algorithms

MDPI

Systematic Review

Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance

Moritz Platt * and Peter McBurney

Department of Informatics, King's College London, London WC2B 4BG, UK
* Correspondence: moritz.platt@kcl.ac.uk; Tel.: +44 20 78365454

Abstract: Consensus algorithms are applied in the context of distributed computer systems to improve their fault tolerance. The explosive development of distributed ledger technology following the proposal of 'Bitcoin' led to a sharp increase in research activity in this area. Specifically, public and permissionless networks require robust leader selection strategies resistant to Sybil attacks in which malicious attackers present bogus identities to induce byzantine faults. Our goal is to analyse the entire breadth of works in this area systematically, thereby uncovering trends and research directions regarding Sybil attack resistance in today's blockchain systems to benefit the designs of the future. Through a systematic literature review, we condense an immense set of research records (N = 21,799) to a relevant subset (N = 483). We categorise these mechanisms by their Sybil attack resistance characteristics, leader selection methodology, and incentive scheme. Mechanisms with strong Sybil attack resistance commonly adopt the principles underlying 'Proof-of-Work' or 'Proof-of-Stake' while mechanisms with limited resistance often use reputation systems or physical world linking. We find that only a few fundamental paradigms exist that can resist Sybil attacks in a permissionless setting but discover numerous innovative mechanisms that can deliver weaker protection in system scenarios with smaller attack surfaces.

Keywords: blockchain; distributed ledger technology; consensus protocol; Sybil attack; member selection; leader selection

MSC: 68M14; 68M15; 68W15

JEL Classification: L86

Citation: Platt, M.; McBurney, P. Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance. *Algorithms* **2023**, *16*, 34. https://doi.org/10.3390/a16010034

Academic Editor: Manki Min

Received: 31 October 2022
Revised: 25 November 2022
Accepted: 27 November 2022
Published: 6 January 2023

1. Introduction

Decentralised systems, such as blockchains underpinning cryptocurrencies, have first introduced the need for Sybil attack resistance (see Section 1.1.5), owing to their openness. As the need for Sybil attack resistance only arises in these truly decentralised systems, research into these attacks is still in its infancy. Many different consensus mechanisms, varying greatly in specification quality, have been proposed after 2008 when Bitcoin [1] set in motion the blockchain era. This environment is particularly conducive to our research: while numerous literature reviews have targeted consensus mechanisms (see Section 3.2), to the best of our knowledge, no previous work focusing on Sybil attack resistance exists. Given the challenging effects the latest 'crypto winter' [2] might have on the blockchain industry, academia's role is to research fit-for-purpose approaches on which mature and useful systems can be built. Providing a classification and taxonomy of Sybil attack resistance schemes is key to this.

1.1. Context

The long and rich history of distributed systems research directly leads up to modern Blockchain consensus: contrary to popular belief [3,4], Nakamoto's consensus mechanism Proof-of-Work (PoW) [1] is not an isolated stroke of genius but, like many modern developments in the field of distributed systems, dependent on the rigorous work of previous generations of researchers [5]. Nakamoto's contribution is to combine well-studied ideas to enable a new class of *distributed* systems, the *decentralised* systems. This section outlines how researchers contribute to the study of decentralised consensus in creative ways, often combining decades-old findings with modern requirements.

1.1.1. Resilient Distributed Systems

The earliest attempts at remotely controlling computers before the post-war era [6] aside, the concept of geographically distributed computers collaborating was introduced in the 1950s. These early computer systems emerged in the military domain and were coordinated by transmitting generalised digital data over standard phone lines [7]. While issues of reliability were of concern in these early designs, these were met by basic error control techniques, like parity checking of input and output data, only [8]. Notably, these early systems assumed that participating computers were fully trusted and secured via military procedures. Formalisations of computer networks and their failure characteristics were put forward alongside the inception of multi-process computing in the 1960s [9]. Back then, Kleinrock [10] laid the foundation for data networking theory by proposing to research the effects of messaging delays and message prioritisation in 'large communication nets'. These theoretical foundations led to the practical implementation of formal message protocols for wide-area communication [11] and subsequently to the implementation of the Advanced Research Projects Agency Network (ARPANET) [12], the predecessor of the modern Internet, that brought with it the notion of various autonomous systems clustered in hierarchical layers [13]. These advances, however, focussed mostly on providing stable means of connecting network members in principle and did not govern higher protocol layers.

1.1.2. Byzantine Failures and Malice

Pease et al. [14] describe the problem of complex faults in a distributed system by giving an example of a bad process reporting one value to a given process and a different value to other processes. Such conflicting (and, potentially, malicious) behaviour cannot be controlled via the simple mechanisms outlined before. Instead, more complex approaches, i.e., consensus mechanisms, must be applied. Inconsistent failure modes, later formalised and termed 'byzantine' failures by Lamport et al. [15], have been widely researched and upper bounds for the proportion of byzantine participants in distributed systems (depending on the consensus mechanism used) are established.

1.1.3. From Distributed to Decentralised Systems

As Table 1 shows, decentralised systems are different from traditional distributed databases, i.e., geographically displaced, loosely coupled, computing facilities [16], since the latter assume a-priori knowledge of participants and their trustworthiness. Furthermore, they fundamentally differ from modern verifiable database systems [17,18] in that they allow cryptographic integrity assurance, but offer no censorship resistance.

Table 1. A comparison of distributed systems according to Tai et al. [19] (p. 758).

Property	Distributed	Verifiable	Blockchain
Sequential	•	•	•
Agreed			•
Ledgered		•	•
Manipulation-Resistant		•	•
Censorship-Resistant			•

Decentralised systems are, therefore, a suitable pattern to address entirely permissionless use cases, intended to be open to the world. While, in practicality, many multi-party use cases do not require this degree of decentralisation [20,21], blockchain systems that aspire to be 'unstoppable, uncensorable world computer[s]' [22] do.

1.1.4. Blockchain

The first large-scale implementation of such a system was 'Bitcoin' [1], a decentralised payment system introduced in 2008. It famously put forward the concept of decentrally collecting new transactions into blocks and forming a chain of these blocks via an energy-intensive, and often criticised [23], 'mining' process to make transactions tamper-proof, thereby coining the term *blockchain*. Beyond Bitcoin, Blockchain systems share common attributes: They can be characterised as systems that process transactions sequentially based on majority agreement and, ultimately, persist them in a tamper-resistant form on an append-only ledger [19]. For the scope of this work, the majority agreement aspect is of primary interest since the population for such a majority agreement depends on the type of system. Familiarity with the blockchain concept is assumed and this definition is provided for completeness only. (Introductory monographs provide a more comprehensive foundation from the perspectives of practitioners [24], financial technologists [25], and academics [26,27].)

Blockchain systems are most commonly categorised along two dimensions: the trust continuum and the anonymity continuum [28]. On the trust continuum, systems can be categorised as permissioned or permissionless: a *permissioned* system employs a governance process to determine who can act as a writer, whereas a *permissionless* system allows anyone to potentially assume this role. On the anonymity continuum, systems can be differentiated by being public or private: a *public* system provides all data in a publicly inspectable form, whereas a *private* one applies explicit or implicit access control mechanisms. These two dimensions can be arbitrarily composed (see Table 2). For this study, the write permission dimension is most relevant.

Table 2. Four archetypes of Blockchain architectures according to Tezel et al. [28] (p. 549).

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

While in permissioned contexts (i.e., *i* and *iii*), it can still be necessary to select a leader to orchestrate data replication, trust assumptions are often more relaxed and more akin to those of earlier distributed systems (see Section 1.1.1). This is the case because the group of potential leaders in permissioned systems can be curated, making for an inherently trustworthy population of potential leaders. In permissionless contexts (i.e., *ii* and *iv*), however, any member of the public qualifies as a potential leader. This means that entities whose goals do not align with maintaining the stability of a system and adhering to its protocol may make themselves available. This makes permissionless leader selection the harder problem.

1.1.5. Sybil Identities: A New Threat

Distributed systems theory has provided in-depth analyses of numerous system failure modes and has provided mitigations for many of those. Most of the early work, however, assumed a priori knowledge of system participants (see Section 1.1.1). In addition to this, while the abuse of telecommunications infrastructure is documented as early as the 1960s [29] and attacks on computer systems occurred frequently from the 1980s onwards [30], attacks commonly were carried out by intruders who targeted systems in which they were not members from the outside. Putting that in perspective to the categories outlined before (see Table 2), it becomes apparent that research of the pre-Blockchain era is most applicable to type *iii* (permissioned/private) systems.

It is not always possible to transfer earlier results to majority-based systems where there is no a-priori knowledge of potential leaders (i.e., type *ii* and *iv* systems) since those constitute a new phenomenon, popularised with the emergence of blockchain technology. From an attack perspective, such systems are fundamentally different from prior deployments as, in them, malicious entities can operate on the same level as trustworthy ones, for there is no authority to distinguish between those entities. This means that common approaches to mitigating intrusion risks—such as identity management, user authentication, or encryption [31]—are not feasible. Furthermore, common strategies to improve fault tolerance, like increasing redundancy, are futile in a scenario where malicious users can present arbitrarily large numbers of identities. The presentation of arbitrary entities with malice—often referred to as 'Sybil Attack' [32]—threatens large-scale peer-to-peer systems in which trusted authorities are absent. This can be attributed to the fact that, when confronted with conflicting information from multiple peers, decentralised systems need to attempt to resolve those conflicts in a way that maintains a correct system state. Determining which piece of information is to be considered *correct* is the main challenge in such scenarios.

Successful Sybil attacks manifest in different ways, depending on the consensus mechanism deployed and the scale of the attack. While successful small-scale attacks might only introduce forks or stall system operation sporadically, others may irrecoverably disable it, forcing users to abandon it or to seek 'hard forks' and the subsequent manual removal of the attacking entities [33], a technique frowned upon due to its economical and ethical ambiguity [34].

1.1.6. Consensus Mechanisms and Sybil Resistance Schemes

More formally, this consensus problem can be defined as one in which 'each process proposes some initial value, and processes that do not fail must reach an irrevocable decision on exactly one of the proposed values' [35]. In the context of blockchain, a *process* can be thought of as any potential writer (see Table 2) in a decentralised system, while *values* take the form of transaction proposals. Consensus mechanisms provide algorithms to reach a decision on a canonical system state when presented with ambiguous inputs. Often they do so by dynamically selecting a single entity—or leader—to assume the role of validator and adjudicator of inputs for a limited time. This selection is often done pseudorandomly or using voting. The target of such a leader selection process is to select a leader who processes any inputs according to the system protocol while avoiding the selection of adversaries that violate system protocol.

In general, at most m adversaries can be tolerated for systems with $3m + 1$ total participants [15]. Therefore, to maintain an operational state, the likelihood of selecting an adversary as a leader in a decentralised system needs to be minimised. This is the purpose of Sybil resistance schemes, many of which will be analysed in this paper. Academic works discussing Sybil resistance schemes come in many different forms, oftentimes as a key component of a consensus mechanism, other times as a standalone proposal. In our work, we focus on extracting any information relevant to Sybil attack resistance from the papers analysed, regardless of which context it is discussed in.

1.2. Motivation

Making sound architectural decisions for decentralised systems is challenging: a variety of different potential designs exist and, apart from usual functional and non-functional requirements, the choice of consensus mechanism shapes decentralised systems in hard-to-revert ways. The choice of consensus mechanism dictates whether a system requires a central admissions process or can be entirely open to the public. Due to the underlying trust assumptions, it furthermore influences the performance of a system, the hardware demands on participants, and the cost of deployment and operation.

Particularly the choice for or against a mechanism with strong Sybil attack resistance properties is decisive: due to being rooted in the blockchain movement, many of the existing consensus mechanisms claim Sybil attack resistance. However, as our analysis will show, many schemes only deliver on that claim under certain, limited, conditions. It is, therefore, necessary to firmly establish a framework that established Sybil attack resistance as one of the key elements of decentralised systems design. This will help the field to focus research efforts on useful areas in which decentralised technology can be applied, rather than reinventing the wheel or making costly design mistakes.

1.3. Organisation

The remainder of this paper is structured as follows: In Section 2, we describe the search strategy applied along with the search systems used to gain the broadest possible exposure to relevant works. In Section 3, we present our results, initially analysing existing secondary literature on consensus mechanisms (see Section 3.2). Subsequently, we analyse the primary literature, i.e., the original works discovered. We group works into mechanisms for democratic processes (see Section 3.3), mechanisms for the education sector (see Section 3.4), mechanisms for the energy sector (see Section 3.5), general purpose mechanisms (see Section 3.6), mechanisms for healthcare (see Section 3.7), mechanisms that seek to improve performance (see Section 3.8), mechanisms for Internet of Things (IoT) (see Section 3.9), mechanisms for media and entertainment (see Section 3.10), mechanisms for supply chain management (see Section 3.11), mechanisms for the telecommunications sector (see Section 3.12), Proof-of-useful-work (PoUW) schemes (see Section 3.13), and mechanisms for vehicles (see Section 3.14). We then conclude with a comment on the current state of literature and avenues for future work (see Section 4).

1.4. Scope

For a comprehensive review, we apply a broad definition of academic works, that includes research papers, technical reports, pre-prints, and theses. We consider any work that describes a consensus mechanism, a leader selection approach, or a Sybil attack resistance scheme reasonably well. This includes many works that describe technologies that do not have Sybil attack resistance as a design goal (including many Byzantine fault tolerance (BFT) schemes). These are included for completeness.

1.5. Contribution

This work offers a comprehensive review of the blockchain consensus mechanism landscape. While many similar efforts have been undertaken (see Section 3.2), this manuscript can be differentiated from those by the method of categorising relevant works: it taxonomises individual contributions using a novel composition of key mechanism attributes (Sybil attack resistance class, reward scheme, and leader selection methodology). This approach allows us to provide an objective and comprehensive overview of the field that clearly describes which Sybil attack resistance class is prevalent in the field. Grouping by industry, furthermore, allows the reader to determine which verticals have seen research interest. Lastly, by analysing the full breadth of the literature, this work shows which technological building blocks are commonly applied within different Sybil attack resistance classes (e.g., PoW in strongly Sybil attack resistant systems). These analyses

provide the groundwork for researchers wishing to extend the state of the art in consensus mechanism research.

2. Methods

The goal of this work is to gain an understanding of the full breadth of available leader selection strategies. During the preliminary screening, consensus mechanisms in the context of blockchain were found in various types of academic literature: while many algorithms are published in dedicated papers that are easy to discover based on their title alone, others are discussed as part of wider research works, such as technical papers introducing new system constructs. Thus, to also include manuscripts in which consensus mechanisms are not the central concern, queries need to be broad. The selection of academic search systems to retrieve manuscripts relevant to the research question is informed by the findings of Gusenbauer and Haddaway [36] who categorise academic search systems. All systems that provide the following functions are considered:

- The system focuses on Computer Science or has a multidisciplinary focus
- The system supports Boolean operators (at least `AND` and `OR`)
- The system supports parentheses
- The system allows for bulk download of 50 results or more

Seven academic search systems (see Table 3) provide this functionality [36], including the highly relevant offerings by the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE). For each of the academic search systems, a broad query is formulated. While individual query syntax varies, queries are modelled after the following example search string:

```
(
Blockchain OR
"Distributed Ledger" OR
"Crypto Currency" OR
Cryptocurrency OR
Cryptocurrencies
) AND (
Consensus OR
"Proof-of-" OR
Membership
)
```

Table 3. Search results returned from targeted search systems.

Operator	Search System	Results
ACM	Guide to Computing Literature	519
Bielefeld University Library	BASE	5890
IEEE	Xplore	1846
Elsevier	ScienceDirect	3186
Elsevier	Scopus	4084
Springer Nature	SpringerLink	3519
Clarivate Analytics	Web of Science	2755

Since this review targets leader selection strategies in the context of blockchain, the term *Blockchain*, or the closely related terms *Distributed Ledger* and *Cryptocurrency* are required. Similarly, since leader selection is central to consensus mechanisms, the term *Consensus*, or the related term *Membership* is required. Furthermore, the commonly used construct *Proof-of-** is admissible.

2.1. Search Results

The total number of results returned (21,799) raises confidence in the search queries being sufficiently broad. The queries were executed in the week of 26 April 2021. The number of results reflects the manuscripts indexed at this time. Since the queries do not

impose any limitations on the manuscript type, a broad range of scientific works, both peer-reviewed and not peer-reviewed, are returned (see Section 1.4). For this review, all result types, including pre-prints, are considered. These results form the input to the following multi-step manuscript screening process (see Figure 1).

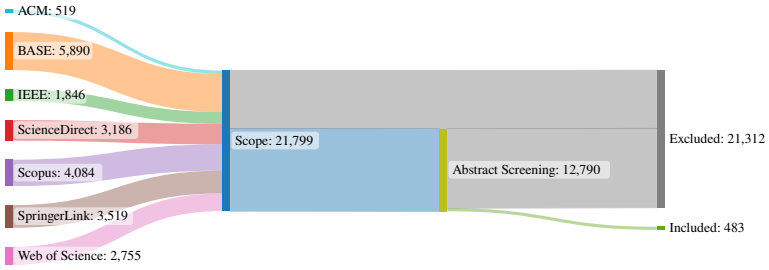

Figure 1. A total of 21,799 records—many of which were duplicates—were obtained from scientific search engines. During the manuscript screening process, 12,790 scientific manuscripts were initially analysed. After de-duplication and analysis of the abstracts and manuscript contents, 483 were found relevant for this study.

2.2. Duplicate Resolution

'EPPI-Reviewer', a software suite for research synthesis, is used to manage sources and screen manuscripts. The step in the review process is to apply the built-in 'Manage Duplicates' functionality to correlate duplicates automatically. While this functionality was found to be less effective than other de-duplication software [37], a significant number of duplicates (7,861) is discovered. Additional instances, however, remain undetected and will be treated manually after this automated step.

2.3. Abstract Screening

Following duplicate resolution, titles and abstracts of results are screened for relevancy. Here, the following questions are answered:

- Is the result published in 2008 or after?
- Is the result written in the English language?
- Does the result describe a primary article (e.g., an original research article) or a secondary article (e.g., a review)?
- Does the article concern the field of computer science?
- Does the article concern decentralised computing?
- Does the article describe a consensus mechanism?

Should either of the questions be answered with *no*, the manuscript is automatically excluded. Should all of the questions be answered with *yes* or *unclear*, the manuscript will be included for further analysis.

The abstract screening process eliminated a large number of manuscripts (9009). However, the remaining candidate list still contained numerous duplicates which were removed manually based on similarities of title, author list, or digital object identifier during abstract screening.

During the manual screening, the full texts of the documents were obtained online. Documents were only considered if digital access was granted to them via King's College London library subscriptions. Manuscripts that would only have been available in print or via interlibrary loan were not obtained. Still, the vast majority of full texts were obtainable and only a very small number could not be accessed. The full texts were then briefly examined to understand whether they were indeed relevant and, only if found so, were fully analysed. They were then categorised as either primary literature (i.e., works that proposed an individual mechanism) or secondary literature (i.e., surveys and taxonomies).

3. Results

We organise the results by common sectors to gain a better understanding of the needs of particular industry verticals. This also helps us to further analyse which system properties occur together, e.g., we find that many use cases in IoT (see Section 3.9) have no or limited Sybil attack resistance due to the limited computational capabilities of IoT devices.

3.1. Aspects of Interest

We are particularly interested in some key elements of Sybil attack resistance schemes. First, what level of Sybil attack resistance they provide when deployed (see Table 4). We assume that the mechanism in question is deployed to a *large-scale* system, as many Sybil attack resistance effects only materialise with high usage volume, as can be seen when considering the likelihood of 51% attacks on PoW systems with low popularity [38]. For Sybil attack resistance, we introduce three categories: Strong Sybil attack resistance; meaning a mechanism that, when applied to a sizeable system, could not be attacked, even by an irrational attacker, unless they incur tremendous cost. Limited Sybil attack resistance; meaning an attacker might be successful with an attack if they are ready to incur significant cost and orchestrate an attack over a long time. No Sybil attack resistance, meaning an attacker could easily overwhelm a public/permissionless system using the mechanism in question. The latter category is not to be seen as criticism of the mechanism: it mostly applies to environments in which the mechanism designers do not have to consider Sybil attacks.

Table 4. Three categories of Sybil attack resistance.

Category	Cost	**Coordination Effort**	**Time Expenditure**
Strong Sybil attack resistance	Excessive	High	Extreme
Limited Sybil attack resistance	High	High	High
No Sybil attack resistance	Negligible	Negligible	Negligible

Second, whether an incentive scheme is part of the proposed mechanism. Here, we analyse whether participants receive rewards for adherence to the protocol and/or punishment for deviating from it. Third, the application of random/pseudorandom numbers during the execution of the mechanism. Fourth, whether the mechanism is somehow linked to the physical world, e.g., by asserting on messages generated by users having access to a central processing unit (CPU) with a Trusted Execution Environment (TEE). Fifth, whether a reputation system is applied in the context of the mechanism: such a system may be used to inform leader selection based on reputation signals from other participants or from central sources. Sixth, whether the mechanism is intended to be applied in permissioned or permissionless settings. Here we are particularly interested in outlier mechanisms with strong Sybil attack resistance that are applied in permissioned settings or mechanisms with weak Sybil attack resistance being applied in permissionless settings. Last, we outline the leader selection method, foremost by analysing whether the mechanism relies on (pseudo-)randomness, an election, or a pre-formed committee. Many mechanisms combine multiple factors. In such case, we aim to call out the dominant factor.

3.2. Secondary Literature

To gain an overview of the available works and to understand which mechanisms are deemed most relevant by the research community, the secondary literature was analysed (see Table 5). Here, we find that most researchers align on a small number of major mechanisms: in the secondary literature analysed, only PoW (see Appendix D.224), Proof-of-Stake (PoS) (see Appendix D.212), Practical Byzantine Fault Tolerance (PBFT) (see Appendix D.147), Delegated Proof-of-Stake (DPoS) (see Appendix D.72), and Proof of Elapsed Time (PoET) (see Appendix D.154) are mentioned by more than half of the works. This foreshadows the analysis of the primary literature where we find several works that have received hardly any attention so far. These most commonly discussed mechanisms

reflect the breadth of the entire field well as they include permissionless mechanisms (e.g., PoW), permissioned mechanisms (e.g., PBFT), and mechanisms that make use of physical world linking (e.g., PoET by using TEE).

Table 5. Secondary literature analysed during manuscript screening.

	PoW (Appendix D.224)	PoS (Appendix D.212)	PBFT (Appendix D.147)	DPoS (Appendix D.72)	PoET (Appendix D.154)	Proof-of-Space (Appendix D.209)	Proof-of-Burn (Appendix D.177)	Proof-of-Activity (Appendix D.168)	Proof-of-Importance (Appendix D.187)	Raft (Appendix D.230)	Proof-of-Authority (Appendix D.157)	dBFT (Appendix D.66)	Proof-of-Luck (Appendix D.157)
Aggarwal and Kumar [39]	●	●	●	●	●	●	●	●	●	○	○	○	○
Aggarwal et al. [40]	●	●	●	●	●	●	●	○	○	○	●	○	○
Ahmad et al. [41]	●	●	●	○	●	○	○	○	○	○	○	○	○
Ali Syed et al. [42]	●	●	●	○	●	●	○	○	○	○	○	○	○
Alsaqqa and Almajali [43]	●	○	●	○	○	●	●	●	●	○	●	○	○
Alsunaidi and Alhaidari [44]	●	●	●	●	○	○	○	●	●	●	○	○	●
Andoni et al. [45]	●	●	●	●	●	●	●	●	○	○	●	○	○
Andrey and Petr [46]	●	●	○	●	○	●	●	●	●	○	○	○	○
Antal et al. [47]	●	●	○	○	○	○	●	●	○	●	●	○	○
Azbeg et al. [48]	●	●	●	●	●	●	●	○	○	○	●	○	○
Bach et al. [49]	●	○	○	●	○	○	○	○	●	○	○	●	○
Bamakan et al. [50]	●	●	●	●	●	●	●	●	●	○	○	●	○
Bashar et al. [51]	●	●	○	○	●	●	●	●	●	○	●	○	●
Belotti et al. [52]	●	●	●	●	●	○	○	○	●	○	○	○	○
Bhutta et al. [53]	●	●	●	●	●	●	●	○	●	○	○	●	●
Dabbagh et al. [54]	●	●	●	○	○	○	○	●	○	●	○	○	○
Dhaiouir and Assar [55]	●	●	●	●	○	○	○	○	○	○	○	○	○
Ferdous et al. [56]	●	●	○	○	○	○	●	○	●	○	○	○	○
Ferrag et al. [57]	●	●	●	●	●	●	●	●	●	○	●	●	○
Fournier and Petrillo [58]	●	○	○	○	○	○	○	○	○	○	○	○	●
Fu et al. [59]	●	●	●	●	○	○	●	●	○	○	○	●	●
Hao et al. [60]	●	○	●	○	○	○	○	○	○	○	○	○	○
Hazari and Mahmoud [61]	●	●	●	○	○	○	●	○	●	○	○	○	○
He et al. [62]	●	●	○	●	●	●	●	●	●	○	○	○	●
Hellwig et al. [63]	●	●	●	●	●	●	○	○	○	○	●	○	○
Honnavalli et al. [64]	○	○	●	○	○	○	○	○	○	○	●	○	○
Indhuja and Venkatesulu [65]	●	●	●	●	●	●	○	●	●	○	○	●	○
Ismail and Materwala [66]	●	●	●	●	●	●	●	●	●	●	●	●	○
Jayabalan and N [67]	●	●	●	○	●	○	○	○	○	●	○	○	○
Jennath and Asharaf [68]	●	●	○	○	●	●	●	●	●	○	●	○	○
Katarya and Vats [69]	●	●	●	●	○	○	○	○	○	●	○	○	○
Kaur et al. [70]	●	●	●	●	●	○	○	○	○	○	●	○	○
Khamar and Patel [71]	●	●	●	●	●	○	○	●	●	●	○	●	●
Lao et al. [72]	●	●	●	○	○	●	●	○	●	○	●	○	○

Table 5. *Cont.*

	PoW (Appendix D.224)	PoS (Appendix D.212)	PBFT (Appendix D.147)	DPoS (Appendix D.72)	PoET (Appendix D.154)	Proof-of-Space (Appendix D.209)	Proof-of-Burn (Appendix D.177)	Proof-of-Activity (Appendix D.168)	Proof-of-Importance (Appendix D.187)	Raft (Appendix D.230)	Proof-of-Authority (Appendix D.157)	dBFT (Appendix D.66)	Proof-of-Luck (Appendix D.157)
Lashkari and Musilek [73]	●	●	●	●	●	●	●	●	○	●	●	●	●
Lasisi and Hsu [74]	○	○	●	○	○	○	○	○	○	○	○	○	○
Lepore et al. [75]	●	●	○	○	○	○	○	○	○	○	○	○	○
MacKenzie et al. [76]	●	●	●	○	○	○	○	○	○	○	○	○	●
Maple and Jackson [77]	●	●	●	○	●	○	○	○	○	○	○	○	○
Masood and Faridi [78]	●	●	○	○	●	●	●	○	○	○	○	○	○
Masood and Faridi [79]	○	○	●	○	○	○	○	○	○	●	○	○	○
Mingxiao et al. [80]	●	●	●	●	○	○	○	○	○	●	○	○	○
Monrat et al. [81]	●	●	●	●	○	○	○	○	○	○	○	○	○
Naz and Lee [82]	●	●	●	●	●	○	○	○	○	○	○	○	○
Nguyen and Kim [83]	●	●	●	●	●	●	●	●	○	●	○	○	●
Nijsse and Litchfield [84]	●	●	●	●	●	○	○	○	○	○	○	○	○
Pahlajani et al. [85]	●	●	○	○	●	●	○	○	○	○	○	○	●
Panda et al. [86]	●	●	○	○	○	○	○	○	○	●	○	○	○
Perez et al. [87]	●	●	○	○	○	○	○	○	●	○	○	○	○
Praveen et al. [88]	●	●	●	●	●	●	●	●	●	●	○	●	○
Ramkumar et al. [89]	●	●	●	○	●	●	●	●	○	○	○	●	○
Sharma and Jain [90]	●	●	●	●	●	●	●	●	●	○	○	○	○
Srivastav et al. [91]	●	●	●	●	○	●	●	○	○	○	○	●	○
Verma et al. [92]	●	●	●	○	●	●	●	●	●	●	○	○	●
Wang et al. [93]	●	●	●	●	○	○	○	○	○	○	○	○	○
Wazid et al. [94]	●	●	●	●	●	●	●	●	●	○	○	●	○
Xiao et al. [95]	●	●	●	○	●	○	○	○	○	○	○	○	○
Xiao et al. [96]	●	●	●	●	●	○	○	○	○	○	●	○	○
Yin et al. [97]	●	●	●	○	●	●	●	○	○	●	○	○	○
Yousuf et al. [98]	●	●	○	○	○	○	○	○	○	○	○	○	○
Zhang and Lee [99]	●	●	●	●	○	○	○	○	○	○	○	○	○
Zhao et al. [100]	●	●	○	○	●	●	○	○	○	○	○	○	○

●: Included, ○: Not included.

3.3. Mechanisms for Democratic Processes

Only five mechanisms were categorised as targeting the facilitation of democratic processes (see Table 6). A key responsibility for such systems is to orchestrate voting on ledger: to support this, an underlying consensus mechanism should make block producer selection subject to a free election [101] (Figure 12), a pre-requisite that is met in the Proof-of-Credibility mechanism proposed by Abuidris et al. [102]. The majority of the mechanisms target permissionless systems, thereby contributing to the debate about the suitability of consensus mechanisms for public democratic blockchain systems [103]. Some mechanisms approach Sybil attack resistance through personal encounters in the physical world [104,105], while others apply PoS-like mechanics to credibility scores [102,106].

Table 6. Consensus mechanisms in *democracy*.

			Inc					Perm		
	Ref	**SA**	**+**	**—**	**Ra**	**Ph**	**Re**	**Pn**	**Pl**	**Sel**
Democratic Byzantine Fault Tolerance [107]	Appendix A.2	▽	○	○	○	○	○	●	○	None
Consensus for e-Democracy [106]	Appendix A.1	▶	○	○	○	○	○	○	●	
Proof-of-Credibility [102]	Appendix A.4	▶	○	○	●	○	●	○	●	Elec.
Encointer [104]	Appendix A.3	▶	○	○	●	●	○	○	●	Rand.
Proof-of-Personhood [105]	Appendix A.5	▶	●	○	●	●	○	○	●	Rand.

Ref: Section reference, **SA**: Sybil attack resistance class, **Inc +**: Reward scheme, **Inc —**: Punishment scheme, **Ra**: Randomisation, **Ph**: Physical world linking, **Re**: Reputation system, **Perm Pn**: Permissioned, **Perm Pl**: Permissionless, **Sel Rand.**: Random leader selection, **Sel Comm.**: Committee-based leader selection, **Sel Elec.**: Leader selection via election. ▲: Strong Sybil attack resistance, ▶: Limited Sybil attack resistance, ▽: No Sybil attack resistance. ●: Applicable, ○: Not applicable.

3.4. Mechanisms for Education

Steiu [108] identifies 'digitalisation and decentralisation of educational certifications' and 'lifelong learning' as key drivers for the deployment of blockchain technology in an educational context. Additionally, Hsu et al. [109] define the main challenges of smart education environments as 'trust, privacy, and transparency'. Consequently, some researchers suggested the application of blockchain technology to these environments. While, with only three mechanisms, the education category is sparse, some commonalities can be made out: as Table 7 shows, none of the proposed Sybil attack resistance schemes explicitly assume a permissionless system. The 'Group-Based Consensus for Educational Systems' [110], for example, assumes a hierarchical system of educational stakeholders.

Table 7. Consensus mechanisms in *education*.

			Inc					Perm		
	Ref	**SA**	**+**	**—**	**Ra**	**Ph**	**Re**	**Pn**	**Pl**	**Sel**
Group-Based Consensus for Educational Systems [110]	Appendix B.1	▽	○	○	○	○	●	●	○	Elec.
Proof-of-Reputation [111]	Appendix B.3	▶	●	○	●	○	●	○	○	
Improved DPoS [112]	Appendix B.2		○	○	○	○	○	○	○	

Ref: Section reference, **SA**: Sybil attack resistance class, **Inc +**: Reward scheme, **Inc —**: Punishment scheme, **Ra**: Randomisation, **Ph**: Physical world linking, **Re**: Reputation system, **Perm Pn**: Permissioned, **Perm Pl**: Permissionless, **Sel Rand.**: Random leader selection, **Sel Comm.**: Committee-based leader selection, **Sel Elec.**: Leader selection via election. ▲: Strong Sybil attack resistance, ▶: Limited Sybil attack resistance, ▽: No Sybil attack resistance. ●: Applicable, ○: Not applicable.

3.5. Mechanisms for Energy

The energy sector is seeing a considerable amount of blockchain-related research (see Table 8). This is not surprising since, as Brilliantova and Thurner [113] attest, relevant requirements are arising in the energy sector as a result of the movement towards peer-to-peer (P2P) energy trading. As Andoni et al. [45] assert, blockchain technology can empower consumers and small electricity generators. While challenges, such as regulatory uncertainty and environmental questions, remain [114], decentralised technology was found to be a good fit for blockchain technology, specifically to combat the existing security issues of smart grid systems [115]. With regards to Sybil attack resistance it is worth mentioning that, apart from two [116,117], all reviewed mechanisms expose limited or no Sybil attack resistance. This can, in most cases, be attributed to the fact that energy trading needs to rely on central entities, like distribution system operators, to provide reliable meter readings [118] both for the consumption and production of electricity. Therefore, permissioned systems [119–131] are dominating the energy space.

Table 8. Consensus mechanisms in *energy*.

			Inc					Perm		
	Ref	**SA**	**+**	**—**	**Ra**	**Ph**	**Re**	**Pn**	**Pl**	**Sel**
Communicate Proof-of-Credit [116]	Appendix C.1	▲	●	◌	●	◌	●	◌	●	Rand.
Decentralised Consensus Decision-Making [117]	Appendix C.7	▲	◌	◌	●	◌	◌	◌	●	Rand.
Consensus Resource Slicing Model [119]	Appendix C.2	▽	◌	◌	●	◌	◌	●	◌	Rand.
Credit-Based PoW [120]	Appendix C.4	▽	●	◌	●	◌	◌	●	◌	Rand.
Dynamic-Reputation Practical Byzantine Fault Tolerance [121]	Appendix C.8	▽	◌	◌	◌	◌	●	●	◌	Elec.
Enhanced Proof-of-Work [132]	Appendix C.9	▽	◌	◌	◌	◌	◌	◌	◌	
Fast, Secure and Distributed Consensus Mechanism for Energy Trading Among Vehicles using Hashgraph [133]	Appendix C.10	▽	◌	◌	●	◌	●	◌	◌	None
Hyper Delegation Proof-of-Randomness [122]	Appendix C.11	▽	◌	◌	◌	◌	◌	●	◌	
Improved Proof of Work [123]	Appendix C.12	▽	◌	◌	●	◌	◌	●	◌	Rand.
Lightweight DPoS for Energy Transmitters [124]	Appendix C.13	▽	●	●	●	◌	◌	●	◌	
Proof-of-Credit-Threshold [125]	Appendix C.15	▽	◌	◌	◌	◌	◌	●	◌	
Proof-of-Energy-Generation [126]	Appendix C.16	▽	●	◌	◌	◌	◌	●	◌	
Proof-of-Cooperation [134]	Appendix C.18	▽	◌	◌	●	◌	●	◌	◌	Elec.
Proof-of-Efficiency [127]	Appendix C.19	▽	◌	◌	◌	◌	●	●	◌	
Proof-of-Generation [128]	Appendix C.20	▽	◌	◌	●	◌	◌	●	◌	Rand.
Proof-of-Work based on Reputation [129]	Appendix C.21	▽	◌	◌	●	◌	◌	●	◌	Comm.
Credibility Consensus [130]	Appendix C.3	▶	●	◌	◌	◌	◌	●	◌	Elec.
Credit-Based Concurrent Block Building Consensus [135]	Appendix C.5	▶	●	◌	●	◌	●	◌	◌	Elec.
Lightweight Credibility-Based Equity Proof Consensus [136]	Appendix C.14	▶	●	◌	●	◌	◌	◌	◌	Rand.
Cross-Layer Trust-Based Consensus [131]	Appendix C.6		●	◌	●	◌	●	●	◌	Rand.
Proof-of-Benefit [137–140]	Appendix C.17		◌	◌	◌	◌	●	◌	●	

Ref: Section reference, **SA**: Sybil attack resistance class, **Inc +**: Reward scheme, **Inc —**: Punishment scheme, **Ra**: Randomisation, **Ph**: Physical world linking, **Re**: Reputation system, **Perm Pn**: Permissioned, **Perm Pl**: Permissionless, **Sel Rand.**: Random leader selection, **Sel Comm.**: Committee-based leader selection, **Sel Elec.**: Leader selection via election. ▲: Strong Sybil attack resistance, ▶: Limited Sybil attack resistance, ▽: No Sybil attack resistance. ●: Applicable, ◌: Not applicable.

3.6. General Purpose Mechanisms

This catch-all category captures the majority (57 %) of all algorithms analysed. It contains all algorithms that are not industry-specific, as well as some targeted at 'exotic' domains, such as astronautics [141]. In this category, a large number of schemes with strong Sybil attack resistance are contained, including those with large overall popularity [142–152]. As seen in Table 9, mechanisms with strong Sybil attack resistance are commonly targeted towards permissionless systems and often apply random leader selection strategies. Mechanisms without Sybil attack resistance, unsurprisingly, target permissioned systems and make use of election-based leader selection. In some cases, these mechanisms follow deterministic leader selection methods that are not captured by our categorisation. Schemes with limited Sybil attack resistance make heavy use of physical world linking to achieve Sybil attack resistance: some by using CPUs [153] or TEEs [146,152,154–158], others

by relying on IP addresses [159–161], mobile phones [162], or physical proximity [163–167]. Incentive schemes are common in mechanisms with strong Sybil attack resistance, likely because these are expected in permissionless systems. Most incentive schemes rely on rewards [142,143,145,149,150,153,153,155,158,163,168–260] for adherence to the protocol, with only some incorporating penalties [158,168–178,261].

Table 9. *General* consensus mechanisms.

			Inc					Perm		
	Ref	**SA**	**+**	**—**	**Ra**	**Ph**	**Re**	**Pn**	**Pl**	**Sel**
Bitcoin-NG [179]	Appendix D.2	▲	●	○	●	○	○	○	●	Rand.
ECDLP-based PoW [180]	Appendix D.4	▲	●	○	●	○	○	○	●	Rand.
PoS Based on Credit Rewards and Punishments [262]	Appendix D.6	▲	○	○	○	○	●	○	●	Elec.
PoS Based on Verifiable Random Functions [181]	Appendix D.7	▲	●	○	●	○	○	○	●	Rand.
PoS for Bitcoin Sidechains [168]	Appendix D.8	▲	●	●	●	○	○	○	●	Rand.
PoS with Behavior Score and Trust Rating [182]	Appendix D.9	▲	●	○	○	○	●	○	●	Elec.
PoS with Waiting-Time First-Price Auctions [183]	Appendix D.12	▲	●	○	●	○	○	○	●	Rand.
PoS with Weighted Voting [184,185]	Appendix D.13	▲	●	○	●	○	●	○	●	Rand.
PoW Based on Power Analysis of Low-End Microcontrollers [187]	Appendix D.15	▲	●	○	●	○	○	○	●	Rand.
PoW on quadratic multivariate equations [263,264]	Appendix D.16	▲	○	○	●	○	○	○	●	Rand.
PoW with Early Stage PoS [188]	Appendix D.17	▲	●	○	●	○	○	○	●	Rand.
PoW with Personalized Difficulty Adjustment [190]	Appendix D.19	▲	●	○	●	○	○	○	●	Rand.
PoW with Quantum-Resistant Hash Collision [191]	Appendix D.20	▲	●	○	○	○	○	○	●	Rand.
pVFR for PoW [265]	Appendix D.21	▲	○	○	●	○	○	○	●	Rand.
Albatross [169]	Appendix D.24	▲	●	●	●	○	○	○	●	Rand.
Alt-PoW [192]	Appendix D.25	▲	●	○	●	○	○	○	●	Rand.
Attack-Tolerant PoW [193]	Appendix D.29	▲	●	○	●	○	○	○	●	Rand.
B4SDC [194]	Appendix D.32	▲	●	○	●	○	○	○	●	Rand.
BeaconBlocks [266]	Appendix D.34	▲	○	○	●	○	○	○	○	Rand.
Block Maturity Level [195]	Appendix D.36	▲	●	○	●	○	○	○	●	Rand.
Bobtail [198]	Appendix D.40	▲	●	○	●	○	○	○	●	Rand.
Chains of Activity [199]	Appendix D.44	▲	●	○	●	○	○	○	●	Rand.
Client-Assisted Consensus [267]	Appendix D.46	▲	○	○	●	○	○	○	○	
CloudPoS [268]	Appendix D.48	▲	○	○	○	○	○	○	●	Elec.
Composite Framework Leveraging Proof-of-Stake and Proof-of-Work [201]	Appendix D.51	▲	●	○	●	○	●	○	●	Rand.
Conflux [202]	Appendix D.52	▲	●	○	●	○	○	○	●	Rand.
Crux [269]	Appendix D.59	▲	○	○	●	○	○	○	●	Elec.
Cumulative Proof-of-Work [204]	Appendix D.60	▲	●	○	●	○	○	○	●	Rand.
Delegated Proof of Stake with Downgrade [270]	Appendix D.68	▲	○	○	●	○	●	○	●	Rand.
Delegated Proof-of-Reputation [206]	Appendix D.71	▲	●	○	○	○	●	○	●	Elec.
Delegated Proof-of-Stake [145]	Appendix D.72	▲	●	○	●	○	○	○	●	Elec.

Table 9. *Cont.*

	Ref	SA	Inc +	Inc −	Ra	Ph	Re	Perm Pn	Perm Pl	Sel
Deterministic Proof-of-Work [271]	Appendix D.75	▲	○	○	○	○	○	○	●	Elec.
Equihash [207]	Appendix D.84	▲	●	○	●	○	○	●	●	Rand.
Error-Correction Code Based Proof-of-Work [208]	Appendix D.85	▲	●	○	○	○	○	○	●	Rand.
Estimable PoW [209]	Appendix D.86	▲	●	○	●	○	○	○	●	Rand.
extended PoS [272]	Appendix D.87	▲	○	○	●	○	○	○	●	Rand.
Fair Proof-of-Work System With Computing Power Rating [210]	Appendix D.89	▲	●	○	●	○	●	○	●	Rand.
Fair selection protocol for committee-based permissionless blockchains [273]	Appendix D.90	▲	○	○	○	○	○	●	●	Rand.
Fantômette [170]	Appendix D.91	▲	●	●	●	○	○	○	●	Rand.
Filtered Proof-of-Work [274]	Appendix D.95	▲	○	○	●	○	○	○	●	Rand.
Goshawk [211]	Appendix D.97	▲	●	○	●	○	○	○	●	Rand.
Greedy Observed Largest Forest [275]	Appendix D.99	▲	○	○	●	○	○	○	●	Rand.
HashCore [276]	Appendix D.104	▲	○	○	●	○	○	○	●	Rand.
Hybrid PoW/PoS [277]	Appendix D.106	▲	○	○	●	○	●	○	○	Rand.
Hybrid PoW/PoS [213]	Appendix D.107	▲	●	○	●	○	○	○	●	Rand.
Hybrid Consensus with flexible Proof-of-Activity [214]	Appendix D.109	▲	●	○	●	○	○	○	●	Rand.
Improved DPoS with K-Means [215]	Appendix D.112	▲	●	○	●	○	●	○	○	Elec.
Interactive Proof-of-Stake [216]	Appendix D.113	▲	●	○	●	○	○	○	●	Rand.
Itsuku [278]	Appendix D.115	▲	○	○	●	○	○	○	●	Rand.
MaGPoS [171]	Appendix D.120	▲	●	●	○	○	○	○	●	
Multi-tokens Proof of Stake [218]	Appendix D.127	▲	●	○	●	○	○	○	●	Rand.
Multiple Winners Proof of Work [219]	Appendix D.128	▲	●	○	●	○	○	○	●	Rand.
NeuCoin [173]	Appendix D.131	▲	●	●	●	○	○	○	●	Rand.
Open Representative Voting [279]	Appendix D.133	▲	○	○	○	○	○	○	●	Elec.
Optical Proof-of-Work [220]	Appendix D.134	▲	●	○	●	○	○	○	●	Rand.
Ouroboros Crypsinous [280]	Appendix D.135	▲	○	○	○	○	○	○	●	Elec.
Ouroboros Genesis [281]	Appendix D.136	▲	○	○	○	○	○	○	●	Rand.
Ouroboros Praos [282]	Appendix D.137	▲	○	○	●	○	○	○	●	Rand.
Parallel Proof-of-Work [221]	Appendix D.138	▲	●	○	●	○	○	○	●	Rand.
Penalty by Consensus in PoW [174]	Appendix D.140	▲	●	●	○	○	○	○	●	Rand.
Pixel [283]	Appendix D.144	▲	○	○	●	○	○	○	●	Rand.
PoolCoin [222]	Appendix D.146	▲	●	○	●	○	●	○	●	Rand.
Prism [223]	Appendix D.149	▲	●	○	●	○	○	○	●	Rand.
Private Proof-of-Effort [284]	Appendix D.150	▲	○	○	●	○	○	○	●	Rand.
Proof of Adjourn [285]	Appendix D.151	▲	○	○	●	○	○	○	●	Rand.
Proof of Contribution [224]	Appendix D.153	▲	●	○	●	○	●	○	●	Rand.
Proof of Experience [225]	Appendix D.155	▲	●	○	●	○	○	○	●	Rand.
Proof of Segmented Work [226]	Appendix D.159	▲	●	○	●	○	○	○	○	Rand.
Proof-of-Accumulated-Work [286]	Appendix D.165	▲	○	○	●	○	○	○	●	Rand.
Proof-of-Activity [149]	Appendix D.168	▲	●	○	●	○	○	○	●	Rand.
Proof-of-Behavior [287]	Appendix D.173	▲	○	○	●	○	●	○	●	
Proof-of-Burn [148]	Appendix D.177	▲	○	○	○	○	○	○	●	

Table 9. *Cont.*

	Ref	SA	Inc +	Inc −	Ra	Ph	Re	Perm Pn	Perm Pl	Sel
Proof-of-Credit [261]	Appendix D.182	▲	○	●	●	○	●	○	○	Rand.
Proof-of-Discrete Logarithm [234]	Appendix D.183	▲	●	○	●	○	○	○	●	Rand.
Proof-of-Equivalence [165]	Appendix D.184	▲	○	○	○	○	●	○	●	Rand.
Proof-of-Human-Work [236]	Appendix D.186	▲	●	○	●	○	○	○	●	Rand.
Proof-of-Importance [150]	Appendix D.187	▲	●	○	○	○	○	○	●	
Proof-of-Interaction [237]	Appendix D.188	▲	●	○	●	○	○	○	●	Rand.
Proof-of-Lottery [238]	Appendix D.190	▲	●	○	●	○	○	○	●	Rand.
Proof-of-Participation [241]	Appendix D.195	▲	●	○	●	○	○	○	●	Rand.
Proof-of-Prestige [288]	Appendix D.199	▲	○	○	●	○	●	○	●	Rand.
Proof-of-Replicated-Storage [289]	Appendix D.202	▲	○	○	○	○	○	○	●	
Proof-of-Reproducibility [290]	Appendix D.203	▲	○	○	○	○	●	○	●	Rand.
Proof-of-Reputation with Nakamoto Fallback [291]	Appendix D.205	▲	○	○	○	○	●	○	●	Elec.
Proof-of-Space [147]	Appendix D.209	▲	○	○	○	○	○	○	●	
Proof-of-Stake [143]	Appendix D.212	▲	●	○	○	○	○	○	●	
Proof-of-Stake for Bitcoin Subchains [245]	Appendix D.213	▲	●	○	●	○	○	○	●	Rand.
Proof-of-Strategy [246]	Appendix D.215	▲	●	○	●	○	●	○	●	Elec.
Proof-of-Work [1,142]	Appendix D.224	▲	●	○	●	○	○	○	●	Rand.
Proof-of-Work Applied to the Clique Problem [292]	Appendix D.225	▲	○	○	●	○	○	○	●	Rand.
Proof-of-Work Based on Analog Hamiltonian [293]	Appendix D.226	▲	○	○	●	○	○	○	●	Rand.
Proof-of-Work on the Inflation Propensity of Collatz Orbits [294]	Appendix D.227	▲	○	○	○	○	○	○	●	Rand.
Reputation Based Hybrid Consensus [250]	Appendix D.237	▲	●	○	●	○	○	○	○	Rand.
Robust Proof-of-Stake [295]	Appendix D.243	▲	○	○	○	○	○	○	○	Rand.
Roll-DPoS [251]	Appendix D.245	▲	●	○	●	○	○	○	●	Rand.
Rollerchain [252]	Appendix D.246	▲	●	○	●	○	○	○	●	Rand.
Satellite-Aided Consensus [141]	Appendix D.249	▲	○	○	○	○	○	○	●	
Service-Zone-Based Hierarchical Consensus [296]	Appendix D.260	▲	○	○	●	○	○	○	●	Rand.
SklCoin [297]	Appendix D.262	▲	○	○	●	○	○	○	●	Rand.
Solida [255]	Appendix D.264	▲	●	○	○	○	○	○	●	Rand.
Thinkey [256]	Appendix D.269	▲	●	○	●	○	○	○	●	Rand.
Time-Memory-Data Trade-Off [257]	Appendix D.270	▲	●	○	●	○	○	○	●	Rand.
Proof-of-Trusted-Execution-Environment-Stake [157]	Appendix D.218	▲	○	○	●	●	○	○	●	Elec.
BFT with Satellite Chains [298]	Appendix D.1	▽	○	○	○	○	○	●	○	
PBFT with Node Quality Control [299]	Appendix D.5	▽	○	○	○	○	●	●	○	Elec.
PoW with Integer Prime Factorisation [189]	Appendix D.18	▽	●	○	●	○	○	○	●	Rand.
Adaptive Wide-Area Replication [300]	Appendix D.22	▽	○	○	●	○	○	●	○	Elec.
AdRaft [301]	Appendix D.23	▽	○	○	●	○	○	●	○	Elec.
Alzahrani and Bulusu's Decentralized Consensus Protocol Utilizing Game Theory and Randomness [302]	Appendix D.26	▽	○	○	●	○	○	●	○	Elec.

Table 9. *Cont.*

	Ref	SA	Inc +	Inc −	Perm Ra	Perm Ph	Perm Re	Perm Pn	Perm Pl	Sel
Amoeba Paxos [303]	Appendix D.27	▽	○	○	○	○	○	●	○	Elec.
Assigned-Majority-Validation [304]	Appendix D.28	▽	○	○	○	○	○	●	○	
Auction-Based Consensus [305]	Appendix D.30	▽	○	○	○	○	○	●	○	Elec.
Authorized Proof of Stake [306]	Appendix D.31	▽	○	○	●	○	○	●	○	Rand.
BLIC [307]	Appendix D.35	▽	○	○	●	○	○	●	○	Rand.
Blockchain for the Common Good [196]	Appendix D.37	▽	●	○	○	○	○	●	○	Elec.
Blockchain-Based Federated Learning Framework with Committee Consensus [308]	Appendix D.39	▽	○	○	○	○	○	●	○	Elec.
Byzantine Set Union Consensus [309]	Appendix D.41	▽	○	○	●	○	○	●	○	Elec.
Casanova [310]	Appendix D.42	▽	○	○	○	○	○	○	○	None
Caucus [311]	Appendix D.43	▽	○	○	●	○	○	○	●	Rand.
CloudPoS (with CSP Invovlement) [268]	Appendix D.47	▽	○	○	○	○	○	●	○	Elec.
Coinami [312]	Appendix D.49	▽	○	○	●	○	○	●	○	Rand.
Committee-Based Byzantine Consensus [313]	Appendix D.50	▽	○	○	●	○	○	●	○	Elec.
Consensus Through Herding [314]	Appendix D.54	▽	○	○	○	○	○	●	○	
Credence-Based Consensus [315,316]	Appendix D.56	▽	○	○	●	○	●	●	○	Elec.
Cross-Application Permissioned Blockchain [317]	Appendix D.58	▽	○	○	○	○	○	●	○	
Dynamic PBFT [318]	Appendix D.61	▽	○	○	○	○	○	●	○	Rand.
DagGrid [319]	Appendix D.62	▽	○	○	●	○	●	●	○	Rand.
Delegate Consensus Algorithm [320]	Appendix D.64	▽	○	○	●	○	○	○	○	Rand.
Delegated Adaptive Byzantine Fault Tolerance [321]	Appendix D.65	▽	○	○	○	○	○	●	○	Elec.
Delegated Proof of Economic Value [321]	Appendix D.67	▽	○	○	○	○	●	●	○	
Dependability-Rank-based Consensus [322]	Appendix D.74	▽	○	○	●	○	●	●	○	Rand.
DEXON [323]	Appendix D.76	▽	○	○	●	○	○	●	○	Rand.
DFINITY [324]	Appendix D.77	▽	○	○	●	○	○	○	●	Rand.
Dynamic Hierarchical Byzantine Fault-Tolerant Consensus Based on Credit [325]	Appendix D.79	▽	○	○	○	○	●	●	○	
Egalitarian Practical Byzantine Fault Tolerance [326]	Appendix D.81	▽	○	○	○	○	○	●	○	
Electronic Identification, Authentication and Trust Services Validating Indy-Plenum [327]	Appendix D.82	▽	○	○	○	○	○	●	○	Comm.
Elpis [328]	Appendix D.83	▽	○	○	●	○	○	●	○	Elec.
Extensible-PBFT [329]	Appendix D.88	▽	○	○	●	○	○	●	○	Elec.
Fast leader-based, randomized Byzantine Agreement [330]	Appendix D.92	▽	○	○	●	○	○	●	○	Rand.
FastBFT [331]	Appendix D.94	▽	○	○	○	○	○	●	○	

Table 9. *Cont.*

	Ref	SA	Inc +	Inc −	Perm Ra	Perm Ph	Perm Re	Perm Pn	Perm Pl	Sel
Geo-Scale Byzantine Fault Tolerance [332]	Appendix D.96	▽	○	○	○	○	○	●	○	
Graph Learning BFT [333]	Appendix D.98	▽	○	○	○	○	○	●	○	
Group-Based Optimized Practical Byzantine Fault Tolerance [334]	Appendix D.102	▽	○	○	○	○	●	●	○	Elec.
HotStuff [335]	Appendix D.105	▽	○	○	○	○	○	●	○	
Hybrid Byzantine Agreement [336]	Appendix D.108	▽	○	○	●	○	○	●	○	Rand.
Identifiable Practical Byzantine Fault Tolerance [337]	Appendix D.110	▽	○	○	●	○	○	●	○	Elec.
Istanbul BFT Consensus [338]	Appendix D.114	▽	○	○	○	○	○	●	○	
Leader-Stable Fast Byzantine Fault Tolerance [339]	Appendix D.116	▽	○	○	○	○	○	○	○	
LFT2 [340]	Appendix D.117	▽	○	○	○	○	○	○	○	Elec.
Lisk-BFT [341]	Appendix D.118	▽	○	○	○	○	○	○	○	Elec.
Majority vOting Cellular Automata [342]	Appendix D.121	▽	○	○	○	○	○	●	○	
Mchain Consensus [343]	Appendix D.122	▽	○	○	●	○	○	●	○	Rand.
Mobile Crowdsourcing Chain [217]	Appendix D.123	▽	●	○	●	○	○	○	○	Elec.
Multi-Block BFT [344]	Appendix D.124	▽	○	○	○	○	○	●	○	
Multi-Round Concession Negotiation [172]	Appendix D.125	▽	●	●	○	○	●	○	○	Elec.
Multi-Supervised Permissioned Blockchain [345]	Appendix D.126	▽	○	○	○	○	○	●	○	Comm.
Multisignature-BFT [346]	Appendix D.129	▽	○	○	●	○	○	●	○	Elec.
Musch [347]	Appendix D.130	▽	○	○	○	○	○	●	○	
Open Business Environment BFT [348]	Appendix D.132	▽	○	○	○	○	●	○	○	
PeerBFT [349]	Appendix D.139	▽	○	○	○	○	○	●	○	
Personal Archive Service System [350]	Appendix D.143	▽	○	○	○	○	○	●	○	Comm.
POA-PBFT [351]	Appendix D.145	▽	○	○	○	○	○	●	○	Comm.
Practical Byzantine Fault Tolerance [144]	Appendix D.147	▽	○	○	○	○	○	●	○	
Practical Layered Consensus Mechanism [352]	Appendix D.148	▽	○	○	○	○	○	○	○	
Proof of Rest [353]	Appendix D.158	▽	○	○	●	○	○	●	○	Rand.
Proof of Training Quality [354]	Appendix D.161	▽	○	○	○	○	○	●	○	
Proof of Usage [227]	Appendix D.162	▽	●	○	●	○	○	●	○	Rand.
Proof-of-Accuracy [355]	Appendix D.166	▽	○	○	●	○	○	○	○	Rand.
Proof-of-Achievement [228]	Appendix D.167	▽	●	○	○	○	○	●	○	
Proof-of-Activity [356]	Appendix D.169	▽	○	○	●	○	○	●	○	Rand.
Proof-of-Atomicity [357,358]	Appendix D.170	▽	○	○	○	○	○	●	○	Comm.
Proof-of-Authority [359]	Appendix D.171	▽	○	○	○	○	○	●	○	
Proof-of-Business [232]	Appendix D.178	▽	●	○	●	○	●	●	○	Elec.
Proof-of-Communication [360]	Appendix D.179	▽	○	○	○	○	●	○	○	Elec.
Proof-of-Contribution [233]	Appendix D.181	▽	●	○	○	○	●	●	○	
Proof-of-Lucky-Id [361]	Appendix D.191	▽	○	○	●	○	○	●	●	Rand.
Proof-of-Majority [362]	Appendix D.192	▽	○	○	●	○	○	●	○	Rand.
Proof-of-Participation-and-Fees [363]	Appendix D.196	▽	○	○	○	○	●	○	●	Elec.

