2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA) | 978-1-6654-9461-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/IICETA51758.2021.9717969

Utilizing Blockchain Technologies with IoT: Review Paper

Mays Adel Khaki
Dept. Computer Science
Iraqi Commission for Computers and Informatics
Informatics Institute for Postgraduate
Baghdad, Iraq
maisalreem92@yahoo.com

Intisar Shaheed Al-Mejibli
University of Information Technology and Communications (UOITC)
Baghdad, Iraq
dr.intisar.almejibli@gmail.com

Amer S. Elameer
University of Information Technology and Communications (UOITC)
Baghdad, Iraq
amerelameer@yahoo.com

***Abstract*—The core aim of the internet of things is providing communication capability between huge numbers of different entities "things". The Abundance feature of connected devices 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. Through its impact, it has made the addition of more devices into the Blockchain ecosystem. Boosting the security of devices used in IoT to accelerate the rate of adoption of Blockchain technology. The main aim of this paper is to investigate the current literature to determine how the management of IoT has become independent and widespread doing away with the need of having to rely on one entity in the storage of data in the new technology, Blockchain assumes the role of a database making it different from the storage methods used in the past. In addition to, the authors have organized the utilization of Blockchain in a well-defined structure. Finally, this paper concluded that by utilization of Blockchain results in improved security and distribution using devices such as sensors which are connected efficiently with the aim of coming up with a secure database which gives rise to lots of business opportunities in the future.**

Keywords—Internet of Things, Security, Blockchain

I. INTRODUCTION AND LITERATURE REVIEW

IoT can be defined as the interconnection via the Internet of computing devices embedded in everyday objects, to provide the facilities and abilities to 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 [1]. 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 and environmental monitoring [2].

There are large numbers of devices that use the Internet of Things to help in the generation of extensive data on the internet. Data generated by IoT is sensitive and critical. Owing to the large amount of data passed over the Internet of Things devices, robust communication technologies are used to ensure reliability and the delivery of data and information. Some of the communication technologies that have been put into use are cellular networks, Bluetooth capabilities, ZigBee and cognitive radio networks [3].

The concept of Blockchain was brought forward by [4] 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 [5], 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.

In the same aspect. Blockchain technology is built on four principles with the first one being a consensus which makes proof of work principle possible. The role of the proof of work enabled by consensus is the verification of actions in the Blockchain network. Fig. 1 visualizes the application domains of Blockchain.

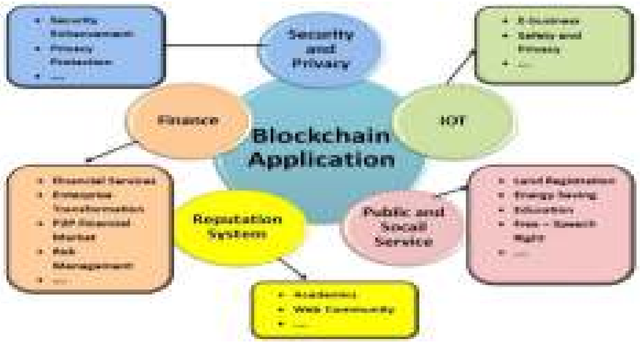

Fig. 1. The Application Domains of Blockchain

As clearly shown in Fig. 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. A fourth pillar 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 [5].

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. It is important to note that Blockchain technology is widely applied in various sectors besides cryptocurrencies [2]. Besides, adopting Blockchain innovation shows that there is a promising future in IoT space and the business world [6]. Owing to its significant impact on society, the primary goal of this paper is to offer full guidance on the use of technology. Case examples are used throughout the document to ensure that security and trust are fully developed.

In the rest of this paper, an overview of existing Blockchain application was highlighted, followed by how in incorporate IoT devices management system on the Blockchain, also Blockchain utilization, Blockchain platforms. Finally, the limitations of using Blockchain in the management of the internet of things

II. THE EXISTING BLOCKCHAIN APPLICATIONS

To achieve a well-designed Blockchain application, three steps need to follow:

A. New Frontier in Data Exchange Framework

Blockchain technology offers help to IoT devices facilitate the exchange of data. Companies and business organization have the choice of using Blockchain to extract data from asset-based devices or the quick response code (QR Code). Devices that can use the internet help in searching through Blockchain records to either update of validating transactions. For instance, an IoT device connected to the Blockchain is moved with site-specific and heat sensitive information which can either be updated or modify information on the Blockchain ledger[7]. The remove updates allow all the parties involved to be in a position of sharing data and the status of the package as they navigate from one community to the other. The sharing of data and package status is crucial in ensuring compliance with conventions [8].

