

Improving blockchain security for the internet of things: challenges and solutions

Mohammed Al-Shabi¹, Abdulrahman Al-Qarafi²

¹Department of Management Information System, College of Business Administration, Taibah University, Medina, Saudi Arabia

²Department of Information System, College of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia

Article Info

Article history:

Received Nov 6, 2021

Revised May 26, 2022

Accepted Jun 25, 2022

Keywords:

Blockchain

Computer architecture

Internet of things

Security

Threats and attacks

ABSTRACT

Due to its uniquely suited to the knowledge era, the blockchain technology has currently become highly appealing to the next generation. In addition, such technology has been recently extended to the internet of things (IoT). In essence, the blockchain concept necessitates the use of a decentralized data operation system to store as well as to distribute data and the transactions across the net. Therefore, this study examines the specific concept of the blockchain as a decentralized data management system in the face of probable protection threats. Furthermore, it discusses the present solutions that can be used to counteract those attacks. The blockchain security enhancement solutions are included in this study by summarizing the key points of these solutions. Several blockchain systems and safety devices that register security defenselessness can be developed using such key points. At last, this paper discusses the pending matters and the outlook research paths of blockchain-IoT systems.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Mohammed Al-Shabi

Department of Management Information System, College of Business Administration, Taibah University
Madinah, Saudi Arabia

Email: mshaby@taibahu.edu.sa; malshabi@gmail.com

1. INTRODUCTION

Because of its decentralized nature, blockchain technology has been very popular and successful in continuously maintaining information records. Such technology is a form of a distributed digital ledger. The most essential aspect of the blockchain technology is that the data is completely protected with the blocks of the blockchain dealings. Further, several reputable organizations are currently striving to ensure the interoperability, the confidentiality, and the safety of the internet of things (IoT) networks [1]. Ferrag *et al.* [2] conducted a given comparison concerning several privacy as well as security approaches for the applications of the fog-based IoT wherein high privacy-preserving schemes were suggested. Dwivedi *et al.* [3] suggested a new plan to change the blockchain paradigms in the medical field. Likewise, further privacy and security features are included in the proposed scheme, which supported the developed cryptographic primitives. It employs trivial digital signatures to ensure that the data would not be incorrectly changed. Besides, it also makes use of a tamper-proof seal to protect such information. In literature, the techniques of privacy-preserving for the IoT data in connected cities have been explained. Support vector machine training, in particular, has been used in conjunction with the technology of blockchain for the purpose of managing the digital city data [4]. In reality, the blockchain methods allow data providers to exchange IoT data in such safe and trustworthy ways. This is since each supplier utilizes its private key for encrypting the data case in a particular location. Security is becoming increasingly important, with the ever-increasing movement toward various desirable properties like decentralization, auditability, insistence, and anonymity. In the survey, the

implementation of blockchain technology within an enormous selection of applications is discussed along with the associated challenges [5].

Figure 1 shows the timeline for a variety of researches concerning blockchain network between 2016 and 2021. Dorri *et al.* [6] discussed the confidentiality and the protection concerns of the internet of things, as well as the defenselessness. A given blockchain-based solution was presented by them as well. Moreover, Li *et al.* [7] reviewed the problems of blockchain protection and the related obstacles under several sorts of threats and attacks. Another blockchain use cases such as Bitcoin, hyper ledger, and Ethereum were briefly explored too. Reyna *et al.* [8] investigated blockchain, focusing on the analysis of the features and the related issues as the blockchain and the internet of things are combined by various analysis techniques and identification. Besides, the involved implementations which support blockchain-IoT were mentioned as well. Despite the fact that Reyna *et al.* have suggested a solution, it is noted that there is insufficient research on the topic of integrity attacks [8]. Salman *et al.* [9] demonstrated blockchain-based systems for resource provenance, secrecy, creditability, and safety assurance, among other protection services. In addition to this, they highlighted a number of issues and obstacles related to blockchain-based protection services, as well as demonstrated insights into present methodologies and implementations' security services [9]. Taylor *et al.* [10] conducted a comprehensive literature review about blockchain cybersecurity; they presented major quantitative and qualitative information. They also highlighted the outlook research paths in blockchain for internet of things protection and computational data security. The confidentiality-preserving properties in blockchain based IoT systems were described by Hassan *et al.* [11].

