Volume: 5, Issue: 6
Page: 209-224
2021

International Journal of
Science and Business
Journal homepage: ijsab.com/ijsb

IJSAB International

# Blockchain For Securing IoT Devices: A Review

**Shavan Askar, Zhwan Mohammed Khalid, Tarik A. Rashid**

## Abstract

Internet of Things (IoT) has grown quickly and receives considerable interest in academia and the market. However, the absence of basic technologies in protection leads to risks and security flaws in IoT privacy. IoT technologies vary from a mission-critical predicament to business-oriented applications (for example, smart grid networks, smart mobility systems, video monitoring, and eHealth) (e.g., Banking, transportation and contract law insurance) (Askar et al., 2011; Al Majeed et al, 2014). Comprehensive security support is required for IoT, particularly for task-critical applications and for business applications downstream. There have been proposals and/or utilizations of some safety methods or approaches. The platform blockchain has been suggested as an outsourced and distributed solution to guarantee protection standards and to motivate the growth of the IoT due to its decentralization and disclosure. A Blockchain is a database that store sequential manner, in multiple machine memories faulty to its opponents, any processed transactions – or records. Both participating customers share these purchases. The details shall not be stored as a public directory; each node user or device is equipped with the same directory as any other node user. In this article, present the basic blockchain structure and outline the safety criteria for developing IoT and then discuss how the IoT using's protection tools and technologies can be used via BC. Also identify the most pertinent IoT technology frameworks based on blockchain. In addition, reviewing numbers of researches provides securing IoT based on BC finally, discuss several challenges will face of IoT and BC.

***Keywords:*** *Blockchain, IoT, Security, cryptocurrency, 5G, blockchain security.*

**IJSB**
**Literature review**
Accepted 29 May 2021
Published 19 August 2021
DOI: 10.5281/zenodo.5222704

About Author (s)

**Shavan Askar (Corresponding Author)**, Assistant Professor, CEO of Arcella Telecom, Erbil Polytechnic University, Erbil, Iraq. Email: shavan.askar@epu.edu.iq.

**Zhwan Mohammed Khalid,** Raparin University, Sulaimany, Iraq. Email: eng.zhwan90@uor.edu.krd.

**Tarik A. Rashid,** Professor, Computer Science and Engineering, University of Kurdistan Hawler, Erbil, Iraq.

## 1. Introduction

Every year, the IoT expands explosively and strives for 5G technology such as smart homes and towns, e-health, digital intelligence etc. In a decentralized method, the IoT devices are related. It is also very difficult to use current common protection methods in IoT nodes communication. Blockchain (BC) is a technology that guarantees a secure transmission of IoT Transactions. It offers a decentralized, distributable and freely accessible, shared directory to store data for IoT blocks processed and checked. Through peer-to-peer topology the public leader's data is processed automatically (Askar, 2017; Fizi & Askar, 2016; Askar, 2016; Keti & Askar, 2015; Qadir & Askar, 2021).

The BC is a technique used for the use of a block in BC among IoT nodes. Blocks are attached and the address of each device for the previous device is given. Blockchain and IoT function together in the form of IoT and cloud convergence. The BC will revolutionize IoT connectivity in the future (Reyna et al., 2018) , Table 1 indicate the outline for integrating the BC and IoT

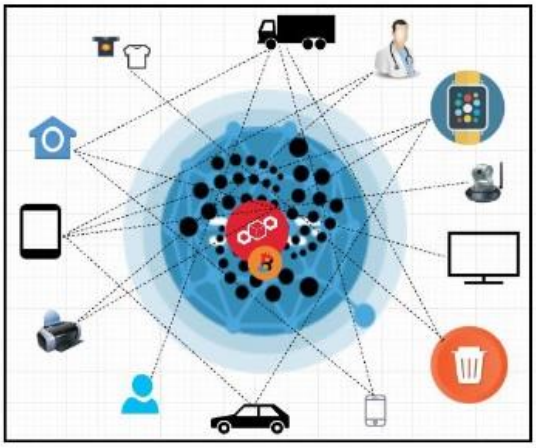

Figure 1: IoT and Blockchains

Table 1 Integrating the BC and IoT

| Objective | Description |
|---|---|
| Basis for decentralization | In IoT and BC the same strategy is adopted. The central system is abolished and a decentralized system is provided. It enhances the risk of failure and efficiency of the whole device. |
| Identification | Both associated users with a special ID may be recognized in the IoT. There is a separate definition for each BC block. BC is a reliable program offering unique information in the public directory |
| Autonomous | Both IoT nodes in BC are able to connect without the centralized mechanism with any node in the network. |
| Reliability | IoT nodes in BC provide network awareness authentication.<br>The numbers are correct, as the miners check before reaching BC.<br>Only validated blocks are added to the BC. |
| Security | The BC secures transfers between nodes. For safe contact, it is a very modern method. BC enables IoT devices to connect securely with each other. |
| Scalability | In BC, IoT devices communicate in real-time with their destination computer through a highly accessible distributed intelligence network. |

