IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 23, 2019, accepted January 12, 2020, date of publication January 24, 2020, date of current version February 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2969230

Scalability Challenges in Healthcare Blockchain System–A Systematic Review

AHMAD AKMALUDDIN MAZLAN[1], SALWANI MOHD DAUD[1], (Member, IEEE), SURIANI MOHD SAM[1], (Member, IEEE), HAFIZA ABAS[1], SITI ZALEHA ABDUL RASID[2], AND MUHAMMAD FATHI YUSOF[1]

[1]Razak Faculty of Technology and Informatics (RFTI), Universiti Teknologi Malaysia (UTM), Kuala Lumpur 54100, Malaysia
[2]Azman Hashim International Business School (AHIBS), Universiti Teknologi Malaysia (UTM), Kuala Lumpur 54100, Malaysia

Corresponding author: Salwani Mohd Daud (salwani.kl@utm.my)

This work was supported in part the Ministry of Education, Malaysia, and in part by the Universiti Teknologi Malaysia under Grant Q.K130000.3556.05G71.

ABSTRACT Blockchain technology is a private, secure, trustworthy, and transparent information exchange performed in a decentralised manner. In this case, the coordination and validation efforts are simplified as the records are designed to update regularly and there is no difference in the two databases. This review focuses on how the blockchain addresses scalability challenges and provides solutions in the healthcare field through the implementation of blockchain technology. Accordingly, 16 solutions fell under two main areas, namely storage optimization and redesign of blockchain. However, limitations persist, including block size, high volume of data, transactions, number of nodes, and protocol challenges. This review consists of six stages, namely identification of research question, procedures of research, screening of relevant articles, keywording based on the abstract, data extraction, and mapping process. Through Atlas.ti software, the selected keywords were used to analyse through the relevant articles. As a result, 48 codes and 403 quotations were compiled. Manual coding was performed to categorise the quotations. The codes were then mapped onto the network as a mapping process. Notably, 16 solutions fell under two main areas, namely storage optimization and redesign of blockchain. Basically, there are 3 solutions compiled for storage optimization and 13 solutions for the redesign of the blockchain, namely blockchain modelling, read mechanism, write mechanism, and bi-directional network.

INDEX TERMS Blockchain, healthcare, scalability, systematic review.

I. INTRODUCTION

In October 2008, Satoshi Nakamoto published the first blockchain article called "Bitcoin: A Peer-to-Peer Electronic Cash System." The Bitcoin system proposed by Satoshi Nakamoto was based on cryptology proofing instead of trust, enabling two or more parties to perform transactions without a mediator. These parties were known as "trusted third party" (TTP). As a result, this proposal solved the verification of private transaction. This transaction was known as the double-spending problem [1], which was the first application of blockchain.

Blockchain technology is a private, secure, trustworthy, and transparent information exchange performed in a decentralised manner. Therefore, the coordination and validation efforts for the decentralised database are simplified as the records are designed to update regularly and there is no difference in the two databases.

The wide-ranged and promising possibility of blockchain technology contributed to enhanced assistance in the healthcare field to medical staff and other parties in healthcare institutions. This improved assistance is in terms of system architecture [2]–[7], verified and authenticated record [3], [5], [8]–[15], storage of medical records [4], [5], [10], [15], [17], [18], [26], interoperability [13], [25], [26], [32], security system [11], [14], [17], [23], [24], and biomedical system [15], [17], [25], [26].

This review focuses on how blockchain addresses scalability challenges and provides solutions in the healthcare field through the implementation of blockchain technology. However, several challenges persists, including the number of nodes [10], [15], [19], [27], [28], transactions [9],

The associate editor coordinating the review of this manuscript and approving it for publication was Malik Jahan Khan.

[10], [15], [28]–[30], high volume of data [13], [20], [30], [32], [33], protocol challenges [9], [10], [15], [28], [34], and block size [10], [12], [30]. To achieve productive benefits, current technology should be developed by solving these challenges.

This systematic review article consists of six sections. Specifically, Section II elaborates on blockchain-based features and highlights the works of literature related to them. Section III highlights the research methodology, questions, and procedures. This is followed by Section IV which elaborates the results based on research questions. Section V addresses the findings and primary challenges in the healthcare system. This article is concluded in Section VI, which also presents future directions.

II. RELATED WORKS

A. BLOCKCHAIN

Blockchain is a Peer-to-Peer (P2P) distributed ledger technology (DLT) which redefines trust in a web-based interstate information network. It was initially invented for the financial industry, followed by the idea of transactions proliferating without a mediator. Similar to governments and corporations, mediators mostly play the role of trusted third party (TTP), who receive, process, and store transactions. However, the trust in TTP is not preferable due to its possibility to fail or malfunction, lose security, become compromised, or result in the absence of the financial system [32].

From the technical point of view, blockchain is a distributed database which is present in a P2P network. It consists of blocks, nodes, and contracts. The blocks contain information and the nodes are the point of connection between participants. Every node stores a local copy, known as the block in the blockchain system. The contracts happened when the consensus of nodes agrees upon the transaction's validity. Thus, the transaction is considered valid [35].

In the case of blockchain systems, the trust is decentralised. Meanwhile, the system and technology play the role of the mediators behind. Importantly, trust in the system among users is essential, which is followed by the sharing of keys between participants.