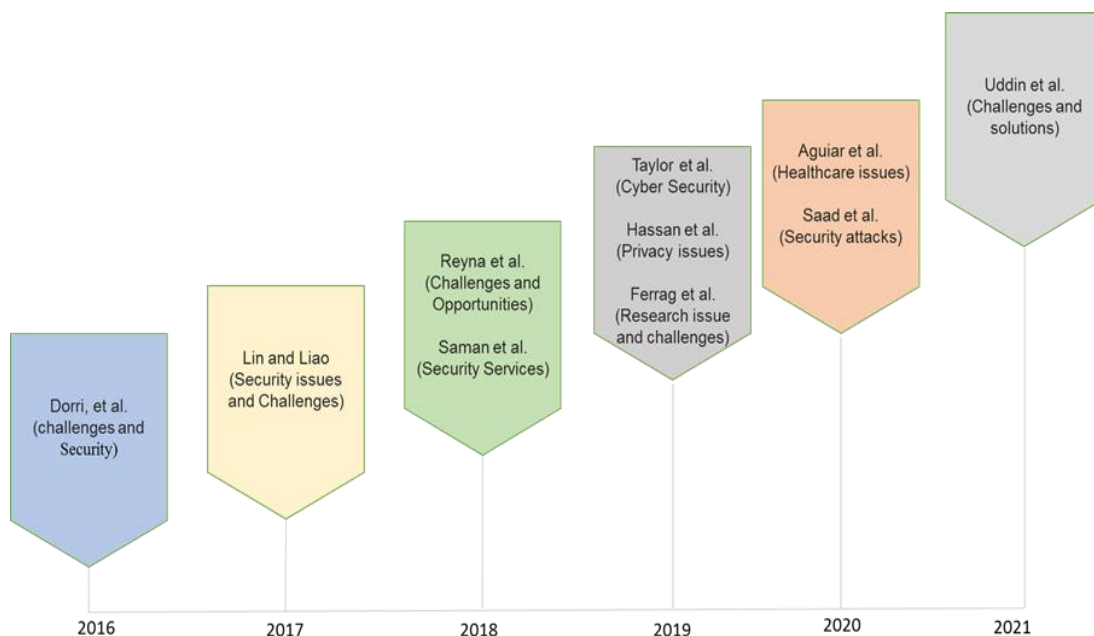


Figure 1. Chart of various literature about protection challenges, attacks, and solutions in blockchain technology from 2016 to 2021

The authors presented the serious challenges that confidentiality leak can cause in IoT managing systems, as well as examined the application of secrecy protection. Furthermore, a number of challenges related to the latter were discussed as well. Ferrag *et al.* [2] illustrated various blockchain IoT implementation scopes, including, internet of events (IoE), internet of content (IoC), edge computing, and number of others. Moreover, They examined the bitcoin system's confidentiality and anonymity; a taxonomy as well as a comparison of state-of-the-art secrecy-preserving blockchain technology were also demonstrated [2]. Aguiar *et al.* [12] conducted a study on blockchain-based techniques of medical implementations. They tested the technologies that the sectors utilized in order to build blockchain networks. Likewise, they presented the confidentiality methods and entrance control utilized in medical services registers involving case situations in order to check patients in remote consideration conditions. In a systematic manner, Saad *et al.* [13] investigated the attack surface regarding blockchain cryptography development, appropriated design and blockchain implementation setting, yet at the same time, presenting itemized solutions and prospects.

The key contributions of the paper can be highlighted as: i) this paper examines the necessary knowledge about the blockchain technology, including its features, participants, and constituents, as well as their own roles, so that the readers become familiar with such technology; ii) this study presents the prevalent security attacks that the blockchain networks are facing and their vulnerabilities, as well as support the outcomes of many current researches. Besides, various applications and opportunities involved in numerous implementations and prospects of blockchain are highlighted discussed too; and iii) this review discusses current solutions for protection for the blockchain network in a variety of environments. Finally, some protection techniques which are able to address the security defenselessness are mentioned in this survey. The latter also identifies few pending matters, research problems, and needs that could help the systems of the blockchain-IoT to develop their capabilities.

The rest of this survey is arranged in the following manner. Blockchain and its associated factors are clarified in the second part. A detailed discussion on blockchain security issues and the challenges is presented in section 3. Further, section 4 overviews the various blockchain solutions to the related obstacles in several fields. Finally, the section 5 concludes with a discussion of unresolved difficulties and possible future research options.

2. BLOCKCHAIN FACTORS AND ISSUES

In this section, the security concerns, and benefits of blockchain elements, such as decentralization, will be discussed, which pose major challenges for data privacy and transparency, as well as confusion in the network. Furthermore, the open-source and anonymous nature of the system allows for flexible configuration, transaction confidentiality, and privacy. Also, will discuss the security concerns of blockchain participants and components, as well as current solutions and proposals.

2.1. Blockchain elements and concerns

2.1.1. Decentralization

In blockchain innovation, decentralization involves scattering capacities all through a framework rather than having all units associated with a focal power, implying the absence of the main control point. In fact, the lack of the central authority within the blockchain is the characteristic that made it safer than others [14]. In the blockchain, each user, who is named as miner as well, is allocated a unique transaction account, which is used to add blocks when the users are approved. The decentralized manner which characterized the info registers used in blockchain presented its progressive quality in that the blockchain networks utilize consensus procedures for the purpose of obtaining the nodes [15]. Based on that, the exchanges are confirmed, and the information would not be erased. Because the decentralized structure of this technology permits peers activities, it additionally presents significant obstacles in the face of private data confidentiality. In view of the same, Zyskind *et al.* [16] studied decentralized individual data operation within private data secrecy worries.

2.1.2. Consensus model

The term "consensus" indicates a group of people who agree on something. The consensus patterns aid the decentralized technologies to take agreed decisions. This permits all registers to come across a only one authority. In reality, the consensus algorithms are needed by the blockchain in order to ensure that each subsequent block is the solely authentic version. In other words, the algorithms will confirm the agreement of each node that every new block which will be added to the blockchain holds the same content [17]. Consensus paradigms ensure that fork attacks do not occur and may preserve against malignant threats as well. The following are the three major characteristics of the consensus model: i) this model is both secure and harmonious while the whole nodes output the same result; ii) the consensus mechanism ensures aliveness assuming the whole taking part nodes have output an outcome, and iii) this given protocol provides fault tolerance so that regaining from the node fails.

