systems that are resistant to bad actors attempting to take over control while allowing anyone to participate freely would be ideally suited for self-governing communities [60]. Any type of community activity, such as elections [61], trade [62], or the administration of the commons [63], could be supported by such systems. However, despite the 15-year history of blockchain technology, there is little evidence that it is being used in this way [64–66], with governance challenges remaining widespread [67]. On the contrary, there is reason to suspect that public blockchain technology, especially in conjunction with cryptocurrencies, might replicate existing social disparities [68,69] or lead to centralisation of power [14,70,71]. An important research gap is, therefore, to analyse whether democratic self-governed systems are implementable, and simply haven't manifested yet, or whether they cannot exist. Addressing this research gap is the purpose of our work.

1.3. Previous Work

Douceur [4] introduced the term *Sybil attack* in a paper of the same name. In Lemma 2 of that paper, it is shown that in a distributed system in which participation is free, an attacker may present arbitrarily many Sybil identities. It is stated informally that in such a free system without trusted, centralised authority, Sybil attacks are always possible.

1.3.1. Common Sybil Attack Mitigation Strategies

Yang *et al.* [15] show that Sybil attacks are not merely a theoretical threat but are observable in existing networks. The most prevalent Sybil attack mitigation strategies for blockchains are PoW, defined by Golle *et al.* [72] as 'primitives which enforce either high communication or high storage complexity on some party', and proof of stake (PoS): 'mechanisms that extend voting power to the stakeholders of the system' [73].

1.3.2. Reputation Systems for Sybil Attack Mitigation

Beyond these, a common Sybil Attack mitigation strategy is the application of reputation systems, in which the relationships between participants in a system are used to derive a measure of trustworthiness for participants that, in turn, determines how much influence these participants have in collaborative tasks [74]. In particular, the work of Yu *et al.* [75], which introduces such a protocol by building on established trust relationships, predates blockchain technology. Agent-based analysis of reputation systems for Sybil attack resistance has been undertaken by Platt and McBurney [42] who find that simple Sybil attacks can be repelled by reputation systems. This result is in line with findings by Seuken and Parkes [76, Theorem 3], who show that systems may achieve 'K-sybil-proofness', i.e. resistance against up to K Sybil identities. However, they further prove that reputation systems alone cannot yield a fully Sybil-proof decentralised system.

1.3.3. Physical-World-Linking to Address Sybil Attacks

An alternative mitigation strategy is that of *physical world linking* [36,77], in which information from the physical world, such as sensor readings, is used to ensure the individuality of participants [77,78]. As discussed well before the era of blockchain [79], such an approach commonly requires trusted hardware, in which case it needs to be considered quasi-permissioned, with trust being anchored in the maker of said trusted hardware. Furthermore, implementations of physical world linking can be vulnerable to attacks in which groups of attackers act in concert, combining device signals to circumvent protocols.

1.4. Contribution

We formalise the notions of *free* and *Sybil attacks* for blockchain systems. In Proposition 2, we formalise and prove the statement by Douceur [4, p. 254], that in a free system without trusted authority, Sybil attacks are always possible. Note that a correct formalisation of *without trusted authority* must also exclude other, potentially very complicated, organisational structures, such as consortia or consensus systems that obfuscate centralisation. We achieve this, for blockchain systems only and not for distributed systems in general, in our definition of *(strongly) permissionless*.

2. Formalising Some Properties of Blockchain Systems

In this section, we will formally define a model for blockchain systems and will rigorously define what it means for such a system to be permissionless, Sybil attack resistant, and free. In the end, we will show that, in our definition of a blockchain system, there can be no system satisfying all three properties.

This is similar to classical theorems in social choice theory: Arrow's impossibility theorem states that there is no voting system satisfying three distinct fairness criteria [52]; the Gibbard–Satterthwaite theorem states that voting systems are susceptible to tactical voting if there is more than one voter and more than two options to choose from [53,54]. In these two cases, as in our application, three desirable properties for systems are defined, and it is shown that no system can satisfy all three simultaneously.

2.1. Formal Model

We approach decentralised systems from a transactional perspective: we assume that the system state is derived from a set of temporally ordered *actions* that comply with the rules of the underlying system protocol and form a *history*. Actions can change the system from one state to another, possibly identical, state. We assume them to be instantaneous and deterministic, and they are taken at discrete timesteps. This aligns with common blockchain implementations, in which transactions are sequentially ordered by compiling them into blocks [80]. We assume that, for any blockchain system, rules are in place that allow it to be determined whether an action is in accordance with the underlying protocol. Typically, protocols require that the content of every block satisfies some cryptographic property; for example, that it contains a hash of the content of the previous block. The definition of 'action' is intentionally abstract to encompass all rule-compliant measures a participant in a blockchain network might initiate. Common actions under existing protocols are to propose transactions and to compile transactions into blocks.

Definition 1.