Table 9. *Cont.*

	Ref	SA	Inc +	Inc −	Ra	Ph	Re	Perm Pn	Perm Pl	Sel
Proof-of-Points [242]	Appendix D.198	▽	●	○	●	○	○	○	●	Elec.
Proof-of-Reputation [364]	Appendix D.204	▽	○	○	○	○	●	●	○	Elec.
Proof-of-Review [243]	Appendix D.206	▽	●	○	○	○	○	○	○	
Proof-of-Sovereignty [365]	Appendix D.208	▽	○	○	○	○	○	●	○	
Proof-of-Stack [366]	Appendix D.211	▽	○	○	●	○	●	●	○	Rand.
Proof-of-Trust [367]	Appendix D.216	▽	○	○	●	○	●	●	●	Comm.
Proof-of-Validation [247]	Appendix D.220	▽	●	○	●	○	○	○	●	Rand.
Proof-of-Verifying [175]	Appendix D.221	▽	●	●	●	○	○	●	○	Rand.
Proof-of-Vote [368,369]	Appendix D.222	▽	○	○	●	○	○	●	○	Comm.
Proof-of-Win [370]	Appendix D.223	▽	○	○	●	○	○	●	○	Rand.
Proteus [371,372]	Appendix D.229	▽	○	○	○	○	○	●	○	
Raft [151]	Appendix D.230	▽	○	○	○	○	○	●	○	Elec.
Randition [373]	Appendix D.231	▽	○	○	●	○	○	●	○	Rand.
Random Leader Selection based on Credit Value [374]	Appendix D.232	▽	○	○	●	○	●	●	○	Elec.
Randomization to PoW [248]	Appendix D.233	▽	●	○	●	○	○	○	●	Rand.
Regulated Bitcoin [249]	Appendix D.235	▽	●	○	●	○	○	●	○	Rand.
Reputaion-Based BFT [375]	Appendix D.236	▽	○	○	●	○	●	●	○	Elec.
Reputation-based Byzantine Fault Tolerance [376]	Appendix D.239	▽	○	○	●	○	●	○	○	Rand.
Rift [377]	Appendix D.241	▽	○	○	○	○	○	○	○	Elec.
Robust Byzantine Agreement [336]	Appendix D.242	▽	○	○	●	○	○	●	○	Rand.
Rock-Scissors-Paper [176]	Appendix D.244	▽	●	●	○	○	○	●	○	
Rotating Multiple Random Sampling [378]	Appendix D.247	▽	○	○	●	○	○	●	○	Rand.
Saguaro [379]	Appendix D.248	▽	○	○	○	○	○	●	○	
Scalable Byzantine Fault Tolerance [380]	Appendix D.250	▽	○	○	●	○	○	●	○	Rand.
Scalable Hierarchical Byzantine Fault Tolerance [381]	Appendix D.251	▽	○	○	○	○	○	●	○	Elec.
Scalable Network-Coded PBFT [382]	Appendix D.252	▽	○	○	○	○	○	●	○	Elec.
Scalable Practical Byzantine Fault Tolerance with Short-Lived Signature Schemes [383]	Appendix D.253	▽	○	○	●	○	○	●	○	Comm.
Score Voting-based BFT Consensus [384]	Appendix D.254	▽	○	○	○	○	●	●	○	Elec.
Security-Aware Genetic Algorithm based Practical Byzantine fault Tolerance [385]	Appendix D.256	▽	○	○	○	○	○	●	○	
Self-Stabilizing Byzantine Consensus [386]	Appendix D.257	▽	○	○	●	○	○	●	○	Rand.
separate-proof-of-deep-learning [387]	Appendix D.259	▽	○	○	○	○	○	○	○	
Sharding Permissioned Blockchains Over Network Clusters [388]	Appendix D.261	▽	○	○	○	○	○	●	○	
Streamlet [389]	Appendix D.266	▽	○	○	○	○	○	●	○	Elec.
Torneo [259]	Appendix D.272	▽	●	○	●	○	○	●	○	Rand.
Two-Tier Voting System Architecture [390]	Appendix D.275	▽	○	○	○	○	○	●	●	
uMine [391]	Appendix D.276	▽	○	○	○	○	○	●	○	
Unitary Interchain Network [392]	Appendix D.277	▽	○	○	○	○	○	○	○	

Table 9. *Cont.*

	Ref	SA	Inc +	Inc −	Inc Ra	Inc Ph	Inc Re	Perm Pn	Perm Pl	Sel
Weak Centralized Consensus Mechanism with Incentive Effects [178]	Appendix D.278	▽	●	●	●	○	○	○	○	Rand.
Weight of Authentication Byzantine Fault Tolerance [393]	Appendix D.279	▽	○	○	○	○	○	○	●	
What, Where, How much [260]	Appendix D.280	▽	●	○	○	○	○	●	○	
Efficient, General, and Scalable Consensus [154]	Appendix D.80	▽	○	○	●	●	○	●	○	Rand.
PoS with Robust Round Robin (PoW Bootstrap) [153]	Appendix D.10	▶	●	○	○	○	○	○	●	Comm.
PoUW as a Problem-Solving Market [186]	Appendix D.14	▶	●	○	●	○	○	○	●	Rand.
Blockchain Reputation-Based Consensus [197]	Appendix D.38	▶	●	○	●	○	●	○	●	Elec.
Circle of Trust [200]	Appendix D.45	▶	●	○	●	○	●	●	●	Elec.
Consensus of Trust [394]	Appendix D.53	▶	○	○	●	○	●	○	○	Rand.
Consensus-based Oracle Protocol for the Secure Trade of Digital Goods [203]	Appendix D.55	▶	●	○	●	○	○	○	○	Rand.
Credit-Based Verifier Selection with Double Consensus [395]	Appendix D.57	▶	○	○	○	○	●	○	○	
Decision-Theoretic Online Learning Consensus [396]	Appendix D.63	▶	○	○	●	○	●	○	●	Rand.
Delegated Proof-of-Reputation [205]	Appendix D.69	▶	●	○	●	○	●	●	○	Elec.
Delegated Proof-of-Reputation [397]	Appendix D.70	▶	○	○	●	○	●	○	●	Elec.
Green-PoW [212]	Appendix D.101	▶	●	○	●	○	○	○	●	Rand.
Guru [398]	Appendix D.103	▶	○	○	●	○	●	○	●	Rand.
Identity-Augmented Proof-of-Stake [399]	Appendix D.111	▶	○	○	○	○	●	○	●	Rand.
Permissionless Proof-of-Reputation-X [400]	Appendix D.142	▶	○	○	●	○	●	○	●	Rand.
Proof-of-Balance [401]	Appendix D.172	▶	○	○	○	○	○	○	●	
Proof-of-Bid [231]	Appendix D.176	▶	●	○	●	○	●	○	●	Rand.
Proof-of-Human-Engagement [235]	Appendix D.185	▶	●	○	●	○	○	○	●	Rand.
Proof-of-Networking [239]	Appendix D.193	▶	●	○	●	○	○	○	○	
Proof-of-Notarized-Work [240]	Appendix D.194	▶	●	○	●	○	○	○	●	Rand.
Proof-of-Review [402]	Appendix D.207	▶	○	○	●	○	●	○	●	Elec.
Proof-of-Spending [244]	Appendix D.210	▶	●	○	●	○	○	○	●	Rand.
Proof-of-Stake with Time Staking [403]	Appendix D.214	▶	○	○	●	○	○	○	●	Rand.
Proof-of-Trust [404,405]	Appendix D.217	▶	○	○	●	○	●	○	●	Rand.
Proof-of-Unique-Human [406]	Appendix D.219	▶	○	○	○	○	●	○	●	
Reputation Consensus [407]	Appendix D.238	▶	○	○	●	○	●	○	●	Rand.
Reverse Hash Chain [408]	Appendix D.240	▶	○	○	●	○	○	○	○	Rand.
Semada Proof-of-Reputation [253]	Appendix D.258	▶	●	○	●	○	●	○	●	Rand.
Software Guard Extension-enabled decentralized intrusion detection framework [254]	Appendix D.263	▶	●	○	○	○	○	○	○	Rand.
Sybil Tolerant Equality Protocol [177]	Appendix D.267	▶	●	●	●	○	●	○	●	
token age based consensus [258]	Appendix D.271	▶	●	○	○	○	●	○	○	

Table 9. *Cont.*

	Ref	SA	Inc		Perm					Sel
			+	−	Ra	Ph	Re	Pn	Pl	
Trust Consensus Protocol [409]	Appendix D.273	▶	○	○	●	○	●	○	○	Elec.
Twice Verifications and Consensuses of Blockchain [410,411]	Appendix D.274	▶	○	○	○	○	●	●	●	Elec.
PoS with Robust Round Robin (Intel SGX Variant) [153]	Appendix D.11	▶	●	○	○	●	○	○	●	Comm.
Basalt [159]	Appendix D.33	▶	○	○	●	●	○	○	●	Rand.
DTNB [160]	Appendix D.78	▶	○	○	●	●	○	○	●	Rand.
LocalCoin [163]	Appendix D.119	▶	●	○	●	●	○	○	●	Rand.
Proof of Block Inclusion [155]	Appendix D.152	▶	●	○	○	●	○	○	●	Rand.
Proof of Elapsed Time [146]	Appendix D.154	▶	○	○	●	●	○	○	●	Rand.
Proof of Luck [152]	Appendix D.157	▶	○	○	●	●	○	○	○	Rand.
Proof of Social Contact [162]	Appendix D.160	▶	○	○	○	●	○	○	●	
Proof of witness presence [164]	Appendix D.163	▶	○	○	○	●	○	○	○	
Proof-of-Context [165]	Appendix D.180	▶	○	○	○	●	●	○	●	Rand.
Proof-of-Location [166]	Appendix D.189	▶	○	○	●	●	●	○	●	Rand.
Proof-of-Queue [156]	Appendix D.201	▶	○	○	●	●	○	●	○	Rand.
Rationality-proof consensus [158]	Appendix D.234	▶	●	●	○	●	○	○	●	
Staked IP-Address Selection [161]	Appendix D.265	▶	○	○	●	●	○	○	●	Rand.
Sybil-Proof Wireless Network Coordinate Based Byzantine Consensus [167]	Appendix D.268	▶	○	○	○	●	○	○	●	Elec.
DPoS with Quantum Entanglement [412]	Appendix D.3		○	○	○	○	○	○	○	
Delegated Byzantine Fault Tolerance [413]	Appendix D.66		○	○	○	○	○	○	○	Elec.
Delegation Based Scalable Byzantine False [*sic*] Tolerance Consensus [414]	Appendix D.73		○	○	○	○	○	○	●	
Fast Probabilistic Consensus with Weighted Votes [415]	Appendix D.93		○	○	●	○	○	●	●	Rand.
Green Mining [416,417]	Appendix D.100		○	○	●	○	○	○	●	Rand.
Permissioned Trusted Trading Network Consensus Algorithm [418]	Appendix D.141		○	○	●	○	○	●	○	Rand.
Proof of Kernel Work [419]	Appendix D.156		○	○	○	○	●	○	○	Rand.
Proof-by-Approval [420]	Appendix D.164		○	○	○	○	○	●	○	Comm.
Proof-of-Behaviour [229]	Appendix D.174		●	○	●	○	●	●	●	
Proof-of-Belief [230]	Appendix D.175		●	○	○	○	○	○	●	
Proof-of-Phone [421]	Appendix D.197		○	○	○	○	○	○	●	
Proof-of-Probability [422]	Appendix D.200		○	○	●	○	○	○	●	Rand.
Proof-of-Work-or-Knowledge [423]	Appendix D.228		○	○	●	○	○	○	●	Rand.
Secure and Scalable Hybrid Consensus [424]	Appendix D.255		○	○	○	○	○	○	●	

Ref: Section reference, **SA**: Sybil attack resistance class, **Inc +**: Reward scheme, **Inc −**: Punishment scheme, **Ra**: Randomisation, **Ph**: Physical world linking, **Re**: Reputation system, **Perm Pn**: Permissioned, **Perm Pl**: Permissionless, **Sel Rand.**: Random leader selection, **Sel Comm.**: Committee-based leader selection, **Sel Elec.**: Leader selection via election. ▲: Strong Sybil attack resistance, ▶: Limited Sybil attack resistance, ▽: No Sybil attack resistance. ●: Applicable, ○: Not applicable.

3.7. Mechanisms for Healthcare

Blockchain algorithms in healthcare are proposed to improve patient centricity of electronic healthcare systems [425,426], the effectiveness of legal medicine [425], the credi-

bility and interoperability between healthcare stakeholders [427], as well as medical supply chain management [428]. Legal barriers, unsurprisingly, constitute a major obstruction to blockchain adoption in the healthcare domain [429], as record sharing (predominantly of electronic health records and personal health records [430]) is a highly regulated activity [431] with disjoint approaches throughout the healthcare field [432]. Consequently, as seen in Table 10, only a single mechanism targets permissionless systems [433] with others targeting permissioned or unspecified deployments [434–441].

Table 10. Consensus mechanisms in *healthcare*.

			Inc					Perm		
	Ref	**SA**	**+**	**—**	**Ra**	**Ph**	**Re**	**Pn**	**Pl**	**Sel**
PoW Applied to Biomedical Image Segmentation [434]	Appendix E.1	▽	○	○	●	○	○	●	○	Rand.
Deep Learning Based Consensus [435]	Appendix E.2	▽	○	○	●	○	○	○	○	Rand.
Lightweight Proof-of-Game [433]	Appendix E.3	▽	○	○	●	○	○	●	●	Rand.
MedBlock [436]	Appendix E.4	▽	○	○	○	○	○	●	○	Comm.
Proof of Policy [438]	Appendix E.6	▽	○	○	○	○	○	●	○	
Proof of Policy [439]	Appendix E.7	▽	○	○	○	○	○	●	○	Comm.
Proof-of-Familiarity [440]	Appendix E.8	▽	○	○	○	○	●	●	○	
proof-of-medical-stake [441]	Appendix E.9	▽	○	○	○	○	●	●	○	
Proof of Artificial Intelligence [437]	Appendix E.5	▶	○	○	●	○	●	○	○	Rand.

Ref: Section reference, **SA**: Sybil attack resistance class, **Inc +**: Reward scheme, **Inc —**: Punishment scheme, **Ra**: Randomisation, **Ph**: Physical world linking, **Re**: Reputation system, **Perm Pn**: Permissioned, **Perm Pl**: Permissionless, **Sel Rand.**: Random leader selection, **Sel Comm.**: Committee-based leader selection, **Sel Elec.**: Leader selection via election. ▶: Limited Sybil attack resistance, ▽: No Sybil attack resistance. ●: Applicable, ○: Not applicable.

3.8. Mechanisms for High Performance

As Oyinloye et al. [442] summarise, 'throughput, scalability, security, energy consumption, and finality' can be considered the main attributes of the overall performance of a blockchain system. This is despite an ongoing debate on the appropriateness of applying traditional performance metrics for standard systems to decentralised systems [443]. And indeed, most papers analysed have the goal of putting forward designs that improve on traditional metrics such as throughput and latency. Of the papers in this category (see Table 11), the vast majority provide no Sybil attack resistance by building on BFT principles. For these papers, similar to early work [14,15], commonly a maximum threshold of byzantine processes (e.g., $1/3$) is assumed. Most papers perform benchmarking against similar mechanisms that do not provide Sybil attack resistance.

Table 11. Consensus mechanisms designed for high performance.

	Ref	SA	Inc					Perm		Sel
			+	−	Ra	Ph	Re	Pn	Pl	
PoS using Fair and Dynamic Sharding Management [444]	Appendix F.4	▲	●	○	●	○	○	○	●	Rand.
Bicomp [445]	Appendix F.7	▲	●	○	●	○	○	○	●	Rand.
Hybrid PoW/PoS [446]	Appendix F.24	▲	●	○	●	○	○	○	●	Rand.
Scalable BFT consensus mechanism through aggregated signature gossip [447]	Appendix F.35	▲	○	○	●	○	○	●	●	
BFT Consensus on FPGA [448]	Appendix F.1	▽	○	○	●	○	○	●	○	Elec.
BFT Consensus with SmartNIC Offloading [448]	Appendix F.2	▽	○	○	●	○	○	●	○	Elec.
PBFT with SVM-Based Trust Evaluation [449]	Appendix F.3	▽	○	○	○	○	●	●	○	Elec.
Autonomous and Controllable High-performance Consensus [450]	Appendix F.5	▽	○	○	○	○	○	○	○	
BEAT [451]	Appendix F.6	▽	○	○	●	○	○	●	○	Elec.
BlockDAG [452]	Appendix F.9	▽	○	○	○	○	○	●	○	Elec.
Checkpoint Consensus [453]	Appendix F.10	▽	○	○	●	○	○	●	○	Rand.
Concordia [454]	Appendix F.11	▽	○	○	●	○	○	●	○	Rand.
Consensus based on the Mortgage Model [455]	Appendix F.12	▽	○	○	●	○	○	●	○	Elec.
Consensus for Mobile Devices using Online Brokers [456]	Appendix F.13	▽	○	○	○	○	○	●	○	
FAST [457]	Appendix F.14	▽	○	○	○	○	○	●	○	None
Fast Probabilistic Consensus within Byzantine Infrastructures [458]	Appendix F.15	▽	○	○	●	○	○	●	○	None
Fast, Dynamic and Robust Byzantine Fault Tolerance [459]	Appendix F.16	▽	○	○	●	○	○	●	○	Rand.
FastPay [460]	Appendix F.17	▽	○	○	○	○	○	●	○	None
FireLedger [461]	Appendix F.18	▽	○	○	○	○	○	●	○	Elec.
FRChain Consensus [462]	Appendix F.19	▽	○	○	●	○	○	●	○	Elec.
Gosig [463]	Appendix F.20	▽	○	○	●	○	○	●	○	Rand.
High Performance and Scalable Byzantine Fault Tolerance [464]	Appendix F.21	▽	○	○	○	○	○	●	○	Rand.
HPBC [465]	Appendix F.23	▽	○	○	●	○	○	●	○	Elec.
Improved Practical Byzantine Consensus [466]	Appendix F.25	▽	○	○	○	○	○	●	○	Elec.
MinBFT-Based Consensus [467]	Appendix F.26	▽	○	○	○	○	○	●	○	
Mixed Byzantine Fault Tolerance [468,469]	Appendix F.27	▽	○	○	○	○	○	●	○	Elec.
Proof-of-Execution [470]	Appendix F.29	▽	○	○	○	○	○	●	○	Elec.
Proof-of-Scalable-Traceability [471]	Appendix F.30	▽	○	○	○	○	○	●	○	Comm.
Proof-of-Vote [369]	Appendix F.31	▽	○	○	○	○	○	●	○	Elec.
Raft with Network Stability Evaluation [472]	Appendix F.32	▽	○	○	○	○	○	●	○	Elec.
Random-Checkers Proof-of-Stake [473]	Appendix F.33	▽	●	●	○	○	○	○	●	Elec.
SACZyzzyva [474]	Appendix F.34	▽	○	○	●	○	○	●	○	Rand.
Scalable Dynamic Multi-Agent Byzantine Fault-Tolerance [475]	Appendix F.36	▽	○	○	○	○	○	●	○	Elec.
Scalable Efficient Byzantine Fault Tolerance [476]	Appendix F.37	▽	○	○	○	○	○	●	○	Elec.

Table 11. *Cont.*

	Ref	SA	Inc +	Inc −	Ra	Ph	Re	Perm Pn	Perm Pl	Sel
Scored PBFT [477]	Appendix F.38	▽	○	○	●	○	●	●	○	Elec.
Stream of Distributed Secrets for Quantum-safe Blockchain [478]	Appendix F.40	▽	○	○	●	○	○	○	○	Rand.
T-PBFT [479]	Appendix F.41	▽	○	○	○	○	●	●	○	Elec.
Blinkchain [480]	Appendix F.8	▶	○	○	●	○	○	○	●	Rand.
High-Performance Blockchain Enhanced Consensus [481]	Appendix F.22	▶	○	○	●	○	○	○	●	Rand.
Multi Party Computation DPoS [482,483]	Appendix F.28	▶	●	○	●	○	○	○	○	Rand.
Self-Referencing Directed Acyclic Graph and Voting-Based PBFT Consensus [484]	Appendix F.39		○	○	●	○	●	○	●	Elec.

Ref: Section reference, **SA**: Sybil attack resistance class, **Inc +**: Reward scheme, **Inc −**: Punishment scheme, **Ra**: Randomisation, **Ph**: Physical world linking, **Re**: Reputation system, **Perm Pn**: Permissioned, **Perm Pl**: Permissionless, **Sel Rand.**: Random leader selection, **Sel Comm.**: Committee-based leader selection, **Sel Elec.**: Leader selection via election. ▲: Strong Sybil attack resistance, ▶: Limited Sybil attack resistance, ▽: No Sybil attack resistance. ●: Applicable, ○: Not applicable.

3.9. Mechanisms for IoT

A large number of papers apply blockchain to IoT (see Table 12), often with the goal of improving the security of IoT stacks [485] or to enable immutable traceability [486]. In common IoT deployments, there is a large disparity of computational capabilities between IoT devices and edge devices [487]. This disparity is also one of the drivers of hierarchicality in these use cases [20]. This favours algorithms with limited or no Sybil attack resistance that offload computation to edge nodes: often these edge nodes are operated centrally, by trustworthy entities.

Table 12. Consensus mechanisms for the 'Internet of Things'.

	Ref	SA	Inc +	Inc −	Ra	Ph	Re	Perm Pn	Perm Pl	Sel
PoW with Mining Tokens [488]	Appendix G.5	▲	●	○	●	○	○	○	○	Rand.
Collaborative Proof-of-Work [489]	Appendix G.8	▲	●	●	●	○	○	○	●	Rand.
Credit-Based Consensus Mechanism [490,491]	Appendix G.13	▲	○	○	●	○	●	○	●	Rand.
Hybrid PoW/PoS [492]	Appendix G.22	▲	●	○	●	○	○	○	●	Rand.
Proof-of-Trading [493]	Appendix G.47	▲	●	○	○	○	○	○	○	Rand.
Random Proof of Work [494]	Appendix G.50	▲	●	○	●	○	○	●	●	Rand.
Three-Dimensional Greedy Heaviest-Observed Sub-Tree Consensus [495]	Appendix G.56	▲	●	○	●	○	○	○	●	Rand.
BFT Consensus Based on Dynamic Permission Adjustment [496]	Appendix G.1	▽	○	○	○	○	●	●	○	Elec.
IoT Adaptive Dynamic Consensus [497]	Appendix G.3	▽	○	○	○	○	○	●	○	
Adaptive Proof-of-Work [498]	Appendix G.6	▽	○	○	●	○	○	●	○	Rand.
Collaborative Trust Based Delegated Proof-of-Stake [499]	Appendix G.9	▽	○	○	●	○	○	●	○	Rand.
Consensus with Elected Leader [500]	Appendix G.10	▽	○	○	●	○	○	●	○	Elec.
Context-based consensus [501]	Appendix G.11	▽	○	○	○	○	○	○	○	Elec.
Double-Layer PBFT [502]	Appendix G.16	▽	○	○	○	○	○	●	○	Elec.
Dynamic Blind Voting [503]	Appendix G.17	▽	○	○	●	○	○	○	○	Rand.

Table 12. *Cont.*

	Ref	SA	Inc +	Inc −	Perm Ra	Perm Ph	Perm Re	Perm Pn	Perm Pl	Sel
Improved PBFT [504]	Appendix G.24	▽	○	○	○	○	○	●	○	Comm.
Lightweight Blockchain based Cybersecurity [505]	Appendix G.25	▽	○	○	○	○	○	●	○	Comm.
Lightweight Consensus for IoT [506]	Appendix G.26	▽	○	○	○	○	○	●	○	
Luckyminer [507]	Appendix G.27	▽	●	○	●	○	○	○	●	Rand.
Multi-Chain Proof of Rapid Authentication [508]	Appendix G.28	▽	○	○	○	○	○	●	○	Comm.
Optimized PBFT Consensus with Speaker [509]	Appendix G.29	▽	○	○	●	○	○	●	○	Rand.
Proof-of-Presence [510]	Appendix G.33	▽	○	○	○	○	○	●	○	Rand.
Proof of Random Count in Hashes [511]	Appendix G.35	▽	○	○	●	○	○	●	○	Rand.
Proof of Reputation [512]	Appendix G.36	▽	○	○	○	○	○	●	○	
Proof-of-Balance [513]	Appendix G.38	▽	○	○	○	○	○	●	○	Elec.
Proof-of-Block-and-Trade [514]	Appendix G.39	▽	○	○	○	○	○	●	○	Rand.
Proof-of-Common-Interest [515,516]	Appendix G.40	▽	○	○	○	○	○	●	○	
Proof-of-Popularity [517]	Appendix G.44	▽	○	○	●	○	●	●	○	Rand.
Proof-of-Stability [518]	Appendix G.46	▽	○	○	○	○	○	●	○	Comm.
Proof-of-Validity [519]	Appendix G.48	▽	○	○	○	○	○	●	○	
ReBFT [520]	Appendix G.51	▽	○	○	○	○	○	●	○	
SCBFT [521]	Appendix G.53	▽	○	○	○	○	○	●	○	
Time-Dependent Consensus [522]	Appendix G.57	▽	○	○	●	○	○	○	○	Rand.
Tree-Chain [523]	Appendix G.58	▽	○	○	●	○	○	●	○	Rand.
Two-Layer-Consensus Architecture for IoT [524]	Appendix G.59	▽	○	○	●	○	○	●	○	Rand.
Weighted Majority Consensus Algorithm [525]	Appendix G.60	▽	○	○	●	○	●	●	○	Rand.
DPoS for Network Intrusion Detection [526]	Appendix G.2	▶	○	○	○	○	●	○	○	Elec.
PBFT Based on Reputation Value [527]	Appendix G.4	▶	○	○	○	○	●	●	○	Elec.
Consensus Algorithm for Mobile-Edge Computing [528]	Appendix G.7	▶	○	○	●	○	●	●	●	Elec.
Credit Reinforce Byzantine Fault Tolerance [529]	Appendix G.12	▶	○	○	●	○	○	○	●	Elec.
Distributed Time-Based Consensus [530]	Appendix G.15	▶	●	○	●	○	○	○	●	Rand.
Edge Computing Blockchain Security Consensus Model [531]	Appendix G.18	▶	○	○	●	○	●	○	○	
Geographic-PBFT [532]	Appendix G.19	▶	○	○	○	○	○	○	●	Elec.
Honesty-Based Distributed Proof-of-Work [533]	Appendix G.20	▶	○	○	●	○	●	●	●	Elec.
Honesty-Based Distributed Proof-of-Authority via Scalable Work [534]	Appendix G.21	▶	○	○	●	○	●	●	●	Elec.
PF-BVM [535]	Appendix G.30	▶	○	○	●	○	●	●	●	
Predictive Proof of Metrics [536]	Appendix G.31	▶	●	○	●	○	●	●	●	Elec.
Proof of Elapsed Work and Luck [537]	Appendix G.32	▶	○	○	●	○	○	○	●	Rand.
Proof-of-Honesty [538,539]	Appendix G.41	▶	○	○	○	○	●	○	○	Rand.
Proof-of-Negotiation/Proof-of-Trust Negotiation [540,541]	Appendix G.42	▶	●	○	●	○	●	○	○	Rand.
Register, Deposit, Vote [542]	Appendix G.52	▶	○	○	○	○	○	○	○	None

Table 12. *Cont.*

	Ref	SA	Inc +	Inc −	Ra	Ph	Re	Perm Pn	Perm Pl	Sel
Sybil Resistant IoT Trust Model [543]	Appendix G.54	▶	○	○	●	○	●	●	○	Rand.
Synergistic Multiple Proof [544]	Appendix G.55	▶	○	○	○	○	●	○	●	
Delegated Proof-of-Proximity [545]	Appendix G.14	▶	○	○	○	●	○	○	○	
Proof-of-Authentication [546–548]	Appendix G.37	▶	○	○	●	●	○	○	○	Elec.
Proof-of-Physical Unclonable Function [549]	Appendix G.43	▶	○	○	●	●	○	○	●	Rand.
Hybrid Consensus [550]	Appendix G.23		○	○	●	○	○	●	●	Rand.
Proof-of-Reputation-X [551]	Appendix G.45		○	○	○	○	●	○	○	
Proof-of-Work Using Maximization-Factorization Statistics [552]	Appendix G.49		○	○	●	○	○	○	○	Rand.
Proof of PUF-Enabled Authentication [553]	Appendix G.34		○	○	○	●	○	○	○	

Ref: Section reference, **SA**: Sybil attack resistance class, **Inc +**: Reward scheme, **Inc −**: Punishment scheme, **Ra**: Randomisation, **Ph**: Physical world linking, **Re**: Reputation system, **Perm Pn**: Permissioned, **Perm Pl**: Permissionless, **Sel Rand.**: Random leader selection, **Sel Comm.**: Committee-based leader selection, **Sel Elec.**: Leader selection via election. ▲: Strong Sybil attack resistance, ▶: Limited Sybil attack resistance, ▽: No Sybil attack resistance. ●: Applicable, ○: Not applicable.

3.10. Mechanisms for Media and Entertainment

Few mechanisms have been proposed for the media and entertainment domain (see Table 13). While Non-fungible tokens (NFTs) have gained considerable popularity in the arts [554,555] as well as media and entertainment [556,557] and have since generated sales of over 940 million USD [558], according to our analysis, no mechanisms specifically for this phenomenon have been developed. Instead, we see a mechanism tailored to gaming which requires centralised infrastructures for score assessment [559] and a mechanism to counteract false and misleading information presented as news [560]. No mechanisms with strong Sybil attack resistance were found in this category.

Table 13. Consensus mechanisms in *media*.

	Ref	SA	Inc +	Inc −	Ra	Ph	Re	Perm Pn	Perm Pl	Sel
Proof-of-Play [559]	Appendix H.3	▽	○	○	●	○	○	●	○	Rand.
Credibility Score [560]	Appendix H.1	▶	○	○	○	○	●	○	●	Elec.
Proof-of-Contribution [561]	Appendix H.2	▶	●	○	○	○	●	○	○	

Ref: Section reference, **SA**: Sybil attack resistance class, **Inc +**: Reward scheme, **Inc −**: Punishment scheme, **Ra**: Randomisation, **Ph**: Physical world linking, **Re**: Reputation system, **Perm Pn**: Permissioned, **Perm Pl**: Permissionless, **Sel Rand.**: Random leader selection, **Sel Comm.**: Committee-based leader selection, **Sel Elec.**: Leader selection via election. ▶: Limited Sybil attack resistance, ▽: No Sybil attack resistance. ●: Applicable, ○: Not applicable.

3.11. Mechanisms for Supply Chain

The supply chain can be characterised as a highly relevant domain for blockchain due to its promise of delivering information transparency and immutability [562] as well as its potential to bring about disintermediation [563]. Supply chain management and IoT (see Section 3.9) often go hand in hand to improve traceability and interoperability and make frequent use of sensor data originating from IoT devices [564]. Therefore, it is not surprising that, in terms of Sybil attack resistance, many properties are shared with the IoT domain: The mechanisms proposed (see Table 14) only deliver limited Sybil attack resistance [565–568] or no Sybil attack resistance [569–571]. This can be attributed to the trustworthy provenance problem: supply chain efforts require trustworthy intermediaries

to prevent physical tampering (e.g., the manipulation of sensors or interference with physical products). Therefore, the mechanisms in this category commonly rely on permissioned systems which can cater to hierarchical architectures [20].

Table 14. Consensus mechanisms in *supply chain*.

			Inc					Perm		
	Ref	**SA**	**+**	**—**	**Ra**	**Ph**	**Re**	**Pn**	**Pl**	**Sel**
Consensus Mechanism for Marine Data Management System [569]	Appendix I.2	▽	○	○	○	○	○	●	○	Elec.
Improved Practical Byzantine Fault Tolerance [570,571]	Appendix I.4	▽	○	○	○	○	○	●	○	Comm.
Multi-Center Practical Byzantine Fault Tolerance [567]	Appendix I.5	▽	○	○	○	○	○	●	○	
Proof of Accomplishment [568]	Appendix I.6	▽	○	○	○	○	●	●	○	
C-dBFT [565]	Appendix I.1	▶	○	○	○	○	○	●	○	
Group-Based PoW [566]	Appendix I.3	▶	●	○	●	○	○	○	○	Rand.
Proof-of-Location [572]	Appendix I.7		○	○	●	○	○	○	●	None

Ref: Section reference, **SA**: Sybil attack resistance class, **Inc +**: Reward scheme, **Inc —**: Punishment scheme, **Ra**: Randomisation, **Ph**: Physical world linking, **Re**: Reputation system, **Perm Pn**: Permissioned, **Perm Pl**: Permissionless, **Sel Rand.**: Random leader selection, **Sel Comm.**: Committee-based leader selection, **Sel Elec.**: Leader selection via election. ▶: Limited Sybil attack resistance, ▽: No Sybil attack resistance. ●: Applicable, ○: Not applicable.

3.12. Mechanisms for Telecom

The application of blockchain in telecom is nascent with only two dedicated mechanisms found (see Table 15). Darmwal [573] explains this by showing that the telecom domain is bound by numerous historic standards of interoperability and predicts that, therefore, adoption will be slow and should focus on lighthouse projects led by established consortia. This prediction is reflected in the fact that mechanisms in this vertical expose only limited Sybil attack resistance [574] or no Sybil attack resistance [575] at all, hinting at the application of the proposed mechanisms in permissioned contexts.

Table 15. Consensus mechanisms in *telecom*.

			Inc					Perm		
	Ref	**SA**	**+**	**—**	**Ra**	**Ph**	**Re**	**Pn**	**Pl**	**Sel**
Proof-of-Majority [575]	Appendix J.2	▽	○	○	○	○	○	●	○	
Delegated Proof-of-Trust [574]	Appendix J.1	▶	○	○	●	○	○	○	○	

Ref: Section reference, **SA**: Sybil attack resistance class, **Inc +**: Reward scheme, **Inc —**: Punishment scheme, **Ra**: Randomisation, **Ph**: Physical world linking, **Re**: Reputation system, **Perm Pn**: Permissioned, **Perm Pl**: Permissionless, **Sel Rand.**: Random leader selection, **Sel Comm.**: Committee-based leader selection, **Sel Elec.**: Leader selection via election. ▶: Limited Sybil attack resistance, ▽: No Sybil attack resistance. ●: Applicable, ○: Not applicable.

3.13. Mechanisms for Useful Work

Useful work schemes are ubiquitous, created with the goal of deriving useful outputs from PoW. As most mechanisms implement mechanics similar to conventional PoW, their Sybil attack resistance properties are strong (see Table 16). It can be differentiated between fixed PoUW schemes, in which a well-defined computational problem exists, and marketplace-based mechanisms, in which problems can be proposed dynamically. The former are often well-specified and provide appropriate difficulty adjustment mechanisms while the latter sometimes lack such considerations and, therefore, have unclear security properties. Marketplace mechanisms can often only provide limited Sybil attack resistance due to the risk of collusion between sellers and buyers and the challenge of objectively establishing the best solution. This is particularly apparent in artificial intelligence (AI)-

based marketplace mechanisms that require the objective evaluation of a potentially large number of proposed machine learning (ML) models.

Table 16. Consensus mechanisms using 'Proofs-of-useful-work'.

			Inc					Perm		
	Ref	**SA**	**+**	**−**	**Ra**	**Ph**	**Re**	**Pn**	**Pl**	**Sel**
PoUW for ML Training [576]	Appendix K.1	▲	○	○	●	○	○	○	●	Rand.
PoW Applied to High-Dimension, Non-Linear Optimisation Problems [577]	Appendix K.2	▲	●	○	●	○	○	○	●	Rand.
PoW Based On NCP-Solving [578]	Appendix K.3	▲	○	○	●	○	○	○	●	Rand.
PoW Based on Random Multivariate Quadratic Equations [579]	Appendix K.4	▲	○	○	●	○	○	○	●	Rand.
PoW on Elements in a Cyclic Group [580]	Appendix K.5	▲	○	○	○	○	○	○	●	Rand.
Calibration of Public Key Cryptographic Systems via Proof-of-Work [581]	Appendix K.7	▲	●	○	●	○	○	○	●	Rand.
Coin.AI [582]	Appendix K.8	▲	●	○	●	○	○	○	●	Rand.
Conquering Generals [583]	Appendix K.9	▲	●	○	●	○	○	○	●	Rand.
Difficulty-based Incentives for Problem Solving [584]	Appendix K.10	▲	●	○	●	○	○	○	●	Rand.
Hybrid Mining [585]	Appendix K.11	▲	●	○	●	○	○	○	●	Rand.
Image-based Proof-of-Work [586]	Appendix K.12	▲	●	○	●	○	○	○	●	Rand.
Proof of Catalytic Space [587]	Appendix K.13	▲	○	○	●	○	○	○	●	
Proof of Deep Learning with Hyperparameter Optimization [588]	Appendix K.14	▲	○	○	●	○	○	○	●	Rand.
Proof of Evolution [589]	Appendix K.15	▲	●	○	○	○	○	○	●	Rand.
Proof-of-Deep-Learning [590,591]	Appendix K.18	▲	●	○	●	○	○	○	●	Rand.
Proof-of-Exercise [592]	Appendix K.19	▲	●	○	●	○	○	○	●	Rand.
Proof-of-Learning [593]	Appendix K.20	▲	●	○	●	○	○	○	●	Rand.
Proof-of-Learning [594]	Appendix K.21	▲	●	○	●	○	○	○	●	Rand.
Proof-of-WorkStore [595]	Appendix K.24	▲	○	○	●	○	○	○	●	Rand.
Reciprocally Useful Work [596]	Appendix K.25	▲	●	○	●	○	○	○	●	Rand.
Proof of Federated Learning [597]	Appendix K.16	▽	○	○	○	○	○	○	○	
Proof-of-Accuracy [598]	Appendix K.17	▽	○	○	○	○	○	●	○	
Proof-of-Learning [599]	Appendix K.22	▽	●	○	●	○	○	○	○	Rand.
BlockML [600]	Appendix K.6	▶	●	○	●	○	○	○	●	Rand.
Proof-of-Search [601]	Appendix K.23	▶	●	○	●	○	○	○	○	Rand.
Susreum [602]	Appendix K.26	▶	○	○	○	○	○	○	●	Elec.
VBFL [603]	Appendix K.27	▶	●	○	●	○	●	○	○	Rand.

Ref: Section reference, **SA**: Sybil attack resistance class, **Inc +**: Reward scheme, **Inc −**: Punishment scheme, **Ra**: Randomisation, **Ph**: Physical world linking, **Re**: Reputation system, **Perm Pn**: Permissioned, **Perm Pl**: Permissionless, **Sel Rand.**: Random leader selection, **Sel Comm.**: Committee-based leader selection, **Sel Elec.**: Leader selection via election. ▲: Strong Sybil attack resistance, ▶: Limited Sybil attack resistance, ▽: No Sybil attack resistance. ●: Applicable, ○: Not applicable.

3.14. Mechanisms for Vehicles

A surprisingly rich domain is the domain of vehicles which shares many benefits and challenges with the domain of IoT. Blockchain applications in the vehicle domain predominantly target data exchange between vehicles, resource sharing (e.g., collaborative use of computing resources), parking coordination, and traffic management [604]. As shown in Table 17, schemes with strong Sybil attack resistance [605–609] are outnumbered by schemes with limited or no Sybil attack resistance. In line with Wang et al. [610],

who attest that blockchain in vehicular security is in its infancy, we find that some of the mechanisms proposed do not make use of the full potential of a decentralised paradigm by being overly hierarchical and by relying on central actors.

Table 17. Consensus mechanisms in *vehicles*.

			Inc					Perm		
	Ref	**SA**	**+**	**-**	**Ra**	**Ph**	**Re**	**Pn**	**Pl**	**Sel**
Consensus Mechanism for Blockchains on IoV [605]	Appendix L.1	▲	○	○	●	○	○	○	○	Elec.
dynamic Proof-of-Work [606–608]	Appendix L.3	▲	●	○	●	○	○	○	●	Rand.
Mixed Consensus Algorithm Based on PoW and PBFT [609]	Appendix L.6	▲	○	○	●	○	●	○	○	Rand.
Consensus Program for Charging Piles [611]	Appendix L.2	▽	●	○	●	○	●	●	○	Elec.
Enhanced DPoS [612]	Appendix L.4	▽	○	○	○	○	●	●	○	
Improved Byzantine Consensus for IoV [613]	Appendix L.5	▽	○	○	●	○	○	●	○	Rand.
Multipoint-Relay-Driven Consensus [614]	Appendix L.7	▽	○	○	●	○	○	●	○	Rand.
Practical Byzantine Fault Tolerance with Forwarding [615]	Appendix L.8	▽	○	○	○	○	○	●	○	None
Proof of Event and Location [616]	Appendix L.9	▽	○	○	○	○	○	●	○	
Proof-of-Communication [617]	Appendix L.10	▽	○	○	●	○	○	○	○	Elec.
Proof-of-Driving [618]	Appendix L.11	▽	○	○	●	○	●	○	○	Rand.
Proof-of-Event with Dynamic Federation [619,620]	Appendix L.12	▽	○	○	●	○	○	●	○	Rand.
Proof-of-Matching [621]	Appendix L.13	▽	●	○	○	○	○	●	○	Comm.
Proof-of-Nonce [622]	Appendix L.14	▽	○	○	●	○	○	●	○	Rand.
Proof-of-Reputation [623]	Appendix L.16	▽	○	○	○	○	●	●	○	None
Proof-of-Utility [624,625]	Appendix L.17	▽	○	○	●	○	○	●	○	Elec.
Proof-of-Vehicular-Services BFT [626]	Appendix L.18	▽	○	○	○	○	●	●	○	Elec.
Reputation-based Miner Node Selection [627]	Appendix L.21	▽	○	○	○	○	○	●	○	
Secured Event-Information Sharing [628]	Appendix L.22	▽	○	○	○	○	○	●		Comm.
Semi-Autonomous Distributed Blockchain-Based Framework for UAVs [629]	Appendix L.23	▽	○	○	○	○	○	●	○	Elec.
Time-Oriented Proof of Work [630]	Appendix L.24	▽	○	○	○	○	○	○	○	
Voting-based Consensus Protocol for VANET [631,632]	Appendix L.25	▽	○	○	●	○	●	●	○	Comm.
Proof-of-Work-at-Proximity [633]	Appendix L.19	▶	●	○	●	○	○	○	○	Rand.
Reputation-Based DPoS [634]	Appendix L.20	▶	○	○	○	○	●	○	○	
Proof-of-Quality-Factor [635]	Appendix L.15	▶	●	●	●	●	○	●	○	Elec.

Ref: Section reference, **SA**: Sybil attack resistance class, **Inc +**: Reward scheme, **Inc −**: Punishment scheme, **Ra**: Randomisation, **Ph**: Physical world linking, **Re**: Reputation system, **Perm Pn**: Permissioned, **Perm Pl**: Permissionless, **Sel Rand.**: Random leader selection, **Sel Comm.**: Committee-based leader selection, **Sel Elec.**: Leader selection via election. ▲: Strong Sybil attack resistance, ▶: Limited Sybil attack resistance, ▽: No Sybil attack resistance. ●: Applicable, ○: Not applicable.

4. Conclusions

The bulk of research interest in the field is focused on a small set of popular mechanisms (see Section 3.2) with Proof-of-Work (PoW), Proof-of-Stake (PoS), and Practical Byzantine Fault Tolerance as the most popular mechanisms. The literature review has shown that, beyond these, many more, seemingly disparate, consensus mechanisms exist

(see Section 3). However, upon closer examination, it can be concluded that there are strong similarities between those.

Amongst the systems with *strong Sybil attack resistance*, we find mostly PoW-like mechanisms that utilise some form of scarce resource constraint (CPU, memory, or otherwise) and PoS-like systems that rely on staking of resources (e.g., cryptocurrencies, stablecoins, reputation tokens, etc.). We also find combinations of the two, e.g., where a PoW bootstrapping phase is combined with a PoS execution phase. Sometimes these mechanisms are combined with reputation systems but the latter are rarely central to their Sybil attack resistance properties.

Systems with *limited Sybil attack resistance* are amongst the most interesting: these often make creative use of reputation systems (e.g., systems in which the right of a user to mine blocks correlates with their peer-to-peer rating). Physical world linking, i.e., the use of information emanating from objects in the physical world, is also most prevalent in this category: we find CPUs, trusted execution environments, and mobile phones to be common objects used. Furthermore, some mechanisms in this category use properties of well-recognised Internet standards such as the Domain Name System or public Internet Protocol (IP) addresses to determine uniqueness. This category, regrettably, is also one that contains mechanisms with overstated Sybil attack resistance properties and, often, poor specification.

Systems *without Sybil attack resistance* are mostly contained for completeness. Apart from rare instances where authors claim Sybil attack resistance, most works in this category target permissioned systems (that do not require mechanisms with Sybil attack resistance). Some authors explicitly exclude Sybil attack resistance considerations from their proposals and suggest applying alternative schemes to achieve it.

4.1. State of the Literature

Sybil attack resistance is a hard-to-achieve property that comes with significant trade-offs in terms of complexity, performance, and cost. Many mechanisms that aspire to provide strong Sybil attack resistance fall short of this goal. The choice of consensus mechanisms is overwhelming and system designers have often opted for designing new mechanisms without a strong need for it. In many ways, this is symptomatic for the wider subject area of distributed ledger technology where, despite some signs of the field maturing, *solutions looking for problems* are still prevalent.

In his 2017 manuscript, Cachin [636] delivered a 'Snake Oil Warning', alerting of the risks arising from consensus mechanism being developed without 'agreement on trust assumptions, security models, formal reasoning methods, and protocol goals' [636] (p. 2). In the context of this paper, we want to reiterate and enforce this warning: many protocols that suggest Sybil attack resistance do not deliver on this implication. Overall, significant quality issues in many of the protocols proposed are apparent. Many of the papers analysed lack formalisation, leaving essential aspects as an exercise to the reader, thereby exposing implementors and users to security risks. Some papers, while peer-reviewed and, in some cases, highly cited, misunderstand fundamental aspects of decentralised computing. This is particularly evident in reputation-based consensus methods that often address Sybil attack resistance through mitigation schemes that, under scrutiny, do not hold.

However, it is not all doom and gloom: recent years have seen some high-quality contributions that have further enhanced the performance of consensus mechanisms, significantly improved their Sybil attack resistance, or produced innovative approaches to saving energy. It is also to be welcomed that authors analyse the use of consensus mechanisms in industry-specific settings to drive appropriate solutions forward. It can therefore be speculated that the works that will stand the test of time will be those that apply rigorous modelling, formal security analysis, and comprehensive threat modelling.

4.2. Gaps

It is a challenging undertaking to compare the Sybil attack resistance properties of consensus mechanisms: there is no canonical approach to specifying consensus mechanisms for blockchain making it hard to formally scrutinise them. Furthermore, there is no common understanding of what constitutes *good* Sybil attack resistance, let alone recognised ways of asserting the Sybil attack resistance qualities of a proposed mechanism. Mechanism designers, in many cases, lack consideration for Sybil attacks in their work. Especially for domain-specific consensus mechanisms, it should be established what the permissioning-approach and, therefore, the threat model is.

4.3. Research Directions

Given the challenges discussed, four dominant directions for consensus mechanism research are conceivable. First, research should focus on introducing more rigorous approaches to the field by adapting existing formal methodologies to blockchain environments. Second, research should be undertaken to formally identify suitable canonical consensus mechanisms for common standard use cases. Third, research should enable incremental innovation of such canonical consensus mechanisms, thereby creating 'best-in-class' mechanisms for various use cases. Fourth, realistic benchmarks should be developed that allow for the objective comparison of non-functional aspects of blockchain systems (e.g., throughput performance or time-to-finality).

4.4. Future Work

Future work should focus on developing a formal framework to objectively quantify the Sybil attack resistance of consensus mechanisms. Formal methods should be applied that yield an objective categorisation of a protocol's Sybil attack resistance.

Author Contributions: Conceptualisation: M.P.; Data curation: M.P.; Investigation: M.P.; Methodology: M.P.; Supervision: P.M.; Writing—original draft: M.P.; Writing—review and editing: M.P. and P.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study does not require ethical clearance according to the rules set out by the research ethics committee of the institution the authors are affiliated with.

Informed Consent Statement: No informed consent was obtained as the study did not involve human participants.

Data Availability Statement: No new data were created or analysed in this study. Data sharing is not applicable to this article.

Acknowledgments: M.P. thanks Daniel Platt for useful discussions.

Conflicts of Interest: The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: M.P. reports a relationship with R3 Ltd. that includes: employment and equity or stocks. M.P. reports a relationship with Amazon Web Services EMEA SARL that includes: employment and equity or stocks.

Abbreviations

The following abbreviations are used in this manuscript:

3D-GHOST	Three-Dimensional Greedy Heaviest-Observed Sub-Tree Consensus
ABC	Auction-Based Consensus
ABM	aggregation block manager
ACM	Association for Computing Machinery
AI	artificial intelligence
APoW	Adaptive Proof-of-Work
ARPANET	Advanced Research Projects Agency Network

ASIC	Application-specific integrated circuit
AV	autonomous vehicle
AWARE	Adaptive Wide-Area Replication
BFT	Byzantine fault tolerance
BLS	Boneh–Lynn–Shacham
BRBC	Blockchain Reputation-Based Consensus
BSC	Byzantine Set Union Consensus
CA	Certificate authority
CAPER	Cross-Application Permissioned Blockchain
CAPEX	Capital expenditure
CFT	crash fault tolerance
Co-PoW	Collaborative Proof-of-Work
CoA	Chains of Activity
CoS	Class of Service
COST	Consensus-based Oracle Protocol for the Secure Trade of Digital Goods
CoT	Consensus of Trust
cPoC	Communicate Proof-of-Credit
CPU	central processing unit
CRBFT	Credit Reinforce Byzantine Fault Tolerance
CT	computerised tomography
CT-DPoS	Collaborative Trust Based Delegated Proof-of-Stake
DABFT	Delegated Adaptive Byzantine Fault Tolerance
DL	deep learning
DLT	distributed ledger technology
DNA	deoxyribonucleic acid
DNS	Domain Name System
DoS	Denial-of-service
DPBFT	Dynamic-Reputation Practical Byzantine Fault Tolerance
DPoEV	Delegated Proof of Economic Value
DPoP	Delegated Proof-of-Proximity
DPoR	Delegated Proof-of-Reputation
DPoS	Delegated Proof-of-Stake
DPoT	Delegated Proof-of-Trust
dPoW	dynamic Proof-of-Work
DPoW	Deterministic Proof-of-Work
DTC	Distributed Time-Based Consensus
ECBCM	Edge Computing Blockchain Security Consensus Model
ECDLP	elliptic curve discrete logarithm problem
EGES	Efficient, General, and Scalable Consensus
eIDAS	electronic IDentification, Authentication and trust Services
ePoW	Enhanced Proof-of-Work
EPoW	Estimable Proof-of-Work
ERC	Ethereum request for comment
FPGA	field-programmable gate array
FPoW	Filtered Proof-of-Work
GeoBFT	Geo-Scale Byzantine Fault Tolerance
GOLF	Greedy Observed Largest Forest
GPBFT	Group-Based Optimized Practical Byzantine Fault Tolerance
GPU	Graphics processing unit
HBA	Hybrid Byzantine Agreement
HDPoA	Honesty-Based Distributed Proof-of-Authority via Scalable Work
HDPoR	Hyper Delegation Proof-of-Randomness
HSBFT	High Performance and Scalable Byzantine Fault Tolerance

HyBE	High-Performance Blockchain Enhanced Consensus
IdAPoS	Identity-Augmented Proof-of-Stake
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IMP-PBFT	Improved Practical Byzantine Consensus
IoT	Internet of Things
IP	Internet Protocol
iPBFT	Improved Practical Byzantine Fault Tolerance
IPBFT	Identifiable Practical Byzantine Fault Tolerance
L1	Layer 1
L2	Layer 2
LC4IoT	Lightweight Consensus for IoT
LDPC	Low-density parity-check code
MAC	Media Access Control
MANET	mobile ad hoc network
MCPBFT	Multi-Center Practical Byzantine Fault Tolerance
McPoRA	Multi-Chain Proof of Rapid Authentication
MCS-Chain	Mobile Crowdsourcing Chain
ML	machine learning
MOCA	Majority vOting Cellular Automata
MPC-DPoS	Multi Party Computation Delegated Proof-of-Stake
MQ	multivariate quadratic
MRI	magnetic resonance imaging
MSig-BFT	Multisignature Byzantine Fault Tolerance
NFT	Non-fungible token
OPEX	Operating expenditure
oPoW	Optical Proof-of-Work
ORV	Open Representative Voting
P2P	peer-to-peer
PASS	Personal Archive Service System
PBFT	Practical Byzantine Fault Tolerance
PKI	public key infrastructure
PL-PoRX	Permissionless Proof-of-Reputation-X
PoA	Proof-of-Achievement
PoAh	Proof-of-Authentication
PoAW	Proof-of-Accumulated-Work
PoC	Proof-of-Cooperation
PoCI	Proof-of-Common-Interest
PoCS	Proof of Catalytic Space
PoD	Proof-of-Driving
PoDLwHO	Proof of Deep Learning with Hyperparameter Optimization
PoEf	Proof-of-Efficiency
PoEG	Proof-of-Energy-Generation
PoET	Proof of Elapsed Time
PoEWAL	Proof of Elapsed Work and Luck
PoFL	Proof of Federated Learning
PoKW	Proof of Kernel Work
PoM	Proof-of-Majority
PoN	Proof-of-Nonce
PoNW	Proof-of-Notarized-Work
PoPF	Proof-of-Participation-and-Fees
PoPUF	Proof-of-Physical Unclonable Function

PoQF	Proof-of-Quality-Factor
PoR	Proof-of-Reputation
PoRe	Proof of Reputation
PoRep	Proof-of-Replicated-Storage
PoRX	Proof-of-Reputation-X
PoS	Proof-of-Stake
PoST	Proof-of-Scalable-Traceability
PoSv	Proof-of-Sovereignty
PoTN	Proof-of-Negotiation/Proof-of-Trust Negotiation
PoUW	Proof-of-useful-work
PoW	Proof-of-Work
PoWaP	Proof-of-Work-at-Proximity
PoWorK	Proof-of-Work-or-Knowledge
PoX	Proof-of-Exercise
PPE	Private Proof-of-Effort
PPoM	Predictive Proof of Metrics
PRNG	Pseudorandom number generator
PUF	physical unclonable function
QoS	Quality of Service
RBA	Robust Byzantine Agreement
RBFT	Reputation-based Byzantine Fault Tolerance
RBitcoin	Regulated Bitcoin
RDV	Register, Deposit, Vote
ReCon	Reputation Consensus
RHC	Reverse Hash Chain
RPBFT	Practical Byzantine Fault Tolerance Based on Reputation Value
RSP	Rock-Scissors-Paper
RUW	Reciprocally Useful Work
SAGA-PBFT	Security-Aware Genetic Algorithm based Practical Byzantine fault Tolerance
SBFT	Scalable Byzantine Fault Tolerance
SDMA-PBFT	Scalable Dynamic Multi-Agent Byzantine Fault-Tolerance
SeBFT	Scalable Efficient Byzantine Fault Tolerance
SENATE	Sybil-Proof Wireless Network Coordinate Based Byzantine Consensus
SharPer	Sharding Permissioned Blockchains Over Network Clusters
SHBFT	Scalable Hierarchical Byzantine Fault Tolerance
SMP	Synergistic Multiple Proof
SodsBC	Stream of Distributed Secrets for Quantum-safe Blockchain
TCNS	Twice Verifications and Consensuses of Blockchain
TEE	Trusted Execution Environment
UAANET	unmanned aerial vehicle ad hoc network
VRF	Verifiable random function
WBFT	Weight of Authentication Byzantine Fault Tolerance
WMCA	Weighted Majority Consensus Algorithm

Appendix A. Description of Mechanisms for Democratic Processes

Appendix A.1. Consensus for e-Democracy [106]

With this consensus mechanism for e-democracy, the authors aim to design a system that is resistant to Sybil attacks, while allowing for a community to grow organically. New nodes are added to the network based on trust relationships with existing nodes, and removed if they are determined to be corrupt. Indeed, the protocol is resistant to Sybil attacks under the assumption of a limited number of attack edges, but might not provide Sybil attack resistance if this number is large.