2.1.3. Transparency and confidentiality

The most attractive aspect of the blockchain network is, in fact, the offered privacy degree. Whereas this may cause some ambiguity in terms of translucence. The blockchain nets conduct frequent self-auditing's of the digital significance ecosystems which range the exchanges; a collection of the latter is known as a block. Corruption is being impossible as well as the translucence are two features that result from this operation. The blockchain network is already regarded as a strong technology since a powerful cipher is used so that to hide the miner's personal information. This technology arranges the interactions in a particular manner which highly enhances accuracy yet removing as well the political and financial threats that are associated with centrally managed operations. Hence, the need for trust is fundamentally decreased. The

platforms that may concurrently manage various implementations from various organizations, empowering effective conversation are created by the blockchain networks [18], [19].

2.2. Blockchain participants and related concern

In computer and blockchain systems, a consensus mechanism is a fault-tolerant technique that is used to obtain the required consensus on a single data value or a single state of the network across distributed processes or multi-agent systems, such as with cryptocurrencies. The miners in the blockchain technologies are enabled to reach consensus; in addition to storing the data which is accessible by all participants. In the following, functions of blockchain network users are discussed [20].

2.2.1. Blockchain miners

In accord with blockchain.info, the number of blockchain miners has raised at an exponential rate from 2011. The number of miners is predicted to arrive to fifty million in 2020, according to these statistics. Based on that, a confidentiality challenge faces the miners within this technology [21].

2.2.2. Blockchain regulators

There is a need of an extensive access into ledger contents so that gaining full control over the business nets. Besides, a detailed analysis concerning the current regulatory area of allocation technologies is carried out by Kakavand *et al.* [22]. Moreover, Yeoh presented the managing challenges surrounding the blockchain [4]. He outlined the major managing obstacles associated with the new spread blockchain network in both the US as well as Europe.

2.2.3. Blockchain developer

The applications and smart contracts that blockchain users utilize are both created by developers. Developers have a variety of opportunities to earn profit by using cryptography to guarantee the accuracy of the ledgers that enable cryptocurrencies. This developer creates the contracts as well as the applications and that the miners utilized. Nordrum [5] presented a timeframe to the developers of blockchain and he explained that the software materials available to them in order to create safe ledgers of blockchain are restricted.

2.2.4. Certificate authority

It runs the diverse certificates that are required for the aim of managing given permissioned blockchain such as Ethereum and Bitcoin; this is with the help of a trustworthy third party. Further, the restricted collection of legal writers or readers is licensed by the authority. However, it is worth mentioning that the trust is the most important problem in the blockchain technologies. In order to solve trust issues, the blockchains are distributing the ledgers through multiple servers controlled by distinct authorities. However, a given bootstrapping issue associated with finding initial ledgers is remained [23].

3. PROPOSED MODEL-IMPROVING BLOCKCHAIN SECURITY FOR IoT: CHALLENGES

3.1. Blockchain security challenges

Transaction Malleability: In the contracted exchanges, the information included in the given hash transactions is not all instantly covered by the agreements. Thus, it is uncommon yet not impossible, that a node change a given transaction within the network in a given manner without the validation of the hash. Furthermore, the transaction malleability, as explained by Wang and Su. [24] is while the exchanges are replayed and altered; this let the exchange entity suppose that the former exchange could not be assured.

3.1.1. Network protection

A given assault takes place at the time an adversary is taking control of parts of a network's communication and splitting it reasonably so that to expand the synchronization retard [25]. The refusal of service assault, for instance, can be utilized for enhancing both boost spending and mining. The attacker in these attacks picks out and covers data of some or many users, which may be possible by the retardation of the block's submission to the given node.

3.1.2. Privacy

Both secrecy and privacy remain major interests for the blockchain exchanges because every node may get the information from the other one. In addition, all the exchanges would be viewed by any person who is seeing the blockchain. Many researches in literature have proposed several solutions to succeed in facing this issue [26]. However, such solutions are only suited to specific implementations, yet they are not able to overcome all of these challenges. Because of the huge amount of knowledge transitions, such hacker

assaults like man-in-the-middle attacks (MITM) as well as a denial-of-service (DoS)/a distributed denial-of-service (DoS/DDoS) can attack the conversations including significant information within the net. Improving the IoT systems presents several distinctive confidentiality issues, including information secrecy as well as pursuit worries for both telephones and vehicles. Recognizing the voice has been incorporated permitting the devices of focusing on conversations while actively transmitting the information into the cloud storage [27].

3.1.3. Expensive redundancy

Although permitting every node in the network to have a copy of every exchange can eliminate the arbitration, it is worth mentioning that such duplication in transactions is monetarily as well as legitimately unreasonable [28]. In view of the same, banks do not appear to be eager to carry out all the transactions within each bank or rather to finish the exchanges of another ones. That recurrence just raises the expenses, yet it does not provide any practical advantages.

3.1.4. Criminal activity

Miners are capable of purchasing and selling a wide range of items thanks to the Bitcoin-enabled third-party exchanging sites. Because such operations are unknown, tracing the miner activity and imposing legal penalties is hard and challenging. Further, concealing, black business sectors, and also ransomware are common instances of criminal activities employing bitcoin. A few underground stores which run online exchange like Tor covered service are utilizing bitcoin which lets the accessibility of the blockchain becomes unsure because of the criminal acts [2].