However, interoperability issues, security deficiencies, lack of data processing and distribution and lack of IT and OT integration remain technical challenges for the rapid growth of IoT. Protection deficiency is one of the most serious problems. In the knowledge network several

wired computing systems directly exchange information with the cloud as production processes get smarter; a stable sand assault occurs. This risk can take many types, as IoT devices have shown that bugs are easier to use. As the number of targets for cyber-criminal botnet is increasing. Distributed IoT-based DDoS attacks have shown their strength in my business (Husain & Askar, 2021; Samann et al, 2021). For IoT security, Blockchain is the perfect solution. The workplace in the (Teslya and Ryabchikov, 2017, Bahga and Madisetti, 2016) Suggested IoT blockchain network. This platform, which uses intelligent contracts, makes it possible to build various distributed applications for production using a decentralized and less trusting IoT applications peer-to-peer network

In summary, the rest of the paper: Introduction of the article in Section one. Section two describes Blockchain Technology. Section three Blockchain-based IoT are discussed. In the fourth section determined Blockchain and IoT use cases. Section fifth reviews previous literature. Lastly, conclusion is presented.

## 2. Blockchain Technology

The blockchain (BC) definition is now subject to extensive study and realistic attention. Blockchain guarantees data integration through a wide range of transaction players with operating evidence that increases decentralized confidence – a blockchain substitute for that trustworthy third party. This would usually be handled using a 'ignore' transactional elements from a reputable third party. A blockchain is a node connection array, in which the header, operating information and additional secure metadata are included for each block. Restore a paper catalog (extending n), thus avoiding alteration or retroactive handling of the documentation. Because blockchains are immune to the abuse of the underlying documents, they are considered to represent a tamper-resistant, incorruptible distributed booklet for almost helpful economic or logical transactions (Pilkington, 2016, Merkle, 1987). The blockchain implicitly promotes basic simplicity, incorruptibility, transparency and the freedom to anonymously store and move info. Outside of the first cryptocurrency applications such as bitcoins, further blockchain frameworks were recently released. In reality, a variety of elements, documents, facts, packets, deals, contracts, monetary transactions or signatures may be present in the details. The blockchain will facilitate a broad variety of functions, including the secure storage and transfer of confidential information, and can allow parties to enter into trustworthy contracts without intermediary involvement. Possible company requests require the filing / receipt of claims; fraud claims identification on various claims for the same treatment by the applicant (e.g., medical office) (e.g., data integrity). The implementation of new, intelligent logistics contracts is another example of implementations where the receiver receives a shipment and the variables pay for them. In addition, the authenticity of articles and programs is also required across multi-stage national procurement, delivery and service chains (this may raise questions about bogus articles and/or needs legal monitoring objects such as medicinal drugs, medical equipment, controlled prescription goods, weapons, and negotiable bonds). In addition, for cyber security in particular integrity important, proposed blockchain architecture is proposed. This paper has little intention of presenting a structured description of a blockchain (or bitcoin); formal definition mathematics are quite complicated (Bashir, 2017, Ouaddah et al., 2017) The aim is more to provide a short description of blockchain technologies in order in potential cases of IoT and IST use in general to explain and promote further research and growth.

In general terms, blockchains establish a collective record of asset possession for all individuals (or companies) who doesn't know each other or trust each other. Blockchain is a "sharing network," a distributed system-based platform. It is a data book replicated in the P2P network through a multitude of computers. The probability of global data processing is significantly

reduced by blockchain documenting operations on many dispersed hosts because of a replication of a decentralized leader. Blockchain is a time-stamped transaction history record which maintains a copy of the system history of transactions; for each censor a copy of that record is maintained local and consensus algorithms allow for sync regardless of the copy. In specific, blocks representing valid transaction sets will have a blockchain; the two blocks will be juxtaposed with a prior block hash throughout the blockchain. The linking blocks are a chain. Network members are anonymous entities, known as nodes (processes, people or users). Depending on the position taken, nodes execute a number of tasks. A node will build, propose, verify and execute transactions to promote consensus and ensure that the data are integral. When transmitting nodes, nodes are signed to verify that they are true owners of the goods that can be replaced with another individual in the blockchain encrypted network via a private key. To ensure node replication a P2P network and consensus algorithms are essential in a blockchain. The condition of the distributed ledger is the responsibility of the peers. P2P ensures that the secure blockchain network does not have a central authority and all nodes will access each other directly via a mechanism allowing for the direct sharing of transactions (e.g. facts, documents, cyber currency). Usually, there are two groups of coworkers: co-workers and co-workers. Simulating the implementation of the transaction by endorsing partners: executing and endorsing the transaction; support policies lay out the guidelines for the acceptance of the transaction. Committing partners are collecting transactions approved by supporting partners, reviewing and modifying their own ledger transactions – Orders that accept and sequence transactions by endorsers to commit partners can also be order nodes. Nodes may be miners or stone signers. Miners are generating new blocks of records. The signers of the block verify the transaction and digitally sign it. A significant assessment must be made for each blockchain network by determining which nodes to connect the next block. This decision is taken by a mechanism of consensus. Miners can install, check and add new blocks of transactions.