B. 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

III. INCORPORATE IOT DEVICES MANAGEMENT SYSTEM ON THE BLOCKCHAIN

There are many distinct advantages to the idea of building intelligent machines capable of communicating and operating across the Blockchain network. Initially, there is the issue of censorship where data transactions between various networks and organizations are recorded permanently. The permanent recording means that monitoring goods moving through various points in the supply chain is made more efficient. Logs made in the Blockchain network can only be tracked and evaluated by everyone who is authorized to gain access to the network [9]. 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 that data can be trusted by all parties involved in the supply chain. The machines will securely record the details of transactions between them, without any form of human control [2]. A person can only replace transactions recorded on Blockchain with access key referred to the private key. No inaccurate information can be fed on the transactions.

Thirdly, the Smart Contract facilities offered by some Blockchain technology networks, such as Ethereum, permit the formation of agreements whenever conditions are fulfilled. This is probably very useful when it comes to, for example, authorizing one payment system when conditions indicate that a service has been provided [6].

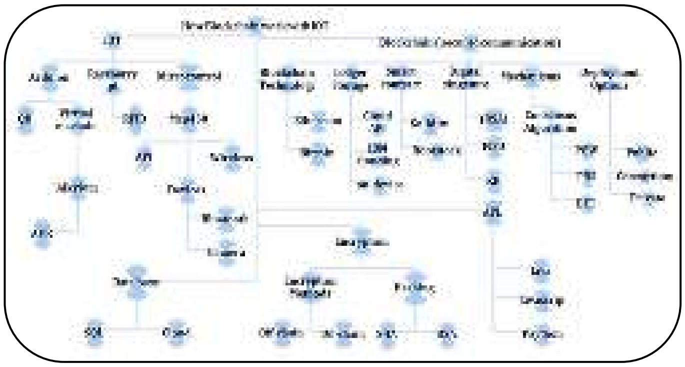

Fig. 2. Blockchain Utilization with IoT

Fourthly, the Blockchain technology system boosts the security of online transactions. Much of the data generated by Internet things is very personal - for example, smart home appliances can access intimate details relating to our everyday life. These are the kind of data that must be amongst devices and platforms to make it meaningful in our lives[10]. However, it also means that there are more opportunities for hackers to attack us [2].

Companies and governments investing in the internet also have to deal with this growing range of data breaches perpetrated by criminals, competitors, and enemies. Moreover, above the fact that it will provide new opportunities, there is a possibility of resembling Blockchain technology and the Internet of Things in the future. This is only possible if the current Internet object model which refers to devices attached to the Blockchain network via the central storage and cloud storage service - continues to emerge; systems are likely to become increasingly bloated, with data volumes still increasing, as well as the number of connected devices.

In the other aspect, the cloud services are likely to become bottlenecks due to the large volumes of data passed through them[11]. Rather than using an expensive data center, Blockchain provides a data storage network through the interconnection of many computer devices which form the network [8].

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, Fig. 2 illustrates it.

IV. BLOCKCHAIN TECHNOLOGY PLATFORMS

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

1) *Ethereum:* Ethereum is one of blockchain platform which provides the possibility for any developer to write and 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 by The Linux Foundation. Intended as a foundation for developing applications or solutions with a modular architecture, Hyperledger Fabric allows components, such as consensus and membership services, to be plug-and-play.

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

4) *R3 Corda:* Corda has been developed to service the specific needs of financial services with generations of disparate legacy financial technology platforms that struggle to interoperate, causing inefficiencies, risk, and spiraling costs.

5) *Quorum:* Is an enterprise-focused version of Ethereum. Quorum is ideal for any application requiring high-speed and high-throughput processing of private transactions within a permission group of known participants.

From the discussion above, the authors prefer the Ethereum platform as a general Blockchain due to Ethereum provide usability and free open source [7].

According to literature, most developers utilize either Ethereum while the other developers utilize Hyperledger fabric. Therefore, a comparison between two blockchain platforms was conducted (Hyperledger fabric, Ethereum). Table I shows the comparison.

TABLE I. COMPARISON BETWEEN BLOCKCHAIN PLATFORMS

Classification	Hyperledger Fabirc	Ethereum
Description of Platform	General purpose blockchain (not just used for payments)	General purpose blockchain (just used for payments)
Governance	Linux Foundation	Ethereum Developers
Currency	None	Ether
Mining Reward	N/A	A static block reward for the ‘ winning’ block, consisting of exactly 5.0 Ether
State	Key-value database	Account data
Consensus	Pluggable:PBFT	Proof of work
Network	Permissioned	Public or Permission
Transaction	Public or Confidential	Anonymous or Private
Privacy	Open to Private	Open
Smart Contracts	Yes (Chaincode)	Yes (Solidity, Serpent, LLL)
Program Languages	Java, Golang	Golang, C++, Python
Scalability	Claims to be scalable	None

V. SMART CONTRACT

A smart contract is a digital contract aimed for running contract independently without human involvement. 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 [12].

