applied sciences

MDPI

Review

Systematic Literature Review of Challenges in Blockchain Scalability

Dodo Khan [1,*], Low Tang Jung [1,2] and Manzoor Ahmed Hashmani [1,2]

[1] Department of Computer and Information Science, Universiti Teknologi PETRONAS (UTP), Seri Iskandar 32610, Malaysia; lowtanjung@utp.edu.my (L.T.J.); manzoor.hashmani@utp.edu.my (M.A.H.)
[2] High Performance Cloud Computing Center (HPC3), Universiti Teknologi PETRONAS (UTP), Seri Iskandar 32610, Malaysia
* Correspondence: dodo_18001633@utp.edu.my

Abstract: Blockchain technology is fast becoming the most transformative technology of recent times and has created hype and optimism, gaining much attention from the public and private sectors. It has been widely deployed in decentralized crypto currencies such as Bitcoin and Ethereum. Bitcoin is the success story of a public blockchain application that propelled intense research and development into blockchain technology. However, scalability remains a crucial challenge. Both Bitcoin and Ethereum are encountering low-efficiency issues with low throughput, high transaction latency, and huge energy consumption. The scalability issue in public Blockchains is hindering the provision of optimal solutions to businesses and industries. This paper presents a systematic literature review (SLR) on the public blockchain scalability issue and challenges. The scope of this SLR includes an in-depth investigation into the scalability problem of public blockchain, associated fundamental factors, and state-of-art solutions. This project managed to extract 121 primary papers from major scientific databases such as Scopus, IEEE explores, Science Direct, and Web of Science. The synthesis of these 121 articles revealed that scalability in public blockchain is not a singular term. A variety of factors are allied to it, with transaction throughput being the most discussed factor. In addition, other interdependent vita factors include storages, block size, number of nodes, energy consumption, latency, and cost. Generally, each term is somehow directly or indirectly reliant on the consensus model embraced by the blockchain nodes. It is also noticed that the contemporary available consensus models are not efficient in scalability and thus often fail to provide good QoS (throughput and latency) for practical industrial applications. Our findings exemplify that the Internet of Things (IoT) would be the leading application of blockchain in industries such as energy, finance, resource management, healthcare, education, and agriculture. These applications are, however, yet to achieve much-desired outcomes due to scalability issues. Moreover, Onchain and offchain are the two major categories of scalability solutions. Sagwit, block size expansion, sharding, and consensus mechanisms are examples of onchain solutions. Offchain, on the other hand, is a lighting network.

Keywords: blockchain; distributed ledger technology scalability; consensus model; scalability solution; throughput

Citation: Khan, D.; Jung, L.T.; Hashmani, M.A. Systematic Literature Review of Challenges in Blockchain Scalability. *Appl. Sci.* **2021**, *11*, 9372. https://doi.org/10.3390/app11209372

Academic Editor: Gianluca Lax

Received: 10 August 2021
Accepted: 3 October 2021
Published: 9 October 2021

1. Introduction

Many online transactions between individuals or organizations are based on a centralized controlled system (or controlled by a third-party organization). For example, a bank or a credit card vendor is acting as a third-party entity in executing a digital payment or money transfer process between two organizations (or individuals). The third-party vendor takes a fee for every successful transaction. In this centralized mechanism, the third-party controls and manages almost all the information of the stakeholders that are involved in the online transaction. This approach requires the third party to uphold the

transaction's security. In contrast, blockchain is an immutable distributed ledger of cryptographically signed transactions maintained by a peer-to-peer network, where no third party is required to manage the information, and trust is no longer an issue among the network participants.

Blockchain technology is one of the most hyped decentralized innovations, with an enlightening future. Blockchain was introduced by Haber and Stornetta [1] and later gained intense attention because of the Bitcoin principle by Namakoto in 2008 [2]. Bitcoin is highly successful in the cryptocurrency arena. Many similar currencies have were launched following Bitcoin. There were 2017 crypto currencies available on the internet by 2019 [3], with different business models. Besides global crypto currency hype, Bitcoin holds the highest market capitalization up to 53%. Blockchain is serving as the fundamental technology behind Bitcoin. The survey conducted by World Economic Forum [4] showed that blockchain will be soaring to 10% of global GDP by 2027.

It has been two decades since the launch of Bitcoin as the first public blockchain application. Till then, blockchain technology had been restricted to cryptocurrency (Bitcoin and Ethereum) public blockchains settings. It has hardly been accepted in other industries since. Among the many hindrances, scalability is found to be the key hurdle in implementing public blockchains in many real business environments. In general, scalability has not been well-defined in the literature.

Basically, the scalability issue arises with the increasing number of nodes and transactions in blockchain. This issue is indeed present in major public blockchain applications (e.g., Bitcoin and Ethereum) because every node needs to store and execute a computational task to validate every transaction. The public blockchains are therefore always demanding a huge amount of computational power, a high bandwidth internet connection, and massive storage space. Transaction throughput and transaction latency are the two most discussed performance metrics in blockchain, and both have not reached a satisfactory QoS level in many recent popular public blockchain systems. For instance, Bitcoin and Ethereum are able to process 7 [5,6] to 20 [7] transactions-per-second (TPS), but they also face high consensus processing time delays (the average time required to mine a block) at a magnitude of up to 10 min. Besides efficiency, the current size of Bitcoin, Ethereum, and Litecoin are, respectively, 305.23 GB, 667.10 GB, and 28.45 GB [8], causing great demand on storage spaces. The time needed to download the whole blockchain is considerable.

Several studies deliberated the concept of scalability trilemma [5,8]. Initially, it was described by Vitalik Buterin, the co-founder of Ethereum [9] . Vitalik stated that trade-offs are inevitable between three important blockchain properties: decentralization, scalability, and security (see Figure 1). Decentralization is the core and the nature of blockchain. Security is an essential propriety, whereas scalability is the main challenge. In other words, the scalability trilemma states that trade-offs are almost inevitable among these characteristics of blockchain [10,11].

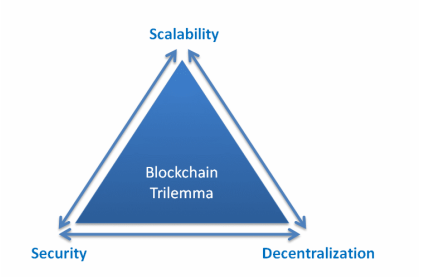

Figure 1. Scalability trilemma.

For example, in Bitcoin, minimizing latency may increase the transaction throughput, but it would make the security vulnerable due to the high chance of the forks forming in public blockchains. It is therefore essential to find a balance between all those three aspects of the blockchain and to consider the requirements of public blockchain applications.

In this article, we performed SLR on the latest research works on the scalability of public blockchains. The SLR started off with a deep investigation into the scalability issue in major public blockchain applications to identify the impacts of the adoption of blockchain technology in areas/fields other than cryptocurrency, after which the potential factors associated with challenges in transaction throughput, energy consumption, number of nodes, latency, storage, etc., were explored and tracked. All the scalability-interdependent elements were systemically scrutinized and linked to the public blockchain consensus mechanism. Many researchers have attempted to address this issue in one of two ways: on-chain or off-chain. Sagwit, block size increases, sharding, and consensus mechanisms are examples of on-chain solutions. Off-chain, on the other hand, is a lighting network. Researchers also studied these examples' impact on blockchain implementations.

The main contribution is two-fold. First, we provide a comprehensive review of public blockchain scalability with a special focus on the critical factors causing the scalability issue, and the related mitigation approaches. Many surveys and reviews have been released on the blockchain scalability challenge in the context of cryptocurrencies, as well as studies that only look at how to address scalability problems with different implementations; however, the problem still exists. Secondly, this SLR is attempting to build a comprehensive knowledge base in the field of public blockchain scalability that could be beneficial to those researchers interested in seeking ways to solve the public blockchain scalability problem in the context of time-critical applications.

This SLR (systematic literature review) consists of nine sections and is structured as follows: Section 1 introduces blockchain technology. Section 2 discusses the key features and the structure of blockchain. Section 3 discusses related work. Section 4 presents the research methodology, the research question, and the data collection procedure. The findings of this SLR are discussed in Section 5. Sections 6–8 exemplify the relevant research on blockchain scalability based on our research questions, and Section 9 concludes this paper.

2. Blockchain Overview

Blockchain technology is considered "revolutionarily" that it is highly likely to disrupt technology ecosystem in offering feasible solutions for securing data due to these strengths: decentralized features, secure data storing capability, lack of trust, data transaction auditability, and transparent data processing. It offers data immutability against different attacks, and provides more advanced data privacy, data security, and data integrity. It is believed that blockchain technology will potentially disrupt every industry that exists and drastically change all aspects of our lives [11–13].

A blockchain is a decentralized shared database maintained by a computer node in a peer-to-peer network. The records in the original bitcoin blockchain include transactions between parties concerned with crypto-currency transfer. Both the parties are assigned a private key and public key as per the public key infrastructure (PKI) [12]. The identity or transaction address of the parties is established by the public key hash value. Transaction parties use their private keys to sign transactions, and other parties can then verify them with the public key of the signator. The transactions are sent to all peer nodes in the network for validation purposes [11,14–16]. Peer nodes agree on the validated transactions by means of a distributed consensus technique and the sequence in which they should occur. The transactions are recorded in a data format called a "block" [12] and are then committed to a shared database to form a linked chain. Each block in the blockchain has a separate timestamp and a cryptographic hash connecting it to the previous block. Blocks

cannot be removed but can be added to a chain [14]. A block of information may be manipulated by peer nodes on the blockchain, and a common database with an ever-growing list of immutable and irreversible records can be created [17].

Distributed consensus mechanism is critical for blockchain since it determines which block can be accepted and inserted into the chain. This is similar to agreeing on distributed power allocation because the node authoring the accepted block can change the state of the database shared by every other peer. To prevent abuse, the power distribution mechanism must be linked to cost and resources. The proof-of-work technique used by the initial Bitcoin blockchain requires nodes to compete by solving a cryptographically complicated puzzle. This puzzle feature ensures three properties: a node must invest a commensurate amount of processing resources to complete it, the next node to successfully solve the puzzle is chosen at random, and a node's claim to having found the puzzle's answer can be easily validated by any other peer nodes. One further concern, however, is the random choice of malicious nodes controlled by an attacker as the official validator, provided they are in line with the same procedure. Once selected, a rogue node might still be able to insert itself into the blockchain blocks of fake transaction data. Thus, after a peer node receives the block proposed by the official validator, there is an implicit consensus follow-up. In that stage, pair nodes can verify the transactions in the new block received and can maintain the previous condition of the blockchain without accepting a new block, if there are any anomalies (e.g., discrepancy of related hash values or missing transaction signing and identity). Otherwise, the node will confirm the new block and accept an updated blockchain if all goes properly. With the amount of acceptance confirmations it receives from several nodes, the probability of a block being rejected decreases exponentially. After a certain number of confirmations, "5–6 in the case of Bitcoin", the block is deemed permanent (occasionally it may take over an hour for this process to be completed). The cost of a blockchain relies on the computer resources needed for the mining process. The miners, who produce new blocks in combination with unrecorded transactions, receive a blockchain of this kind to create new blocks. Mining companies are competing to solve a mathematical riddle for gaining a price, and substantial investment in computer resources is needed for mining in blockchain. The prices of electricity for trading in P2P energy typically fall below the prices of energy purchases from a business of utilities [18].

