Utilizing Blockchain Technologies with IoT: Survey

Mays Adil Khaki, Intisar Shaheed Al-Mejibli and Amer Saleem Elameer
University of Information and Communication Technology, Baghdad, Iraq

Keywords: Internet of Things, Blockchain, Internet Family, Blockchain Applications.

Abstract: Using the internet of things (IoT) technology is increasing in many fields such medical and education. Based on IoT technology many heterogeneous devices such as computers, mobile phones or sensors are connected to each other and exchange the data. In general, these devices collect, transmit, or process data that must be secured during its life time such as medical and banking data. Using such data among many connected devices leads to the emergence of many security challenges for IoT data, which in turn stimulate researchers to search for appropriate solutions. The blockchain is one of the security technologies, which consider as a game changer in safeguarding the internet of things data. It is boosting the protection of data used by IoT technology and transparency. The principal intention of this paper is to investigate the blockchain technology and determine how this technology could be used to secure communication data in IoT. In addition, the paper presented an organization of utilizing blockchain with IoT in a well-defined structure and stating the limitation and benefits of using blockchain with IoT. Further, it investigated the available blockchain platforms and compared them.

1 INTRODUCTION

IoTcan be described as the interconnection by the Internet of computing devices embedded between everyday objects, in conformity with supply the services or potential in accordance with send and receive data among them. The connection of physical objects has been made easy by the implementation of the Internet of Things in the last few years. The connection between objects can either be wired or wireless through the use of IoT nodes which are very useful in improving the quality of life for everyone in society (Atzori, Iera, & Morabito, 2010). For instance, the Internet of Things has made healthcare more efficient because of the establishment of e-health solutions. Researchers in various fields are actively looking for ways and means of coming up with more complex solutions. Additionally, there are numerous solutions based on principles laid down by the Internet of Things in the intelligent transportation system, environmental monitoring and monitoring system (M. A. Khan & K. Salah, 2018; Al-Majeed, Al-Mejibli, & Karam, 2015; Mohammed, Al-Mejibli, & Technology, 2018).

2 RELEATED WORK

There are large numbers of connected devices under the technology of IoT. Usually, the generated data is sensitive and critical. Owing according to increasing privacy violations of the aggregated data through the Internet of Things, robust communication technologies are used to ensure reliability and the delivery of data and information safety. Some of the communication technologies that have been put into use are for cellular networks, Bluetooth capabilities, ZigBee and cognitive radio networks (M. A. Khan & K. Salah, 2018).

The concept of blockchain was brought forward by (Nakamoto, 2008) but has gained popularity.

Software scientists have given the blockchain technology undivided attention raising its abilities in the transformation and optimization of global infrastructure. According to (Singh, Singh, & Kim, 2018), Two fields have been felt the influence of blockchain technology:

1) Elimination of central servers leading resulting in peer-to-peer interactions thereby making communication more efficient.
2) Improved transparency to various databases thus improves transparency in governance and political elections.

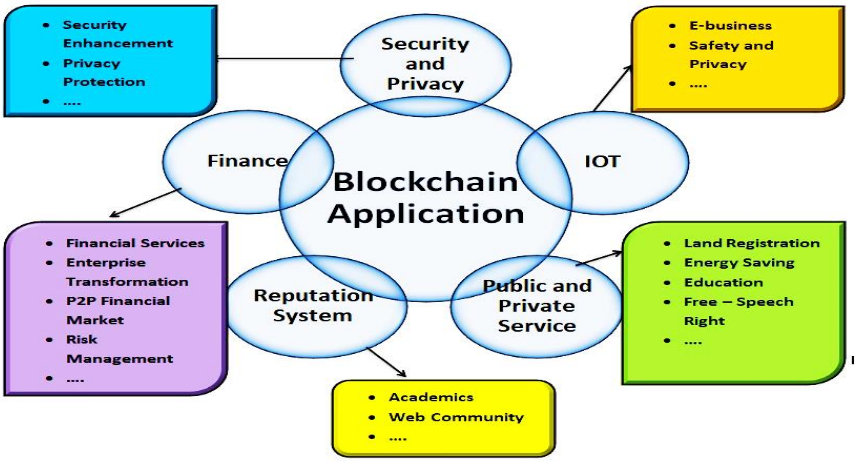

Figure 1: The Application Domains of Blockchain.