Appendix A.2. Democratic Byzantine Fault Tolerance [107]

Democratic Byzantine Fault Tolerance proposes a deterministic BFT leader selection mechanism without a coordinator. The proposed architecture does not propose methods to achieve Sybil attack resistance and is, modifications excluded, only suitable for permissioned systems.

Appendix A.3. Encointer [104]

Similar to Proof-of-Personhood (see Appendix A.5), Encointer uses 'randomised pseudonym key signing parties' to link identities in the real world to digital ones. This approach delivers stronger Sybil attack resistance than Proof-of-Personhood as no organisers are required to facilitate key signing parties and the assignment to locations is non-deterministic. However, a cabal of attackers might still overwhelm a smaller system by controlling multiple identities through multiple instances of the Encointer mobile phone application.

Appendix A.4. Proof-of-Credibility [102]

Proof-of-Credibility, similar to PoS, aligns voting shares with the cryptocurrency stake held. Additionally, it introduces a mechanism to counteract a collapse in prices, that could allow attackers to obtain a disproportionally large number of voting shares. This mechanism yields a credibility score, indicating the degree of confidence in a miner being a non-Sybil entity.

Appendix A.5. Proof-of-Personhood [105]

Proof-of-Personhood is designed to provide Sybil attack resistance without the computational overhead of PoW or the economic effects of PoS. This is achieved via 'pseudonymous parties' in which on-ledger identities are linked to real-world identities. However, should organisers of such parties act maliciously, they might be able to create Sybil identities. Therefore, under strict assumptions, the protocol provides limited Sybil attack resistance.

Appendix B. Description of Mechanisms for Education

Appendix B.1. Group-Based Consensus for Educational Systems [110]

In this consensus mechanism for the educational domain, a reputation system is applied that incentivises adherence to the protocol and punishes deviations from it. The protocol uses a role-based approach in which ministries, schools, students, and enterprises each operate their own node set and proxy nodes. Within these node sets, DPoS is performed using the aforementioned reputation system rating as stake. As a permissioned protocol with fixed user groups, Sybil attack resistance is not a design goal.

Appendix B.2. Improved DPoS [112]

The paper proposes a rough sketch of a consensus mechanism for a blockchain-based distance education system. It argues that the system would be more secure and transparent than current systems. However, further research is needed to formalise details of the design as important aspects, such as whether a permissioned or permissionless approach will be used for the blockchain, have not been considered.

Appendix B.3. Proof of Reputation (PoRe) [111]

PoRe is a consensus algorithm for RPchain, an academic social networking service, that makes use of a reputation system. At its core, it constitutes a difficulty-adjusted PoW protocol in which participants earn reputation by publishing content transactions. In turn, participants receive a difficulty reduction for this positive contribution to the system. It can be assumed that this approach prevents basic Sybil attacks, while more complex ones in which a malicious user executes a complex program of attack, would not be preventable.

Appendix C. Description of Mechanisms for Energy

Appendix C.1. Communicate Proof-of-Credit (cPoC) [116]

cPoC constitutes a dampened PoW protocol in which the difficulty of the cryptographic puzzle depends not only on global parameters but also on parameters specific to the individual node generating the PoW. The core parameters to achieve this are 'credit score' and 'communication reliability'. Strong Sybil attack resistance can be assumed under the expectation that the damping parameters are selected conservatively.

Appendix C.2. Consensus Resource Slicing Model [119]

The proposed mechanism constitutes a 'licensing chain' which is a construct in which 'each node [. . .] must be approved to join'. Amongst the member nodes of the system, leader selection is then conducted randomly. Due to its permissioned approach, no Sybil attack resistance is provided by the consensus mechanism.

Appendix C.3. Credibility Consensus [130]

In this consensus mechanism for the energy vertical, a 'credibility score' is awarded to nodes that perform well during the 'arbitration' (i.e., transaction validation) phase of the protocol. In a permissionless setting, this scoring would be susceptible to Sybil attacks in which Sybil attackers arbitrate their own transactions.

Appendix C.4. Credit-Based PoW [120]

This PoW mechanism for energy trading is designed to improve transaction latency. The mechanism is intended for a permissioned system in which 'consensus nodes' (i.e., potential miners) need to be 'authorised' (i.e., admitted by a central entity). Therefore this mechanism is not created to provide Sybil attack resistance.

Appendix C.5. Credit-Based Concurrent Block Building Consensus [135]

The proposed consensus mechanism is designed to improve performance and promote energy trading efficiency. It is based on a reputation system using a 'credit value' metric which is applied to determine which nodes get to participate in the consensus process. The credit value is updated based on the node's performance in validating and publishing blocks. Nodes with superior credit values are selected to participate in consensus. The leader node is then chosen from the group of consensus nodes. The Sybil attack resistance properties of the algorithm are limited, as attackers may collude to create multiple high-credit value nodes.

Appendix C.6. Cross-Layer Trust-Based Consensus [131]

The consensus mechanism that is part of the system architecture proposed resembles PoS with 'trust coins' constituting stake. 'Trust coins' constitute a 'stable cryptocurrency', that, consequently, would have to be issued centrally. Depending on how trust coins are acquired, this most likely renders the system permissioned and, therefore, removes Sybil attack resistance from the scope.

Appendix C.7. Decentralized Consensus Decision-Making [117]

In this reputation-weighted PoW scheme, potential leaders are competing for the right to mine blocks by PoW. Additionally, an individual difficulty adjustment is applied, making the PoW puzzle easier for those who hold stake. The resulting system can be considered to provide similar Sybil attack resistance to previous PoS/PoW hybrid schemes.

Appendix C.8. Dynamic-Reputation Practical Byzantine Fault Tolerance (DPBFT) [121]

DPBFT introduces a central coordinator, the 'Monitoring node' to PBFT. This node serves as the central entry point to the system and calculates a 'reputation value' for all registered nodes on it: an expression of how performant the node was and how well it

adhered to the protocol. As a permissioned system, DPBFT does not provide Sybil attack resistance.

Appendix C.9. Enhanced Proof-of-Work (ePoW) [132]

ePoW constitutes a low-difficulty PoW mechanism. While information on the permissioning model of the intended system is absent, it can be speculated that the proposed mechanism would only be applied in permissioned networks. This is due to the lack of difficulty adjustments and the risk of forks arising from this.

Appendix C.10. Fast, Secure and Distributed Consensus Mechanism for Energy Trading among Vehicles Using Hashgraph [133]

In the proposed protocol, a directed acyclic graph-based data structure is proposed. Therefore, establishing finality is a challenge. The proposed system introduces the concept of 'famous' witnesses. These witnesses act as markers for the ordering of events. However, since there is no limitation on the influx of events to the system, Sybil attacks cannot be effectively prevented this way. While this might be appropriate for the use case, this mechanism cannot be applied to other domains that require strong Sybil attack resistance.

Appendix C.11. Hyper Delegation Proof-of-Randomness (HDPoR) [122]

HDPoR is a permissioned protocol in which a central entity, 'transaction management', performs the sortation of proposed transactions into shards to facilitate parallel processing. The mechanism sketched is intended for permissioned networks and does not provide Sybil attack resistance.

Appendix C.12. Improved Proof of Work [123]

In this consensus mechanism for the energy domain, one or multiple centralised entities, or consensus supervision nodes, as well as non-centralised entities (committer nodes) are used to validate transactions. These entities can be either energy producers or energy suppliers. Due to the centralised nature of the mechanism, no Sybil attack resistance is provided.

Appendix C.13. Lightweight DPoS for Energy Transmitters [124]

This simple DPoS protocol requires potential leaders to 'deposit [funds] to an account under public supervision' [124] (p. 169). Upon deposit of the funds, a stablecoin-like token would be issued to the depositor's on-ledger identity. This approach requires a trusted issuer and has, therefore, to be considered permissioned and not providing Sybil attack resistance.

Appendix C.14. Lightweight Credibility-Based Equity Proof Consensus [136]

The proposed mechanism employs a reputation system based on accounting accuracy, which selects accounting nodes. Accounting nodes are responsible for packaging transactions and adding them to the blockchain. In addition to accounting accuracy, a randomisation component based on hash values is proposed to prevent collusion among malicious accounting nodes. This approach, however, cannot effectively prevent Sybil attacks, should an attacker create large numbers of nodes.

Appendix C.15. Proof-of-Credit-Threshold [125]

The Proof-of-Credit-Threshold consensus mechanism is intended for the Energy domain to improve operational efficiency and to ensure security in a microgrid. The mechanism makes use of a reputation system based on credit, a measure of the ability of a participant to supply previously agreed-upon amounts of electricity. It can be assumed that the protocol is intended for a permissioned setting because of the need for a central entity or trusted metering hardware. Thus, Sybil attacks are not addressed by the mechanism.

Appendix C.16. Proof-of-Energy-Generation (PoEG) [126]

PoEG is a PoS-like algorithm that incentivises energy 'prosumers' (i.e., entities who both consume and produce electricity) to achieve a particular consumption profile (e.g., consume as much energy as they produce) based on a consumption-production function. Participants can claim stake depending on their use of the energy network as evidenced by transactions. This means that the correctness of the protocol is reliant on the correctness of production/consumption data. This, in turn, requires trusted third parties to assess the production/consumption or to provide trusted metering hardware. Therefore, the protocol is intended to be deployed into a permissioned setting and cannot be considered to provide Sybil attack resistance.

Appendix C.17. Proof-of-Benefit [137–140]

This consensus mechanism has been proposed to facilitate the trading of electricity between electric vehicles and the power grid. It has been designed to provide a high degree of scalability and performance, while also ensuring that the power grid system performs optimally. Leader selection in the system is based on a reputation system that takes into account the benefits brought to the network by a node, as calculated by a function that is designed to measure adherence to the stated goal of the system. The protocol is intended to be permissionless and claims resistance against Sybil attacks. However, no experimental data is given to support these claims and no details on the node admission procedure are provided. Therefore, the Sybil attack resistance properties are unclear.

Appendix C.18. Proof-of-Cooperation [134]

Proof-of-Cooperation (PoC) utilises a reputation system built on cooperation credit, a numerical representation of how well miners have adhered to the protocol historically. It is unclear whether the proposed system is intended for permissioned or permissionless systems, however, it can be assumed that no Sybil attack resistance would be achievable based on the PoC mechanism alone, as it could be attacked by an orchestrated Sybil attack from an attacker with perfect knowledge of the protocol.

Appendix C.19. Proof-of-Efficiency (PoEf) [127]

PoEf is a consensus mechanism that incentivises efficient energy production/consumption by implementing a reputation system that benefits participants with a favourable consumption profile. Information on leader selection is absent but it can be assumed that trusted hardware or central coordination is necessary to gather production/consumption data in a tamper-proof way.

Appendix C.20. Proof-of-Generation [128]

In Proof-of-Generation 'prosumers' qualify as potential miners: those with the highest 'feed-in generation' of electricity become leadership candidates. However, since the metadata necessary to make this selection (e.g., electricity meter data) need to be supplied by a centralised and trusted entity, the proposed mechanism cannot be considered to provide Sybil attack resistance.

Appendix C.21. Proof-of-Work Based on Reputation [129]

In this mechanism, a reputation system based on ratings by energy entities is devised. The relative rating determines the likelihood of a given committee member to participate in consensus. Committee members are, however, predetermined. Therefore this mechanism is suited for permissioned systems.

Appendix D. Description of General Purpose Mechanisms

Appendix D.1. BFT with Satellite Chains [298]

This consensus mechanism allows to connect multiple permissioned sub-systems with a larger permissioned super-system. Agreements of mutual trust between the systems involved are required, as assets can be exchanged between sub-systems. Due to the permissioning requirement, no Sybil attack resistance is provided.

Appendix D.2. Bitcoin-NG [179]

In this slight modification of Bitcoin's PoW protocol, the concept of 'microblocks' that do not require mining is introduced. This is done to minimise transaction confirmation delay. Since regular, Bitcoin-like PoW is still frequently undertaken, the Sybil attack resistance of Bitcoin-NG should be comparable.

Appendix D.3. DPoS with Quantum Entanglement [412]

While the authors describe the proposed scheme as being inspired by DPoS, information on the leader selection in the proposed scheme is absent. Therefore, the Sybil attack resistance properties remain unclear.

Appendix D.4. ECDLP-Based PoW [180]

The authors propose an alternative PoW scheme based on the solution of ECDLP problems over elliptic curves. The proposed protocol can be assumed to have strong Sybil resistance and to be secure against common attacks.

Appendix D.5. PBFT with Node Quality Control [299]

Bao [299] introduces a reputational rating scheme to PBFT that probes participant nodes frequently with simple challenges. Those that solve the challenges appropriately are ranked higher and therefore more likely to be selected as leaders. Since the challenges are administered centrally, the system is to be considered permissioned and, therefore, not resistant to Sybil attacks.

Appendix D.6. PoS Based on Credit Rewards and Punishments [262]

To avoid forks, especially under poor synchronisation conditions, Li et al. [262] propose a voting-based PoS algorithm to select a canonical leader. The proposal also suggests using a reputation system that rewards participants with 'credits' for participating in leader election and penalises them for diverging from the voting protocol. The Sybil attack resistance of the proposed protocol are comparable to other PoS mechanisms.

Appendix D.7. PoS Based on Verifiable Random Functions [181]

Algorand applies PoS for Sybil attack resistance. The stake aligns with the monetary value a user holds in the system, similar to other PoS protocols. The Sybil attack resistance characteristics are, therefore, comparable to those.

Appendix D.8. PoS for Bitcoin Sidechains [168]

In this consensus mechanism for sidechains, proof-of-stake is used to determine nodes to confirm updates to the sidechain. To incentivise nodes to vote for updates, a fee is levied that can only be redeemed once a transaction in persisted. The protocol targets sidechains to the Bitcoin blockchain, which in itself provides strong Sybil attack resistance. Using proof-of-stake, the sidechains inherit this resistance.

Appendix D.9. PoS with Behavior Score and Trust Rating [182]

Cheng et al. [182] propose an autonomous reputation system (i.e., one that does not need off-ledger input) as an addition to PoS. The modification achieves a modest

improvement in stake gains of small nodes. As the proposed behaviour score and trust rating only modify existing stake, it can be speculated that the strong Sybil attack resistance properties of PoS are maintained regardless of the modification.

Appendix D.10. PoS with Robust Round Robin (PoW Bootstrap) [153]

A variation on the aforementioned mechanism uses an initialisation step to the protocol that mines identities from a random distribution. The authors propose to utilise PoW for initial mining. Potential attacks arising from this, e.g., an attacker creating numerous Sybil identities initially only to launch an attack later, are, however, not discussed.

Appendix D.11. PoS with Robust Round Robin (Intel SGX Variant) [153]

To allow for deterministic leader selection while counteracting Sybil attacks, Ahmed-Rengers and Kostiainen [153] introduce a mechanism that establishes long-lived identities. They propose tying those identities to existing hardware infrastructure such as Intel SGX to limit the number of Sybil identities an attacker can create.

Appendix D.12. PoS with Waiting-Time First-Price Auctions [183]

In a bid to disincentivise 'coin hoarding', Deuber et al. [183] propose a novel minting mechanism for PoS. In this minting mechanism, contrary to that used in many other PoS implementations, users engage in waiting-time first-price auctions in which they bid cryptocurrency they already hold to obtain newly minted cryptocurrency at a specified time in the future. As such, it can be assumed that the Sybil attack resistance properties of the protocol are equivalent to those of earlier PoS mechanisms.

Appendix D.13. PoS with Weighted Voting [184,185]

This addition to conventional PoS introduces a reputation system based on the historical adherence of validators to the protocol. Those that have followed the protocol historically are more likely to be selected as leaders. The scheme can be considered to provide strong Sybil attack resistance assuming reasonable parameters of the reputation function.

Appendix D.14. PoUW as a Problem-Solving Market [186]

[186] design an open market for PoUWs on which consumers (problem uploaders) interact with producers (miners). It can be assumed that the Sybil attack resistance characteristics are comparable to earlier established PoW schemes.

Appendix D.15. PoW Based on Power Analysis of Low-End Microcontrollers [187]

Kim et al. [187] propose an ASIC-resistant PoW scheme based on a power analysis: this allows targeting the unique power consumption patterns on the microcontroller. In terms of Sybil attack resistance, the proposed scheme is equivalent to previous PoW schemes.

Appendix D.16. PoW on Quadratic Multivariate Equations [263,264]

In this novel PoW, similar to [579] (see Appendix K.4), miners solve quadratic multivariate equations in the finite field to achieve quantum attack resistance. As a conventional PoW mechanism, its Sybil attack resistance properties are strong.

Appendix D.17. PoW with Early Stage PoS [188]

Acknowledging that it is relatively easy to conduct a 51 % attack on new blockchain systems with limited capitalisation, Chen et al. [188] propose a combination of conventional PoW and PoS. In their proposal, PoS is used in the early phases of establishing a blockchain but subsequently converges to pure PoW. The Sybil attack resistance properties are equivalent to those of conventional PoW schemes or exceed those.

Appendix D.18. PoW with Integer Prime Factorisation [189]

Janjanam et al. [189] present a PoW system with low difficulty and without difficulty adjustment that may lead to frequent forks when deployed in practice. It provides no Sybil attack resistance.

Appendix D.19. PoW with Personalized Difficulty Adjustment [190]

Chou et al. [190] introduce a scheme to increase PoW difficulty for miners who have previously been successful in mining blocks with the goal of decreasing the probability of consecutive winning. This strategy cannot be successful in a permissionless setting since attackers may create Sybil identities to evade the penalty. Therefore, the scheme does not contribute to Sybil attack resistance, however, as a PoW protocol, ignoring the difficulty adjustment, it provides strong Sybil attack resistance.

Appendix D.20. PoW with Quantum-Resistant Hash Collision [191]

While the authors acknowledge that Bitcoin, as a PoW cryptocurrency, is relatively resistant to improved speeds of quantum computers in the foreseeable future, they analyse the application of 'Momentum' [637] in the context of PoW. They conclude that by applying this mechanism, in contrast to Bitcoin's current PoW, a quantum computer wouldn't be able to achieve a quadratic running time advantage.

Appendix D.21. VFRs for PoW [265]

Han et al. [265] use Verifiable random function (VRF) with the intention of ensuring that PoWs cannot be split between different machines (a technique known as 'pooled mining'). The mechanism provides the same, if not better, Sybil attack resistance when compared to conventional PoW schemes.

Appendix D.22. Adaptive Wide-Area Replication [300]

Adaptive Wide-Area Replication (AWARE) is a voting-weight tuning and leader positioning scheme that is designed to increase the speed of quorum formation in a peer-to-peer network. Through a self-assessment procedure, consensus latency is minimised. As a BFT mechanism it is intended for permissioned networks and is not resistant to Sybil attacks.

Appendix D.23. AdRaft [301]

In their 2021 paper, Fu et al. [301] propose an improvement to Raft to improve throughput and reduce latency. This is achieved by re-designing the Raft voting mechanism. Sybil attack resistance is not a concern of this contribution and no mechanisms to introduce Sybil attack resistance are described.

Appendix D.24. Albatross [169]

Albatross complements PBFT mechanics with PoS-based leader selection. This is being done with the goal of creating a novel blockchain consensus algorithm for permissionless networks that can provide high throughput. Its Sybil attack resistance properties are equivalent to those of other PoS protocols.

Appendix D.25. Alt-PoW [192]

This extension to Bitcoin PoW is designed with the goal of allowing for a faster, more energy-efficient termination by introducing the concept of progress in mining. Instead of subjecting miners to solving a contested problem with high difficulty, Alt-PoW gives miners a network view of their competitors. This allows reasonable miners to cease mining of a particular block if they deem their resources more effectively deployed on another chain. The Sybil attack resistance properties are to be considered similar to other PoW protocols.

Appendix D.26. Alzahrani and Bulusu's Decentralized Consensus Protocol Utilizing Game Theory and Randomness [302]

Alzahrani and Bulusu [302] propose a consensus mechanism that pseudorandomly selects a group of participant nodes as validators. While this avoids attacks that rely on bribing existing validators, it does not provide Sybil attack resistance since the creation of new potential validator nodes is not capped by a systemic ceiling.

Appendix D.27. Amoeba Paxos [303]

This extension of EPaxos is designed to perform well in geographically distributed private telecommunications networks. This is done by introducing workload awareness by computing suitable partitioning schemes for data. Sybil attack resistance is not a design goal of this protocol for permissioned environments.

Appendix D.28. Assigned-Majority-Validation [304]

Assigned-Majority-Validation appears to refer to a centrally managed, Proof-of-Achievement (PoA)-like, consensus mechanism in which only previously permissioned nodes can participate. Therefore, it does not provide Sybil attack resistance.

Appendix D.29. Attack-Tolerant PoW [193]

Kitakami and Matsuoka [193] propose an individual difficulty adjustment for PoW in which those participants that have mined blocks before are penalised by having the difficulty of the PoW to be provided increased. It can be assumed that this approach is ineffective in a permissionless scenario where attackers can create new identities without cost. Therefore, the Sybil attack resistance properties can be considered identical to PoW without difficulty adjustment.

Appendix D.30. Auction-Based Consensus [305]

In Auction-Based Consensus (ABC) miners enter into a continuous double auction for the right to include transactions in a block. The miner with the lowest bid earns the right to generate a block. This counterintuitive approach is applied to 'improve the fairness and justice' on the network. This approach, however, is not Sybil-resistant and therefore only suitable for permissioned networks.

Appendix D.31. Authorized Proof of Stake [306]

Van Toan et al. [306] propose a PoS mechanism for a permissioned system. In this scheme, only permissioned nodes engage in PoS which, in addition to the usual block generation privileges, also grants block redaction privileges. As a permissioned system, no Sybil attack resistance is provided.

Appendix D.32. B4SDC [194]

The authors of B4SDC aim to address forking, low efficiency, and centralisation of traditional PoS schemes with their proposal. Sybil attack resistance is not a concern of the protocol and it can be assumed that Sybil attack resistance characteristics are equal to those of earlier PoS protocols.

Appendix D.33. Basalt [159]

Auvolat et al. [159] create a PoS-like leader selection mechanism that removes the requirement for a native cryptocurrency as stake. They do that by linking IP addresses to individual user identities. This approach provides some Sybil attack resistance but is not fully Sybil attack resistant as attackers may obtain a large number of IP-addresses, indistinguishable from benign addresses, easily. For example by using public cloud computing facilities.

Appendix D.34. BeaconBlocks [266]

The BeaconBlocks consensus mechanism removes the need for off-ledger timing input into PoS, thereby eliminating the risks of attacks on clock synchronisation protocols. Therefore, the proposed protocol can be assumed to provide similar Sybil attack resistance to earlier PoS schemes.

Appendix D.35. BLIC [307]

BLIC is a two-stage consensus protocol, composed of a PoET phase for leader election and a BFT phase for block generation. As a mechanism intended for a permissioned platform, it does not provide Sybil attack resistance.

Appendix D.36. Block Maturity Level [195]

The proposed scheme constitutes a difficulty-adjustment approach to PoW that requires miners—under certain conditions in early-stage blockchains—to mine more than one block to be entitled to a reward. While a formal treatment of the Sybil attack resistance properties is absent, it can be assumed that they are comparable to other PoW solutions.

Appendix D.37. Blockchain for the Common Good [196]

In this mechanism for permissioned networks, leader selection is conducted via a Raft-like mechanism (see Appendix D.230). The authors introduce the concept of periodic re-votes to prevent 'domination'. As a permissioned mechanism, no Sybil attack resistance is provided.

Appendix D.38. Blockchain Reputation-Based Consensus (BRBC) [197]

At the centre of BRBC is a monitoring and voting mechanism that constitutes a reputation system taking into account the behaviour of nodes. New potential miners can be added to the system by existing ones and various safeguards are proposed to provide sophisticated Sybil attack resistance for simpler attacks. However, more complex attacks, in which attackers covertly build up a positive reputation with the goal of creating Sybils, can likely not be prevented with the measures proposed.

Appendix D.39. Blockchain-Based Federated Learning Framework with Committee Consensus [308]

In this committee-based approach, leaders are elected periodically based on their past performance. This constitutes a permissioned model in which 'initial nodes [are] responsible for node management' [308] (p. 237). As such, no Sybil attack resistance is provided.

Appendix D.40. Bobtail [198]

Bobtail presents a variation of Bitcoin's PoW consensus with the goal of minimising block confirmation time variance. The changes to the protocol have no effect on the Sybil attack resistance of the base protocol.

Appendix D.41. Byzantine Set Union Consensus (BSC) [309]

BSC is positioned as a building block for permissioned blockchains. It improves on fault-tolerance of other BFT protocols by reducing the impact faulty participants can have. As a permissioned protocol, it does not deliver Sybil attack resistance.

Appendix D.42. Casanova [310]

Casanova is a leaderless, protocol that relies on pre-Nakamoto techniques. The authors envision it to be deployed in conjunction with a PoS blockchain that could provide Sybil attack resistance. However, on its own, it constitutes a mechanism suitable only for permissioned settings and does not provide any Sybil attack resistance.

Appendix D.43. Caucus [311]

Caucus constitutes a mechanism to randomly select a leader from a pool of candidates. However, the protocol does not address the question of limiting the number of participants. Therefore, in itself, the protocol does not provide Sybil attack resistance.

Appendix D.44. Chains of Activity (CoA) [199]

The CoA protocol addresses the network fragility that can ensue on a longest-chain PoS system if nodes act rational rather than altruistic. Periodic checkpointing is introduced to combat such rational forks. The proposed protocol exhibits strong Sybil attack resistance properties, similar to other PoS protocols.

Appendix D.45. Circle of Trust [200]

The circle of trust protocol constitutes a semi-permissioned system backed by a PoS-based reputation system. In this system, 30 % of voting power is guaranteed to be available to the 'chain owner' (thereby making the system semi-permissioned) and 10 % of voting power is available to the address that holds the largest funds. The rest of the voting power aligns with the 'trust score' of individual members. While the latter is abusable through Sybil attacks, the circle of trust mechanisms can be thought of as providing some Sybil attack resistance due to the aforementioned static voting power threshold.

Appendix D.46. Client-Assisted Consensus [267]

Client-Assisted Consensus is a consensus mechanism for blockchains where clients, instead of leaders, coordinate the protocol. This allows for parallel execution and reduces transaction size. Sybil attack resistance is not central to the proposed consensus mechanism. However, the authors suggest that a PoW scheme can be introduced to selected clients to join a BFT committee in order to mitigate Sybil attacks. Under the assumption of the application of a strong PoW protocol, the overall mechanism can be considered to provide equally strong Sybil attack resistance.

Appendix D.47. ClouDPoS (with CSP Invovlement) [268]

ClouDPoS using CSPs is a centralised protocol in which users can stake cloud resources (i.e., CPU, memory, and networking resources) by instructing a CSP to withold access from them. As a permissioned approach, this mechanism does not provide Sybil attack resistance.

Appendix D.48. ClouDPoS (with Resource Utilisation) [268]

ClouDPoS, in the decentralised flavour, is misleadingly named as it constitutes a PoW approach: to 'stake' compute resources, the miner is required to 'instantiate a VM that consumes [. . .] CPU slices, [. . .] memory, and [. . .] networking bandwidth' [268] (p. 305) equating to the amount staked. As such, it may provide strong Sybil attack resistance under the assumption that the reliability of this stake commitment is high.

Appendix D.49. Coinami [312]

Coinami constitutes a permissioned PoUW scheme in which a public key infrastructure (PKI) of authorities is used to assign deoxyribonucleic acid (DNA) sequence alignment tasks to potential leaders. As it is intended for a permissioned system, this mechanism does not exhibit Sybil attack resistance.

Appendix D.50. Committee-Based Byzantine Consensus [313]

In this permissioned mechanism, committees are formed to improve confirmation time over previous BFT protocols. To efficiently rotate the committee, an election algorithm taking into account previous consensus performance and participants' authentication information is applied. As a permissioned protocol, Sybil resistance is not a design concern.

Appendix D.51. Composite Framework Leveraging Proof-of-Stake and Proof-of-Work [201]

The proposed algorithm combines a PoW setup phase, during which nodes can build stake, with a PoS operational phase during which nodes can lock collateral to assume 'Masternode' status. Regular nodes can also qualify for 'Masternode' status, should they participate in high-volume cryptocurrency transactions. The PoS mechanics of the protocol indicate strong Sybil attack resistance.

Appendix D.52. Conflux [202]

This is a PoW-based consensus mechanism with a comparatively fast block generation rate. This is achieved by optimistically processing concurrent blocks. The Sybil attack resistance of the proposed protocol can be considered comparable to those of other PoW schemes.

Appendix D.53. Consensus of Trust (CoT) [394]

CoT introduces a reputation system based on 'credit value', a metric that measures the level of trust that a node has earned. Individual credit values are calculated based on trust relationships with other nodes. The credit value influences the probability to get elected as a delegate node for participating in the consensus process. Delegate nodes then take turns generating new blocks. This approach provides some Sybil attack resistance but may not be able to withstand complex, well-orchestrated, Sybil attacks in which large networks of identities are created to mutually influence their credit value positively.

Appendix D.54. Consensus Through Herding [314]

Inspired by the social phenomenon of 'herding', in which people follow a popular choice, Hubert Chan et al. [314] introduce a new approach to achieve consensus by assuming an honest participant would choose the most popular of two conflicting options. Sybil attack resistance is discussed in passing and it is suggested that central access control (e.g., through a centrally managed PKI) could be used to achieve it. However, Sybil attack resistance is not a concern of the core protocol and, therefore, not provided by it.

Appendix D.55. Consensus-based Oracle Protocol for the Secure Trade of Digital Goods 1122 (COST) [203]

COST is an on-ledger consensus protocol for information originating from oracles (off-ledger). The essential contribution of this work is a compensation scheme for validators as well as an incentivisation mechanism that discourages validators from voting dishonestly. Pools of validators with random selection are introduced to prevent Sybil attacks. It is, however, acknowledged that this approach provides only limited protection. The authors recommend employing identity management to reduce the risk of Sybil attacks.

Appendix D.56. Credence-Based Consensus [315,316]

A reputation system based on 'credence value' is introduced in ROAchain. This value is fixed at the inception of the chain and increases with subsequent protocol rounds for those participants who adhere to the protocol. Participants with high values gain a higher likelihood of being selected as leaders. While this approach provides some Sybil attack resistance, more complex Sybil attack scenarios in which an attacker pretends to be a legitimate user while building up 'credence' to strike later, would not be prevented if deployed in a permissionless setting. Since ROAchain is a permissioned design, the absence of Sybil attack resistance is expected.

Appendix D.57. Credit-Based Verifier Selection with Double Consensus [395]

In this reputation-based consensus mechanism, nodes are rated along two dimensions: 'quality of historical task completion' and 'verification success rate'. Reputation scores are recalculated sporadically. It is unclear whether the proposed algorithm targets permissioned

or permissionless systems. It can, however, be assumed that, if deployed to a permissionless system, limited Sybil attack resistance would be provided due to the risk of attackers forming a large group of Sybil nodes.

Appendix D.58. Cross-Application Permissioned Blockchain (CAPER) [317]

CAPER follows a pluggable consensus model on the base layer, supporting common crash fault tolerance (CFT) protocols, like Paxos, or BFT protocols, like PBFT. The consensus model targets permissioned systems and is therefore not designed with Sybil attack resistance in mind.

Appendix D.59. Crux [269]

Crux is a consensus mechanism that builds on DPoS for Sybil attack resistance. Stakeholders cast votes congruent with their stake and selected leaders subsequently engage in XPaxos. The Sybil attack resistance properties are comparable to those of other PoS schemes.

Appendix D.60. Cumulative Proof-of-Work [204]

In the cumulative PoW protocol introduced in the context of Graphchain, new transactions are validated by previous ones, forming a connected graph with the goal of achieving fair and predictable rewards for participant nodes. Sybil attack resistance is a key consideration of the protocol and the Sybil attack resistance properties can be assumed to be equivalent to Nakamoto-style PoW despite the differences in protocol architecture.

Appendix D.61. Dynamic PBFT [318]

Dynamic PBFT allows nodes to join and leave an established decentralised network during the runtime of the protocol. It, furthermore, introduces measures to penalise misbehaving replicas. As a mechanism for permissioned settings, it does not provide Sybil attack resistance.

Appendix D.62. DagGrid [319]

DagGrid introduces a directed acyclic graph blockchain on the DNS resolver side where random selection with priority is used to construct committees. The committee-building approach is informed by a reputation system that takes a number of metadata attributes (e.g., 'the geographical area of the resolver, software implementation [...], etc.' [319] (p. 759)) into account. As these attributes cannot be gathered autonomously, but have to originate from off-ledger sources, the proposed mechanism can conceivably only be implemented in a permissioned setting.

Appendix D.63. Decision-Theoretic Online Learning Consensus [396]

This algorithm employs a reputation system in which nodes that make consistently reliable assertions with low latency are rated highly. These highly rated nodes are then selected to participate in BFT consensus. While this approach provides some Sybil attack resistance, it can likely be circumvented by a strategic attacker that builds up the necessary reputation over time.

Appendix D.64. Delegate Consensus Algorithm [320]

In this protocol, a group of delegates to perform a BFT subprotocol is selected pseudo-randomly. This is done to improve the performance of the overall process. No measures to introduce Sybil attack resistance are taken.

Appendix D.65. Delegated Adaptive Byzantine Fault Tolerance (DABFT) [321]

Upon the generation of a new block, DABFT selects a committee of 'most relevant' nodes for validation. This selection process is based on the 'rule of relevancy' scheme,

which is informed by the reputation value of a node determined by Delegated Proof of Economic Value (DPoEV) (see Appendix D.67). Therefore, this process is equally centrally controlled, can only be considered for permissioned systems, and provides no Sybil attack resistance.

Appendix D.66. Delegated Byzantine Fault Tolerance [413]

dBFT is a consensus mechanism based on the PBFT algorithm. It determines the group of leaders using voting, thereby improving the performance of the system in the dimensions of block time and transaction confirmation time. The mechanism does not provide Sybil attack resistance and, therefore, needs to be combined with an appropriate scheme when deployed to a permissionless environment.

Appendix D.67. Delegated Proof of Economic Value [321]

DPoEV constitutes a centrally-managed, PoS-like, reputation system in which the 'economic value' of a node is determined and used as an approximation of their initial stake. Such a concept, however, needs to rely on external signals and can, therefore, only be effective in a permissioned setting and does, accordingly, not provide Sybil attack resistance.

Appendix D.68. Delegated Proof of Stake with Downgrade [270]

To target a perceived 'rich getting richer' effect Ge et al. [638] in PoS, the authors propose a hybrid consensus mechanism combining features of PoW and DPoS. An initial PoW 'Screening' phase is used to identify a set of candidate nodes which are pooled together with a set of nodes chosen based on stake. A subsequent DPoS-style voting process is used to elect a final set of witness nodes. The Sybil attack resistance properties are difficult to assert without formal treatment, however, it can be assumed that they are similar to DPoS or PoW schemes deployed in isolation.

Appendix D.69. Delegated Proof-of-Reputation (DPoR) [205]

DPoR (Note that multiple algorithms with the name DPoR exist [205,206,397].) is intended for systems that '[fit] the characteristics of a permissioned chain' in which enterprises can engage in carbon emission trading. The system approximates PoS and allows for the assignment of voting power to participants based on their previous performance. As a protocol intended for a permissioned system, no Sybil attack resistance is provided.

Appendix D.70. Delegated Proof-of-Reputation (DPoR) [397]

In DPoR, a numeric approximation of 'reputation' determines the priority to be selected as a block producer. The reputation score is calculated based on the 'historical quality of task [*sic*] and the success rate of verification'. As such, ad-hoc Sybil attacks are preventable while orchestrated ones may still be successful.

Appendix D.71. Delegated Proof-of-Reputation (DPoR) [206]

Do et al. [206] introduce a DPoS-like reputation system, centring on the metrics of 'staked amount, resource usage and transaction activity' [206] (p. 91). Resource usage is a problematic metric due to self-reporting bias, and transaction activity is prone to wash trading: therefore, these metrics could easily be exaggerated by attackers. Since the foundation of the protocol is, however, the staked amount, strong Sybil attack resistance characteristics, similar to other DPoS protocols can be assumed.

Appendix D.72. Delegated Proof-of-Stake [145]

DPoS extends the PoS paradigm by allowing stakeholders to elect a group of potential block producers whom they trust, thereby removing the need for participating in consensus themselves. Even though the centralisation that ensues from this approach has been

criticised, the Sybil attack resistance properties of the algorithm are similar to those of regular PoS algorithms.

Appendix D.73. Delegation Based Scalable Byzantine False [sic] Tolerance Consensus [414]

DSBFT constitutes a two-layer consensus mechanism. To form committees, PoW is used. Then, within a committee, consensus on a block is reached through BFT. This is done with the goal of enabling the benefits of both mechanisms: security through PoW and scalability through BFT. The Sybil attack resistance of the proposed scheme is non-obvious, as PoW is only performed during the onboarding of a new client and not continuously.

Appendix D.74. Dependability-Rank-Based Consensus [322]

Dependability-Rank-based consensus constitutes a reputation-based consensus mechanism for permissioned networks. In this algorithm, 'bookkeepers' (participants who qualify as miners) are selected for mining subsequent blocks with a probability that aligns with their dependability rank. The mechanism is intended to be used in permissioned networks and does not offer Sybil attack resistance.

Appendix D.75. Deterministic Proof-of-Work [271]

Deterministic Proof-of-Work (DPoW) constitutes a PoW/PBFT-hybrid, coordinated by 'sharding servers'. The size of the shard controlled by a server is determined by the participation in PoW. The authors claim a significant consensus time improvement over previous, unsharded, PoW protocols. The implications of sharding on Sybil attack resistance are not obvious, but it can be assumed the Sybil attack resistance properties are similar to previous PoW protocols.

Appendix D.76. DEXON [323]

Among other proposals, DEXON introduces a single-chain protocol that selects leaders based on a novel verifiable random function that has advantages over previous work in terms of fairness. Sybil attack resistance is, however, not a concern of the protocol and is not achieved by its implementation.

Appendix D.77. DFINITY [324]

In DFINITY, consensus is achieved by pseudorandom leader selection using a decentralized randomness beacon. The algorithm proposed, by design, does not incorporate mechanisms to achieve Sybil attack resistance but would, instead, rely on external methods to provide Sybil attack resistance identities.

Appendix D.78. DTNB [160]

In DTNB nodes can obtain 'mining qualification' though a pseudorandom selection process based on their communicated IP address. While this approach provides some Sybil attack resistance, coordinated Sybil attacks that make use of techniques to obtain larger numbers of IP addresses (e.g., IP address blocks) cannot be mitigated.

Appendix D.79. Dynamic Hierarchical Byzantine Fault-Tolerant Consensus Based on Credit [325]

In this system using a reputation system, participants with higher credit are deterministically selected as leaders. Adherence to the protocol is quantified via a reward and punishment regimen. As an algorithm for a permissioned environment, no Sybil attack resistance is provided.

Appendix D.80. Efficient, General, and Scalable Consensus [154]

The key contribution of Chen et al. [154] is an extension to (permissioned) BFT systems that run in a public environment. As these may suffer from Denial-of-service (DoS) attacks, Efficient, General, and Scalable Consensus (EGES) introduces a protocol that allows for the

introduction of a large number of fake committee nodes to deter such attacks. This does, however, not contribute to Sybil attack resistance.

Appendix D.81. Egalitarian Practical Byzantine Fault Tolerance [326]

A simplification of PBFT is introduced with this mechanism in which data is backed up and verified without the involvement of the leader. The consensus mechanism is designed for permissioned systems and does not provide Sybil attack resistance.

Appendix D.82. Electronic Identification, Authentication and Trust Services Validating Indy-Plenum [327]

Abraham et al. [327] extend 'Indy-Plenum', in itself an implementation of an Reputation-based Byzantine Fault Tolerance (RBFT) consensus protocol [639], by adding functionality to verify electronic IDentification, Authentication and trust Services (eIDAS) identity assertions attached to transactions. This additional validation is, however, not contributing to Sybil attack resistance. Instead, the system proposed relies on trusted validator nodes, or 'Stewards', rendering it permissioned.

Appendix D.83. Elpis [328]

Elpis constitutes a multi-leader consensus protocol that can tolerate byzantine faults combined with network asynchrony. The protocol is presented with the goal of performance improvements which the authors quantify by a factor of 3.5 over common BFT protocols. Sybil attack resistance is not a design goal of the protocol and is not provided by it.

Appendix D.84. Equihash [207]

This asymmetric PoW protocol relies on memory as a scarce resource. Therefore, it does not require professional ASIC or Graphics processing unit (GPU) equipment but uses memory readily available in commodity hardware. As a common PoW approach, this mechanism is resistant to Sybil attacks.

Appendix D.85. Error-Correction Code Based Proof-of-Work [208]

This alternative PoW utilises randomly generated Low-density parity-check code (LDPC) matrices to achieve ASICs resistance. The proposed mechanism has Sybil attack resistance properties comparable to earlier PoW schemes.

Appendix D.86. Estimable PoW [209]

Estimable Proof-of-Work (EPoW) constitutes a variation on Nakamoto-style nonce-based PoW by introducing upper and lower bounds for difficulty adjustments to allow for fairer cooperative mining. The scheme can be assumed to provide similar Sybil attack resistance to existing PoW protocols.

Appendix D.87. Extended PoS [272]

e-PoS is a PoS variant that aims to provide a higher level of decentralisation and fairness when compared to previous PoS schemes. The authors deem other PoS schemes to suffer from centralization due to a 'rich getting richer' [638] effect. They counteract this by introducing 'baseline stake', an amount of wealth that nodes must exceed to qualify as miners. This value is intended to strike a balance between allowing participation by a broad group of miners while deterring attacks. It can be assumed, given reasonable configurations of baseline stake calculation, that the overall protocol exhibits Sybil attack resistance similar to other PoS algorithms.

Appendix D.88. Extensible-PBFT [329]

In this BFT mechanism, VRFs are employed to randomly select leaders, an approach that is well-suited for permissioned networks but cannot be used to prevent Sybil attacks in

permissionless networks where an attacker can present a large number of potential leader identities.

Appendix D.89. Fair Proof-of-Work System with Computing Power Rating [210]

In this PoW protocol, each miner is evaluated by their computing power, number of blocks generated, and ongoing participation. It is proposed to adjust difficulty and reward based on this evaluation to make mining fairer. This scheme is, however, likely attackable by miners understating their actual computing power. Therefore, the Sybil attack resistance of the protocol is likely lower than that of conventional PoW. But, under the assumption of conservative configuration, still comparatively high.

Appendix D.90. Fair Selection Protocol for Committee-Based Permissionless Blockchains [273]

The proposed selection protocol is used for composing committees in permissionless environments. It encompasses two main aspects: mining, during which nodes are proposed, and a confirmation phase in which they are selected. For Sybil attack resistance the authors propose two potential solutions: PoW and Proof of Identity via a centralised provider. This makes the protocol suitable for consortiums and federations in both permissioned and permissionless settings.

Appendix D.91. Fantômette [170]

Fantômette extends the Caucus mechanism (see Appendix D.43) by introducing a PoS-like incentive model to achieve strong Sybil attack resistance. This incentive model requires participants to place security deposits locking some of their funds.

Appendix D.92. Fast Leader-Based, Randomized Byzantine Agreement [330]

The author proposes multiple consensus mechanisms for a permissioned distributed ledger, with the goal of minimising the number of rounds required to reach consensus. A novel leader-based, randomised BFT algorithm is presented that reaches consensus in two rounds, under the assumption of the honesty of the selected leader, and in 6 rounds under the assumption of a byzantine leader. As a protocol for a permissioned environment, no Sybil attack resistance is necessary, and thus the number of malicious actors that it can tolerate is not a key concern.

Appendix D.93. Fast Probabilistic Consensus with Weighted Votes [415]

FPC is a fast probabilistic protocol that is designed to provide robustness in an environment with malicious actors. FPC stipulates that the voting power of a node is proportional to its reputation. No concrete scheme to achieve this is presented. Instead, the authors make a generic reference to 'mana', which is some function of reputation and can be derived from 'any good or [resource]'. This may take the form of stake or any other quantifiable measure of influence. The Sybil attack resistance of the protocol is dependent on the implementation of 'mana'.

Appendix D.94. FastBFT [331]

FastBFT is a protocol that applies message aggregation and secret sharing to reduce message complexity, thus achieving better scalability than existing BFT protocols. It makes extensive use of TEEs to improve efficiency and security and is therefore well suited for demanding next-generation blockchain systems. Sybil attack resistance is not addressed through means of the protocol.

Appendix D.95. Filtered Proof-of-Work [274]

Filtered Proof-of-Work (FPoW) is a simple variation of common PoW protocols that subjects miners to solving 'dummy mathematical puzzle[s]' before the actual PoW. This is done to detect any miners that utilise ASIC hardware. Those miners are subsequently

removed from the pool of eligible miners. The Sybil attack resistance properties are equivalent to common PoW protocols.

Appendix D.96. Geo-Scale Byzantine Fault Tolerance [332]

This protocol is designed with distributed system deployments spanning large areas in mind. In Geo-Scale Byzantine Fault Tolerance (GeoBFT), geographically close nodes are assigned to local clusters to minimise latency. The protocol is not designed for Sybil attack resistance and is intended to be operated in a permissioned context.

Appendix D.97. Goshawk [211]

Goshawk is a two-layer consensus mechanism with different mining difficulties. It aims to improve efficiency as well as fairness. To benefit throughput the microblock concept is applied. Microblocks are mined with a lower difficulty and thus can be produced more frequently. Periodically, these microblocks are checkpointed into keyblocks, which are mined with regular difficulty. This approach can be considered to provide Sybil attack resistance similar to PoW under the assumption of reasonable difficulty configuration.

Appendix D.98. Graph Learning BFT [333]

GL BFT is a consensus mechanism which is designed to achieve instant finality and high performance. It utilises path learning to adapt to network conditions, and uses node traversal to reduce message overhead. As a mechanism providing small group consensus, it is applicable to private blockchain platforms such as Hyperledger Fabric and does not provide Sybil attack resistance.

Appendix D.99. Greedy Observed Largest Forest (GOLF) [275]

GOLF constitutes a replacement of the Greedy Observed Heaviest Sub-Tree method applied to fork handling in some newer blockchain protocols. GOLF takes into account not only all sibling blocks of a forked block but also all sibling blocks of the forked block's isotopes. This allows for better resistance against some common attacks. It is conceivable that this change in approach has no fundamental effect on Sybil attack resistance.

Appendix D.100. Green Mining [416,417]

The paper by Jacquet and Mans [416,417] appears to sketch a scheme in which some inherent property of a block indicates whether it is 'ready' to be mined, or not. This approach is susceptible to attacks from transaction censorship (i.e., an attacker could withhold certain proposed transactions or compile them in a way that is useful to generate a certain hash output). This potential attack aside, the Sybil attack resistance properties are non-obvious since the workings of transaction proposal selection are unclear.

Appendix D.101. Green-PoW [212]

This PoW scheme aims to reduce unnecessarily consumed electricity during mining by not only granting the winner of a PoW competition rights to mine a block, but by also granting special status to runner-ups. However, due to the risk of a successful miner creating Sybil runner-ups, the protocol provides limited Sybil attack resistance.

Appendix D.102. Group-Based Optimized Practical Byzantine Fault Tolerance [334]

Group-Based Optimized Practical Byzantine Fault Tolerance (GPBFT) extends previous work of Bao [299] (see Appendix D.5) that includes some changes to the message passing logic. From Sybil attack resistance perspective, this protocol, however, behaves identically.

Appendix D.103. Guru [398]

Guru constitutes a reputation mechanism that can be operated in conjunction with existing consensus mechanisms, such as PBFT or HoneyBadger. Guru introduces a repu-

tation system to committee selection that rewards participants for correct behaviour and penalises them for incorrect behaviour. While the authors discuss Sybil attack resistance of their protocol and choose protocol parameters to deter Sybil attacks, they remain possible if conducted by a sufficiently powerful adversary. Therefore, the protocol has limited Sybil attack resistance.

Appendix D.104. HashCore [276]

To provide resistance against novel ASICs,, specifically designed to be efficient in solving Bitcoin's PoW puzzle, Georghiades et al. [276] propose a workload which common general purpose processors are optimally equipped for solving. This is done with the intention of making PoW mining more accessible. The Sybil attack resistance properties are similar to existing PoW and PoUW schemes.

Appendix D.105. HotStuff [335]

HotStuff is a BFT mechanism using a three-phase commit protocol to achieve consensus. It is highly performant, moving at the *actual* network delay (as opposed to the *maximum* delay) and exhibiting linear communication complexity in the number of replica nodes. Sybil resistance is not a design goal of this BFT scheme.

Appendix D.106. Hybrid PoW/PoS [277]

This hybrid protocol for collaborative intrusion detection networks constitutes a reputation-based difficulty adjustment mechanism. Dependent on the participant's stake, the difficulty of the PoW puzzle is adapted. Given sensible protocol parameters, this approach can be considered to provide high Sybil attack resistance.

Appendix D.107. Hybrid PoW/PoS [213]

To lower the 51 % attack risk of low-capitalisation blockchains, Harvilla and Du [213] propose a PoW/PoS hybrid in which any PoW-mined block has to be confirmed via PoS. The Sybil attack resistance of this approach is presumably comparable to those of PoS and PoW if deployed individually.

Appendix D.108. Hybrid Byzantine Agreement [336]

Similar to Robust Byzantine Agreement (RBA), this protocol achieves partition resilience and is tolerant to up to $1/3$ corrupt nodes. In contrast to RBA, it only achieves 'weakly fair validity', meaning a lower degree of likelihood for all participants to be selected as leaders over time. As a permissioned protocol, it does not provide Sybil attack resistance.

Appendix D.109. Hybrid Consensus with Flexible Proof-of-Activity [214]

In this hybrid PoS/PoW protocol, the weight assigned to a node is determined by its PoW capabilities in combination with the value of tokens staked. The probability of gaining leader status is proportional this weight. This is done with the goal of improving stability by eliminating the risk of forks. The Sybil attack resistance properties are comparable to those of traditional PoW.

Appendix D.110. Identifiable Practical Byzantine Fault Tolerance [337]

Identifiable Practical Byzantine Fault Tolerance (IPBFT) extends BFT by adding a mechanism to prevent leaders that failed to follow the protocol historically from serving as leaders at a later point. This approach requires a Certificate authority (CA) to revoke misbehaving peers' certificates and is, therefore, only suited for a permissioned network.

Appendix D.111. Identity-Augmented Proof-of-Stake (IdAPoS) [399]

This protocol applies PoS mechanics to a reputation system. The reputation system relies purely on participants in the systems mutually evaluating each other. Using Sybil

attack mitigation strategies, simple Sybil attacks can be prevented, while more complex ones would likely not be preventable.

Appendix D.112. Improved DPoS with K-Means [215]

In this modification of conventional DPoS, a K-means algorithm is used to select suitable nodes. Nodes are selected based on their previous voting activity and, derived from this, the probability of voting for nodes that adhere to the protocol, or violate it. The Sybil attack resistance of the protocol can be considered to be comparable to other DPoS protocols.

Appendix D.113. Interactive Proof-of-Stake [216]

To improve its resilience against forks, Chepurnoy [216] introduces a modification to longest-chain PoS which mandates multiple miners to collaborate on the creation of a new block (rather than a single entity). The Sybil attack resistance properties of the underlying PoS protocol remain unchanged.

Appendix D.114. Istanbul BFT Consensus [338]

The Istanbul BFT consensus algorithm is leader-based, and highly resilient, tolerating f out of n faulty processes with $n \geq 3f + 1$. It is used in the Quorum blockchain, a permissioned fork of Ethereum, to implement state machine replication. Due to its permissioned nature, no Sybil attack resistance mechanism is provided.

Appendix D.115. Itsuku [278]

Itsuku constitutes a PoW algorithm that is 'memory-hardened', i.e., it does not rely on computational power alone. The algorithm improves issues with the application of Argon2 as a memory-hard password hashing function that the authors have previously observed. It provides Sybil attack resistance properties similar to the well-known CPU-bound PoW schemes.

Appendix D.116. Leader-Stable Fast Byzantine Fault Tolerance [339]

FBFT constitutes a secure and scalable sharding-enabled consensus mechanism. It is designed with the goal of reducing message complexity inside shards and reducing the processing efficiency of cross-shard transactions. On its own it does not provide Sybil attack resistance, rather, it relies on a fair selection protocol utilizing PoW, or a centralised CA-based admissions process.

Appendix D.117. LFT2 [340]

ICON uses a consensus algorithm titled LFT2, which is similar to PBFT. In it, leaders are tasked with packaging transactions in blocks and broadcasting them to other nodes. Recipient nodes can, subsequently, verify that the received block is proposed by a valid leader and express the result of the verification by vote. This approach is susceptible to Sybil attackers negatively influencing the outcome of the voting process.

Appendix D.118. Lisk-BFT [341]

The proposed BFT consensus mechanism is intended for the Lisk blockchain ecosystem. The mechanism is designed to be deployed in the context of an existing PoS/DPoS Sybil attack resistance scheme and does not provide Sybil attack resistance on its own.

Appendix D.119. LocalCoin [163]

The LocalCoin scheme requires users to validate individual transactions on a network based on their spatial relationship. While the protocol is focused on preventing certain attacks, foremost double-spend attacks, as efficiently as PoW, it is not fully Sybil attack resistant: for a block to be created, a minimum number of users have to verify each

transaction. However, attackers may censor proposed transactions or may otherwise gain the ability to act as block producers if they present a sufficiently large number of Sybils.