The blockchain is basically made up of a series of cryptographically linked blocks carrying a list of transactions such as the traditional public ledger [12]. Figure 2 illustrates a simplified example of a blockchain structure. Every block points to a similar related block by a relation that is conceptually the hash value of the previous block called the parent block. The first block in the chain is referred as Genesis block, and it has no prior block [17].

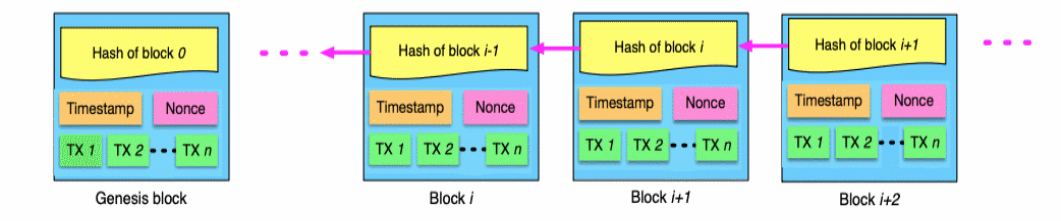

Figure 2. An example of blockchain consisting of a continuous linked block.

A block is fundamentally divided into 2 sections, the block body and the block header. Block header carries these metadata: block version, Prev-hash, timestamp, Merkle tree, bits, and Nonce value, whereas the block body comprises a list of transactions. The quantity of the transactions is entirely dependent on the size of the block.

In general, there are two types of blockchain: the permissioned and the permissionless. The permissionless blockchain is open for anyone to join and perform transactions. It permits all participants to take part in the consensus process in forming the chain. Bitcoin [2] and Ethereum [13] are the classic examples of permissionless blockchain. Permissioned blockchain is a private chain allowing only proprietary users to join and perform transactions. Users may belong to one or more organizations. In case of more than one organization, the chain is referred as consortium-based blockchain. Hyperledger fabric [14] and multichain [15] are examples of private and consortium-based blockchain in which the number of participations is restricted.

2.1. Digital Signature

A digital signature [7] is an asymmetric cryptography deployed in a trustless environment. Every block in the blockchain is assigned a public and private key. The private key is like a password that no one has access to except the owner, and it is needed to sign-in to blockchain to perform the transaction. The public key is visible to every node in the blockchain network, and it is used to access the signed transaction that was broadcasted across the entire network. The digital signature works in two phases for signing into a transaction.

2.2. Consensus Mechanism

The consensus mechanism specifies how to have every node to agree on the verified state of the ledger. It is a process of approving/verifying transactions to avoid the double-spending issue. The consensus mechanism is characterized as either proof-based or voting-based mechanism. Proof-based is mostly utilized in public/permissionless blockchain. Proof-of-work (PoW) protocol is well recognized as the proof-based consensus mechanism. However, it suffers from high energy consumption and required specialized hardware and resources. It consumes more computation energy in verifying blockchain transactions. Proof-of-stake (PoS) is another example of proof-based mechanism. It can process transactions much faster than PoW but is vulnerable to other possible risks such as the Agency issues. Ethereum is known to gradually implement the PoS because of reduced energy consumption and better scalability. The voting-based consensus model is typically used in private Blockchain. PBFT is one good example of voting-based consensus model.

2.3. The Key Characteristics of Blockchain

This section discusses the key characteristics of blockchain on decentralization, persistency, and auditability.

2.3.1. Decentralization

Decentralization: in the traditional centralized system, a trusted authority is required to validate every occurring transaction in the network. However, the decentralized environment does not support any governing authority or single entity to control the whole network. All the nodes in the network collectively manage the network, i.e., decentralized governance. The transaction in blockchain can therefore be accomplished between 2 peers (P2P) without the approval of a central agency.

2.3.2. Persistency

Each transaction occurring in the blockchain network is spread and stored across the network, which can amount to 100 s and 1000 s of nodes. It is therefore not possible to tamper or alter the data in the blockchain [16]. In addition, each block must be validated by every other node in the network and the transaction in those blocks must also be verified. Data tempering is thus impossible.

2.3.3. Auditability

Every confirmed transaction in blockchain is stored on the Block with a timestamp. Consequently, it is extremely convenient for other nodes to verify and track the prior transaction in the distributed network. For example, in Bitcoin, every transaction is connected to prior transaction through a hashed link that proves the auditability of the stored data.

3. Related Work

It is noticed that blockchain technology has somehow been restricted to cryptocurrencies (Bitcoin and Ethereum). It is yet to be widely accepted in other industries. Among the many hindrances, scalability is found to be the key hurdle in implementing public blockchains in many real business environments. In this section, we concisely discuss the importance of scalability in blockchain. Moreover, we also present the related literature on works that have been conducted in the past that focused on scalability in blockchain.

There are claims that blockchain is the technology that will disrupt the technology eco-system. However, it is yet to achieve this outcome due to its scalability issue. Many researchers have attempted to address the scalability issue by proposing different solutions, but the problem persists. Many surveys and reviews have been published on the blockchain scalability challenge and on the evaluation of the proposed solutions with different implementations. Recently, the authors of the survey published in [19] evaluated the blockchain scalability challenges in the healthcare domain and went on to provide potential solutions for those challenges. Similarly, another author in [4] published a survey that broadly classified and compared the blockchain scalability solutions. The review published in [17] sees the author discussing different consensus protocols in blockchain scalability perspective. Other studies related to blockchain scalability can be found in [5–8,20], and perhaps more will come. This paper presents a comprehensive novel study that none of the available surveys and reviews have discussed. This survey evaluates public blockchain scalability with special focus on the critical factors that are causing the scalability problem. This survey also comprehensively evaluates the related blockchain scalability mitigation approaches. We attempt to build a comprehensive knowledge base for public blockchain scalability due to deal with the scarcity of such comprehensive research in public blockchain domain. Table 1 lists some currently available blockchain scalability surveys and reviews.

Table 1. Some recent survey and review articles on blockchain scalability.

Reference	Year	Cite	Title	1st Authors
[21]	2020	24	Scalability challenges in healthcare blockchain system—a systematic review	Ahmad Akmaluddin Mazlan
[5]	2020	107	Solutions to scalability of blockchain: a survey	Qiheng Zhou
[8]	2020	28	Scaling blockchains: a comprehensive survey	Abdelatif Hafid
[22]	2019	63	A Survey on the scalability of blockchain systems	Junfeng Xie
[23]	2016	1559	Where is current research on blockchain technology?—a systematic review.	Jesse Yli-Huumo
[7]	2018	83	Blockchain and scalability	Anamika Chauhan
[8]	2018	105	A survey of scalability solutions on blockchain	Soohyeong Kim
[24]	2018	305	A survey about consensus algorithms used in blockchain	Nguyen, Giang-Truong
[25]	2019	45	Survey: sharding in blockchains	Guangsheng Yu

4. Survey Methodology

This systematic literature review was conducted based on the Preferred Reporting Items for Systematic Review and Meta-Analyses (PRISMA) [26]. The standard guidelines by Kitchenham [27] were applied to align this SLR with the computer science domain. Figure 3 illustrates the complete methodology adopted in this SLR.

This methodology section lays out the methods for this SLR. It includes the formation of research questions, the eligibility criteria for selecting the most relevant articles, the knowledge sources, paper search, study collections, and data extraction. Table 2 illustrates the method designed for this SLR.

Table 2. Method for this SLR based on PRISMA protocol.

Title	Description
Abstract	It provides a concise overview of this paper, which includes the background of the research, the methodology, and the key findings.
Methodology	Research question Selection criteria Information sources Screening process Data extraction process
Introduction	This section presents the existing knowledge base as well as a straightforward problem statement, and the finding of the study.
Result Discussion	This section provides the findings and analyses for the research works
Conclusion	Concludes the outcomes of the entire research and provides some relevant future directions.

This study deeply investigates the public blockchain scalability issue, the factors involved with it, and the available solutions. A knowledge base is eventually created based on the issues identified in the investigation. The following research questions are entirely focused on the scalability of public blockchains scope and are designed through a methodical discussion among the members in this research team.

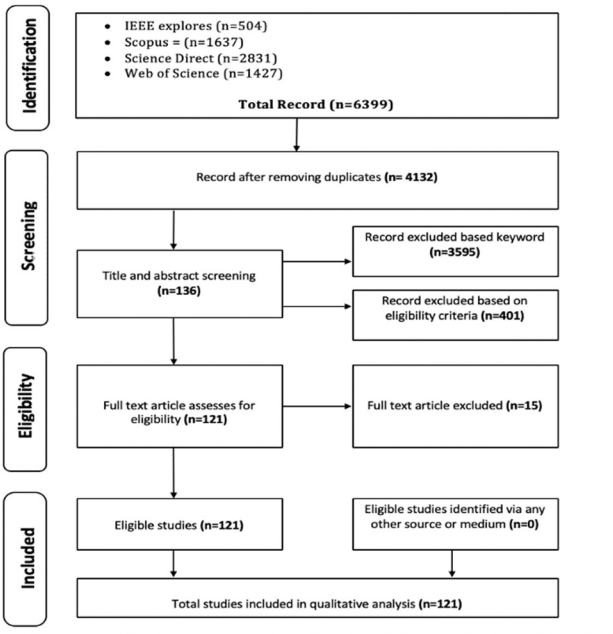

Figure 3. Paper search and selection process.

4.1. Research Questions

- RQ1: How can the scalability issue impact blockchain implementation?

The motive of this study is to investigate and deeply review the public blockchain scalability issue. RQ1 is therefore aimed to review all relevant papers/information from the academic research works that are directly correlated to scalability issue to understand its vital impact on public blockchain implementation.

- RQ2: What vital root factors are causing scalability issue in blockchain?

This question is correlated to the probable reasons and their connections, which are creating hindrances in leveraging blockchain technology for large-scale implementation. RQ2 is dependent on RQ1 because it shall lead to the creation of knowledge based on public blockchain scalability issues and pairing to the intended research directions.

- RQ3: How researchers address the scalability issues in blockchain?

This question seeks to understand the state-of-art solutions pertaining to public blockchain scalability issues. RQ3 seeks to uncover how other researchers have addressed scalability in public blockchains. This SLR is looking at studies that have proposed specific solutions that were either implemented, simulated, or formally proven instead of mere idea/vision presented in published papers.