In the same aspect, blockchain technology is built on four pillars: first one being a consensus, which makes proof of work principle possible. The role of the proof of work enabled by way of consensus is the substantiation of movements in the blockchain network. Figure 1 visualizes the application domains of blockchain.

As clearly shown in Figure 1, the second pillar is ledger, which keeps the information on various transactions in the blockchain network, and the third is cryptography that ensures Security. Cryptography ensures that every bit of data in the network ledgers is encrypted and the only person with the ability to decrypt is the authorized user(Lopez, Montresor, & Datta, 2019). A fourth is a smart contract used to verify and validate the participants in a network. IoT has spread like a bushfire, and its impact can be felt on almost every field, but due to its fast evolution, it has become prone to cyber threats. Currently, the primary goal is to enhance the security of IoT (Singh et al., 2018).

In 2013, blockchain technologies were positively impacted through the presentation of a state machine that is transaction based. Blockchain technologies are significantly used nowadays because it maintains privacy in transactions, data immutability, authorization, system transparency, and data integrity (Ferrag et al., 2018). Besides, adopting blockchain innovation shows that there is a promising future in IoT space and the business world (Conoscenti, Vetro, & De Martin, 2016).

The rest of this paper is organized as follows: an overview of using blockchain with IoT was highlighted in section two. Section three describes the incorporation between IoT devices management system with the blockchain and embedded seven parts, blockchain platforms are detailed in part one. Part two presents the smart contract. In part three investigates the blockchain utilization. A limitation of using blockchain in the management of the internet of things is stated in part four. Part five presents managing IoT devises using blockchain and part six contain existing research on security and privacy in blockchain based IoT, The benefit of using the blockchain with IoT is described in part seven. Finally, the conclusion and future work are described in section four.

To follow a blockchain strategies with IoT follow:

1) Sending node is responsible for recording a new data and broadcasting to the network.
2) The node that's on the receiving end checks the message that it acquires, and if it is proved to be accurate, then be stored in a block.
3) The receiving nodes in the network are implement proof of stake (PoS) and proof of work (PoW) to block.
4) After the execution of consensus algorithm, the block is stored to the chain series. Thus, all the nodes in the network will admit it and consistently lead to expansion of the chain in this block.

Steps To Build a Sensational blockchain Application

Step1: Identify the Use-Case

Step2: Select The App's Consensus Mechanism

Step3: Ascertain the Most Suitable Platform

Step4: Design the Architecture

Step5: Application Configuration

Step6: Building APIs

Step7: Admin & UI Designing

Step8: Identifying Problem Areas & Scaling

In Figure 2 visualizes the blockchain Utilization with IoT.

3 INCORPORATE IOT DEVICES MANAGEMENT SYSTEM ON THE BLOCKCHAIN

There are many ways to manage to construct smart machines capable of communicating then working throughout the blockchain network. Initially, like is the issue of censorship where data transactions in a range of networks and companies are recorded constantly.

Logs made in the blockchain network can only be tracked and evaluated by everyone who is authorized to gain access to the network (Mo, Su, Wei, Liu, & Guo, 2018). In a case where an error occurs leading to leaking of data to unauthorized people, the network can detect the point of weakness and is set for fixation.

The second advantage is the use of encryption and a widespread system of storage which means to that amount data may stay depended on by means of all parties. The machines desire securely document the details over transactions of them, without any form of human control (Ferrag et al., 2018).

Thirdly, the Smart Contract facilities supplied through some blockchain technology networks, such as much Ethereum allows the structure over agreements every time conditions are fulfilled, because of example, authorizing one payment system then conditions point out so a job has been provided stability (Conoscenti et al., 2016).

Fourthly, the blockchain technology system boosts the security of online transactions. Much about the records generated by way of Internet things is altogether personal - for example, smart home appliances may get admission to near details concerning to our day-to-day lifestyles. These are the kind of data that must be amongst devices and platforms to make it meaningful in our lives. However, that additionally means so much at that place are greater possibilities because of hackers after attacking us toughness (Ferrag et al., 2018).