(a) Let A be a non-empty set of actions, containing an element none $\in A$. none is called no action*. Let*

$$\mathrm{HIST}_0 \subset \left\{ f : \mathbb{N} \times \mathbb{N} \to A : \begin{array}{c} \textit{ex. at most finitely many } s \in \mathbb{N} \\ \textit{with: } \exists t \in \mathbb{N} \textit{ s.t. } f(s,t) \neq \textit{none} \end{array} \right\}$$

and $\mathrm{HIST} \subset \mathrm{HIST}_0$ *be defined as those histories in which every action is in accordance with the underlying protocol.* HIST *is called the set of possible histories of the protocol. An element* $\mathrm{hist} \in \mathrm{HIST}$ *is called* finite *if $f(s,t) \neq$ none for at most finitely many $(s,t) \in \mathbb{N} \times \mathbb{N}$. For $(s,t) \in \mathbb{N} \times \mathbb{N}$ we call s a* participant *and t a* point in time*.*

(b) Let B be the set of all possible blocks. Then B is contained in A in the sense that for every block B there is the action of proposing it. An element $\mathrm{hist} \in \mathrm{HIST}$ *is a collection of actions, and it defines a tree of blocks in which each branch obeys the rules of the protocol. This tree is called* blockchain defined by hist*.*

(c) A decision function is a function

$$\mathrm{dec} : \mathrm{HIST} \to \{(b_1, b_2, \ldots, b_k) \in B^k \textit{ for any } k \geq 0\} \cup \{\varnothing\}$$

satisfying the following property: if $\mathrm{dec}(\mathrm{hist}) = (b_1, b_2, \ldots, b_k)$*, then* $(b_1, b_2, \ldots, b_k)$ *must be a branch in the blockchain defined by* hist*. If* $\mathrm{dec}(\mathrm{hist}) = \varnothing$ *we say that* dec *makes no decision for the history* hist*.*

A minor point is that, in blockchain systems, views on what is the current state of the system may differ between system participants for short timeframes (e.g. due to replication delays). In our simplified model, we assume that all participants have an aligned view of all actions. The difficulty that remains is that participants may be presented with a history exhibiting multiple branches, each of which is in accordance with the underlying protocol. Decision functions, as illustrated in Figure 1, allow participants to resolve such conflicts.

Commonly, system protocols employ decision functions that apply probabilistic techniques to this problem, such as the 'longest chain' rule in Bitcoin or the Ethereum fork-choice algorithm that takes into account the weight of a branch. In some scenarios,

a decision function may select none of the existing branches as correct; for example, where multiple branches of equal length exist in Bitcoin. In our formalism, the decision function in this case would return $\varnothing$ instead of a preferred branch.

Zorn's lemma [81,82] may be used to construct decision functions. However, it is never needed if only deciding on finite histories (which is the only case considered in this manuscript), and additional choices would need to be made if deciding on infinite histories.

Definition 2 (Weakly Permissionless)**.** *A protocol is called weakly permissionless if for all finite* hist $\in$ HIST *there exists a branch* $(b_1, \ldots, b_k) \in B^k$ *such that for any future behaviour of the participants in* hist *and for any participant* s^* *not in* hist*, there exists a continuation* $\widetilde{\text{hist}}$ *of* hist *defining a branch* $(b_1, \ldots, b_{k+n})$ *such that for all legal blocks* b^* *we have*

$$\text{dec}(\widetilde{\text{hist}} + (s^*, b^*)) = (b_1, \ldots, b_{k+n}, b^*).$$

Here, $\widetilde{\text{hist}} + (s^*, b^*)$ *denotes the history that is equal to* $\widetilde{\text{hist}}$ *but has one additional action added to it, namely the action of a participant* s^* *to propose the block* b^* *at time* 1 *after the last action in* $\widetilde{\text{hist}}$*.*

Informally, this means the following: hist is the state of the system of a blockchain at a given time, including all actions that led to its current state, potentially including forks. If the system is weakly permissionless, then a new participant can get some future block b^* accepted by the decision function, and no one can stop them. If there is even a small chance that the new participant cannot get their block accepted, no matter their actions, then that protocol would not be weakly permissionless. Of course, we do not expect that the new participant can get all blocks they want accepted: before their block b^* is accepted, there may come other accepted blocks $b_{k+1}, \ldots, b_{k+n}$ that were not suggested by the new participant. There are no conditions on the content of b^*, except that it must be legal according to the blockchain protocol.

Definition 3 (Strongly permissionless)**.** *A protocol is called strongly permissionless if for all finite* hist $\in$ HIST *and for any future behaviour of the participants in* hist*, there exists an infinitely long continuation* $\widetilde{\text{hist}}$ *of* hist *and a positive integer* N_0 *such that the following is true: for all* $N > N_0$*, the majority of accepted blocks in* $\widetilde{\text{hist}}$*, cut off at time* N*, have been proposed by participants who did not have any activity in* hist*.*

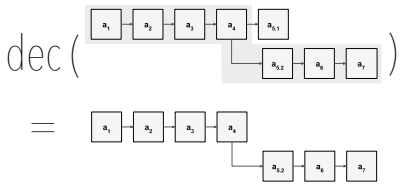

Figure 1. A decision function dec takes an ambiguous history (e.g. one with forks) as input and derives a canonical history as output.

In contrast to *weakly* permissionless protocols, *strongly* permissionless protocols are characterised not only by allowing new participants to *occasionally* propose transactions but by, eventually, allowing them to propose a *majority* of transactions.