Encryption mechanisms are used to safely distinguish the data source and sink of network communication. When the (miner) node uses the archive files, the data is entered in the directory network.. This is decided. The consensus procedure generally consists of three steps: the Transaction Final Phase in which an appropriate transaction is simulated; process in which the transaction sequence in the directory is recorded; and the Validation Process and engagement Process when committing partners check and notify the transaction received from orders when committing peers. The network's P2P messages typically help discovery (initial discovery by blockchains of other network people), transaction (request, invoke and deploy transactions), synchronization (continued blockchain on all nodes).

Once a mining node is connected to the P2P network, a miner has several activities to carry out. (Bashir, 2017).

Network synchronization: import the relevant blockchain on request from other network nodes for historic blocks. Transaction authentication: transactions sent through the network shall be authenticated through the replication and validation of digital signatures and outputs by nodes with complete functionality. Block validation: blocks validating against rules established; this applies to each block transaction and the nonce value. New blocks creation: as stated, by merging validated network transactions, minerals may propose a new block. Work Proof (PoW), which means miners can identify the correct block by solving the compute puzzle: The nonce fields of the miner are modified in the header again and again until the hash created is less than the threshold of default.

Rewards: after resolved the node to the puzzle, the outcome is broadcast by other nodes that cause the block to be checked and approved; the miner is rewarded 'somehow' if the block is approved. Please note that PoW requires non-negligible computational capital. In certain cases,

the above block header is located, a number of transactions transferred into the proposed block on a P2P network are collected, the previous block header doubles the hash with the nonce is computed, and the hash is calculated if the calculated hash is less than that of the current degree of threshold complexity. The Powerful Dilemma.

A hash is an algorithm that generates a message or file for a variable length which can map a data object into a smaller fixed-size data object. This is an entity that creates a data object-based attribute (like the Stable Hash algorithm Two [SHA-2]) (the "hash result"). The optical picture is seen in Fig. 2. Typical hashes have a unique safety feature to guarantee storage or to generate text or documentation for cryptographic digestion (in order to ensure data integrity, thereby providing an electronic signature). A Merkle tree has an encryption brush on the nodes and a hatch on unwoven nodes. It contains the tree. The tree is often referred to as a hash tree. The Hash Bree safely and effectively manages the data structure content (Merkle, 1987). In a blockchain, the hash value is created by each transaction in the collection comprising the block(Khalid and Askar, 2021). Merkle Tree has to do with links. A hash of the previous block header and a time stamp, the results of the hacking operation are shown in the block header. The new heading is used to produce a (32-bit) cryptographic operation. Then add the nonce to the blockchain.

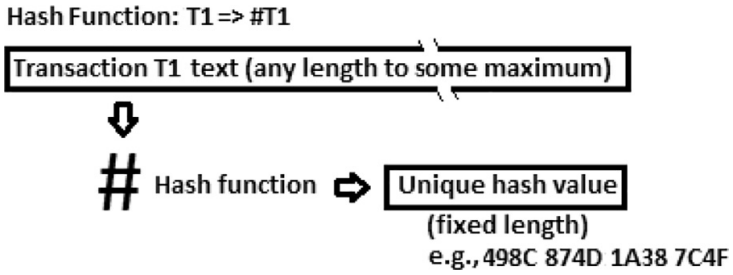


Figure 2: Hash function

## 3. Blockchain-based IoT

Blockchain is a real directory documents which are stored point by point in a distributed way and are separate from any central authority. Any log can be encrypted and time stamped, and only user-searched blocks with the private key can be accessed and edited. Any block is linked to the previous and subsequent chains, and each transfer updates the whole chain. (Kshetri, 2017, Watanabe, 2018) . After registering on the blockchain master, it is exceedingly difficult or impossible to uninstall the editor from a block. The anonymity of the contact and transaction are guaranteed. As blockchain has so many revolutionary features, it has been used for IoT development and continues to be used. Figure 3 shows a small number of blockchain representative requests.