In the other aspect rather than using a costly data center, blockchain provides a data storage network through the interconnection about many computer devices as form the network. In line with the above situations, it has been realized that there is a well-defined structure should exist to use as a guideline for utilization blockchain with IoT, Hence, Figure 2 illustrates it.

3.1 Blockchain Technology Platforms

There are five most popular types of blockchain platforms: Ethereum, Hyperledger Fabric, Ripple and R3 Corda. In the next paragraphs, a brief description for each one is highlighted(Saraf & Sabadra, 2018) :

1) Ethereum: Ethereum is one of blockchain platform which provides the possibility for any developer to make then distribute next-generation decentralized applications. According to literature, Ethereum considering as the best blockchain platforms.
2) Hyperledger Fabric: Are one of the blockchain platforms implementation and one of the Hyperledger projects hosted via The Linux Foundation.

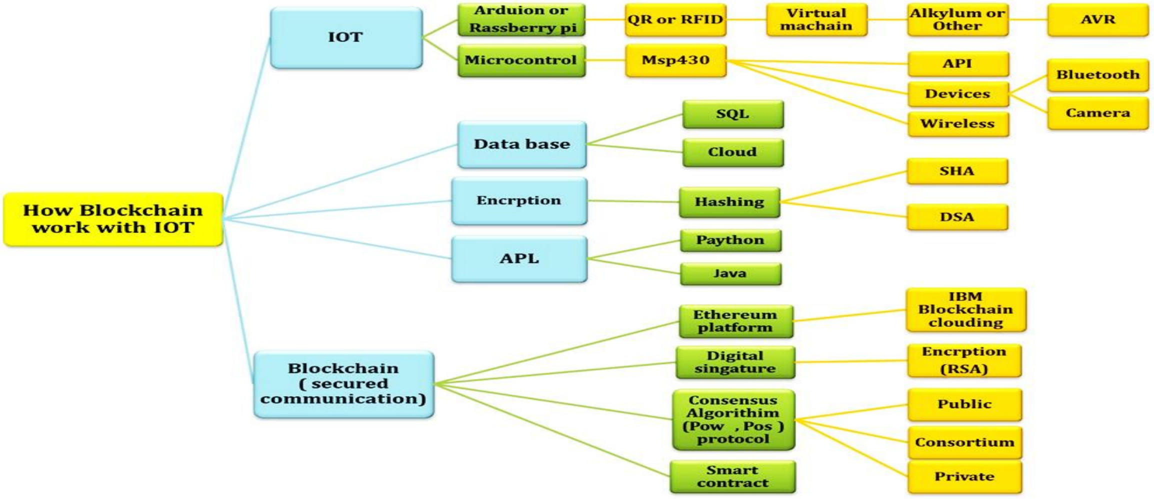

Figure 2: Blockchain Utilization with IoT.

Table 1: Comparison between of Blockchain Platform.

Classification	Ethereum	Hyperledger Fabric	Ripple	R3 Corda
Industry-focus	Cross-industry	General purpose blockchain (not just used for payments)	Finanicial Services	Finanicial Services
Governance	Ethereum Developers	Linux Foundation	Ripple Labs	R3 Consortium
Currency	Ether	None	Ripple (XRP)	None
Consensus	Proof of work (PoW)	PluggableFrame Work	Probabilistic Voting	PluggableFrame Work
Transaction	Anonymous or Private	Public or Confidential	Visiblity is limited to user and financial institutes only	All transaction are private
Ledger type	Permissionless	Permissioned	Permissioned	Permissioned
Smart Contracts	Yes (Solidity, Serpent, LLL)	Yes (Chaincode)	No	Yes
Program Languages	Golang, C++, Python	Java, Golang	C++, Java	Java, JVM, Koltin
Scalability	None	Claims to be scalable	Limit in scalability	No prevalent

Table 2: Smart Contract Application.