B. USE OF BLOCKCHAIN IN HEALTHCARE SYSTEM

Blockchain-based application in medicine offers a remarkable opportunity for healthcare support. Four primary categories of health or clinical blockchain applications were found in previous literature. The first category was the improvement in electronic medical record management for primary patient care. This could be seen from the provision of record access on multiple disconnected healthcare institutions, prevention of data duplication, security, and scalability. The second category was the applications which enhanced insurance claim processes, such as "smart health profiles" for insurance applicants or recipients, the sharing of medical record using smart contracts in blockchain and management of pre-authorization payments. Meanwhile, the third category was the applications which facilitated clinical or biomedical research, including the applications which assisted with the collection and management of patient-generated health data for research purposes. It also consisted of those which facilitated data sharing among researchers. Following that, the fourth category was the application which connected various healthcare players or providers. This application allowed consumers to anonymously engage with the caregiver, including private engagement with the rate of deal transaction.

The significant potential of blockchain is indicated through the increase in grant researches, proposed applications or techniques, technical reviews, and eye-catching. Subsequently, the increase in healthcare institutions and industry is achieved according to the adoption of this blockchain technology. However, the blockchain-based application is a relatively new technology. This is added with the abundance of inaccurate information, uncertainties, and speculations about the potential utility of blockchain in the healthcare field. Therefore, a clear focus and judgement are necessary to achieve accurate results.

Notably, there are challenges and opportunities related to the blockchain-based application in healthcare domain which needs to be investigated in many viewpoints. A distributed system which eliminated the intermediaries possesses a strong potential of disrupting various healthcare procedures [31].

III. RESEARCH METHODOLOGY

A. SYSTEMATIC REVIEW EXECUTION

This review involves six stages, namely (1) the identification of research question, (2) research procedures, (3) screening of relevant articles, (4) keywording based on the abstract, (5) data extraction, and (6) mapping process.

B. IDENTIFICATION OF A RESEARCH QUESTION

Understanding the research questions is an essential task before the research procedures are carried out. Following are the research questions related to scalability challenges in blockchain and healthcare system:

1) WHAT ARE THE SCALABILITY CHALLENGES IN BLOCKCHAIN-BASED APPLICATIONS IN HEALTHCARE?

This research question is vital in understanding various blockchain scalability challenges in the healthcare system. Specifically, the relevant articles from scientific databases need to be reviewed to determine the specific scalability challenges which require solutions. Following that, the map of scalability issues can be presented after the categorisation of the challenges.

2) WHAT ARE THE BLOCKCHAIN-BASED SOLUTIONS WHICH HAVE BEEN PROPOSED FROM THE IDENTIFIED CHALLENGES?

Despite numerous applications being proposed, not all have been successfully developed into a working prototype. There are various challenges in real-world implementations which could be identified through the review of relevant articles. Therefore, understanding and mapping the solutions in relation to the challenges are crucial. These solutions would then highlight the research gap and lead the direction of future research.

3) HOW ARE THE SOLUTIONS AND LIMITATIONS CURRENTLY BEING ADDRESSED?

This research question aims to achieve an understanding of the blockchain-based healthcare applications proposed by researchers as a guide for future projects. These applications and proposed solutions need to be categorised through mapping techniques. Notably, various modifications and improvements have been done. As a result, clear directions on positive research prospects for blockchain-based applications in the healthcare industry could be achieved.

C. CONDUCTING RESEARCH

To develop the most substantial findings, several approaches need to be implemented including search strategy, inclusion, and exclusion criteria.

1) SEARCH STRATEGY

In extracting the related articles in keyword form, the research strategy was first conducted using the key term-based method. The specific words searched on Google Scholar included "blockchain", "healthcare", and "scalability" among others. This was followed by the selection and downloading of all articles from the earliest to the latest publication. The aforementioned articles, reports, and publications originated from various sources including journals, conferences, IEEE, ACM, and SCOPUS.

2) EXCLUSION AND INCLUSION CRITERIA

After the questions related to the scope were proposed, all the primary studies were considered to identify the suitable information related to this study's systematic review. In this case, 184 articles were excluded as they were clearly focused on "blockchain" instead of "blockchain in healthcare." Meanwhile, 18 prime articles were included and tagged for data extraction. Table 1 below presents the articles with the corresponding ID.

TABLE 1. Exclusion and inclusion criteria.

Criteria	Details
Exclusion	Not cited. Published between 2015 until 2019. Duplications of articles from different sources. Titles does not mention or relate to healthcare.
Inclusion	Cited at least once. Systematic review related to healthcare and blockchain. Published after 2015. Abstract, introduction or conclusion is related to healthcare research.

D. SCREENING OF RELEVANT ARTICLES

The identified articles would be screened based on several citations provided by the database. It was crucial for the relevant articles to be cited at least once. Therefore, 38 articles which citation ranged from once to 38 times were obtained, and they were relevant to this systematic review. This was followed by the addition of 38 articles into the software using Atlas.ti.

E. KEYWORDING BASED ON THE ABSTRACT

Generally, every article would present essential keywords after the abstract section. Subsequently, 34 keywords from relevant articles were compiled in Atlas.ti. However, the keywords relevant to this review were "blockchain", "scalability," and "healthcare."

F. DATA EXTRACTION AND MAPPING PROCESS

Using Atlas.ti software, the selected keywords were used to search for all the relevant articles. As a result, approximately 48 codes and 403 quotations were compiled from the results. The codes were then manually coded to categorise the quotations. The mapping of codes was conducted onto the network as a mapping process. In this process, the relation between the codes was created. The scheme of the codes network is shown in Section V.

IV. RESULTS

In this section, the results of the systematic review are presented. In reference to this research strategy, a total of 305 articles was collected from the source.

Following the first screening which was based on the titles of the articles and citations, 184 articles were excluded. The remaining 121 articles were those which were not related to healthcare. Nevertheless, the unrelated articles were left for further selection. Additionally, healthcare application might have been stated in the abstracts, therefore, it was obtained by the research protocol. Then, duplications were eliminated by merging the 25 articles from Mendeley, leading the reduction of the selected articles to 38.