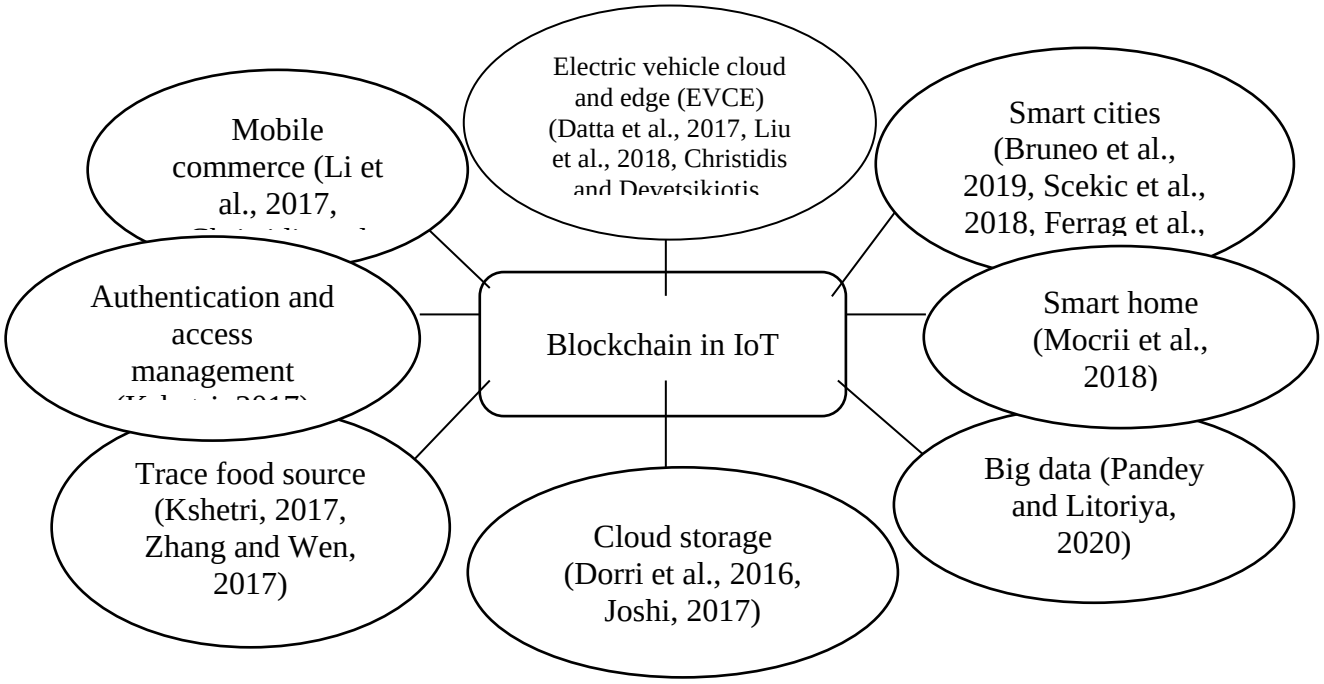


Figure 3: Blockchain IoT implementations

An example of blockchains in IoT Sec demonstrates that integrity for ITSs is constantly required; it often necessitates anonymity, and the availability (not reproduction) of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) traffic is commonly required and often indispensable for other functions. The atmosphere data provided by a sensor cluster is connected to a gateway point in an IoT-enhanced environment (The V2V and V2I data are usually exclusively local, although a number of summarized or administrative information can be sent to a central repository). At that time, a blockchain will be created that will represent aggregated data. Data may then be sent to a computer system that may be part of a business or governmental organization (and may actually implement data at the time) (where data will be re-corded in a blockchain transaction). Figure 5 demonstrates an IoT protection e-health application; the portal or site-level computer in this case serves as a miner and generates a blockchain for the knowledge of the physician to pass to a distant medical facility.

It is currently unknown which of the above-mentioned Blockchain methods (in a vertical implementation or on a platform) would be implemented; however, blockchains can and should be used in all types of transactions at the application level. For example, the parking fee is charged by the different financial institution that supports the transaction; or the content of any graphics, photos, pictures, videos or data chain of custody is assured. Other ITS implementations which contain insurance data including UBI or fractional ownership of independent cars. Other applications may include insurance data. In comparison, Medical sensor data, health statements, screenshots for video monitoring can include data (Yue et al., 2016, Magyar, 2017).