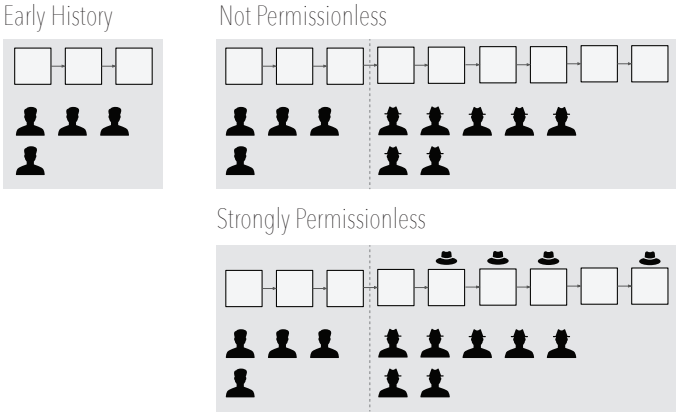

Figure 2. Left: a Blockchain created by some participants. Top right: an example of a Blockchain that is not weakly permissionless and not strongly permissionless. A large number of new participants (shown with a hat) joined but they are not allowed to create blocks. All blocks going forward are created by the original participants. Bottom right: an example of a Blockchain that is strongly permissionless. New participants joined and are creating a majority of new blocks (shown with a hat) going forward, which cannot be prevented by the original participants.

The adherence of Bitcoin, the archetypal strongly permissionless protocol, to Definition 3 can be illustrated as follows: hist $\in$ HIST could be the current state of the Bitcoin blockchain. This includes the full blockchain, including forks. A new participant s^* can immediately propose any legal block a^*, containing the required PoW, to be added to the longest chain which will be accepted by the decision function dec, the 'longest chain' rule. In this case $n = 0$. That is, the participant s^* does not need to take any actions to improve their own standing in the protocol, since a correct PoW immediately entitles them to propose a block. Given appropriate resource expenditure, the participant could propose new blocks in perpetuity. This is illustrated in Figure 2: in the strongly permissionless system shown, a majority of new blocks were created by new participants.

Definition 4 (Sybil attack vulnerable)**.** *A system with finite history* hist *is vulnerable to Sybil attacks if for any behaviour of the participants in* hist*, there exist arbitrarily long continuations* $\widetilde{\text{hist}}$ *of* hist *such that a majority of accepted blocks in* $\widetilde{\text{hist}}$ *have been proposed by participants not in* hist *and these participants have expended only negligible explicit monetary cost.*

In the context of decentralised systems, an attack is understood as the realisation of a threat, representing a harmful action aimed at exploiting vulnerabilities within the system [83]. A type of attack that has received particular attention in the blockchain community is the Sybil attack [36]: Informally, in accordance with Douceur [4, p. 251], we define a Sybil attack on a decentralised system as a series of protocol-conforming actions through which an attacker presents multiple identities with the intent of seizing control of a substantial fraction of the system. Attackers achieve the seizure of control by skewing collective decisions, such as voting, in their favour. A potential result of a successful Sybil attack on a strongly permissionless system is the attacker increasing

the probability of proposing new blocks, thereby being able to censor block contents and, ultimately, centralising power over the system. It is intuitively clear that a Sybil attack is only possible if a malicious actor can take many actions while expending only negligible explicit monetary cost. In accordance with Saleh [13, p. 1157], we formally define this as:

Definition 5 (Free)**.** *A system is* free *if all actions can be taken by incurring only negligible explicit monetary cost.*

Notably, staking requirements common in cryptocurrencies, which are perceived not as monetary costs but as commitments for potential financial gain, are excluded by this definition.

2.2. An Impossibility Theorem for Sybil Attack Resistance

We define three properties of interest for blockchain systems: permissionless in Definition 2 and Definition 3, Sybil attack vulnerable in Definition 4, and free in Definition 5. Here is how these notions are related to each other:

Proposition 1. *Any Sybil attack vulnerable system is strongly permissionless.*

Proof. Definition 3 and Definition 4 are the same, except that Sybil attack vulnerability has an additional restriction that is not present in the definition of strongly permissionless. □

Most importantly, there is no system that satisfies all three requirements:

Proposition 2 (Impossibility Theorem for Sybil Attack Resistance)**.** *A blockchain protocol cannot be strongly permissionless, Sybil attack-resistant, and free.*

Proof. By definition, a system that is *free* and *strongly permissionless* must be *Sybil attack vulnerable*. Therefore, such a system cannot be *Sybil attack-resistant*, which illustrates the claim. □

3. Illustration of the Trilemma Using Existing Blockchain Systems

In consideration of Proposition 2, an analysis of existing blockchain systems has been performed for illustrative purposes, acknowledging that the described Trilemma may not encompass all aspects of these real-world systems in their entirety. To this end, we selected two particularly popular blockchain systems with associated cryptocurrencies to illustrate common combinations of characteristics, potentially extending beyond the immediate scope of defined assumptions. Both systems are representative of a large number of others that use PoW (see subsection 3.1) or PoS (see subsection 3.2) in similar ways. The remaining combination – strongly permissionless and free but not Sybil attack resistant – is rare, as systems with these characteristics can be disrupted as a result of targeted Sybil attacks and are, therefore, mostly of theoretical interest. To shed light on this combination of characteristics, we selected a technique that has so far been discussed only theoretically (see subsection 3.3). Figure 3 shows the different possible combinations, visualising Proposition 2.