3.1.5. Vulnerabilities in smart contracts

At the time a given platform is carried out in the blockchain, such smart network will have protection defenselessness due to a program's fault. It has been determined that the amount of about 8,833 from 19,366 of smart contracts of Ethereum are susceptible to bugs which includes exchange requesting dependence, maltreated exemptions and reentrancy defenselessness as well. Atzei *et al.* [29] suggested a scientific categorization of defenselessness as well as classified the various sorts of vulnerabilities into three stages which are the blockchain, rigidity, and Ethereum virtual machine. Moreover, the defenselessness gives rise to network problems within codifying, protection, confidentiality as well as the performance of the program involving the scalability of the blockchain.

3.2. Other challenges

3.2.1. Ambiguous terminology

Because of the restricted skill pool accessible for blockchain, both real and comprehend requirements of administrative organizations for industry specialists so that to explain this technology as well as other associated worries have expanded [3]. Those specific requirements and all of the likely results of fake threat analysis, as well as its leaning to under regulate, highly raise the chance of capture via the organizers. Actually, both names distributed ledger technology (DLT) and blockchain are much more perplexing. Thus, there is an absence of technical comprehension among authorities, users, and business companies.

3.2.2. Risk of adoption

Even though there are predicted economic advantages, the adoption and application expenses of DLT/blockchain of current activities can speedily become fundamental. This can be often mostly valid for the present users with IT platforms or the written procedures so that to fit the existing criteria, that may needs expensive redesigns [30]. The operational expenses related to the adopting DLT/blockchain are still ambiguous. In a short period of time, particular back-office procedures cannot be simply extracted or substituted with the DLT/blockchain solution. Therefore, the industry users have to keep in mind these three quick activities are: i) assessing the business effect and making long-term plans, ii) distinguishing and catching interior open doors, and iii) carrying out post-exchange as well as manual processes.

3.2.3. Economic impact

It is not always clear whether the blockchain is outperforming centralization in connection with execution, scalability, rate of transfer, protection, or confidentiality. In addition, DTL also has to overcome obstacles such as excessive exchange expenses, economic scaling, as well as prolonged check periods. Further, until a signal of concept is tested, there is doubt regarding the use cases that are applicable and practical [31]. If the DTL/blockchain is not greatly used, considering the wide economic influences on the medium in long term would likely be difficult. Thus, there are three specific areas which need additional examination are: i) expenses and motives of the organization, ii) the environment of marketplace (in which manner cryptocurrencies are littered with competition and request), and iii) operations of decision-making.

4. PROPOSED MODEL-IMPROVING BLOCKCHAIN SECURITY FOR IoT: SOLUTIONS

4.1. Security vulnerability and tools

Smart contract of the blockchain provide secrecy and protection. Their flaws, however, have to be fully comprehended. This section discusses some protection equipment's so that to supply the frame of data required for constructing safe blockchain platform. Since decentralization is one of blockchain characteristics, it has a long history of stability, which has attracted companies to implement it in their business operations, notably in Internet of Things. Moreover, the main protection challenge with IoT is to determine and take control of the users who are connecting on large platforms with no violation of confidentiality laws [32].

In terms of design, the blockchain network is regarded as secure. In actual situations, however, built-in implementations may be susceptible as well. The contracts, for example, are impacted monetarily by a variety of unpleasant situations as well as threats. A given reentrant issue with split decentralized autonomous organization (DAO) led to losing of almost forty million dollars during June 2016. Besides, in 2017, attackers took about thirty-two million dollars. Those excessive professional cases are able to make the platform gravely susceptible for the attackers so that exploiting the safety bugs of given networks.

4.2. Blockchain for privacy and security

Privacy and confidentiality are still pressing issues with blockchain transactions because each node may access data from another node, and anyone viewing the blockchain can see all transactions. The present solutions for blockchain in literature for confidentiality as well as safety are summarized in Table 1. These solutions for blockchain are studies by researchers based on the Basic theory, attributes, and other characteristics of privacy and security. They review the restrictions on these solutions with suggested scheme for these issues.

4.3. Blockchain-IoT privacy preserving approach

The privacy preservation of the blockchain includes the anonymity of users and the confidentiality of the content. The solutions for the current blockchain in literature of confidentiality-preserving are summarized in Table 2. The table also presents the solutions privacy preservation in blockchain in studies based on basic theory, attributes, and other features and limitations of privacy and security.