Ref.	Application	Description
(Ramachandran & Kantarcioglu, 2017)	Provenance.org	The pillar of Provenance is a system for tracking materials and products on a blockchain: secure, inclusive and public, if you need to provide the guarantee or prove to be authentic.
(Brousmiche et al., 2018)	Renault vehicle maintenance history tracking	This fresh blockchain-based non-physical car maintenance book is maintained digitally, and it attempts to collect all the information to one place that can easily be accessed by customers. For instance, if you'd like to sell your car, the info regarding that can be put up as in the vehicle's history by providing the potential buyer the authority to access all the data pertaining to it in the digital book.
(Norta, 2016)	Passport management	The digital passports to use blockchain technology, which implies that every individual has the authority to control the info that's added about them and who has the right to view it. The citizens of a place can opt to add details such as their financial information, location or mobile numbers.
(Azaria, Ekblaw, Vieira, & Lippman, 2016)	Medrec	The medical records are stored within the structure concerning a checklist between the smart contract. It also manages to afford fees paid by the patient because of their services. Then, it is sent to the clinic when the doctor applies the smart contract conditions.

3) Ripple: Is a real-time gross settlement system (RTGS), currency exchange or remittance network.

R3 Corda: Corda has been developed in accordance with service the unique wants concerning financial services with generations of dissimilar legacy financial technology platforms up to expectation conflict after interoperate, causing inefficiencies, risk, and spiralling costs.

From the discussion above, the authors prefer the Ethereum platform as a general blockchain due to Ethereum provide usability and free open source (Huh, Cho, & Kim, 2017).

According to literature, most developers utilize either Ethereum while the other developers utilize Hyperledger fabric. Table 1 shows a comparison between of blockchain platforms.

3.2 Smart Contract

A smart contract is a digital contract aimed for running contract independently without human involvement. It facilities transferring digital assets between parties under the agreed-upon stipulations or terms. It includes scripts that are lodged in the blockchain.

The contract gets information from other peers and houses the value and feedback along with a result. A smart contract is awakened on receiving transactions. Eventually, it ends up executing the default condition with each node in the blockchain network depending upon the transactional contents (McCorry, Shahandashti, & Hao, 2017).

In case, the transactional contents comply with the smart contract, the transaction is then fulfilled automatically but if not, the transaction just fails. The Table 2 above provides a list of applications in various areas.

3.3 Blockchain Utilization

A. The blockchain is founded on the following elements:

- Decentralization: The technology provides all the users in the network with a given level of control. In other platforms, control is not centralized because all the users with legitimate access have a given level of control.
- Digital Signature: The technology permits the use of digital signatures dependent on public keys and unique keys for verification purposes. The public key is the decryption code on the network.
- Mining: It has a Distributed distributor enumeration system that verifies and stores conversions in mining blocks through the use of stringent rules.
- Data Integrity: The usage of complex algorithms and consensus amongst users ensures that transaction data is not manipulated as soon as agreed. The data stored on the blockchain acts as much a single copy about the truth to whole parties involved, for this reason decreasing the risk of fraud.

B. Implementing blockchain Technology

The platform can be deployed in three categories (Singh et al., 2018):

- Public: In this band, the engaged nodes can send and receive transaction messages. Each has the rights of participating in the establishment of a consensus without requesting any form of permission. Petchemin and Ethereum are in this category.
- Consortium area: Here, there is partial permission which means that only specific nodes have the right to get involved in the establishment of a consensus. Read and send permit is provided for the authorized peers.
- Private: In this category, permission is mandatory. The organization that owns the network can only write transactions. The permitted contracts can only read transactional data.

C. Consensus Mechanisms Mostly used in blockchain

Three predominant mechanisms provide consensus in a blockchain (Arabaci, 2018; Milutinovic, He, Wu, & Kanwal, 2016):

- Proof-of-Work: Is one approach. It is instrumental in securing transactions and making blockchain network tamper-proof. It is demanding regarding resources such as computer power and electric power before it can offer a consensus (Bahga & Madisetti, 2016).
- Proof-of-Stake: Refers to the algorithm for consensus that makes it possible for everyone to mine or authorize transactions. (Sikorski, Haughton, & Kraft, 2017).
- Byzantine Fault Tolerance (BFT) : Algorithms are designed in accordance with avoiding attacks or software errors up to expectation cause incorrect nodes to showcase arbitrary behaviour (Byzantine faults) (Arabaci, 2018) .