4.2. Inclusion and Exclusion Criteria

The inclusion and exclusion criteria in this SLR are structured to solely accept the documents or articles that directly dealt with the scalability of public blockchains as a problem. The main scope is the factors that are becoming a hindrance to implement blockchain on a large scale. In addition, this SLR is also targeting articles that attempt to solve the scalability issue. The solution should have been implemented or simulated and is feasible instead of just highlighting the trend or idea without considering the feasible implementation of the solution. Five key eligibility criteria are designed for this SLR. The criteria are shown in Table 3.

Table 3. Inclusion and exclusion criteria for this SLR.

Criteria	Quantity
1	The study must be original research work instead of a review or a survey paper.
2	The papers focusing on the blockchain scalability issue (directly or indirectly) and highlighting the relevant reasons/factors.
3	Papers proposing a feasible solution aiming to solve the blockchain scalability (method, technique, model, and framework).
4	The proposed solutions have been evaluated (implemented, simulated, and formal proof).
5	The papers are published in peer-reviewed journals/conference journals.
6	The papers should only be in English language.

4.3. Information and Data Sources

The relevant information and data sources were determined after exhaustive deliberations between research team members based on the literature reviewed. As mentioned, this study focuses on the fundamental issue of scalability in public blockchains; as such, we converged on computer science literature in academic journals and conference proceedings for a quality SLR research. The data sources searched include both significant and focused computer sciences and multidisciplinary databases. Articles were obtained from the following sources. These sources have maximum coverage of quality articles in our domain, such as ISI- and Scopus-indexed articles [16,27].

- Scopus;
- IEEE explore;

- Science Direct;
- Web of Science.

4.4. Search Process

As per the PRISMA activity guidelines [26], predefined search protocols are essential to avoid any bias during the article search. As such, our search protocols were designed to undertake the specific literature search from the above-mentioned publication portals via their internal search engines.

The keywords used in our search strings were identified after several exhaustive test searches, and viable keywords were tested exhaustively. Initially, keywords such as "Blockchain" and "scalability" were applied to different databases. Unfortunately, it revealed that these keywords are rather too limited in scope. Eventually, different combinations of keywords were manipulated in the search strings to discover papers containing explicit technical synonym of "Blockchain" and "scalability". This approach was adopted to conduct the search for articles between years 2010 and 2019. That is, all relevant articles published during these years are included in this SLR.

It was observed that in using the "scalability process" search string, such search string did not return a uniform hit on every database. By searching in IEEE Explore by using "Blockchain" and its relevant technical synonyms such as "Bitcoin" and "cryptocurrency", it turned out that the search yielded papers well matched to the search requirements. However, in other databases, these keywords returned a huge number of irrelevant papers mostly related to the economy and/or cryptocurrency domains. Hence, different search strings must be designed for different databases. The complete search strings for this SLR are listed in the Appendix A.

4.5. Screening Process

To ensure the relevancy of every searched article to the research questions, incremental approach has been used. Therefore, our first step is to screen the downloaded papers to remove duplicated articles obtained from the different data sources. Then, the title of every paper was carefully filtered to eliminate irrelevant papers, i.e., those with no relevancy to the research questions. For example, the search string returned articles related to blockchain but not discussing the scalability issue; the scope is thus out of this SLR. However, occasionally it could be rather hard to decide on the relevancy by just reading the title of the paper. This demanded a more careful reading of the abstract of every paper to decide the eventual acceptance of the paper. As a matter of fact, our predefined inclusion and exclusion criteria were vital to screen each article for its relevancy to the RQs.

4.6. Data Extraction

A Microsoft excel form was designed for executing the data extraction process based on the PRISMA activity guidelines. This was to extract the required information from the papers with respect to the research questions. The form had three main parts, namely, the characteristic/demographics of the selected papers, the technical aspect of blockchain (including its scalability) issue, and the quality assessment of the selected papers. Data were extracted from all the papers that passed through the quality assessment. The objective was to record accurately only the needed information from the papers. The quality assessment was conducted based on the standard PRISMA guidelines. Demographics of the papers included the title of the article, author(s) of the paper, country of the author, publication type/place, and publication year. The technical aspects of blockchain included the information about blockchain and its scalability issue, blockchain type, performance efficiency, application areas, and factors involved in scalability (throughput, latency, storage, and bandwidth power efficiency).

It should be highlighted here that the validity of the form is mandatory to ensure authenticity of the data gathered. The form was therefore rigorously tested on 25 randomly selected papers and was revised iteratively per each validating process.

5. Discussion on Consolidated Paper

This section discusses the analysis of the 121 selected papers published between 2011 and 2019. It provides insight into the research trend in the last decade on scalability issue and the available solutions for public blockchains. The discussion focuses on the following:

1. The distribution of blockchain based publications concerning scalability issue over time.
2. The distribution of types of blockchain publication.
3. The distribution of countries of publication.
4. The distribution of application areas of blockchain.

To appropriately answer the research questions, the data collected during the data extraction process were properly compiled, and the demographic data were analyzed for the mentioned years of publications.

Figure 4 illustrates the year-wise analysis of the selected papers. The increasing interest of academic research on public blockchain scalability is observed in a rising number of publications over the years. It is noted that majority of the academic research on public blockchains concerning scalability were in 2018–2019.

There was not much blockchain research until 2015, probably because time was required for blockchain to gain momentum after the launching of bitcoin in 2008. The research on blockchain scalability started to emerge in 2016, specially in public blockchains.

The research in scalability emerged in 2016, when there were 10 published articles; by 2019 there were over 60, a factor of 6× in 3 years. Over these years, blockchain began to disrupt more and more applications on a larger scale. It is therefore logical that the research community should start addressing the burning scalability issue in public blockchains.

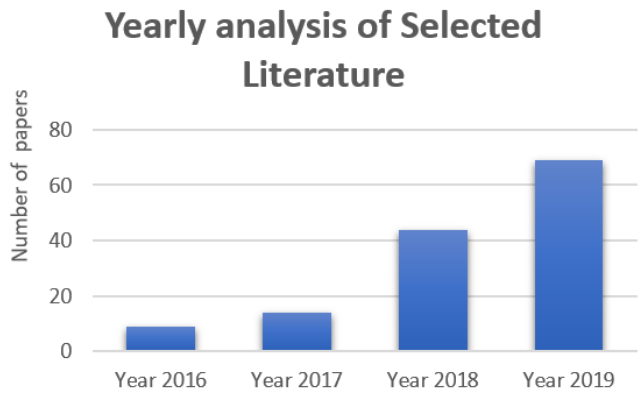

Figure 4. Figure illustrates the year wise distribution of published paper in the blockchain domain.

Figure 5 displays the details on the types of publications for the selected articles in this SLR. The following are the types of publications included (and identified) in this study.

- Journals;
- Conference proceedings;
- Book chapters;
- Workshops;
- Symposiums.

The findings revealed that most of the publications concerning public blockchain scalability were published in conferences and journals, i.e., 54 papers out of the 121 articles were published in conference proceedings, followed by 33 in journal publications. The remaining articles were in book chapters (20), symposium (8), and workshops (6).

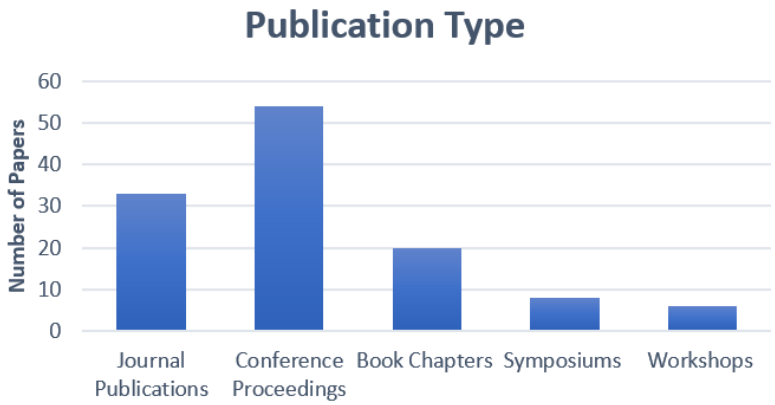

Figure 5. Figure illustrates the analysis of selected paper types in the blockchain domain.

Figure 6 shows the statistics about the geographical distribution of the selected papers. It is noticed that China leads with 24 articles, followed by the USA with 13 papers (published in academia or industries). Moreover, India is the 4th leading country with eight papers, and closely followed by UK, Switzerland, and Australia with eight, seven, and seven papers, respectively. Only seven countries have over five publications. The rest are below five. This analysis reflects the interest of the research community on blockchain scalability around the world.

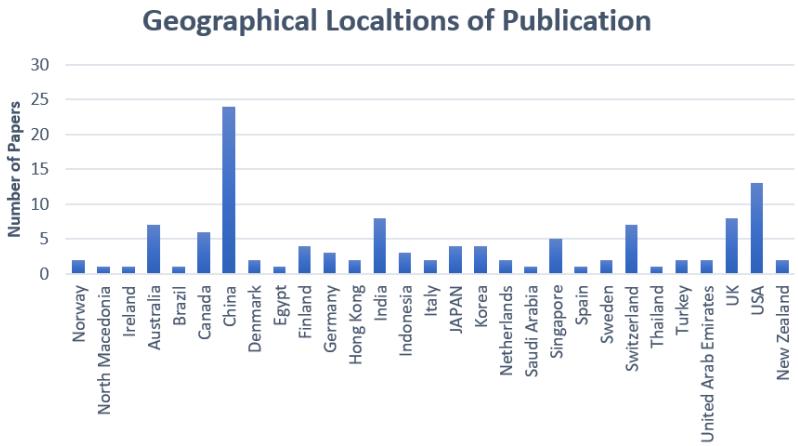

Figure 6. Figure illustrate the analysis of geographic distribution of selected paper in the blockchain domain.

6. RQ1: How Scalability Issue Can Impact Blockchain Implementation?

Blockchain was made famous by Bitcoin in 2008 [2], and since then it has already advanced into several industries. There are claims that blockchain is the technology that will disrupt the technology eco-system. However, it is yet to witness much growth and disruption apart from cryptocurrency. Figure 7 is about public blockchain applications except cryptocurrency. From our SLR, cryptocurrency (Bitcoin and Ethereum) is noted as the state-of-the-art application of public blockchains. Next to cryptocurrency, IoT is the most discussed blockchain-related application, with 17 publications. Our findings also revealed that although blockchain is very applicable to IoT applications, it is yet to achieve the preferred outcomes due to scalability issues. Blockchain appeared to be influencing

and disrupting many other industries such as finance, resource management, healthcare, education, and agriculture [17].