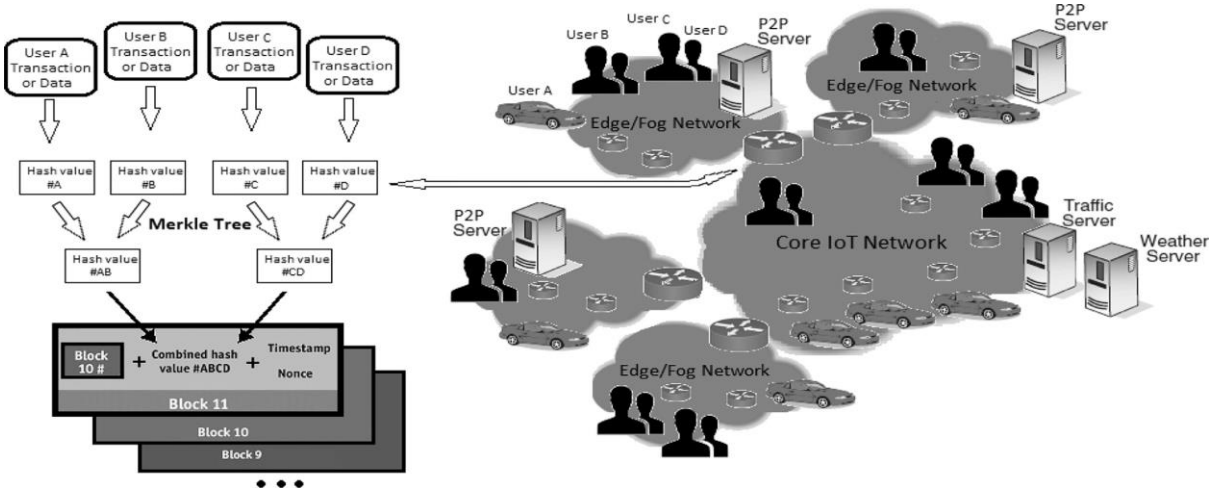


Figure. 4. Use of a smart city/vehicle transport/ITS-IPOT/CPS blockchain application (gateway example).

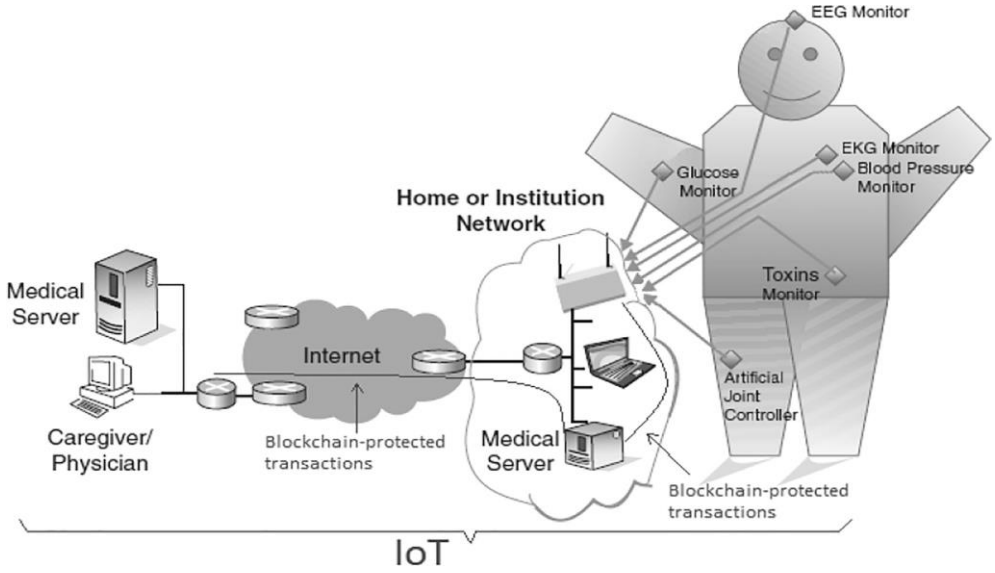


Figure. 5. E-health use of blockchain (example).

## 4. Blockchain and IoT use cases

The BC-IoT integration strategy provides a plethora of thrilling possibilities. It brings up new opportunities for both of them. The below are some of the outcomes:

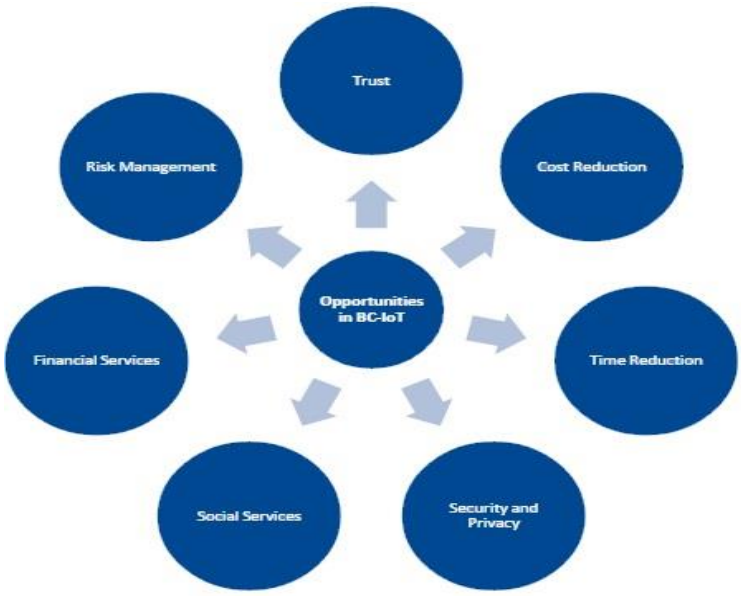


Figure 6: BC-IoT opportunities

**4.1 Creating a Trusting Bond between the Parties:** This approach would promote trust among various connected devices due to its security features. Only certified devices can communicate in the network, and any block of a transaction must be checked by miners before it can reach the BC.
**4.2 Reduce Time:** This is a time-consuming strategy. It decreases transaction time from day to day.
**4.3 Social Services:** This solution provides linked devices with public and social services. Both linked devices are able to communicate with them and share information.
**4.4 Financial Services:** Without a third party this method transfers funds securely. It offers fast, safe and private funding. Moving costs and time were minimized.
**4.5 Security and Privacy:** The equipment and records are safe and confidential.
**4.6 Risk management:** This method has been influential in assessing and reducing the likelihood of capital and transactions loss.
**4.7 Reduce the Cost:** This will minimize expenses when it deals with the third party directly. It removes all nodes from the sender and the recipient. The correspondence is clear.