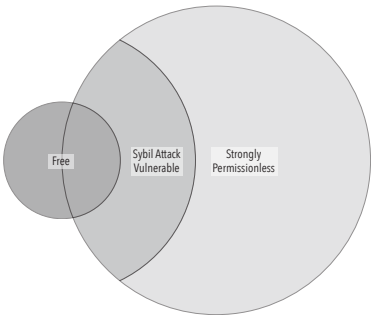

Figure 3. Diagram showing how free, Sybil attack vulnerable, and strongly permissionless blockchain systems are related. By Proposition 1, Sybil attack vulnerable systems are a subset of strongly permissionless systems. By Proposition 2, the intersection of the two circles "Free" and "Strongly Permissionless" and the complement of "Sybil Attack Vulnerable" is empty.

Table 2. A comparison of common Blockchain systems. The ∘ symbol indicates whether they meet the definition of strongly permissionless (SP), Sybil attack-resistant (SAR), or free (F).

Sec.	System	Mechanism	SP	SAR	F
3.1	Bitcoin	Proof of work (PoW)	∘	∘	
3.2	Ethereum 2	Proof of stake (PoS)		∘	∘
3.3		Proof of lucky ID (PoL)	∘		∘

3.1. Proof of Work

Proof of work (PoW) is the archetypal approach to preventing Sybil attacks. While it predates Bitcoin [84], its use in the context of decentralised networks dates back to this cryptocurrency [5]. Strong permissionlessness is central to Bitcoin's design, in which messages are exchanged on a best-effort basis between nodes that are able to leave and join the network at will [5]. Arbitrary nodes can participate in the consensus mechanism in a censorship-resistant manner that can recover from network partitions. Nakamoto [5] motivates the use of PoW by emphasising that it enables *one central processing unit (CPU), one vote* [5, p. 3] mechanics that, under the assumption that 'a majority of CPU power is controlled by honest nodes' [5, p. 3], can secure the existence of the Bitcoin system in perpetuity. While attackers can easily create arbitrary numbers of accounts, PoW prevents these from interfering with consensus. However, despite the potential of block rewards offsetting the costs, participation in Bitcoin's consensus mechanism is costly, since it requires significant computational effort and, consequently, physical resources to provide it.

3.2. Proof of Stake

To the best of our knowledge, the first mention of proof of stake (PoS) occurred in Bitcoin circles: here, it was proposed to align the influence in majority-based activities

with 'the number of bitcoins you can prove you own' [85]. The most popular implementation of this concept is Ethereum, conceived as a PoW system [86] and recently successfully transitioned to PoS during the Ethereum 2 merge [87]. Note that the restrictiveness of Definition 3 excludes Ethereum 2: the current Ethereum 2 stakeholders possess the ability to collude and effectively bar external participation by virtue of the requirement to deposit cryptocurrency into the protocol's deposit contract to qualify as validator [88]. Consequently, those without access to the Ethereum cryptocurrency are perpetually excluded from the validator pool, making them unable to propose blocks. Ethereum's PoS system exhibits strong Sybil attack resistance: similar to other blockchain systems, users can create arbitrary accounts for the Ethereum 2 blockchain. However, due to the prerequisite of staking cryptocurrency to act as a validator, unfunded accounts would not be selected for participation in some of the network activities. Participation in Ethereum 2 (including in the role of validator) is free according to our unrestrictive Definition 5, which ignores transaction fees and staking requirements of Ethereum 2 cryptocurrency.

3.3. Proof of Lucky ID

Ogawa *et al.* [89] introduced proof of lucky ID (PoL), a mechanism that can be used to illustrate the class of strongly permissionless and free systems that are not Sybil attack-resistant. In PoL, a miner is selected pseudorandomly using their ID. We assume a simplified ID supply mechanism that allows users to self-generate IDs[3]. The random selection of nodes from the pool of participants can be considered an approach that achieves strong permissionlessnes. Depending on the ID supply mechanism, this mechanism is, however, highly susceptible to Sybil attacks: where a self-generated ID is used [89, p. 1216] and no further restrictions on ID generation are made, an attacker can easily conduct a Sybil attack by creating many IDs, thereby increasing the likelihood of being randomly selected. Note that it is conceivable to alter the protocol by applying other ID supply mechanisms that are less free or less permissionless, but may in turn lead to Sybil attack resistance. Under the assumption of a free ID supply mechanism, PoL can be considered equally free.

4. Future Work

We adopt a binary view of the three desirable characteristics of permissionlessness, Sybil attack resistance, and freeness. However, blockchain systems in actual implementation do not always lend themselves to binary classification. For instance, in our work, the characteristic of freeness is defined dichotomously. In reality, however, there is a wide range of costs of participation between blockchain systems of different characteristics and popularity. The same may apply to the remaining two characteristics. For example, PoS systems do not satisfy our definition of *permissionless*. Yet, they may be considered permissionless for practical purposes in some cases.

An extension of the theorem, for example by introducing a scalar representation of the desired characteristics, could provide further insight into the underpinning relationships. Furthermore, given the parallels between voting and blockchain consensus, applying social choice theory to blockchain consensus is a promising approach for future work.

We gave a very simple definition of *Sybil attack vulnerable* (Definition 4), which subsequently made it easy to formally reason about it. Instead, one may be able to formalise the notions of *attack* and subsequently *Sybil attack*, relating them to informal

definitions from the literature. One could then define a Sybil attack vulnerable system as a system in which such (formally defined) Sybil attacks are possible. The difficulty in doing this is to find corresponding definitions of permissionless and free which can be related to real-world protocols and still have the property that there is no protocol that complies with all three new definitions: permissionless, free, and Sybil attack resistant.