Every selected paper discusses and states that scalability is a critical issue in public blockchains. These papers manifested the fact that blockchain is yet to be able to "scale-up" at par to the centralized infrastructure, be it in cryptocurrency or some other applications. Scalability in public blockchains is recognized as the vital issue that is affecting the performance and efficiency in the blockchain associated applications.

The following section discusses the scalability issue based on the consolidated data from the articles reviewed. This is to justify the impact of scalability in the top three public blockchain-associated applications, namely, Bitcoin, Ethereum, and IoT.

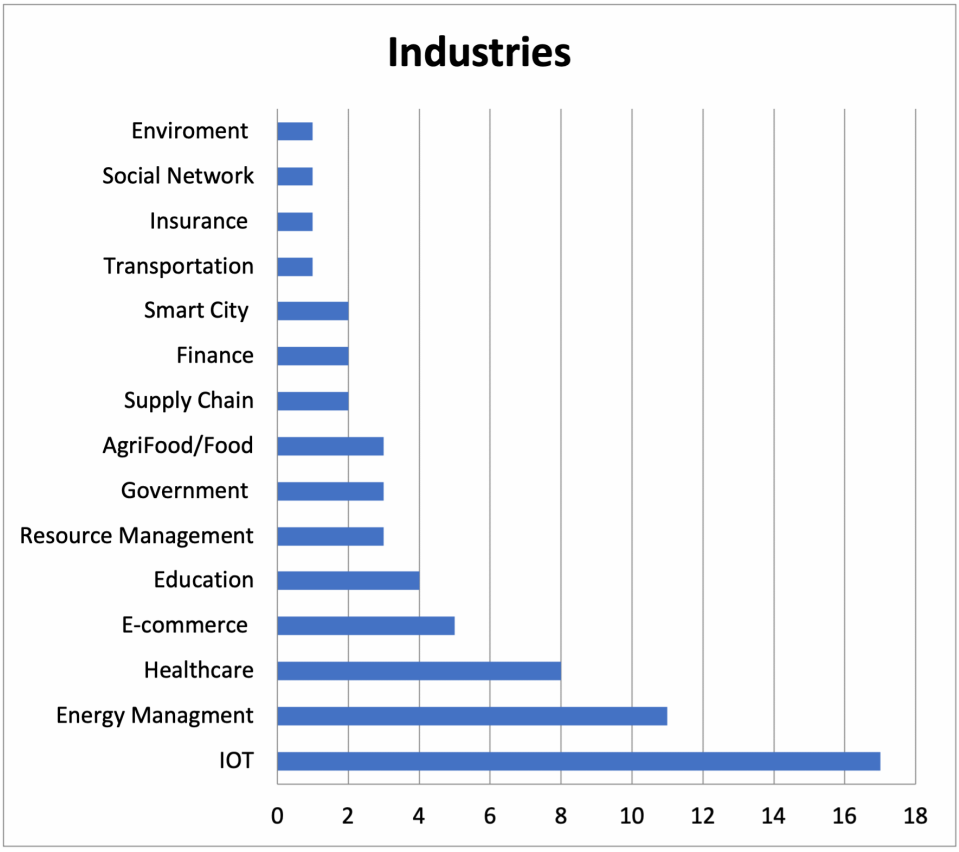

Figure 7. Blockchain application domain per selected papers.

Scalability Issue in Major Public Blockchains Application (Bitcoin and Ethereum)

The high acceptance of cryptocurrency is escalating the burning scalability issue in public blockchains [6,7,28]. The number of transactions with Bitcoin and Ethereum is increasing every day [5,7]. More 13,000 transactions take place with Bitcoin everyday [7]. This high number of transactions is making Bitcoin transactions bulky. One of the processes in public blockchains is to verify the source of the transaction, and every node needs to store and validate every transaction. It is therefore a challenge to the miners to verify every transaction in Bitcoin as it scales up in volume. This is happening because of the inefficient proof-of-work (PoW) [29] consensus mechanism deployed in the Bitcoin in verifying and validating every single transaction. PoW is unfortunately the most frequently used consensus protocol [17]. It is worth to notice that the total number of transactions in Ethereum has continuously grown over the years [7]; many thousands of transactions have occurred every day in recent years. In Ethereum, the limited block size cannot accommodate all the transactions submitted by the miners. It is therefore challenging for the miners to verify every transaction. The consequence is that the miners tend to select transactions with more rewards for the sake of securing more rewards. The transactions with

fewer rewards are left in the queue, leading to longer transaction latency [30]. It is estimated that more than 10 k transactions are waiting to be verified.

The highest transaction throughput in Bitcoin is capped at 7 TPS (Transaction-per-second). In contrast to the VISA counterpart, 400 TPS is the norm [5,6,29–31] The block interval latency (in public blockchains) is in a magnitude of up to 10 min [32]for a transaction to be verified. Ethereum was to be theoretically verified at the rate of 1k TPS, but due to certain limitations in its structure, is more likely to be verified at 20 TPS. This is far less than other electronic payment methods such as PayPal—at 193 TPS. Besides the inefficiency in the transaction verification process, another crucial factor of importance is storage, which needs to be seriously considered [5]. As transactions grows, the required storage capacity for blocks needs to scale up at tandem. It is reported that currently, Bitcoin storage is more than 305.23 GB [8], Ethereum is at 667.110 GB [8], and LiteCoin at 28.45 GB. It should be mentioned here that energy consumption is also a crucial issue in public blockchain implementation. When comparing the consumption of electricity by Bitcoin with other cryptocurrencies, Bitcoin was in the 49th position [5]. It is interesting to note that actual consumption of electricity by Bitcoin is less than the predicted scale, which may suggest that the Bitcoin could not scale well per expectations and predictions.

The combination of all the limitations mentioned above is apparently degrading the performance of public blockchain decentralized applications. The low throughput, high latency, high storage, and high energy consumption cannot satisfy the large-scale implementation of blockchain in time-mission-critical or real-time applications.

The Internet of Things (IoT) is a technology that is growing aggressively, and it is embracing blockchain as an integral component in IoT security applications. IoT was tagged as "The Global Infrastructure of the Information Society" by ITU in 2015 [14]. Besides the many benefits, IoT has some limitations. Public blockchains have been technically considered to address those issues by decentralizing computation powers, processing, and storage. Unfortunately, public blockchain is still suffering from scalability matters in IoT applications [33,34]. Principally, public blockchain technology is not suitable for lightweight IoT devices. In blockchain, a node is supposed to verify every transaction and perform search in every block, likely an extremely heavy load for lightweight IoT devices. As discussed earlier, public blockchains require massive resources to support their operations and are highly constrained by consensus delay, making it almost impossible to deploy them in small/low spec IoT devices. It would not be possible for IoT devices to verify a transaction without a massive amount of historical data. IoT therefore needs to either carry high storage by itself or rely on a centralized server. While considering the large-scale storage requirement in public blockchains, it is worth to also examine the financial aspects. For example, in Ethereum, it costs 2 × 105 US Dollars per gigabyte of data storage, making it probably highly expensive to implement IoT networks with blockchain [35].

The storage requirement for the IoT network is very much dependent on the types of application. As such, the overall data storage size could be destructive in IoT-enabled blockchain since each block would be replicated n times in the n-node public blockchain networks. For example, in smart city application, vehicular traces of 700 cars for 24 h demand a storage capacity of close to 4.03 GB, which is about 0.24 MB per hour per car [36].

In public blockchains, high latency can be due to transaction confirmation. This behavior may cause inconsistency in a decentralized environment. The usual tolerated latency in blockchain is not suitable in many IoT applications. For example, in Bitcoin, the confirmation time is 10 min, which can be an extremely long delay for sensitive IoT applications such as vehicular networks. In the light of all these limitations, it is obvious that scalability issue is persisting and degrading the performance of IoTs enabled with blockchain.

7. RQ2: What Vital Root Factors Are Causing Scalability Issue in Blockchain?

With the increasing popularity of Blockchain technology and its permissionless application such as cryptocurrency-based applications, scalability issue has become a primary focus in the blockchain research community. Many researchers are attempting to analyze in details on this issue [5,37]. From our SLR, there seems to be no rule-of-thumb or state-of-the-art research with good matrices to address scalability issue in public blockchains. This section intends to discuss factors causing scalability in more detail.

Figure 8 illustrates the factors causing scalability issue in public blockchains. Among these factors, transaction throughput has received the most attention. Out of the 121 selected papers, 39 papers discussed transaction throughput as main factor/concern for low scalability in public blockchains. Twenty papers highlighted the consensus mechanism as the second most discussed factor concerning public blockchain scalability. Consensus mechanism is somewhat related to throughput. There are nine papers talked about the computational power involving scalability in public blockchains. Latency and storage are discussed in six papers. The remaining factors such as block size, cost issue, number of nodes, network load, and overall performance are discussed in 1–3 articles, respectively. There are 23 papers clearly stating scalability as an issue, but reasons causing scalability are somewhat unclear. The Table 4 shows the factors related to scalability issues, along with the relevant reference.

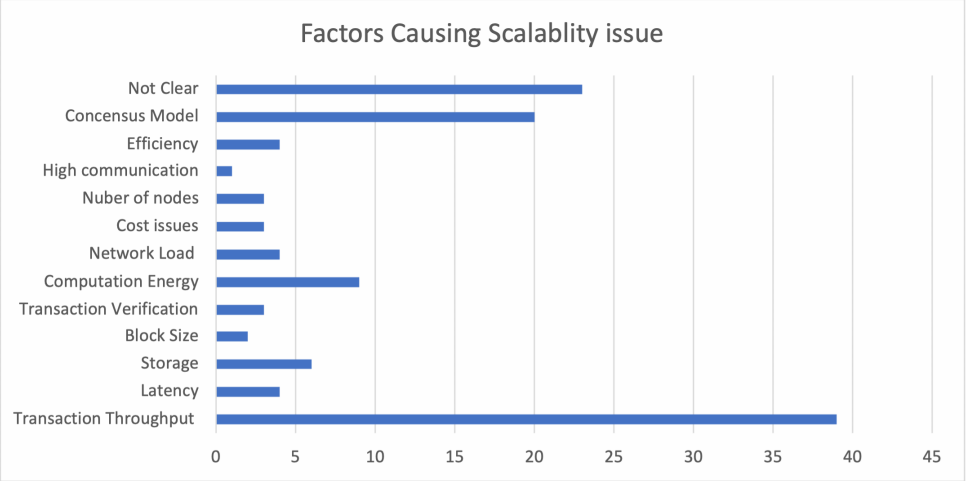

Figure 8. Identified factors causing scalability issue in public blockchains.

Table 4. Factors related to blockchain scalability.