Appendix D.120. MaGPoS [171]

MaGPoS is a consensus mechanism that uses the physical principles of a lattice of magnetic dipoles to achieve consensus. It is designed with the goals of improving scalability over other PoS implementations and minimising energy requirements. For Sybil attack resistance, PoS is used. Therefore, the Sybil attack resistance of MaGPoS is comparable to other PoS implementations.

Appendix D.121. Majority vOting Cellular Automata [342]

Taking inspiration from Zero-T Ising-Glauber Consensus and cellular automata, Wang [342] proposes a scalable consensus model, Majority vOting Cellular Automata (MOCA). Consensus between participants is achieved by applying concepts from the domain of physics. However, Sybil attacks are not a concern for the protocol, as it is, apparently, tailored towards permissioned systems.

Appendix D.122. Mchain Consensus [343]

The Mchain consensus is a two-layer consensus mechanism intended for use in a permissioned setting. Proposed transactions are confirmed by a single (presumably randomly selected) node on the base-layer network and then relayed to the higher layer for permanent storage. Should a node on the base layer submit an invalid block to the higher layer, it would be penalised. The approach does not provide censorship resistance or Sybil attack resistance.

Appendix D.123. Mobile Crowdsourcing Chain [217]

The consensus mechanism employed by Mobile Crowdsourcing Chain (MCS-Chain) constitutes a race in which the miner who can earliest demonstrate having collected valid transaction proposals of a certain volume, wins the right to produce a block. This approach is highly vulnerable to Sybil attacks, as colluding transaction proposers might engage in wash trading to influence the chances of being selected.

Appendix D.124. Multi-Block BFT [344]

In this lightly-modified PBFT scheme, a batch of messages, representing multiple blocks, is propagated to peers, thereby nominally improving throughput. As a BFT scheme Sybil attack resistance is not a concern to the protocol.

Appendix D.125. Multi-Round Concession Negotiation [172]

In this mechanism, which does not discuss Sybil attack resistance, leaders enter into a 'concession consultation' phase, allowing them to find a satisfying compromise in the case of conflict. Good consultation performance is rewarded by the protocol, while the opposite is penalised.

Appendix D.126. Multi-Supervised Permissioned Blockchain [345]

In this protocol, two classes of nodes exist: a predetermined set of 'supervisory nodes', that control access to the network and audit transactions and 'ordinary nodes' that propose transactions. As such, the system is not resilient against Sybil attacks.

Appendix D.127. Multi-Tokens Proof of Stake [218]

MPoS is a consensus protocol built on staking tokens on various chains. Parachain tokens, defined as tokens that are not the native token of the main chain, can also be staked in addition to the main chain's native token. Intuitively, this may weaken the security guarantees of the system when compared with PoS on the native token only, since parachain

tokens may be vulnerable to additional attacks. However, under the assumption of strong security of parachain tokens, the overall system is likely to provide equally strong security.

Appendix D.128. Multiple Winners Proof of Work [219]

MWPoW is a variation on earlier PoW protocols that sets out to improve decentralization by increasing the likelihood of resource-constrained miners earning rewards. Furthermore, the protocol allows for more flexibility in block size and block interval, making it more adaptive to changing network conditions. The Sybil attack resistance properties can be considered similar to those of earlier PoW schemes.

Appendix D.129. Multisignature-BFT [346]

Multisignature Byzantine Fault Tolerance (MSig-BFT) constitutes an extension to BFT, appropriate for permissioned networks, in which not only a leader is selected but also a set of 'witnesses'. This role serves the purpose of pre-validating any proposed block to supervise leader decisions. However, as the protocol is designed for permissioned networks, no Sybil attack resistance is provided by it.

Appendix D.130. Musch [347]

Musch is a window-based BFT consensus mechanism that does not provide Sybil attack resistance.

Appendix D.131. NeuCoin [173]

NeuCoin uses PoS for Sybil attack resistance. The configuration of the PoS protocol diverges from common PoS protocols in some key aspects: low minimum stake age, no influence of coin age on stake, and punishment of misbehaving stakers. The Sybil attack resistance properties are, however, not influenced by these reconfigurations and remain strong.

Appendix D.132. Open Business Environment BFT [348]

In this BFT scheme for permissioned ledgers, a credit score is assigned to each node based on its past behaviour in the system. Nodes with higher credit scores have a greater probability of becoming leaders following re-election (view change). This scheme aims to solve the problem of consensus failures and message overhead under Byzantine failures. As a BFT protocol, Sybil attack resistance is not a design concern.

Appendix D.133. Open Representative Voting (ORV) [279]

ORV is a PoS scheme in which representatives vote on transactions and blocks are confirmed if they get enough votes to reach a quorum. A variation on common PoS schemes is the role of the principal representative, which holds more than 0.1 % of the total supply of cryptocurrency: only representative votes are made available to other nodes to minimise network traffic. The Sybil attack resistance of the proposed scheme is equivalent to that of common PoS schemes.

Appendix D.134. Optical Proof-of-Work [220]

Instead of conventional CPU, memory, or storage resources, Optical Proof-of-Work (oPoW) uses photonic coprocessor output which the authors believe to offer a better Capital expenditure (CAPEX)/Operating expenditure (OPEX) ratio in the current economic environment. This is due to the comparatively low energy consumption of photonic coprocessors in relation to their purchase price. Under this assumption, unnecessary energy consumption is lower when compared to conventional PoW. It can be assumed that this PoW scheme has good Sybil attack resistance properties, similar to conventional PoW schemes.

Appendix D.135. Ouroboros Crypsinous [280]

Ouroboros Crypsinous proposes some changes to Ouroboros Genesis, namely in leadership election and transaction processing. It, however, exposes comparable Sybil attack resistance properties to Ouroboros Genesis.

Appendix D.136. Ouroboros Genesis [281]

Ouroboros Genesis is a PoS protocol that allows participants to join a PoS system using only genesis block information. It provides the same strong Sybil attack resistance properties as other PoS-based protocols.

Appendix D.137. Ouroboros Praos [282]

Ouroboros Praos is a PoS protocol with strong security guarantees, namely, tolerating any message delay introduced with malice, and the ability to withstand the corruption of any previously honest protocol participant (as long as the overall tolerable threshold of maliciously-held stake is not exceeded). Therefore, their protocol provides Sybil attack resistance guarantees as strong as those of previous protocols or stronger.

Appendix D.138. Parallel Proof-of-Work [221]

Parallel Proof-of-Work is a mechanism that encourages collaborative mining. While the claimed performance improvement seems largely related to difficulty adjustments and might not manifest in a real-world environment with economic incentives, the Sybil attack resistance properties of the scheme can be considered identical to previous PoW schemes.

Appendix D.139. PeerBFT [349]

PeerBFT introduces BFT characteristics to the ordering service of Hyperledger Fabric. It does this by having each peer audit the ordering service and change to a new ordering service if necessary. The authors present results that compare the protocol's performance to Hyperledger Fabric with Solo ordering: in their experiment, PeerBFT achieved approximately 90.8 % of transactions per second of the Solo ordering service. As a permissioned protocol, no Sybil attack resistance is provided.

Appendix D.140. Penalty by Consensus in PoW [174]

Adewumi and Liwicki [174] offer a variation on the conventional PoW paradigm by suggesting to introduce 'penalty by consensus'. This entails specifying a network-wide ceiling on power consumption that nodes would have to adhere to in order to reap mining rewards. Details on the implementation of this scheme are, however, absent.

Appendix D.141. Permissioned Trusted Trading Network Consensus Algorithm [418]

In this permissioned consensus mechanism, a random partition algorithm is proposed to split peers in the network into subcommittees. Global consensus is then performed using a proof-of-work protocol, thus combining the partitions. While the parameters of the proposed PoW scheme are not fully clear, under the assumption of the Sybil attack resistance of the PoW scheme, the overall mechanism would exhibit strong Sybil attack resistance. This, however, can be considered irrelevant due to the permissioned nature of the encompassing system.

Appendix D.142. Permissionless Proof-of-Reputation-X [400]

Permissionless Proof-of-Reputation-X (PL-PoRX) constitutes an extension of the semi-centralized Proof-of-Reputation-X (PoRX) algorithm. In contrast to PoRX, PL-PoRX is designed for permissionless systems and makes use of a procedure that allows only existing miners on a network to admit new identities. To prevent Sybil attacks, the protocol demands a deposit from newly admitted accounts. Furthermore, an abstract 'investigation' process is introduced, designed to deduplicate newly created accounts. Whether the imple-

mentation of such a process is Sybil attack resistant determines the Sybil attack resistance class of the entire protocol. Since this is not further specified, limited Sybil attack resistance can be assumed.

Appendix D.143. Personal Archive Service System [350]

Personal Archive Service System (PASS) appears to be conceptualised as a permissioned system in which 'subjects' (ordinary participants) submit information to 'certifiers' (permissioned entities) who engage in a verification protocol. Due to the central involvement of 'certifiers' in consensus, it provides no Sybil attack resistance.

Appendix D.144. Pixel [283]

Drijvers et al. [283] introduce a multi-signature scheme and discuss how its application in a PoS context can reduce bandwidth, storage, and computing requirements. The proposed mechanism does not affect Sybil attack resistance.

Appendix D.145. POA-PBFT [351]

POA-PBFT constitutes a variation on DPOS-BFT. In contrast to this mechanism, no voting is used to determine a leader. Instead, leaders are '[appointed] and [removed] by the central bank' [351] (p. 53,598), rendering the system strictly permissioned and centralised. Therefore, no Sybil attack resistance is provided.

Appendix D.146. PoolCoin [222]

PoolCoin uses a two-layer PoW mechanism with difficulty adjustment based on a reputation system. The reputation system quantifies the adherence of a miner to the protocol. The Sybil attack resistance can be considered comparable to pure PoW schemes.

Appendix D.147. Practical Byzantine Fault Tolerance [144]

While not the first work to address Byzantine faults, Castro and Liskov [144] first set out to present a *practical* implementation of a replication algorithm that can withstand such faults. The major improvement that gives it significance to this day is its ability to function in asynchronous environments while providing an acceptable response time. Sybil attack resistance is not of concern for this algorithm. Therefore, permissionless systems making use of it commonly incorporate other techniques to achieve resistance.

Appendix D.148. Practical Layered Consensus Mechanism [352]

He et al. [352] give a practical example of a layered consensus mechanism that constitutes a two-phase protocol in which transaction ordering and transaction verification form two distinct steps. The authors suggest that these steps require different BFT and can, therefore, be implemented through different protocols (e.g., CFT consensus for the transaction ordering step and BFT consensus for the verififcation step). No preventive measures against Sybil attacks are proposed and the protocol discussed does not provide Sybil attack resistance.

Appendix D.149. Prism [223]

Prism is a deconstruction of Nakamoto-style PoW with the goal of improving the 'fundamental measures' of a PoW blockchain. The authors define these as the maximum tolerable fraction of adversary-controllable hashing power, the system throughput, and its confirmation latency. The protocol's Sybil attack resistance properties are equivalent to those of regular Nakamoto-style PoW.

Appendix D.150. Private Proof-of-Effort [284]

Alberini et al. [284] motivate Private Proof-of-Effort (PPE) as a technique to enable verifiable polling involving mutually-distrustful parties. The mechanism can be used to

enable a 'one vote per effort' paradigm that uses proofs that are, in contrast to PoW, *privately* verifiable. The authors list some potential types of 'effort' that can be applied in the context of the protocol, some of which provide Sybil resistance (e.g., proofs of storage, symmetric captchas, or human interaction). Notably, the protocol does not mandate a concrete view of 'effort'.

Appendix D.151. Proof of Adjourn [285]

To achieve the main goal of counteracting 51 % attacks on PoW, PoAj enforces an Adjourn Period in which all network nodes halt their activities. The first phase can be considered a transaction collection and block formation phase, while the second one is a cooling-down phase in which potential forks are resolved. If the risk of a fork occurs, blocks predominantly made up of large transactions are more likely to be selected as canonical. Under the assumption of reasonable configuration, the Sybil attack resistance properties of the proposed protocol are similar to those of pure PoW.

Appendix D.152. Proof of Block Inclusion [155]

As part of the 'Obscuro' Layer 2 (L2) protocol, a Proof of Block Inclusion mechanism is introduced that uses a lottery and synchronisation with the Layer 1 (L1) in order to achieve consensus. To provide Sybil attack resistance, leaders, or aggregators, need to be registered with the L1 and pay a significant stake. They also need to be in control of a TEE. Proof of Block Inclusion provides Sybil attack resistance under the assumption that attackers cannot conceivably register large numbers of identities. However, no formal treatment of the possibility of such an attack under consideration of their economic conditions is provided.

Appendix D.153. Proof of Contribution [224]

This modification to Bitcoin PoW constitutes a PoW/PoS hybrid. A difficulty adjustment scheme is a core aspect of the protocol. It benefits successful miners who have adhered to the protocol in the past. Centralisation effects aside, it can be assumed that the proposed scheme has Sybil attack resistance properties comparable to other PoW schemes.

Appendix D.154. Proof of Elapsed Time [146]

PoET, a consensus mechanism proposed by the chip maker Intel, builds on TEEs to achieve Sybil attack resistance. While the reference implementation of PoET was written for an abstract TEE, Intel's current specification defines a concrete implementation for SGX, Intel's TEE product. PoET is used to stochastically elect individual peers that prove access to a TEE. Sybil attack resistance is given under the assumption of the ability of the TEE to uniquely identify a processor and under an economic model in which it is unfeasible for an attacker to acquire a large number of TEEs.

Appendix D.155. Proof of Experience [225]

PoE constitutes a mining difficulty adjustment protocol that aims to counteract the trend of excessive mining centralisation by rewarding miners based on their experience, i.e., by whether they have incurred unrecognised mining efforts in previous cycles. It is designed for Bitcoin, but the idea can be extended to other cryptocurrencies. The mechanism can be assumed to provide the same strong Sybil attack resistance properties as in the Bitcoin PoW model.

Appendix D.156. Proof of Kernel Work (PoKW) [419]

PoKW is a refinement of PoW and is designed to reduce the energy consumption of blockchain-based systems by limiting the set of nodes eligible for mining and, thereby, the difficulty of PoW. It intends to support more democratic public blockchain networks. In contrast to previous PoW implementations, PoKW makes it difficult for an attacker to

monopolise the process of creating new blocks. However, due to the security model that stipulates a constant limit of adversarial network nodes, and a lack of formalisation of the reputation system parameters (i.e., the proposed whitelist), the Sybil attack resistance properties remain unclear.

Appendix D.157. Proof of Luck [152]

Proof-of-Luck is a consensus mechanism built on the guarantees made by TEEs. It's designed to achieve high performance during transaction validation while being energy efficient and resistant to rational attackers. As in other TEE-based schemes, TEE-enabled devices serve to provide Sybil attack resistance. This approach provides Sybil attack resistance under the assumption of uncompromised TEE and a high cost of acquisition of TEE devices. Outside of these assumptions, however, the mechanisms by which the consensus is achieved may be vulnerable to Sybil attacks.

Appendix D.158. Proof of Rest [353]

The proposed PoR mechanism centres on a difficulty adjustment scheme in which nodes that have recently built a block are subjected to an increased difficulty value, while nodes without a history of contributing to block finalisation are assigned lower difficulty. This is intended to incentivise equally distributed node activity. This approach, however, can only be effective in permissioned systems since, in a permissionless setting, it could easily be evaded by creating additional accounts.

Appendix D.159. Proof of Segmented Work [226]

Proof of Segmented Work is a PoW/PoS hybrid mechanism aimed at reducing the energy consumption of conventional PoW by increasing propagation speed. To qualify for mining, prospective leaders need to stake some of their cryptocurrency holdings. Subsequently, they are allocated to a sub-pool from which, ultimately, the miner is chosen. The combined protocol can, therefore, be assumed to have Strong Sybil attack resistance.

Appendix D.160. Proof of Social Contact [162]

Martinez et al. [162] propose a social Sybil control scheme implemented in which mobile devices broadcast digitally signed beacons with their identity. A unique user identity is attached to a mobile phone which is carried by a person. When two phones are in range, the beacons of both devices log time stamps to a registry. Martinez et al. [162] propose two simple methods to detect Sybil attacks: first, comparing timestamps of interactions recorded on the ledger and, second, comparing the number of interactions between a given node and others. While the authors evaluate these methods using real mobility traces, it can be assumed that Sybil attacks would not be fully preventable by these mechanisms, as an attacker would likely behave differently from a user from the mobility trace dataset. It can be speculated that a more complex Sybil attack, in which an attacker controls a large number of real or spoofed devices, would not be preventable.

Appendix D.161. Proof of Training Quality [354]

In this proof-of-useful work for permissioned systems, nodes engage in federated learning with the goal of training a global model. The training process is conducted with differential privacy to protect sensitive training data. To share the trained models for use in applications, a collaborative architecture that enables secure retrieval and accurate model training is designed based on permissioned blockchain. Due to its permissioned nature, Sybil attack resistance is not considered.

Appendix D.162. Proof of Usage [227]

PoU is a consensus mechanism for permissioned blockchains that incentivizes users to trade cryptocurrency. Nodes that engage in a larger volume of currency transfers have

a higher chance of being selected as validators, and thus earn rewards. The proposed approach is susceptible to wash trading and does not provide Sybil attack resistance. However, neither of these issues is in scope for this protocol as it targets a permissioned setting.

Appendix D.163. Proof of witness Presence [164]

Proof of witness presence is based on PoL, a mechanism to verify citizens' spatial position by utilising signals exchanged between wireless transmitting devices. By measuring signal attenuation or message propagation times, the position of a device in relation to another can be approximated. It is not clear from the manuscript how this approach could be utilised in leader selection, however, it can be speculated that Sybil attack resistance would be limited due to the reliance on potentially spoofable hardware.

Appendix D.164. Proof-by-Approval [420]

Proof-by-Approval is a form of PoA in which a node gains permission to create a new block if its address is on a static list curated off-ledger. Therefore it is suited for permissioned systems only and cannot be considered Sybil-resistant.

Appendix D.165. Proof-of-Accumulated-Work [286]

Proof-of-Accumulated-Work (PoAW) decouples the provision of PoW from the right to mine new blocks by assigning virtual stakes to those that did computational work. As such, the protocol has Sybil attack resistance properties that are very similar to previous PoW protocols.

Appendix D.166. Proof-of-Accuracy [355]

The Proof-of-Accuracy consensus mechanism centres on 'several resources for the access to which consensus protocol participants compete' [355] (p. 493). The protocol, however, relies on a pseudorandomly selected 'temporary coordinator' to randomise the resources. Therefore, the protocol can be considered vulnerable to Sybil attacks, for example in a situation in which an attacker creates numerous addresses to increase the probability of being selected as 'temporary coordinator'.

Appendix D.167. Proof-of-Achievement [228]

In this proof-of-interaction-like (see Appendix D.188) proposal, which effectively requires a permissioned system, participants are rewarded with stake for completing mobile phone games. A central operator is required for administering the games and asserting the player's performance. Therefore, no Sybil attack resistance is provided.

Appendix D.168. Proof-of-Activity [149]

Bentov et al. [149] extend the Bitcoin PoW protocol to include a PoS-like stakeholder selection with the goal of improving against attacks. The Sybil attack resistance properties remain as strong as in the original protocol, as the changed mechanics do not influence this attack vector.

Appendix D.169. Proof-of-Activity [356]

Proof-of-Activity, described as a 'socially oriented' protocol in which validators will be selected based on their ability to provide 'useful activity in the network'. Concretely, the protocol follows PoS principles and assigns stake to those who provide such activity. The paper does not suggest how usefulness is to be quantified and by whom but it can be speculated that some off-ledger entity would be responsible to do so, therefore rendering it permissioned and, as a consequence, not Sybil attack resistant.

Appendix D.170. Proof-of-Atomicity [357,358]

This mechanism sketch describes a completely centralised system in which 'the administrator who [created] the ledger [gives] 100 % approval.' Lee and Yoon [357] (p. 40) to create a new block. No Sybil attack resistance is provided through this approach.

Appendix D.171. Proof-of-Authority [359]

Proof-of-Authority is a consensus mechanism that constitutes a building block for permissioned networks. It relies on a small number of authorised nodes to validate transactions. It is, therefore, popular for private or consortium blockchains. Proof-of-Authority, similar to other permissioned or BFT mechanisms, requires little energy.

Appendix D.172. Proof-of-Balance [401]

Motivated by 'cue-authenticated signalling' in which certain inherently useful traits of individuals are also considered signals for quality [640], Ehrlich and Guzova [401] introduce Proof-of-Balance in an extensive paper: at the core of the proposed scheme is a mechanism which assigns stake in 'proportion to each agent's existing "stake" in the fiat monetary system' [401] (p. 6). This is rationalised through the realisation that as 'every resource can be bought or sold for money, an adversary of sufficient wealth can acquire the majority of any resource' [401] (p. 41). In order to implement this scheme, the authors rely on balance verification in the fiat banking system. The verification protocol includes several safeguards for individual and institutional byzantine failures: while the authors claim that these safeguards are comprehensive enough to provide Sybil attack resistance comparable to PoW, the risk of byzantine failures at the institutional level, and the catastrophic results such failure might have, prompts us to classify the protocol as one providing limited Sybil attack resistance.

Appendix D.173. Proof-of-Behavior [287]

Proof-of-Behavior is an overlay of a conventional PoS consensus mechanism, meaning, a Proof-of-Behavior system would be initialised with stake according to the cryptocurrency holdings of participants. Subsequently, the positive behaviour of participants according to the protocol is rewarded via stake accrual. Assuming appropriate parameters for the behaviour function, the proposed mechanism can deliver strong Sybil attack resistance.

Appendix D.174. Proof-of-Behaviour [229]

Proof-of-Behaviour is proposed with the goal of avoiding the computational cost of PoW and, instead, providing opportunities to create new blocks and receive rewards for proving positive behaviour. However, the spoofability of the proofs is highly concerning. Sybil attack resistance would only be provided in scenarios in which these are not spoofable and objectively verifiable. This, however, seems unlikely to be achievable for the very broad range of endorsed activities (i.e., 'doing some concrete actions in the real world' [229] (p. 23:3)). Therefore, unless the proof scheme, which is not detailed in the paper, provides Sybil attack resistance, the system cannot provide Sybil attack resistance.

Appendix D.175. Proof-of-Belief [230]

This scheme applies the principles of tacit coordination games to blockchain consensus in order to create a self-governing system. In contrast to PoW or PoS, this 'proof of belief' system would reward those who have contributed to the system's development. Additionally, normative consensus is to be achieved by payments made by voters in support of or opposition to particular blocks, rather than through voting alone. Through this incentive-based system, it is hoped that the mechanism will yield more adaptive and resilient public blockchain systems. The Sybil attack resistance properties of the proposed system cannot be determined unambiguously without further analysis, even though claims are made that the system would be secure against such attacks.

Appendix D.176. Proof-of-Bid [231]

Proof-of-Bid centres on using Bitcoin blocks as hard-to-forge external sources of randomness. To qualify to participate in a lottery determining a leader, anyone who funds a given Bitcoin address can place a bid for participation. Following this declaration, an applicant with a winning bid will be selected randomly as the leader. To deter repeat participation, addresses that have participated previously will have decreased odds of winning: this process can be considered a simple reputation system. While this protocol achieves some Sybil attack resistance, attackers can, relatively easily, generate addresses to participate in the lottery, thereby creating Sybils.

Appendix D.177. Proof-of-Burn [148]

Proof-of-Burn relies on the simple principle of requiring leaders to exhibit proof that they have incurred an expense by sending cryptocurrency to an inaccessible address, thereby rendering it unspendable. Most commonly, this approach is used in conjunction with proof-of-work mining to decouple the creation of cryptocurrency from its application to obtain leadership privileges. The Sybil attack resistance properties of this algorithm are comparable to those of common PoW schemes not relying on Proof-of-Burn.

Appendix D.178. Proof-of-Business [232]

In this mechanism for permissioned systems, a reputation system based on user activity (measured by payments and rewards) is proposed. This method, while potentially effective in a permissioned setting, would suffer from issues such as wash trading in permissionless scenarios. Therefore, no Sybil attack resistance is provided by it.

Appendix D.179. Proof-of-Communication [360]

Proof-of-Communication is a consensus mechanism that builds on a graph-based reputation system in which users that communicate extensively (i.e., issue numerous transactions with different targets) are preferred. This approach, however, does not exhibit Sybil attack resistance, as an attacker may create a large subgraph of Sybil identities to improve their chance of being selected for block creation.

Appendix D.180. Proof-of-Context [165]

Proofs-of-context are simple sets of cryptographically signed messages that indicate agreement by the signers that they have been in geographic proximity of the proof holder. While this technique can be effective to detect byzantine behaviour in an environment in which Sybils are absent, it does not exhibit Sybil attack resistance as attacks may create an arbitrary number of Sybil signers.

Appendix D.181. Proof-of-Contribution [233]

In this consensus mechanism sketch, a reputation system is proposed which endorses participants that make 'contributions to the community' [233] (p. 70). It is unclear how these contributions can be encoded in a digital and unspoofable form and the authors suggest that centralised surveillance technology could be used to achieve this. This ethically concerning approach, however, requires a permissioned system and, thus, does not provide Sybil attack resistance.

Appendix D.182. Proof-of-Credit [261]

This reputation system resembles PoS in that it assigns 'credit', a currency that determines the likelihood of being selected as leader, to individual nodes. It can be differentiated from similar proposals by its punitive nature: instead of rewarding participants for correct behaviour, those that behave incorrectly get penalised. The penalty is then rewarded to those that report the incorrect behaviour. This produces a strongly Sybil attack resistance scheme but comes with the downside of maintaining a fixed initial set of validators over

the lifetime of the system under the assumption that these remain honest. This renders the proposal quasi-permissioned.

Appendix D.183. Proof-of-Discrete Logarithm [234]

Huang et al. [234] propose an alternative PoW, in which computations on discrete logarithms in smooth-order groups are conducted. As such the proposed scheme offers comparable Sybil attack resistance characteristics to other PoW schemes.

Appendix D.184. Proof-of-Equivalence [165]

Proof-of-Equivalence is a protocol to establish the equivalence of a set of blocks of transactions in monetary terms. Using a reputation system that benefits users that have historically earned high fees for their participation in the protocol, trustworthy leaders are selected. This PoS-like approach provides similar Sybil attack resistance properties to other PoS protocols.

Appendix D.185. Proof-of-Human-Engagement [235]

Similar to the proof-of-human-work algorithm (see Appendix D.186), proof-of-human-engagement relies on participants solving automatically generated, Captcha-like, challenges. However, in contrast to proof-of-human-work, the proposed scheme creates challenges with only a small number of potential solutions. Therefore, Sybil attacks may be possible if an attacker creates a number of Sybils far exceeding the number of human users.

Appendix D.186. Proof-of-Human-Work [236]

In Proof-of-Human-Work, participation in consensus entails solving computer-generated challenges. Such challenges, while being automatically generated, are difficult for computers to solve, but easily solvable by humans. Therefore, human effort is required in order to qualify as a miner. This approach is strongly Sybil attack resistant under the assumption that generated challenges remain hard to solve for computers.

Appendix D.187. Proof-of-Importance [150]

Proof-of-importance is a PoS-like consensus mechanism. In addition to stake, it also factors in account activity to determine which nodes are eligible to act as leaders. The Sybil attack resistance properties can be considered roughly identical to PoS, despite the risk of the account activity metric being attacked through wash trading.

Appendix D.188. Proof-of-Interaction [237]

Minimising the energy required to achieve Sybil resistance is a key concern for many novel protocols such as Proof-of-Interaction, proposed by Abegg et al. [237], in which nodes are required to sequentially gather signatures from a subset of the entire network to participate. While such an approach in itself is not Sybil attack resistant, Abegg et al. [237] also propose an extension of Proof-of-Interaction in which participants are required to stake 'money' to entitle for participation, thereby approximating a PoS approach.

Appendix D.189. Proof-of-Location [166]

Proof-of-Location constitutes a PoS approach in which participants accumulate stake by continuously providing proof of their geographic location. Amoretti et al. [166] put some thought into Sybil attacks on the Proof-of-Location protocol and conclude that uncoordinated groups of colluding peers do not pose a risk. However, it is unclear how concerted attacks of large cabals of malicious actors would affect the Sybil attack resistance of a Proof-of-Location system.

Appendix D.190. Proof-of-Lottery [238]

Proof-of-Lottery is a simple reformulation of PoS. Participants need to actively stake parts of their holdings by acquiring 'lottery tickets' that are then selected via a pseudorandom procedure. Attacks on the source of randomness aside (e.g., it might be possible for a malicious miner to withhold certain lottery ticket transactions to influence the result of the lottery), the mechanism should provide Sybil attack resistance identical to common PoS protocols.

Appendix D.191. Proof-of-Lucky-Id [361]

PoL is a pseurandomisation scheme consisting of two phases: 'Omikuji' and 'Draw': 'Omikuji' is a random ID generation process and 'Draw' is a pseudorandom selection process from the set of IDs. The authors propose two potential mechanisms for 'Omikuji': one based on self-generated IDs and one based on IDs generated by external identity providers. The former is vulnerable to Sybil attacks while the latter constitutes a permissioned approach.

Appendix D.192. Proof-of-Majority [362]

This consensus method for a permissioned setting constitutes a randomised turn-taking protocol that does not provide Sybil attack resistance.

Appendix D.193. Proof-of-Networking [239]

In this sketch of a consensus mechanism, Ghiro et al. [239] propose to use proof of delivering IP packets between clients of an ad-hoc network to quantify the contribution of individual nodes. This quantification could, in turn, serves as a basis for leader selection. The Sybil attack resistance of this approach is likely limited, as attackers could generate a large number of the required proofs via Sybil nodes and out-of-band communication.

Appendix D.194. Proof-of-Notarized-Work [240]

In view of the high energy consumption of PoW, Abubakar et al. [240] propose a modification of this mechanism called Proof-of-Notarized-Work (PoNW). By means of this modification, the group of those who can participate in the PoW is limited to a subgroup selected by means of a Pseudorandom number generator (PRNG). With this approach, Abubakar et al. [240] aim to achieve a compromise between the robustness of PoW and the high performance of BFT-based algorithms. However, since random selection cannot prevent attacks in the face of very large numbers of Sybil identities, PoNW only provides limited Sybil attack resistance.

Appendix D.195. Proof-of-Participation [241]

Proof-of-Participation is a consensus protocol that utilises Proof-of-Work mining in combination with Proof-of-Stake validation. To qualify for mining, participants stake cryptocurrency. Thereby they enter a mining pool with artificially low difficulty. Other problems with low-difficulty PoW protocols, such as the increased risk of forks, aside, the protocol can be considered to provide strong Sybil attack resistance.

Appendix D.196. Proof-of-Participation-and-Fees [363]

Proof-of-Participation-and-Fees (PoPF), as aptly summarised in the name, constitutes a reputation system. More precisely this system uses a composite rating based on 'participation' (the frequency of a node acting as a miner) and 'fees' (the transaction fees a user has paid). A mature system set up like this might provide significant Sybil attack resistance, but doubt remains: wash trading (bogus transactions with the goal of generating fees for a higher rating), as well as the self-perpetuating nature of the participation score, could enable well-orchestrated Sybil attacks.

Appendix D.197. Proof-of-Phone [421]

The authors of this scheme propose the introduction of 'Authenticated Mining Units', purpose-built trusted hardware modules to operate in smartphones. Since mechanical engineering challenges, like the trustworthiness of device attestation, are not discussed in the paper, no assessment of Sybil attack resistance can be made.

Appendix D.198. Proof-of-Points [242]

The proposed PoP protocol resembles a collaborative PoW system in which participants can co-create location proofs. LPs are generated using nearby devices as witnesses while protecting collusion attacks through a traceable-detectable-prefix scheme that preserves user privacy. However, as a protocol for a permissioned system, a semi-trusted party is still needed to admit users into the network.

Appendix D.199. Proof-of-Prestige [288]

In this consensus mechanism a reputation based on 'prestige', a quantification of the useful work a participant has performed, is introduced. 'Prestige' can be gained from others, but it also replenishes over time. It can be assumed that the Sybil attack resistance properties are similar to other PoS schemes.

Appendix D.200. Proof-of-Probability [422]

In proof-of-probability transaction proposers subject miners to unnecessary work. Thereby, they create a PoW on the transaction level, instead of on the protocol/block level. The Sybil attack resistance class cannot be trivially determined due to the perceived high risk of forks stemming from the low-difficulty PoW mechanism.

Appendix D.201. Proof-of-Queue [156]

The proof-of-queue protocol is designed for permissioned blockchains. It extends PoET's lottery technique by a random selection procedure in which every node has an equal chance of becoming the leader. As such, the Sybil attack resistance properties are quite strong. Sybil attacks could, however, still be conceivably conducted by attackers that are in control of a large number of SGX devices.

Appendix D.202. Proof-of-Replicated-Storage [289]

Proof-of-Replicated-Storage is an implementation of a Proof-of-Replicated-Storage (PoRep) protocol that 'provably resists Sybil attacks' [289] (p. 357). It achieves Sybil attack resistance by allowing the prover to defend a claim that unique storage resources are dedicated to a given data file.

Appendix D.203. Proof-of-Reproducibility [290]

In the work of Al-Mamun et al. [290], a PoW phase is combined with a PoS phase, using node age as stake. This provides the same Sybil resistance properties as conventional PoW.

Appendix D.204. Proof-of-Reputation [364]

In Proof-of-Reputation (PoR) a reputation system based on 'trust value' is applied. The authors acknowledge that this approach is susceptible to Sybil behaviour and coin the term 'newcomer attack' for a reputation attack by a Sybil entity. They address this issue by requiring a central admissions process to the ledger.

Appendix D.205. Proof-of-Reputation with Nakamoto Fallback [291]

In the first layer of this PoR/PoS hybrid, a reputation system based on mutual ratings is introduced. Kleinrock et al. [291] recognise that this approach alone might be attackable and lead to undesirable results (such as Sybil attacks), therefore, they introduce a second

consensus layer: this layer uses PoS, which can be considered to provide strong Sybil attack resistance.

Appendix D.206. Proof-of-Review [243]

PoR is a PoS-like mechanism in which stake is accumulated by successfully providing input in the form of reviews. Central entities, or bookmakers, are determined by a committee. It is not clear, how the committee is formed, therefore, it is unclear whether the proposal targets permissioned or permissionless systems. In a permissionless case, it can be assumed that no Sybil attack resistance is provided by the protocol due to the possibility of attackers creating large numbers of fake reviews.

Appendix D.207. Proof-of-Review [402]

Proof-of-Review constitutes a simple multidirectional reputation system in which the likelihood of being selected as 'nominated round leader' depends on the ratings received from peers. While this approach might protect against trivial Sybil attacks, Sybil attack resistance against more complex attacks in which a malicious user executes a complex program in which Sybils are rated highly is not provided.

Appendix D.208. Proof-of-Sovereignty [365]

Proof-of-Sovereignty (PoSv) is a PoA-like protocol in which a central authority, the 'Digital Asset Reserve-Organisation' can assign signing keys to individual miners. As a permissioned approach, PoSv does not provide Sybil attack resistance.

Appendix D.209. Proof-of-Space [147]

In their 2015 paper, Dziembowski et al. [147] put forward the concept of Proof-of-Space that entails that a prospective miner dedicates 'a significant amount of disk space as opposed to computation' [147] (p. 585). The mechanism employs graph pebbling, a concept that can be used 'to establish tradeoffs between time and space required for arithmetic expression evaluation' [641] (p. 24). It can be assumed that Proof of Space provides similar Sybil attack resistance characteristics when compared to PoW under the assumption that the acquisition of storage space follows similar economic patterns as the acquisition of CPU cycles.

Appendix D.210. Proof-of-Spending [244]

Liu [244] propose a variety of proof-of-spending protocols, all based on the principle that spending cryptocurrency increases the likelihood of being selected as a miner. This approach can be effective against small-scale Sybil attacks but might be limited in light of complex attacks in which large cabals of attackers perform wash trading to increase the likelihood of being selected as leaders.

Appendix D.211. Proof-of-Stack [366]

In proof-of-stack, nodes place bets on other nodes. Depending on their betting strategy (i.e., which nodes they are betting on) and other's strategies, nodes are assigned a weight: higher weights increase the likelihood of being selected. However, proof-of-stack needs to rely on centralised access control to the network, using a 'coordinator', thus rendering it permissioned.

Appendix D.212. Proof-of-Stake [143]

Similar to PoW, the concept of this consensus mechanism originated in Bitcoin circles. It was proposed as an alternative to PoW where, instead of investing computational effort into solving a mining competition, block creation rights would be awarded to participants proportional to their cryptocurrency holdings and rewards would be provided to those who

create new blocks. Albeit criticised for a 'rich getting richer' [638] effect, this mechanism provides strong Sybil attack resistance.

Appendix D.213. Proof-of-Stake for Bitcoin Subchains [245]

The consensus protocol proposed by Bartoletti et al. [245] introduces PoS mechanics to sidechains, or 'subchains', of the Bitcoin blockchain. 'Meta-nodes' receive messages for inclusion on the subchain by other participants and are rewarded with transaction fees. These fees subsequently contribute to stake, informing the likelihood of a given node being selected. The mechanism can be considered strongly Sybil attack resistant as it applies common PoS mechanics.

Appendix D.214. Proof-of-Stake with Time Staking [403]

Burmaka et al. [403] propose a modification to PoS in which the time a node is present on a network serves as stake. To avoid attackers accumulating stake, modular arithmetic is introduced. However, this approach only provides very weak Sybil attack resistance as attackers with the powers to create large numbers of Sybils will accumulate significant stake regardless.

Appendix D.215. Proof-of-Strategy [246]

The blockchain-based crowdsourcing system proposed by Cai et al. [246] essentially presents itself as an inflationary PoS system, in which block rewards ('S-coins') are distributed that allow participants to build up stake. These can be exchanged for reputation tokens ('R-coins') that form the basic unit in the reputation system by those that want to act as verifiers on the system. Due to the inflationary PoS nature, the systems proposed have the same strong Sybil attack resistance that other PoS systems provide.

Appendix D.216. Proof-of-Trust [367]

PoT combines hybrid public/private blockchain technology with a reputation system. Due to the permissioned nature of the base consortium, the overall mechanism does not require measures to achieve Sybil attack resistance. This is justified by the authors who state that Sybil attacks on the protocol are very unlikely due to an expected re-evaluation by the consortium.

Appendix D.217. Proof-of-Trust [404,405]

Proof-of-Trust uses a decentralised reputation system at the core of the protocol. Using this reputation system, participants can assign trust values to each other. The cumulative trust of a node then determines the difficulty of a PoW puzzle a miner has to solve in order to mine a subsequent block. The difficulty will be adjusted inversely proportionally to its trust value. This combination of mechanisms provides limited Sybil attack resistance as an attacker might be able to inflate their score in the system, thereby gaining disproportional influence. This is despite measures like 'trust decay' in which trust values deteriorate over time.

Appendix D.218. Proof-of-Trusted-Execution-Environment-Stake [157]

In this protocol, principles of PoS are combined with TEE by assigning randomized and stake-dependent timeouts to all active validators. Thereby, the selection is limited to stakeholders who own a TEE device. This yields similar properties to regular PoS, while offering additional robustness in light of 'Nothing at Stake' and 'Grinding' attacks. The Sybil attack resistance class is comparable to regular PoS.

Appendix D.219. Proof-of-Unique-Human [406]

In this proposed scheme, the biometric data of potential leaders is linked with a unique user identifier on-ledger. The scheme then proposes a reputation system to which

a peer review of biometric data is essential: those participants that have their biometric information validated by others in the real world gain reputation. The numerous ethical challenges aside, this approach is susceptible to Sybil attacks conducted by attackers that generate bogus verification events.

Appendix D.220. Proof-of-Validation [247]

LightChain is a blockchain protocol for resource-constrained environments that sets out to provide integrity even under corruption of the majority of peers. It does, however, not provide any mechanism to prevent an influx of Sybil identities and can, therefore, not be considered Sybil attack resistance.

Appendix D.221. Proof-of-Verifying [175]

This centralised protocol assumes the existence of a 'global trust authority' that admits nodes to the permissioned system. These nodes can then acquire cryptocurrency from a central stablecoin issuer and, ultimately, stake this currency for mining permissions. As this permissioned protocol leans heavily on centralisation for access control, no Sybil attack resistance is provided.

Appendix D.222. Proof-of-Vote [368,369]

In this permissioned proposal, the main entities, or 'comissioners', maintain the consortium blockchain system together. They promote and demote worker nodes, or 'butlers'. As a permissioned system, this approach does not provide Sybil attack resistance.

Appendix D.223. Proof-of-Win [370]

In this mechanism for permissioned systems, individual nodes can participate in simple binary competitions amongst each other with the winning player becoming eligible for mining. The mechanism is designed for permissioned systems and does not provide Sybil attack resistance.

Appendix D.224. Proof-of-Work [1,142]

This early consensus mechanism, going back to work by Dwork and Naor [142] is applied in the Bitcoin cryptocurrency [1] as follows: in PoW miners compete to solve a cryptographical puzzle. The miner who proves to solve the puzzle earns the right to create a new block, thereby earning rewards and fees paid by others. The strong Sybil attack resistance properties of the algorithm have been tested over time with Bitcoin being operational for over a decade without major compromising incidents.

Appendix D.225. Proof-of-Work Applied to the Clique Problem [292]

In this minor modification of PoW, miners are required to find the largest clique in a big graph. This approach is presented as an alternative to the Bitcoin PoW scheme that incentivises both the utilisation of computing power and memory by miners. The Sybil attack resistance properties are identical to those of Bitcoin PoW.

Appendix D.226. Proof-of-Work Based on Analog Hamiltonian [293]

Kalinin and Berloff [293] propose a low-difficulty PoW scheme based on analog Hamiltonian optimisers. While it is unclear whether lowering the difficulty would result in the dramatic performance improvements suggested by the authors, it can be assumed that the proposed scheme would deliver strong Sybil attack resistance under the assumption of an appropriate adaption of difficulty.

Appendix D.227. Proof-of-Work on the Inflation Propensity of Collatz Orbits [294]

Bocart [294] propose an alternative to the Hashcash utilised in Bitcoin PoW. As such it provides the same Sybil attack resistance properties.

Appendix D.228. Proof-of-Work-or-Knowledge [423]

Proof-of-Work-or-Knowledge (PoWorK) allows participants to provide a PoW or, alternatively, 'knowledge of a witness to a public statement'. Whether this approach can provide Sybil attack resistance depends on the source of knowledge. Should this be derived from a strongly Sybil attack-resistant source (e.g., a PoS blockchain), the overall protocol could be considered strongly Sybil attack resistant. Where it is derived from a weaker source, this would not be the case.

Appendix D.229. Proteus [371,372]

In this BFT protocol, a subset of nodes is selected as a leadership committee. It does not provide Sybil attack resistance.

Appendix D.230. Raft [151]

Raft is a consensus mechanism created with the goal of easy understanding. It is similar to Paxos in terms of fault tolerance and performance, but it is decomposed into more manageable subproblems. Raft outlines all major components needed for practical implementation. Raft does not provide Sybil attack resistance and needs to be combined with an appropriate scheme to achieve Sybil attack resistance if deployed to a permissionless environment.

Appendix D.231. Randition [373]

Randition is a Tendermint variant that improves upon system performance by sharding. This is done by implementing Algorand's cryptographic sortition algorithm to allow for safe and autonomous sharding. The proposed algorithm is only safe under the assumption of 100 % consensus amongst validators, which is met in a permissioned or private blockchain environment. It does, however, not provide Sybil attack resistance.

Appendix D.232. Random Leader Selection Ba000sed on Credit Value [374]

In this consensus mechanism, a simple reputation system based on 'credit value', a measure of trustworthiness that can only be 'obtained through honesty [*sic*] behavior' [374] (p. 89), is introduced. The system is intended for permissioned systems and is, therefore, not designed for Sybil attack resistance.

Appendix D.233. Randomization to PoW [248]

This modification to Nakamoto-style PoW entails the combination of a difficulty limitation and a pseudorandom miner selection process. Since miners are selected from a pool of IDs, the proposed approach is highly vulnerable to Sybil attacks and potentially other attacks.

Appendix D.234. Rationality-Proof Consensus [158]

Rationality-proof consensus combines a simple round-robin leader selection strategy with hardware features to help prevent Sybil attacks. Furthermore, prospective block producers need to submit a deposit to be considered for leader selection, which is forfeited if they act maliciously. The protocol provides Sybil attack resistance only under the assumption that an attacker cannot obtain access to a large number of hardware devices.

Appendix D.235. Regulated Bitcoin (RBitcoin) [249]

With RBitcoin Ahuja et al. [249] propose an addition to the Bitcoin protocol that would allow miners to add evidence of their regulatory license to a Coinbase transaction. This would allow asset holders to only transact via blocks mined by an entity with a regulatory license. Subsequently, by only taking the history of those blocks into account, a 'longest legal branch' of asset transactions could be formed. This would effectively form an inner network (group of miners with regulatory accreditation) within a wider permissionless

network (Bitcoin). Therefore, the inner network with regulatory endorsement needs to be considered permissioned.

Appendix D.236. Reputation-Based BFT [375]

A credit score between 0.1 and 1 is introduced as an approximation for a node's 'degree of credibility'. Based on this credit score, nodes on a network receive different permissions (i.e., leader, follow [*sic*], and checkpoint). Nodes receive an increase in credit score for adhering to the protocol rules (e.g., for validating block contents). Such a simple reputation system deployed to a permissionless environment would be vulnerable to Sybil attacks from adversaries that build a positive reputation before attacking. Since the algorithm is designed for a 'federated chain system', i.e., a permissioned system, this problem does, however, not manifest.

Appendix D.237. Reputation Based Hybrid Consensus [250]

The authors propose a reputation system-backed consensus mechanism that aims to improve trustworthiness and efficiency in e-commerce blockchain systems. A node's reputation is calculated based on past performance. Nodes then engage in a two-stage PoW process to mine 'microblocks' and, subsequently, regular blocks. Various difficulty adjustment functions are used in each stage to account for the varying sizes of blocks. Known issues with low-difficulty schemes (e.g., risk of forks) aside, the system can be considered to provide Sybil attack resistance comparable to common PoW schemes.

Appendix D.238. Reputation Consensus [407]

Reputation Consensus (ReCon) introduces a reputation-based consensus mechanism, initialised via an external reputation source. After initialisation, trust values for individual participants are updated on a per-block basis with the goal of capturing the likelihood of malice of a participant. While, according to the authors, this mechanism can withstand more than $1/2$ malicious actors, it can not be considered strongly Sybil attack resistant as no technique to limit the influx of malicious actors onto the system is proposed and a powerful attacker might be able to maintain more than $1/2$ of nodes on a network if only negligible cost is associated with creating them.

Appendix D.239. Reputation-Based Byzantine Fault Tolerance [376]

In this BFT mechanism, a reputation system is introduced using a numeric 'reputation value' to express the adherence of participants to the protocol. While this approach may be effective for simple Sybild attacks, its ability to provide Sybil attack resistance for complex and well-orchestrated Sybil attacks needs to be doubted as an attacker may be able to build a reputation on Sybil accounts before attacking.

Appendix D.240. Reverse Hash Chain [408]

Kim and Lee [408] propose to utilise Reverse Hash Chains (RHCs) as a low-difficulty PoW scheme for smart home environments. As with other PoW schemes with artificially low difficulty, the Sybil attack resistance properties are difficult to reason about as, under high volume, a large number of forks would be expected from such a system.

Appendix D.241. Rift [377]

Rift constitutes a complex, multi-level permissioning scheme for consortium systems. Its complexities stem from an effort to replicate hierarchies that are found in common compliance processes. As a permissioned protocol, it does not provide Sybil attack resistance but relies on a central point of authentication.

Appendix D.242. Robust Byzantine Agreement [336]

This BFT protocol provides partition resilience and tolerates up to 1/3 corruptions. In contrast to Hybrid Byzantine Agreement (HBA) it achieves 'strongly fair validity', meaning any participant has a reasonably high probability of being chosen as leader. As a protocol for a permissioned environment, it does not provide Sybil attack resistance.

Appendix D.243. Robust Proof-of-Stake [295]

Li et al. [295] introduce the concept of 'dynamic coin age' to minimise the group of eligible leaders. This is done with the goal of reducing the risk of coin age accumulation attacks. The Sybil attack resistance properties of the proposed algorithm are comparable to those of conventional PoS algorithms.

Appendix D.244. Rock-Scissors-Paper [176]

Rock-Scissors-Paper (RSP) is a PoS/PoW hybrid with individual difficulty adjustment. To participate in leader selection, participants stake a fixed proportion of their holdings (i.e., 5 %). Thereby, they entitle to submit their device specifications. Based on these, they can participate in a difficulty-adjusted PoW. This approach, however, is highly susceptible to Sybil attacks, as malicious users might create multiple accounts with limited funds and, from these, create multiple accounts with low specifications, thereby inflating the chances of being selected as leader.

Appendix D.245. Roll-DPoS [251]

The Roll-DPoS protocol is bootstrapped using the Ethereum blockchain: Ethereum request for comment (ERC)-20 wallet holders can elect to back a single block producer by 'pledging backing'. The amount of currency they hold at a provided cut-off time will then enforce the weight of the backing stake. Here, funds on Ethereum act as stake, thereby inheriting from the Sybil attack resistance properties of the Ethereum blockchain.

Appendix D.246. Rollerchain [252]

Chepurnoy et al. [252] introduce a modification to common PoW schemes that allows nodes to conduct 'pruning', i.e., the removal of full blocks not needed for mining from the transaction history. This is done with the goal of reducing storage requirements but has no influence on Sybil attack resistance properties, which remain comparable to conventional PoW schemes.

Appendix D.247. Rotating Multiple Random Sampling [378]

In this protocol, designed for permissioned settings, miners, or, 'master nodes' are randomly selected, thus requiring a Sybil-free environment.

Appendix D.248. Saguaro [379]

Saguaro closely resembles Sharding Permissioned Blockchains Over Network Clusters (SharPer) in that it supports multi-level pluggable consensus for permissioned systems. As such, the protocol is not designed to provide Sybil attack resistance.

Appendix D.249. Satellite-Aided Consensus [141]

This mechanism targets the astronautics domain, specifically, geostationary earth orbit satellites. It constitutes a permissionless consensus protocol for space-terrestrial blockchains. Sybil attack resistance in the protocol is achieved through random oracles and a principle similar to PoS.

Appendix D.250. Scalable Byzantine Fault Tolerance [380]

Scalable Byzantine Fault Tolerance (SBFT) is positioned as a protocol that combines multiple improvements over conventional PBFT, thereby making the former more perfor-

mant in terms of throughput and latency than the latter. The main contribution is the move away from a peer-to-peer topology to a star topology. Sybil attack resistance is not a design consideration of the protocol which is, therefore, appropriate in permissioned settings only.

Appendix D.251. Scalable Hierarchical Byzantine Fault Tolerance [381]

In Scalable Hierarchical Byzantine Fault Tolerance (SHBFT) nodes are allocated to the 'primary net layer' or one of multiple 'secondary net layers'. Some nodes, namely 'secondary nodes' communicate across layer boundaries. As a mechanism for permissioned networks, no Sybil attack resistance capabilities are provided.

Appendix D.252. Scalable Network-Coded PBFT [382]

In this framework for PBFT consensus in permissioned networks, two main optimisations to PBFT are proposed: effective sharding of nodes on a PBFT system and reducing the maximum required bandwidth between them. As a PBFT protocol, Sybil attack resistance has not been given consideration.

Appendix D.253. Scalable Practical Byzantine Fault Tolerance with Short-Lived Signature Schemes [383]

To minimise the time necessary for signature validation in PBFT, Fan [383] proposes a blockchain-based key-sharing scheme to distribute and rotate short-length cryptographic keys. While this has shown to improve the performance of PBFT, Sybil attack resistance is not a concern of the protocol, as it assumes a permissioned setting.

Appendix D.254. Score Voting-Based BFT Consensus [384]

The basis of this consensus mechanism is a multi-dimensional reputation system which considers some fixed factors (e.g., hardware configuration) and behavioural parameters (i.e., the adherence to the mechanism). The reputation of the node determines whether it can act as a leader or not. All nodes that exceed a reputational threshold qualify for leader election. This approach is designed for a permissioned system and does not provide Sybil attack resistance.

Appendix D.255. Secure and Scalable Hybrid Consensus [424]

SSHC sets out to provide a secure and scalable hybrid consensus for sharding blockchains. It proposes a fair sharding selection scheme, selecting committee members in each shard. A PoW selection process is applied to allow new nodes to join while minimising the risk of Sybil entities joining the network. It is, however, not clear how the sporadic use of PoW affects Sybil attack resistance.

Appendix D.256. Security-Aware Genetic Algorithm Based Practical Byzantine fault Tolerance [385]

Security-Aware Genetic Algorithm based Practical Byzantine fault Tolerance (SAGA-PBFT) proposes some modifications to PBFT with the goal of achieving better performance as measured by transaction commit times. As a permissioned protocol, its Sybil attack resistance is comparable to common PBFT implementations.

Appendix D.257. Self-Stabilizing Byzantine Consensus [386]

Binun et al. [386] propose an improvement to BFT-SMaRT that prevents a situation in which the BFT consensus algorithm implementation could deadlock. The improvement does, however, not impact Sybil attack resistance of this algorithm intended for permissioned systems.

Appendix D.258. Semada Proof-of-Reputation [253]

Semada Proof-of-Reputation, alternatively titled 'Anchor Protocol' by the authors, constitutes a simple PoS-like reputation system. Here, 'reputation scores' quantify the likelihood of a user being selected as a miner. Reputation can be accumulated by siding with the majority of other miners on the platform. This approach provides some Sybil attack resistance but is still vulnerable to well-orchestrated attacks that introduce Sybil identities that, initially, adhere to the protocol and only conduct an attack after maturing.

Appendix D.259. Separate-Proof-of-Deep-Learning [387]

S-PoDL is a proof of useful work mechanism in which miners work on deep-learning models to generate blocks. Training data sets are released in stages and the models with the highest accuracy are used to generate blocks. Test datasets are used to validate proposed models. This allows for more efficient use of resources, as well as improved security and privacy. This approach requires central orchestration via full nodes that evaluate and validate proposed models. Therefore, the proposed algorithm can only be effective in a permissioned setting where all full nodes can be trusted.

Appendix D.260. Service-Zone-Based Hierarchical Consensus [296]

In this PoW-based sharding protocol, participants are assigned to 'service-zone consensus groups' with the goal of improving throughput and latency. During the formation of consensus groups, PoW and VRF are employed to achieve Sybil attack resistance. Depending on the parameters of PoW, Sybil attack resistance can be considered strong.

Appendix D.261. Sharding Permissioned Blockchains Over Network Clusters [388]

Similar to CAPER, SharPer constitutes a framework to apply existing consensus protocols in a layered fashion: SharPer distinguishes between intra-shard consensus and cross-shard consensus in order to improve scalability. It is intended for permissioned blockchains and therefore does not consider Sybil attacks an attack vector.

Appendix D.262. SklCoin [297]

SklCoin uses PoS mechanics to determine a consensus group to generate a collective block signature. The mechanism provides Sybil attack resistance characteristics that are comparable to those of other common PoS schemes.

Appendix D.263. Software Guard Extension-Enabled Decentralized Intrusion Detection Framework [254]

This consensus mechanism is designed to improve the decentralisation and efficiency of existing protocols. Its key idea is that a history of participating in block creation influences the difficulty of future participation. This limits the number of potential leaders to a smaller set which is designed to improve the efficiency of the network. However, Sybil attack resistance is not addressed. It is conceivable that an attacker might create a large number of identities to influence the outcome of the selection process.

Appendix D.264. Solida [255]

Abraham et al. [255] propose a Byzantine consensus in which at any given time, a single committee member serves as the leader, combining a batch of transactions for inclusion into the ledger. PoW is applied as a Sybil-attack resistance scheme, meaning participants have to solve a computational puzzle to qualify as leaders.