Moreover, it should be acknowledged that the conclusions drawn in our manuscript are subject to the paradigm established by our formalisation (see section 2). It is plausible that alternative formalisations, yet to be explored, might offer different perspectives.

5. Conclusion

Blockchain systems that are *permissionless* (i.e. allow public participation without limitations), *resistant to Sybil attacks* (i.e. not vulnerable to attackers that skew collective decisions), and *free* (i.e. require expenditure of only negligible explicit monetary cost) are highly desirable for many applications; notably, for democratic self-governance. However, there is reason to believe that these three properties cannot be achieved in a blockchain system simultaneously. Therefore, we raised the question of proving their compatibility.

We have shown that no blockchain system can concurrently achieve the three desirable characteristics defined within the framework outlined in section 2, leading to the negative conclusion of this question within the defined paradigm. Furthermore, we categorised existing popular blockchain systems by the set of desirable characteristics they exhibit. For example, Bitcoin is *strongly permissionless* and *Sybil attack-resistant* but not *free*, whereas, Ethereum 2 is *Sybil attack-resistant* and *free* but not *strongly permissionless*. These findings have implications for the designers of future blockchain systems, who can apply them to address the tradeoffs between characteristics more consciously. A more deliberate treatment of these tradeoffs may enable systems that focus on two of the three dimensions and, thereby, achieve a better problem-solution fit. Our results also help to critically evaluate common claims that certain protocols are free and permissionless. A noteworthy limitation of our work is that the definition of *permissionless* is restrictive and excludes some systems that have been labelled permissionless by others, and this should be considered when interpreting this work.

Understanding whether given blockchain applications deliver on the promise of decentralisation remains a central challenge for the credibility of this emerging technology. While it was shown that systems that simultaneously exhibit all three desirable characteristics cannot exist under our formalisation, we recognise that blockchain technology offers great potential for applications, in self-governance and beyond, if the technological trade-offs are understood, managed, and communicated.

Acknowledgements

M.P. would like to acknowledge Daniel Körnlein for his helpful comments and Moti Yung for reviewing an earlier version of this paper. D.P. was supported by the Eric and Wendy Schmidt AI in Science Postdoctoral Fellowship, a Schmidt Futures program. M.P. and D.P. acknowledge reviewer #1 for suggesting an alternative definition of Sybil attack vulnerability, which prompted the discussion in section 4.

Funding

No funding was received for conducting this study.

Disclosure Statement

The authors report that there are no competing interests to declare.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Notes

[1]See subsection 1.1 and Definition 4 for a more comprehensive description.
[2]Notwithstanding Definitions 2 and 3.
[3]This configuration is somewhat artificial and likely not in line with the intentions of Ogawa *et al.* [89]. It is used here solely to illustrate the class of non-Sybil attack resistant systems.

References

[1] Rennels. Distributed fault-tolerant computer systems. Computer. 1980 Mar;13(3):55–65.
[2] Avižienis A. Framework for a taxonomy of fault-tolerance attributes in computer systems. In: Proceedings of the 10th Annual International Symposium on Computer Architecture; Stockholm, Sweden. ACM; 1983. p. 16–21.
[3] Pease M, Shostak R, Lamport L. Reaching agreement in the presence of faults. Journal of the ACM. 1980 Apr;27(2):228–234.
[4] Douceur JR. The Sybil attack. In: Druschel P, Kaashoek F, Rowstron A, editors. Proceedings of the 1st International Workshop on Peer-to-Peer Systems; Cambridge, MA, USA. Springer; 2002. p. 251–260.
[5] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system ; 2008. Accessed 19 April 2023; Available from: `https://bitcoin.org/bitcoin.pdf`.
[6] Sedlmeir J, Buhl HU, Fridgen G, et al. The energy consumption of blockchain technology: Beyond myth. Business & Information Systems Engineering. 2020 Jun;62(6):599–608.
[7] Zhang R, Preneel B. Lay down the common metrics: Evaluating proof-of-work consensus protocols' security. In: Proceedings of the 2019 Symposium on Security and Privacy; May; San Francisco, CA, USA. IEEE; 2019. p. 175–192.
[8] Poux P, De Filippi P, Deffains B. Maximal extractable value and the blockchain commons [Social Science Research Network]; 2022. Available from: `https://ssrn.com/abstract=4198139`.
[9] Gervais A, Karame GO, Wüst K, et al. On the security and performance of proof of work blockchains. In: Proceedings of the 2016 Conference on Computer and Communications Security; Oct.; Vienna, Austria. ACM; 2016. p. 3–16; CCS'16.
[10] Racsko P. Blockchain and democracy. Society and Economy. 2019 Sep;41(3):353–369.
[11] De Angelis S, Lombardi F, Zanfino G, et al. Security and dependability analysis of blockchain systems in partially synchronous networks with Byzantine faults. International Journal of Parallel, Emergent and Distributed Systems. 2023 Oct;:1–21.