No.	Factor	Description	Ref. Source
1	Transaction Throughput	This implies the total number of transactions that the protocol may handle in one second.	[7,14,36,38–73]
2	Latency	This applies to the time it takes for a transaction to be initiated to achieve a consensus on it. It is also regarded as a finality.	[33,59,69,74,75]
3	Storage	It refers to the total space/capacity a blockchain network can consume.	[36,71,76–81]
4	Block Size	This is total storage capacity of a block to be utilized by the transactions. The network will reject the block if it exceeds the storage capacity.	[77,82]
5	Computation energy	This indicates if the algorithm (or the utilizing system) consumes a significant amount of energy for block mining.	[42,79,83–90]
6	Network load	This implies the number of transactions being carried by the network.	[91–94]

7	Cost issue	This implies the total cost associated with verifying a transaction in blockchain.	[13,50,55,64]
8	Number of nodes	This refers to the total number of nodes available in the blockchain network.	[95–97]
9	Consensus model	Consensus mechanism represents the process of approving/verifying blockchain transactions.	[6,45,47,49,54,56,57, 59,60,63,71,73,83,84, 90,98–116]

It should be mentioned here that public blockchain scalability is not a singular term. It is a combination of various parameters, and these parameters are interdependent. In many papers, every parameter is discussed somehow directly or indirectly to the consensus model deployed. For example, transaction throughput, latency, and computational energy are dependent on the efficiency/performance of the consensus model. Block size and storage are also interdependent. Block size can affect transaction throughput and latency, which in turn can be indirectly linked to consensus model. A larger block can store more transactions, thus directly raising the throughput, but it also causes an increase in block propagation time. In Bitcoin, the block interval is about 10 min with a block size of around 1 MB, to illustrate the limits on the number of transactions that can be stored in each block.

The consensus mechanism is a process in which the nodes in the public blockchains network agree with each other about the ledger that they hold. The consensus protocol is thus the most fundamental and indispensable component in Blockchain. It provides the essential process flow for the nodes to verify and validate every single transaction and hence to append a new block to a blockchain. It follows that a high network bandwidth would be consumed when the whole network updates its chain. For example, Bitcoin uses PoW as its core consensus model, and for the mining process, it requires specialized hardware with stable internet connection. Collectively, this is resource-hungry. It may have a high processing time, resulting in thousands of transactions (per second) waiting in the queue to be verified. This constitutes a pressing latency factor in the public blockchain. Consensus mechanism is considered a crucial challenge in public blockchain applications. It is known to cause bottleneck and restrict transaction throughput [116] in the permissionless blockchain (Bitcoin and Ethereum) [29].

7.1. Latency

Latency in blockchain is referring to the processing time for a transaction measured starting from getting an input till the transaction is completed at the output [24]. In permissionless blockchain, thousands of nodes need consensus to verify and process a transaction. Transactions are buffered in a queue waiting to be verified, thus logically causing increased latency. In public blockchains, every node verifies and stores every single transaction for upholding data integrity and data security but unfortunately compromises the latency [35,117] . High latency in blockchain, however, may be used to ensure consistency in the decentralized public blockchain networks.

7.2. Number of Nodes

Entities connected to blockchain network are considered as nodes. The inter-nodes latency increases when many nodes get connected to the network [19]. The number of transactions increases with the increasing number of nodes, and so, more transactions are getting involved in the consensus process. This is bound to affect the transaction throughput and latency. Additionally, the growing number of nodes leads to increasing computational energy [21]. Nodes in public blockchains care split into two categories: partial node (lightweight nodes) and full nodes. The processing of partial nodes is completely dependent on the full nodes. Although the partial nodes are not needed to store a whole blockchain, the processing workload on public blockchains grows as number of nodes increases. This is of certain to affect the throughput. The involvement with many participants may lead to performance degradation because of the higher number of nodes on

every stage of transaction. The threshold on the number of nodes (participants) may also be a crucial issue.

7.3. Block Size

Typically, the size of one block is around 1 MB in Bitcoin [5,118]. This is considered very small and limits the number of transactions that can be stored. It is apparent that large block size is able to accumulate more transactions and directly increase the throughput and lower the latency [5], but the larger block would prompt an increase in block propagation time because heavier block needs more time to be transmitted over the network. In addition, handling more transactions in one block would demand more computational resources [118].

7.4. Computational Cost/Energy

This implies the total cost associated in verifying a transaction [119]. It includes the required amount of bandwidth in block propagation and, most importantly, the mining process. The mining process is associated with the consensus mechanism in the permissionless blockchain. Bitcoin uses PoW consensus mechanism that the mining process requires specialized hardware to mine a block. The special high-end hardware consumes more energy, and as a whole this higher energy consumption means more computation cost [117] , which in return may impinge on the implementation scale of a public blockchain.

7.5. Transaction Cost

Transaction fee plays a vital role in public blockchains, i.e., Bitcoin. Miner tends to make selection of the transactions to be verified based on the fee associated with it. This directly affects the confirmation time of a transaction, thus influencing the throughput and latency. The transaction with a small fee may suffer massive confirmation delays, and this logically happens because the consensus mechanism promises to reward miners based on the associated fee in a transaction.

7.6. Storage

Public blockchain storage is another essential factor to be seriously considered in the context of scalability. Public blockchain storage requirement grows in tandem with the increasing number of nodes and transactions [5]. As such, full nodes that store complete block data demand high storage capacity. Moreover, high storage requirements can be relieved by increasing partial nodes in public blockchains [35]. Although partial nodes do not store the whole blockchain, they may considerably increase the workload. Throughput would therefore be affected, and addressing high storage requirements is non-trivial.

8. RQ3: How Researchers Address the Scalability Issue in Blockchain?

Some significant solutions to public blockchains scalability are discussed in this section based on the literature reviewed. Scalability challenges are also mentioned in this discussion. At macro level, researchers have attempted to address this issue in two ways: on-chain or off-chain. On-chain solutions tend to address scalability issues by working on elements within the blockchain, whereas off-chain prefers to process transactions outside of the chain. Along with these classifications, there are several application-based solutions designed to achieve the required scalability. For example, DAG [120] and NormaChain [86] for IoT, BlockTrail [40] for auditing, e-commerce EBCM [86,109] and supply chain [55].

8.1. On-Chain Solution

On-chain solutions tend to address scalability issues by working on elements within the blockchain. This section will discuss on-chain approaches to address the scalability issue of blockchain.

8.1.1. Block-Data-Related Approaches

1. Block size increase

The big block size is typical of on-chain solutions. In this approach, the public blockchain scalability issue has some significant linkages to the block size [119]. Obviously, the big block can accommodate more transactions, which would undoubtedly improve the overall throughput. Bitcoin unlimited [8] is an example of a big block. This method increases transmission limit and decreases cost related to transmission as compared to the conventional method. However, it downgrades block prorogation efficiency (in time) and may increase the blockchain forking chances, leading to the probability of orphan block to incur higher maintenance cost. The full node would be more expensive to operate through this approach. Miners prefer this approach because the increased block size can accommodate more transactions in one block, and they incur a larger transaction fee when mining that block.

8.1.2. Segwit

In Segwit method [121], the block size is kept constant while adding more transactions to the block. This approach aims to extract the signature data from the transaction and store it outside the base transaction block to effectively allow more spaces for new transactions. In this approach, the validating part is kept separated from actual data of the transaction. As the digital signature contributes almost 70% to the transaction, the signature must be stored in the data structure called the witness and is isolated from the transaction to resolve the malleability of the transaction [8]. In addition, Segwit has launched a new transaction size unit. A single transaction is divided into two sections. Non-witness (it should be stored in the block as usual) and witness data (it will transfer to extended block). Moreover, non-witness data bytes are counted as 4 WU each, whereas the witness data byte is counted as 1 WU each. The highest storage space for a block is 4 WU, which is equivalent to the old maximum block size of 1 MB, if no node uses Segwit.

8.1.3. Sharding

Sharding was traditionally proposed in the field of database for storage optimization in commercial databases. It was later adopted in public blockchains to address the scalability issue. It is considered to be one of the effective methods. In the sharding technique, the nodes are broken into several chunks called shards [122] . Each shard possesses a small part of nodes. Every shard is responsible for processing small portions of a transaction. Therefore, the transaction is processed in parallel. The parallel processing of the transaction improves the authentication mechanism that ultimately maximizes the throughput of the entire blockchain network. The Byzantine consensus algorithm is used in between the nodes within shards to agree on the state of the transaction [25]. There is an immense need for the inter-shard communication protocol for cross-shard transaction. The total computation energy increases with the increasing number of shards. In this technique, every shard process transaction with the same throughput, and by increasing the number of shards, results in a linear increase in throughput. Elastico [123] and OmniLedger [124] implemented the sharding technique to increase the throughput. The only difference between them is that Elastico is unable to process inter-shared transactions while OmniLedger processes them atomically using an atomic Commit Protocol. Another approach utilizing sharding is the rapid chain [79].

Sharding technique is the only viable solution if transaction stays in the same shard, which is considered to be the most significant limitation. As a matter of fact, inter-shard

transaction cannot be automatically executed by Elastico. OmniLedger supports inter-shard transactions but high shard size is hard to select. However, large shards are not scalable because whole network executes the Byzantine consensus, and small shards are not scalable because they would result in a huge number of shards. Furthermore, small shards are more vulnerable to security risk. Each shard is fault-tolerant, up to, at the most, a third of the shard's size. Moreover, the shard size would decrease if the number of malicious nodes remained constant, making the shard highly likely to fail.

8.1.4. Consensus-Protocol-Related Approaches

In this section, some major consensus techniques are discussed. These techniques have been implemented and applied in different applications for the sake of improving scalability in public blockchains. Based on this SLR findings, the consensus protocol is found to be the second-most-discussed factor. The inefficiency in the consensus protocol is the main cause of scalability issue in public blockchains. The research community has therefore tried to address the scalability issue with different innovative consensus approaches.

1. Proof of work

In 2008, Satoshi Nakamoto (an individual or a group) proposed the initial idea of Proof-of-Work (PoW) model with Bitcoin [2]. Since then, it has been widely used in public blockchains, especially in cryptocurrencies like the Bitcoin. In this model, the miners (nodes) on every transaction compete to solve an intensive mathematical puzzle (hashing), to win a chance to add the next Block to the chain and to earn a reward in the form of Bitcoin for their energy consumed and work done in the mining process [24,125]. For getting a chance to append a new Block, every miner (node) must justify that it has accomplished sufficient work done. Therefore, it is referred to as proof-of-work consensus protocol. It is important to mention here that the Bitcoin dynamically controls the difficulty level of the cryptographic puzzle [126] .