Appendix D.265. Staked IP-Address Selection [161]

In this protocol, IP addresses controlled serve as stake metric. Using an external source of randomness, a miner IP address is selected, thereby making it more likely for those that own more IP addresses to gain miner privileges. This approach in itself presents an

Sybil attack vector, as attackers may be able to gain access to larger IP blocks to conduct Sybil attacks. Therefore, only limited Sybil attack resistance is provided by this approach.

Appendix D.266. Streamlet [389]

Streamlet is a simple, permissioned, consensus protocol for pedagogy. Here, an epoch leader is determined who proposes a new block on which all other participants subsequently vote. As a permissioned protocol, Streamlet provides no Sybil attack resistance.

Appendix D.267. Sybil Tolerant Equality Protocol [177]

This consensus mechanism incentivises nodes to validate blocks by providing rewards for nodes that act honestly and punishing those that don't. Sybil attack resistance is central to the proposal with two mechanisms standing out. First, any new node incurs a fee to join the network. Second, a reputation system exists that aligns rewards with a node's past behaviour. While these measures can likely deter Sybil attacks in mature networks, complex attacks on smaller networks may still be successful due to the constant cost of creating a Sybil identity.

Appendix D.268. Sybil-Proof Wireless Network Coordinate Based Byzantine Consensus [167]

The Sybil attack resistance mechanics of Sybil-Proof Wireless Network Coordinate Based Byzantine Consensus (SENATE) are designed with the intuition that Sybil identities are likely to occur in close geographic proximity (to the attacker). To prevent such attacks, Jiang et al. [167] propose to geographically partition the space in which users of the system are active, and achieve meta-consensus from the results of the subgroups. While this approach may be effective against small-scale Sybil attacks, those attackers that have the means to deploy Sybil nodes in a geographically dispersed fashion would still be successful.

Appendix D.269. Thinkey [256]

Thinkey employs PoS as part of the committee selection phase of its protocol, thereby providing strong Sybil attack resistance. Committees then form layer-2 networks, or 'transaction chains', which act as shards for system-wide workloads.

Appendix D.270. Time-Memory-Data Trade-Off [257]

TMD-TO describes a consensus protocol which allows a player to choose the resources they want to spend on solving a PoW puzzle. This is in contrast to pure PoW and Proof-of-Space, which require energy or space, respectively. The goal of this approach is to offer flexibility by accommodating trade-offs between these resources, thereby allowing for a smaller total expenditure. The Sybil attack resistance properties can be considered comparable to that of pure PoW and Proof-of-Space.

Appendix D.271. Token Age Based Consensus [258]

The proposed consensus protocol utilises a reputation system based on 'reputation tokens' which are assigned according to interactions with others. A token age function is introduced that incentivizes active participation in the network by assigning a higher weight to those who have been participating for longer periods of time. Qualifying nodes (i.e., those with sufficient balances and token ages) are selected through an unspecified process. Similar to other P2P reputation systems, basic Sybil attacks may be averted but the Sybil attack resistance under orchestrated attacks is questionable.

Appendix D.272. Torneo [259]

The Torneo consensus mechanism is based on Proof of Luck. In this scheme for permissioned networks, each node generates a random number and notifies the other nodes. The winning node is chosen at random and can add the next block to the chain.

Therefore, the scheme relies on a fixed number of potential leaders and is not resistant to Sybil attacks.

Appendix D.273. Trust Consensus Protocol [409]

The proposed Trust-CP mechanism relies on a reputation system that quantifies activities like participation in community tasks and experience ratings to determine the likelihood of being selected as a leader. As common in reputation-based protocols, nodes that malfunction are to be rated poorly and should be removed from the system. Such a reputation-based approach can be effective for small-scale Sybil attacks but is unlikely to prevent well-orchestrated ones, executed by attackers with perfect knowledge of the protocol.

Appendix D.274. Twice Verifications and Consensuses of Blockchain [410,411]

Twice Verifications and Consensuses of Blockchain (TCNS) makes use of a reputation-based consensus mechanism based on a measure called 'reputation degree'. This measure is calculated based on a participant's history of delivering useful work. As such the protocol achieves Sybil attack resistance but might be vulnerable to more concerted Sybil attacks.

Appendix D.275. Two-Tier Voting System Architecture [390]

In the proposed two-layer architecture a permissionless layer using an appropriate consensus mechanism (e.g., PoW or PoS) is combined with a permissioned layer that runs a PBFT consensus mechanism. The authors propose different roles for the different layers (e.g., only the inner layer might perform destructive operations). Due to the weak Sybil attack resistance properties of the inner permissioned system, the compound system is considered to have equally limited Sybil attack resistance.

Appendix D.276. uMine [391]

In this Proof of Human-Work scheme, a static consortium of 'captcha generators' is proposed. These would create challenges that are deemed to only be solvable by humans. Since this approach demands a permissioned system with trusted generators, no Sybil attack resistance is provided.

Appendix D.277. Unitary Interchain Network [392]

In the sketched algorithm for a multichain protocol, participants can increase the likelihood of becoming miners by volunteering as oracles for adjacent blockchains. This brings the inherent risk of Sybil attacks through attackers that deploy multiple oracles that the protocol does not seem to address.

Appendix D.278. Weak Centralized Consensus Mechanism with Incentive Effects [178]

As a reaction to the perception of centralisation in DPoS, this paper proposes a consensus mechanism that has the goal of incentivising fairer leader selection. In contrast to DPoS, this mechanism uses opportunity verification and random guessing to select representatives, which is intended to provide a more fair leader selection model. Due to the random selection process, no Sybil attack resistance is provided.

Appendix D.279. Weight of Authentication Byzantine Fault Tolerance [393]

Weight of Authentication Byzantine Fault Tolerance (WBFT) is a basic BFT scheme that introduces fixed 'weights' for participants: weight 1 for unauthenticated particicpants and weight 1.5 for authenticated participants. The leader selection probability then anchors on the weight of a potential participant. This does, however, not improve the Sybil attack resistance of BFT in a meaningful way as attackers can still increase their cumulative weight dramatically when conducting Sybil attacks.

Appendix D.280. What, Where, How Much [260]

In this mechanism for permissioned systems or systems with a 'high entry threshold for new nodes' [260], where nodes are rewarded based on their participation in the protocol. As a permissioned protocol, no Sybil attack resistance is provided.

Appendix E. Description of Mechanisms for Healthcare

Appendix E.1. PoW Applied to Biomedical Image Segmentation [434]

This PoUW scheme subjects prospective miners to participation in biomedical image segmentation, a technique that is used, among others, in brain magnetic resonance imaging (MRI) and lung computerised tomography (CT) scans. This work has some beneficial properties for PoUW, such as utilising most computational power for the main task, instead of auxiliary functions. Due to the complexity of the task, a central coordinator is assumed to orchestrate the mechanism. The mechanism, therefore, does not provide Sybil attack resistance.

Appendix E.2. Deep Learning Based Consensus [435]

In this PoUW scheme, potential leaders perform useful work in the form of biomedical image segmentation tasks. Since the proposed scheme requires a trustworthy task publisher, the proposed mechanism provides no Sybil attack resistance. Especially scenarios in which task publishers and miners collude could easily be used to bring about Sybil attacks.

Appendix E.3. Lightweight Proof-of-Game [433]

This lightweight PoW scheme with very low difficulty is positioned as an algorithm suitable for resource-constraint devices in the medical domain. While it is positioned as an approach in both permissioned and permissionless settings, due to its artificially low difficulty, it can be assumed not to provide Sybil attack resistance or resistance to forks.

Appendix E.4. MedBlock [436]

In this permissioned system, a central certificate authority is responsible for admitting nodes to the network. Nodes that are admitted in such a way participate in a vote to determine a single miner, or 'endorser', for a region. This approach, suited only for permissioned networks, provides no Sybil attack resistance.

Appendix E.5. Proof of Artificial Intelligence [437]

This consensus mechanism is based on a reputation system in which multiple aspects of a miner's past performance are considered (i.e., number of blocks previously mined, percentage of 'faulty transactions', how long miners took to mine a block, or their age on the network). These factors inform the likelihood to be selected as a miner. While this approach may effectively prevent basic Sybil attacks, more complex Sybil attacks, in which attackers temporarily adhere to the protocol to boost their reputation, may not be prevented.

Appendix E.6. Proof of Policy [438]

Proof of Policy (Note that multiple algorithms named Proof of Policy [438,439] exist.) employs a centrally controlled authority to verify the identities of users. The proposed scheme is predominantly concerned with access control of healthcare data. It applies strict centralisation of participation through the use of an administrator, who manages access control lists (ACLs). No Sybil attack resistance is provided by this centralised method.

Appendix E.7. Proof of Policy [439]

Proof of Policy is a consensus mechanism for blockchain systems that verifies user access policies using attribute-based ring signatures. As common in the medical domain, the mechanism exhibits permissioned characteristics through private access control. Sybil

attack resistance is not provided by Proof of Policy as it is not a primary aim, although the mechanism could be extended to achieve this property.

Appendix E.8. Proof-of-Familiarity [440]

The proposed scheme introduces a reputation system for medical decision gathering in which 'individual qualitative achievements' of participants are encoded numerically. This is done via the 'individual familiarity index'. It is unclear if and how the medical decision-making ability influences consensus technically. Regardless, Sybil attack resistance is not provided as the proposed system is intended to be permissioned.

Appendix E.9. Proof-of-Medical-Stake [441]

PoMS is a PoS-based consensus mechanism for blockchain that encourages stakeholders to validate transactions by rewarding them with stake. The initial stake is based on the willingness of participants to share medical data, with those that share more data receiving a larger stake. Subsequently, a reputation system is employed that rewards adherence to the protocol and penalises divergence from it. As a permissioned system, it employs a central identity management system and, therefore, no Sybil attack resistance is provided.

Appendix F. Description of Mechanisms for High Performance

Appendix F.1. BFT Consensus on FPGA [448]

A further optimisation proposed by Bravo et al. [448] is to utilise field-programmable gate arrays (FPGAs) to improve response times during BFT message exchange. This optimisation is equally only applicable in permissioned settings.

Appendix F.2. BFT Consensus with SmartNIC Offloading [448]

Bravo et al. [448] propose two optimisations to BFT, for permissioned systems. In this modification serialisation of messages and line-rate hashing is offloaded to SmartNICs in a bid to accelerate BFT.

Appendix F.3. PBFT with SVM-Based Trust Evaluation [449]

In this proposal for permissioned systems, PBFT is extended by a reputation system in which a 'trust level', or 'credit value', is assigned to each potential miner node. This value subsequently evolves over time 'according to the node's behaviour in the blockchain' [449] (p. 374). As a mechanism designed for permissioned networks, no Sybil attack resistance is provided.

Appendix F.4. PoS Using Fair and Dynamic Sharding Management [444]

This meta-PoS scheme randomly assigns nodes to shards. Within the shards created, nodes conduct PoS leader election. This allows for the parallel operation of shards with sporadic synchronisation. The Sybil attack resistance properties can be assumed to be comparable to conventional, unsharded, PoS.

Appendix F.5. Autonomous and Controllable High-Performance Consensus [450]

The paper, albeit hard to follow, seems to suggest imposing a central limitation to the number of miner nodes coupled with a simple round-robin selection of those. This approach provides no Sybil attack resistance.

Appendix F.6. BEAT [451]

BEAT constitutes a set (BEAT0, BEAT1, BEAT2, BEAT3, and BEAT4) of PBFT algorithms designed for high performance in permissioned settings. The protocol family delivers higher efficiency than HoneyBadgerBFT which is the protocol the authors believe to be best-in-class. As a suite of protocols for permissioned systems, Sybil attack resistance is not a design concern for BEAT.

Appendix F.7. Bicomp [445]

Bicomp presents itself as a two-layer PoW consensus mechanism in which 'microblocks' can be mined in parallel to be then checkpointed into 'macroblocks' periodically. This is done in the interest of improving throughput performance by parallelisation. The proposed scheme can be considered to provide strong Sybil attack resistance, similar to other PoW schemes.

Appendix F.8. Blinkchain [480]

With the goal of reducing latency, in this protocol, participants are assigned to shards according to their geographic position. Limited Sybil attack resistance is provided by requiring participants to provide PoW upon joining the system. This safeguard can, however, be circumvented by an attacker ready to expend large amounts of energy.

Appendix F.9. BlockDAG [452]

Gai et al. [452] address the issue of consistency in directed acyclic graph-based systems by introducing a block concept on top of the directed acyclic graph structure. A permissioned component, or consortium blockchain, is required in the proposed system architecture, rendering it permissioned and, therefore, not Sybil attack resistance.

Appendix F.10. Checkpoint Consensus [453]

The goal of CHECO is to introduce horizontal scalability by decoupling consensus and transaction validation. Determining a leader, or 'facilitator', is essentially a pseudorandom selection from the set of all nodes: a process which does not provide Sybil attack resistance.

Appendix F.11. Concordia [454]

Concordia is a consensus mechanism for permissioned blockchain systems that relies on a gossip-based communication protocol to verify the validity of proposed transactions. The mechanism is designed with the goal of achieving high transaction throughput while ensuring security and liveness. As a BFT protocol, it does not provide Sybil attack resistance.

Appendix F.12. Consensus based on the Mortgage Model [455]

The proposed high-performance consensus mechanism is based on a 'mortgage model' that brings with it a voting process to elect a producer node in each round. The elected node has the responsibility to finalise a block, which is then broadcasted to and voted on by other producer nodes. As a mechanism for a permissioned network, no Sybil attack resistance is provided.

Appendix F.13. Consensus for Mobile Devices Using Online Brokers [456]

This leaderless BFT protocol allows mobile devices to store transactions in a directed acyclic graph structure. Sybil attack resistance is not a concern of the protocol and is not provided by it. Therefore, a permissioned environment is assumed.

Appendix F.14. FAST [457]

The goal of FAST is to provide a consensus mechanism for a permissioned blockchain that provides high throughput performance. FAST selects leaders, or 'master' nodes, in a round-robin fashion and does, therefore, not provide Sybil attack resistance.

Appendix F.15. Fast Probabilistic Consensus within Byzantine Infrastructures [458]

FPC-BI is a leaderless consensus mechanism reliant on random number generation. The authors recognise that, in its current form, Sybil attacks are possible and that improvements are needed for the mechanism to be practical. However, the protocol is shown to resist Byzantine attacks under a permissioned setting.

Appendix F.16. Fast, Dynamic and Robust Byzantine Fault Tolerance [459]

FDRBFT is a BFT consensus mechanism designed to provide high throughput performance as well as scalability and robustness. The proposed algorithm is resistant to nodes entering and exiting the network at runtime. As a BFT protocol, Sybil attack resistance is not a design consideration.

Appendix F.17. FastPay [460]

FastPay is a leaderless consensus protocol for permissioned systems. Its design goal is one of high performance and scalability, claiming to achieve 80,000 transactions per second. As a permissioned protocol, it does not provide Sybil attack resistance.

Appendix F.18. FireLedger [461]

FireLedger uses an eventually-consistent BFT consensus mechanism for permissioned networks. As such, it does not provide Sybil attack resistance.

Appendix F.19. FRChain Consensus [462]

FRChain is presented as a highly performant consensus protocol using collective signing and Boneh–Lynn–Shacham (BLS) encryption for permissioned blockchains. The protocol does not provide Sybil attack resistance. Its throughput performance was shown to only drop sub-linearly upon increasing the network size.

Appendix F.20. Gosig [463]

This BFT mechanism for permissioned systems achieves safety, scalability, and liveness under adaptive attacks. It does not provide an Sybil attack resistance scheme.

Appendix F.21. High Performance and Scalable Byzantine Fault Tolerance [464]

Jiang and Lian [464] introduce High Performance and Scalable Byzantine Fault Tolerance (HSBFT) with the goal of improving on the communication complexity of PBFT to achieve higher scalability and better performance. Modifications to PBFT include subprotocols to add and remove nodes at runtime. The proposed mechanism provides no Sybil attack resistance.

Appendix F.22. High-Performance Blockchain Enhanced Consensus [481]

High-Performance Blockchain Enhanced Consensus (HyBE) combines a PoW phase with, presumably, fixed difficulty for leader selection. Successful nodes would subsequently enter a PBFT phase. It is, however, unclear whether this simplified PoW stage can provide the same Sybil attack resistance of a complete PoW protocol. Therefore, HyBE needs to be considered to be providing limited Sybil attack resistance.

Appendix F.23. HPBC [465]

This algorithm for permissioned, or 'consortium', systems, is presented as an alternative to PoW that provides BFT. While some future work is outlined to improve Sybil attack resistance of the algorithm, in its current form, none is provided.

Appendix F.24. Hybrid PoW/PoS [446]

In this hybrid scheme, PoS and PoW are combined with the stated goal of making block intervals more consistent than those of PoW. This is done with the intention of providing investors 'revenue uniformly against their investment' [446] (p. 400). In contrast to earlier hybrid schemes, the one proposed by Gupta et al. [446] employs an *outer* PoS loop. The Sybil attack resistance of the proposed scheme can be assumed to be similar to those of non-hybrid PoS or PoW systems.

Appendix F.25. Improved Practical Byzantine Consensus [466]

The Improved Practical Byzantine Consensus (IMP-PBFT) mechanism introduces changes to PBFT with the goal of improving its consensus convergence speed. This is achieved by introducing a voting mechanism to determine the 'most recognised master node'. The protocol does not address permissionless settings and does, therefore, not provide Sybil attack resistance.

Appendix F.26. MinBFT-Based Consensus [467]

With this application of the MinBFT consensus mechanism, the authors aim to improve BFT performance in scenarios in which only a small proportion of participants is malicious. The mechanism is not intended for a permissionless system and does not provide Sybil attack resistance.

Appendix F.27. Mixed Byzantine Fault Tolerance [468,469]

To improve throughput performance and fault tolerance of (permissioned) consortium blockchains, Du et al. [468,469] propose a two-layer consensus mechanism in which 'mini blocks' are created with weak consistency guarantees which are then, periodically, combined into 'large blocks' with stronger consistency guarantees. As a mechanism for permissioned systems, it does not provide Sybil attack resistance.

Appendix F.28. Multi Party Computation Delegated Proof-of-Stake (MPC-DPoS) [482,483]

MPC-DPoS is designed as a DPoS-based mechanism that utilises logic ring-based election in combination with Yao's millionaires' algorithm for leader selection. In MPC-DPoS, a number of candidate nodes are selected from the entirety of the nodes in system and are, subsequently, logically grouped into a ring structure. Stake in the system is then determined based on a node's equity multiplied by a random number. Nodes that are not elected during a round have their stake increased for the next election and nodes that are elected have their stake reset. No limitations on candidate nodes are imposed by the protocol, therefore it can be assumed to be vulnerable to coordinated Sybil attacks.

Appendix F.29. Proof-of-Execution [470]

Gupta et al. [470] propose proof-of-execution with the goal of improving throughput performance of PBFT. They approach this through the introduction of speculative processing, by which transactions are executed prior to consensus finalisation. As a 'drop-in' replacement for PBFT, proof-of-execution does not provide Sybil attack resistance.

Appendix F.30. Proof-of-Scalable-Traceability (PoST) [471]

PoST operates on the assumption of the honesty of more than $1/2$ of involved compute nodes. Should this assumption be violated, the PoST protocol would delegate validation to 'shared storage', a centralised component. Therefore this protocol has to be considered to be appropriate for permissioned systems only.

Appendix F.31. Proof-of-Vote [369]

This centralised mechanism for permissioned blockchains introduces four roles ('comissioner', 'butler', 'butler candidate', and 'ordinary user') to capture a hierarchy of permissions for block validation. As a permissioned protocol, it does not provide Sybil attack resistance.

Appendix F.32. Raft with Network Stability Evaluation [472]

In this modification of the Raft protocol, a network quality evaluation based on peer feedback is introduced. This, however, does not change the Sybil attack resistance properties when compared to Raft.

Appendix F.33. Random-Checkers Proof-of-Stake [473]

In the context of the work on 'P Coin', an unweighted PoS protocol is proposed. Namely, one where any validator that holds stake, irrespective of size, gains equal mining rights. This approach is highly susceptible to attackers that create Sybil accounts with minimal balances and does, therefore, not provide Sybil attack resistance.

Appendix F.34. SACZyzzyva [474]

The authors propose a speculative BFT protocol with the goal of increasing resilience. The resulting algorithm, indeed, only requires $3f + 1$ replicas to tolerate f faults. It furthermore tolerates slow replicas. As a BFT protocol it does, however, not provide Sybil attack resistance and is intended for permissioned settings.

Appendix F.35. Scalable BFT Consensus Mechanism through Aggregated Signature Gossip [447]

The proposed multi-level BFT consensus mechanism aims to achieve high performance (as measured by transaction finalisation time and transaction throughput) while delivering a high degree of decentralisation. This is approached through validator committees, sets of dedicated nodes that are responsible for block production. The proposed protocol can operate in permissioned and permissionless configurations: Sybil attacks are prevented by requiring nodes to lock up a certain amount of stake, thereby, providing PoS-like Sybil attack resistance.

Appendix F.36. Scalable Dynamic Multi-Agent Byzantine Fault-Tolerance (SDMA-PBFT) [475]

SDMA-PBFT is a consensus mechanism for permissioned systems that aims to reduce the communication costs of PBFT. According to the authors, the protocol fulfils this goal by allowing for the formation of multiple autonomous systems at agent nodes to enable message multi-casting. As a permissioned system, SDMA-PBFT does not provide Sybil attack resistance.

Appendix F.37. Scalable Efficient Byzantine Fault Tolerance (SeBFT) [476]

SeBFT offers a communication complexity of $O(n)$ and allows nodes to join and exit the protocol freely. As a PBFT protocol, Sybil attack resistance is not addressed at the protocol level.

Appendix F.38. Scored PBFT [477]

Chen et al. [477] propose this algorithm with the goal of improving the consensus fault tolerance of PBFT. This goal is approached by introducing a basic reputation system to PBFT that is populated during a scoring stage that occurs after the reply stage. During the scoring stage, delays in message passing are penalised, with the goal of bringing about a committee that consists of the best-performing nodes. The proposed protocol is intended to be used in permissioned networks and does not offer Sybil attack resistance.

Appendix F.39. Self-Referencing Directed Acyclic Graph and Voting-Based PBFT Consensus [484]

This protocol is a variation of PBFT that selects validators based on their reputation, or the 'weight of [their] account[s]' [484, p. 282]. However, it is not obvious, what this weight refers to. Therefore, the Sybil attack resistance properties cannot be determined unequivocally.

Appendix F.40. Stream of Distributed Secrets for Quantum-Safe Blockchain (SodsBC) [478]

SodsBC is a protocol for permissioned networks, intended for networks with a fixed size of 'about one hundred participants' [478, p. 249]. It delivers high performance and quantum safety but does not provide Sybil attack resistance as part of the core protocol.

Appendix F.41. T-PBFT [479]

To improve fault tolerance, reduce the probability of view changes, and reduce the protocol communication complexity, Gao et al. [479] introduce T-PBFT for permissioned systems. A performance gain over previous PBFT architectures is sought by narrowing down the number of consensus nodes according to an internal reputation system based on a performance metric. As a protocol targeting a permissioned environment, no Sybil attack resistance is provided.

Appendix G. Description of Mechanisms for IoT

Appendix G.1. BFT Consensus Based on Dynamic Permission Adjustment [496]

This consensus mechanism is designed for IoT devices. Unlike traditional consensus mechanisms, it adjusts the voting weight of each node dynamically according to its communication performance and voting behaviour. This is done with the goal of ensuring that the system is not impacted by malicious nodes in a hostile environment, while still being able to converge quickly in a more honest environment.

Appendix G.2. DPoS for Network Intrusion Detection [526]

In this article, Jinhua et al. [526] propose a voting-based addition to DPoS: nodes can express their disapproval towards other nodes, thereby building a reputation system. Upon falling behind the reputation threshold, a node will be 'excluded from the detection system' [526] (p. 3192). This approach is highly susceptible to Sybil attacks in which attackers create Sybil identities that outvote legitimate nodes. Therefore the mechanism is only appropriate for permissioned networks and provides no significant Sybil attack resistance.

Appendix G.3. IoT Adaptive Dynamic Consensus [497]

In this mechanism for permissioned systems in the IoT domain, conventional BFT consensus is extended with the capability of probing potential leaders for availability through 'heartbeat' messages. This is done to accommodate scenarios in which larger proportions of potential leaders become absent due to connectivity issues. No Sybil attack resistance is provided by the given algorithm due to its permissioned nature.

Appendix G.4. Practical Byzantine Fault Tolerance Based on Reputation Value (RPBFT) [527]

RPBFT uses a reputation system to determine a leader for each consensus round. For this, a 'reputation value' is used as a numerical approximation of a candidate's trustworthiness. This value appears to be based mostly on 'service delay', a measure of latency. This algorithm for IoT orchestration does not provide Sybil attack resistance and is intended for permissioned systems.

Appendix G.5. PoW with Mining Tokens [488]

The proposed algorithm effectively constitutes a PoS-augmented PoW system in which stake in the form of 'mining tokens' determines the difficulty of the PoW puzzle. The entirety of the stake is allocated in the genesis block and is subsequently distributed to different nodes. It can be assumed that this combination of PoS and PoW provides strong Sybil attack resistance.

Appendix G.6. Adaptive Proof-of-Work (APoW) [498]

APoW introduces a capability assessment of participating miner devices in which a 'target adaptor' estimates the computational power of a node. Subsequently, the PoW difficulty is set accordingly. A trusted entity to determine the capability of a node is, however, required as, otherwise, attackers might easily underreport this metric. Therefore, this algorithm is only suitable for permissioned networks in which Sybil attack resistance is not a concern.

Appendix G.7. Consensus Algorithm for Mobile-Edge Computing [528]

In this scheme, dedicated to the IoT domain, the voting power of a participant is calculated based on its reputation. Reputation is measured by considering the opinions submitted by the participant's clients and the opinions of other participants. As such, the protocol is Sybil attack resistant under naive attacks but might not withstand well-orchestrated attacks.

Appendix G.8. Collaborative Proof-of-Work (Co-PoW) [489]

Co-PoW is a consensus mechanism for IoT that incentivises collaboration among miners to improve performance. It follows a two-layer architecture, with macroblock miners solving PoW puzzles to create blocks that contain control information, and microblock miners packing transactions without strong Sybil attack resistance guarantees. A dynamic weight is assigned to participating devices to express their trustworthiness numerically.

Appendix G.9. Collaborative Trust Based Delegated Proof-of-Stake (CT-DPoS) [499]

CT-DPoS is a consensus mechanism for permissioned systems that achieves a random selection from a pool of 'control authorities' in industrial automation scenarios. The authors recognise the hierarchical nature of this domain and, therefore, do not intend for the protocol to provide Sybil attack resistance.

Appendix G.10. Consensus with Elected Leader [500]

Consensus with elected leader constitutes a simple turn-taking protocol in which individual participants form sub-groups. This is done with the goal of making permissioned systems more tolerant of partitioning. As a protocol targeting a permissioned environment, no Sybil attack resistance is provided.

Appendix G.11. Context-Based Consensus [501]

In this consensus mechanism for appendable-block blockchains, consensus is performed inside shards, or 'contexts', and then propagated through gateways to neighbouring shards. This is done with the goal of reducing latency and increasing throughput. The authors discuss the susceptibility to Sybil and 1 % attacks, and find that in particular configurations the mechanism is susceptible to Sybil attacks.

Appendix G.12. Credit Reinforce Byzantine Fault Tolerance (CRBFT) [529]

This modification of PBFT introduces an AI reputation system for the detection of 'malicious [...] and invalid nodes'. The system uses 'credit' to quantify the well-behavedness of a participant node. Fixed credit is awarded for adherence to the protocol but the credit balance can also be influenced by the AI reputation system. While this may provide basic Sybil attack resistance against simple attacks, complex ones, in which attackers accumulate 'credit' to strike later, are not preventable by the mechanism. Therefore, limited Sybil attack resistance can be attributed to CRBFT.

Appendix G.13. Credit-Based Consensus Mechanism [490,491]

This PoW mechanism employs weighting via a reputation system built on 'credit value'. Participants can earn credit for adherence to the protocol: nodes that follow the protocol well are rewarded with a lower PoW difficulty. This provides high Sybil attack resistance under the assumption of conservative parameters for credit value benefits.

Appendix G.14. Delegated Proof-of-Proximity (DPoP) [545]

DPoP employs a distance-bounding consensus technique: nodes that are in close proximity to an event over which consensus should be established can play a more significant role in the consensus mechanism. This approach provides good Sybil attack resistance under the assumption of simple Sybil attacks but would be less effective in a scenario where

an attacker would be able to deploy multiple Sybil sensors to bootstrap further virtual Sybil identities.

Appendix G.15. Distributed Time-Based Consensus (DTC) [530]

DTC is optimised for low-resource IoT devices and relies on randomised leader selection based on waiting time. As a mechanism to achieve Sybil attack resistance, the authors introduce hurdles for creating identities on the network, either by 'burn[ing] coin in Bitcoin' or by 'receiv[ing] a certificate from trusted CAs'. While this may provide some Sybil attack resistance, the economic properties (i.e., cost of attack) have not been explored, therefore limited Sybil attack resistance is to be assumed.

Appendix G.16. Double-Layer PBFT [502]

This mechanism includes a two-layer consensus mechanism, designed to improve the performance of 'massive' networks. As a permissioned system, no Sybil attack resistance is provided.

Appendix G.17. Dynamic Blind Voting [503]

In this mechanism, miners are selected via a pseudorandom process based on the contents of a unified Mempool. While this approach may lead to selecting a suitable miner in a permissioned setting, it can be easily evaded in a permissionless setting where an attacker can create an arbitrary number of miner nodes. Therefore, the mechanism does not provide Sybil attack resistance.

Appendix G.18. Edge Computing Blockchain Security Consensus Model (ECBCM) [531]

ECBCM constitutes a reputation system based on the 'prestige' metric. 'Prestige' is a numeric representation of a node's trustworthiness as well as a measure of a node's ability to provide computing resources. ECBCM is designed to be used in an edge computing service model, where there are two types of users: potential leaders (edge nodes), and those who use the services provided by the edge nodes. ECBCM constitutes a three-step protocol: first, the election phase (aided by the prestige metric), second, the block consensus phase (led by the elected leader node), and, third, an eviction phase in which nodes falling under the prestige threshold are removed. Similar to other reputation systems presented here, when deployed into a permissionless setting, limited effectiveness against well-orchestrated Sybil attacks must be assumed.

Appendix G.19. Geographic-PBFT [532]

In this consensus mechanism stationary, or 'fixed', IoT devices enjoy special permissions. Lao et al. [532] hypothesise that those are less likely to take part in Sybil attacks and are, therefore, well suited to play a leading role in a geographic consensus mechanism. Nodes report their location and, upon detection of inconsistencies in their reports, are removed from the system. While the mechanism is portrayed as suitable for a permissionless setting, details on detecting Sybil identities are sparse. The authors seem to rely on reports of Sybil identities by non-malicious users—an approach that must be characterised as providing limited Sybil attack resistance only.

Appendix G.20. Honesty-Based Distributed Proof-of-Work [533]

In Honesty-Based Distributed Proof-of-Work, all prospective participant nodes are required to continuously perform basic PoW. By solving PoW puzzles correctly, they improve their 'honesty' score, thereby improving their chances to be elected leader while simultaneously decreasing the difficulty of the PoW assigned to them. In this proposal, individual IoT devices would directly participate in PoW. This reputation system is, however, unlikely to provide strong Sybil attack resistance in a permissionless setting, as attackers

could create malicious identities that qualify as leaders with relatively low computational effort.

Appendix G.21. Honesty-Based Distributed Proof-of-Authority via Scalable Work (HDPoA) [534]

HDPoA is largely identical to Honesty-Based Distributed Proof-of-Work (see Appendix G.20) and has comparable Sybil attack resistance properties.

Appendix G.22. Hybrid PoW/PoS [492]

In this PoS/PoW hybrid, PoW is used as a checkpointing technology for PoS. In the context of the proposed protocol, PoS blocks are to be created by resource-constraint devices. The hybrid scheme can be assumed to provide high Sybil attack resistance.

Appendix G.23. Hybrid Consensus [550]

Hybrid consensus is a mechanism for a two-layer blockchain architecture, consisting of a permissionless blockchain, using a consensus mechanism with strong Sybil attack resistance properties, and one or more permissioned networks. The latter is connected to the permissionless blockchain via 'hybrid nodes' that act as oracles for the permissioned networks.

Appendix G.24. Improved PBFT [504]

In this permissioned protocol, nodes that prove ongoing participation in the scheme can qualify as 'consensus nodes' and, therefore, as block producers, if they have a high degree of activity. Since, in this protocol, admission relies on a central CA, no Sybil attack resistance is provided.

Appendix G.25. Lightweight Blockchain based Cybersecurity [505]

The Lightweight Blockchain based Cybersecurity scheme is proposed by Abdulkader et al. [505] with the goal of 'increas[ing] the transactions [sic] throughput and minimum [sic] the block appending waiting time'. It makes use of an intermediary, called aggregation block manager (ABM), that receives instructions from other participants. Since aggregators commonly have to be determined via unspecified off-ledger governance processes, aggregator-based mechanisms normally cannot be considered Sybil-resistant.

Appendix G.26. Lightweight Consensus for IoT (LC4IoT) [506]

LC4IoT is a lightweight consensus algorithm for blockchains that is designed to be used in IoT contexts. A central aspect of the proposed protocol is oracles: any valid transaction requires the signature of an oracle in order to be added to the blockchain. Therefore, it constitutes a permissioned mechanism that does not provide Sybil attack resistance.

Appendix G.27. Luckyminer [507]

In this mechanism, a responsible miner, or 'Luckyminer', is determined based on the hash of the proposed transaction. This approach is highly susceptible to Sybil attack resistance due to the fact that attackers may register arbitrary addresses to conduct attacks.

Appendix G.28. Multi-Chain Proof of Rapid Authentication (McPoRA) [508]

McPoRA, a consensus mechanism for permissioned networks, follows a protocol which assumes nodes to be to be predefined and granted a unique identifier. These nodes then collect data from network users.

Appendix G.29. Optimized PBFT Consensus with Speaker [509]

In this modified PBFT algorithm for IoT and Edge Computing, the role of a 'speaker' that relays information to 'congressmen' is introduced, thereby improving performance at

the cost of fault tolerance. The proposed algorithm is intended for a permissioned setting and does not provide Sybil attack resistance.

Appendix G.30. PF-BVM [535]

In PF-BVM, nodes maintain a trust score, the percentage of decisions made in accordance with neighbouring nodes. Only nodes that maintain a high score over a longer time are entitled to participate in consensus. While this approach would likely prevent most simpler Sybil attacks, orchestrated Sybil attacks by a clique of attackers might still be successful.

Appendix G.31. Predictive Proof of Metrics (PPoM) [536]

PPoM constitutes a reputation-based consensus mechanism that employs a rating scheme for all participants. It is based on Class of Service (CoS) and Quality of Service (QoS). Similar to other reputation systems described earlier, the mechanism relies on participants on the network rating each other. While this approach can provide some Sybil attack resistance, more complex and well-orchestrated Sybil attacks would not be preventable with this mechanism.

Appendix G.32. Proof of Elapsed Work and Luck (PoEWAL) [537]

PoEWAL constitutes a difficulty-adjusted PoW scheme in which the time miners spend on computing the PoW solution is fixed. As such, difficulty-adjustment schemes can increase the likelihood of forks (i.e., in cases where multiple miners solve the puzzle in the allotted time), the authors propose to add a 'luck' component, giving miners with lower nonces priority in the case of a tie. This pseudorandom approach, however, paves the way for Sybil attacks, as malicious node operators can create multiple solutions to the low-difficulty PoW puzzle, thereby increasing their chances of being selected.

Appendix G.33. Proof-of-Presence [510]

The proposed mechanism constitutes a turn-taking consensus protocol in which a token is periodically passed between participants to indicate leadership. This protocol requires a permissioned setting and could easily be stalled by a Sybil attack.

Appendix G.34. Proof of Physical Unclonable Function (PUF)-Enabled Authentication [553]

Proof of PUF-Enabled Authentication is designed for IoT networks that are characterised by limited processing power. It uses physical unclonable function to uniquely identify devices. However, the Sybil attack resistance of Proof of PUF-Enabled Authentication has not been explored: this indicates application in a permissioned IoT network.

Appendix G.35. Proof of Random Count in Hashes [511]

Hossain et al. [511] propose a simple leader selection method for private and permissioned blockchains based on deriving pseudorandom numbers from message payloads. As a method for permissioned systems, it does not provide Sybil attack resistance.

Appendix G.36. Proof of Reputation [512]

This consensus mechanism for permissioned systems employs a reputation system designed for more secure data sharing in a smart city environment. Trustworthiness Criteria for the proposed reputation system are reputation (a measure of satisfaction with a service provider), legal compliance, and compliance with preferences. A score is generated for each criterion and the average is used to rank trustworthiness. Only nodes with a high ranking are able to participate in consensus. As a permissioned mechanism, no Sybil attack resistance is considered.

Appendix G.37. Proof-of-Authentication (PoAh) [546–548]

PoAh is a lightweight consensus algorithm that utilises Media Access Control (MAC) addresses as unique IDs of nodes in the network. This approach allows for Sybil attack resistance, however, complex Sybil attacks with a large number of virtual devices would not be preventable.

Appendix G.38. Proof-of-Balance [513]

In this permissioned protocol, 'vendors' form shards for validator selection. This requires an assignment of nodes to sets based on their vendor characteristics and, therefore, a trusted source of vendor information or a central coordinator. Therefore, the proposed algorithm does not provide Sybil attack resistance.

Appendix G.39. Proof-of-Block-and-Trade [514]

This consensus mechanism, intended for permissioned systems, aims to improve computational overhead for transaction verification. It does not address Sybil attack resistance.

Appendix G.40. Proof-of-Common-Interest (PoCI) [515,516]

Doku et al. [515], Doku and Rawat [516] only give limited insight into the leader selection mechanics of PoCI which resembles a peer-to-peer network with many distinct individual data stores rather than an implementation of DLT. Regardless, it can be assumed that Sybil attack resistance is not a concern of the protocol as it, presumably, is intended to be used in a permissioned setting only.

Appendix G.41. Proof-of-Honesty [538,539]

Proof-of-Honesty is a consensus mechanism for IoT designed to be computationally efficient and scalable. It makes use of a reputation system that employs an 'honesty metric', a numerical property that quantifies the trustworthiness by evaluating previous adherence to the protocol. The authors aim to prevent Sybil attacks by relying on this metric for leader selection. Any Byzantine nodes, as evidenced by a low score, are restricted from participating in the consensus process. Such an approach, while effective for small-scale Sybil attacks, may be ineffective against more powerful attackers. Those may be able to subvert the reputation system by controlling a large number of nodes.

Appendix G.42. Proof-of-Negotiation/Proof-of-Trust Negotiation (PoTN) [540,541]

The PoTN mechanism makes use of a reputation system in which a numeric 'trust value' is assigned to each participant. While this provides sufficient Sybil attack resistance for simpler attacks under the assumption of a well-bootstrapped system, an orchestrated attack by a malicious user with perfect knowledge of the protocol and large commitment is still conceivable.

Appendix G.43. Proof-of-Physical Unclonable Function (PoPUF) [549]

PoPUF enforces a challenge-response protocol ahead of the actual consensus protocol. This additional step ensures that only participants in control of a PUF-enabled device can participate and act as miners. Therefore, the user identity is tied to a PUF, providing limited Sybil attack resistance since a scenario is conceivable in which an attacker gains possession of many physical PUF devices, or manages to virtualise these.

Appendix G.44. Proof-of-Popularity [517]

In this permissioned protocol, potential leaders are rated by 'knowledge ranking' and 'proposal ranking' systems. The rating, in turn, determines the likelihood of being selected as a leader. As a permissioned protocol, no Sybil attack resistance is provided.

Appendix G.45. Proof-of-Reputation-X (PoRX) [551]

The PoRX scheme constitutes a reputation system overlay for other Proof-of-X consensus protocols to improve upon their suitability for Industrial Internet of Things (IIoT) use cases. The goal of the overlay is to reduce the difficulty of the underlying consensus mechanism by providing additional trust information. While the authors claim that Sybil attacks can be mitigated through identity registration, it is not clear how effective this would be in practice due to details on the identity registration contract being sparse. Therefore, the Sybil attack resistance properties cannot be established firmly.

Appendix G.46. Proof-of-Stability [518]

Similar to MedBlock (see Appendix E.4) and Improved PBFT (see Appendix G.24), Proof-of-Stability requires a permissioned environment, implemented via a centrally managed CA. Therefore, no Sybil attack resistance is provided.

Appendix G.47. Proof-of-Trading [493]

The Proof-of-Trading consensus is designed with the goal of producing a sustainable consensus mechanism for edge of networks in which computational resources are scarce. A reputation system based on 'Knowlegde Coins' is used to select leaders based on their contributions as quantified by their trading stake. Potential leaders are still required to partake in PoW to prevent Sybil attacks, but the difficulty of the hash puzzles they face is dynamically adjusted based on their stake.

Appendix G.48. Proof-of-Validity [519]

Proof-of-Validity is a mechanism designed for the application in permissioned robotics systems. In the mechanism, robots with a clean 'bill of health' (i.e., no known faults), can participate as miners. Sybil attack resistance is not a concern of the mechanism as it seems to assume a permissioned setting.

Appendix G.49. Proof-of-Work Using Maximization-Factorization Statistics [552]

In this PoW scheme, consensus difficulty is limited with the goal of allowing resource-constrained devices to participate in PoW. The effects of such difficulty ceilings on Sybil attack resistance and the risk of forks cannot be determined trivially, therefore, no assessment of Sybil attack resistance is provided.

Appendix G.50. Random Proof of Work [494]

This PoW scheme employs a random number search mechanism that, according to the authors, is well-suited for the IoT domain due to its lower difficulty. While there is concern that such a scheme could undermine security, if difficulty is kept artificially low, strong Sybil attack resistance properties, similar to other PoW models, can be assumed.

Appendix G.51. ReBFT [520]

This variation of BFT aims to improves robustness by dividing the consensus process into a 'control flow' and a 'data flow' component and by managing the the former centrally. From a performance perspective, ReBFT does not offer significant improvements over PBFT. However, In contrast to PBFT, ReBFT makes use of more sophisticated leader selection strategies, like health status-based leader selection. ReBFT assumes a permissioned environment and, therefore, does not provide Sybil attack resistance.

Appendix G.52. Register, Deposit, Vote (RDV) [542]

RDV is a voting-based consensus mechanism, designed to be more democratic, fairer and more decentralised than PoW. Key to the scheme is a time-bound voting phase in which all registered nodes can cast their vote. The result of the voting process is used to determine whether a transaction is valid or not. To avoid Sybil attacks, participants have to

pay a deposit upon joining the system. It can be speculated that this provides Sybil attack under small-scale attacks but that, due to the low constant cost of joining, more complex attacks cannot be avoided.

Appendix G.53. SCBFT [521]

SCBFT constitutes a permissioned consensus mechanism for IoT devices. In this mechanism, the private key material for IoT devices is generated by a centralised private key generator with the goal of reducing the overhead of maintaining a PKI that would occur in the case of self-managed key material. The proposed mechanism is intended for permissioned systems and does not provide Sybil attack resistance.

Appendix G.54. Sybil Resistant IoT Trust Model [543]

In this proposal, a reputation system based on 'trust points' is established, which allows peers to reward nodes for executing transaction proposals correctly. In terms of Sybil attack resistance, this approach can be rated similar to other P2P reputation systems: it would likely withstand simple Sybil attacks but could not withstand orchestrated Sybil attacks.

Appendix G.55. Synergistic Multiple Proof (SMP) [544]

SMP introduces a reputation system based on the 'collaboration degree' of IoT devices which is used to dynamically adjust the difficulty of mining. This is done to save energy and promote collaboration among devices. While this may protect from simple Sybil attacks, more complex attacks in a permissionless setting are unlikely preventable. This is due to the fact that an attacker might create a network of Sybil nodes to inflate their collaboration degree.

Appendix G.56. Three-Dimensional Greedy Heaviest-Observed Sub-Tree Consensus 2963 (3D-GHOST) [495]

3D-GHOST constitutes a two-layer consensus mechanism with PoW being applied to the mining of 'macroblocks' (blocks carrying 'control information'). The protocol was designed with the goal of improving security and network performance over previous blockchain protocols used in IoT contexts. It can be assumed that this approach provides equally strong Sybil attack resistance characteristics to earlier PoW protocols.

Appendix G.57. Time-Dependent Consensus [522]

The proposed Time-Dependent Consensus technique is intended to randomly select a block generator between nodes. This is done by subjecting nodes to an arbitrary waiting period before they can create new blocks. This mechanism would, however, not be effective under a Sybil attack because an attacker might create multiple nodes to increase their chances of being selected as a block generator.

Appendix G.58. Tree-Chain [523]

Tree-Chain is designed as a protocol catering specifically to the requirements of IoT that relies on simple randomisation for leader selection. It is intended for permissioned networks with a central CA from which participants have to acquire a certificate for admission. Therefore, no Sybil attack resistance is provided.

Appendix G.59. Two-Layer-Consensus Architecture for IoT [524]

In this approach, a layered system architecture is proposed: on the 'base layer', individual nodes perform low-difficulty PoW, while the 'top layer' constitutes a permissioned system. As a permissioned system, the consensus mechanism does not provide Sybil attack resistance.

Appendix G.60. Weighted Majority Consensus Algorithm (WMCA) [525]

WMCA represents a non-Sybil attack-resistant consensus mechanism for the IoT vertical that penalises miners for misjudging transaction validity. This reputation system is, however, highly vulnerable to Sybil attacks and is therefore only suited for permissioned systems.

Appendix H. Description of Mechanisms for Media and Entertainment

Appendix H.1. Credibility Score [560]

The authors devise a PoS-like reputation system in which users gain stake for desirable activities (e.g., reporting 'fake news') and lose stake for undesirable activities. While this approach leads to a robust system under the assumption of a majority of honest users and uncoordinated Sybil attacks, it may not provide Sybil attack resistance in face of a highly strategic adversary.

Appendix H.2. Proof-of-Contribution [561]

The Proof-of-Contribution consensus mechanism is designed for intellectual property registration and related transactions on blockchains. For leader election, a 'contribution value' is applied that quantifies users' behaviours and actions. The node with the highest contribution value is entitled to generate a new block, and thus receives a reward. To address Sybil attacks the authors propose a cooling function that reduces the contribution value for new users. While this can be considered to prevent basic Sybil attacks, more complex ones are unlikely affected by this scheme.

Appendix H.3. Proof-of-Play [559]

In Proof-of-Play, investing effort into a game serves as a leadership qualification mechanism. It can be assumed that Proof-of-Play targets permissioned settings, since administrative tasks like the provision of a game executable, setting of appropriate game difficulty and tamper-proof evaluation of gaming success need to be orchestrated centrally. Concerning Sybil attack resistance, the authors take the perspective that the cognitive demand of gaming constitutes a Sybil attack resistance technique. This notion is similar to other proof of human work schemes.

Appendix I. Description of Mechanisms for Supply Chain

Appendix I.1. C-dBFT [565]

To address issues in the supply chain traceability of tea products, an authorised Byzantine Fault Tolerance-based consensus mechanism is proposed. A reputation system based on credit values is designed to motivate all participating nodes to participate in voting activities. Weights are assigned to each node according to their performance in several aspects in order to determine the most suitable consensus nodes and backup nodes. While it can be speculated that the reputation system using reward and punishment can prevent some Sybil attacks, more complex ones are not taken into account. However, due to the hierarchical structure, the system can be categorised as centralised. Therefore, Sybil attack resistance is likely not a design goal of the protocol.

Appendix I.2. Consensus Mechanism for Marine Data Management System [569]

This scheme simplifies PBFT by relaxing the assumptions around the existence of Byzantine nodes. This is done under the assumption of the authors that 'in mature systems [...] there will be no Byzantine nodes with malicious actions' [569] (p. 24). The resulting consensus mechanism relies on electing a 'main node' responsible for record keeping. This approach does not provide Sybil attack resistance.

Appendix I.3. Group-Based PoW [566]

In this PoW protocol, only a subset of pseudorandomly selected members qualifies for participation in PoW. While this is done in the interest of improving the 'computational overhead', it raises questions of Sybil attack resistance: specifically, an attacker might be able to increase their chances of being selected pseudorandomly when presenting Sybil identities.

Appendix I.4. Improved Practical Byzantine Fault Tolerance (iPBFT) [570,571]

iPBFT proposes some improvements over PBFT, namely, 'scheduling nodes' are introduced to verify transactions and then sign them if they are valid. These nodes are centrally managed off-ledger by a consortium. Therefore, Sybil attack resistance cannot be considered a design goal.

Appendix I.5. Multi-Center Practical Byzantine Fault Tolerance (MCPBFT) [567]

The proposed system represents a two-layer PBFT algorithm participants are assigned to subgroups ('consensus sets'). The primaries of each consensus set then engage in super-consensus, eventually forming a system-wide view across shards. This approach, intended for permissioned networks, does not provide Sybil attack resistance.

Appendix I.6. Proof of Accomplishment [568]

In this mechanism for permissioned systems, a reputation system with five dimensions is made available to participants. The likelihood of being selected as a leader depends on the rating a user achieves. No Sybil attack resistance is provided by the mechanism due to its permissioned nature.

Appendix I.7. Proof-of-Location [572]

The proof-of-location protocol specifies how a subset of geographically distributed nodes can reach consensus on a message proposed by a neighbouring node. It does, however, not specify how this technique could be used to reach system-wide consensus.

Appendix J. Description of Mechanisms for Telecom

Appendix J.1. Delegated Proof-of-Trust (DPoT) [574]

Lwin et al. [574] propose a consensus mechanism for mobile ad hoc networks (MANETs). The proposed scheme is a trust management system employing a combination of policy-based and reputation-based trust management. The reputation component is anchored in trust values, a metric that determines whether a node is trustworthy based on the node's past behaviour. The policy component is implemented through a series of rules that dictate how and when trust values are updated. To validate blocks in the proposed scheme, a DPoT algorithm is used: following this, nodes with high trust values are elected as validators. While the reputation system can prevent small-scale Sybil attacks, well-orchestrated ones are unlikely preventable due to the possibility of a large number of Sybil identities colluding to artificially inflate their score.

Appendix J.2. Proof-of-Majority (PoM) [575]

In the PoM mechanism, 'broker nodes' qualify as leaders. The authors do, however, not prescribe a leader election methodology. Notably, the proposed consensus mechanism is of a permissioned nature, requiring registration with a central node for each broker. Consequently, this consensus mechanism is best suited for a closed group of mutually trusting entities.

Appendix K. Description of Mechanisms for Useful Work

Appendix K.1. PoUW for ML Training [576]

In this PoUW scheme, miners train machine learning models and are rewarded in cryptocurrency for their work. A verification process is used to ensure that the models are trained accurately, and that the results are made available to the public.

Appendix K.2. PoW Applied to High-Dimension, Non-Linear Optimisation Problems [577]

In this PoUW scheme, miners can engage in tasks with relevance to scientific computing, such as high-dimensional, non-linear objective functions. The Sybil attack resistance can be considered similar to those of ordinary PoW.

Appendix K.3. PoW Based On NCP-Solving [578]

Géraud et al. [578] propose solving nilcatenations on a given transactional graph as a 'community-serving', or, useful, PoW. The Sybil attack resistance properties are comparable to other PoW schemes.

Appendix K.4. PoW Based on Random Multivariate Quadratic Equations [579]

In this paper, a problem that has not previously been used for PoUW, namely the multivariate quadratic (MQ) problem, is introduced. The benefits of this problem over established ones are presented as improved ASIC resistance, post-quantum resistance, and a useful result. The Sybil attack resistance properties are similar to those of systems using different PoW schemes.

Appendix K.5. PoW on Elements in a Cyclic Group [580]

Hastings et al. [580] propose to employ the problem of 'comput[ing] the discrete logarithm of an element in a cyclic group' as PoUW. The scheme provides the same beneficial Sybil attack resistance properties as other PoW schemes.

Appendix K.6. BlockML [600]

In this PoUW scheme, suppliers post a ML training task with an associated reward, and miners train machine learning models to try to complete the task in a performant way. The best-performing model is selected as the solution, and the corresponding miner gets rewarded. This has the potential to be more energy-efficient than conventional PoW schemes while still providing security. While the protocol is intended for a permissionless setting, it is doubtful that strong Sybil attack resistance would be provided due to the risks of suppliers and miners colluding for block creation rights.

Appendix K.7. Calibration of Public Key Cryptographic Systems via Proof-of-Work [581]

Boyd and Carr [581] design a useful PoW scheme that outputs relevant data for parameter generation of the Schnorr signature scheme. The authors speculate that such a computational puzzle not only yields useful results but may also be more resistant to ASICs than existing schemes. The Sybil attack resistance level is equivalent to that of earlier PoW algorithms.

Appendix K.8. Coin.AI [582]

Coin.AI requires miners to provide PoW in the form of AI model data. Miners would only be granted permission to mine a block if the performance of the model submitted by them provably exceeds some threshold. The mechanism exhibits similar Sybil attack resistance characteristics of other PoW mechanisms.

Appendix K.9. Conquering Generals [583]

In this PoUW mechanism the authors propose a compensation-based platform for algorithm research, specifically for addressing an NP-hard computational problems. As a PoUW scheme, it provides Sybil attack resistance similar to other PoW mechanisms.

Appendix K.10. Difficulty-Based Incentives for Problem Solving [584]

This PoUW scheme rewards miners for providing solutions for optimisation problems that have scientific relevancy. The problems proposed are NP-complete. Miners are given an incentive in the form of a lower difficulty to mine a block. The Sybil attack resistance properties can be considered similar to those of common PoW schemes.

Appendix K.11. Hybrid Mining [585]

The term hybrid mining describes a two-stage consensus protocol in which miners can choose between providing common PoW by solving a common moderately hard puzzle (i.e., Hashcash) and providing PoUW in the form of solutions to user-generated computational problems (e.g., protein folding). The protocol has the Sybil attack resistance properties of common PoW protocols.

Appendix K.12. Image-Based Proof-of-Work [586]

In this Proof-of-Work algorithm, useful work is undertaken: miners perform computationally intensive tasks by analysing the entropy of pixel subsets within images. The algorithm provides comparable Sybil attack resistance properties to other PoW algorithms.

Appendix K.13. Proof of Catalytic Space (PoCS) [587]

PoCS is a Proof-of-Space scheme. As in other Proof-of-Space schemes, a Prover 'wastes' space on dedicated storage, which can be used to prove that they have access to a certain amount of resources. It can be differentiated from regular Proof-of-Space by making use of the space utilised by a prover to encode useful data. The Sybil attack resistance properties can be considered similar to those of regular Proof-of-Space.

Appendix K.14. Proof of Deep Learning with Hyperparameter Optimization (PoDLwHO) [588]

PoDLwHO is a PoUW algorithm that mandates miners to perform calculations necessary for hyperparameter tuning of complex AI models, thereby benefiting the training of deep learning models. Due to its similarity with common PoW protocols, PoDLwHO can be considered equivalent to those in terms of Sybil attack resistance.

Appendix K.15. Proof of Evolution [589]

In this algorithm that maintains all the security guarantees of PoW and, therefore, provides strong Sybil attack resistance, useful PoW is performed. Proofs take the shape of results of computations for the execution of genetic algorithms.

Appendix K.16. Proof of Federated Learning (PoFL) [597]

PoFL is a proof of useful work scheme in which miners are rewarded for training machine learning models that are useful to some task requester. To protect data privacy, data tokenisation is applied. Leader selection is not the subject of the paper, however, due to the risk of collusion between task requesters and solvers, and the need for trustworthy evaluation of the resulting model, likely, no Sybil attack resistance would be provided if deployed to a permissionless setting.

Appendix K.17. Proof-of-Accuracy [598]

This protocol for the permissioned 'BytoChain', resembles PoUW in that it rewards miners for selecting the highest-value transactions as measured by the 'accuracy' metric of proposed ML models. As a permissioned system, it does not provide Sybil attack resistance.