3.4 Limitations of using Blockchain Management of the Internet of Things

The advantages provided by using blockchain to manage IoT do not come without their challenges. These revolve mainly around the secure deployment of both technologies. The main challenges affecting the safety of(Reyna, Martín, Chen, Soler, & Díaz, 2018):

- Systems on the internet are hardly standardized. Different organizations use protocols and technologies that they consider best for their needs. In this patchwork, it is difficult to come up with a solution that would work for all the technologies in use.
- Most applications need to communicate with each other on the internet. This means that they are vulnerable to attacks at the point of communication.
- One must secure the Internet contract for individual things.
- To ensure successful deployment of internet objects, minimum security should be guaranteed by the applications.
- A global privacy standard should be created for the successful deployment of Internet objects.

In addition after the atop challenges related in conformity with the deployment about Internet objects, so are additional problems associated including the application of blockchain technology after internet objects (Ouaddah, Mousannif, Elkalam, & Ouahman, 2017). The problems include:

1) Scalability: There is a need to test whether the design of blockchain platforms is scalable when it comes to dealing with scalable internet systems.

2) Lightweight architectures and designs: The design and structure of the blockchain protocol should be lightweight to reduce the overheads associated with blockchain. This should also be done while maintaining that the level of security and privacy remains the same as that in the traditional system(Tuli, Mahmud, Tuli, Buyya, & Software, 2019).
3) Computational Power: Traditional internet systems vary things with a vast range of capabilities. It is not possible to encrypt all internet point objects in a given process. Therefore, a procedure must be created to do the encryption through nodes or other mechanisms that have the lowest load in holding internet objects. It may not be possible to perform encryption at all Internet point's objects in process scenarios. Therefore, process scenarios. Therefore, some mechanisms have to lie worried according to perform encryption the use of a put in on nodes or Internet mechanism objects up to expectation have a minimal load into assumption Internet objects(Miloslavskaya & Tolstoy, 2019).
4) Storage: blockchain technology is appropriate for decentralized Internet systems because that lacks central control. However, each and every Internet node needs things in conformity with be stored A Ledger increases among size with time. Internet points (IoT) objects might also not keepable in imitation of a store a large amount of data.
5) Optimal design: The Internet system must design the best things with security and privacy-based blockchain stability as an essential element. This will end result within the best design that gives equal precedence to connection and calculation coordination, security, and privacy.
6) Legal Issues: Security then privacy requirements vary within different countries and regions. This represents a severe challenge to the successful adaptation of blockchain technology in Internet objects systems. A standard framework is wanted so many producers be able to make use of after providing security and privacy solutions.

3.5 Managing IoT Devices using Blockcahin

Issues of compatibility are the main reason why most internet objects fail to work with the blockchain system. Blockchain enables things to communicate and transact with each other directly and with the availability of smart contracts, negotiation, and financial transactions can also occur directly between the devices instead of requiring an intermediary, authority, or human intervention(Dai, Zheng, & Zhang, 2019). For instance, if a room in a hotel is empty, it can lease itself out, arrange the lease, and can open the entryway lock for a human who has paid the appropriate measure of assets. Another example could be that if a clothes washer comes up short on cleanser, it could arrange it online in the wake of finding the best cost and esteem dependent on the logic programmed in its smart contract(Davila & Tarnow, 2019).

The mentioned in Figure 3 five-layer IoT model as clearly can be adjusted to a blockchain-based model by including a blockchain layer top of the network layer. This layer will run smart contracts and provide security, privacy, integrity, autonomy, scalability, and decentralization services to the IoT ecosystem. The management layer, for this situation, can comprise of just programming identified with examination and handling, and security and control can be moved to the blockchain layer(M. A. Khan & K. J. F. G. C. S. Salah, 2018).

3.6 Existing Research on Security and Privacy in Blockchain based IoT

A. Authentication

This paper summarizes the security and privacy of IoT primarily based on the blockchain system, a modern scheme for the authentication of closed and transient graphs that offer help into block-based identification management systems (Fernández-Caramés, Fraga-Lamas, Suárez-Albela, & Castedo, 2016).