## 5. Literature Review

In (Zyskind and Nathan, 2015) A decentralized data management tool allows people to view and track their data. A protocol was also used to transform a blockchain into a manager for automatic access without confidence. In contrast to Bitcoin, there systems' transactions are notoriously financial – they are used to provide instructions such as data collection, query, and sharing. Finally, they discuss possible blockchain extensions that could be used in a very systematic approach to trustworthy social computing problems. In (Ouaddah et al., 2016) Offer a modern blockchain IoT-based platform for access management. The first contribution is to make a reference model of the IT requirements' aims, models, design, and mechanisms accessible to them.. Fair Access was also launched as a completely decentralized pseudonym and privacy system which enables users to have their data in possession and control. System for management authorization. They also used the blockchain to extend our idea to an access management provider that is decentralized. Fair Access provided, in contrast to Bitcoin financial transactions, new transaction forms used to award, transfers and revoke access. In (Lundbaek et al., 2016) The systematic study proposed of regulated blockchains operated and

controlled by institutions, which either did not produce cryptocurrencies or created rewards for cryptographic puzzle solvers. View these methods as mechanisms for instantiation of a diverse technology for the machine pieces such as the cryptographic puzzle. Owners of such a blockchain have solver puzzles as their regulated tools, and use a mathematical model to calculate ideal parameters for the puzzle system or other blockchain components. They demonstrated this approach by adding the blockchains to record hashing of transactions in financial systems in order to improve their integrity and that of their audits. They created a complex Mathematical Model to derive MINLP Optimization problems in order to provide evidence of work as a cryptographic puzzle for the calculation of optimal work configuration parameters that offers possible conflictive factors such as availability, resilience, security and costs. In some circumstances, we explain the usefulness of such a mining calculus. Random variables in our mathematical model formulation are true. In (Lee and Lee, 2017) Concentrate on a stable firmware upgrade problem that is a basic safety concern in an IoT world for embedded devices (Ahmed & Askar, 2021; Mohammed & Askar, 2021; Ali & Askar, 2021; Hamad & Askar, 2021). A new software upgrade scheme utilizing blockchain technology was introduced to safely verify a firmware version, to confirm firmware consistency, and to download the most current firmware for the built-in computers. The proposal calls for an embedded system to upgrade its firmware to nodes in a blockchain network to find out whether its firmware is up to date or not (Abdulkahleq & Askar, 2021; Khalid & Askar, 2021). Otherwise, the embedded system would update the new firmware from a peer-to-peer node network. When the firmware update has been completed, it checks the integrity, i.e. the correctness of the firmware. The proposed scheme makes sure the embedded device code is up-to-date and not corrupted. This reduces threats aimed at bugs in embedded applications. In (Moinet et al., 2017) Latest blockchain application in the field of autonomous wireless networks as a safe decentral storage for cryptographic keys and trust details. The Blockchain Authentication and Trust Module and their knowledge based trust paradigm demonstrate how to use a blockchain immutability to provide high-problem solutions in the area of ad-hoc decentralized networks. More specifically, their was demonstrated how a complete solution can be developed, which provides security and trust assessment mechanisms in a evolutionary network. In (Abdullah et al., 2017) Presented Kerberos' common security concerns. However, as the Internet, especially in a big data context, is increasingly being used in large networks, security vulnerabilities are frequently found. In a period in which greater safety standards are required, new technologies are required to quickly improve data use and integration. Blockchain technology, pioneered by Bitcoin, has provided scalable solutions to many fundamental security issues confronting Big Data (Sulaiman & Askar, 2015; Fares & Askar, 2016). In (Zhang et al., 2017) They created an authentication scheme for the Blockchain software. The customer maintains his identities in the cloud, stores his encrypted personal information in blockchain storage and has an intelligent contract with independent consent from the website / software. If an individual logs into a website or application, a provider uses an Off-Blockchain Response Protocol to confirm the identity of the user and to gather user information. In (Alexopoulos et al., 2017) explored the merits of protecting TM authentication schemes using free distributed heads (ODLs), such as blockchain technologies. They model these structures formally and investigate how blockchain can contribute to alleviating attacks. Following formal argumentation, they find that cryptography, blockchain technologies and ODLs in general may have significant advantages over previous methods in terms of trust management. In (Rodrigues et al., 2017) It provides modern architecture through new technology like blockchain and intelligent contracts, offering new opportunities in multi-domain scalable DDoS mitigation solutions. In (Xu et al., 2018) The Block Chain-Centralized Docker Trust discusses in particular its susceptibility to Denial-of-Service Attacks (DoS) and proposes a possible remedy (DDT). A blockchain with decentralization of confidence is the

alternative proposed. DoS is significantly minimized by providing Docker's photos with a signature testing service. The scalability and reliability of the proposed blockchain solution is shown by a performance assessment. We still use a DDT and performance tests at some Docker Trust Technology Prototype Amazon Web Services data centres (AWS).