Table 1. Blockchain for confidentiality and protection

Source	Suggested scheme	Basic theory	Attributes	Other characteristics	Restrictions
Gai <i>et al.</i> [33]	Summarized the obstacles associated with safety and confidentiality of the blockchain	Case studies for validation and recommendation	Privacy, security, efficiency, effectiveness	Optimum tractability	Absence of blockchain instruments distributes as well as permits
Kshetri [34]	Comparison between blockchain and cloud for secrecy and protection	Determine the advantages and disadvantages of cloud versus blockchain	Integrity, efficiency, confidentiality, safety	Smaller storage needed for the blockchain than the cloud	-
Singh <i>et al.</i> [35]	Secure as well as efficiency smart home architecture based on the blockchain and cloud computing	Processing exchange and the analysis of protection in smart contracts	Privacy, security, secrecy, solidity, scalability	Irregularity packet detection, rise rate of transfer, minimal latency	Managing restricted safety threats and long periods of performance

Table 2. The blockchain for confidentiality preserving scheme

Source	Proposed scheme	Basic theory	attributes	Other features	limitations
Liu <i>et al.</i> [36]	Blockchain-based site secrecy- preserving crowd-comprehending system	Preserve the employee's place as well as rise the success average of the allocated work	Preserve re-identification location privacy	Efficiency, security	Transmitted information can be malignant factor, quality assessment issue
Kuo <i>et al.</i> [37]	Confidentiality-preserving paradigm position in the blockchain on a network of contracts	Implementing of hierarchical privacy preserving model; on the blockchain as well as valuing it on 3 medical genomic datasets	Improve predictive decision support system	Learning iteration, redox, excitation time	Topology, evaluating huge amount of information forward confidentiality denounces
Gai <i>et al.</i> [38]	Energy exchanging with miner's secrecy utilizing the blockchain in smart net	Differential privacy, neighboring energy trading privacy preserving	Efficiency, user's privacy	-	-
Kouicem <i>et al.</i> [39]	Position confidentiality approach relied on blockchain	Location based- K-anonymity	Efficiency, user's security	Good response duration as well as scalability execution raised	More stability with regard to the snapshot theory

4.4. Some examples related to attack solutions

4.4.1. Liveness attack

Li *et al.* [40] suggested the consensus record of conflux which effectively encrypts two distinct block generation methodologies for the purpose of fighting the dynamic attack. The first strategy is based on an optimal solution which permits speedy affirmation. Furthermore, the second strategy employs a moderate solution which ensures the consensus' s advance. Conflux may be a decentralized and an expandable framework with rise throughput as well as quick affirmation inside the blockchain network [15]. It joins the two methodologies into an incorporated consensus protocol with the help of an adaptive weight technique.

4.4.2. DAO attack

Decentralized autonomous organizations (DAOs) have been used as venture capital funds for crypto and distributed. The DAO was hacked due to vulnerabilities in its code base. The DAO insider attack on the RPL internet of things net was demonstrated by Ghaleb *et al.* [41] in order to relieve the given attack, the authors have proposed a novel strategy based on trials conducted with the Contiki instrument, which is a less-strength created device for the insufficient resource tools.

4.4.3. BGP hijacking attack

The BGPCoin program which was suggested by Xing *et al.* [42] could be a reliable blockchain-based resource solution. The platform improves the smart grid for the aim of implementing as well as supervising resource tasks on mood renitent Ethereum blockchain. On the blockchain of Ethereum as well as smart network programming, the BGPCoin program offers a reliable solution of border gateway protocol (BGP) protection.

4.4.4. Sybil attack

A Sybil attack is a type of online security threat in which a single person attempts to take control of a network by generating many accounts, nodes, or computers. Swathi *et al.* [43] suggested a strategy to restrict Sybil attacks in the blockchain platforms. This is through observing the attitude of other nodes as well as identifying the nodes which can be advancing the blocks of a specific miner [43].

4.5. Some countermeasures

This passage presents the current blockchain-based networks countermeasures and finding out algorithms which would be used so that to confirm confidentiality and protection. In order to provide extensive outline, this report examined some of the present studies as well as references from systematic databases in the net. The following passage present a resume of the latest solutions that are used in blockchain settings. Such solutions address the safety threats and supply strong privacy.

4.5.1. Quantitative framework

- a. Application: the quantitative method can be divided into two parts. The simulator of the blockchain is the first section, while the protection paradigm schema is the second. The stimulator behaves like the activities of the blockchain networks. As a result, the input parameters are both the grid and the consensus record [44].
- b. Impact: for the purpose of testing the attacks, the quantitative regulation generates a high fundamental procedure. As a result, the system aids in the building the blockchain network's security.

4.5.2. Lightning network

- a. Application: the exchange receipts that are dual signed are produced by the lightning grid. The exchange is alleged to be adequate after the engaged sides have signed the transaction just for acknowledging the novel check [45].
- b. Impact: such lightning net aids two persons to manage the exchanges between them with no obstruction from an outsider user. The pair signing guarantees the exchange safety for both concerned sides.

4.5.3. Integration of blockchain with artificial intelligence

- a. Application: artificial intelligence (AI) is the process of creating a machine which is capable of doing works that requires intellect.
- b. Impact: the protection staff may use machine learning in order to discover unusual acts with the grid and discomfit the assaults on the platform [45].

4.5.4. Town crier

- a. Application: the crier performs by way of regaining information from customers as well as gathering data from hypertext transfer protocol (HTTP) websites [45]. An accurately remarkable message of the blockchain reached the customer network through the crier.
- b. Impact: while demanding information from given customers, the announcer serves safety. A neighborhood interviewer or town crier provides intense protection that can be a solid example for the smart network of blockchain.

4.5.5. Segwit

- a. Application: a Segwit can be defined as a quality of the side chain which works alongside with the foremost blockchain grid [46]. Besides, the information Signature are shifted to the prolonged side chain from the initial blockchain network.
- b. Impact: utilizing the side chain leads to freeing further space of the blockchain as well as allowing for extra transactions to be performed. Moreover, by the order of the Merkel tree, the signature data is put in an equivalent part of the blockchain. Based on such position, the total size of the block ending has raised with no obstruction with size of the block. Further, the diversity of data enhances the network protection.