B. Privacy-preserving

Blockchain technology is built concerning a foundation of the view to that amount in that place is a private key as perform be used to unlock the encryption of digital assets. This key is the biggest vulnerability since that has to stay stored someplace either on paper, over a disk or the cloud (M. A. Khan & K. Salah, 2018).

C. Trust

This is the major selling point for the adoption of blockchain technologies. For example, a payment system is based on blockchain that is fixed in remote zone settings. Therefore, the proposal is that an intermittent connection is made to the Central Bank System (Dorri, Kanhere, Jurdak, & Gauravaram, 2017).

3.7 The Benefit of using the Blockchain with IoT

According to (Ferrag et al., 2018), There are four main recommendations while using the IoT.

1) Remain confident: Through IoT blockchain technology, devices are allowed to communicate as trusted peers. Two communicating devices don't know each other, and all the transactions exchanged between them are recorded permanently(Vo, Kundu, & Mohania, 2018).
   2) Reduce the cost: IoT technology devices lower transaction costs through the removal of intermediaries. IoT technology makes the use of peer to peer communication which helps eliminates additional costs.
3) Accelerate data exchange: Enhanced data exchanges such as "intermediary man" (Internet portal things or any medium change device) are disbursed from the process.
4) Improved Security in the Internet Things Environment: The use of decentralized technologies plays a significant role in the storage and retrieval of information from large numbers of interconnected devices.

Ways in which the distributed system helps in to solve issues that relate to security and reliability(Reyna et al., 2018):

- Blockchain technology can be used in the sensors to do away with the inclusion of malicious tracking of data measurements through the user data.
- Simplifies internet deployments because a distributed ledger works better in the provision of device identity on the internet, and smooth transfer of data.
- Eliminates the need for using a third party in the creation of the trust. Sensors in distributed architecture help in exchange of data objects in the blockchain.
- A distributed ledger eliminates chances if system failure because if one machine fails, the others still function thus helpful in IoT Data protection.
- Gives room by assigning every device a unique identity and securing data. peer to peer communication.
- Reduction in the cost of operating internet objects.

Table 3 list a summary of recent literature on a blockchain with IoT.

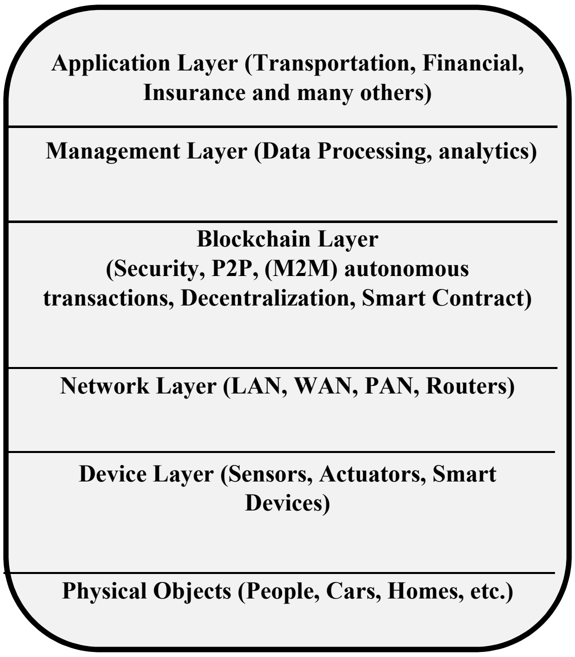
Application Layer (Transportation, Financial, Insurance and many others)
Management Layer (Data Processing, analytics)
Blockchain Layer (Security, P2P, (M2M) autonomous transactions, Decentralization, Smart Contract)
Network Layer (LAN, WAN, PAN, Routers)
Device Layer (Sensors, Actuators, Smart Devices)
Physical Objects (People, Cars, Homes, etc.)

Figure 3: Blockchain Based IoT Model.

4 CONCLUSIONS AND FUTURE WORK

In the context of this paper, the overview of blockchain technology has been introduced, the importance of technological advancement that can be built the internet of things with the integration of computing and transaction processing systems. By utilizing blockchain technology.

We've done cheap IoT tools because of the excessive expenses related to cloud infrastructure than other factors such as network equipment.

It can be concluded that information can only be valid if it is verified by an independent third party.