In the next screening process, the abstracts of the selected articles were examined. In some cases, the introduction and the conclusion were based on the criteria defined in Section III.C.2 to further screen the article.

All of the selected articles were scrutinised, which were followed by three more articles being included to refer to other articles from a specific article. In these articles, the topic of healthcare was mentioned in one of the sections as a potential application of blockchain, leading to new solutions. However, three articles were excluded due to the absence of substantial information regarding scalability issues.

At the end of this phase, 41 articles were selected in this study, which would be included on the list in the references section.

V. DISCUSSIONS

In this section, the compilation of articles was made into two categories, namely (A) Summary of Challenges and (B) Summary of Solutions. Five main challenges were discussed, including details on scalability issues and 16 solutions under two main categories.

A. SUMMARY OF CHALLENGES

Following are the issues reviewed from relevant articles to provide insights on the issue of scalability challenges.

1) BLOCK SIZE

Block size refers to the maximum capacity for a block to be filled up with transactions. If the capacity is exceeded, the block will be rejected by the network.

Blockchain is a decentralized database system. Therefore, distributed ledger indicates that every transaction is processed by every node and consists of a copy of the entire state of the ledger [10], [12]. However, only the important ledgers for specific nodes would be sufficient in the healthcare system instead of the complete copy of the ledger.

Another example for the block size issue is the unprocessed patient data including genomic, critical organs, and others. Although bigger data packets on-chain contribute to higher storage costs, more data are available on-chain to audit [30]. Therefore, a balance in the ubiquitous store and exchange transactions is essential.

2) HIGH VOLUME

High volume is defined by the high number of transactions occurred at a real-time. When a Blockchain system is used as a database to store patient profile data, millions of records could be replicated on all Blockchain participants in a large-scale healthcare scenario [20]. As a result, an overflow of information would take place. Notably, this overflow of information leads to a severe problem of high volume of data storage in healthcare institutions in the development of scalable interconnected provider [13].

In various cases, unprocessed files including raw genomic date may amount more than 1 TB per genome. Therefore, they should be avoided when patient data were placed on-chain [30]. Furthermore, placing high-volume biomedical data on the blockchain-based system is not a proper action due to its critical performance degradation [32]. This action consists of significant energy, delay, and overhead which are not suitable for most resource constrained IoT devices [33]. Subsequently, higher costs of the deployment would take place.

3) TRANSACTIONS

A blockchain transaction is a form of conducting business with multiple entities in a specific network. The blockchain market development is progressive as developers continue identifying the latest methods to conduct blockchain transactions. However, challenges are present when the blockchain system scales up the technology for high transaction volume [15]. Specifically, the current set-up of the Ethereum blockchain requires the verification of every transaction by every single validator on the network. This is a factor in the slow speed of the network based on the data load [9]. Therefore, a long duration is required to reach a consensus or verification of digital identity. Similarly, Ethereum, one of the popular blockchain-based providers, is also faced with scalability challenges including the speed of transaction verification [10].

Existing solutions require the blockchain to generate high amount of transactions to be processed and connected to the network. This transaction results in the degradation of overall performance. Another case to be considered is the possibility for the capability rate of data synchronization in the system to be lower than the rate of transactions required to record in the blockchain system [28]. Overall, the duration of response towards the request increases as the number of computing devices increases [29].

Zero-knowledge proof (ZKP) is the crypto-based method to verify other entities. It provides a permit for the system to hide a transaction origin, destination, and content while allowing the transfers to be immutable. However, the disadvantage of ZKP's is its computational intensity. Specifically, it requires multiple rounds of verification process between the sender and the receiver, which increases with every series of process. Furthermore, this transaction leads to further network delay and reduces scalability [24]. The maximum rate of transaction validation within the bitcoin network is ≈ 7 transactions per second, which leads to a limited throughput of large blockchain networks [31].

4) NUMBER OF NODES

A node is a component on a blockchain-based system. It is the foundation of the technology which represents each entity connected to the network. Logarithmically, if more nodes are added to the network, the internode latency increases with every additional node [10]. Additionally, the increasing number of nodes leads to an increase in computational resources in an IoT environment.

The difficulty in running blockchain-based applications would significantly increase with the increased number of members or patients in the system. This is followed by the increment in the computational requirements of the whole blockchain infrastructure [15]. Therefore, it is crucial for research and trials to ensure that the implementing of the blockchain applications is cost-effective [19].

Lightweight nodes, which are known as *partial nodes, are* dependent on the full nodes to function. Although the whole blockchain does not need to be stored, the increased number of lightweight nodes may significantly lead to workload on blockchain servers. As a result, the scalability and throughput of blockchain applications would be affected [27].

Logically, blockchain with the involvement of a large community or participants possesses higher reliability and provides better protection and higher reliability. However, this involvement would lead to performance degradation due to the increase in the number of entities in every stage [28]. To illustrate, writing or reading the data will result in slow progress of every transaction completion, which also requires numerous computer resources. Notably, although the definition of the threshold number of large communities is the key issue, it has yet to be addressed or adequately tested.

In the healthcare field, the connection of large communities connected is expected, which will involve the use of blockchain. Therefore, a high amount of transactions will be generated and recorded due to the increased usage of blockchain. The blockchain-distributed ledger will append new transactions after the agreement of multiple entities on every transaction linked to the transactions in the ledger. Although this process seems complex, it is effective as a limited size of the blockchain is given [28]. Pre-authorization payments are even used by some parties using short-term data sharing to decrease the amount of memory usage in the blockchain.

Another issue is present in the process of blockchain to identify, verify, or use earlier transactions. Therefore, with multiple processes happening at real-time, the system performance degrades with larger size of the blockchain [28].