Appendix K.18. Proof-of-Deep-Learning [590,591]

In this PoUW scheme, miners undertake deep learning (DL), an AI technique. In order to qualify for block production, miners need to produce a deep learning model along with proof that it generates proper outputs. As such, the Sybil attack resistance properties of the proposed PoUW scheme are comparable to common PoW.

Appendix K.19. Proof-of-Exercise [592]

Proof-of-Exercise (PoX) constitutes a PoUW scheme providing solutions to real-world matrix-based computation problems. While such a scheme may be more challenging to implement than common PoW mechanisms, their Sybil attack resistance properties are equivalent.

Appendix K.20. Proof-of-Learning [593]

In this algorithm, miners, or 'trainers', engage in ML competitions. By training and submitting models for these competitions, miners provide useful PoW. Thereby strong Sybil attack resistance is achieved.

Appendix K.21. Proof-of-Learning [594]

In this PoUW protocol miners undertake ML training work, specifically model-free reinforcement learning, or *Q*-learning. The protocol's Sybil attack resistance parameters can be considered similar to other PoW schemes.

Appendix K.22. Proof-of-Learning [599]

In this PoUW mechanism, nodes are rewarded with leadership permissions for providing a trained ML model which exceeds a defined performance threshold. Consequently, the mechanism requires a trusted entity to make problems available and truthfully verify the model performance. Therefore, the proposed mechanism is suited for a permissioned system and does not provide Sybil attack resistance.

Appendix K.23. Proof-of-Search [601]

In this PoUW scheme, user-submitted computational problems are solved by candidates to qualify as leaders. As commonly practised in such schemes, the miner who solves the problem with the best solution is rewarded. Several open questions for such schemes (e.g., collusion of problem proposer and miner, objective evaluation of result) call into question the resistance of the protocol to complex Sybil attacks.

Appendix K.24. Proof-of-WorkStore [595]

In this PoUW scheme, miners participate in video compression to generate PoW. The Sybil attack resistance properties are equivalent to other PoW schemes.

Appendix K.25. Reciprocally Useful Work [596]

Reciprocally Useful Work (RUW) is a PoUW scheme with a well-defined protocol for creating tasks at runtime, a level of detail that many similar proposals lack. The proposed protocol can be expected to deliver strong Sybil attack resistance, similar to other PoW/PoUW schemes.

Appendix K.26. Susreum [602]

In Susreum principles of PoS are combined with PoW. For leader selection, a PoS algorithm, using 'lines of code' committed as stake metric is performed. Later, selected leaders are required to perform PoW. This approach provides limited Sybil attack resistance, as attackers might create arbitrarily inflated code to gain stake.

Appendix K.27. VBFL [603]

The contribution of Chen et al. [603] can be broadly classified as a PoUW/PoS hybrid with a reputation system that rewards miners for contributing correctly to federated learning, an AI technique. While this proposal is shown to achieve reasonable global accuracy under the assumption of a limited number of malicious nodes ($3/20$), it provides no strong Sybil attack resistance, as a well-orchestrated attack on the protocol deployed into a permissionless setting would likely be successful.

Appendix L. Description of Mechanisms for Vehicles

Appendix L.1. Consensus Mechanism for Blockchains on IoV [605]

In this variation of PoS for coordination in the IoV, the stake is calculated based on the number 'tickets' a potential leader holds. Tickets only provide staking value for a limited time, thereby preventing affluent stakeholders from dominating the leader election. The Sybil attack resistance properties of the proposed mechanism are comparable to conventional PoS.

Appendix L.2. Consensus Program for Charging Piles [611]

In this consensus mechanism, a reputation system is introduced that rewards nodes for adherence to the protocol and punishes them for deviations from it. As a protocol for permissioned settings, it does not provide Sybil attack resistance.

Appendix L.3. dynamic Proof-of-Work [606–608]

dynamic Proof-of-Work (dPoW) introduces a difficulty adjustment scheme based on throughput. The proposed scheme is somewhat counter-intuitive, indicating *high* difficulty when throughput is *low*, and vice versa. It is furthermore unclear how throughput would be made available to the system in an unspoofable fashion. Regardless, the Sybil attack resistance properties can be considered high, in line with previous PoW schemes.

Appendix L.4. Enhanced DPoS [612]

To prevent collusion between highly-staked attackers, Kang et al. [612] propose a PoS scheme in which stake is not calculated objectively (i.e., by considering the sum of the stake held by a participant), but using a subjective logic model: the opinion of other vehicles informs the reputation. It can be assumed that this protocol would only be deployed into a permissioned system. Therefore Sybil attack resistance is not considered an area of concern.

Appendix L.5. Improved Byzantine Consensus for IoV [613]

In this algorithm for the vehicle domain, the authors differentiate between 'roadside communication nodes' (centrally managed permissioned nodes) and 'vehicle-mounted communication nodes'. A 'roadside communication node' is selected pseudorandomly to act as a leader. The system assumes a fixed set of 'roadside communication nodes' and does, therefore, not provide Sybil attack resistance.

Appendix L.6. Mixed Consensus Algorithm Based on PoW and PBFT [609]

The proposed hybrid consensus algorithm, combining PoW and PBFT, is created to achieve efficiency in VANETs that are characterised by being resource-constrained. Due to the hybrid nature of the algorithm, PoW is applied to improve security while practical PBFT enhances efficiency. The application of PoW benefits Sybil attack resistance. PBFT, on the other hand, allows a smaller number of consensus nodes to be used which reduces processing time and improves efficiency. Participants are, furthermore, rated through a reputation scheme in which direct trust and indirect trust are taken into account.

Appendix L.7. Multipoint-Relay-Driven Consensus [614]

In this protocol, participants assemble groups of other nodes according to their position in unmanned aerial vehicle ad hoc network (UAANET). The proposed scheme is, however, not resistant to Sybil attacks since it relies on an honest majority of nodes and does not introduce mechanisms to prevent Sybil identities from joining.

Appendix L.8. Practical Byzantine Fault Tolerance with Forwarding [615]

This consensus mechanism closely follows the common PBFT sequence for message passing between UAVs. As a method that is designed for permissioned networks, it does not provide Sybil attack resistance.

Appendix L.9. Proof of Event and Location [616]

Proof of Event and Location is a mechanism to form consensus over traffic events. As a permissioned mechanism, it relies on centrally managed roadside units that act as oracles to validate events and calculate trust values. Roadside units form the heart of 'trust zones', spatially separated areas, in which a set of vehicles operate. Due to the centralised nature of roadside units, no Sybil attack resistance is provided by the algorithm.

Appendix L.10. Proof-of-Communication [617]

Proof-of-Communication introduces an endorsement scheme in which participant miners receive 'points' for endorsing transactions. The miners with the biggest balance, in turn, earn the right to add a subsequent block. This approach is susceptible to Sybil attacks and would, therefore, likely only be applied in permissioned systems.

Appendix L.11. Proof-of-Driving (PoD) [618]

PoD constitutes a pre-filtering protocol that has the goal of removing malicious actors from a set of potential leaders. Upon finalisation of filtering, the remaining subset participates in a BFT consensus mechanism. Pre-filtering is achieved using a PoS-like reputation system that assigns 'driving tokens', an expression of the distance driven, as stake. A central validating entity is needed to provide the assessment of distance driven in an unspoofable way. Therefore, a permissioned setting and, subsequently, no Sybil attack resistance is assumed.

Appendix L.12. Proof-of-Event with Dynamic Federation [619,620]

In this scheme for accident recording for autonomous vehicles (AVs), a local subgroup of AV nodes in a permissioned network are formed to attest to the plausibility of transaction data and to persist it. While this approach may be subject to Sybil attacks in a permissionless setting, this is not a design goal of this federated protocol.

Appendix L.13. Proof-of-Matching [621]

As a geo-aware consensus mechanism, in Proof-of-Matching AVs constitute nodes on a network and use internal computational resources to participate in the consensus mechanism. Details on how validators form agreement are sparse, but it can be assumed that these would follow a process with BFT characteristics. Therefore, it can be assumed that the set of validators needs to be pre-determined. Consequently, the algorithm would provide no Sybil attack resistance.

Appendix L.14. Proof-of-Nonce [622]

Proof-of-Nonce (PoN) constitutes a pseudorandom leader selection mechanism, deemed suitable for autonomous driving use cases by the authors. As such, it is notably not Sybil attack resistant and relies on the admitting authority of a permissioned system.

Appendix L.15. Proof-of-Quality-Factor (PoQF) [635]

PoQF constitutes a voting-based reputation system in which individual vehicles vote on the validity and quality factor of a message received. While vehicles self-register, 'regulation authorities' maintain the register and can expire accounts at will, thereby rendering the system permissioned.

Appendix L.16. Proof-of-Reputation [623]

Proof-of-Reputation manifests as a two-layer consensus mechanism for IoV scenarios. The main consensus layer is a permissioned network, and the lower layer (termed 'physical layer' by the authors) follows a reputation-based methodology. In this lower layer, vehicles hold reputation values that dictate the likeliness of any transaction proposed by them being included in a block. This reputation value is, presumably, influenceable by the main consensus layer or other off-ledger means. Due to its goal of serving permissioned systems, this mechanism does not provide Sybil attack resistance.

Appendix L.17. Proof-of-Utility [624,625]

During the block verifier selection that is part of proof-of-utility, nodes select a subset of their peers as 'verifiers'. The selection criterion here is the highest possible 'utility', approximated by block verification times. No mechanism to introduce Sybil attack resistance is proposed as the overall scheme is intended for permissioned networks.

Appendix L.18. Proof-of-Vehicular-Services BFT [626]

In this reputation-backed mechanism, individual participants hold a rating based on their 'service providing rate' and 'efficiency'. They are more likely to be selected for mining if they are rated highly. It can be assumed that this mechanism would be applied in permissioned settings and would, therefore, not have to provide Sybil attack resistance. This aligns with the assessment that, in its current form, the mechanism would be vulnerable to Sybil attacks.

Appendix L.19. Proof-of-Work-at-Proximity (PoWaP) [633]

In PoWaP, PoW is not executed on the network level, but within subgroups of nodes in close geographic proximity. This is done with the intention of minimising latency between nodes. The Sybil attack resistance properties are non-obvious, as it is hard to reason about how a global view, combined from smaller PoW systems, that in themselves have incentive compatibility, would manifest. It can, however, be assumed that the Sybil attack resistance are not as strong as those of global PoW, as attackers might target PoWaP by forming geographically concentrated attacks.

Appendix L.20. Reputation-Based DPoS [634]

The proposed consensus mechanism for the vehicular domain follows DPoS mechanics by employing a multi-weight reputation system. Reputation per participant is initialised as a constant and, subsequently, can be updated through interactions with other participants. The selection of miners within the vehicular network is based on these reputation values with a higher reputation value corresponding to a greater chance of being selected as a miner. Complex Sybil attacks would not be preventable by such a reputation system, as a malicious participant could create multiple entities to then undertake manipulative interactions with the goal of increasing the reputation of a single entity.

Appendix L.21. Reputation-Based Miner Node Selection [627]

In this consensus mechanism for vehicles, a reputation system is used to determine which nodes are trustworthy and can be used in the consensus process. The mechanism is designed to automatically remove malicious or compromised nodes from the consensus process: a centralised reputation server applies an artificial neural network to assign repu-

tation values to nodes. The neural network takes numerous factors around the adherence of a node to the protocol into account. Nodes with low reputation are removed from the set of potential validators. This approach requires a central coordinating entity to manage the reputation scores and perform node removal and is, therefore, permissioned. Consequently, no Sybil attack resistance is provided.

Appendix L.22. Secured Event-Information Sharing [628]

As per the proposed system flow outlined by the authors [628] (Figure 2), a central 'cloud server' is responsible for the admission of new entities to the network and their authentication. Therefore, the proposed protocol can be considered to be designed exclusively for permissioned networks, and not to provide Sybil attack resistance.

Appendix L.23. Semi-Autonomous Distributed Blockchain-Based Framework for UAVs [629]

To avoid the computational requirements of common permissionlesss protocols, this blockchain-based framework for UAVs has been proposed by Ge et al. [629]. The proposed protocol employs a 'policy list', an off-ledger store of UAVs with access to the system, thereby rendering it permissioned and devoid of Sybil attack resistance.

Appendix L.24. Time-Oriented Proof of Work [630]

In time-oriented Proof of Work, a leader is selected pseudorandomly based on the minimum hash value received within a given period. This method is proposed with the intention of minimising the risk of forks. It is, however, vulnerable to Sybil attacks due to the random selection of nodes from an unconstrained group of candidates.

Appendix L.25. Voting-Based Consensus Protocol for VANET [631,632]

The protocol proposed by Ayaz et al. [631,632] is a variation of a PBFT protocol that selects the most appropriate node to relay a message based on a reputation system. As such, it is only suited to permissioned systems and does not offer Sybil attack resistance.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 13 June 2021).
2. Chohan, U.W. Crypto Winters. *SSRN Electron. J.* **2022**. [CrossRef]
3. Humayun, M.; Belk, R.W. "Satoshi is Dead. Long Live Satoshi": The Curious Case of Bitcoin's Creator. In *Consumer Culture Theory*; Cross, S.N.N., Ruvalcaba, C., Venkatesh, A., Belk, R.W., Eds.; Emerald Publishing: Bingley, UK, 2018; pp. 19–35. [CrossRef]
4. van Flymen, D. Proof of Work. In *Learn Blockchain by Building One*; Apress: Berkeley, CA, USA, 2020; pp. 39–53. [CrossRef]
5. Narayanan, A.; Clark, J. Bitcoin's academic pedigree. *Commun. ACM* **2017**, *60*, 36–45. [CrossRef]
6. Luebbert, W.F. Commemoration of 1940 Remote Computing Demonstration by Stibitz. *Ann. Hist. Comput.* **1981**, *3*, 68–70.
7. Astrahan, M.M.; Jacobs, J.F. History of the Design of the SAGE Computer-The AN/FSQ-7. *IEEE Ann. Hist. Comput.* **1983**, *5*, 340–349. [CrossRef]
8. Everett, R.R.; Zraket, C.A.; Benington, H.D. SAGE: A data-processing system for air defense. In Proceedings of the Eastern Joint Computer Conference: Computers with Deadlines to Meet on XX—IRE-ACM-AIEE '57 (Eastern), Papers and Discussions Presented at the Washington, DC, USA, 9–13 December 1957; ACM Press: New York, New York, USA, 1958; pp. 148–155. [CrossRef]
9. Adair, R.J.; Bayles, R.U.; Comeau, L.W.; Creasy, R.J. *A Virtual Machine System for the 360/4*; Technical Report; International Business Machines Corporation, Cambridge Scientific Center: Cambridge, MA, USA, 1966.
10. Kleinrock, L. Information Flow in Large Communication Nets. Ph.D. Thesis, Massachu-Setts Institute of Technology, Cambridge, UK, 1961.
11. Marill, T.; Roberts, L.G. Toward a cooperative network of time-shared computers. In Proceedings of the Fall Joint Computer Conference on XX—AFIPS '66 (Fall), San Francisco, CA, USA, 7–10 November 1966; ACM Press: New York, New York, USA, 1966; p. 425. [CrossRef]
12. Cerf, V.; Harslem, E.; Heafner, J.; Metcalfe, R.; White, J. An Experimental Service for Adaptable Data Reconfiguration. *IEEE Trans. Commun.* **1972**, *20*, 557–564. [CrossRef]
13. He, Y.; Siganos, G.; Faloutsos, M. Internet Topology. In *Encyclopedia of Complexity and Systems Science*; Springer: New York, NY, USA, 2009; pp. 4930–4947. [CrossRef]
14. Pease, M.; Shostak, R.; Lamport, L. Reaching Agreement in the Presence of Faults. *J. ACM* **1980**, *27*, 228–234. [CrossRef]

15. Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.* **1982**, *4*, 382–401. [CrossRef]
16. Davenport, R. The state of the art of distributed databases. *Inf. Manag.* **1979**, *2*, 231–247. [CrossRef]
17. Zhang, M.; Xie, Z.; Yue, C.; Zhong, Z. Spitz. *Proc. VLDB Endow.* **2020**, *13*, 3449–3460. [CrossRef]
18. Antonopoulos, P.; Kaushik, R.; Kodavalla, H.; Rosales Aceves, S.; Wong, R.; Anderson, J.; Szymaszek, J. SQL Ledger: Cryptographically Verifiable Data in Azure SQL Database. In *Proceedings of the 2021 International Conference on Management of Data*; ACM: New York, NY, USA, 2021; pp. 2437–2449. [CrossRef]
19. 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, Scitepress, Porto, Portugal, 24–26 April 2017; pp. 755–764. [CrossRef]
20. Platt, M.; Bandara, R.J.; Drăgnoiu, A.E.; Krishnamoorthy, S. Information Privacy in Decentralized Applications. In *Trust Models for Next-Generation Blockchain Ecosystems*; Rehman, M.H.U., Svetinovic, D., Salah, K., Damiani, E., Eds.; EAI/Springer Innovations in Communication and Computing, Springer International Publishing: Cham, Switzerland, 2021. [CrossRef]
21. Platt, M.; McBurney, P. Self-Governing Public Decentralised Systems. In Proceedings of the 10th International Workshop on Socio-Technical Aspects in Security and Trust, Virtual Event, 14 September 2020; Groß, T., Viganò, L., Eds.; Springer: Guildford, UK, 2021; pp. 154–167. [CrossRef]
22. Leising, M. Post-Bitcoin Technology Has Geeks, Giants, and Hackers Excited. Available online: https://www.bloomberg.com/news/articles/2017-03-23/post-bitcoin-technology-has-geeks-giants-and-hackers-excited (accessed on 28 October 2022).
23. Platt, M.; Sedlmeir, J.; Platt, D.; Xu, J.; Tasca, P.; Vadgama, N.; Ibañez, J.I. The Energy Footprint of Blockchain Consensus Mechanisms Beyond Proof-of-Work. In Proceedings of the 21st International Conference on Software Quality, Reliability and Security, Hainan, China, 6–10 December 2021; pp. 1135–1144. [CrossRef]
24. Hellwig, D.; Karlic, G.; Huchzermeier, A. *Build Your Own Blockchain*; Management for Professionals, Springer International Publishing: Cham, Switzerland, 2020. [CrossRef]
25. Lewis, A. *The Basics of Bitcoins and Blockchains*; Mango Publishing: Miami, FL, USA, 2018; p. 408.
26. Xu, X.; Weber, I.; Staples, M. *Architecture for Blockchain Applications*; Springer International Publishing: Cham, Switzerland, 2019. [CrossRef]
27. Gayvoronskaya, T.; Meinel, C. *Blockchain*; Springer International Publishing: Cham, Switzerland, 2021. [CrossRef]
28. Tezel, A.; Papadonikolaki, E.; Yitmen, I.; Hilletofth, P. Preparing construction supply chains for blockchain technology: An investigation of its potential and future directions. *Front. Eng. Manag.* **2020**, *7*, 547–563. [CrossRef]
29. Lapsley, P. Phreaking out ma bell. *IEEE Spectr.* **2013**, *50*, 30–35. [CrossRef]
30. Lukasik, S.J. Protecting users of the cyber commons. *Commun. ACM* **2011**, *54*, 54–61. [CrossRef]
31. Uzunov, A.V.; Fernandez, E.B.; Falkner, K. Securing distributed systems using patterns: A survey. *Comput. Secur.* **2012**, *31*, 681–703. [CrossRef]
32. Douceur, J.R. The Sybil Attack. In Proceedings of the Peer-to-Peer Systems, First International Workshop, IPTPS 2002, Cambridge, MA, USA, 7–8 March 2002; Druschel, P., Kaashoek, F., Rowstron, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2002; pp. 251–260.
33. Dhillon, V.; Metcalf, D.; Hooper, M. The DAO Hacked. In *Blockchain Enabled Applications*; Apress: Berkeley, CA, USA, 2017; pp. 67–78. [CrossRef]
34. Kim, T.W.; Zetlin-Jones, A. The Ethics of Contentious Hard Forks in Blockchain Networks with Fixed Features. *Front. Blockchain* **2019**, *2*. [CrossRef]
35. Aguilera, M.K. Stumbling over Consensus Research: Misunderstandings and Issues. In *Replication*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 59–72. [CrossRef]
36. Gusenbauer, M.; Haddaway, N.R. Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources. *Res. Synth. Methods* **2020**, *11*, 181–217. [CrossRef] [PubMed]
37. Jubb, A.; Carr, E.; Sanderson, A.; Baragula, E.; McCool, R.; Glanville, J. What is the most efficient de-duplication software for use in systematic reviews? *Cochrane Database Syst. Rev.* **2020**, *9*, (*Suppl. 1*). [CrossRef]
38. Sayeed, S.; Marco-Gisbert, H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Appl. Sci.* **2019**, *9*, 1788. [CrossRef]
39. Aggarwal, S.; Kumar, N. Cryptographic consensus mechanisms. In *The Blockchain Technology for Secure and Smart Applications across Industry Verticals*; Aggarwal, S., Kumar, N., Raj, P., Eds.; Elsevier: Amsterdam, The Netherlands, 2021; pp. 211–226. [CrossRef]
40. Aggarwal, A.; Gaba, S.; Mittal, M. A Comparative Investigation of Consensus Algorithms in Collaboration with IoT and Blockchain. In *Transforming Cybersecurity Solutions using Blockchain*; Agrawal, R.; Gupta, N., Eds.; Springer: Singapore, 2021; pp. 115–140. [CrossRef]
41. Ahmad, A.; Saad, M.; Kim, J.; Nyang, D.; Mohaisen, D. Performance Evaluation of Consensus Protocols in Blockchain-based Audit Systems. In Proceedings of the 2021 International Conference on Information Networking (ICOIN), Jeju Island, Korea, 13–16 January 2021; pp. 654–656. [CrossRef]
42. Ali Syed, T.; Alzahrani, A.; Jan, S.; Siddiqui, M.S.; Nadeem, A.; Alghamdi, T. A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations. *IEEE Access* **2019**, *7*, 176838–176869. [CrossRef]

43. Alsaqqa, S.; Almajali, S. Blockchain Technology Consensus Algorithms and Applications: A Survey. *Int. J. Interact. Mob. Technol. (iJIM)* **2020**, *14*, 142. [CrossRef]
44. Alsunaidi, S.J.; Alhaidari, F.A. A Survey of Consensus Algorithms for Blockchain Technology. In Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 3–4 April 2019; pp. 1–6. [CrossRef]
45. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [CrossRef]
46. Andrey, A.; Petr, C. Review of Existing Consensus Algorithms Blockchain. In Proceedings of the 2019 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS), Sochi, Russia, 23–27 September 2019; pp. 124–127. [CrossRef]
47. Antal, C.; Cioara, T.; Anghel, I.; Antal, M.; Salomie, I. Distributed Ledger Technology Review and Decentralized Applications Development Guidelines. *Future Internet* **2021**, *13*, 62. [CrossRef]
48. Azbeg, K.; Ouchetto, O.; Jai Andaloussi, S.; Fetjah, L. An Overview of Blockchain Consensus Algorithms: Comparison, Challenges and Future Directions. In *Advances on Smart and Soft Computing*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 357–369. [CrossRef]
49. Bach, L.M.; Mihaljevic, B.; Zagar, M. Comparative analysis of blockchain consensus algorithms. In Proceedings of the 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 21–25 May 2018; pp. 1545–1550. [CrossRef]
50. Bamakan, S.M.H.; Motavali, A.; Babaei Bondarti, A. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Syst. Appl.* **2020**, *154*, 113385. [CrossRef]
51. Bashar, G.; Hill, G.; Singha, S.; Marella, P.; Dagher, G.G.; Xiao, J. Contextualizing Consensus Protocols in Blockchain: A Short Survey. In Proceedings of the 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Los Angeles, CA, USA, 12–14 December 2019; pp. 190–195. [CrossRef]
52. Belotti, M.; Bozic, N.; Pujolle, G.; Secci, S. A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3796–3838. [CrossRef]
53. Bhutta, M.N.M.; Khwaja, A.A.; Nadeem, A.; Ahmad, H.F.; Khan, M.K.; Hanif, M.A.; Song, H.; Alshamari, M.; Cao, Y. A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access* **2021**, *9*, 61048–61073. [CrossRef]
54. Dabbagh, M.; Choo, K.K.R.; Beheshti, A.; Tahir, M.; Safa, N.S. A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities. *Comput. Secur.* **2021**, *100*, 102078. [CrossRef]
55. Dhaiouir, S.; Assar, S. A Systematic Literature Review of Blockchain-Enabled Smart Contracts: Platforms, Languages, Consensus, Applications and Choice Criteria. In *Research Challenges in Information Science*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 249–266. [CrossRef]
56. Ferdous, M.S.; Chowdhury, M.J.M.; Hoque, M.A. A survey of consensus algorithms in public blockchain systems for crypto-currencies. *J. Netw. Comput. Appl.* **2021**, *182*, 103035. [CrossRef]
57. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. *IEEE Access* **2020**, *8*, 32031–32053. [CrossRef]
58. Fournier, G.; Petrillo, F. Architecting Blockchain Systems. In Proceedings of the 42nd International Conference on Software Engineering Workshops, Seoul, Korea, 27 June–19 July 2020; ACM: New York, NY, USA, 2020; pp. 664–670. [CrossRef]
59. Fu, X.; Wang, H.; Shi, P. A survey of Blockchain consensus algorithms: Mechanism, design and applications. *Sci. China Inf. Sci.* **2021**, *64*, 121101. [CrossRef]
60. Hao, Y.; Li, Y.; Dong, X.; Fang, L.; Chen, P. Performance Analysis of Consensus Algorithm in Private Blockchain. In Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV), Changshu, China, 26–30 June 2018; pp. 280–285. [CrossRef]
61. Hazari, S.S.; Mahmoud, Q.H. Comparative evaluation of consensus mechanisms in cryptocurrencies. *Internet Technol. Lett.* **2019**, *2*, e100. [CrossRef]
62. He, Q.; Guan, N.; Lv, M.; Yi, W. On the Consensus Mechanisms of Blockchain/DLT for Internet of Things. In Proceedings of the 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES), Graz, Austria, 6-8 June 2018; pp. 1–10. [CrossRef]
63. Hellwig, D.; Karlic, G.; Huchzermeier, A. Consensus Mechanisms. In *Build Your Own Blockchain*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 53–74. [CrossRef]
64. Honnavalli, P.B.; Cholin, A.S.; Pai, A.; Anekal, A.D.; Anekal, A.D. A Study on Recent Trends of Consensus Algorithms for Private Blockchain Network. In *Blockchain and Applications*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 31–41. [CrossRef]
65. Indhuja, E.; Venkatesulu, M. A Survey of Blockchain Technology Applications and Consensus Algorithm. In *Sustainable Communication Networks and Application*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 173–187. [CrossRef]
66. Ismail, L.; Materwala, H. A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions. *Symmetry* **2019**, *11*, 1198. [CrossRef]
67. Jayabalan, J.; N, J. A Study on Distributed Consensus Protocols and Algorithms: The Backbone of Blockchain Networks. In Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 27–29 January 2021; pp. 1–10. [CrossRef]

68. Jennath, H.S.; Asharaf, S. Survey on Blockchain Consensus Strategies. In *ICDSMLA 2019*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 637–654. [CrossRef]
69. Katarya, R.; Vats, V.K. A Survey on Blockchain Technologies and Its Consensus Algorithms. In *Recent Innovations in Computing*; Singh, P.K.; Singh, Y.; Kolekar, M.H.; Kar, A.K.; Chhabra, J.K.; Sen, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2021; pp. 741–752. [CrossRef]
70. Kaur, S.; Chaturvedi, S.; Sharma, A.; Kar, J. A Research Survey on Applications of Consensus Protocols in Blockchain. *Secur. Commun. Netw.* **2021**, *2021*, 6693731. [CrossRef]
71. Khamar, J.; Patel, H. An Extensive Survey on Consensus Mechanisms for Blockchain Technology. In *Data Science and Intelligent Applications*; Kotecha, K., Piuri, V., Shah, H.N., Patel, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2021; pp. 363–374. [CrossRef]
72. Lao, L.; Li, Z.; Hou, S.; Xiao, B.; Guo, S.; Yang, Y. A Survey of IoT Applications in Blockchain Systems. *ACM Comput. Surv.* **2021**, *53*, 1–32. [CrossRef]
73. Lashkari, B.; Musilek, P. A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access* **2021**, *9*, 43620–43652. [CrossRef]
74. Lasisi, A.; Hsu, S. Consensus Mechanism in Enterprise Blockchain. In Proceedings of the 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, 1–3 July 2019; pp. 228–228. [CrossRef]
75. Lepore, C.; Ceria, M.; Visconti, A.; Rao, U.P.; Shah, K.A.; Zanolini, L. A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS. *Mathematics* **2020**, *8*, 1782. [CrossRef]
76. MacKenzie, B.; Ferguson, R.I.; Bellekens, X. An Assessment of Blockchain Consensus Protocols for the Internet of Things. In Proceedings of the 2018 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), Hamammet, Tunisia, 20–21 December 2018; pp. 183–190. [CrossRef]
77. Maple, C.; Jackson, J. Selecting Effective Blockchain Solutions. In *Euro-Par 2018: Parallel Processing Workshops*; Mencagli, G., Heras, D.B., Cardellini, V., Casalicchio, E., Jeannot, E., Wolf, F., Salis, A., Schifanella, C., Manumachu, R.R., Ricci, L., et al., Eds.; Springer: Berlin/Heidelberg, Germany, 2019; pp. 392–403. [CrossRef]
78. Masood, F.; Faridi, A.R. Consensus Algorithms In Distributed Ledger Technology For Open Environment. In Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 14–15 December 2018; pp. 1–6. [CrossRef]
79. Masood, F.; Faridi, A.R. Distributed Ledger Technology for Closed Environment. In Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 13–15 March 2019; pp. 1151–1156.
80. Mingxiao, D.; Xiaofeng, M.; Zhe, Z.; Xiangwei, W.; Qijun, C. A review on consensus algorithm of blockchain. In Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 5–8 October 2017; pp. 2567–2572. [CrossRef]
81. Monrat, A.A.; Schelen, O.; Andersson, K. A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access* **2019**, *7*, 117134–117151. [CrossRef]
82. Naz, S.; Lee, S.U.J. Why the new consensus mechanism is needed in blockchain technology? In Proceedings of the 2020 Second International Conference on Blockchain Computing and Applications (BCCA), Antalya, Turkey, 2–5 November 2020; pp. 92–99. [CrossRef]
83. Nguyen, G.T.; Kim, K. A Survey about Consensus Algorithms Used in Blockchain. *J. Inf. Process. Syst.* **2018**, *14*, 101–128. [CrossRef]
84. Nijsse, J.; Litchfield, A. A Taxonomy of Blockchain Consensus Methods. *Cryptography* **2020**, *4*, 32. [CrossRef]
85. Pahlajani, S.; Kshirsagar, A.; Pachghare, V. Survey on Private Blockchain Consensus Algorithms. In Proceedings of the 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), Chennai, India, 25–26 April 2019; pp. 1–6. [CrossRef]
86. Panda, S.S.; Mohanta, B.K.; Satapathy, U.; Jena, D.; Gountia, D.; Patra, T.K. Study of Blockchain Based Decentralized Consensus Algorithms. In Proceedings of the TENCON 2019—2019 IEEE Region 10 Conference (TENCON), Kochi, India, 17–20 October 2019, pp. 908–913. [CrossRef]
87. Perez, M.R.L.; Lagman, A.C.; Legaspi, J.B.C.; De Angel, R.D.M.; Awat, K.A.S. Suitability of IoT to Blockchain Network based on Consensus Algorithm. In Proceedings of the 2019 IEEE 11th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM), Laoag, Philippines, 29 November–1 December 2019; pp. 1–5. [CrossRef]
88. Praveen, G.; Anand, M.; Singh, P.K.; Ranjan, P. An Overview of Blockchain Consensus and Vulnerability. In *Information and Communication Technology for Intelligent Systems*; Senjyu, T., Mahalle, P.N., Perumal, T., Joshi, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2021; pp. 459–468. [CrossRef]
89. Ramkumar, N.; Sudhasadasivam, G.; Saranya, K. A Survey on Different Consensus Mechanisms for the Blockchain Technology. In Proceedings of the 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 28–30 July 2020; pp. 458–464. [CrossRef]
90. Sharma, K.; Jain, D. Consensus Algorithms in Blockchain Technology: A Survey. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 6–8 July 2019; pp. 1–7. [CrossRef]

91. Srivastav, R.K.; Agrawal, D.; Shrivastava, A. A Survey on Vulnerabilities and Performance Evaluation Criteria in Blockchain Technology. *ADCAIJ Adv. Distrib. Comput. Artif. Intell. J.* **2020**, *9*, 91–105. [CrossRef]
92. Verma, N.; Jain, S.; Doriya, R. Review on Consensus Protocols for Blockchain. In Proceedings of the 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 19–20 February 2021; pp. 281–286. [CrossRef]
93. Wang, Q.; Huang, J.; Wang, S.; Chen, Y.; Zhang, P.; He, L. A Comparative Study of Blockchain Consensus Algorithms. *J. Phys. Conf. Ser.* **2020**, *1437*, 012007. [CrossRef]
94. Wazid, M.; Das, A.K.; Shetty, S.; Jo, M. A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things. *IEEE Access* **2020**, *8*, 88700–88716. [CrossRef]
95. Xiao, Y.; Zhang, N.; Li, J.; Lou, W.; Hou, Y.T. Distributed Consensus Protocols and Algorithms. In *Blockchain for Distributed Systems Security*; Wiley: Hoboken, NJ, USA, 2019; pp. 25–50. [CrossRef]
96. Xiao, Y.; Zhang, N.; Lou, W.; Hou, Y.T. A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1432–1465. [CrossRef]
97. Yin, H.; Wei, Y.; Li, Y.; Zhu, L.; Shi, J.; Gai, K. Consensus in Lens of Consortium Blockchain: An Empirical Study. In *Algorithms and Architectures for Parallel Processing*; Qiu, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 282–296. [CrossRef]
98. Yousuf, R.; Jeelani, Z.; Khan, D.A.; Bhat, O.; Teli, T.A. Consensus Algorithms in Blockchain-Based Cryptocurrencies. In Proceedings of the 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 19–20 February 2021; pp. 1–6. [CrossRef]
99. Zhang, S.; Lee, J.H. Analysis of the main consensus protocols of blockchain. *ICT Express* **2020**, *6*, 93–97. [CrossRef]
100. Zhao, W.; Yang, S.; Luo, X. On Consensus in Public Blockchains. In Proceedings of the 2019 International Conference on Blockchain Technology, Atlanta, GA, USA, 14–17 July 2019; ACM: New York, NY, USA, 2019; pp. 1–5. [CrossRef]
101. Dhillon, A.; Kotsialou, G.; McBurney, P.; Riley, L. Voting over a Distributed Ledger: An Interdisciplinary Perspective. *Found. Trends Microeconomics* **2021**, *12*, 200–268. [CrossRef]
102. Abuidris, Y.; Kumar, R.; Yang, T.; Onginjo, J. Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. *ETRI J.* **2021**, *43*, 357–370. [CrossRef]
103. Tozzi, C. Decentralizing democracy: Approaches to consensus within blockchain communities. *Teknokultura Rev. Cult. Digit. Movimientos Soc.* **2019**, *16*, 181–195. [CrossRef]
104. Brenzikofer, A. Encointer—Local Community Cryptocurrencies with Universal Basic Income. *arXiv* **2019**, arXiv:1912.12141.
105. Borge, M.; Kokoris-Kogias, E.; Jovanovic, P.; Gasser, L.; Gailly, N.; Ford, B. Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France, 26–28 April 2017; pp. 23–26. [CrossRef]
106. Poupko, O.; Talmon, N. A Consensus Protocol for e-Democracy. *arXiv* **2020**, arXiv:2007.15949.
107. Crain, T.; Gramoli, V.; Larrea, M.; Raynal, M. DBFT: Efficient Leaderless Byzantine Consensus and its Application to Blockchains. In Proceedings of the 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 1–3 November 2018; pp. 1–8. [CrossRef]
108. Steiu, M.F. Blockchain in education: Opportunities, applications, and challenges. *First Monday* **2020**, *25*. [CrossRef]
109. Hsu, C.H.; Alavi, A.H.; Li, H. Guest Editorial: Blockchain in Smart Education. *Educ. Technol. Soc.* **2022**, *25*, 71–73.
110. Wang, B.; Hu, Y.; Li, S.; Niu, J. A Blockchain Consensus Mechanism for Educational Administration System. In Proceedings of the 2019 IEEE 2nd International Conference on Electronics Technology (ICET), Chengdu, China, 10–13 May 2019; pp. 603–608. [CrossRef]
111. Qin, D.; Wang, C.; Jiang, Y. RPchain: A Blockchain-Based Academic Social Networking Service for Credible Reputation Building. In *Blockchain—ICBC 2018*; Chen, S.; Wang, H.; Zhang, L.J., Eds.; Springer: Berlin/Heidelberg, Germany, 2018; pp. 183–198. [CrossRef]
112. Liu, X. Exploration & Research on Distance Education System Based on Blockchain Technology. *J. Phys. Conf. Ser.* **2021**, *1769*, 012041. [CrossRef]
113. Brilliantova, V.; Thurner, T.W. Blockchain and the future of energy. *Technol. Soc.* **2019**, *57*, 38–45. . [CrossRef]
114. Wang, N.; Zhou, X.; Lu, X.; Guan, Z.; Wu, L.; Du, X.; Guizani, M. When Energy Trading Meets Blockchain in Electrical Power System: The State of the Art. *Appl. Sci.* **2019**, *9*, 1561. [CrossRef]
115. Hasan, M.K.; Alkhalifah, A.; Islam, S.; Babiker, N.B.M.; Habib, A.K.M.A.; Aman, A.H.M.; Hossain, M.A. Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9065768. [CrossRef]
116. Fu, X.; Wang, H.; Wang, Z. Research on Block-Chain-Based Intelligent Transaction and Collaborative Scheduling Strategies for Large Grid. *IEEE Access* **2020**, *8*, 151866–151877. [CrossRef]
117. Hu, B.; Zhou, C.; Tian, Y.C.; Hu, X.; Junping, X. Decentralized Consensus Decision-Making for Cybersecurity Protection in Multimicrogrid Systems. *IEEE Trans. Syst. Man, Cybern. Syst.* **2021**, *51*, 2187–2198. [CrossRef]
118. Montakhabi, M.; Zobiri, F.; van der Graaf, S.; Deconinck, G.; Orlando, D.; Ballon, P.; Mustafa, M.A. An Ecosystem View of Peer-to-Peer Electricity Trading: Scenario Building by Business Model Matrix to Identify New Roles. *Energies* **2021**, *14*, 4438. [CrossRef]

119. Hu, M.; Shen, T.; Men, J.; Yu, Z.; Liu, Y. CRSM: An Effective Blockchain Consensus Resource Slicing Model for Real-Time Distributed Energy Trading. *IEEE Access* **2020**, *8*, 206876–206887. [CrossRef]
120. Guo, J.; Ding, X.; Wu, W. A Blockchain-Enabled Ecosystem for Distributed Electricity Trading in Smart City. *IEEE Internet Things J.* **2021**, *8*, 2040–2050. [CrossRef]
121. Cai, W.; Jiang, W.; Xie, K.; Zhu, Y.; Liu, Y.; Shen, T. Dynamic reputation–based consensus mechanism: Real-time transactions for energy blockchain. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 155014772090733. [CrossRef]
122. Huh, J.H.; Kim, S.K. The Blockchain Consensus Algorithm for Viable Management of New and Renewable Energies. *Sustainability* **2019**, *11*, 3184. [CrossRef]
123. Liu, Q.; Tong, B.; Li, D.; Lu, Y.; Fu, Y.; Chen, L.; Zhao, K. An Integrated Energy Service Transaction Model Based on Energy Blockchain. *Int. J. Heat Technol.* **2020**, *38*, 293–300. [CrossRef]
124. Jiang, L.; Xie, S.; Maharjan, S.; Zhang, Y. Blockchain Empowered Wireless Power Transfer for Green and Secure Internet of Things. *IEEE Netw.* **2019**, *33*, 164–171. [CrossRef]
125. Wang, L.; Wu, J.; Yuan, R.; Zhang, D.; Liu, J.; Jiang, S.; Zhang, Y.; Li, M. Dynamic Adaptive Cross-Chain Trading Mode for Multi-Microgrid Joint Operation. *Sensors* **2020**, *20*, 6096. [CrossRef] [PubMed]
126. Moniruzzaman, M.; Yassine, A.; Benlamri, R. Blockchain-based Mechanisms for Local Energy Trading in Smart Grids. In Proceedings of the 2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT), Charlotte, NC, USA, 6–9 October 2019; pp. 110–114. [CrossRef]
127. Olivares-Rojas, J.C.; Reyes-Archundia, E.; Gutierrez-Gnecchi, J.A.; Cerda-Jacobo, J.; Gonzalez-Murueta, J.W. A Novel Multitier Blockchain Architecture to Protect Data in Smart Metering Systems. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1271–1284. [CrossRef]
128. Zhao, F.; Guo, X.; Chan, W.K.V. Individual Green Certificates on Blockchain: A Simulation Approach. *Sustainability* **2020**, *12*, 3942. [CrossRef]
129. Yahaya, A.S.; Javaid, N.; Javed, M.U.; Shafiq, M.; Khan, W.Z.; Aalsalem, M.Y. Blockchain-Based Energy Trading and Load Balancing Using Contract Theory and Reputation in a Smart Community. *IEEE Access* **2020**, *8*, 222168–222186. [CrossRef]
130. Guan, Z.; Lu, X.; Yang, W.; Wu, L.; Wang, N.; Zhang, Z. Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid. *J. Parallel Distrib. Comput.* **2021**, *147*, 34–45. [CrossRef]
131. Chowdhury, M.J.M.; Usman, M.; Ferdous, M.S.; Chowdhury, N.; Harun, A.I.; Jannat, U.S.; Biswas, K. A Cross-Layer Trust-Based Consensus Protocol for Peer-to-Peer Energy Trading Using Fuzzy Logic. *IEEE Internet Things J.* **2022**, *9*, 14779–14789. [CrossRef]
132. Keshk, M.; Turnbull, B.; Moustafa, N.; Vatsalan, D.; Choo, K.K.R. A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks. *IEEE Trans. Ind. Inform.* **2020**, *16*, 5110–5118. [CrossRef]
133. Bansal, G.; Bhatia, A. A Fast, Secure and Distributed Consensus Mechanism for Energy Trading Among Vehicles using Hashgraph. In Proceedings of the 2020 International Conference on Information Networking (ICOIN), Barcelona, Spain, 7–10 January 2020; pp. 772–777. [CrossRef]
134. Khalid, R.; Samuel, O.; Javaid, N.; Aldegheishem, A.; Shafiq, M.; Alrajeh, N. A Secure Trust Method for Multi-Agent System in Smart Grids Using Blockchain. *IEEE Access* **2021**, *9*, 59848–59859. [CrossRef]
135. Liu, N.; Tan, L.; Zhou, L.; Chen, Q. Multi-party Energy Management of Energy Hub: A Hybrid Approach with Stackelberg Game and Blockchain. *J. Mod. Power Syst. Clean Energy* **2020**, *8*, 919–928. [CrossRef]
136. Lu, X.; Guan, Z.; Zhou, X.; Wu, L.; Du, X.; Guizani, M. An Efficient and Privacy-Preserving Energy Trading Scheme Based on Blockchain. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6. [CrossRef]
137. Liu, C.; Chai, K.K.; Zhang, X.; Chen, Y. Proof-of-Benefit: A Blockchain-Enabled EV Charging Scheme. In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–6. [CrossRef]
138. Liu, H.; Zhang, Y.; Yang, T. Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing. *IEEE Netw.* **2018**, *32*, 78–83. [CrossRef]
139. Liu, C.; Chai, K.K.; Zhang, X.; Chen, Y. Peer-to-peer electricity trading system: Smart contracts based proof-of-benefit consensus protocol. *Wirel. Netw.* **2021**, *27*, 4217–4228. [CrossRef]
140. Liu, C.; Chai, K.K.; Zhang, X.; Chen, Y. Enhanced Proof-of-Benefit: A Secure Blockchain-Enabled EV Charging System. In Proceedings of the 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 22–25 September 2019; pp. 1–6. [CrossRef]
141. Ling, X.; Gao, Z.; Le, Y.; You, L.; Wang, J.; Ding, Z.; Gao, X. Satellite-Aided Consensus Protocol for Scalable Blockchains. *Sensors* **2020**, *20*, 5616. [CrossRef]
142. Dwork, C.; Naor, M. Pricing via Processing or Combatting Junk Mail. In *Advances in Cryptology—CRYPTO' 92*; Brickell, E.F., Ed.; Springer: Berlin/Heidelberg, Germany, 1992; pp. 139–147. [CrossRef]
143. QuantumMechanic. Proof of Stake Instead of Proof of Work. Available online: https://bitcointalk.org/index.php?topic=27787.0 (accessed on 26 October 2022).
144. Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI '99), New Orleans, LA, USA, 22–25 February 1999; pp. 173–186.
145. Larimer, D. DPOS Consensus Algorithm—The Missing White Paper. Available online: https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper (accessed on 27 October 2022).

146. Intel. PoET 1.0 Specification. Available online: https://sawtooth.hyperledger.org/docs/core/releases/1.0/architecture/poet.html (accessed on 10 October 2021).
147. Dziembowski, S.; Faust, S.; Kolmogorov, V.; Pietrzak, K. Proofs of Space. In *Advances in Cryptology—CRYPTO 2015*; Gennaro, R., Robshaw, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; pp. 585–605. [CrossRef]
148. Stewart, I. Proof of Burn. Available online: https://en.bitcoin.it/wiki/Proof{_}of{_}burn (accessed on 26 October 2022).
149. Bentov, I.; Lee, C.; Mizrahi, A.; Rosenfeld, M. Proof of Activity. *ACM Sigmetrics Perform. Eval. Rev.* **2014**, *42*, 34–37. [CrossRef]
150. NEM. Harvesting. Available online: https://nem.io/xem/harvesting-and-poi/ (accessed on 13 May 2020).
151. Ongaro, D.; Ousterhout, J. In Search of an Understandable Consensus Algorithm. In Proceedings of the 2014 USENIX Annual Technical Conference (USENIX ATC 14), Philadelphia, PA, USA, 19–20 June 2014; USENIX Association: Philadelphia, PA, USA, 2014; pp. 305–319.
152. Milutinovic, M.; He, W.; Wu, H.; Kanwal, M. Proof of Luck. In Proceedings of the Proceedings of the 1st Workshop on System Software for Trusted Execution, Trento, Italy, 12–16 December 2016; ACM: New York, NY, USA, 2016; pp. 1–6. [CrossRef]
153. Ahmed-Rengers, M.; Kostiainen, K. Don't Mine, Wait in Line: Fair and Efficient Blockchain Consensus with Robust Round Robin. *arXiv* **2018**. arXiv:1804.07391.
154. Chen, X.; Zhao, S.; Qi, J.; Jiang, J.; Song, H.; Wang, C.; Li, T.O.; Chan, T.H.H.; Zhang, F.; Luo, X.; et al. Efficient and DoS-resistant Consensus for Permissioned Blockchains *arXiv*, **2018**, arXiv:1808.02252.
155. Carlyle, J.; Malene, T.; Manai, C.; Shah, N.; Thomas, G.; Willis, R. Obscuro. Available online: https://whitepaper.obscu.ro/assets/images/obscuro-whitepaper-0-10-0.pdf (accessed on 27 October 2022).
156. Bashar, G.D.; Avila, A.A.; Dagher, G.G. PoQ: A Consensus Protocol for Private Blockchains Using Intel SGX. In *Security and Privacy in Communication Networks*; Park, N., Sun, K., Foresti, S., Butler, K., Saxena, N., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 141–160. [CrossRef]
157. Andreina, S.; Bohli, J.M.; Karame, G.O.; Li, W.; Marson, G.A. PoTS: A Secure Proof of TEE-Stake for Permissionless Blockchains. *IEEE Trans. Serv. Comput.* **2022**, *15*, 2173–2187. [CrossRef]
158. Martin, J.P.; Jung, E. Rationality-proof consensus: Extended abstract. *arXiv* **2018**, arXiv:1811.00742.
159. Auvolat, A.; Bromberg, Y.D.; Frey, D.; Taïani, F. BASALT: A Rock-Solid Foundation for Epidemic Consensus Algorithms in Very Large, Very Open Networks. *arXiv* **2021**, arXiv:2102.04063.
160. Cong, X.; Zi, L.; Du, D.Z. DTNB: A Blockchain Transaction Framework With Discrete Token Negotiation for the Delay Tolerant Network. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 1584–1599. [CrossRef]
161. Cabellos Aparicio, A. Design and Implementation of a Proof-of-Stake Consensus Algorithm for Blockchain. Ph.D. Thesis, UPC Universitat Politècnica de Catalunya, Barcelona, Spain, 2018.
162. Martinez, M.; Hekmati, A.; Krishnamachari, B.; Yun, S. Mobile Encounter-based Social Sybil Control. In Proceedings of the 2020 Seventh International Conference on Software Defined Systems (SDS), Paris, France, 20–23 April 2020; pp. 190–195. [CrossRef]
163. Chatzopoulos, D.; Gujar, S.; Faltings, B.; Hui, P. LocalCoin. In Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Paderborn, Germany, 5–8 July 2016; ACM: New York, NY, USA, 2016; pp. 365–366. [CrossRef]
164. Pournaras, E. Proof of witness presence: Blockchain consensus for augmented democracy in smart cities. *J. Parallel Distrib. Comput.* **2020**, *145*, 160–175. [CrossRef]
165. Chatzopoulos, D.; Gujar, S.; Faltings, B.; Hui, P. Mneme: A Mobile Distributed Ledger. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications, Toronto, ON, Canada, 6–9 July 2020; pp. 1897–1906. [CrossRef]
166. Amoretti, M.; Brambilla, G.; Medioli, F.; Zanichelli, F. Blockchain-Based Proof of Location. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 146–153. [CrossRef]
167. Jiang, Z.; Cao, Z.; Krishnamachari, B.; Zhou, S.; Niu, Z. SENATE: A Permissionless Byzantine Consensus Protocol in Wireless Networks for Real-Time Internet-of-Things Applications. *IEEE Internet Things J.* **2020**, *7*, 6576–6588. [CrossRef]
168. Longo, R.; Podda, A.S.; Saia, R. Analysis of a Consensus Protocol for Extending Consistent Subchains on the Bitcoin Blockchain. *Computation* **2020**, *8*, 67. [CrossRef]
169. Berrang, P.; von Styp-Rekowsky, P.; Wissfeld, M.; Franca, B.; Trinkler, R. Albatross—An optimistic consensus algorithm. In Proceedings of the 2019 Crypto Valley Conference on Blockchain Technology (CVCBT), Rotkreuz, Switzerland, 24–26 June 2019; pp. 39–42. [CrossRef]
170. Azouvi, S.; McCorry, P.; Meiklejohn, S. Betting on Blockchain Consensus with Fantômette. *arXiv* **2018**, arXiv:1805.06786.
171. Mckinnon, T. MaGPoS—A novel decentralized consensus mechanism combining magnetism and proof of stake. *arXiv* **2019**, arXiv:1906.08176.
172. Jiang, Y.; Cheng, X.; Zhu, J.; Xu, Y. A consensus mechanism based on multi-round concession negotiation. *Comput. Stand. Interfaces* **2021**, *74*, 103488. [CrossRef]
173. Davarpanah, K.; Kaufman, D.; Pubellier, O. NeuCoin: The First Secure, Cost-efficient and Decentralized Cryptocurrency. *arXiv* **2015**, arXiv:1503.07768.
174. Adewumi, T.P.; Liwicki, M. Inner For-Loop for Speeding Up Blockchain Mining. *Open Comput. Sci.* **2020**, *10*, 42–47. [CrossRef]

175. Kang, J.; Xiong, Z.; Jiang, C.; Liu, Y.; Guo, S.; Zhang, Y.; Niyato, D.; Leung, C.; Miao, C. Scalable and Communication-Efficient Decentralized Federated Edge Learning with Multi-blockchain Framework. In *Blockchain and Trustworthy Systems*; Zheng, Z., Dai, H.N., Fu, X., Chen, B., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 152–165. [CrossRef]
176. Kim, D.H.; Ullah, R.; Kim, B.S. RSP Consensus Algorithm for Blockchain. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019; pp. 1–4. [CrossRef]
177. Shin, H.; Son, K.; Han, D. Sybil Tolerant Consensus Method Using Mutual Proof of Validation. In Proceedings of the 2020 2nd International Electronics Communication Conference, Singapore, 8–10 July 2020; ACM: New York, NY, USA, 2020; pp. 1–8. [CrossRef]
178. Mu, Y.; Chen, W.; Liang, X.; Gao, Y. A Weak Centralized Consensus Mechanism with More Incentive Effects. *J. Phys. Conf. Ser.* **2019**, *1302*, 032037. [CrossRef]
179. Das, D. Toward Next Generation of Blockchain Using Improvized Bitcoin-NG. *IEEE Trans. Comput. Soc. Syst.* **2021**, *8*, 512–521. [CrossRef]
180. Meneghetti, A.; Sala, M.; Taufer, D. A New ECDLP-Based PoW Model. *Mathematics* **2020**, *8*, 1344. [CrossRef]
181. Gilad, Y.; Hemo, R.; Micali, S.; Vlachos, G.; Zeldovich, N. Algorand. In Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai China, 28 October 2017; ACM: New York, NY, USA, 2017; pp. 51–68. [CrossRef]
182. Cheng, Y.; Hu, X.; Zhang, J. An Improved Scheme of Proof-of-Stake Consensus Mechanism. In Proceedings of the 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Hohhot, China, 24–26 October 2019; pp. 826–8263. [CrossRef]
183. Deuber, D.; Döttling, N.; Magri, B.; Malavolta, G.; Thyagarajan, S.A.K. Minting Mechanism for Proof of Stake Blockchains. In *Applied Cryptography and Network Security*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 315–334. [CrossRef]
184. Leonardos, S.; Reijsbergen, D.; Piliouras, G. Weighted Voting on the Blockchain: Improving Consensus in Proof of Stake Protocols. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 376–384. [CrossRef]
185. Leonardos, S.; Reijsbergen, D.; Piliouras, G. Weighted voting on the blockchain: Improving consensus in proof of stake protocols. *Int. J. Netw. Manag.* **2020**, *30*, e2093. [CrossRef]
186. Dotan, M.; Tochner, S. Proofs of Useless Work—Positive and Negative Results for Wasteless Mining Systems. *arXiv* **2020**, arXiv:2007.01046.
187. Kim, H.; Kim, K.; Kwon, H.; Seo, H. ASIC-Resistant Proof of Work Based on Power Analysis of Low-End Microcontrollers. *Mathematics* **2020**, *8*, 1343. [CrossRef]
188. Chen, L.; Xu, L.; Gao, Z.; Lu, Y.; Shi, W. Protecting Early Stage Proof-of-Work Based Public Blockchain. In Proceedings of the 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Luxembourg, 25–28 June 2018; pp. 122–127. [CrossRef]
189. Janjanam, M.B.; Pinnamaneni, S.P.; Atmakuri, P. An Efficient Proof-of-Work Mechanism for Computational Feasibility in Blockchain. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 820–821. [CrossRef]
190. Chou, C.N.; Lin, Y.J.; Chen, R.; Chang, H.Y.; Tu, I.P.; Liao, S.W. Personalized Difficulty Adjustment for Countering the Double-Spending Attack in Proof-of-Work Consensus Protocols. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1456–1462. [CrossRef]
191. Aggarwal, D.; Brennen, G.; Lee, T.; Santha, M.; Tomamichel, M. Quantum Attacks on Bitcoin, and How to Protect Against Them. *Ledger* **2018**, *3*. [CrossRef]
192. Sharkey, S.; Tewari, H. Alt-PoW: An Alternative Proof-of-Work Mechanism. In Proceedings of the 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA, 4–9 April 2019; pp. 11–18. [CrossRef]
193. Kitakami, M.; Matsuoka, K. An Attack-Tolerant Agreement Algorithm for Block Chain. In Proceedings of the 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), Taipei, Taiwan, 4–7 December 2018; pp. 227–228. [CrossRef]
194. Liu, G.; Dong, H.; Yan, Z.; Zhou, X.; Shimizu, S. B4SDC: A Blockchain System for Security Data Collection in MANETs. *IEEE Trans. Big Data* **2022**, *8*, 739–752. [CrossRef]
195. Memon, M.; Bajwa, U.A.; Ikhlas, A.; Memon, Y.; Memon, S.; Malani, M. Blockchain Beyond Bitcoin: Block Maturity Level Consensus Protocol. In Proceedings of the 2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS), Bangkok, Thailand, 22–23 November 2018; pp. 1–5. [CrossRef]
196. Jain, S.; Simha, R. Blockchain for the Common Good: A Digital Currency for Citizen Philanthropy and Social Entrepreneurship. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1387–1394. [CrossRef]
197. de Oliveira, M.T.; Reis, L.H.; Medeiros, D.S.; Carrano, R.C.; Olabarriaga, S.D.; Mattos, D.M. Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications. *Comput. Netw.* **2020**, *179*, 107367. [CrossRef]
198. Bissias, G.; Levine, B.N. Bobtail: A Proof-of-Work Target that Minimizes Blockchain Mining Variance. *arXiv* **2017**, arXiv:1709.08750.