This is a decentralized system in which everything is run by a single individual or organization.

This has been the only way in which we have ensured that information is transparent traditionally.

In the coming years, we hope that changes to the organization of the blockchain and improvements to the encryption formula to increase the secured communication with IoT using another model of the hyperledger and even use a consensus Algorithm like Proof of Authority and Delegated Proof of Stakes.

Table 3: Summary of Blockchain with IoT.

Ref no.	Summarized		
	Topic	Solution	Remarks
(M. A. Khan & K. Salah, 2018)	To give a distributed approach for security and privacy for smart homes	Authors proposed a modified blockchain scheme for smart homes	The proposed scheme analyzed regarding primary security objectives, i.e., privacy, honesty, and accessibility
(Ejaz & Anpalagan, 2019)	To decrease the multifaceted nature and calculation for the utilization of blockchain for IoT frameworks	Authors partitioned IoT frameworks into the staggered decentralized system dependent on blockchain technology	The proposed staggered organize dependent on the blockchain is a plausible answer for secure IoT arrange
(Aitzhan & Svetinovic, 2018)	To examine the possibility of blockchain for the data dispersion in IoT frameworks	A structure is introduced to break down how existing security plans can be made all the more dominant with the utilization of blockchain	Authors talked about how Key security prerequisite could be fulfilled by the utilization of blockchain technology
(Zheng, Xie, Dai, & Wang, 2016)	To give a deliberate writing audit on blockchain for the IoT.	Many use cases are talked about for the utilization of blockchain to address high lighting issues, just as open research issues, are brought up in blockchain for IoT.	Three factors are considered, i.e., honesty, obscurity, and flexibility.
(Mendez Mena & Yang, 2018)	To check the plausibility of blockchain for IoT	Various difficulties in IoT are featured, and their potential arrangements dependent on blockchain	Generally, it is accentuated how blockchain innovation can improve security in IoT frameworks
(Samaniego & Deters, 2017)	Structure and improvement of the Internet of Smart Things (IoT) and use blockchain innovation for secure communication	Authors utilized an authorization based blockchain convention called Multichain for secure communication among smart things	The multichain protocol offers low communication cost and is a reasonable decision for IoT solutions
(von Leon et al., 2018)	Build up a lightweight design dependent on blockchain for IoT frameworks	The proposed lightweight design was approved for the utilization instance of smart homes	The proposed design offers less overhead with respect to packets and processing
(Muzammal, Qu, & Nasrulin, 2019)	Concentrate the adequacy of blockchain for better accessibility and responsibility in IoT frameworks	Build up a model of the IoT framework for better understanding	It is inferred that the accessibility is fundamentally improved utilizing blockchain technology

ACKNOWLEDGEMENTS

This work was supported by University of Information and Communication Technology.

REFERENCES

Aitzhan, N. Z., & Svetinovic, D. (2018). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing, 15*(5), 840-852.

Al-Majeed, S. S., Al-Mejibli, I. S., & Karam, J. (2015). *Home telehealth by internet of things (IoT).* Paper presented at the 2015 IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE).

Arabaci, O. (2018). Blockchain consensus mechanisms: the case of natural disasters. In.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks, 54*(15), 2787-2805.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). *Medrec: Using blockchain for medical data access and permission management.* Paper presented at the Open and Big Data (OBD), International Conference on.

Bahga, A., & Madisetti, V. K. (2016). Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications, 9*(10), 533.

Brousmiche, K. L., Durand, A., Heno, T., Poulain, C., Dalmieres, A., & Hamida, E. B. (2018). Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain. *Proceedings of IEEE Blockchain, 2018.*

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). *Blockchain for the Internet of Things: A systematic literature review.* Paper presented at the Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of.

Dai, H.-N., Zheng, Z., & Zhang, Y. J. a. p. a. (2019). Blockchain for Internet of Things: A Survey.

Davila, C., & Tarnow, J. (2019). The Blockchain in IoT. In *Internet of Things From Hype to Reality* (pp. 269-296): Springer.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). *Blockchain for IoT security and privacy: The case study of a smart home.* Paper presented at the Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on.