5) PROTOCOL

In the current set-up of the Ethereum blockchain, the verification of every transaction is required by every validator on the network. Due to this phenomenon, a fairly slower network occurs depending on the data load [9]. Besides, blockchain may be impractical in various other applications due to its immutable characteristic [10].

In some emergency cases, some patient's issues, including unpredictable access, could not be resolved by the blockchain system. Furthermore, the permission of access to their records to a surgeon (or other parties) was not authorized previously during emergency [15]. Patients are also often reluctant to be involved or give their consent to data sharing due to the currently inadequate appropriate mechanisms. Therefore, in cases like these, a fair duration length is needed to obtain fast response of the system, including the agreement of all entities on the critical transactions [28]. Overall, protocols related to security, storage, validation, and access must satisfy the latency and throughput requirements to achieve the efficiency of blockchain [32].

B. SUMMARY OF SOLUTIONS

Table 2 illustrates the solutions which are categorised under two main areas, namely storage optimisation and redesign of blockchain, reviewed from relevant articles to prove insights regarding scalability challenges.

Fig. 1 presents the scalability solutions and issues mapped using Atlas.ti version 8.0 to present the mind map of categorisation. This is followed by the details of the solutions discussed in Section V.B.1 and Section V.B.2.

TABLE 2. Category of solutions.

Challenges	Solutions
1. Block Size 2. High Volume of Data 3. Transactions 4. Number of Nodes	Storage Optimization
1. Protocol 2. Block Size	Redesigning Blockchain

1) STORAGE OPTIMIZATION

In this section, block size and a high volume of data are focused on. Basically, there are 3 solutions compiled for storage optimization.

To ensure scalable data integrity and maintain a hash of the original data for exchange, Zhang (2018) proposed FHIRChain by enhancing the size of the reference pointer of the data [12]. Based on the complexity of data exchange, N represented the size of the original data, while ϵ represented the size of its reference pointer is. In the case of space complexity, the total amount of data stored on-chain was described as $O(\text{hash}(N) + \epsilon)$.

The fixed value of the hashed output of a variable-length input consumes a constant amount of space. Compared to the size of actual data, the size of a data reference pointer is scalably smaller. Therefore, instead of actual data, Zhang's design used constant size of the data which enhanced the scalability features.

The second solution for storage optimisation is the mini blockchain. Bruce [36] proposed a concept for transaction process, which was called mini-blockchain. It is a process which aims to remove the requirement for storing the entire blockchain to enhance the scalability.

Basic operations could be optimised by separating the functions of the blockchain into individual mechanisms. In this scheme, the script system and the old interlocking transaction records are discarded to trim the block. Next, it is replaced with a simpler concept of basic operations. In this case, an account tree was involved as the balance sum, including any transactions. The key of these operations is to specify these functions into groups of transactions which are included in the database in periodic intervals of time.

A novel scheme known as VerSum was proposed in another study. It solves low server-side overhead by enabling the outsourcing of expensive computations over a high number of public logs to a collection of servers, including Certificate Transparency log, Namecoin blockchain, and Bitcoin among others [37]. Furthermore, VerSum clients verify that the output is accurate by cross-checking with the outputs from multiple servers. In another case, VerSum develops a conflict resolution protocol to determine any mistakes occurring from outsourcing and accurately identifies the right output.

FIGURE 1. **Mapping of scalability issues with solutions.**

2) REDESIGNING BLOCKCHAIN

The issues focused in this section are transactions, number of nodes, and protocol. Essentially, there are four categories for 13 solutions for the redesign of the blockchain, namely blockchain modelling, read mechanism, write mechanism, and bi-directional network.

Blockchain modelling consists of three solutions, namely FHIRChain, Healthchain, DeepLinQ, and OmniPHR. Specifically, FHIRChain is a blockchain architecture proposed by Zhang *et al.* [12]. It was designed to meet the requirements from the Office of the National Coordinator for Health IT (ONC) for secure and scalable sharing of clinical data. By integrating FHIR with blockchain architecture, FHIRChain produces lightweight reference pointers without sharing actual databases. This is followed by an exchange of these pointers via the blockchain component. FHIRChain functions as the solution for network coverage, especially in the clinics or telemedicine clinics in rural areas, by enabling scalable data-sharing without having to exchange data with another centralised repository [12].

HealthChain was proposed by Ahram *et al.* [22]. Powered by Blockchain, it primarily benefits from the modular architecture of Hyperledger fabric which enables confidentiality, scalability, and security in health informatics. Its implementation of smart contracts ensures proper authorization and specifies the privileges on its permitted network.

Proposed by Chang *et al.* [34], DeepLinQ is a multi-layer blockchain architecture which improves flexibility, accountability, and scalability through on-demand queries, proxy appointment, subgroup signatures, granular access control, and smart contracts. This blockchain architecture aims to support privacy-preserving data sharing [34].

OmniPHR was proposed by Roehrs *et al.* [38]. It is an architecture of elasticity, interoperability, and scalability of single-view Personal Health Records (PHR) data. Distributed on a P2P network, it aims towards the partition of PHR in data blocks. Furthermore, it is indicated from the evaluation of the architecture that OmniPHR could ensure the division of PHR into data blocks and proportional distribution in a routing overlay network.

Notably, it could be seen from the OmniPHR that the latency remained stable despite the increase in the number of nodes, routing overlays, and backbone routers. Subsequently, a more significant number of messages was transmitted at the same time in the network

Secondly, read mechanism consists of solutions, namely short-term data sharing and caching system. Zhang *et al.* [20] proposed that a more scalable and secure alternative is required in short-term data sharing. This is essential to store and exchange encrypted metadata through a reference pointer and expiration configuration. Furthermore, users would be able to maintain their data ownership and incorporate the data with existing healthcare services through the exchange of encrypted reference pointers. Additionally, user data sharing could be performed at critical times, such as accidents, to provide fast treatment and prevent the delay of process in a timely manner.