[12] Gans J, Gandal N. More (or less) economic limits of the blockchain. Cambridge, MA, USA: National Bureau of Economic Research; 2019. Working Paper 26534. Available from: https://www.nber.org/papers/w26534.
[13] Saleh F. Blockchain without waste: Proof-of-stake. The Review of Financial Studies. 2020 Jul;34(3):1156–1190.
[14] Sai AR, Buckley J, Fitzgerald B, et al. Taxonomy of centralization in public blockchain systems: A systematic literature review. Information Processing & Management. 2021 Jul; 58(4):102584.
[15] Yang Z, Wilson C, Wang X, et al. Uncovering social network Sybils in the wild. ACM Transactions on Knowledge Discovery from Data. 2014 Feb;8(1):1–29.
[16] Kleinrock L. Information flow in large communication nets [Thesis proposal]; 1961.
[17] Aviziens. Fault-tolerant systems. IEEE Transactions on Computers. 1976 Dec; C–25(12):1304–1312.
[18] Hu VC, Kuhn DR, Ferraiolo DF. Access control for emerging distributed systems. Computer. 2018 Oct;51(10):100–103.
[19] Bacon J, Moody K. Access control in distributed systems. In: Herbert A, Spärck Jones K, editors. Computer systems. Cham, Switzerland: Springer; 2004. p. 21–28.
[20] Hartwich E, Rieger A, Sedlmeir J, et al. Machine economies. Electronic Markets. 2023 Jul;33(1):36.
[21] Rocco G. Public blockchains as a means to resist information censorship Master's thesis. New York, NY, USA: City University of New York; 2019. Available from: https://academicworks.cuny.edu/gc_etds/2995/.
[22] Jarvis C. Cypherpunk ideology: objectives, profiles, and influences (1992–1998). Internet Histories. 2021 Jun;6(3):315–342.
[23] Bohr J, Bashir M. Who uses Bitcoin? an exploration of the Bitcoin community. In: Proceedings of the 12th Annual International Conference on Privacy, Security and Trust; Jul.; Toronto, ON, Canada. IEEE; 2014. p. 94–101.
[24] Glaser F, Zimmermann K, Haferkorn M, et al. Bitcoin – asset or currency? revealing users' hidden intentions. In: Proceedings of the 22nd European Conference on Information Systems; Jun.; Tel Aviv, Israel. AIS; 2014. p. 1–14. Available from: https://aisel.aisnet.org/ecis2014/proceedings/track10/15/.
[25] Jonker N. What drives the adoption of crypto-payments by online retailers? Electronic Commerce Research and Applications. 2019 May;35:100848.
[26] Beinke JH, Nguyen D, Teuteberg F. Towards a business model taxonomy of startups in the finance sector using blockchain. In: Proceedings of the 2018 International Conference on Information Systems; San Francisco, CA, USA; 2018. p. 1–9. Available from: https://aisel.aisnet.org/icis2018/crypto/Presentations/9.
[27] Aquilina M, Frost J, Schrimpf A. Tackling the risks in crypto: Choosing among bans, containment and regulation. Journal of the Japanese and International Economies. 2024 Mar;71:101286.
[28] Piazza F. Bitcoin in the Dark Web: A shadow over banking secrecy and a call for global response. Southern California Interdisciplinary Law Journal. 2017;26(3):493–520.
[29] Trozze A, Kamps J, Akartuna EA, et al. Cryptocurrencies and future financial crime. Crime Science. 2022 Jan;11(1).
[30] Hamdan S, Hudaib A, Awajan A. Detecting Sybil attacks in vehicular ad hoc networks. International Journal of Parallel, Emergent and Distributed Systems. 2019 May;36(2):69–79.
[31] Paulavičius R, Grigaitis S, Igumenov A, et al. A decade of blockchain: Review of the current status, challenges, and future directions. Informatica. 2019 Jan;30(4):729–748.
[32] Tai S, Eberhardt J, Klems M. Not ACID, not BASE, but SALT - a transaction processing perspective on blockchains. In: Proceedings of the 7th International Conference on Cloud Computing and Services Science; Porto, Portugal. SciTePress; 2017. p. 755–764.
[33] Tholoniat P, Gramoli V. Formal verification of blockchain byzantine fault tolerance. In: Tran DA, Thai MT, Krishnamachari B, editors. Handbook on blockchain. Cham, Switzer-