4.5.6. Tendermint

Blocking is a notion introduced by Tendermint; where protection is given through a modulated conciliation protocol with supported share guarantee. Within the Tendermint consensus procedure, every block ought to be signed by the certifiers in a cryptographic manner. The latter are users who ensure their concerns to the system safety through shutting their own funding depending on the help of a bonding exchange [47].

5. OPEN ISSUES FOR FUTURE STUDIES

The adoption of blockchain in various academic and commercial domains now offers numerous research opportunities. However, like with any new technology, there are issues and challenges. In this passage, some pending matters as well as the obstacles of future studies are reported to complete the survey.

5.1. Vulnerability

The blockchain networks are vulnerable regardless of providing a strong process to IoT protection. The consensus technique that is founded on the mix strength of the user has vanished, for that reason permitting the attackers to huddle the blockchain. In a similar way, attackers can be able to compromise accounts of the blockchain using specific keys with restricted fortuitousness. The miners must realize powerful techniques to guarantee the secrecy of transaction and obviate aggressive assaults, which ends up in double spending.

5.2. Flexibility against combined assault

Numerous protection arrangements and implementations have been presented as well as suggested for IoT of blockchain. Besides, every one of them has been intended to deal with specific safety problems and risks. The major investigation includes fostering a system which can be flexible contra several combined assaults while taking into account the execution feasibility of such suggested arrangements.

5.3. Policies for zero-day assaults

A zero-day assault can be defined as a software unit mechanism which happens while there is an absence of the countermeasure's contra such defenselessness. It is hard to expect the probability of these assaults, and each apparatus is able to be compromised by the same. In the development period, the majority of the associated dubious acts are identified. Some of the latter, however, are identified when examining the processes. The liabilities must be declaimed by a protection spot when defenselessness is being exploited. Furthermore, the varied Markov model can be described by utilizing an assault diagram which combines time-subordinate covariant so that to expect zero-day assaults.

5.4. Blockchain particular infrastructure

Saving information on the database of blockchain means storing them on the grid's IoT nodes which cannot be omitted. This implies that data is forced upon the user's nodes, which forces great expenses on the decentralized grid. In particular, one ought to comprehend that storage restricted IoT equipment's might not save huge blockchains which develop like blocks are included. Likewise, IoT apparatuses store information on such blockchains which are not beneficial for their exchanges. Subsequently, determining the tools which

upholds the divided storage of enormous scope blockchain-particular blockchains turns out to be without a doubt a troublesome issue. Moreover, addressing administration as well as fundamental protocols have substantial functions inside the base of blockchain. Mainly, the accuracy among the instruments with plentiful resources of computing should be instituted inside the blockchain. Moreover, the implementation programming mediator must be a kind miner.

5.5. Security requirements

The blockchain can monitor the data collected by the sensors for IoT safety, preventing it from being duplicated by incorrect data. By taking into account blockchain-IoT, considering particular situations that intend to ease the protection parameters, assault countermeasures, trust, and confidentiality is absolutely so essential. The IoT of blockchain should fulfill specific security needs, which are outlined in the following:

5.5.1. Secure key exchange

This is regarded like a crucial function in order to protect during the whole of communications in a given cryptographic process. It is a network pier for assault prohibition. It must be ensured that a key have to be safely shared across the networks.

5.5.2. Resource-exhausted assault resilient

Resource exhaustion assaults are protection exploitation of the intended framework or grid which must be avoided. The assault can be taken advantage of through extreme key process, or whilst multiple exchanges take place inside the network. Such attacks have the potential to shut down the entire network.

5.5.3. Resource utilization

Using power as well as memory can extend the operation's period. In a blockchain exchange framework, the new grid design may effectively use the resources for each role. Other facilities such as fog/osmotic computing, aspect-crowd modeling, as well as other distributed concepts enhance protection and resource utilization.

5.5.4. Performance trade-off

Excepting the need of cryptographic for expanding safety and competence, the user must not neglect or compromise the framework's execution and manage the application throughout simultaneous process. Ideally, it is desirable to make all the features of the collected data private, but due to the system performance goals (efficiency and accuracy), resource limitations or the potential negative impact on data utility. It is not always possible as doing so may affect the performance of the whole system.

5.5.5. Insider threat management

It restrains risk, conflict, revealing, and supervising of the workers. Besides, there is a need for non-compromising patterns to identify and restrain false alerts in the blockchain sides. Insider threats are one of today's most challenging cybersecurity issues that is not well addressed by commonly employed security solutions.

5.6. Pending questions

- a. How many blockchains are needed to safeguard the internet of things milieu?
- b. What are the vulnerabilities of smart network, and how do smart grids react to the altered conditions of IoT milieu?
- c. In which situations may blockchain be utilized in IoT grids?
- d. In the coming age of quantum computing, how secure will blockchain framework be?
- e. How would the problem of latency in the creation of block within blockchain and cryptographic operations be treated with no compromising secrecy?