TABLE 3. Method or model for scalability issues.

Method / Model	Summary
Reference pointer of FHIRChain [12]	Enhancing the size of the reference pointer of the data to make it scalably smaller.
Mini blockchain [36]	Enhance the scalability by removing the requirement for storing the entire blockchain.
VerSum [37]	Use smaller computational resources by enabling the outsourcing computations over a high number of public logs to a collection of servers.
FHIRChain [12]	It was designed for secure and scalable sharing of clinical data. FHIRChain produces lightweight reference pointers without sharing actual databases and as a solution for network coverage, especially in the clinics or telemedicine clinics in rural areas.
HealthChain [22]	Its implementation of smart contracts ensures proper authorization and specifies the privileges on its permitted network.
DeepLinQ [34]	Multi-layer blockchain architecture which improves flexibility, accountability, and scalability through on-demand queries, proxy appointment, subgroup signatures, granular access control, and smart contracts.
OmniPHR [38]	Latency remained stable despite the increase in the number of nodes, routing overlays, and backbone routers. Plus, significant number of messages was transmitted at the same time in the network.
Short-term data sharing [20]	Able to store and exchange encrypted metadata through a reference pointer and expiration configuration. Essential for healthcare services subscription or even in emergency situations.
Caching system [27]	This design improves throughput performance with the use of less FPGA power and work area. Besides, remarkable reduction of workload by 103 times was observable from the result.
Smart contract [5]	It has the potential of reducing fraud as a legal digital agent to create, store, and enforce contract. It builds on trust between publisher and subscriber.
Tokenization [12]	This method will complement the process of encryption by generating a pair of keys for user and registers.
Chord algorithm [28]	The algorithm provide service for OmniPHR distribution on the P2P network for adaptation to changes of workload, linkage for distributed network, and managing amount of workload.
Sharding [39]	It divides the mining network into smaller parallel chains. Therefore, each shard process is in parallel with other shards, leading to a micro block from each shard. Zilliqa claimed that this process is linearly scalable to the expansion of the blockchain network.
Practical Byzantine Fault Tolerant (PBFT) consensus protocol [39]	Improved the finality of transactions and no confirmation is required for additional (next) block. However, only happened if the group consensus occurs in a sequential.
TrustChain [40]	Self-reinforcing trust are enabled by the preferring agents who have been helpful to the other agents in the past.
Lightning network [41]	The design of network of micropayment channels enables bitcoin scalability and micropayments to the near-instant transactions. It represents the transactions and funds transfer could be performed without the risk of counterparty theft.

A caching system was proposed by Sanka and Cheung [27] through FPGA due to low resource consumption and low power performance. Originally, high power and resource consumption occur when cached by CPU during high workload. Notably, SHA-256 hash functions to reduce the server workload during high task management, and scalability issue is solved when it is included in the use of FPGA. This design improves throughput performance with the use of less FPGA power and work area. Besides, remarkable reduction of workload by 103 times was observable from the result.

Write mechanism consists of seven solutions, namely smart contract, algorithm, fault-tolerant, consensus protocol, trust-chain, sharding and, peer authentication.

Gökalp *et al.* [5] analysed that smart contract technology has the potential of reducing insurance fraud at all ranges of level from corporate management of funds to individual claims. Furthermore, insurance fraud prevention could be performed with lower costs due to less overhead required to maintain and operate the system. Furthermore, it mainly functions as a legal digital agent to create, store, and enforce

TABLE 4. Solutions for scalability issues.

Solutions	Category	
1. Mini blockchain [36]		Storage Optimization
2. VerSum [37]		
3. Reference pointer FHIRChain [12]		
4. FHIRChain [12]	Blockchain modelling	Redesigning Blockchain
5. HealthChain [22]		
6. DeepLinQ [34]		
7. OmniPHR [38]		
8. Short-term data sharing [20]	Read mechanism	
9. Caching system [27]		
10. Smart contract [5]	Write mechanism	
11. Chord algorithm [28]		
12. Tokenization [12]		
13. Sharding [39]		
14. Practical Byzantine Fault Tolerant (PBFT) consensus protocol [39]		
15. TrustChain [40]		
16. Lightning network [41]	Bi-directional	

contracts by supporting data exchange in a real-time manner with the blockchain architecture.

Based on the algorithm approach, two techniques are involved, namely tokenization and chord algorithm. As token-based permission was designed to encrypt the users' digital content. Therefore, the content decryption could only be carried out by the token-holder. This method will generate a new pair of signing keys for two or more token-holders (user and registers) including users' digital identities [12]. The attributes of the Chord algorithm as the search service for OmniPHR distribution on the P2P network are elasticity (adapting to changes of workload), interoperability (being part of a collaborative and distributed network), and scalability. Elasticity refers to its adaptability to changes of workload, interoperability refers to its involvement in a collaborative and distributed network, while scalability refers to its ability in managing the increased amount of workload [38].

Zilliqa [39] is the first public blockchain platform which implements sharding. It automatically divides the mining network into smaller parallel chains known as "shards". All transactions are divided into small portions. Therefore, each shard process is in parallel with other shards, leading to a micro block from each shard. One complete block consists of micro blocks which are then incorporated into the blockchain. Based on the proposed system, sharding could be applied to the architecture, transaction processes, micro block, and computational resources. Additionally, Zilliqa claimed that this process is linearly scalable with the application of computation with parallelisable computation load, train neural nets, and application with high complexity and high precision algorithms.