In (Li et al., 2018) The approach suggested assigns a computer ID to authenticate without a central authority in the Blockchain. In order to immediately follow updates to the data condition through the data security system, significant data (i.e. the company firmware) is added to the blockchain. The framework based on Fabric hyper book open source framework has been used to review the proposed architecture. In (Kumari et al., 2018) New archeology design suggested integrating disruptive technology such as blockchain and intelligent contracts to provide new possibilities for DDoS mitigation tools that are scalable and effective across several areas. In (Yin et al., 2018) A new authentication anti-quantum transaction regime is presented in the blockchain. Key to this is the mixture of public and private master keys for the building of lightweight non-determinative wallet (Seed Key). Based on Bonsai Trees technology, a new authentication scheme was proposed with the key to extending a gill to several locations. The system was developed. The space used to ensure that a private master key is random and secure is used for each transaction signature. The safety test and examination are complete. Their research supports theoretical blockchain use in the post-quantum era. In (Biswas et al., 2018) Scalability of LEDs and quick transaction exercise in Blockchain are the key obstacles in this integration. The number of transactions which join Blockchain reduces by adding the scalability of local leaders without sacrificing the validation of the pair on local and international transactions. There is also a decline in transactions entering the world Blockchain. The test bed evaluations show that global partner weights and block sizes decline dramatically. The approach also implicitly enhances the load allocation to the processing scale for all peers.

In (Minoli and Occhiogrosso, 2018) As Castle-Approach protectors to defend different IoT-centric implementations, Blockchain Frameworks (BCMs) are part of the Protected mosaic. A block chain is a database that handles all transactions or data saved sequentially in the computer memory building to show an adversary. This transaction is shared by interested consumers. Information is retained and/or distributed as a shared directory, in the same directory as all other network users and nodes, each user or system node. In (Srivastava et al., 2019) It is about using Blockchain technologies to preserve the Internet of Things (IoT) for patient remote control systems. The article explains the benefits and the practical obstacles of blockchain based patient access management techniques for IoT devices. The article also examines the different possibly suitable IoT coding technologies.

Table 2 displays a list of publications that was used Blockchain in various Objectives in IoT

| Author(s) | Objectives | Description |
|---|---|---|
| (Zyskind and Nathan, 2015) | A decentralized personal data, very comprehensive approach to trustworthy social computing issues. | A decentralized framework for managing personal data ensures that consumers control and monitor their data. |
| (Ouaddah et al., 2016) | access control framework | The blockchain was used to implement it to a decentralized provider of access management. Fair Access providers, contrary to Bitcoin financial transactions. |
| (Lundbaek et al., 2016) | Financial process authentication | regulated blockchains operated and controlled by institutions, which either did not produce |

| | | |
|---|---|---|
| | Optimization of governed blockchains | cryptocurrencies or created rewards for cryptographic puzzle solvers |
| (Lee and Lee, 2017) | Stable firmware upgrade focused on blockchain for embedded systems in an internet setting | A new software upgrade scheme utilizing blockchain technology was introduced to safely verify a firmware version, to confirm firmware consistency, and to download the most current firmware for the built-in computers |
| (Moinet et al., 2017) | Wireless sensor network focused on Blockchain for autonomous sensor networks | blockchain application in the field of autonomous wireless networks as a safe decentral storage for cryptographic keys and trust details |
| (Abdullah et al., 2017) | Hadoop is Kerberos-based | Blockchain applications to improve the authentication of Big Data in the distributed environment |
| (Zhang et al., 2017) | smart agreement to give of website/application separate permissions | Constructed a dynamically distributed blockchain application user authentication system. |
| (Alexopoulos et al., 2017) | protecting TM authentication schemes using free distributed heads (ODLs) | Beyond the hype: Use of trust authentication blockchains, They model these structures formally and investigate how blockchain can contribute to alleviating attacks. Following formal argumentation, they find that cryptography, blockchain technologies and ODLs in general may have significant advantages |
| (Rodrigues et al., 2017) | Emerging technologies' modern architecture, security in all connected world networks and services | modern architecture through new technology like blockchain and intelligent contracts, offering new opportunities in multi-domain scalable DDoS mitigation solutions |
| (Xu et al., 2018) | Denial-of-Service attacks | decentralize content trust for docker images dependent on Blockchain |
| (Li et al., 2018) | a single device ID and record | The suggested solution assigns a machine ID to authenticate and registers in the blockchain without a central authority. |
| (Kumari et al., 2018) | ECC for IoT and cloud servers | a secure authentication scheme based on elliptic curve encryption on IoT and cloud servers |
| (Yin et al., 2018) | Novel blockchain authentication system for anti-quantum transactions. | A new authentication anti-quantum transaction regime is presented in the blockchain.<br>Key to this is the mixture of public and private master keys for the building of lightweight non-determinative wallet (Seed Key) |
| (Biswas et al., 2018) | Blockchain leader scalability and transaction volume | Modular Blockchain System for safe transaction in IoT |
| (Minoli and Occhiogrosso, 2018) | security mosaic, IoT Defense Blockchain Mechanism | Blockchain mechanisms (BCMs) are part of the protection mosaic as protections under the Castle-Approach to secure various IoT-centric applications |
| (Srivastava et al., 2019) | Monitoring devices for remote patients, such as A lightweight, secure IoT medical system health care blockchain | explained the advantages of blockchain based security approaches in remote patient control with IoT devices and also realistic hurdles |