199. Bentov, I.; Gabizon, A.; Mizrahi, A. Cryptocurrencies without Proof of Work. In *Financial Cryptography and Data Security*; Clark, J., Meiklejohn, S., Ryan, P.Y., Wallach, D., Brenner, M., Rohloff, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; pp. 142–157. [CrossRef]
200. Ravindran, R. Circle of Trust: A High Volume, Energy Efficient, Stake Blind and High Attack Tolerant Blockchain Consensus Protocol. In Proceedings of the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 16–18 January 2019; pp. 1–4. [CrossRef]
201. Baudlet, M.; Fall, D.; Taenaka, Y.; Kadobayashi, Y. The Best of Both Worlds: A New Composite Framework Leveraging PoS and PoW for Blockchain Security and Governance. In Proceedings of the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 28–30 September 2020; pp. 17–24. [CrossRef]
202. Li, C.; Li, P.; Zhou, D.; Yang, Z.; Wu, M.; Yang, G.; Xu, W.; Long, F.; Yao, A.C.C. A Decentralized Blockchain with High Throughput and Fast Confirmation. In Proceedings of the 2020 USENIX Annual Technical Conference (USENIX ATC 20), USENIX Association, Philadelphia, PA, USA, 15–17 July 2020; pp. 515–528.
203. Muller, M.; Rodriguez Garzon, S.; Kupper, A. COST: A Consensus-Based Oracle Protocol for the Secure Trade of Digital Goods. In Proceedings of the 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Oxford, UK, 3–6 August 2020; pp. 72–81. [CrossRef]
204. Boyen, X.; Carr, C.; Haines, T. Graphchain. In Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts—BCC '18, Incheon, Korea, 4 June 2018; ACM Press: New York, NY, USA, 2018; pp. 21–33. [CrossRef]
205. Hu, Z.; Du, Y.; Rao, C.; Goh, M. Delegated Proof of Reputation Consensus Mechanism for Blockchain-Enabled Distributed Carbon Emission Trading System. *IEEE Access* **2020**, *8*, 214932–214944. [CrossRef]
206. Do, T.; Nguyen, T.; Pham, H. Delegated Proof of Reputation. In Proceedings of the 2019 International Electronics Communication Conference, Okinawa, Japan, 7–9 July 2019; ACM: New York, NY, USA, 2019; pp. 90–98. [CrossRef]
207. Biryukov, A.; Khovratovich, D. Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem. *Ledger* **2017**, *2*, 1–30. [CrossRef]
208. Jung, H.; Lee, H.N. ECCPoW: Error-Correction Code based Proof-of-Work for ASIC Resistance. *Symmetry* **2020**, *12*, 988. [CrossRef]
209. Hsueh, C.W.; Chin, C.T. EPoW: Solving blockchain problems economically. In Proceedings of the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), San Francisco, CA, USA, 4–8 August 2017; pp. 1–8. [CrossRef]
210. Nakahara, R.; Inaba, H. Proposal of Fair Proof-of-Work System Based on Rating of User's Computing Power. In Proceedings of the 2018 IEEE 7th Global Conference on Consumer Electronics (GCCE), Nara, Japan, 9–12 October 2018; pp. 746–748. [CrossRef]
211. Wan, C.; Tang, S.; Zhang, Y.; Pan, C.; Liu, Z.; Long, Y.; Liu, Z.; Yu, Y. Goshawk: A Novel Efficient, Robust and Flexible Blockchain Protocol. In *Information Security and Cryptology*; Guo, F., Huang, X., Yung, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2019; pp. 49–69. [CrossRef]
212. Lasla, N.; Al-Sahan, L.; Abdallah, M.; Younis, M. Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm. *Comput. Netw.* **2022**, *214*, 109118. [CrossRef]
213. Harvilla, M.; Du, J. Prospective Hybrid Consensus for Project PAI. *arXiv* **2019** arXiv:1902.02469.
214. Liu, Z.; Tang, S.; Chow, S.S.; Liu, Z.; Long, Y. Fork-free hybrid consensus with flexible Proof-of-Activity. *Future Gener. Comput. Syst.* **2019**, *96*, 515–524. [CrossRef]
215. Liu, W.; Li, Y.; Wang, X.; Peng, Y.; She, W.; Tian, Z. A donation tracing blockchain model using improved DPoS consensus algorithm. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 2789–2800. [CrossRef]
216. Chepurnoy, A. Interactive Proof-of-stake. *arXiv* **2016**, arXiv:1601.00275.
217. Feng, W.; Yan, Z. MCS-Chain: Decentralized and trustworthy mobile crowdsourcing based on blockchain. *Future Gener. Comput. Syst.* **2019**, *95*, 649–666. [CrossRef]
218. Pang, Y. A New Consensus Protocol for Blockchain Interoperability Architecture. *IEEE Access* **2020**, *8*, 153719–153730. [CrossRef]
219. Xu, Y.; Huang, Y. MWPoW: Multiple Winners Proof of Work Protocol, a Decentralisation Strengthened Fast-Confirm Blockchain Protocol. *Secur. Commun. Netw.* **2019**, *2019*, 3674274. [CrossRef]
220. Dubrovsky, M.; Ball, M.; Penkovsky, B. Optical Proof of Work. *arXiv* **2019**, arXiv:1911.05193.
221. Hazari, S.S.; Mahmoud, Q.H. A Parallel Proof of Work to Improve Transaction Speed and Scalability in Blockchain Systems. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 916–921. [CrossRef]
222. Kaci, A.; Rachedi, A. PoolCoin: Toward a distributed trust model for miners' reputation management in blockchain. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020; pp. 1–6. [CrossRef]
223. Bagaria, V.; Kannan, S.; Tse, D.; Fanti, G.; Viswanath, P. Prism. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; ACM: New York, NY, USA, 2019; pp. 585–602. [CrossRef]
224. Xue, T.; Yuan, Y.; Ahmed, Z.; Moniz, K.; Cao, G.; Wang, C. Proof of Contribution: A Modification of Proof of Work to Increase Mining Efficiency. In Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 July 2018; pp. 636–644. [CrossRef]

225. Masseport, S.; Darties, B.; Giroudeau, R.; Lartigau, J. Proof of Experience: Empowering Proof of Work protocol with miner previous work. In Proceedings of the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 28–30 September 2020; pp. 57–58. [CrossRef]
226. Monem, M.; Ahmad, A.; Jumana.; Ahmed, R.; Arif, H. Efficient Blockchain System based on Proof of Segmented Work. In Proceedings of the 2020 IEEE Region 10 Symposium (TENSYMP), Dhaka, Bangladesh, 5–7 June 2020; pp. 989–992. [CrossRef]
227. Masseport, S.; Lartigau, J.; Darties, B.; Giroudeau, R. Proof of usage: User-centric consensus for data provision and exchange. *Ann. Telecommun.* **2020**, *75*, 153–162. [CrossRef]
228. Komiya, K.; Nakajima, T. Increasing Motivation for Playing Blockchain Games Using Proof-of-Achievement Algorithm. In *HCI in Games*; Fang, X., Ed.; Springer: Berlin/Heidelberg, Germany, 2019; pp. 125–140. [CrossRef]
229. Grollemund, P.M.; Lafourcade, P.; Thiry-Atighehchi, K.; Tichit, A. Proof of Behavior. In *Open Access Series in Informatics (OASIcs), Proceedings of the 2nd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2020), Toulouse, France, 26–27 October 2020*; Anceaume, E., Bisière, C., Bouvard, M., Bramas, Q., Casamatta, C., Eds.; Schloss Dagstuhl–Leibniz-Zentrum für Informatik: Dagstuhl, Germany, 2021; Volume 82, pp. 11:1–11:6. [CrossRef]
230. Abramowicz, M. Autonocoin: A Proof-of-Belief Cryptocurrency. *Ledger* **2016**, *1*, 119–133. [CrossRef]
231. Chan, W.K.; Chin, J.J.; Goh, V.T. Proof of Bid as Alternative to Proof of Work. In *Advances in Cyber Security*; Anbar, M., Abdullah, N., Manickam, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 60–73. [CrossRef]
232. Hu, Q.; Wang, W.; Bai, X.; Jin, S.; Jiang, T. Blockchain Enabled Federated Slicing for 5G Networks with AI Accelerated Optimization. *IEEE Netw.* **2020**, *34*, 46–52. [CrossRef]
233. Komiya, K.; Nakajima, T. Community Cash: A Community-Based Cryptocurrency for Implementing Activity-Based Micro-Pricing. In *Smart Blockchain*; Qiu, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2019; pp. 66–75. [CrossRef]
234. Huang, K.; Zhang, X.; Wang, X.; Mu, Y.; Rezaeibagha, F.; Xu, G.; Wang, H.; Zheng, X.; Yang, G.; Xia, Q.; et al. HUCDO: A Hybrid User-centric Data Outsourcing Scheme. *ACM Trans. Cyber-Phys. Syst.* **2020**, *4*, 1–23. [CrossRef]
235. Chen, Q.; Zhang, S.; Wei, W. Proof of Human Engagement on Decentralized Networks. In *Proceedings of the Future Technologies Conference (FTC) 2018*; Arai, K., Bhatia, R., Kapoor, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2019; pp. 712–717. [CrossRef]
236. Blocki, J.; Zhou, H.S. Designing Proof of Human-Work Puzzles for Cryptocurrency and Beyond. In *Theory of Cryptography*; Hirt, M., Smith, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; pp. 517–546. [CrossRef]
237. Abegg, J.P.; Bramas, Q.; Noel, T. Blockchain using Proof-of-Interaction. *arXiv* **2020**, arXiv:2002.07763.
238. Lee, S.b.; Hwang, D.; Kim, J.; Kim, K.H. Proof-of-Lottery: Design for Block Producing Algorithm Based on PoS for Scalability. In Proceedings of the 2020 International Conference on Information Networking (ICOIN), Barcelona, Spain, 7–10 January 2020; pp. 666–669. [CrossRef]
239. Ghiro, L.; Maccari, L.; Cigno, R.L. Proof of networking: Can blockchains boost the next generation of distributed networks? In Proceedings of the 2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS), Isola, France, 6–8 February 2018; pp. 29–32. [CrossRef]
240. Abubakar, M.; Jaroucheh, Z.; Al-Dubai, A.; Buchanan, B. PoNW: A Secure and Scalable Proof-of-Notarized-Work Based Consensus Mechanism. In Proceedings of the 2020 4th International Conference on Vision, Image and Signal Processing, Bangkok, Thailand, 9–11 December 2020; ACM: New York, NY, USA, 2020; pp. 1–8. [CrossRef]
241. Nandwani, A.; Gupta, M.; Thakur, N. Proof-of-Participation: Implementation of Proof-of-Stake Through Proof-of-Work. In *International Conference on Innovative Computing and Communications*; Bhattacharyya, S., Hassanien, A.E., Gupta, D., Khanna, A., Pan, I., Eds.; Springer: Berlin/Heidelberg, Germany, 2019; pp. 17–24. [CrossRef]
242. Lin, Z.; Luo, Y.; Fu, S.; Xie, T. BIMP: Blockchain-Based Incentive Mechanism with Privacy Preserving in Location Proof. In *Algorithms and Architectures for Parallel Processing*; Qiu, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 520–536. [CrossRef]
243. Matsuyama, Y. Divergence Family Contribution to Data Evaluation in Blockchain Via Alpha-EM and Log-EM Algorithms. *IEEE Access* **2021**, *9*, 24546–24559. [CrossRef]
244. Liu, C. Proof of spending in block-chain systems. *arXiv* **2018**, arXiv:1804.11136.
245. Bartoletti, M.; Lande, S.; Podda, A.S. A Proof-of-Stake Protocol for Consensus on Bitcoin Subchains. In *Financial Cryptography and Data Security*; Brenner, M., Rohloff, K., Bonneau, J., Miller, A., Ryan, P.Y., Teague, V., Bracciali, A., Sala, M., Pintore, F., Jakobsson, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; pp. 568–584. [CrossRef]
246. Cai, X.; Wang, Y.; Lin, F.; Tang, C.; Chen, Z. A Blockchain-Based Crowdsourcing System with QoS Guarantee via a Proof-of-Strategy Consensus Protocol. In *Blockchain and Trustworthy Systems*; Zheng, Z., Dai, H.N., Fu, X., Chen, B., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 72–86. [CrossRef]
247. Hassanzadeh-Nazarabadi, Y.; Kupcu, A.; Ozkasap, O. LightChain: Scalable DHT-Based Blockchain. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 2582–2593. [CrossRef]
248. Sumathy Kingslin, R.Z. An Effective Randomization Framework to POW Consensus Algorithm of Blockchain (RPoW). *Int. J. Eng. Adv. Technol.* **2019**, *8*, 1793–1797. [CrossRef]
249. Ahuja, A.; Ribeiro, V.J.; Pal, R. A Regulatory System for Optimal Legal Transaction Throughput in Cryptocurrency Blockchains. *arXiv* **2021**, arXiv:2103.16216.
250. Sun, Y.; Zhang, R.; Xue, R.; Su, Q.; Li, P. A Reputation Based Hybrid Consensus for E-Commerce Blockchain. In *Web Services—ICWS 2020*; Ku, W.S., Kanemasa, Y., Serhani, M.A., Zhang, L.J., Eds.; Springer: Cham, Switzerland, 2020; pp. 1–16. [CrossRef]

251. Fan, X.; Chai, Q. Roll-DPoS. In Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Virtual, 5–7 November 2018; ACM: New York, NY, USA, 2018; pp. 482–484. [CrossRef]
252. Chepurnoy, A.; Larangeira, M.; Ojiganov, A. Rollerchain, a Blockchain with Safely Pruneable Full Blocks. *arXiv* **2016**, arXiv:1603.07926.
253. Calcaterra, C.; Kaal, W.A. Reputation Protocol for the Internet of Trust. In *Legal Tech and the New Sharing Economy*; Compagnucci, M.C., Forgó, N., Kono, T., Teramoto, S., Vermeulen, E.P.M., Eds.; Springer: Cham, Switzerland, 2020; pp. 155–179. [CrossRef]
254. Liu, G.; Yan, Z.; Feng, W.; Jing, X.; Chen, Y.; Atiquzzaman, M. SeDID: An SGX-enabled decentralized intrusion detection framework for network trust evaluation. *Inf. Fusion* **2021**, *70*, 100–114. [CrossRef]
255. Abraham, I.; Malkhi, D.; Nayak, K.; Ren, L.; Spiegelman, A. Solida: A Blockchain Protocol Based on Reconfigurable Byzantine Consensus. In *Leibniz International Proceedings in Informatics (LIPIcs), Proceedings of the 21st International Conference on Principles of Distributed Systems (OPODIS 2017), Lisboa, Portugal, 18–20 December 2017;* Aspnes, J., Bessani, A., Felber, P., Leitão, J., Eds.; Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik: Dagstuhl, Germany, 2018; Volume 95, pp. 25:1–25:19. [CrossRef]
256. Chen, S.; Dai, W.; Dai, Y.; Fu, H.; Gao, Y.; Guo, J.; He, H.; Liu, Y. Thinkey: A Scalable Blockchain Architecture. *arXiv* **2019**, arXiv:1904.04560.
257. Mihaljevic, M.J. A Blockchain Consensus Protocol Based on Dedicated Time-Memory-Data Trade-Off. *IEEE Access* **2020**, *8*, 141258–141268. [CrossRef]
258. Sun, S.; Liu, Y.; Guo, G. A Privacy-Preserving and Robust Reputation System Based on Blockchain. In Proceedings of the 2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), Xiamen, China, 16–18 December 2019; pp. 634–639. [CrossRef]
259. Lucas, B.; Paez, R.V. Consensus Algorithm for a Private Blockchain. In Proceedings of the 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, 12–14 July 2019; pp. 264–271. [CrossRef]
260. Mazurok, I.; Pienko, V.; Leonchyk, Y. Empowering Fault-Tolerant Consensus Algorithm by Economic Leverages. In Proceedings of the 15th International Conference on ICT in Education, Research and Industrial Applications, Integration, Harmonization and Knowledge Transfer, Kherson, Ukraine, 12–15 June 2019.
261. Han, X.; Yuan, Y.; Wang, F.Y. A Fair Blockchain Based on Proof of Credit. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 922–931. [CrossRef]
262. Li, L.; Yan, J.; Peng, H.; Yang, Y. An Improved Consensus Mechanism for the Blockchain Based on Credit Rewards and Punishments. In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology, Hilo, HI, USA, 12–14 March 2020; ACM: New York, NY, USA, 2020; pp. 105–109. [CrossRef]
263. Chen, J.; Gan, W.; Hu, M.; Chen, C.M. On the Construction of a Post-Quantum Blockchain. In Proceedings of the 2021 IEEE Conference on Dependable and Secure Computing (DSC), Aizuwakamatsu, Fukushima, Japan, 30 January–2 February 2021; pp. 1–8. [CrossRef]
264. Chen, J.; Gan, W.; Hu, M.; Chen, C.M. On the construction of a post-quantum blockchain for smart city. *J. Inf. Secur. Appl.* **2021**, *58*, 102780. [CrossRef]
265. Han, R.; Lin, H.; Yu, J. VRF-Based Mining Simple Non-outsourceable Cryptocurrency Mining. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*; Garcia-Alfaro, J., Navarro-Arribas, G., Herrera-Joancomarti, J., Eds.; Springer: Cham, Switzerland, 2020; pp. 287–304. [CrossRef]
266. Hartl, A.; Zseby, T.; Fabini, J. BeaconBlocks: Augmenting Proof-of-Stake with On-Chain Time Synchronization. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 353–360. [CrossRef]
267. Liu, J.; Ren, K. Improving Blockchains With Client-Assistance. *IEEE Trans. Comput.* **2022**, *71*, 1230–1236. [CrossRef]
268. Tosh, D.; Shetty, S.; Foytik, P.; Kamhoua, C.; Njilla, L. CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 302–309. [CrossRef]
269. Li, P.; Peng, J.; Yang, L.; Zheng, Q.; Pan, G. Crux—A New Fast, Flexible and Decentralized Consensus Algorithm with High Fault Tolerance Rate. In *Smart Blockchain*; Qiu, M., Ed.; Springer: Cham, Switzerland, 2018; pp. 66–76. [CrossRef]
270. Yang, F.; Zhou, W.; Wu, Q.; Long, R.; Xiong, N.N.; Zhou, M. Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism. *IEEE Access* **2019**, *7*, 118541–118555. [CrossRef]
271. Cheng, Z.; Wu, G.; Wu, H.; Zhao, M.; Zhao, L.; Cai, Q. A New Hybrid Consensus Protocol: Deterministic Proof Of Work. *arXiv* **2018**, arXiv:1808.04142.
272. Saad, M.; Qin, Z.; Ren, K.; Nyang, D.; Mohaisen, D. e-PoS : Making Proof-of-Stake Decentralized and Fair. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 1961–1973. [CrossRef]
273. Liu, Y.; Liu, J.; Zhang, Z.; Yu, H. A fair selection protocol for committee-based permissionless blockchains. *Comput. Secur.* **2020**, *91*, 101718. [CrossRef]
274. Ashik, M.H.; Shahriar Maswood, M.M.; Alharbi, A.G.; Medhi, D. FPoW: An ASIC-resistant Proof-of-Work for Blockchain Applications. In Proceedings of the 2020 IEEE Region 10 Symposium (TENSYMP), Dhaka, Bangladesh, 5–7 June 2020; pp. 1608–1611. [CrossRef]
275. Zhao, J.; Yu, J.; Liu, J.K. Consolidating Hash Power in Blockchain Shards with a Forest. In *Information Security and Cryptology*; Liu, Z., Yung, M., Eds.; Springer: Cham, Switzerland, 2020; pp. 309–322. [CrossRef]

276. Georghiades, Y.; Flolid, S.; Vishwanath, S. HashCore: Proof-of-Work Functions for General Purpose Processors. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 1951–1959. [CrossRef]
277. Kolokotronis, N.; Brotsis, S.; Germanos, G.; Vassilakis, C.; Shiaeles, S. On Blockchain Architectures for Trust-Based Collaborative Intrusion Detection. In Proceedings of the 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 8–13 July 2019; pp. 21–28. [CrossRef]
278. Coelho, F.; Larroche, A.; Colin, B. *Itsuku: A Memory-Hardened Proof-of-Work Scheme*; Technical Report; MINES ParisTech—PSL Research University: Paris, France, 2017.
279. Morais, R.; Crocker, P.; Melo de Sousa, S. A Tool for Implementing Privacy in Nano. In Proceedings of the 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Oxford, UK, 3–6 August 2020; pp. 159–163. [CrossRef]
280. Kerber, T.; Kiayias, A.; Kohlweiss, M.; Zikas, V. Ouroboros Crypsinous: Privacy-Preserving Proof-of-Stake. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 157–174. [CrossRef]
281. Badertscher, C.; Gaži, P.; Kiayias, A.; Russell, A.; Zikas, V. Ouroboros Genesis. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; ACM: New York, NY, USA, 2018; pp. 913–930. [CrossRef]
282. David, B.; Gaži, P.; Kiayias, A.; Russell, A. Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain. In *Advances in Cryptology—EUROCRYPT 2018*; Nielsen, J.B., Rijmen, V., Eds.; Springer: Cham, Switzerland, 2018; pp. 66–98. [CrossRef]
283. Drijvers, M.; Gorbunov, S.; Neven, G.; Wee, H. Pixel: Multi-signatures for Consensus. In Proceedings of the 29th USENIX Security Symposium (USENIX Security 20), USENIX Association, San Diego, CA, USA, 12–14 August 2020; pp. 2093–2110.
284. Alberini, G.; Moran, T.; Rosen, A. Public Verification of Private Effort. In *Theory of Cryptography*; Dodis, Y., Nielsen, J.B., Eds.; Springer: Cham, Switzerland, 2015; pp. 169–198. [CrossRef]
285. Sayeed, S.; Marco-Gisbert, H. Proof of Adjourn (PoAj): A Novel Approach to Mitigate Blockchain Attacks. *Appl. Sci.* **2020**, *10*, 6607. [CrossRef]
286. Amar, D.; Zilpa, L. Incentive-Based Ledger Protocols for Solving Machine Learning Tasks and Optimization Problems via Competitions. In Proceedings of the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach, CA, USA, 16–17 June 2019; pp. 2838–2846. [CrossRef]
287. Wang, L.e.; Bai, Y.; Jiang, Q.; C. M. Leung, V.; Cai, W.; Li, X. Beh-Raft-Chain: A Behavior-Based Fast Blockchain Protocol for Complex Networks. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 1154–1166. [CrossRef]
288. Krol, M.; Sonnino, A.; Al-Bassam, M.; Tasiopoulos, A.; Psaras, I. Proof-of-Prestige: A Useful Work Reward System for Unverifiable Tasks. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 293–301. [CrossRef]
289. Damgård, I.; Ganesh, C.; Orlandi, C. Proofs of Replicated Storage Without Timing Assumptions. In *Advances in Cryptology—CRYPTO 2019*; Boldyreva, A., Micciancio, D., Eds.; Springer: Cham, Switzerland, 2019; pp. 355–380. [CrossRef]
290. Al-Mamun, A.; Li, T.; Sadoghi, M.; Zhao, D. In-memory Blockchain: Toward Efficient and Trustworthy Data Provenance for HPC Systems. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 3808–3813. [CrossRef]
291. Kleinrock, L.; Ostrovsky, R.; Zikas, V. Proof-of-Reputation Blockchain with Nakamoto Fallback. In *Progress in Cryptology—INDOCRYPT 2020*; Bhargavan, K., Oswald, E., Prabhakaran, M., Eds.; Springer: Cham, Switzerland, 2020; pp. 16–38. [CrossRef]
292. Bag, S.; Ruj, S.; Sakurai, K. On the Application of Clique Problem for Proof-of-Work in Cryptocurrencies. In *Information Security and Cryptology*; Lin, D., Wang, X., Yung, M., Eds.; Springer: Cham, Switzerland, 2016; pp. 260–279. [CrossRef]
293. Kalinin, K.P.; Berloff, N.G. Blockchain platform with proof-of-work based on analog Hamiltonian optimisers. *arXiv* **2018**, arXiv:1802.10091.
294. Bocart, F. Inflation Propensity of Collatz Orbits: A New Proof-of-Work for Blockchain Applications. *J. Risk Financ. Manag.* **2018**, *11*, 83. [CrossRef]
295. Li, A.; Wei, X.; He, Z. Robust Proof of Stake: A New Consensus Protocol for Sustainable Blockchain Systems. *Sustainability* **2020**, *12*, 2824. [CrossRef]
296. Kwak, J.Y.; Yim, J.; Ko, N.S.; Kim, S.M. The Design of Hierarchical Consensus Mechanism Based on Service-Zone Sharding. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1387–1403. [CrossRef]
297. Jaroucheh, Z.; Ghaleb, B.; Buchanan, W.J. SklCoin: Toward a Scalable Proof-of-Stake and Collective Signature Based Consensus Protocol for Strong Consistency in Blockchain. In Proceedings of the 2020 IEEE International Conference on Software Architecture Companion (ICSA-C), Salvador, Brazil, 16–20 March 2020; pp. 143–150. [CrossRef]
298. Li, W.; Sforzin, A.; Fedorov, S.; Karame, G.O. Towards Scalable and Private Industrial Blockchains. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, BCC '17, Incheon, Korea, 4 June 2018; Association for Computing Machinery: New York, NY, USA, 2017; pp. 9–14. [CrossRef]
299. Bao, X. A Decentralized Secure Mailbox System based on Blockchain. In Proceedings of the 2020 International Conference on Computer Communication and Network Security (CCNS), Xi'an, China, 21–23 August 2020; pp. 136–141. [CrossRef]
300. Berger, C.; Reiser, H.P.; Sousa, J.; Bessani, A. AWARE: Adaptive Wide-Area Replication for Fast and Resilient Byzantine Consensus. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 1605–1620. [CrossRef]

301. Fu, W.; Wei, X.; Tong, S. An Improved Blockchain Consensus Algorithm Based on Raft. *Arab. J. Sci. Eng.* **2021**, *46*, 8137–8149. [CrossRef]
302. Alzahrani, N.; Bulusu, N. Towards True Decentralization: A Blockchain Consensus Protocol Based on Game Theory and Randomness. In *Decision and Game Theory for Security*; Bushnell, L., Poovendran, R., Başar, T., Eds.; Springer: Cham, Switzerland, 2018; pp. 465–485. [CrossRef]
303. Tan, H.; Golab, W. Optimizing All-to-All Data Transmission in WANs. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 3677–3690. [CrossRef]
304. Jill, D.E. The Verex Blockchain: A Non-Anonymous Decentralized Ledger with an Assigned-Majority-Validation Consensus Protocol. Available online: https://zenodo.org/record/1173637#.Y4Xdk31BxPY (accessed on 26 October 2022).
305. Ai, Z.; Liu, Y.; Wang, X. ABC: An Auction-Based Blockchain Consensus-Incentive Mechanism. In Proceedings of the 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS), Hong Kong, China, 2–4 December 2020; pp. 609–616. [CrossRef]
306. Van Toan, N.; Park, U.; Ryu, G. RCANE: Semi-Centralized Network of Parallel Blockchain and APoS. In Proceedings of the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, 11–13 December 2018; pp. 1–6. [CrossRef]
307. Bose, S.; Raikwar, M.; Mukhopadhyay, D.; Chattopadhyay, A.; Lam, K.Y. BLIC: A Blockchain Protocol for Manufacturing and Supply Chain Management of ICS. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1326–1335. [CrossRef]
308. Li, Y.; Chen, C.; Liu, N.; Huang, H.; Zheng, Z.; Yan, Q. A Blockchain-Based Decentralized Federated Learning Framework with Committee Consensus. *IEEE Netw.* **2021**, *35*, 234–241. [CrossRef]
309. Dold, F. The GNU Taler System: Practical and Provably Secure Electronic Payments. Ph.D. Thesis, Universite Rennes, Rennes, France, 2019.
310. Butt, K.; Sorensen, D.; Stay, M. Casanova. *arXiv* **2018**, arXiv:1812.02232.
311. Azouvi, S.; McCorry, P.; Meiklejohn, S. Winning the Caucus Race: Continuous Leader Election via Public Randomness. *arXiv* **2018**, arXiv:1801.07965.
312. Ileri, A.M.; Ozercan, H.I.; Gundogdu, A.; Senol, A.K.; Ozkaya, M.Y.; Alkan, C. Coinami: A Cryptocurrency with DNA Sequence Alignment as Proof-of-work. *arXiv* **2016**, arXiv:1602.03031.
313. Meng, Y.; Cao, Z.; Qu, D. A Committee-Based Byzantine Consensus Protocol for Blockchain. In Proceedings of the 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 23–25 November 2018; pp. 1–6. [CrossRef]
314. Hubert Chan, T.H.; Pass, R.; Shi, E. Consensus through Herding. In *Advances in Cryptology—EUROCRYPT 2019*; Ishai, Y., Rijmen, V., Eds.; Springer: Cham, Switzerland, 2019; pp. 720–749. [CrossRef]
315. He, G.; Su, W.; Gao, S.; Yue, J.; Das, S.K. ROAchain: Securing Route Origin Authorization With Blockchain for Inter-Domain Routing. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1690–1705. [CrossRef]
316. He, G.; Su, W.; Gao, S.; Yue, J. TD-Root: A trustworthy decentralized DNS root management architecture based on permissioned blockchain. *Future Gener. Comput. Syst.* **2020**, *102*, 912–924. [CrossRef]
317. Amiri, M.J.; Agrawal, D.; Abbadi, A.E. CAPER. *Proc. VLDB Endow.* **2019**, *12*, 1385–1398. [CrossRef]
318. Hao, X.; Yu, L.; Zhiqiang, L.; Zhen, L.; Dawu, G. Dynamic Practical Byzantine Fault Tolerance. In Proceedings of the 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018, pp. 1–8. [CrossRef]
319. Chen, W.; Yang, X.; Zhang, H.; Xu, Y.; Pang, Z. Big Data Architecture for Scalable and Trustful DNS based on Sharded DAG Blockchain. *J. Signal Process. Syst.* **2021**, *93*, 753–768. [CrossRef]
320. Lei, K.; Fang, J.; Zhang, Q.; Lou, J.; Du, M.; Huang, J.; Wang, J.; Xu, K. Blockchain-Based Cache Poisoning Security Protection and Privacy-Aware Access Control in NDN Vehicular Edge Computing Networks. *J. Grid Comput.* **2020**, *18*, 593–613. [CrossRef]
321. Deng, Q. Blockchain Economical Models, Delegated Proof of Economic Value and Delegated Adaptive Byzantine Fault Tolerance and their implementation in Artificial Intelligence BlockCloud. *J. Risk Financ. Manag.* **2019**, *12*, 177. [CrossRef]
322. Chen, J.; Yao, S.; Yuan, Q.; He, K.; Ji, S.; Du, R. CertChain: Public and Efficient Certificate Audit Based on Blockchain for TLS Connections. In Proceedings of the IEEE INFOCOM 2018—IEEE Conference on Computer Communications, Honolulu, HI, USA, 16–19 April 2018; pp. 2060–2068. [CrossRef]
323. Chen, T.Y.; Huang, W.N.; Kuo, P.C.; Chung, H.; Chao, T.W. DEXON: A Highly Scalable, Decentralized DAG-Based Consensus Algorithm. *arXiv* **2018**, arXiv:1811.07525.
324. Hanke, T.; Movahedi, M.; Williams, D. DFINITY Technology Overview Series, Consensus System. *arXiv* **2018**, arXiv:1805.04548.
325. Li, F.; Liu, K.; Liu, J.; Fan, Y.; Wang, S. DHBFT: Dynamic Hierarchical Byzantine Fault-Tolerant Consensus Mechanism Based on Credit. In *Web and Big Data*; Wang, X., Zhang, R., Lee, Y.K., Sun, L., Moon, Y.S., Eds.; Springer: Cham, Switzerland, 2020; pp. 3–17. [CrossRef]
326. He, L.; Hou, Z. An Improvement of Consensus Fault Tolerant Algorithm Applied to Alliance Chain. In Proceedings of the 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, 12–14 July 2019, pp. 1–4. [CrossRef]

327. Abraham, A.; Theuermann, K.; Kirchengast, E. Qualified eID Derivation Into a Distributed Ledger Based IdM System. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1406–1412. [CrossRef]
328. Garg, M.; Peluso, S.; Arun, B.; Ravindran, B. Generalized Consensus for Practical Fault Tolerance. In Proceedings of the 20th International Middleware Conference, Davis, CA, USA, 9–13 December 2019; ACM: New York, NY, USA, 2019; pp. 55–67. [CrossRef]
329. Li, Y.; Wang, Z.; Fan, J.; Zheng, Y.; Luo, Y.; Deng, C.; Ding, J. An Extensible Consensus Algorithm Based on PBFT. In Proceedings of the 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Guilin, China, 17–19 October 2019; pp. 17–23. [CrossRef]
330. Locher, T. Fast Byzantine Agreement for Permissioned Distributed Ledgers. In Proceedings of the 32nd ACM Symposium on Parallelism in Algorithms and Architectures, Virtual, 15–17 July 2020; ACM: New York, NY, USA, 2020; pp. 371–382. [CrossRef]
331. Liu, J.; Li, W.; Karame, G.O.; Asokan, N. Scalable Byzantine Consensus via Hardware-Assisted Secret Sharing. *IEEE Trans. Comput.* **2019**, *68*, 139–151. [CrossRef]
332. Gupta, S.; Rahnama, S.; Hellings, J.; Sadoghi, M. ResilientDB. *Proc. VLDB Endow.* **2020**, *13*, 868–883. [CrossRef]
333. Oh, M.; Ha, S.; Yoon, J.H.; Lee, K.W.; Son, Y.; Yeom, H.Y. Graph Learning BFT: A Design of Consensus System for Distributed Ledgers. *IEEE Access* **2020**, *8*, 161739–161751. [CrossRef]
334. Bao, Z.; Liu, Y.; Zhang, W. A Group-Based Optimized Practical Byzantine Fault Tolerance Consensus Algorithm. In *Blockchain Technology and Application*; Xu, K., Zhu, J., Song, X., Lu, Z., Eds.; Springer: Cham, Switzerland, 2021; pp. 95–115. [CrossRef]
335. Yin, M.; Malkhi, D.; Reiter, M.K.; Gueta, G.G.; Abraham, I. HotStuff. In Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing, Toronto, ON, Canada, 29 July–2 August 2019; ACM: New York, NY, USA, 2019; pp. 347–356. [CrossRef]
336. Kuo, P.C.; Chung, H.; Chao, T.W.; Cheng, C.M. Fair Byzantine Agreements for Blockchains. *IEEE Access* **2020**, *8*, 70746–70761. [CrossRef]
337. Liang, L.; Cao, X.; Zhang, J.; Sun, C. SLC: A Permissioned Blockchain for Secure Distributed Machine Learning against Byzantine Attacks. In Proceedings of the 2020 Chinese Automation Congress (CAC), Shanghai, China, 6–8 November 2020; pp. 7073–7078. [CrossRef]
338. Moniz, H. The Istanbul BFT Consensus Algorithm. *arXiv* **2020**, arXiv:2002.03613.
339. Liu, Y.; Liu, J.; Li, D.; Yu, H.; Wu, Q. FleetChain: A Secure Scalable and Responsive Blockchain Achieving Optimal Sharding. In *Algorithms and Architectures for Parallel Processing*; Qiu, M., Ed.; Springer: Cham, Switzerland, 2020; pp. 409–425. [CrossRef]
340. Lim, G.; Kwon, Y.; Kim, Y. Analysis of LFT2. *arXiv* **2020**, arXiv:2004.04294.
341. Hackfeld, J. A lightweight BFT consensus protocol for blockchains. *arXiv* **2019**, arXiv:1903.11434.
342. Wang, Z. MOCA: A Scalable Consensus Algorithm Based on Cellular Automata. In Proceedings of the 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 23–25 November 2018; pp. 314–318. [CrossRef]
343. Zhao, B.; Fan, P.; Ni, M. Mchain: A Blockchain-Based VM Measurements Secure Storage Approach in IaaS Cloud With Enhanced Integrity and Controllability. *IEEE Access* **2018**, *6*, 43758–43769. [CrossRef]
344. Kim, S.; Lee, S.; Jeong, C.; Cho, S. Byzantine Fault Tolerance Based Multi-Block Consensus Algorithm for Throughput Scalability. In Proceedings of the 2020 International Conference on Electronics, Information, and Communication (ICEIC), Barcelona, Spain, 19–22 January 2020; pp. 1–3. [CrossRef]
345. Bao, Z.; Wang, K.; Zhang, W. An Auditable and Secure Model for Permissioned Blockchain. In Proceedings of the 2019 International Electronics Communication Conference, Okinawa, Japan, 7–9 July 2019; ACM: New York, NY, USA, 2019; pp. 139–145. . [CrossRef]
346. Chen, C.W.; Su, J.W.; Kuo, T.W.; Chen, K. MSig-BFT: A Witness-Based Consensus Algorithm for Private Blockchains. In Proceedings of the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, 11–13 December 2018; pp. 992–997. [CrossRef]
347. Jalalzai, M.M.; Busch, C. Window Based BFT Blockchain Consensus. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 971–979. [CrossRef]
348. Wu, W.; Gao, Z. An Improved Blockchain Consensus Mechanism Based on Open Business Environment. *IOP Conf. Ser. Earth Environ. Sci.* **2020**, *428*, 012043. [CrossRef]
349. Ma, J.; Jo, Y.; Park, C. PeerBFT: Making Hyperledger Fabric's Ordering Service Withstand Byzantine Faults. *IEEE Access* **2020**, *8*, 217255–217267. [CrossRef]
350. Chen, Z.; Lu, Z.; Sane, A.; Bhimsain, A. Trustworthy When Human and Bots Are Mingled. In Proceedings of the 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), New York, NY, USA, 1–3 August 2020; pp. 76–81. [CrossRef]
351. Zhang, J.; Tian, R.; Cao, Y.; Yuan, X.; Yu, Z.; Yan, X.; Zhang, X. A Hybrid Model for Central Bank Digital Currency Based on Blockchain. *IEEE Access* **2021**, *9*, 53589–53601. [CrossRef]
352. He, S.; Ning, Y.; Chen, H.; Xing, C.; Zhang, L.J. Layered Consensus Mechanism in Consortium Blockchain for Enterprise Services. In *Blockchain—ICBC 2019*; Joshi, J.; Nepal, S.; Zhang, Q.; Zhang, L.J., Eds.; Springer: Cham, Switzerland, 2019; pp. 49–64. [CrossRef]

353. Shen, W.; Huang, X.; Yu, Y.; Gu, L.; Pan, J.; Ling, L. Blockchain Based on PoR Consensus Mechanism. In Proceedings of the 2020 IEEE 3rd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE), Shenyang, China, 20–22 Novvember 2020; pp. 73–76. [CrossRef]
354. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4177–4186. [CrossRef]
355. Kudin, A.M.; Kovalenko, B.A.; Shvidchenko, I.V. Blockchain Technology: Issues of Analysis and Synthesis. *Cybern. Syst. Anal.* **2019**, *55*, 488–495. [CrossRef]
356. Belfer, R.; Kashtalian, A.; Nicheporuk, A.; Markowsky, G.; Sachenko, A. Proof-Of-Activity Consensus Protocol based on a Network's Active Nodes. In Proceedings of the 1st International Workshop on Intelligent Information TEchnologies and Systems of Information, IntelITSIS 2020, Khmelnytskyi, Ukraine, 23–25 March 2020; pp. 239–251.
357. Lee, E.; Yoon, Y.I. Project Management Model Based on Consistency Strategy for Blockchain Platform. In Proceedings of the 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), Honolulu, HI, USA, 29–31 May 2019; pp. 38–44. [CrossRef]
358. Lee, E.; Yoon, Y.; Lee, G.M.; Um, T.W. Blockchain-based Perfect Sharing Project Platform based on the Proof of Atomicity Consensus Algorithm. *Teh. Vjesn. Tech. Gaz.* **2020**, *27*. [CrossRef]
359. Wood, G. PoA Private Chains. Available online: https://github.com/ethereum/guide/blob/master/poa.md (accessed on 26 October 2022).
360. Chen, Y.; Xie, H.; Lv, K.; Wei, S.; Hu, C. DEPLEST: A blockchain-based privacy-preserving distributed database toward user behaviors in social networks. *Inf. Sci.* **2019**, *501*, 100–117. [CrossRef]
361. 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 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1212–1218. [CrossRef]
362. Kim, J.T.; Jin, J.; Kim, K. A study on an energy-effective and secure consensus algorithm for private blockchain systems (PoM: Proof of Majority). In Proceedings of the 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 17–19 October 2018; pp. 932–935. [CrossRef]
363. Fu, X.; Wang, H.; Shi, P.; Mi, H. PoPF: A Consensus Algorithm for JCLedger. In Proceedings of the 2018 IEEE Symposium on Service-Oriented System Engineering (SOSE), Bamberg, Germany, 26–29 March 2018; pp. 204–209. [CrossRef]
364. Gai, F.; Wang, B.; Deng, W.; Peng, W. Proof of Reputation: A Reputation-Based Consensus Protocol for Peer-to-Peer Network. In *Database Systems for Advanced Applications*; Pei, J., Manolopoulos, Y., Sadiq, S., Li, J., Eds.; Springer: Cham, Switzerland, 2018; pp 666–681. [CrossRef]
365. Hegadekatti, K.; Yatish, S.G. Proof-of-Sovereignty (PoSv) As a Method to Achieve Distributed Consensus in Crypto-Currency Networks. *SSRN Electron. J.* **2016**. [CrossRef]
366. Barhanpure, A.; Belandor, P.; Das, B. Proof of Stack Consensus for Blockchain Networks. In *Security in Computing and Communications*; Thampi, S.M., Madria, S., Wang, G., Rawat, D.B., Calero, J.M.A., Eds.; Springer: Cham, Switzerland, 2019; pp. 104–116. [CrossRef]
367. Zou, J.; Ye, B.; Qu, L.; Wang, Y.; Orgun, M.A.; Li, L. A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services. *IEEE Trans. Serv. Comput.* **2019**, *12*, 429–445. [CrossRef]
368. Li, K.; Li, H.; Wang, H.; An, H.; Lu, P.; Yi, P.; Zhu, F. PoV: An Efficient Voting-Based Consensus Algorithm for Consortium Blockchains. *Front. Blockchain* **2020**, *3*. [CrossRef]
369. Li, K.; Li, H.; Hou, H.; Li, K.; Chen, Y. Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain. In Proceedings of the 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Bangkok, Thailand, 18–20 December 2017; pp. 466–473. [CrossRef]
370. Gupta, H.; Janakiram, D. Colosseum. In Proceedings of the Third ACM Workshop on Blockchains, Cryptocurrencies and Contracts—BCC '19, Auckland, New Zealand, 8 July 2019; ACM Press: New York, New York, USA, 2019; pp. 23–25. [CrossRef]
371. Jalalzai, M.M.; Busch, C.; Richard, G.G. Proteus: A Scalable BFT Consensus Protocol for Blockchains. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 308–313. [CrossRef]
372. Jalalzai, M.M.; Busch, C.; Richard, G.G. Consistent BFT Performance for Blockchains. In Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks—Supplemental Volume (DSN-S), Portland, OR, USA, 24–27 June 2019, pp. 17–18. [CrossRef]
373. Moh, M.; Nguyen, D.; Moh, T.S.; Khieu, B. Blockchain for Efficient Public Key Infrastructure and Fault-Tolerant Distributed Consensus. In *Blockchain Cybersecurity, Trust and Privacy*; Choo, K.K.R., Dehghantanha, A., Parizi, R.M., Eds.; Springer: Cham, Switzerland, 2020; pp. 69–97. [CrossRef]
374. He, G.; Su, W.; Gao, S. Chameleon: A Scalable and Adaptive Permissioned Blockchain Architecture. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018; pp. 87–93. [CrossRef]
375. Dingyu, W.; Dingmin, W.; Lupin, Q.; MinLong, X. A Byzantine consensus based on proof-of-work of nodes' behaviors. *J. Phys. Conf. Ser.* **2020**, *1684*, 012049. [CrossRef]

376. Lei, K.; Zhang, Q.; Xu, L.; Qi, Z. Reputation-Based Byzantine Fault-Tolerance for Consortium Blockchain. In Proceedings of the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, 11–13 December 2018; pp. 604–611. [CrossRef]
377. Khan, F.A.; Abubakar, A.; Mahmoud, M.; Al-Khasawneh, M.A.; Alarood, A.A. Rift: A high-performance consensus algorithm for consortium blockchain. *Int. J. Recent Technol. Eng.* **2019**, *7*, 989–997.
378. Fan, Y.; Zou, J.; Liu, S.; Yin, Q.; Guan, X.; Yuan, X.; Wu, W.; Du, D. A blockchain-based data storage framework: A rotating multiple random masters and error-correcting approach. *Peer-to-Peer Netw. Appl.* **2020**, *13*, 1486–1504. [CrossRef]
379. Amiri, M.J.; Lai, Z.; Patel, L.; Loo, B.T.; Lo, E.; Zhou, W. Saguaro: An Edge Computing-Enabled Hierarchical Permissioned Blockchain. *arXiv* **2021**, arXiv:2101.08819.
380. Golan Gueta, G.; Abraham, I.; Grossman, S.; Malkhi, D.; Pinkas, B.; Reiter, M.; Seredinschi, D.A.; Tamir, O.; Tomescu, A. SBFT: A Scalable and Decentralized Trust Infrastructure. In Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Portland, OR, USA, 24–27 June 2019; pp. 568–580. [CrossRef]
381. Li, Y.; Qiao, L.; Lv, Z. An Optimized Byzantine Fault Tolerance Algorithm for Consortium Blockchain. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 2826–2839. [CrossRef]
382. Choi, B.; Sohn, J.y.; Han, D.J.; Moon, J. Scalable Network-Coded PBFT Consensus Algorithm. In Proceedings of the 2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, 7–12 July 2019; pp. 857–861. [CrossRef]
383. Fan, X. Scalable Practical Byzantine Fault Tolerance with Short-Lived Signature Schemes. In Proceedings of the 28th Annual International Conference on Computer Science and Software Engineering, CASCON '18, Markham, ON, Canada, 29–31 October 2018; IBM Corp.: Armonk, NY, USA, 2018; pp. 245–256.
384. Li, C.; Zhang, J.; Yang, X.; Youlong, L. Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices. *Inf. Process. Manag.* **2021**, *58*, 102602. [CrossRef]
385. Kashyap, R.; Arora, K.; Sharma, M.; Aazam, A. Security-Aware GA Based Practical Byzantine Fault Tolerance for Permissioned Blockchain. In Proceedings of the 2019 4th International Conference on Control, Robotics and Cybernetics (CRC), Tokyo, Japan, 27–30 September 2019; pp. 162–168. [CrossRef]
386. Binun, A.; Dolev, S.; Hadad, T. Self-stabilizing Byzantine Consensus for Blockchain. In *Cyber Security Cryptography and Machine Learning*; Dolev, S., Hendler, D., Lodha, S., Yung, M., Eds.; Springer: Cham, Switzerland, 2019; pp. 106–110. [CrossRef]
387. Luo, X.; Yang, P.; Wang, W.; Gao, Y.; Yuan, M. S-PoDL: A two-stage computational-efficient consensus mechanism for blockchain-enabled multi-access edge computing. *Phys. Commun.* **2021**, *46*, 101338. [CrossRef]
388. Amiri, M.J.; Agrawal, D.; Abbadi, A.E. SharPer: Sharding Permissioned Blockchains Over Network Clusters. *arXiv* **2019**, arXiv:1910.00765.
389. Chan, B.Y.; Shi, E. Streamlet: Textbook Streamlined Blockchains. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, New York, NY, USA, 21–23 October 2020; ACM: New York, NY, USA, 2020; pp. 1–11. [CrossRef]
390. Khalid, M.H.; Murtaza, M.; Saeed, A.; Raza, M. Proposing 2-tier Architecture for Permission-ed and Permission-less Blockchain Consensus Algorithms Based on Voting System. In Proceedings of the 2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA), Sydney, Australia, 25–27 November 2020; pp. 1–6. [CrossRef]
391. Kopp, H.; Kargl, F.; Bösch, C.; Peter, A. uMine: A Blockchain Based on Human Miners. In *Information and Communications Security*; Naccache, D., Xu, S., Qing, S., Samarati, P., Blanc, G.; Lu, R.; Zhang, Z.; Meddahi, A., Eds.; Springer: Cham, Switzerland, 2018; pp. 20–38. [CrossRef]
392. Guo, H.; Zheng, H.; Xu, K.; Kong, X.; Liu, J.; Liu, F.; Gai, K. An Improved Consensus Mechanism for Blockchain. In *Smart Blockchain*; Qiu, M., Ed.; Springer: Cham, Switzerland, 2018; pp. 129–138. [CrossRef]
393. Heo, G.; Yang, D.; Doh, I.; Chae, K. Design of Blockchain System for Protection of Personal Information in Digital Content Trading Environment. In Proceedings of the 2020 International Conference on Information Networking (ICOIN), Barcelona, Spain, 7–10 January 2020; pp. 152–157. [CrossRef]
394. Lv, S.; Li, H.; Wang, H.; Wang, X. CoT: A Secure Consensus of Trust with Delegation Mechanism in Blockchains. In *Blockchain Technology and Application*; Si, X.; Jin, H.; Sun, Y.; Zhu, J.; Zhu, L.; Song, X.; Lu, Z., Eds.; Springer: Cham, Switzerland, 2020; pp 104–120. [CrossRef]
395. Liang, D.; An, J.; Cheng, J.; Yang, H.; Gui, R. The Quality Control in Crowdsensing Based on Twice Consensuses of Blockchain. In Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers, Singapore, 8–12 October 2018; ACM: New York, NY, USA, 2018; pp. 630–635. [CrossRef]
396. Bugday, A.; Ozsoy, A.; Öztaner, S.M.; Sever, H. Creating consensus group using online learning based reputation in blockchain networks. *Pervasive Mob. Comput.* **2019**, *59*, 101056. [CrossRef]
397. An, J.; Cheng, J.; Gui, X.; Zhang, W.; Liang, D.; Gui, R.; Jiang, L.; Liao, D. A Lightweight Blockchain-Based Model for Data Quality Assessment in Crowdsensing. *IEEE Trans. Comput. Soc. Syst.* **2020**, *7*, 84–97. [CrossRef]
398. Biryukov, A.; Feher, D.; Khovratovich, D. *Guru: Universal Reputation Module for Distributed Consensus Protocols*; Technical Report; University of Luxembourg: Luxembourg, 2017.
399. Platt, M.; McBurney, P. Sybil attacks on identity-augmented Proof-of-Stake. *Comput. Netw.* **2021**, *199*, 108424. [CrossRef]
400. Bou Abdo, J.; El Sibai, R.; Demerjian, J. Permissionless proof-of-reputation-X: A hybrid reputation-based consensus algorithm for permissionless blockchains. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4148. [CrossRef]

401. Ehrlich, C.; Guzova, A. KRNC: New Foundations for Permissionless Byzantine Consensus and Global Monetary Stability. *arXiv* **2019**, arXiv:1909.07433.
402. Khan, D.; Tang, L.; Ahmed, M. Proof-of-Review: A Review based Consensus Protocol for Blockchain Application. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*. [CrossRef]
403. Burmaka, I.; Stoianov, N.; Lytvynov, V.; Dorosh, M.; Lytvyn, S. Proof of Stake for Blockchain Based Distributed Intrusion Detecting System. In *Mathematical Modeling and Simulation of Systems (MODS'2020)*; Shkarlet, S.; Morozov, A.; Palagin, A., Eds.; Springer: Cham, Switzerland, 2021; pp. 237–247. [CrossRef]
404. Bahri, L.; Girdzijauskas, S. When Trust Saves Energy. In Proceedings of the Companion of the The Web Conference 2018 on The Web Conference 2018—WWW '18; ACM Press: New York, New York, USA, Lyon, France, 23–27 April 2018; pp. 1165–1169. [CrossRef]
405. Bahri, L.; Girdzijauskas, S. Trust Mends Blockchains: Living up to Expectations. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 1358–1368. [CrossRef]
406. Hajialikhani, M.; Jahanara, M. UniqueID: Decentralized Proof-of-Unique-Human. *arXiv* **2018**, arXiv:1806.07583.
407. Biryukov, A.; Feher, D. ReCon: Sybil-resistant consensus from reputation. *Pervasive Mob. Comput.* **2020**, *61*, 101109. [CrossRef]
408. Kim, D.; Lee, J. A Reverse Hash Chain Path-Based Access Control Scheme for a Connected Smart Home System. *IEEE Consum. Electron. Mag.* **2021**, *10*, 93–100. [CrossRef]
409. Shala, B.; Trick, U.; Lehmann, A.; Ghita, B.; Shiaeles, S. Novel trust consensus protocol and blockchain-based trust evaluation system for M2M application services. *Internet Things* **2019**, *7*, 100058. [CrossRef]
410. An, J.; Yang, H.; Gui, X.; Zhang, W.; Gui, R.; Kang, J. TCNS: Node Selection With Privacy Protection in Crowdsensing Based on Twice Consensuses of Blockchain. *IEEE Trans. Netw. Serv. Manag.* **2019**, *16*, 1255–1267. [CrossRef]
411. An, J.; Liang, D.; Gui, X.; Yang, H.; Gui, R.; He, X. Crowdsensing Quality Control and Grading Evaluation Based on a Two-Consensus Blockchain. *IEEE Internet Things J.* **2019**, *6*, 4711–4718. [CrossRef]
412. Gao, Y.L.; Chen, X.B.; Xu, G.; Yuan, K.G.; Liu, W.; Yang, Y.X. A novel quantum blockchain scheme base on quantum entanglement and DPoS. *Quantum Inf. Process.* **2020**, *19*, 420. [CrossRef]
413. Neo. Neo Consensus Mechanism. Available online: https://docs.neo.org/docs/en-us/basic/consensus/dbft.html (accessed on 26 October 2022).
414. Liu, Y.; Ai, Z.; Tian, M.; Guo, G.; Jiang, L. DSBFT: A Delegation Based Scalable Byzantine False Tolerance Consensus Mechanism. In *Algorithms and Architectures for Parallel Processing*; Qiu, M., Ed.; Springer: Cham, Switzerland, 2020; pp. 426–440. [CrossRef]
415. Müller, S.; Penzkofer, A.; Kuśmierz, B.; Camargo, D.; Buchanan, W.J. Fast Probabilistic Consensus with Weighted Votes. In *Proceedings of the Future Technologies Conference (FTC)*; Arai, K., Kapoor, S., Bhatia, R., Eds.; Springer: Cham, Switzerland, 2021; pp. 360–378. [CrossRef]
416. Jacquet, P.; Mans, B. Green Mining: Toward a less energetic impact of cryptocurrencies. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 29 April–2 May 2019; pp. 210–215. [CrossRef]
417. Jacquet, P.; Mans, B. Blockchain moderated by empty blocks to reduce the energetic impact of crypto-moneys. *Comput. Commun.* **2020**, *152*, 126–136. [CrossRef]
418. Min, X.; Li, Q.; Liu, L.; Cui, L. A Permissioned Blockchain Framework for Supporting Instant Transaction and Dynamic Block Size. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016. [CrossRef]
419. Lundbæk, L.N.; Janes Beutel, D.; Huth, M.; Jackson, S.; Kirk, L.; Steiner, R. Proof of Kernel Work: A democratic low-energy consensus for distributed access-control protocols. *R. Soc. Open Sci.* **2018**, *5*, 180422. [CrossRef] [PubMed]
420. Akhilesh, N.; Aniruddha, M.; Sowmya, K. Implementation of Blockchain for Secure Bank Transactions. In Proceedings of the 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), Bengaluru, India, 21–22 February 2020; pp. 1–10. [CrossRef]
421. Kim, J.M.; Won Lee, J.; Lee, K.; Huh, J. Proof of Phone: A Low-cost Blockchain Platform. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019; pp. 1–4. [CrossRef]
422. Kim, S.; Kim, J. POSTER: Mining with Proof-of-Probability in Blockchain. In Proceedings of the 2018 on Asia Conference on Computer and Communications Security, Incheon, Korea, 4–8 June 2018; ACM: New York, NY, USA, 2018; pp. 841–843. [CrossRef]
423. Baldimtsi, F.; Kiayias, A.; Zacharias, T.; Zhang, B. Indistinguishable Proofs of Work or Knowledge. In *Advances in Cryptology—ASIACRYPT 2016*; Cheon, J., Takagi, T., Eds.; Springer, Berlin/Heidelberg, Germany, 2016; pp. 902–933. [CrossRef]
424. Liu, Y.; Liu, J.; Wu, Q.; Yu, H.; Hei, Y.; Zhou, Z. SSHC: A Secure and Scalable Hybrid Consensus Protocol for Sharding Blockchains With a Formal Security Framework. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 2070–2088. [CrossRef]
425. Roman-Belmonte, J.M.; la Corte-Rodriguez, H.D.; Rodriguez-Merchan, E.C. How blockchain technology can change medicine. *Postgrad. Med.* **2018**, *130*, 420–427. [CrossRef] [PubMed]
426. Junaid, S.B.; Imam, A.A.; Balogun, A.O.; Silva, L.C.D.; Surakat, Y.A.; Kumar, G.; Abdulkarim, M.; Shuaibu, A.N.; Garba, A.; Sahalu, Y.; et al. Recent Advancements in Emerging Technologies for Healthcare Management Systems: A Survey. *Healthcare* **2022**, *10*, 1940. [CrossRef] [PubMed]
427. Krichen, M.; Ammi, M.; Mihoub, A.; Almutiq, M. Blockchain for Modern Applications: A Survey. *Sensors* **2022**, *22*, 5274. [CrossRef] [PubMed]