Zilliqa [39] also used an optimised Practical Byzantine Fault Tolerant (PBFT) consensus protocol in the their proposed blockchain system, which improved the finality of transactions. In fact, PBFT functions differently compared to Point of Work (PoW) which enables the consensus to multiple confirmations. However, PBFT only enables the group consensus to occur in a sequence.

Notably, the advantage of PBFT is that no confirmation is required for additional block. Instead, PBFT relies on a dedicated block, which is dependent on the correct leader. With the absence of progress in the consensus process, the declaration of leader change could be independently done. Due to finality, the current transaction only needs to be stored in the latest phase. Furthermore, PBFT could directly influence the scalability of Blockchain. An example of this phenomenon is the Byzantine fault-tolerant algorithms, which eliminate scalability challenges due to pre-decided validating entities. The pre-decided validating activities involve pre-preparation phase, preparation phase, and engagement phase. To be specific, the pre-preparation phase involves the next group agreement on the leader's direction, preparation phase involves the verification of pre-preparation messages, while engagement phase involves the validation decision.

In respect of transaction speed and consensus, TrustChain was proposed by Otte and Poulwelse [40] for blockchain scalability and throughput improvement. With the use of data structure, which is resilient against various types of malicious behaviours, TrustChain illustrates the possibility to accurately record community contributions by agents. Subsequently, the mechanisms of self-reinforcing trust are enabled by the preferring agents who have been helpful to the other agents in the past.

Bi-directional consists of the lightning network, which is the one of the solutions to scalability issues. In the case of transaction speed and consensus, lightning network was proposed for blockchain scalability and throughput improvement. The development of the network of micropayment channels enables bitcoin scalability and micropayments to the near-instant transactions. These channels represent real Bitcoin transactions through the use of Bitcoin scripting opcodes. Subsequently, funds transfer could be performed without the risk of counterparty theft, especially with long-term miner risk mitigations. [41].

VI. CONCLUSION

The challenges compiled in this review included block size, the high volume of data, transactions, number of nodes, and protocol challenges. Table 3 are the compilation of those methods or models with remarks based on its strengths or weaknesses. Furthermore, able IV shows the identification of 16 solutions, which were categorised into two main areas, namely storage optimization and redesigning blockchain. Basically, there are 3 solutions compiled for storage optimization and 13 solutions for the redesign of the blockchain, namely blockchain modelling, read mechanism, write mechanism, and bi-directional network.

ACKNOWLEDGMENT

The authors would like to thank the Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, for acknowledging and supporting this research work.

REFERENCES

[1] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, ''Secure and trustable electronic medical records sharing using blockchain,'' in *Proc. AMIA Annu. Symp.*, Washington, DC, USA, 2017, pp. 650–659.

[2] B. Koteska, E. Karafiloski, and A. Mishev, ''Blockchain implementation quality challenges: A literature review,'' presented at the Proc. SQAMIA 6th Workshop Softw. Quality, Anal., Monitor., Improvement, Appl., Belgrade, Serbia, 2017.

[3] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, ''Internet of things security: A top-down survey,'' *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018. Accessed: Sep. 16, 2019, doi: 10.1016/j.comnet.2018.03.012.

[4] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, ''Everything You wanted to know about the blockchain: Its promise, components, processes, and problems,'' *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, Jul. 2018. Accessed: Sep. 16, 2019, doi: 10.1109/MCE.2018.2816299.

[5] E. Gökalp, M. O. Gökalp, S. Çoban, and P. E. Eren, ''Analysing opportunities and challenges of integrated blockchain technologies in healthcare,'' presented at the Euro Symp. Syst. Anal. Design, Gdansk, Poland, vol. 333, 2018, pp. 174–183.

[6] J. Park, S. Park, K. Kim, and D. Lee, ''CORUS: Blockchain-based trustworthy evaluation system for efficacy of healthcare remedies,'' in *Proc. IEEE Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Dec. 2018, pp. 181–184.

[7] K. Subbiah and M. Hinojales, *The Age of Blockchain: A Collection of Articles*. New York, NY, USA, IndraStra Open Access, 2018, pp. 2–27, Accessed: Sep. 16, 2019, doi: 10.5281/zenodo.1202390.

[8] D. Macrinici, C. Cartofeanu, and S. Gao, ''Smart contract applications within blockchain technology: A systematic mapping study,'' *Telematics Informat.*, vol. 35, no. 8, pp. 2337–2354, 2018. Accessed: Sep. 16, 2019, doi: 10.1016/j.tele.2018.10.004.

[9] I. Radanović and R. Likić, ''Opportunities for use of blockchain technology in medicine,'' *Appl. Health Economics Health Policy*, vol. 16, no. 5, pp. 583–590, Jul. 2018. Accessed: Sep. 16, 2019, doi: 10.1007/s40258-018-0412-8.

[10] J. H. Mosakheil, ''Security threats classification in blockchains,'' M.S. thesis, Dept. Graduate Fac., St. Cloud State Univ., St. Cloud, MN, USA, 2018. Accessed: Sep. 16, 2019. [Online]. Available: http://repository.stcloudstate.edu/msia_etds/48

[11] L. A. Linn and M. B. Koo, ''Blockchain for health data and its potential use in health IT and health care related research,'' in *Proc. ONC/NIST Blockchain Healthcare Res. Workshop (ONC/NIST)*, Gaithersburg, MD, USA, 2016, pp. 1–10.

[12] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, ''FHIRChain: Applying blockchain to securely and scalably share clinical data,'' *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, Mar. 2018. Accessed: Sep. 16, 2019, doi: 10.1016/j.csbj.2018.07.004.