2. Proof of stake

Proof-of-stake (PoS) [127] consensus model is considered an energy-efficient version of PoW because, comparatively, it saves more energy than PoW. In this model, miners (nodes) are supposed to affirm the ownership on the currency they have. Therefore, the miner (node) possessing the highest number of currencies would be given a chance for adding next block to the chains. It is believed that the miners (nodes) possessing more currency would not attack the blockchain network or it would be less likely they would attack. Furthermore, the node associated with higher monetary reward will dominantly control the network [125] because it will always secure chance to publish the block. This is not fair to newer nodes with less currency. There are various PoS variants available with the deployment of the appropriate stake size for selecting a node to append the next block in public blockchains, e.g., peercoin and Blackcoin.

3. Delegated Proof-of-Stake consensus

The Delegated PoS (DPoS) [18] is considered a variant of the proof-of-stake. It does not constitute a significant improvement, but the discrepancy between the proof-of-stake (PoS) and the DPoS is mainly based on direct democracy, while the other is based on a democratic representative [107]. In DPoS model, the miners (nodes) are given the right to find their representative, which is called delegate. The delegate is required to perform three tasks, including creating, validating, and verifying the block. The process of validating would be much faster if a limited miner (nodes) performed the validation process instead of the whole network. Therefore, it would directly affect the transaction throughput. Furthermore, the delegates are accountable for controlling and managing the block size. The dishonest delegate should not be a concern because every node has the right to vote for delegate of their choice. Bitshares is an example of DPoS implementation.

4. Practical byzantine fault tolerance

PBFT consensus protocol is typically used to accept Byzantine faults [18] and is often used by permissioned blockchain, i.e., Hyperledger, because it is able handle up to 1/3 malicious byzantine replica. This model works in rounds process. There are predefined steps to follow in every round in selecting a primary node. The processing of PBFT consensus protocol is divided into three stages: pre-prepared, prepared, and commit. The node should get the majority of 2/3 votes from all the nodes to change the state of the Blockchain. This will confirm that majority of the nodes are identifiable and known to every node. Some practical variants of PBFT have been proposed, such as the Steller consensus model [34]. There is not much difference between PBFT and Steller. In PBFT, every node requires one to inquire about other nodes, whereas in Stellar Consensus Model other nodes can choose which set of participants to rely on.

5. Proof of authority/proof of identity consensus model

Proof of identity/proof of authority consensus model [8] rely on the complete publishing nodes. This protocol only involves nodes whose identity is linked to real-life information. In the PoA/PoID model, nodes need to reveal their real-life identities to gain a chance to publish a new Block. The defined identity should be identifiable and confirmable in the blockchain network. Furthermore, the nodes are required to put their real-life identity at stake along with their reputation to earn the chance to become a publishing node. However, the reputation of these nodes is a concern based on their actions and activities performed in the network, which means any malicious activity in the publishing can ruin their reputation in the public blockchain networks. However, their reputation would improve if the node performed in the way that other nodes agreed on. There is much less of a chance for a node with a poor reputation to become a publishing node. It is therefore essential for publishing to retain high status. It is not preferred to implement this model in permissionless blockchain because it requires trust between nodes.

6. Proof of elapsed time

The PoET consensus protocol randomly chooses the leader by running an election protocol [18]. It was often named as chance-based SGX-based election model. In this model, the leader is chosen to be responsible for adding the next block to the blockchain. In the processing of random leader votes, this model would concern thousands of entrusted nodes and free participation. Therefore, for experiencing the efficiency of this model, it is essential that the election of leader should be distributed between the most available nodes, while the remaining nodes would be kept responsible for ensuring transparency in the selection process and confirm that there is no manipulation in the whole leader selection process. The need for a transparent mechanism in the selection of the leader could be fulfilled by the trustworthy execution environment (TEE), in which security would remain constant during the process. Intel SGX and TEE are supposed to execute the validation and mining process. Every miner needs permission to execute the code within the TEE for waiting time, and miner with the shortest wait-time becomes leader node. Any internal and external tampering could be avoided by the TEE function. This model requires special equipment or hardware, which is considered a drawback.

7. Bitcoin-NG

Bitcoin-NG [128] is new generation consensus model derived from PoW Consensus model [2]. It splits time into different epochs, and a leader is responsible for transaction sterilization in each epoch. This model introduces two new types of Block: the critical block and the microblock. The critical block does not carry transaction data, and it is generated by the miner (nodes) via PoW model and is only used for the leader selection. In contrast, the leader is responsible for creating a microblock containing transaction data. The transaction can therefore be processed continuously unless the next leader ensures to decrease transaction confirmation time which improved the throughput.

8. Proof of reputation consensus mechanism

In PoR [56] protocol, a node's reputation is made on the basis of its assets, transactional activities, and participation in the consensus process. A leader who possesses the best reputation will be able to generate a new Block. Voting process will be initiated for new block validation. There is another scalable protocol on the similar idea of reputation, known as delegated proof of reputation [99]. The protocol's novelty is that it replaces coin staking with a reputation-based method.

8.2. Off-Chain Solutions

The off-chain blockchain scalability solution is designed to increase the transaction throughput by executing the transaction outside of the main blockchain.

Lightening Network

In the lightening network, it is possible that in the Bitcoin network two nodes would be able to create an off-chain trading channel, where those two nodes would be able to process the transaction with low latency [129]. There are three main phases in the lightening network, namely, establishing, trading, and closing the channel. Firstly, it is extremely important to open the payment channel with the nodes sharing the payment channel. After the opening of the channel, some coins need to be placed on the multi-signature address for sharing with other nodes. In this way, nodes are prevented from scamming with the coins arbitrarily. Opening the channel would be accomplished by an on-chain exchange, which would charge a transaction fee to the main chain. Now, once the channel is opened, the transaction will be an off-chain transaction. So, those transactions are not supposed to be stored on the main chain, and it may charge 0 waiting time and transactional fee. The channel would be closed after the process of payment was completed. The final stage would be to notify all nodes and append this new block to the main chain, which would appear on the on-chain. So, in this way, the multiple transactions could take place off the chain and the complete process would create two transaction records on the main chain [8].

Let us suppose A and B are maintaining a channel and B and C are also maintaining a channel each. This enables A and C to contact each other, which increases the throughput. This technique can reduce transaction costs, wait/standby time, and reduce the load on the main chain. However, as fee for transaction is decreasing or has disappeared, there would be no or less benefit for miners, so their ecosystem may change. Raiden network is another example that has been implemented in Ethereum. It is known as Ethereum version of Lightening Network [18]]. It follows the same process and protocol for operation as Lightening network except for the transaction details. Its state channels transfer smart contract details as well.

8.3. Other Potential Attempts to Address the Blockchain Scalability Issue

Some other potential attempts to address blockchain scalability are briefly presented here:

TrustChain [111] is designed for permissionless/public blockchains and the data structure is entirely tamper-proof and used by agents to store their transactional record. It enables the design of a separate immutable chain of temporally organized interactions with other agents. It is inherently in parallel that every agent creates its own genesis block. Concept Superlight [76] is mainly used in public blockchains and seeks to address the problem of scalability. It is not mandatory for all nodes to store the whole blockchain locally for verification of each transaction. So, the nodes in this framework may validate the transaction using their header. Block Summarization [78] decreases the additional storage for transferable transactions. This approach allows resource-constrained lightweight nodes to store blockchain shaped in such a way that transactions can be independently verified to eventually decrease full node dependency. FRChain [100] consensus model is

mostly utilized in permissioned blockchain. It is immune to multiple nodes and blockchain network failures. For block propagation and block validation, FRChain utilizes mutual signing over multicast trees. Fast BFT [64] is a faster and scalable consensus protocol. The inventive idea of this protocol is a message grouping technique that uses hardware-based, protected execution environments (TEEs) and lightweight secret sharing. Satellite chains [96] affect the notion of satellite chains that can run many consensual protocols in private at the same time, thereby significantly increasing the scalability of the system's premises to meet industrial standards.

9. Conclusions

Blockchain has grown rapidly in the last two decades after the immense success of public blockchain networks such as Bitcoin and Ethereum. However, it has not disrupted as many industries as was expected because of the fundamental issue of scalability, which has become a major concern, especially when applying blockchain to the real-world business environment. As a matter of fact, major crypto currencies are also facing the same scalability problem. As such, public blockchain scalability is fast becoming an active research topic in academia and in industries, where many sectors are trying to adopt the blockchain in their practical applications. In this study, we found that scalability is not a singular term. There are a number of factors attached to it, including transaction throughput, number of nodes, storage, block size, high communication, latency, cost, and the verification process. Out of these, transaction throughput is the most discussed factor and is strongly linked to a consensus mechanism. It is found that most of the factors are interdependent and are somehow directly or indirectly linked to a consensus mechanism. It is also noticed that the contemporary available consensus models are not efficient enough to address the scalability issue and fail to provide required throughput and latency for industrial applications, specifically for those demanding time mission-critical (or real-time) responses such as IoT. IoT is high on the list of technologies adopting Blockchain. Other than IoT, blockchain seems to be impacting other industries such as energy, finance, resource management, healthcare, education, and agriculture; however, it is yet to achieve desired outcomes due to scalability issues, especially in public blockchain settings. The research community has attempted to address the scalability issue with different techniques. In this study, we discussed the major scalability solutions along with their challenges with respect to blockchain technology. It is foreseeable that within the next few years, blockchain will transform a lot of applications and the transformation will be driven by scalability balanced with decentralization and security requirements. In this paper, we have highlighted several potential research open issues such as the huge amount of public blockchain data storage that needs to be considered, huge bandwidth consumption, and consensus approaches aimed at addressing scalability in public blockchain systems.

Author Contributions: Manuscript preparation, study concept, and design D.K., L.T.J.; research methodology, design, data analysis, and review and visualization, D.K., M.A.H.; critical comparison, D.K., L.T.J.; survey deductions, D.K.; validation framework design, D.K., L.T.J, and M.A.H.; proof-reading, editing, and formatting, L.T.J., M.A.H. All authors have read and agreed to the published version of the manuscript.