6. CONCLUSION

The blockchain technology causes a revolution on the IoT sector. Such technology has the potential to bring firms, ministries, as well as even countries together. Because of its decentralized structure, it is well-known and highly regarded. Many blockchain assaults, associated protection problems, and actual instances were reported in this review. Furthermore, the latter demonstrated many security problems, obstacles, weaknesses, and assaults which block the expanded blockchain adoption from multiple sides. It additionally clarified different blockchain implementations and advantages and mentioned several associated Chances. To conclude, it outlined the present solutions for various milieus and pending research problems.




REFERENCES

- [1] R. de Best, "Number of Blockchain wallet users worldwide from November 2011 to February 7, 2022(in millions)," *Statista*, 2022.
- [2] M. A. Ferrag, A. Derhab, L. Maglaras, M. Mukherjee, and H. Janicke, "Privacy-preserving schemes for Fog-based IoT applications: threat models, solutions, and challenges," in *2018 International Conference on Smart Communications in Network Technologies (SaCoNeT)*, Oct. 2018, pp. 37–42., doi: 10.1109/SaCoNeT.2018.8585538.
- [3] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors (Switzerland)*, vol. 19, no. 2, pp. 1–17, 2019, doi: 10.3390/s19020326.
- [4] P. Yeoh, "Regulatory issues in blockchain technology," *Journal of Financial Regulation and Compliance*, vol. 25, no. 2, pp. 196–208, May 2017, doi: 10.1108/JFRC-08-2016-0068.
- [5] A. Nordrum, "Is it time to become a blockchain developer? [Resources_Careers]," *IEEE Spectrum*, vol. 54, no. 9, Sep. 2017, doi: 10.1109/MSPEC.2017.8012232.
- [6] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," *arXiv preprint arXiv:1608.05187*, Aug. 2016.
- [7] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, no. 5, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020.
- [8] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/j.future.2018.05.046.
- [9] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: a state of the art survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 858–880, 2019, doi: 10.1109/COMST.2018.2863956.
- [10] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 147–156, May 2020, doi: 10.1016/j.dcan.2019.01.005.
- [11] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, vol. 97, pp. 512–529, Aug. 2019, doi: 10.1016/j.future.2019.02.060.
- [12] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Computing Surveys*, vol. 53, no. 2, pp. 1–27, 2020, doi: 10.1145/3376915.
- [13] M. Saad *et al.*, "Exploring the attack surface of blockchain: a systematic overview," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1977–2008, Apr. 2019, doi: 10.1109/COMST.2020.2975999.
- [14] M. Anderson, "Exploring decentralization: blockchain technology and complex coordination," *Journal of Design and Science*, 2019.
- [15] Y. Maleh, M. Shojafar, M. Alazab, and I. Romdhani, *Blockchain for cybersecurity and privacy: architectures, challenges, and applications*. CRC Press, 2020., doi: 10.1201/9780429324932.
- [16] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, May 2015, pp. 180–184., doi: 10.1109/SPW.2015.27.
- [17] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, 2018, doi: 10.1504/IJWGS.2018.095647.
- [18] M. Maroufi, R. Abdolee, and B. M. Tazekand, "On the convergence of blockchain and internet of things (IoT) technologies," *Journal of Strategic Innovation and Sustainability*, vol. 14, no. 1, Mar. 2019, doi: 10.33423/jsis.v14i1.990.
- [19] S. B. ElMamy, H. Mrabet, H. Gharbi, A. Jemai, and D. Trentesaux, "A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0," *Sustainability*, vol. 12, no. 21, Nov. 2020, doi: 10.3390/su12219179.
- [20] B. Bordel, R. Alcarria, D. Martin, and Á. Sánchez-Picot, "Trust provision in the internet of things using transversal blockchain networks," *Intelligent Automation and Soft Computing*, vol. 25, no. 1, pp. 155–170, 2018, doi: 10.31209/2018.100000052.
- [21] R. Kumar, M. F. Tahir, S. Kumar, A. Zia, H. Memon, and W. Mahmood, "Challenges in adoption of blockchain in developing countries," in *2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST)*, Dec. 2019, pp. 1–8., doi: 10.1109/ICEEST48626.2019.8981674.
- [22] H. Kakavand, N. K. De Sevres, and B. Chilton, "The blockchain revolution: an analysis of regulation and technology related to distributed ledger technologies," *SSRN Electronic Journal*, 2017, doi: 10.2139/ssrn.2849251.
- [23] Y. Tang *et al.*, "ChainFS: blockchain-secured cloud storage," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018, pp. 987–990.
- [24] W. Wang and C. Su, "CCBRN: a system with high embedding capacity for covert communication in Bitcoin," in *IFIP Advances in Information and Communication Technology*, vol. 580 IFIP, Springer, 2020, pp. 324–337, doi: 10.1007/978-3-030-58201-2_22.
- [25] Z. Lejun *et al.*, "A covert communication method using special bitcoin addresses generated by vanitygen," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 597–616, 2020, doi: 10.32604/cmc.2020.011554.
- [26] S. Li, F. Liu, J. Liang, Z. Cai, and Z. Liang, "Optimization of face recognition system based on azure IoT edge," *Computers, Materials & Continua*, vol. 61, no. 3, pp. 1377–1389, 2019, doi: 10.32604/cmc.2019.06402.
- [27] D.-Y. Kim, S. D. Min, and S. Kim, "A DPN (delegated proof of node) mechanism for secure data transmission in IoT services," *Computers, Materials and Continua*, vol. 60, no. 1, pp. 1–14, 2019, doi: 10.32604/cmc.2019.06102.
- [28] L. Xu, C. Xu, Z. Liu, Y. Wang, and J. Wang, "Enabling comparable search over encrypted data for IoT with privacy-preserving," *Computers, Materials & Continua*, vol. 60, no. 2, pp. 675–690, 2019, doi: 10.32604/cmc.2019.05276.
- [29] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (SoK)," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10204, Springer, 2017, pp. 164–186, doi: 10.1007/978-3-662-54455-6_8.
- [30] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7702–7712, Oct. 2019, doi: 10.1109/JIOT.2019.2901840.
- [31] IBM, "What is Block Storage?," IBM, 2019. <https://www.ibm.com/cloud/learn/block-storage> (accessed Jun. 24, 2019).
- [32] R. Li, Q. Wang, Q. Wang, D. MGalindo, and M. Ryan, "SoK: TEE-assisted confidential smart contract," *arXiv preprint arXiv:2203.08548*, 2022.
- [33] K. Gai, M. Qiu, X. Sun, and H. Zhao, "Security and privacy issues: a survey on FinTech," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10135, Springer, 2017, pp. 236–247., doi: 10.1007/978-3-319-52015-5_24.