428. Shah, I.; Doshi, C.; Patel, M.; Tanwar, S.; Hong, W.C.; Sharma, R. A Comprehensive Review of the Technological Solutions to Analyse the Effects of Pandemic Outbreak on Human Lives. *Medicina* **2022**, *58*, 311. [CrossRef] [PubMed]
429. Mackey, T.K.; Kuo, T.T.; Gummadi, B.; Clauson, K.A.; Church, G.; Grishin, D.; Obbad, K.; Barkovich, R.; Palombini, M. "Fit-for-purpose?" challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC Med.* **2019**, *17*, 68. [CrossRef] [PubMed]
430. Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. *Int. J. Med. Inform.* **2020**, *134*, 104040. [CrossRef] [PubMed]
431. Lee, T.F.; Chang, I.P.; Kung, T.S. Blockchain-Based Healthcare Information Preservation Using Extended Chaotic Maps for HIPAA Privacy/Security Regulations. *Appl. Sci.* **2021**, *11*, 10576. [CrossRef]
432. Hashim, F.; Shuaib, K.; Sallabi, F. Connected Blockchain Federations for Sharing Electronic Health Records. *Cryptography* **2022**, *6*, 47. [CrossRef]
433. Kumar, A.; Kumar Sharma, D.; Nayyar, A.; Singh, S.; Yoon, B. Lightweight Proof of Game (LPoG): A Proof of Work (PoW)'s Extended Lightweight Consensus Algorithm for Wearable Kidneys. *Sensors* **2020**, *20*, 2868. [CrossRef]
434. Li, B.; Chenli, C.; Xu, X.; Jung, T.; Shi, Y. Exploiting Computation Power of Blockchain for Biomedical Image Segmentation. In Proceedings of the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach, CA, USA, 16–17 June 2019; pp. 2802–2811. [CrossRef]
435. Li, B.; Chenli, C.; Xu, X.; Shi, Y.; Jung, T. DLBC: A Deep Learning-Based Consensus in Blockchains for Deep Learning Services. *arXiv* **2019**, arXiv:1904.07349.
436. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *J. Med. Syst.* **2018**, *42*, 136. [CrossRef] [PubMed]
437. Kumar, N.; Parangjothi, C.; Guru, S.; Kiran, M. Peer Consonance in Blockchain based Healthcare Application using AI-based Consensus Mechanism. In Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 1–3 July 2020; pp. 1–7. [CrossRef]
438. Pohl, M.; Nahhas, A.; Bosse, S.; Turowski, K. Proof of Provision: Improving Blockchain Technology by Cloud Computing. In Proceedings of the 9th International Conference on Cloud Computing and Services Science, SCITEPRESS—Science and Technology Publications, Heraklion, Crete, Greece, 2–4 May 2019; pp. 523–527. [CrossRef]
439. Mythili, R.; Venkataraman, R. Proof of Policy (PoP): A New Attribute-Based Blockchain Consensus Protocol. In *Computational Methods and Data Engineering*; Singh, V., Asari, V., Kumar, S., Patel, R., Eds.; Springer: Singapore, 2021; pp. 451–464. [CrossRef]
440. Yang, J.; Onik, M.; Lee, N.Y.; Ahmed, M.; Kim, C.S. Proof-of-Familiarity: A Privacy-Preserved Blockchain Scheme for Collaborative Medical Decision-Making. *Appl. Sci.* **2019**, *9*, 1370. [CrossRef]
441. Malamas, V.; Dasaklis, T.; Kotzanikolaou, P.; Burmester, M.; Katsikas, S. A Forensics-by-Design Management Framework for Medical Devices Based on Blockchain. In Proceedings of the 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 8–13 July 2019; pp. 35–40. [CrossRef]
442. Oyinloye, D.P.; Teh, J.S.; Jamil, N.; Alawida, M. Blockchain Consensus: An Overview of Alternative Protocols. *Symmetry* **2021**, *13*, 1363. [CrossRef]
443. Merrad, Y.; Habaebi, M.H.; Elsheikh, E.A.A.; Suliman, F.E.M.; Islam, M.R.; Gunawan, T.S.; Mesri, M. Blockchain: Consensus Algorithm Key Performance Indicators, Trade-Offs, Current Trends, Common Drawbacks, and Novel Solution Proposals. *Mathematics* **2022**, *10*, 2754. [CrossRef]
444. Lee, D.R.; Jang, Y.; Kim, H. Poster: A Proof-of-Stake (PoS) Blockchain Protocol using Fair and Dynamic Sharding Management. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; ACM: New York, NY, USA, 2019; pp. 2553–2555. [CrossRef]
445. Jiao, Z.; Tian, R.; Shang, D.; Ding, H. Bicomp: A Bilayer Scalable Nakamoto Consensus Protocol. *arXiv* **2018** arXiv:1809.01593.
446. Gupta, K.D.; Rahman, A.; Poudyal, S.; Huda, M.N.; Mahmud, M.A.P. A Hybrid POW-POS Implementation Against 51 percent Attack in Cryptocurrency System. In Proceedings of the 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Sydney, NSW, Australia, 11–13 December 2019; pp. 396–403. [CrossRef]
447. Long, J.; Wei, R. Scalable BFT Consensus Mechanism Through Aggregated Signature Gossip. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 360–367. [CrossRef]
448. Bravo, M.; István, Z.; Sit, M.K. Towards Improving the Performance of BFT Consensus For Future Permissioned Blockchains. *arXiv* **2020**, arXiv:2007.12637.
449. Du, N.; Liang, Z.; Huang, Y.; Guo, Z.; Yang, H.; Wang, S. Performance optimisation Method of PBFT Consensus for Supply Chain Integration SVM. In Proceedings of the 2020 7th International Conference on Dependable Systems and Their Applications (DSA), Xi'an, China, 28–29 November 2020; pp. 371–377. [CrossRef]
450. Chengfu, Y. Research on Autonomous and Controllable High-performance Consensus Mechanism of Blockchain. In Proceedings of the 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, 25–27 August 2020; pp. 223–228. [CrossRef]
451. Duan, S.; Reiter, M.K.; Zhang, H. BEAT: Asynchronous BFT Made Practical. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; ACM: New York, NY, USA, 2018; pp. 2028–2041. [CrossRef]

452. Gai, K.; Hu, Z.; Zhu, L.; Wang, R.; Zhang, Z. Blockchain Meets DAG: A BlockDAG Consensus Mechanism. In *Algorithms and Architectures for Parallel Processing*; Qiu, M., Ed.; Springer: Cham, Switzerland, 2020; pp. 110–125. [CrossRef]
453. Cong, K.; Ren, Z.; Pouwelse, J. A Blockchain Consensus Protocol With Horizontal Scalability. In Proceedings of the 2018 IFIP Networking Conference (IFIP Networking) and Workshops, Zurich, Switzerland, 14–16 May 2018; pp. 1–9. [CrossRef]
454. Santiago, C.; Ren, S.; Lee, C.; Ryu, M. Concordia: A Streamlined Consensus Protocol for Blockchain Networks. *IEEE Access* **2021**, *9*, 13173–13185. [CrossRef]
455. Lin, T.; Yang, X.; Wang, T.; Peng, T.; Xu, F.; Lao, S.; Ma, S.; Wang, H.; Hao, W. Implementation of High-Performance Blockchain Network Based on Cross-Chain Technology for IoT Applications. *Sensors* **2020**, *20*, 3268. [CrossRef]
456. Kiamari, M.; Krishnamachari, B.; Naveed, M.; Yun, S. Distributed Consensus for Mobile Devices using Online Brokers. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020; pp. 1–3. [CrossRef]
457. Khan, N. FAST: A MapReduce Consensus for High Performance Blockchains. In Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, Shenzhen, China, 4 November 2018; ACM: New York, NY, USA, 2018; pp. 1–6. [CrossRef]
458. Popov, S.; Buchanan, W.J. FPC-BI: Fast Probabilistic Consensus within Byzantine Infrastructures. *J. Parallel Distrib. Comput.* **2021**, *147*, 77–86. [CrossRef]
459. Song, A.; Wang, J.; Yu, W.; Dai, Y.; Zhu, H. Fast, Dynamic and Robust Byzantine Fault Tolerance Protocol for Consortium Blockchain. In Proceedings of the 2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), Xiamen, China, 16–18 December 2019; pp. 419–426. [CrossRef]
460. Baudet, M.; Danezis, G.; Sonnino, A. FastPay: High-Performance Byzantine Fault Tolerant Settlement. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, New York, NY, USA, 21–23 October 2020; ACM: New York, NY, USA, 2020; pp. 163–177. [CrossRef]
461. Buchnik, Y.; Friedman, R. FireLedger. *Proc. VLDB Endow.* **2020**, *13*, 1525–1539. [CrossRef]
462. Chander, G.; Deshpande, P.; Chakraborty, S. A Fault Resilient Consensus Protocol for Large Permissioned Blockchain Networks. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 33–37. [CrossRef]
463. Li, P.; Wang, G.; Chen, X.; Long, F.; Xu, W. Gosig: a scalable and high-performance byzantine consensus for consortium blockchains. In Proceedings of the 11th ACM Symposium on Cloud Computing, Virtual, 19–21 October 2020; ACM: New York, NY, USA, 2020; pp. 223–237. [CrossRef]
464. Jiang, Y.; Lian, Z. High Performance and Scalable Byzantine Fault Tolerance. In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 15–17 March 2019; pp. 1195–1202. [CrossRef]
465. Jiang, Y.; Ding, S. A High Performance Consensus Algorithm for Consortium Blockchain. In Proceedings of the 2018 IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 7–10 December 2018; pp. 2379–2386. [CrossRef]
466. Gao, Z.; Yang, L. Optimization Scheme of Consensus Mechanism Based on Practical Byzantine Fault Tolerance Algorithm. In *Blockchain Technology and Application*; Springer: Singapore, 2020; pp. 187–195. [CrossRef]
467. Huang, T.L.; Huang, J. Design and analysis of a distributed consensus protocol for real-time blockchain systems. In Proceedings of the 2020 International Computer Symposium (ICS), Tainan, Taiwan, 17–19 December 2020; pp. 179–184. [CrossRef]
468. Du, M.; Chen, Q.; Ma, X. MBFT: A New Consensus Algorithm for Consortium Blockchain. *IEEE Access* **2020**, *8*, 87665–87675. [CrossRef]
469. Du, M.; Chen, Q.; Chen, J.; Ma, X. An Optimized Consortium Blockchain for Medical Information Sharing. *IEEE Trans. Eng. Manag.* **2021**, *68*, 1677–1689. [CrossRef]
470. Gupta, S.; Hellings, J.; Rahnama, S.; Sadoghi, M. Proof-of-Execution: Reaching Consensus through Fault-Tolerant Speculation. *arXiv* **2019**, arXiv:1911.00838.
471. Al-Mamun, A.; Zhao, D. SciChain: Trustworthy Scientific Data Provenance. *arXiv* **2020**, arXiv:2002.00141.
472. Kim, D.; Doh, I.; Chae, K. Improved Raft Algorithm exploiting Federated Learning for Private Blockchain performance enhancement. In Proceedings of the 2021 International Conference on Information Networking (ICOIN), Jeju Island, Korea, 13–16 January 2021; pp. 828–832. [CrossRef]
473. Chomsiri, T.; Kongsup, K. P Coin: High Speed Cryptocurrency Based on Random-Checkers Proof of Stake. In Proceedings of the 2018 Joint 10th International Conference on Soft Computing and Intelligent Systems (SCIS) and 19th International Symposium on Advanced Intelligent Systems (ISIS), Toyama, Japan, 5–8 December 2018; pp. 524–529. [CrossRef]
474. Gunn, L.J.; Liu, J.; Vavala, B.; Asokan, N. Making Speculative BFT Resilient with Trusted Monotonic Counters. In Proceedings of the 2019 38th Symposium on Reliable Distributed Systems (SRDS), Lyon, France, 1–4 October 2019; pp. 133–13309. [CrossRef]
475. Feng, L.; Zhang, H.; Chen, Y.; Lou, L. Scalable Dynamic Multi-Agent Practical Byzantine Fault-Tolerant Consensus in Permissioned Blockchain. *Appl. Sci.* **2018**, *8*, 1919. [CrossRef]
476. Jiang, Y.; Lian, Z. Scalable Efficient Byzantine Fault Tolerance. In Proceedings of the 2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Chongqing, China, 11–13 October 2019; pp. 1736–1742. [CrossRef]

477. Chen, Y.; Chen, Q.; Xie, Y. A Methodology for High-efficient Federated-learning with Consortium Blockchain. In Proceedings of the 2020 IEEE 4th Conference on Energy Internet and Energy System Integration (EI2), Wuhan, China, 30 October–1 November 2020; pp. 3090–3095. [CrossRef]
478. Dolev, S.; Wang, Z. SodsBC: Stream of Distributed Secrets for Quantum-safe Blockchain. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; pp. 247–256. [CrossRef]
479. Gao, S.; Yu, T.; Zhu, J.; Cai, W. T-PBFT: An EigenTrust-based practical Byzantine fault tolerance consensus algorithm. *China Commun.* **2019**, *16*, 111–123. [CrossRef]
480. Basescu, C.; Kokoris-Kogias, E.; Ford, B.A. Low-latency Blockchain Consensus. In Proceedings of the 38th IEEE Symposium on Security and Privacy, San Jose, CA, USA, 22–24 May 2017.
481. Al-Mamun, A.; Zhao, D. BAASH: Enabling Blockchain-as-a-Service on High-Performance Computing Systems. *arXiv* **2020**, arXiv:2001.07022.
482. Luo, Y.; Deng, X.; Wu, Y.; Wang, J. MPC-DPOS: An efficient consensus algorithm based on secure multi-party computation. In Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, Xi'an, China, 9–11 December 2019; ACM: New York, NY, USA, 2019; pp. 105–112. [CrossRef]
483. Luo, Y.; Chen, Y.; Chen, Q.; Liang, Q. A New Election Algorithm for DPos Consensus Mechanism in Blockchain. In Proceedings of the 2018 7th International Conference on Digital Home (ICDH), Guilin, China, 30 November–1 December 2018; pp. 116–120. [CrossRef]
484. Cao, K.; Lin, F.; Qian, C.; Li, K. A High Efficiency Network Using DAG and Consensus in Blockchain. In Proceedings of the 2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), Xiamen, China, 16–18 December 2019; pp. 279–285. [CrossRef]
485. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A. Internet of Things: Security and Solutions Survey. *Sensors* **2022**, *22*, 7433. [CrossRef]
486. Lei, M.; Xu, L.; Liu, T.; Liu, S.; Sun, C. Integration of Privacy Protection and Blockchain-Based Food Safety Traceability: Potential and Challenges. *Foods* **2022**, *11*, 2262. [CrossRef] [PubMed]
487. Gu, F.; Yang, X.; Li, X.; Deng, H. Computational Resources Allocation and Vehicular Application Offloading in VEC Networks. *Electronics* **2022**, *11*, 2130. [CrossRef]
488. Gupta, Y.; Shorey, R.; Kulkarni, D.; Tew, J. The applicability of blockchain in the Internet of Things. In Proceedings of the 2018 10th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 3–7 January 2018; pp. 561–564. [CrossRef]
489. Liu, Y.; Wang, K.; Qian, K.; Du, M.; Guo, S. Tornado: Enabling Blockchain in Heterogeneous Internet of Things Through a Space-Structured Approach. *IEEE Internet Things J.* **2020**, *7*, 1273–1286. [CrossRef]
490. Huang, J.; Kong, L.; Chen, G.; Wu, M.Y.; Liu, X.; Zeng, P. Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3680–3689. [CrossRef]
491. Huang, J.; Kong, L.; Chen, G.; Cheng, L.; Wu, K.; Liu, X. B-IoT: Blockchain Driven Internet of Things with Credit-Based Consensus Mechanism. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 1348–1357. [CrossRef]
492. Huang, Y.; Zeng, Y.; Ye, F.; Yang, Y. Incentive Assignment in PoW and PoS Hybrid Blockchain in Pervasive Edge Environments. In Proceedings of the 2020 IEEE/ACM 28th International Symposium on Quality of Service (IWQoS), Hang Zhou, China, 15–17 June 2020; pp. 1–10. [CrossRef]
493. Lin, X.; Li, J.; Wu, J.; Liang, H.; Yang, W. Making Knowledge Tradable in Edge-AI Enabled IoT: A Consortium Blockchain-Based Efficient and Incentive Approach. *IEEE Trans. Ind. Inform.* **2019**, *15*, 6367–6378. [CrossRef]
494. Du, X.F.; Lu, Y.M.; Han, D.Q. Point-to-Point Offline Authentication Consensus Algorithm in the Internet of Things. In *Artificial Intelligence and Security*; Sun, X., Wang, J., Bertino, E., Eds.; Springer: Cham, Switzerland, 2020; pp. 655–663. [CrossRef]
495. Du, M.; Wang, K.; Liu, Y.; Qian, K.; Sun, Y.; Xu, W.; Guo, S. Spacechain: A Three-Dimensional Blockchain Architecture for IoT Security. *IEEE Wirel. Commun.* **2020**, *27*, 38–45. [CrossRef]
496. Liao, D.; Li, H.; Wang, W.; Wang, X.; Zhang, M.; Chen, X. Achieving IoT data security based blockchain. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 2694–2707. [CrossRef]
497. Hu, X.; Zheng, Y.; Su, Y.; Guo, R. IoT Adaptive Dynamic Blockchain Networking Method Based on Discrete Heartbeat Signals. *Sensors* **2020**, *20*, 6503. [CrossRef] [PubMed]
498. Chuang, I.H.; Chiang, S.H.; Chao, W.C.; Huang, S.H.; Zeng, B.L.; Kuo, Y.H. A Hierarchical Blockchain-based Data Service Platform in MEC Environments. In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology, Hilo, HI, USA, 12–14 March 2020; ACM: New York, NY, USA, 2020; pp. 95–99. [CrossRef]
499. Chen, J.; Wu, J.; Liang, H.; Mumtaz, S.; Li, J.; Konstantin, K.; Bashir, A.K.; Nawaz, R. Collaborative Trust Blockchain Based Unbiased Control Transfer Mechanism for Industrial Automation. *IEEE Trans. Ind. Appl.* **2020**, pp. 1. [CrossRef]
500. Melnik, E.V.; Klimenko, A.; Korobkin, V.V. Fault-Tolerant Management for the Edge Devices on the Basis of Consensus with Elected Leader. In *Software Engineering Perspectives in Intelligent Systems*; Silhavy, R., Silhavy, P., Prokopova, Z., Eds.; Springer, Cham, Switzerland, 2020; pp. 464–474. [CrossRef]

501. Lunardi, R.C.; Alharby, M.; Nunes, H.C.; Zorzo, A.F.; Dong, C.; van Moorsel, A. Context-based consensus for appendable-block blockchains. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; pp. 401–408. [CrossRef]
502. Li, W.; Feng, C.; Zhang, L.; Xu, H.; Cao, B.; Imran, M.A. A Scalable Multi-Layer PBFT Consensus for Blockchain. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 1146–1160. [CrossRef]
503. Cho, S.; Park, S.Y.; Lee, S.R. Blockchain Consensus Rule Based Dynamic Blind Voting for Non-Dependency Transaction. *Int. J. Grid Distrib. Comput.* **2017**, *10*, 93–106. [CrossRef]
504. Fan, K.; Wang, S.; Ren, Y.; Yang, K.; Yan, Z.; Li, H.; Yang, Y. Blockchain-Based Secure Time Protection Scheme in IoT. *IEEE Internet Things J.* **2019**, *6*, 4671–4679. [CrossRef]
505. Abdulkader, O.; Bamhdi, A.M.; Thayananthan, V.; Elbouraey, F.; Al-Ghamdi, B. A Lightweight Blockchain Based Cybersecurity for IoT environments. In Proceedings of the 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Paris, France, 21–23 June 2019; pp. 139–144. [CrossRef]
506. Moudoud, H.; Cherkaoui, S.; Khoukhi, L. An IoT Blockchain Architecture Using Oracles and Smart Contracts: the Use-Case of a Food Supply Chain. In Proceedings of the 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Istanbul, Turkey, 8–11 September 2019; pp. 1–6. [CrossRef]
507. Huang, C.W.; Chen, Y.C. ZeroCalo: A Lightweight Blockchain Based on DHT Network. In Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, Xi'an, China, 9–11 December 2019; ACM: New York, NY, USA, 2019; pp. 38–42. [CrossRef]
508. Alkhodair, A.; Mohanty, S.; Kougianos, E.; Puthal, D. McPoRA: A Multi-chain Proof of Rapid Authentication for Post-Blockchain Based Security in Large Scale Complex Cyber-Physical Systems. In Proceedings of the 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Limassol, Cyprus, 6–8 July 2020; pp. 446–451. [CrossRef]
509. Guo, S.; Hu, X.; Guo, S.; Qiu, X.; Qi, F. Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System. *IEEE Trans. Ind. Inform.* **2020**, *16*, 1972–1983. [CrossRef]
510. Mamun, Q.; Khan, M.A. A Group Mutual Exclusion protocol for the Use Case of IoT-Blockchain Integration In Work-Safe Scenario. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 25–30. [CrossRef]
511. Hossain, M.T.; Badsha, S.; Shen, H. PoRCH: A Novel Consensus Mechanism for Blockchain-Enabled Future SCADA Systems in Smart Grids and Industry 4.0. In Proceedings of the 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Vancouver, BC, Canada, 9–12 September 2020; pp. 1–7. [CrossRef]
512. Majdoubi, D.E.; El Bakkali, H.; Sadki, S. Towards Smart Blockchain-Based System for Privacy and Security in a Smart City environment. In Proceedings of the 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech), Marrakesh, Morocco, 24–26 November 2020; pp. 1–7. [CrossRef]
513. Liao, S.; Wu, J.; Li, J.; Bashir, A.K. Proof-of-Balance: Game-Theoretic Consensus for Controller Load Balancing of SDN. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 231–236. [CrossRef]
514. Biswas, S.; Sharif, K.; Li, F.; Maharjan, S.; Mohanty, S.P.; Wang, Y. PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain. *IEEE Internet Things J.* **2020**, *7*, 2343–2355. [CrossRef]
515. Doku, R.; Rawat, D.B.; Garuba, M.; Njilla, L. Fusion of Named Data Networking and Blockchain for Resilient Internet-of-Battlefield-Things. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020. [CrossRef]
516. Doku, R.; Rawat, D.B. IFLBC: On the Edge Intelligence Using Federated Learning Blockchain Network. In Proceedings of the 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Baltimore, MD, USA, 25–27 May 2020; pp. 221–226. [CrossRef]
517. Li, G.; Dong, M.; Yang, L.T.; Ota, K.; Wu, J.; Li, J. Preserving Edge Knowledge Sharing Among IoT Services: A Blockchain-Based Approach. *IEEE Trans. Emerg. Top. Comput. Intell.* **2020**, *4*, 653–665. [CrossRef]
518. Fan, K.; Sun, S.; Yan, Z.; Pan, Q.; Li, H.; Yang, Y. A blockchain-based clock synchronization Scheme in IoT. *Future Gener. Comput. Syst.* **2019**, *101*, 524–533. [CrossRef]
519. Falcone, S.; Zhang, J.; Cameron, A.; Abdel-Rahman, A. Blockchain Design for an Embedded System. *Ledger* **2019**. [CrossRef]
520. Lin, W.; Yin, X.; Wang, S.; Khosravi, M.R. A Blockchain-enabled decentralized settlement model for IoT data exchange services. *Wirel. Netw.* **2020**. [CrossRef]
521. Hou, M.; Kang, T.; Guo, L. A Blockchain Based Architecture for IoT Data Sharing Systems. In Proceedings of the 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Austin, TX, USA, 23–27 March 2020; pp. 1–6. [CrossRef]
522. Mohanty, S.N.; Ramya, K.; Rani, S.S.; Gupta, D.; Shankar, K.; Lakshmanaprabu, S.; Khanna, A. An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. *Future Gener. Comput. Syst.* **2020**, *102*, 1027–1037. [CrossRef]
523. Dorri, A.; Jurdak, R. Tree-Chain: A Fast Lightweight Consensus Algorithm for IoT Applications. In Proceedings of the 2020 IEEE 45th Conference on Local Computer Networks (LCN), Sydney, Australia, 16–19 November 2020; pp. 369–372. [CrossRef]

524. Bai, H.; Xia, G.; Fu, S. A Two-Layer-Consensus Based Blockchain Architecture for IoT. In Proceedings of the 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, 12–14 July 2019; pp. 1–6. [CrossRef]
525. Alhejazi, M.M.; Mohammad, R.M.A. Enhancing the blockchain voting process in IoT using a novel blockchain Weighted Majority Consensus Algorithm (WMCA). *Inf. Secur. J. A Glob. Perspect.* **2022**, *31*, 125–143. [CrossRef]
526. Jinhua, F.; Mixue, X.; Yongzhong, H.; Hongwei, T. A New Network Intrusion Detection System based on Blockchain. *Int. J. Perform. Eng.* **2019**, *15*, 3187. [CrossRef]
527. Guo, S.; Qi, Y.; Jin, Y.; Li, W.; Qiu, X.; Meng, L. Endogenous Trusted DRL-Based Service Function Chain Orchestration for IoT. *IEEE Trans. Comput.* **2022**, *71*, 397–406. [CrossRef]
528. Asheralieva, A.; Niyato, D. Reputation-Based Coalition Formation for Secure Self-Organized and Scalable Sharding in IoT Blockchains With Mobile-Edge Computing. *IEEE Internet Things J.* **2020**, *7*, 11830–11850. [CrossRef]
529. Chen, P.; Han, D.; Weng, T.H.; Li, K.C.; Castiglione, A. A novel Byzantine fault tolerance consensus for Green IoT with intelligence based on reinforcement. *J. Inf. Secur. Appl.* **2021**, *59*, 102821. [CrossRef]
530. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *J. Parallel Distrib. Comput.* **2019**, *134*, 180–197. [CrossRef]
531. Xuan, S.; Chen, Z.; Chung, I.; Tan, H.; Man, D.; Du, X.; Yang, W.; Guizani, M. ECBCM: A prestige-based edge computing blockchain security consensus model. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*. [CrossRef]
532. Lao, L.; Dai, X.; Xiao, B.; Guo, S. G-PBFT: A Location-based and Scalable Consensus Protocol for IoT-Blockchain Applications. In Proceedings of the 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS), New Orleans, LA, USA, 18–22 May 2020; pp. 664–673. [CrossRef]
533. Alrubei, S.; Ball, E.; Rigelsford, J. A Secure Distributed Blockchain Platform for Use in AI-Enabled IoT Applications. In Proceedings of the 2020 IEEE Cloud Summit, Harrisburg, PA, USA, 21–22 October 2020; pp. 85–90. [CrossRef]
534. Alrubei, S.M.; Ball, E.; Rigelsford, J.M. The Use of Blockchain to Support Distributed AI Implementation in IoT Systems. *IEEE Internet Things J.* **2022**, *9*, 14790–14802. [CrossRef]
535. Baniata, H.; Kertesz, A. PF-BVM: A Privacy-aware Fog-enhanced Blockchain Validation Mechanism. In Proceedings of the 10th International Conference on Cloud Computing and Services Science. SCITEPRESS—Science and Technology Publications, Prague, Czech Republic, 7–9 May 2020; pp. 430–439. [CrossRef]
536. Bhamidipati, V.S.V.; Chan, M.; Jain, A.; Murthy, A.S.; Chamorro, D.; Muralidhar, A.K. Predictive Proof of Metrics—A New Blockchain Consensus Protocol. In Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019; pp. 498–505. . [CrossRef]
537. Raghav.; Andola, N.; Venkatesan, S.; Verma, S. PoEWAL: A lightweight consensus mechanism for blockchain in IoT. *PErvasive Mob. Comput.* **2020**, *69*, 101291. [CrossRef]
538. Makhdoom, I.; Tofigh, F.; Zhou, I.; Abolhasan, M.; Lipman, J. PLEDGE: A Proof-of-Honesty based Consensus Protocol for Blockchain-based IoT Systems. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020; pp. 1–3. [CrossRef]
539. Makhdoom, I.; Tofigh, F.; Zhou, I.; Abolhasan, M.; Lipman, J. PLEDGE: An IoT-oriented Proof-of-Honesty based Blockchain Consensus Protocol. In Proceedings of the 2020 IEEE 45th Conference on Local Computer Networks (LCN), Sydney, NSW, Australia, 16–19 November 2020; pp. 54–64. [CrossRef]
540. Feng, J.; Zhao, X.; Lu, G.; Zhao, F. PoTN: A Novel Blockchain Consensus Protocol with Proof-of-Trust Negotiation in Distributed IoT Networks. In Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things—IoT S&P'19, London, UK, 15 November 2019; ACM Press: New York, New York, USA, 2019; pp. 32–37. [CrossRef]
541. Feng, J.; Zhao, X.; Chen, K.; Zhao, F.; Zhang, G. Towards random-honest miners selection and multi-blocks creation: Proof-of-negotiation consensus mechanism in blockchain networks. *Future Gener. Comput. Syst.* **2020**, *105*, 248–258. [CrossRef]
542. Solat, S. RDV: An Alternative To Proof-of-Work And A Real Decentralized Consensus For Blockchain. In Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, Shenzhen, China, 4 November 2018; ACM: New York, NY, USA, 2018; pp. 25–31. [CrossRef]
543. Asiri, S.; Miri, A. A Sybil Resistant IoT Trust Model Using Blockchains. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1017–1026. [CrossRef]
544. Liu, Y.; Wang, K.; Lin, Y.; Xu, W. LightChain: A Lightweight Blockchain System for Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3571–3581. [CrossRef]
545. Ledwaba, L.P.; Hancke, G.P.; Mitrokotsa, A.; Isaac, S.J. A Delegated Proof of Proximity Scheme for Industrial Internet of Things Consensus. In Proceedings of the IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society, Singapore, 18–21 October 2020; pp. 4441–4446. [CrossRef]
546. Maitra, S.; Yanambaka, V.P.; Abdelgawad, A.; Puthal, D.; Yelamarthi, K. Proof-of-Authentication Consensus Algorithm: Blockchain-based IoT Implementation. In Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020; pp. 1–2. [CrossRef]
547. Puthal, D.; Mohanty, S.P. Proof of Authentication: IoT-Friendly Blockchains. *IEEE Potentials* **2019**, *38*, 26–29. [CrossRef]

548. Puthal, D.; Mohanty, S.P.; Nanda, P.; Kougianos, E.; Das, G. Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019; pp. 1–5. [CrossRef]
549. Asif, R.; Ghanem, K.; Irvine, J. Proof-of-PUF Enabled Blockchain: Concurrent Data and Device Security for Internet-of-Energy. *Sensors* **2020**, *21*, 28. [CrossRef]
550. Chen, J. Hybrid blockchain and pseudonymous authentication for secure and trusted IoT networks. *ACM SIGBED Rev.* **2018**, *15*, 22–28. [CrossRef]
551. Wang, E.K.; Liang, Z.; Chen, C.M.; Kumari, S.; Khan, M.K. PoRX: A reputation incentive scheme for blockchain consensus of IIoT. *Future Gener. Comput. Syst.* **2020**, *102*, 140–151. [CrossRef]
552. Kumar, G.; Saha, R.; Rai, M.K.; Thomas, R.; Kim, T.H. Proof-of-Work Consensus Approach in Blockchain Technology for Cloud and Fog Computing Using Maximization-Factorization Statistics. *IEEE Internet Things J.* **2019**, *6*, 6835–6842. [CrossRef]
553. Mohanty, S.P.; Yanambaka, V.P.; Kougianos, E.; Puthal, D. PUFchain: A Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE). *IEEE Consum. Electron. Mag.* **2020**, *9*, 8–16. [CrossRef]
554. Valeonti, F.; Bikakis, A.; Terras, M.; Speed, C.; Hudson-Smith, A.; Chalkias, K. Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs). *Appl. Sci.* **2021**, *11*, 9931. [CrossRef]
555. Ippolito, J. Crypto-Preservation and the Ghost of Andy Warhol. *Arts* **2022**, *11*, 47. [CrossRef]
556. Colicev, A. How can non-fungible tokens bring value to brands. *Int. J. Res. Mark.* **2022**. [CrossRef]
557. Zaucha, T.; Agur, C. Newly minted: Non-fungible tokens and the commodification of fandom. *New Media Soc.* **2022**, 146144482210804. [CrossRef]
558. Bao, H.; Roubaud, D. Recent Development in Fintech: Non-Fungible Token. *FinTech* **2021**, *1*, 44–46. [CrossRef]
559. Yuen, H.Y.; Wu, F.; Cai, W.; Chan, H.C.; Yan, Q.; Leung, V.C. Proof-of-Play: A Novel Consensus Model for Blockchain-based Peer-to-Peer Gaming System. In Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure—BSCI '19, Auckland, New Zealand, 8 July 2019; ACM Press: New York, New York, USA, 2019; pp. 19–28. [CrossRef]
560. Chen, Q.; Srivastava, G.; Parizi, R.M.; Aloqaily, M.; Ridhawi, I.A. An incentive-aware blockchain-based solution for internet of fake media things. *Inf. Process. Manag.* **2020**, *57*, 102370. [CrossRef]
561. Song, H.; Zhu, N.; Xue, R.; He, J.; Zhang, K.; Wang, J. Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection. *Inf. Process. Manag.* **2021**, *58*, 102507. [CrossRef]
562. Kim, J.S.; Shin, N. The Impact of Blockchain Technology Application on Supply Chain Partnership and Performance. *Sustainability* **2019**, *11*, 6181. [CrossRef]
563. Dutta, P.; Choi, T.M.; Somani, S.; Butala, R. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transp. Res. Part E Logist. Transp. Rev.* **2020**, *142*, 102067. [CrossRef]
564. Rejeb, A.; Keogh, J.G.; Treiblmaier, H. Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management. *Future Internet* **2019**, *11*, 161. [CrossRef]
565. Mao, T.; Fan, Y.; Yang, J.; Wei, H. A Research on Tea Traceability Consensus Mechanism Based on Blockchain Technology. In *New Developments of IT, IoT and ICT Applied to Agriculture*; Nakamatsu, K., Kountchev, R., Aharari, A., El-Bendary, N., Hu, B., Eds.; Springer: Singapore, 2021; pp. 129–137. [CrossRef]
566. Li, H.; Han, D.; Tang, M. Logisticschain: A Blockchain-Based Secure Storage Scheme for Logistics Data. *Mob. Inf. Syst.* **2021**, *2021*, 1–15. [CrossRef]
567. Li, X.; Lv, F.; Xiang, F.; Sun, Z.; Sun, Z. Research on Key Technologies of Logistics Information Traceability Model Based on Consortium Chain. *IEEE Access* **2020**, *8*, 69754–69762. [CrossRef]
568. Kumar, G.; Saha, R.; Buchanan, W.J.; Geetha, G.; Thomas, R.; Rai, M.K.; Kim, T.H.; Alazab, M. Decentralized accessibility of e-commerce products through blockchain technology. *Sustain. Cities Soc.* **2020**, *62*, 102361. [CrossRef]
569. Fang, Z.; Wei, Z.; Wang, X.; Xie, W. A Blockchain Consensus Mechanism for Marine Data Management System. In *Blockchain and Trustworthy Systems*; Zheng, Z., Dai, H.N., Fu, X., Chen, B., Eds.; Springer: Singapore, 2020; pp. 18–30. [CrossRef]
570. Mao, D.; Hao, Z.; Wang, F.; Li, H. Innovative Blockchain-Based Approach for Sustainable and Credible Environment in Food Trade: A Case Study in Shandong Province, China. *Sustainability* **2018**, *10*, 3149. [CrossRef]
571. Mao, D.; Hao, Z.; Wang, F.; Li, H. Novel Automatic Food Trading System Using Consortium Blockchain. *Arab. J. Sci. Eng.* **2019**, *44*, 3439–3455. [CrossRef]
572. Fu, Y.; Chen, H.; Qian, J.; Dong, Y. A PoL Protocol for Spatiotemporal Blockchain. In *Security and Privacy in Digital Economy*; Yu, S., Mueller, P., Qian, J., Eds.; 2020; Springer: Singapore, pp. 591–605. [CrossRef]
573. Darmwal, R. Blockchain in Telecom Sector: An Analysis of Potential Use Cases. *Telecom Bus. Rev.* **2017**, *10*, 68–75.
574. Lwin, M.T.; Yim, J.; Ko, Y.B. Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks. *Sensors* **2020**, *20*, 698. [CrossRef] [PubMed]
575. Lin, W.; Xu, X.; Qi, L.; Zhang, X.; Dou, W.; Khosravi, M.R. A Proof-of-Majority Consensus Protocol for Blockchain-enabled Collaboration Infrastructure of 5G Network Slice Brokers. In Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, Taipei, Taiwan, 6 October 2020; ACM: New York, NY, USA, 2020; pp. 41–52. [CrossRef]

576. Lihu, A.; Du, J.; Barjaktarevic, I.; Gerzanics, P.; Harvilla, M. A Proof of Useful Work for Artificial Intelligence on the Blockchain. *arXiv* **2020**, arXiv:2001.09244.
577. Li, W. Adapting Blockchain Technology for Scientific Computing. *arXiv* **2018**, arXiv:1804.08230.
578. Géraud, R.; Naccache, D.; Roşie, R. Twisting Lattice and Graph Techniques to Compress Transactional Ledgers. In *Security and Privacy in Communication Networks*; Lin, X., Ghorbani, A., Ren, K., Zhu, S., Zhang, A., Eds.; Springer, Cham, Switzerland, 2018; pp. 108–127. [CrossRef]
579. Ding, J. A New Proof of Work for Blockchain Based on Random Multivariate Quadratic Equations. In *Applied Cryptography and Network Security Workshops*; Springer, Cham, Switzerland, 2019; pp. 97–107. [CrossRef]
580. Hastings, M.; Heninger, N.; Wustrow, E. Short Paper: The Proof is in the Pudding. In *Financial Cryptography and Data Security*; Goldberg, I., Moore, T., Eds.; Springer, Cham, Switzerland, 2019; pp. 396–404. [CrossRef]
581. Boyd, C.; Carr, C. Valuable Puzzles for Proofs-of-Work, In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*; Garcia-Alfaro, J., Herrera-Joancomartí, J., Livraga, G., Rios, R., Eds.; Springer, Cham, Switzerland, 2018; pp. 130–139. [CrossRef]
582. Baldominos, A.; Saez, Y. Coin.AI: A Proof-of-Useful-Work Scheme for Blockchain-Based Distributed Deep Learning. *Entropy* **2019**, *21*, 723. [CrossRef]
583. Loe, A.F.; Quaglia, E.A. Conquering Generals. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Munich, Germany, 15 June 2018; ACM: New York, NY, USA, 2018; pp. 54–59. [CrossRef]
584. Philippopoulos, P.; Ricottone, A.; G. Oliver, C. Difficulty Scaling in Proof of Work for Decentralized Problem Solving. *Ledger* **2020**, *5*. [CrossRef]
585. Chatterjee, K.; Goharshady, A.K.; Pourdamghani, A. Hybrid mining. In Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, Limassol, Cyprus, 8–12 April 2019; ACM: New York, NY, USA, 2019; pp. 374–381. [CrossRef]
586. Billings, J. Image-based Proof of Work Algorithm for the Incentivization of Blockchain Archival of Interesting Images. *arXiv* **2017**, arXiv:1707.04558.
587. Pietrzak, K. Proofs of Catalytic Space. In *Leibniz International Proceedings in Informatics (LIPIcs), Proceedings of the 10th Innovations in Theoretical Computer Science Conference (ITCS 2019), San Diego, CA, USA, 10–12 January 2019*; Blum, A., Ed.; Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik: Dagstuhl, Germany, 2018; Volume 124, pp. 59:1–59:25. [CrossRef]
588. Mittal, A.; Aggarwal, S. Hyperparameter Optimization Using Sustainable Proof of Work in Blockchain. *Front. Blockchain* **2020**, *3*. [CrossRef]
589. Bizzaro, F.; Conti, M.; Pini, M.S. Proof of Evolution: Leveraging blockchain mining for a cooperative execution of Genetic Algorithms. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; pp. 450–455. [CrossRef]
590. Chenli, C.; Li, B.; Shi, Y.; Jung, T. Energy-recycling Blockchain with Proof-of-Deep-Learning. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 19–23. [CrossRef]
591. Chenli, C.; Li, B.; Jung, T. DLchain: Blockchain with Deep Learning as Proof-of-Useful-Work. In *Lecture Notes in Computer Science*; Ferreira, J.E., Palanisamy, B., Ye, K., Kantamneni, S., Zhang, LJ., Eds.; Springer: Cham, Switzerland, 2020; pp. 43–60. [CrossRef]
592. Shoker, A. Sustainable blockchain through proof of exercise. In Proceedings of the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 30 October–1 November 2017; pp. 1–9. [CrossRef]
593. Bravo-Marquez, F.; Reeves, S.; Ugarte, M. Proof-of-Learning: A Blockchain Consensus Mechanism Based on Machine Learning Competitions. In Proceedings of the 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA, 4–9 April 2019; pp. 119–124. [CrossRef]
594. Qiu, C.; Wang, X.; Yao, H.; Du, J.; Yu, F.R.; Guo, S. Networking Integrated Cloud–Edge–End in IoT: A Blockchain-Assisted Collective Q -Learning Approach. *IEEE Internet Things J.* **2021**, *8*, 12694–12704. [CrossRef]
595. Arslan, S.S.; Goker, T. Compress-Store on Blockchain: A Decentralized Data Processing and Immutable Storage for Multimedia Streaming. *arXiv* **2019**, arXiv:1905.10458.
596. Mauri, L.; Damiani, E.; Cimato, S. Be Your Neighbor's Miner: Building Trust in Ledger Content via Reciprocally Useful Work. In Proceedings of the 2020 IEEE 13th International Conference on Cloud Computing (CLOUD), Beijing, China, 19–23 October 2020; pp. 53–62. [CrossRef]
597. Qu, X.; Wang, S.; Hu, Q.; Cheng, X. Proof of Federated Learning: A Novel Energy-Recycling Consensus Algorithm. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 2074–2085. [CrossRef]
598. Li, Z.; Yu, H.; Zhou, T.; Luo, L.; Fan, M.; Xu, Z.; Sun, G. Byzantine Resistant Secure Blockchained Federated Learning at the Edge. *IEEE Netw.* **2021**, *35*, 295–301. [CrossRef]
599. Lan, Y.; Liu, Y.; Li, B. Proof of Learning (PoLe): Empowering Machine Learning with Consensus Building on Blockchains. *arXiv* **2020**, arXiv:2007.15145.
600. Merlina, A. BlockML: A useful proof of work system based on machine learning tasks. In Proceedings of the 20th International Middleware Conference Doctoral Symposium, Davis, CA, USA, 9–13 December 2019; ACM: New York, NY, USA, 2019; pp. 6–8. [CrossRef]
601. Shibata, N. Proof-of-Search: Combining Blockchain Consensus Formation With Solving Optimization Problems. *IEEE Access* **2019**, *7*, 172994–173006. [CrossRef]

602. Badreddin, O.; Hamou-Lhadj, W.; Chauhan, S. Susereum: Towards a Reward Structure for Sustainable Scientific Research Software. In Proceedings of the 2019 IEEE/ACM 14th International Workshop on Software Engineering for Science (SE4Science), Montreal, QC, Canada, 28 May 2019; pp. 51–54. [CrossRef]
603. Chen, H.; Asif, S.A.; Park, J.; Shen, C.C.; Bennis, M. Robust Blockchained Federated Learning with Model Validation and Proof-of-Stake Inspired Consensus. *arXiv* **2021**, arXiv:2101.03300.
604. Alladi, T.; Chamola, V.; Sahu, N.; Venkatesh, V.; Goyal, A.; Guizani, M. A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks. *IEEE Commun. Surv. Tutorials* **2022**, *24*, 1212–1239. [CrossRef]
605. Han, Q.; Yang, Y.; Ma, Z.; Li, J.; Shi, Y.; Zhang, J.; Yang, S. CMBIoV: Consensus Mechanism for Blockchain on Internet of Vehicles. In *Blockchain and Trustworthy Systems*; Zheng, Z., Dai, HN., Fu, X., Chen, B.; Eds.; Springer: Singapore, 2020; pp. 347–352. [CrossRef]
606. Javaid, U.; Aman, M.N.; Sikdar, B. A Scalable Protocol for Driving Trust Management in Internet of Vehicles With Blockchain. *IEEE Internet Things J.* **2020**, *7*, 11815–11829. [CrossRef]
607. Javaid, U.; Sikdar, B. A Secure and Scalable Framework for Blockchain Based Edge Computation Offloading in Social Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 4022–4036. [CrossRef]
608. Javaid, U.; Sikdar, B. A Lightweight and Secure Energy Trading Framework for Electric Vehicles. In Proceedings of the 2021 International Conference on Sustainable Energy and Future Electric Transportation (SEFET), Hyderabad, India, 21–23 January 2021; pp. 1–6. [CrossRef]
609. Liu, X.; Huang, H.; Xiao, F.; Ma, Z. A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs. *IEEE Internet Things J.* **2020**, *7*, 4101–4112. [CrossRef]
610. Wang, X.; Xu, C.; Zhou, Z.; Yang, S.; Sun, L. A Survey of Blockchain-based Cybersecurity for Vehicular Networks. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020. [CrossRef]
611. He, Q.; Xu, Y.; Yan, Y.; Wang, J.; Han, Q.; Li, L. A consensus and incentive program for charging piles based on consortium blockchain. *CSEE J. Power Energy Syst.* **2018**, *4*, 452–458. [CrossRef]
612. Kang, J.; Xiong, Z.; Niyato, D.; Ye, D.; Kim, D.I.; Zhao, J. Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2906–2920. [CrossRef]
613. Hu, W.; Hu, Y.; Yao, W.; Li, H. A Blockchain-Based Byzantine Consensus Algorithm for Information Authentication of the Internet of Vehicles. *IEEE Access* **2019**, *7*, 139703–139711. [CrossRef]
614. Jian, X.; Leng, P.; Wang, Y.; Alrashoud, M.; Hossain, M.S. Blockchain-Empowered Trusted Networking for Unmanned Aerial Vehicles in the B5G Era. *IEEE Netw.* **2021**, *35*, 72–77. [CrossRef]
615. Ferrag, M.A.; Maglaras, L. DeliveryCoin: An IDS and Blockchain-Based Delivery Framework for Drone-Delivered Services. *Computers* **2019**, *8*, 58. [CrossRef]
616. Nurfatih, M.S.; bin Idris, M.Y.; Stiawan, D.; Winanto, E.A. Enhancing Trust Model of Information Vehicular Ad-Hoc Networks Through Blockchain Consensus Algorithm. In Proceedings of the 2020 3rd International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, 24–25 November 2020; pp. 487–492. [CrossRef]
617. Ghribi, E.; Khoei, T.T.; Gorji, H.T.; Ranganathan, P.; Kaabouch, N. A Secure Blockchain-based Communication Approach for UAV Networks. In Proceedings of the 2020 IEEE International Conference on Electro Information Technology (EIT), Chicago, IL, USA, 31 July 2020–1 August 2020; pp. 411–415. [CrossRef]
618. Kudva, S.; Badsha, S.; Sengupta, S.; Khalil, I.; Zomaya, A. Towards secure and practical consensus for blockchain based VANET. *Inf. Sci.* **2021**, *545*, 170–187. [CrossRef]
619. Guo, H.; Meamari, E.; Shen, C.C. Blockchain-inspired Event Recording System for Autonomous Vehicles. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018; pp. 218–222. [CrossRef]
620. Guo, H.; Li, W.; Nejad, M.; Shen, C.C. Proof-of-Event Recording System for Autonomous Vehicles: A Blockchain-Based Solution. *IEEE Access* **2020**, *8*, 182776–182786. [CrossRef]
621. Bathen, L.A.D.; Flores, G.H.; Jadav, D. RiderS: Towards a Privacy-Aware Decentralized Self-Driving Ride-Sharing Ecosystem. In Proceedings of the 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Oxford, UK, 3–6 August 2020; pp. 32–41. [CrossRef]
622. Ahn, N.Y.; Lee, D.H. Secure Vehicle Communications Using Proof-of-Nonce Blockchain. *arXiv* **2020**, arXiv:2011.07846.
623. Chai, H.; Leng, S.; Zhang, K.; Mao, S. Proof-of-Reputation Based-Consortium Blockchain for Trust Resource Sharing in Internet of Vehicles. *IEEE Access* **2019**, *7*, 175744–175757. [CrossRef]
624. Dai, Y.; Xu, D.; Zhang, K.; Maharjan, S.; Zhang, Y. Permissioned Blockchain and Deep Reinforcement Learning for Content Caching in Vehicular Edge Computing and Networks. In Proceedings of the 2019 11th International Conference on Wireless Communications and Signal Processing (WCSP), Xi'an, China, 23–25 October 2019; pp. 1–6. [CrossRef]
625. Dai, Y.; Xu, D.; Zhang, K.; Maharjan, S.; Zhang, Y. Deep Reinforcement Learning and Permissioned Blockchain for Content Caching in Vehicular Edge Computing and Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4312–4324. [CrossRef]
626. Islam, S.; Badsha, S.; Sengupta, S. A Light-weight Blockchain Architecture for V2V Knowledge Sharing at Vehicular Edges. In Proceedings of the 2020 IEEE International Smart Cities Conference (ISC2), Piscataway, NJ, USA, 28 September–1 October 2020; pp. 1–8. [CrossRef]

627. Maskey, S.R.; Badsha, S.; Sengupta, S.; Khalil, I. Reputation-Based Miner Node Selection in Blockchain-Based Vehicular Edge Computing. *IEEE Consum. Electron. Mag.* **2021**, *10*, 14–22. [CrossRef]
628. Dwivedi, S.K.; Amin, R.; Vollala, S. Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. *J. Inf. Secur. Appl.* **2020**, *54*, 102554. [CrossRef]
629. Ge, C.; Ma, X.; Liu, Z. A semi-autonomous distributed blockchain-based framework for UAVs system. *J. Syst. Archit.* **2020**, *107*, 101728. [CrossRef]
630. Liu, J.; Zhang, X.; Li, Y.; Cui, Q.; Tao, X. Blockchain-Empowered Content Cache System for Vehicle Edge Computing Networks. In *Blockchain and Trustworthy Systems*; Zheng, Z., Dai, HN., Tang, M., Chen, X., Eds.; Springer: Singapore, 2020; pp. 410–421. [CrossRef]
631. Ayaz, F.; Sheng, Z.; Tian, D.; Liang, G.Y.; Leung, V. A Voting Blockchain based Message Dissemination in Vehicular Ad-Hoc Networks (VANETs). In Proceedings of the ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6. [CrossRef]
632. Ayaz, F.; Sheng, Z.; Tian, D.; Leung, V.C.M. Blockchain-Enabled Security and Privacy for Internet-of-Vehicles. In *Internet of Vehicles and its Applications in Autonomous Driving. Unmanned System Technologies*; Gupta, N., Prakash, A., Tripathi, R., Eds.; Springer: Cham, Switzerland, 2021; pp. 123–148. [CrossRef]
633. Fujihara, A. PoWaP: Proof of Work at Proximity for a crowdsensing system for collaborative traffic information gathering. *Internet Things* **2020**, *10*, 100046. [CrossRef]
634. Ma, X.; Ge, C.; Liu, Z. Blockchain-Enabled Privacy-Preserving Internet of Vehicles: Decentralized and Reputation-Based Network Architecture; Springer: Berlin/Heidelberg, Germany, 2019; pp. 336–351. [CrossRef]
635. Ayaz, F.; Sheng, Z.; Tian, D.; Guan, Y.L. A Proof-of-Quality-Factor (PoQF)-Based Blockchain and Edge Computing for Vehicular Message Dissemination. *IEEE Internet Things J.* **2021**, *8*, 2468–2482. [CrossRef]
636. Cachin, C. Blockchains and Consensus Protocols: Snake Oil Warning. In Proceedings of the 2017 13th European Dependable Computing Conference (EDCC), Geneva, Switzerland, 4–8 September 2017; pp. 1–2. [CrossRef]
637. Larimer, D. Momentum—A Memory-hard Proof-of-Work Via Finding Birthday Collisions. Available online: http://www.hashcash.org/papers/momentum.pdf (accessed on 27 October 2022).
638. Ge, L.; Wang, J.; Zhang, G. Survey of Consensus Algorithms for Proof of Stake in Blockchain. *Secur. Commun. Netw.* **2022**, *2022*, 2812526. [CrossRef]
639. Aublin, P.L.; Mokhtar, S.B.; Quema, V. RBFT: Redundant Byzantine Fault Tolerance. In Proceedings of the 2013 IEEE 33rd International Conference on Distributed Computing Systems, Philadelphia, PA, USA, 8–11 July 2013; pp. 297–306. [CrossRef]
640. Biernaskie, J.M.; Perry, J.C.; Grafen, A. A general model of biological signals, from cues to handicaps. *Evol. Lett.* **2018**, *2*, 201–209. [CrossRef] [PubMed]
641. Loui, M.C. A note on the pebble game. *Inf. Process. Lett.* **1980**, *11*, 24–26. [CrossRef]