Funding: This study is conducted in Universiti Teknologi PETRONAS (UTP) under the Fundamental Research Grant Scheme (FRGS) from the Ministry of Higher Education (MOHE) Malaysia.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

Acknowledgments: The authors extend their deep regards and acknowledgement to Universiti Teknologi PETRONAS for provision of resources and materials for the completion of this research work.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Search Strings: EEE Explore

(Blockchain OR Block Chain OR Distributor Ledger Technology OR DLT OR Cryptocurrency OR Crypto-currency OR Bitcoin OR Ethereum) AND (scalability OR scalable OR Scaling OR extensible) AND (Problem OR Issue OR challenge OR Solution OR Framework OR protocol OR Model OR Algorithm)

Search Strings: Science Direct

1. ("Blockchain" OR "Block Chain" OR "Distributor Ledger Technology" OR "Bitcoin") ("Scalability" OR "Scalable" OR "Scaling" OR "extensible") ("Problem" OR "issue" OR "challenge")

2. ("Blockchain" OR "Block Chain" OR "Distributor Ledger Technology" OR "Bitcoin ") ("Scalability" OR "Scalable" OR "Scaling" OR "extensible") ("Solution" OR "Framework" OR "protocol")

Search Strings: Web of Science

ALL = (Blockchain* OR Block chain OR Bitcoin OR "Distributor Ledger Technology" OR DLT OR Cryptocurrency) AND ALL = (Scalability OR Scalable OR Scaling OR extensible) AND ALL = (Problem OR Issue OR challenge OR Solution OR Framework OR protocol OR Model OR Algorithm) AND PY = (2010–2019)

Search Strings: Scopus

+("Blockchain scalability" (+(Blockchain bitcoin Block Chain) +(scalability Scalable Scaling) +(Problem issue challenge) +(Solution Framework protocol Model Algorithm))

References

1. Haber, S. and W.S. Stornetta. *How to time-stamp a digital document*. in *Conference on the Theory and Application of Cryptography*. 1990. Springer.
2. Nakamoto, S., *Bitcoin: A peer-to-peer electronic cash system.* Decentralized Business Review, 2008: p. 21260.
3. Tapscott, A. and D. Tapscott, *How blockchain is changing finance.* Harvard Business Review, 2017. **1**(9): p. 2-5.
4. Shift, D. *Technology Tipping Points and Societal Impact (2015)*. in *World Economic Forum Survey Report. http://www3. weforum. org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015. pdf# page*.
5. Zhou, Q., et al., *Solutions to scalability of blockchain: A survey.* IEEE Access, 2020. **8**: p. 16440-16455.
6. Cong, K., Z. Ren, and J. Pouwelse. *A blockchain consensus protocol with horizontal scalability*. in *2018 IFIP Networking Conference (IFIP Networking) and Workshops*. 2018. IEEE.
7. Chauhan, A., et al. *Blockchain and scalability*. in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. 2018. IEEE.
8. Kim, S., Y. Kwon, and S. Cho. *A survey of scalability solutions on blockchain*. in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*. 2018. IEEE.
9. Hafid, A., A.S. Hafid, and M. Samih, *Scaling blockchains: A comprehensive survey.* IEEE Access, 2020. **8**: p. 125244-125262.
10. Del Monte, G., D. Pennino, and M. Pizzonia, *Scaling blockchains without giving up decentralization and security.* arXiv preprint arXiv:2005.06665, 2020.
11. Monte, G.D., D. Pennino, and M. Pizzonia. *Scaling blockchains without giving up decentralization and security: a solution to the blockchain scalability trilemma*. in *Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems*. 2020.
12. Lee Kuo Chuen, D., *Handbook of digital currency*. 2015, Elsevier.
13. Wood, G., *Ethereum: A secure decentralised generalised transaction ledger.* Ethereum project yellow paper, 2014. **151**(2014): p. 1-32.
14. Androulaki, E., et al. *Hyperledger fabric: a distributed operating system for permissioned blockchains*. in *Proceedings of the thirteenth EuroSys conference*. 2018.
15. Greenspan, G., *Multichain private blockchain-white paper.* URl: http://www. multichain. com/download/MultiChain-White-Paper. pdf, 2015: p. 57-60.
16. Das, M., X. Tao, and J.C. Cheng, *BIM security: A critical review and recommendations using encryption strategy and blockchain.* Automation in construction, 2021. **126**: p. 103682.
17. Liu, W., et al., *A systematic literature review on applications of information and communication technologies and blockchain technologies for precision agriculture development.* Journal of Cleaner Production, 2021: p. 126763.
18. Network-Fast, R., *cheap, scalable token transfers for Ethereum.* Accessed: Jul, 2018. **7**: p. 2020.
19. Mosakheil, J.H., *Security threats classification in blockchains.* 2018.

20. Thakur, S. and J.G. Breslin. *Cost Analysis of Blockchains-based Peer to Peer Energy Trade*. in *2020 IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*. 2020. IEEE.
21. Mazlan, A.A., et al., *Scalability challenges in healthcare blockchain system—a systematic review.* IEEE Access, 2020. **8**: p. 23663-23673.
22. Xie, J., et al., *A survey on the scalability of blockchain systems.* IEEE Network, 2019. **33**(5): p. 166-173.
23. Yli-Huumo, J., et al., *Where is current research on blockchain technology?—a systematic review.* PloS one, 2016. **11**(10): p. e0163477.
24. Nguyen, G.-T. and K. Kim, *A survey about consensus algorithms used in blockchain.* Journal of Information processing systems, 2018. **14**(1): p. 101-128.
25. Yu, G., et al., *Survey: Sharding in blockchains.* IEEE Access, 2020. **8**: p. 14155-14181.
26. Keele, S., *Guidelines for performing systematic literature reviews in software engineering*. 2007, Citeseer.
27. Kitchenham, B.A. *Systematic review in software engineering: where we are and where we should be going*. in *Proceedings of the 2nd international workshop on Evidential assessment of software technologies*. 2012.
28. Atlam, H.F., et al., *Blockchain with internet of things: Benefits, challenges, and future directions.* International Journal of Intelligent Systems and Applications, 2018. **10**(6): p. 40-48.
29. Khan, D., et al. *A Critical Review of Blockchain Consensus Model*. in *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. 2020. IEEE.
30. Weber, I., et al. *On availability for blockchain-based systems*. in *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*. 2017. IEEE.
31. Sun, J., J. Yan, and K.Z. Zhang, *Blockchain-based sharing services: What blockchain technology can contribute to smart cities.* Financial Innovation, 2016. **2**(1): p. 1-9.
32. Tosh, D., et al. *CloudPoS: A proof-of-stake consensus design for blockchain integrated cloud*. in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. 2018. IEEE.
33. Cao, B., et al., *A many-objective optimization model of industrial internet of things based on private blockchain.* IEEE Network, 2020. **34**(5): p. 78-83.
34. Ferrag, M.A., et al., *Blockchain technologies for the internet of things: Research issues and challenges.* IEEE Internet of Things Journal, 2018. **6**(2): p. 2188-2204.
35. Wang, X., et al., *Survey on blockchain for Internet of Things.* Computer Communications, 2019. **136**: p. 10-29.
36. Sanka, A.I. and R.C. Cheung. *Efficient high performance FPGA based NoSQL caching system for blockchain scalability and throughput improvement*. in *2018 26th International Conference on Systems Engineering (ICSEng)*. 2018. IEEE.
37. Croman, K., et al. *On scaling decentralized blockchains*. in *International conference on financial cryptography and data security*. 2016. Springer.
38. Sedky, G. and A. El Mougy. *BCXP: Blockchain-centric network layer for efficient transaction and block exchange over Named Data Networking*. in *2018 IEEE 43rd Conference on Local Computer Networks (LCN)*. 2018. IEEE.
39. Nadiya, U., K. Mutijarsa, and C.Y. Rizqi. *Block summarization and compression in bitcoin blockchain*. in *2018 International Symposium on Electronics and Smart Devices (ISESD)*. 2018. IEEE.
40. Ahmad, A., et al. *Blocktrail: A scalable multichain solution for blockchain-based audit trails*. in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. 2019. IEEE.
41. Liu, M., et al. *Deep reinforcement learning based performance optimization in blockchain-enabled Internet of vehicle*. in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. 2019. IEEE.
42. Shabandri, B. and P. Maheshwari. *Enhancing IoT security and privacy using distributed ledgers with IOTA and the tangle*. in *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*. 2019. IEEE.
43. Ni, Z., et al. *Evolutionary Game for Consensus Provision in Permissionless Blockchain Networks with Shards*. in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. 2019. IEEE.
44. Gorenflo, C., et al., *FastFabric: Scaling hyperledger fabric to 20 000 transactions per second.* International Journal of Network Management, 2020. **30**(5): p. e2099.
45. Manshaei, M.H., et al., *A game-theoretic analysis of shard-based permissionless blockchains.* IEEE Access, 2018. **6**: p. 78100-78112.
46. Arote, P. and J. Kuri. *Hybrid Decentralized Solution for Bitcoin Zero-Confirmation Transactions*. in *2019 11th International Conference on Communication Systems & Networks (COMSNETS)*. 2019. IEEE.
47. Asgaonkar, A., P. Palande, and R.S. Joshi. *Is the cost of proof-of-work consensus quasilinear?* in *Proceedings of the ACM India Joint International Conference on Data Science and Management of Data*. 2018.
48. Ricci, S., et al., *Learning blockchain delays: a queueing theory approach.* ACM SIGMETRICS Performance Evaluation Review, 2019. **46**(3): p. 122-125.
49. Wang, J. and H. Wang. *Monoxide: Scale out blockchains with asynchronous consensus zones*. in *16th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 19)*. 2019.
50. Sun, H., et al. *Multi-blockchain model for central bank digital currency*. in *2017 18th International conference on parallel and distributed computing, applications and technologies (PDCAT)*. 2017. IEEE.
51. Bandara, E., et al. *Mystiko—blockchain meets big data*. in *2018 IEEE International Conference on Big Data (Big Data)*. 2018. IEEE.
52. Liu, M., et al., *Performance optimization for blockchain-enabled industrial Internet of Things (IIoT) systems: A deep reinforcement learning approach.* IEEE Transactions on Industrial Informatics, 2019. **15**(6): p. 3559-3570.