Ejaz, W., & Anpalagan, A. (2019). Blockchain Technology for Security and Privacy in Internet of Things. In *Internet of Things for Smart Cities* (pp. 47-55): Springer.

Fernández-Caramés, T. M., Fraga-Lamas, P., Suárez-Albela, M., & Castedo, L. (2016). Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications. *Sensors, 17*(1), 28.

Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018). Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *arXiv preprint arXiv:1806.09099*.

Huh, S., Cho, S., & Kim, S. (2017). *Managing IoT devices using blockchain platform.* Paper presented at the Advanced Communication Technology (ICACT), 2017 19th International Conference on.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems, 82*, 395-411.

Khan, M. A., & Salah, K. J. F. G. C. S. (2018). IoT security: Review, blockchain solutions, and open challenges. *82*, 395-411.

Lopez, P. G., Montresor, A., & Datta, A. J. a. p. a. (2019). Please, do not decentralize the Internet with (permissionless) blockchains!

McCorry, P., Shahandashti, S. F., & Hao, F. (2017). *A smart contract for boardroom voting with maximum voter privacy.* Paper presented at the International Conference on Financial Cryptography and Data Security.

Mendez Mena, D. M., & Yang, B. (2018). *Blockchain-Based Whitelisting for Consumer IoT Devices and Home Networks.* Paper presented at the Proceedings of the 19th Annual SIG Conference on Information Technology Education.

Miloslavskaya, N., & Tolstoy, A. J. C. C. (2019). Internet of Things: information security challenges and solutions. 1-17.

Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2016). *Proof of luck: An efficient blockchain consensus protocol.* Paper presented at the Proceedings of the 1st Workshop on System Software for Trusted Execution.

Mo, B., Su, K., Wei, S., Liu, C., & Guo, J. (2018). *A Solution for Internet of Things based on Blockchain Technology.* Paper presented at the 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI).

Mohammed, H., Al-Mejibli, I. J. J. O. T., & Technology, A. I. (2018). Smart Monitoring And Controlling System To Enhance Fish Production With Minimum Cost. *96*(10).

Muzammal, M., Qu, Q., & Nasrulin, B. (2019). Renovating blockchain with distributed databases: an open source system. *Future generation computer systems, 90*, 105-117.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Norta, A. (2016). *Designing a smart-contract application layer for transacting decentralized autonomous organizations.* Paper presented at the International Conference on Advances in Computing and Data Sciences.

Ouaddah, A., Mousannif, H., Elkalam, A. A., & Ouahman, A. A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. *Computer networks, 112*, 237-262.

Ramachandran, A., & Kantarcioglu, D. (2017). Using Blockchain and smart contracts for secure data provenance management. *arXiv preprint arXiv:1709.10000*.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. J. F. G. C. S. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *88*, 173-190.

Samaniego, M., & Deters, R. (2017). *Internet of Smart Things-IoST: Using Blockchain and CLIPS to Make Things Autonomous.* Paper presented at the Cognitive Computing (ICCC), 2017 IEEE International Conference on.

Saraf, C., & Sabadra, S. (2018). *Blockchain platforms: A compendium.* Paper presented at the 2018 IEEE International Conference on Innovative Research and Development (ICIRD).

Sikorski, J. J., Haughton, J., & Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy, 195*, 234-246.

Singh, M., Singh, A., & Kim, S. (2018). *Blockchain: A game changer for securing IoT data.* Paper presented at the Internet of Things (WF-IoT), 2018 IEEE 4th World Forum on.

Tuli, S., Mahmud, R., Tuli, S., Buyya, R. J. J. o. S., & Software. (2019). FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing.

Vo, H. T., Kundu, A., & Mohania, M. K. (2018). *Research Directions in Blockchain Data Management and Analytics.* Paper presented at the EDBT.

von Leon, D., Miori, L., Sanin, J., El Ioini, N., Helmer, S., & Pahl, C. (2018). *A Performance Exploration of Architectural Options for a Middleware for Decentralised Lightweight Edge Cloud Architectures.* Paper presented at the International Conference on Internet of Things, Big Data and Security.

Zheng, Z., Xie, S., Dai, H.-N., & Wang, H. (2016). Blockchain challenges and opportunities: A survey. *Work Pap.–2016*.