land: Springer; 2022. Springer Optimization and Its Applications; p. 389–412.
[34] Nabben K, Zargham M. Permissionlessness. Internet Policy Review. 2022;11(2):1–10.
[35] Tezel A, Papadonikolaki E, Yitmen I, et al. Preparing construction supply chains for blockchain technology: An investigation of its potential and future directions. Frontiers of Engineering Management. 2020 May;7(4):547–563.
[36] Platt M, McBurney P. Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance. Algorithms. 2023 Jan; 16(1):34.
[37] Valenta M, Sandner P. Comparison of Ethereum, Hyperledger Fabric and Corda. Frankfurt School Blockchain Center; 2017. FSBC working paper. Available from: `http://explore-ip.com/2017_Comparison-of-Ethereum-Hyperledger-Corda.pdf`.
[38] Nadir RM. Comparative study of permissioned blockchain solutions for enterprises. In: Proceedings of the 2019 International Conference on Innovative Computing; Nov.; Lahore, Pakistan. IEEE; 2019. p. 1–6.
[39] Polge J, Robert J, Traon YL. Permissioned blockchain frameworks in the industry: A comparison. ICT Express. 2021 Jun;7(2):229–233.
[40] Bach LM, Mihaljevic B, Zagar M. Comparative analysis of blockchain consensus algorithms. In: Proceedings of the 41st International Convention on Information and Communication Technology, Electronics and Microelectronics; may; Opatija, Croatia. IEEE; 2018. p. 1545–1550.
[41] Anceaume E, Busnel Y, Sericola B. Byzantine-tolerant uniform node sampling service in large-scale networks. International Journal of Parallel, Emergent and Distributed Systems. 2021 Jun;36(5):412–439.
[42] Platt M, McBurney P. Sybil attacks on identity-augmented proof-of-stake. Computer Networks. 2021 Nov;199:108424.
[43] Meir R, Talmon N, Shahaf G, et al. Sybil-resilient social choice with low voter turnout. In: Baumeister D, Rothe J, editors. Proceedings of the 2022 European Conference on Multi-Agent Systems; Düsseldorf, Germany. Springer; 2022. p. 257–274.
[44] Castro M, Liskov B. Practical Byzantine fault tolerance. In: Proceedings of the 3rd Symposium on Operating Systems Design and Implementation; Feb.; New Orleans, LA, USA. USENIX; 1999. p. 173–186.
[45] Ongaro D, Ousterhout J. In search of an understandable consensus algorithm. In: Proceedings of the 2014 USENIX Annual Technical Conference; Jun.; Philadelphia, PA, USA. USENIX; 2014. p. 305–320.
[46] Back A. Hashcash - a denial of service counter-measure ; 2002. Accessed 30 December 2023; Available from: `http://www.hashcash.org/papers/hashcash.pdf`.
[47] Leshno J, Strack P. Bitcoin: An impossibility theorem for proof-of-work based protocols. New Haven, CT, USA: Yale University; 2019. Cowles Foundation Discussion Paper 2204R. Available from: `https://ssrn.com/abstract=3487355`.
[48] Platt M, Ojeka S, Drăgnoiu AE, et al. Energy demand unawareness and the popularity of Bitcoin: Evidence from Nigeria. Oxford Open Energy. 2023;2.
[49] Platt M, Sedlmeir J, Platt D, et al. The energy footprint of blockchain consensus mechanisms beyond proof-of-work. In: Companion Proceedings of the 21st International Conference on Software Quality, Reliability and Security; Hainan, China. IEEE; 2021. p. 1135–1144.
[50] Treiblmaier H. Blockchain technology and sustainability. In: Abraham MA, editor. Encyclopedia of sustainable technologies. 2nd ed.; Vol. 3. Elsevier; 2024. p. 850–860.
[51] Li Y, Cheng J, Li H, et al. A survey of consensus mechanism based on reputation model. In: Xingming S, Zhang X, Xia Z, et al., editors. Proceedings of the 8th International Conference on Artificial Intelligence and Security; Qinghai, China. Springer; 2022. p. 208–221.
[52] Arrow KJ. A difficulty in the concept of social welfare. Journal of Political Economy. 1950 aug;58(4):328–346.
[53] Gibbard A. Manipulation of voting schemes: A general result. Econometrica. 1973 Jul; 41(4):587.