53. Min, X., et al. *A permissioned blockchain framework for supporting instant transaction and dynamic block size*. in *2016 IEEE Trustcom/BigDataSE/ISPA*. 2016. IEEE.
54. Herrera-Joancomartí, J. and C. Pérez-Solà. *Privacy in bitcoin transactions: new challenges from blockchain scalability solutions*. in *International Conference on Modeling Decisions for Artificial Intelligence*. 2016. Springer.
55. Malik, S., S.S. Kanhere, and R. Jurdak. *Productchain: Scalable blockchain framework to support provenance in supply chains*. in *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*. 2018. IEEE.
56. Zhuang, Q., et al. *Proof of reputation: A reputation-based consensus protocol for blockchain based systems*. in *Proceedings of the 2019 International Electronics Communication Conference*. 2019.
57. Spasovski, J. and P. Eklund. *Proof of stake blockchain: performance and scalability for groupware communications*. in *Proceedings of the 9th International Conference on Management of Digital EcoSystems*. 2017.
58. Inagaki, T., et al. *Profile-based Detection of Layered Bottlenecks*. in *Proceedings of the 2019 ACM/SPEC International Conference on Performance Engineering*. 2019.
59. Vukolić, M. *The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication*. in *International workshop on open problems in network security*. 2015. Springer.
60. Yin, J., et al. *Revisiting the incentive mechanism of Bitcoin-NG*. in *Australasian Conference on Information Security and Privacy*. 2018. Springer.
61. Khalil, R. and A. Gervais. *Revive: Rebalancing off-blockchain payment networks*. in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 2017.
62. Yu, Y., R. Liang, and J. Xu. *A scalable and extensible blockchain architecture*. in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*. 2018. IEEE.
63. Gao, Y., S. Kawai, and H. Nobuhara, *Scalable Blockchain Protocol Based on Proof of Stake and Sharding.* Journal of Advanced Computational Intelligence and Intelligent Informatics, 2019. **23**(5): p. 856-863.
64. Liu, J., et al., *Scalable byzantine consensus via hardware-assisted secret sharing.* IEEE Transactions on Computers, 2018. **68**(1): p. 139-151.
65. Burchert, C., C. Decker, and R. Wattenhofer, *Scalable funding of bitcoin micropayment channel networks.* Royal Society open science, 2018. **5**(8): p. 180089.
66. Chow, S.S., et al. *Sharding blockchain*. in *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)*. 2018. IEEE.
67. Rıfat Özyılmaz, K., H. Patel, and A. Malik, *Split-Scale: Scaling Bitcoin by Partitioning the UTXO Space.* arXiv e-prints, 2018: p. arXiv: 1809.08473.
68. Chen, H. and Y. Wang, *SSChain: A full sharding protocol for public blockchain without data migration overhead.* Pervasive and Mobile Computing, 2019. **59**: p. 101055.
69. Tsai, W.-T., et al. *A system view of financial blockchains*. in *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*. 2016. IEEE.
70. Biswas, S., et al., *A scalable blockchain framework for secure transactions in IoT.* IEEE Internet of Things Journal, 2018. **6**(3): p. 4650-4659.
71. Ehmke, C., F. Wessling, and C.M. Friedrich. *Proof-of-property: a lightweight and scalable blockchain protocol*. in *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*. 2018.
72. Vukolić, M. *Rethinking permissioned blockchains*. in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. 2017.
73. Hazari, S.S. and Q.H. Mahmoud. *A parallel proof of work to improve transaction speed and scalability in blockchain systems*. in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. 2019. IEEE.
74. Putri, B.D.C. and R.F. Sari. *The effect of latency on selfish-miner attack on block receive time bitcoin network using NS3*. in *2018 12th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*. 2018. IEEE.
75. Frahat, R.T., M.M. Monowar, and S.M. Buhari. *Secure and scalable trust management model for IoT P2P network*. in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*. 2019. IEEE.
76. Blum, R. and T. Bocek. *Superlight–A Permissionless, Light-client Only Blockchain with Self-Contained Proofs and BLS Signatures*. in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. 2019. IEEE.
77. Lu, Q., et al. *Design pattern as a service for blockchain applications*. in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*. 2018. IEEE.
78. Palai, A., M. Vora, and A. Shah. *Empowering light nodes in blockchains with block summarization*. in *2018 9th IFIP international conference on new technologies, mobility and security (NTMS)*. 2018. IEEE.
79. Zamani, M., M. Movahedi, and M. Raykova. *Rapidchain: Scaling blockchain via full sharding*. in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 2018.
80. Gao, Z., et al. *Scalable blockchain based smart contract execution*. in *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*. 2017. IEEE.
81. Chen, J., Z. Lv, and H. Song, *Design of personnel big data management system based on blockchain.* Future Generation Computer Systems, 2019. **101**: p. 1122-1129.

82. Yamada, Y., T. Nakajima, and M. Sakamoto. *Blockchain-LI: a study on implementing activity-based micro-pricing using cryptocurrency technologies*. in *Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi Media*. 2016.
83. Han, R., N. Foutris, and C. Kotselidis. *Demystifying crypto-mining: Analysis and optimizations of memory-hard pow algorithms*. in *2019 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS)*. 2019. IEEE.
84. Jiang, Y. and Z. Lian. *High performance and scalable byzantine fault tolerance*. in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*. 2019. IEEE.
85. Dorri, A., et al., *LSB: A Lightweight Scalable Blockchain for IoT security and anonymity.* Journal of Parallel and Distributed Computing, 2019. **134**: p. 180-197.
86. Liu, C., et al., *Normachain: A blockchain-based normalized autonomous transaction settlement system for iot-based e-commerce.* IEEE Internet of Things Journal, 2018. **6**(3): p. 4680-4693.
87. Sarda, A., et al. *NoCo: An Efficient Transaction Propagation Protocol for Open Blockchains*. in *2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T)*. 2018. IEEE.
88. Bansal, G., et al. *Smartchain: a smart and scalable blockchain consortium for smart grid systems*. in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*. 2019. IEEE.
89. Bai, H., G. Xia, and S. Fu. *A two-layer-consensus based blockchain architecture for iot*. in *2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC)*. 2019. IEEE.
90. Xiang, F., et al., *Jointgraph: A DAG-based efficient consensus algorithm for consortium blockchains.* Software: Practice and Experience, 2019.
91. Worley, C. and A. Skjellum. *Blockchain tradeoffs and challenges for current and emerging applications: generalization, fragmentation, sidechains, and scalability*. in *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)*. 2018. IEEE.
92. Imtiaz, M.A., et al. *Churn in the bitcoin network: Characterization and impact*. in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 2019. IEEE.
93. Kaneko, Y. and T. Asaka. *DHT clustering for load balancing considering blockchain data size*. in *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)*. 2018. IEEE.
94. Zhong, G., et al. *FastProxy: Hardware and software acceleration of stratum mining proxy*. in *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*. 2019. IEEE.
95. de Oliveira, M.T., et al. *Towards a blockchain-based secure electronic medical record for healthcare applications*. in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. 2019. IEEE.
96. Li, W., et al. *Towards scalable and private industrial blockchains*. in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. 2017.
97. Han, R., et al., *On the performance of distributed ledgers for internet of things.* Internet of Things, 2020. **10**: p. 100087.
98. Bugday, A., et al., *Creating consensus group using online learning based reputation in blockchain networks.* Pervasive and Mobile Computing, 2019. **59**: p. 101056.
99. Do, T., T. Nguyen, and H. Pham. *Delegated proof of reputation: A novel blockchain consensus*. in *Proceedings of the 2019 International Electronics Communication Conference*. 2019.
100. Chander, G., P. Deshpande, and S. Chakraborty. *A fault resilient consensus protocol for large permissioned blockchain networks*. in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 2019. IEEE.
101. Blom, F. and H. Farahmand. *On the scalability of blockchain-supported local energy markets*. in *2018 International Conference on Smart Energy Systems and Technologies (SEST)*. 2018. IEEE.
102. Zou, J., et al., *A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services.* IEEE Transactions on Services Computing, 2018. **12**(3): p. 429-445.
103. Zheng, Z., et al. *An overview of blockchain technology: Architecture, consensus, and future trends*. in *2017 IEEE international congress on big data (BigData congress)*. 2017. IEEE.
104. Wang, Z. *MOCA: A Scalable Consensus Algorithm Based on Cellular Automata*. in *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*. 2018. IEEE.
105. Ravindran, R. *Circle of Trust: A High Volume, Energy Efficient, Stake Blind and High Attack Tolerant Blockchain Consensus Protocol*. in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*. 2019. IEEE.
106. Zhu, X. *Research on blockchain consensus mechanism and implementation*. in *IOP Conference Series: Materials Science and Engineering*. 2019. IOP Publishing.
107. Liu, D., et al., *Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain.* IEEE Transactions on Industrial Informatics, 2019. **15**(6): p. 3527-3537.
108. Zander, M., T. Waite, and D. Harz, *DAGsim: Simulation of DAG-based distributed ledger protocols.* ACM SIGMETRICS Performance Evaluation Review, 2019. **46**(3): p. 118-121.
109. Xu, Y., et al. *E-commerce blockchain consensus mechanism for supporting high-throughput and real-time transaction*. in *International Conference on Collaborative Computing: Networking, Applications and Worksharing*. 2016. Springer.
110. Thakkar, P., S. Nathan, and B. Viswanathan. *Performance benchmarking and optimizing hyperledger fabric blockchain platform*. in *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*. 2018. IEEE.

111. Otte, P., M. de Vos, and J. Pouwelse, *TrustChain: A Sybil-resistant scalable blockchain.* Future Generation Computer Systems, 2020. **107**: p. 770-780.
112. Jalalzai, M.M. and C. Busch. *Window based BFT blockchain consensus*. in *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)*. 2018. IEEE.
113. El-Hindi, M., et al. *Blockchaindb-towards a shared database on blockchains*. in *Proceedings of the 2019 International Conference on Management of Data*. 2019.
114. Maiyya, S., et al., *Database and distributed computing fundamentals for scalable, fault-tolerant, and consistent maintenance of blockchains.* Proceedings of the VLDB Endowment, 2018. **11**(12).
115. Spasovski, J. and P. Eklund, *Proof of Stake Blockchain: Performance and Scalability for Groupware Communications, Copenhagen*. Denmark.
116. Li, Y., L. Qiao, and Z. Lv, *An optimized byzantine fault tolerance algorithm for consortium blockchain.* Peer-to-Peer Networking and Applications, 2021: p. 1-14.
117. Konstantinidis, I., et al. *Blockchain for business applications: A systematic literature review*. in *International Conference on Business Information Systems*. 2018. Springer.
118. Conoscenti, M., A. Vetro, and J.C. De Martin. *Blockchain for the Internet of Things: A systematic literature review*. in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. 2016. IEEE.
119. Garzik, J., *Block size increase to 2MB.* Bitcoin Improvement Proposal, 2015. **102**.
120. Zou, J., et al. *3d-dag: A high performance dag network with eventual consistency and finality*. in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*. 2018. IEEE.
121. Lombrozo, E., J. Lau, and P. Wuille, *Segregated witness (consensus layer).* Bitcoin Core Develop. Team, Tech. Rep. BIP, 2015. **141**.
122. Mechkaroska, D., V. Dimitrova, and A. Popovska-Mitrovikj. *Analysis of the possibilities for improvement of blockchain technology*. in *2018 26th Telecommunications Forum (TELFOR)*. 2018. IEEE.
123. Luu, L., et al. *A secure sharding protocol for open blockchains*. in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 2016.
124. Kokoris-Kogias, E., et al. *Omniledger: A secure, scale-out, decentralized ledger via sharding*. in *2018 IEEE Symposium on Security and Privacy (SP)*. 2018. IEEE.
125. Baliga, A., *Understanding blockchain consensus models.* Persistent, 2017. **4**: p. 1-14.
126. De Filippi, P., *What blockchain means for the sharing economy.* Harvard Business Review, 2017. **15**: p. 1-5.
127. Vasin, P., *Blackcoin's proof-of-stake protocol v2.* URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf, 2014. **71**.
128. Eyal, I., et al. *Bitcoin-ng: A scalable blockchain protocol*. in *13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16)*. 2016.
129. Poon, J. and T. Dryja, *The bitcoin lightning network: Scalable off-chain instant payments*. 2016.