In case, the transactional contents comply with the smart contract, the transaction is then fulfilled automatically but if not, the transaction just fails.

Any business model including a contract can make efficient use of smart contract to reduce the response duration. The price paid to the middlemen is also cut down, as in the case of running a real estate, one does need to hunt for a real estate agent. No landlord needs to stash extra fee to the middlemen. The use of it ranges so long that even automobile organizations are ready on their feet to invest in blockchain and smart contract [13].

The insurance businesses are glad to witness the development of technology as now they can hand out various insurance contracts depending upon the driver's driving style. With the huge collection of data, the insurance companies can construct reasonable and accurate content [14]. The Table II below provides a list of these applications in various areas.

TABLE II. APPLICATION

Ref.	Classification	Goal
[15]	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.
[16]	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.
[17]	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.
[18]	Medrec	The medical records are stored in the form of a checklist in the smart contract. It also manages to pay fees paid by the patient for their services. Then, it is sent to the clinic when the doctor applies the smart contract conditions.

VI. 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. Special keys are only known by the administration (Blockchain).
- 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 use of complex algorithms and consensus among users ensures that transaction data is not manipulated once agreed. The data stored on the Blockchain acts as a single copy of the truth to all parties involved, thus reducing the risk of fraud.

B. Implementing Blockchain Technology

The platform can be deployed in three categories [5]:

- 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 [19],[20]:

- 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 [21].

- Proof-of-Stake: Refers to the algorithm for consensus that makes it possible for everyone to mine or authorize transactions. Proof of stake is defined by the number of crypto coins (Bitcoin) a mine owns. The higher the number of crypto coins reserved by a mine, the more the mining power possessed[22].
- Byzantine Fault Tolerance (BFT) :Algorithms are designed to avoid attacks and software errors that cause faulty nodes to exhibit arbitrary behavior (Byzantine faults). BFT [19] provides consensus despite the participation of maliciously misbehaving (Byzantine) nodes.

VII. Limitations of Using Blockchain IN the 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 [3]:

- 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 to the above challenges related to the deployment of Internet objects, there are also problems associated with the application of blockchain technology to internet objects[23]. 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.

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, some mechanisms should be devised to perform encryption using a set of nodes or Internet mechanism objects that have a minimal load in holding Internet objects.

4) Storage: Blockchain technology is suitable for decentralized Internet systems because it lacks central control. However, every Internet node needs things to be stored A Ledger increases in size with time. Internet points (IoT) objects may not be able to store a large amount of data.

5) Optimal design: The Internet system must design the best things with security and privacy-based blockchain as an essential element. This will result in an ideal design that gives equal priority to connection and calculation coordination, security, and privacy.

6) Legal Issues: Security and privacy standards vary in different countries and regions. This represents a severe challenge to the successful adaptation of blockchain technology in Internet objects systems. A standard framework is needed that manufacturers can use to provide security and privacy solutions.

VIII. System Architecture

Issues of compatibility are the main reason why most internet objects fail to work with blockchain system. Incompatibility results from lack of adequate hardware resources. In other Internet platforms, incompatibility issues are solved through the adoption through the use of a virtual machine architecture that has partitions. To solve the problem of interoperability in Blockchain, the same technique can be applied in Blockchain technology.

Some of the components that make up the Blockchain Architecture is discussed here [24].

A. Aryl Blockchain Node

The node is connected to the Ethereal Cocktail just like in any other blockchain node. The node functions in devices that are capable of allowing interactions in the blockchain and plays the role of monitoring the smart contract [24].

In the following paragraphs, the explanations about Ethereum Blockchain component are highlighted.

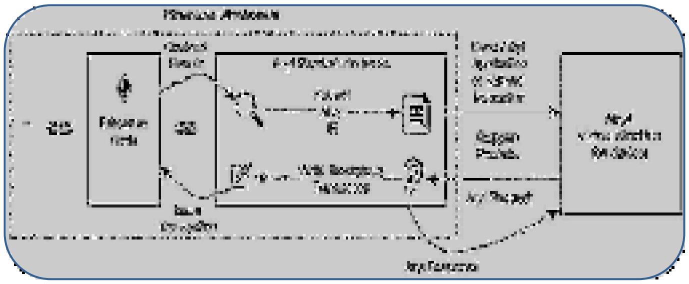

Fig. 3. Ethereum Blockchain

B. Alkyl Virtual Machine: This virtual machine relies on the Aryl blockchain node, and therefore it has to wait for assistance from the run-time system as well. The fact that it has relied on the assistance of other components doesn't mean that the Internet device has to work on other things while on waiting mode. On receiving the request, Alkyl Virtual Machine executes instructions received in the right manner[7]. Therefore, the Aryl blockchain node is considered as being a positive node considering the Alkyl Virtual Machines connected [24]. Fig. 4 visualizes Blockchain platform for industrial internet of things (BPIIoT).