[13] R. Prakash, ''Adoption of block-chain to enable the scalability and adoption of accountable care,'' presented at the NIST Workshop Blockchain Healthcare, Gaithersburg, MD, USA, Aug. 2016, pp. 1–7.

[14] S. Shetty, X. Liang, D. Bowden, J. Zhao, and L. Zhang, ''Blockchain-based decentralized accountability and self-sovereignty in healthcare systems,'' in *Business Transformation through Blockchain, Palgrave Macmillan*, Cham, Switzerland: Springer, 2018, doi: 10.1007/978-3-319-99058-3_5.

[15] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, ''Blockchain in healthcare applications: Research challenges and opportunities,'' *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, Jun. 2019. Accessed: Sep. 16, 2019, doi: 10.1016/j.jnca.2019.02.027.

[16] Medium.com. (2018). *International IT company TMA Solutions Announces Partnership with OriginTrail*. Accessed: Sep. 16, 2019. [Online]. Available: https://medium.com/origintrail/international-it-company-tma-solutions-announces-partnership-with-origintrail-fe2a312a2f95

[17] T. T. Kuo, H.-E. Kim, and L. Ohno-Machado, ''Blockchain distributed ledger technologies for biomedical and health care applications,'' *J. Amer. Med. Inform. Assoc.*, vol. 24, no. 6, pp. 1211–1220, Nov. 2017. Accessed: Sep. 16, 2019, doi: 10.1093/jamia/ocx068.

[18] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, ''Integrating blockchain for data sharing and collaboration in mobile healthcare applications,'' in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Bologna, Italy, Sep. 2017, pp. 1–5.

[19] E. Meinert, A. Alturkistani, K. A. Foley, T. Osama, and J. Car, ''Blockchain implementation in health care: Protocol for a systematic review,'' *JMIR Res. Protocols*, vol. 8, no. 2, 2019, Art. no. e10994. Accessed: Sep. 16, 2019, doi: 10.2196/10994.

[20] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, ''Blockchain technology use cases in healthcare,'' in *Adv. Comput.*, vol. 111, pp. 1–41, Jun. 2018. Accessed: Sep. 16, 2019, doi: 10.1016/bs.adcom.2018.03.006.

[21] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, ''Applying software patterns to address interoperability in blockchain-based healthcare apps,'' in *Proc. 24th Pattern Lang. Program. Conf.*, Vancouver, QC, Canada, Jun. 2017, pp. 1–17.

[22] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, ''Blockchain technology innovations,'' in *Proc. IEEE Technol. Eng. Manage. Conf. (TEMSCON)*, Silicon Valley, CA, USA, Jun. 2017, pp. 137–141.

[23] W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao, ''A survey of blockchain applications in different domains,'' in *Proc. Int. Conf. Blockchain Technol. Appl.*, Xi'an, China, 2018, pp. 17–21.

[24] X. Liang, S. Shetty, and D. Tosh, ''Exploring the attack surfaces in blockchain enabled smart cities,'' presented at the IEEE Int. Smart Cities Conf., Kansas City, MO, USA, Sep. 2018, doi: 10.1109/ISC2.2018.8656852.

[25] T. T. Kuo and L. Ohno-Machado, ''ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks,'' 2018, *arXiv:1802.01746*. [Online]. Available: https://arxiv.org/abs/1802.01746

[26] T. T. Kuo, H. Z. Rojas, and L. Ohno-Machado, ''Comparison of blockchain platforms: A systematic review and healthcare examples,'' *J. Amer. Med. Inform. Assoc.*, vol. 26, no. 5, pp. 462–478, 2019. Accessed: Sep. 16, 2019, doi: 10.1093/jamia/ocy185.

[27] A. I. Sanka and R. C. C. Cheung, ''Efficient high performance FPGA based NoSQL caching system for blockchain scalability and throughput improvement,'' in *Proc. 26th Int. Conf. Syst. Eng. (ICSEng)*, Sydney, NSW, Australia, Dec. 2018, pp. 1–8.

[28] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019. Accessed: Sep. 16, 2019, doi: 10.1109/ACCESS.2019.2903554.
[29] A. P. Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of blockchain technology," *Math. Found. Comput.*, vol. 1, no. 2, pp. 121–147, 2018. Accessed on Sep. 16, 2019, doi: 10.3934/mfc.2018007.
[30] O. O. , "Donoghue, A. A. Vazirani, D. Brindley, and E. Meinert, "Design choices and trade-offs in health care blockchain implementations: Systematic review," *J. Med. Internet Res.*, vol. 21, no. 5, 2019, Art. no. e12426. Accessed: Sep. 16, 2019, doi: 10.2196/12426.
[31] S. Angraal, H. M. Krumholz, and W. L. Schulz, "Blockchain technology: Applications in health care," *Circulat., Cardiovascular Qual. Outcomes*, vol. 10, no. 9, 2017, Art. no. e003800. Accessed: Sep. 16, 2019, doi: 10.1161/CIRCOUTCOMES.117.003800.
[32] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, p. 56, 2019. Accessed on Sep. 16, 2019, doi: 10.3390/healthcare7020056.
[33] D. M. E.-D. M. Hussein, M. H. N. Taha, and N. E. M. Khalifa, "A blockchain technology evolution between business process management (BPM) and Internet-of-Things (IoT)," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 8, pp. 442–450, 2018. Accessed: Sep. 16, 2019, doi: 10.14569/IJACSA.2018.090856.
[34] E. Y. Chang, S.-W. Liao, C.-T. Liu, W.-C. Lin, P.-W. Liao, W.-K. Fu, C.-H. Mei, and E. J. Chang, "DeepLinQ: Distributed multi-layer ledgers for privacy-preserving data sharing," presented at the IEEE Int. Conf. Artif. Intell. Virtual Reality, Taichung, Taiwan, 2019, pp. 173–178.
[35] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*. Cheltenham, U.K.: Edward Elgar, 2016. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660
[36] J. D. Bruce,*The Mini-Blockchain Scheme*. White paper. 2., Jul. 2014. [Online]. Available: https://cryptonite.info/files/mbc-scheme-rev3.pdf
[37] J. van den Hooff, N. Zeldovich, and M. F. Kaashoek, "VerSum: Verifiable computations over large public logs," in *Proc. 2014 ACM SIGSAC Conf. Comput. Commun. Secur.*, Scottsdale, AZ, USA, 2014, pp. 1304–1316.
[38] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records," *J. Biomed. Inform.*, vol. 71, pp. 70–81, Jul. 2017. Accessed: Sep. 16, 2019, doi: 10.1016/j.jbi.2017.05.012.
[39] Zilliqa. (2017). *The ZILLIQA Technical Whitepaper*. The ZILLIQA Team, Version 0.1. Accessed: Aug. 2017. [Online]. Available: https://docs.zilliqa.com/whitepaper.pdf
[40] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A Sybil-resistant scalable blockchain," *Future Gener. Comput. Syst.*, vol. 29, no. 5, pp. 333–335, 2017. Accessed: Sep. 16, 2019, doi: 10.1016/j.future.2017.08.048.
[41] J. Poon and T. Dryja. *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. Version 0.5.9.2. Accessed: Jan. 14, 2016. [Online]. Available: https://lightning.network/lightning-network-paper.pdf