- [34] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, Nov. 2017, doi: 10.1016/j.telpol.2017.09.003.
- [35] S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: a secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology," *International Journal of Distributed Sensor Networks*, vol. 15, no. 4, Apr. 2019, doi: 10.1177/1550147719844159.
- [36] Y. Liu, J. E. Fieldsend, and G. Min, "A framework of fog computing: architecture, challenges, and optimization," *IEEE Access*, vol. 5, pp. 25445–25454, 2017, doi: 10.1109/ACCESS.2017.2766923.
- [37] T.-T. Kuo, J. Kim, and R. A. Gabriel, "Privacy-preserving model learning on a blockchain network-of-networks," *Journal of the American Medical Informatics Association*, vol. 27, no. 3, pp. 343–354, Mar. 2020, doi: 10.1093/jamia/ocz214.
- [38] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019, doi: 10.1109/TII.2019.2893433.
- [39] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: a top-down survey," *Computer Networks*, vol. 141, pp. 199–221, 2018.
- [40] C. Li *et al.*, "A decentralized blockchain with high throughput and fast confirmation," in *Proceedings of the 2020 USENIX Annual Technical Conference*, 2020, pp. 515–528.
- [41] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, "Addressing the DAO insider attack in RPL's internet of things networks," *IEEE Communications Letters*, vol. 23, no. 1, pp. 68–71, Jan. 2019, doi: 10.1109/LCOMM.2018.2878151.
- [42] Q. Xing, B. Wang, and X. Wang, "Poster: Bgpcoin: a trustworthy blockchain-based resource management solution for bgp security," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2017, pp. 2591–2593., doi: 10.1145/3133956.3138828.
- [43] P. Swathi, C. Modi, and D. Patel, "Preventing sybil attack in blockchain using distributed behavior monitoring of miners," in *2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019*, 2019, pp. 1–6., doi: 10.1109/ICCCNT45670.2019.8944507.
- [44] E.-R. Latifa, E. K. My Ahemed, E. G. Mohamed, and A. Omar, "Blockchain: bitcoin wallet cryptography security, challenges and countermeasures," *Journal of Internet Banking and Commerce*, vol. 22, no. 3, pp. 1–29, 2017.
- [45] F. Idelberger, G. Governatori, R. Riveret, and G. Sartor, "Evaluation of logic-based smart contracts for blockchain systems," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9718, Springer, 2016, pp. 167–183., doi: 10.1007/978-3-319-42019-6_11.
- [46] A. Kiayias, "Speed-security tradeoffs in blockchain protocols," *CiteseerCryptology ePrint Archive*, pp. 1–19, 2015.
- [47] J. Kwon, "TenderMint: consensus without mining," Draft v. 0.6, fall 1, no. 11, 2014.

BIOGRAPHIES OF AUTHORS



Mohammed Al-Shabi    received his bachelor's degree (B.Sc. Computer Science) from Technology University at Iraq (1997), Postgraduate Master (M.Sc. Computer Science) from Putra Malaysia University at 2002), and Ph.D. (Computer Science) from Putra Malaysia University, Malaysia (2006). He is currently an associate professor in the Department of Management Information System, College of Business Administration at Taibah University, Kingdom of Saudi Arabia. Prior to joining Taibah University, he worked in the faculty of a computer at Qassim University, Saudi Arabia. His research interests include wireless security, cryptography, UML, stenography multistage interconnection network, vehicular ad-hoc network-cloud, smart and intelligent computing and apply mathematically. He can be contacted at email: mshaby@taibahu.edu.sa.



Abdulrahman Al-Qarafi    received his bachelor's degree (B.Sc. Information System) from Taibah University (2011), Postgraduate Master from University of Manchester in the UK (2015), and Ph.D. (Computer Science) from University of Stirling in the UK. Currently, he is an assistant professor in the College of Computer Science and Engineering (Information System Department) at Taibah university. His research interests include artificial intelligence, machine learning algorithms, and the use of big data in blockchain technologies. He can be contacted at email: asalqarafi@taibahu.edu.sa.