Fig. 4. BPIIoT Archetacture

As clearly shown in fig. 4, this platform consists of three layers: proximity networks, a service platform, and domain applications as well as the data flow and control flow among these components.

IX. EXISTING RESEARCH ON SECURITY AND PRIVACY IN BLOCKCHAIN- BASED IOT

A. Authentication

This paper summarizes the security and privacy of IoT based on the blockchain system, a new scheme for the authentication of closed and transient graphs that offer assistance in block-based identity management systems [25].

B. Privacy-preserving

Blockchain technology is built on a foundation of the philosophy that there is a private key that can be used to unlock the encryption of digital assets. This key is the largest vulnerability since it has to be stored somewhere either on paper, on a disk or the cloud [3].

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 [26].

X. THE BENEFIT OF USING THE BLOCKCHAIN WITH IOT

According to [2], 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[27]. Organizations and businesses can, therefore, use the technology without fearing loss of integrity for their data and information.

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 eliminate additional costs which in the traditional forms of communication.

3) *Accelerate data exchange:* Enhanced data exchanges such as "intermediary man" (Internet portal things or any medium change device) are disbursed from the process. Block-based contracts and notebooks reduce the time needed to complete the transmission of IoT device information and time used in processing.

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. The exchange of data and security of the interconnected devices have been enhanced as well. Ways in which the distributed system helps in to solve issues that relate to security and reliability [28]:

- Blockchain technology can be used in the of 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 in the internet, and smooth transfer of data.
- Eliminates the need of 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 helps in the elimination of bottlenecks and cases of inefficiency.
- Reduction in the cost of operating internet objects. Moreover, publishing because intermediaries are not involved in operations.
- Various Internet devices can handle issues directly through the use of which provides an easy way of troubleshooting devices.

XI. LESSONS LEARNED

In line with the above situation, 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.

TABLE III. SUMMARY OF BLOCKCHAIN LITERATURE

Ref no.	Summarized		
	Objective	Solution	Remarks
[3]	To provide 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 goals, i.e., confidentiality, integrity, and availability
[29]	To reduce the complexity and computation for the use of blockchain for IoT systems	Authors divided IoT systems into the multi-level decentralized network based on blockchain technology	The proposed multi-level network based on blockchain is a feasible solution for secure IoT network
[30]	To investigate the prospect of blockchain for the information distribution in IoT systems	A design is presented to analyze that how existing security schemes can be made more powerful with the use of blockchain	Authors discussed how Key security requirement could be satisfied by the use of blockchain technology
[28]	To provide a systematic literature review on blockchain for the IoT	Many use cases are discussed for the use of blockchain to address high lighting issues, as well as open research issues, are pointed out in blockchain for IoT	Three factors are taken into account, i.e., integrity, anonymity, and adaptability
[10]	To check the feasibility of blockchain for IoT	Different challenges in IoT are highlighted, and their potential solutions based on blockchain	Overall, it is emphasized how blockchain technology can improve security in IoT systems
[31]	Design and development of the Internet of Smart Things (IoST) and use blockchain technology for secure communication	Authors used a permission-based blockchain protocol called Multichain for secure communication among smart things	The multichain protocol offers low communication cost and is a suitable choice for IoT solutions
[32]	Develop a lightweight architecture based on blockchain for IoT systems	The proposed lightweight architecture was validated for the use case of smart homes	The proposed architecture offers less overhead regarding packets and processing
[11]	Study the effectiveness of blockchain for better availability and accountability in IoT systems	Develop a prototype of the IoT system for better understanding	It is concluded that the availability is significantly improved using blockchain technology

The integrity of the information is lost, and the system can no longer be trusted.

Besides, the blockchain is an open-source distributed ledger that uses cryptography to verify, track and record transactions in a network. The objective is to find out whether this technology, when used in conjunction with the Internet of Things devices can improve supply chains in businesses through increasing efficiency, trust in the integrity of the process, openness, traceability, and customer satisfaction. Table III list a summary of recent literature on blockchain with IoT.