[54] Satterthwaite MA. Strategy-proofness and arrow's conditions: Existence and correspondence theorems for voting procedures and social welfare functions. Journal of Economic Theory. 1975 Apr;10(2):187–217.
[55] Poupko O, Shahaf G, Shapiro E, et al. Sybil-resilient conductance-based community growth. In: van Bevern R, Kucherov G, editors. Proceedings of the 14th International Computer Science Symposium in Russia; Novosibirsk, Russia. Springer; 2019. p. 359–371.
[56] Tozzi C. Decentralizing democracy: approaches to consensus within blockchain communities. Teknokultura. 2019 Oct;16(2):181–195.
[57] Cila N, Ferri G, de Waal M, et al. The blockchain and the commons: Dilemmas in the design of local platforms. In: Proceedings of the 2020 Conference on Human Factors in Computing Systems; Apr.; Honolulu, HI, USA. ACM; 2020. p. 1–14.
[58] Mukhametov DR. Self-organization of network communities via blockchain technology: Reputation systems and limits of digital democracy. In: Proceedings of the 2020 Conference on Systems of Signal Synchronization, Generating and Processing in Telecommunications; Jul.; Svetlogorsk, Russia. IEEE; 2020. p. 1–7.
[59] Wright A, De Filippi P. Decentralized blockchain technology and the rise of lex cryptographia. SSRN Electronic Journal. 2015;.
[60] Razzaq A, Murad M, Talib R, et al. Use of blockchain in governance: A systematic literature review. International Journal of Advanced Computer Science and Applications. 2019;10(5).
[61] Dhillon A, Kotsialou G, McBurney P, et al. Voting over a distributed ledger: An interdisciplinary perspective. Foundations and Trends in Microeconomics. 2021;12(3):200–268.
[62] Wongthongtham P, Marrable D, Abu-Salih B, et al. Blockchain-enabled peer-to-peer energy trading. Computers & Electrical Engineering. 2021 Sep;94:107299.
[63] Rozas D, Tenorio-Fornés A, Díaz-Molina S, et al. When Ostrom meets blockchain: Exploring the potentials of blockchain for commons governance. SAGE Open. 2021 Jan; 11(1):215824402110025.
[64] DuPont Q. Experiments in algorithmic governance. In: Campbell-Verduyn M, editor. Bitcoin and beyond. Routledge; 2017. p. 157–177.
[65] Ziolkowski R, Miscione G, Schwabe G. Decision problems in blockchain governance: Old wine in new bottles or walking in someone else's shoes? Journal of Management Information Systems. 2020 Apr;37(2):316–348.
[66] Cengiz F. Blockchain governance and governance via blockchain: decentralized utopia or centralized dystopia? Policy Design and Practice. 2023 Aug;6(4):446–464.
[67] Rikken O, Janssen M, Kwee Z. Governance challenges of blockchain and decentralized autonomous organizations. Information Polity. 2019 Dec;24(4):397–417.
[68] Chohan UW. Cryptocurrencies and inequality. In: Goutte S, Guesmi K, Saadi S, editors. Cryptofinance. Singapore: World Scientific Publishing; 2021. p. 49–62.
[69] Walsh M. Bitcoin, cryptocurrencies & the climate crisis. Irish Marxist Review. 2021; 10(30):80–89.
[70] Leonardos N, Leonardos S, Piliouras G. Oceanic games: Centralization risks and incentives in blockchain mining. In: Mathematical research for blockchain economy. Cham, Switzerland: Springer; 2020. p. 183–199.
[71] Heo K, Yi S. (de)centralization in the governance of blockchain systems: cryptocurrency cases. Journal of Organization Design. 2023 Mar;.
[72] Golle P, Jarecki S, Mironov I. Cryptographic primitives enforcing communication and storage complexity. In: Blaze M, editor. Proceedings of the 6th International Conference on Financial Cryptography; Southampton, Bermuda. Springer; 2003. p. 120–135.
[73] Bentov I, Gabizon A, Mizrahi A. Cryptocurrencies without proof of work. In: Clark J, Meiklejohn S, Ryan PY, et al., editors. Proceedings of the 2016 Conference on Financial Cryptography and Data Security; Christ Church, Barbados. Springer; 2016. p. 142–157.
[74] Seuken S, Parkes DC. Sybil-proof accounting mechanisms with transitive trust. In: Proceedings of the 2014 International Conference on Autonomous Agents and Multi-Agent Systems; Paris, France. ACM; 2014. p. 205–212.

[75] Yu H, Kaminsky M, Gibbons PB, et al. SybilGuard. ACM SIGCOMM Computer Communication Review. 2006 Aug;36(4):267–278.
[76] Seuken S, Parkes D. On the Sybil-proofness of accounting mechanisms. In: Proceedings of the 11th Workshop on the Economics of Networks, Systems and Computation; Jun.; San Jose, CA, USA; 2011. Available from: https://netecon.seas.harvard.edu/NetEcon11/Papers/Seuken_netecon11.pdf.
[77] Zhang K, Liang X, Lu R, et al. Sybil attacks and their defenses in the internet of things. IEEE Internet of Things Journal. 2014 Oct;1(5):372–383.
[78] Zhang Y, Liu W, Lou W, et al. Location-based compromise-tolerant security mechanisms for wireless sensor networks. IEEE Journal on Selected Areas in Communications. 2006 Feb;24(2):247–260.
[79] Yee B, Tygar JD. Secure coprocessors in electronic commerce applications. In: Proceedings of the 1st USENIX Workshop on Electronic Commerce; New York, NY, USA; 1995. p. 155–170.
[80] Gupta S, Sadoghi M. Blockchain transaction processing. In: Sakr S, Zomaya AY, editors. Encyclopedia of big data technologies. Cham, Switzerland: Springer; 2019. p. 366–376.
[81] Kuratowski C. Une méthode d'élimination des nombres transfinis des raisonnements mathématiques. Fundamenta Mathematicae. 1922;3:76–108.
[82] Zorn M. A remark on method in transfinite algebra. Bulletin of the American Mathematical Society. 1935 Oct;41(10):667–670.
[83] Paulauskas N, Garsva E. Computer system attack classification. Elektronika Ir Elektrotechnika. 2006;66(2):84–87.
[84] Narayanan A, Clark J. Bitcoin's academic pedigree. Queue. 2017 Aug;15(4):20–49.
[85] QuantumMechanic. Proof of stake instead of proof of work ; 2011. Accessed 28 April 2023; Available from: https://bitcointalk.org/index.php?topic=27787.0.
[86] Buterin V. A next generation smart contract & decentralized application platform ; 2014. Accessed 28 April 2023; Available from: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.
[87] Kapengut E, Mizrach B. An event study of the Ethereum transition to proof-of-stake. Commodities. 2023 Mar;2(2):96–110.
[88] Ethereum Foundation. Proof-of-stake (PoS) ; 2024. Accessed 24 February 2024; Available from: https://ethereum.org/developers/docs/consensus-mechanisms/pos.
[89] Ogawa T, Kima H, Miyaho N. Proposal of Proof-of-Lucky-Id (PoL) to solve the problems of PoW and PoS. In: Proceedings of the 2018 International Conference on Internet of Things and Green Computing and Communications and Cyber, Physical and Social Computing and Smart Data; Jul.; Halifax, Canada. IEEE; 2018. p. 1212–1218.