AHMAD AKMALUDDIN MAZLAN was born in Tangkak, Johor, Malaysia, in 1992. He received the B.S. and M.S. degrees in computer science majoring in information security and assurance and artificial intelligence from the Universiti Sains Islam Malaysia (USIM), Negeri Sembilan, in 2015 and 2018, respectively. He is currently pursuing the Ph.D. degree with the Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia. His research areas are focusing on artificial intelligence, blockchain, big data, and the IoT.

SALWANI MOHD DAUD (Member, IEEE) received the B.Eng. degree (Hons.) in electronics engineering from the University of Liverpool, in 1984, the M.Eng. degree in electrical engineering, in 1989, and the Ph.D. degree in electrical engineering from Universiti Teknologi Malaysia, in 2006. She is currently a Professor of the Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia (UTM). She is also a Registered Professional Technologist from the Malaysia Board of Technologists (MBOT) and a Registered Graduate Engineer with the Board of Engineers Malaysia (BEM). She has been with UTM for more than 30 years and has vast experience in teaching and research. Her research areas are focusing on artificial intelligence, blockchain, and the IoT. She is currently teaching machine learning and system design for security for postgraduate program. She is also leading few research grants in the related topics and had secured more than RM2 millions of R&D funds. She also has published more than 100 academic articles in journal, proceedings and books. She is also the Head of the Cyber Physical Systems Research Group.

SURIANI MOHD SAM (Member, IEEE) received the Ph.D. degree from the Univerisiti Teknologi Malaysia, in 2013. She currently serves as a Senior Lecturer with the Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia. She has been in the research field of networking particularly in quality-of-service (Qos) for several years. These includes in the field of data communication, wireless communication, and telecommunication. The IoT elements have become the main concern in her students' projects and research. She has authored or coauthored journals, conference articles, and book chapters in the field of QoS for several types of communication networking strategies. She is also a member of the Cyber Physical Systems Research Group, UTM, and the IEEE Society.

HAFIZA ABAS received the B.Sc. degree (Hons.) in information technology from Universiti Utara Malaysia, the M.Sc. degree in information technology from Universiti Putra Malaysia (UPM), and the Ph.D. degree in information science from Universiti Kebangsaan Malaysia (UKM). She serves as an Academic Staff with the Universiti Teknologi Malaysia (UTM), Kuala Lumpur, for more than 20 years. She is currently a Senior Lecturer with the Razak Faculty of Technology and Informatics, UTM. Her perseverance permits her to grasp 28 research grants awarded by various agencies. She shines in emotional intelligence, social, and soft skills. Academically, she endures collaborating with academic scholars from various universities. At the same time, she has also published and present articles in local and international conferences. To sustain her role as an Academic Scholar, she is currently involved in a few professional associations. She has obtained research and other awards related to writing and publishing articles.

SITI ZALEHA ABDUL RASID received the B.Sc., M.B.A., and Ph.D. degrees. She is currently an Associate Professor in accounting with the Azman Hashim International Business School, Universiti Teknologi Malaysia (UTM), Kuala Lumpur. She also served as a Research Panelist with the Center of Excellence, Chartered Institute of Management Accountant (CIMA), Southeast Asia. She is actively involved in research activities and has led nine research projects and a member of many research projects. She has authored or coauthored more than 100 articles and research articles in journals, conference proceedings, and technical reports. Her research interests are in management accounting, risk management, corporate governance, and blockchain technology. She is also an Associate Member of the Malaysian Institute of Accountant and a member of the British Accounting and Finance Association. She is also the Associate Chair of the School of Postgraduate Studies, UTM.

MUHAMMAD FATHI YUSOF is currently a Research Fellow (Law and Constitution) and a Senior Lecturer with the Perdana Science, Technology and Innovation Policy Centre, Faculty of Technology and Informatics Razak, Universiti Teknologi Malaysia (UTM), Kuala Lumpur. He is also the Deputy Director of the Islamic Centre, UTM. His research areas are in constitutional law, law and policy, electoral systems, Islamic law, and cyber law. He is also leading research on policy for blockchains technology and a special government taskforce to enhance the function of state legislative assembly. He had headed many research projects in various themes, including on electoral systems, integrity in project management, and policy on disaster management.