XII. CONCLUSION 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 on the internet with the integration of computing and transaction processing systems. By utilize blockchain technology, We've done expensive IoT tools because of the high costs associated with cloud infrastructure and other factors such as network equipment. In the coming years, we hope that changes to the organization of the blockchain and improvements to the encryption formula to increase the security of social networks using another model of the hyper ledger or BigchainDB and even use a consensus Algorithm like Proof of Authority and Delegated Proof of Stakes.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer Networks, vol. 54, pp. 2787-2805, 2010.

[2] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," arXiv preprint arXiv:1806.09099, 2018.

[3] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395-411, 2018.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[5] M. Singh, A. Singh, and S. Kim, "Blockchain: A game changer for securing IoT data," in the Internet of Things (WF-IoT), 2018 IEEE 4th World Forum on, 2018, pp. 51-55.

[6] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of, 2016, pp. 1-6.

[7] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in Advanced Communication Technology (ICACT), 2017 19th International Conference on, 2017, pp. 464-467.

[8] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Big Data (BigData Congress), 2017 IEEE International Congress on, 2017, pp. 557-564.

[9] B. Mo, K. Su, S. Wei, C. Liu, and J. Guo, "A Solution for the Internet of Things based on Blockchain Technology," in 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), 2018, pp. 112-117.

[10] D. M. Mendez Mena and B. Yang, "Blockchain-Based Whitelisting for Consumer IoT Devices and Home Networks," in Proceedings of the 19th Annual SIG Conference on Information Technology Education, 2018, pp. 7-12.

[11] M. Muzammal, Q. Qu, and B. Nasrulin, "Renovating blockchain with distributed databases: an open source system," Future Generation Computer Systems, vol. 90, pp. 105-117, 2019.

[12] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in International Conference on Financial Cryptography and Data Security, 2017, pp. 357-375.

[13] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," Peer-to-Peer Networking and Applications, vol. 10, pp. 983-994, 2017.

[14] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," Ieee Access, vol. 4, pp. 2292-2303, 2016.

[15] A. Ramachandran and D. Kantarcioglu, "Using Blockchain and smart contracts for secure data provenance management," arXiv preprint arXiv:1709.10000, 2017.

[16] K. L. Brousmiche, A. Durand, T. Heno, C. Poulain, A. Dalmieres, and E. B. Hamida, "Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain," Proceedings of IEEE Blockchain, vol. 2018, 2018.

[17] A. Norta, "Designing a smart-contract application layer for transacting decentralized autonomous organizations," in International Conference on Advances in Computing and Data Sciences, 2016, pp. 595-604.

[18] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in Open and Big Data (OBD), International Conference on, 2016, pp. 25-30.

[19] O. Arabaci, "Blockchain consensus mechanisms: the case of natural disasters," ed, 2018.

[20] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in Proceedings of the 1st Workshop on System Software for Trusted Execution, 2016, p. 2.

[21] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," Journal of Software Engineering and Applications, vol. 9, p. 533, 2016.

[22] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," Applied Energy, vol. 195, pp. 234-246, 2017.

[23] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," Computer Networks, vol. 112, pp. 237-262, 2017.

[24] J. Ellul and G. J. Pace, "AlkylVM: A Virtual Machine for Smart Contract Blockchain Connected Internet of Things," in New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on, 2018, pp. 1-4.

[25] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and L. Castedo, "Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications," Sensors, vol. 17, p. 28, 2016.

[26] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on, 2017, pp. 618-623.

[27] H. T. Vo, A. Kundu, and M. K. Mohania, "Research Directions in Blockchain Data Management and Analytics," in EDBT, 2018, pp. 445-448.

[28] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," Work Pap.–2016, 2016.

[29] W. Ejaz and A. Anpalagan, "Blockchain Technology for Security and Privacy in the Internet of Things," in the Internet of Things for Smart Cities, ed: Springer, 2019, pp. 47-55.

[30] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures the blockchain, and anonymous messaging streams," IEEE Transactions on Dependable and Secure Computing, vol. 15, pp. 840-852, 2018.

[31] M. Samaniego and R. Deters, "Internet of Smart Things-IoST: Using Blockchain and CLIPS to Make Things Autonomous," in Cognitive Computing (ICCC), 2017 IEEE International Conference on, 2017, pp. 9-16.

[32] D. von Leon, L. Miori, J. Sanin, N. El Ioini, S. Helmer, and C. Pahl, "A Performance Exploration of Architectural Options for a Middleware for Decentralised Lightweight Edge Cloud Architectures," in International Conference on Internet of Things, Big Data and Security, 2018.