## 6. Challenges

The IoT and BC will face several challenges including size, shopping, abilities, discovery, etc. The problems of the integration method are as follows.

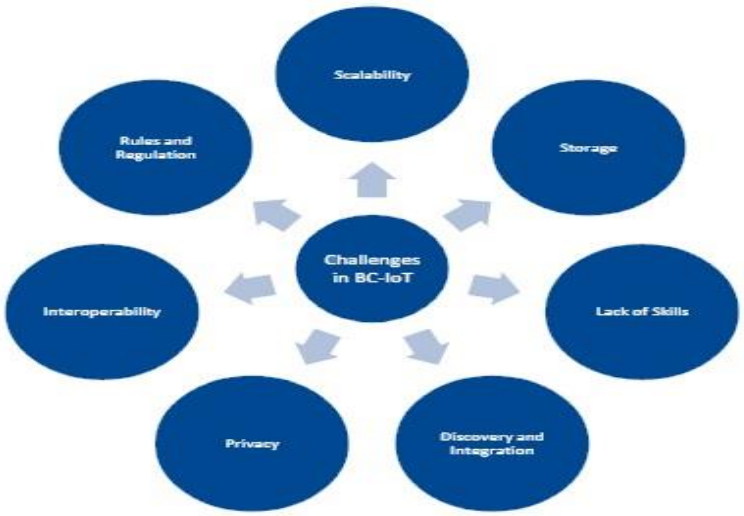


Figure 5: BC-IoT challenges

Table 3. Challenges of Blockchain in IoT

| challenges | Description |
|---|---|
| Scalability (Roy et al., 2018) | Due to its high transaction load, the BC can become hanged. The Bitcoin storage has risen to over 197 GB Think about the load being loaded if IoT is integrated in BC than is present. |
| Lack of Skills (Banafa, 2017) | The BC has become a modern invention. Very few people worldwide are aware of it. Therefore, training people on technology is also a difficulty. |
| Storage (Banafa, 2017) | Each IoT node contains the digital ledger. By then, the storage capacity will grow which will be a challenge to any connected system and will become a heavy load. |
| Privacy (Kumar and Mallick, 2018) | The booklet is publicly distributed to all connected nodes. You will see the transactions in the leader. In the integrated solution secrecy is also a challenge. |
| Discovery and Integration (Mohanta et al., 2020) | BC is not necessarily intended for IoT. The discovery of another device in BC and IoT is a very difficult process for the linked computers. IoT nodes can then explore one another, but cannot detect and merge the BC with another system. |
| Interoperability (Atlam et al., 2018) | The BC can be private or public. The BC-IoT solution also poses barriers to interoperability between public and private blockchains. |
| Rules and Regulation (Dai et al., 2019) | The IoT-BC will operate internationally and is thus faced with several guidelines and regulations for the worldwide application of this strategy. |

## 7. Conclusion

Blockchain was initially linked to digital currencies, but many other technological future developments arise, including IoT data integrity applications transacted via a massive multi-leverage network and archiving infrastructure. In this article, we intend to offer through overview of the IoT blockchain, which received a large amount of attention. With blockchain mix, IoT reflects the immense technological progress in various fields of human life, including Electric Car Clouds and Edge (EVEC), mobile trading, food supply monitoring, etc., rendering our business smarter. Blockchains are benefited in that the architecture can be applied synergistically across the layers and regions of the IoT ecosystem, both in the underlying and the layer of communication models. Blockchain is an ideal concept for the construction of IoT that opens, controls, stable and convenient IoT and Industrial Chain. Blockchain integration and IoT provides modern and novel market structures and IoT implementations for distribution. Future research will also be carried out in order to define which IoT implementations are ideally suited to incorporate blockchain-based security mechanisms at

functional level and to optimally implement the distributed ledgers (databases) that support IoT.

**References**

Abdulkhaleq, I. S., Askar, S. (2021). Evaluating the Impact of Network Latency on the Safety of Blockchain Transactions. International Journal of Science and Business, 5(3), 71-82.

ABDULLAH, N., HAKANSSON, A. & MORADIAN, E. Blockchain based approach to enhance big data authentication in distributed environment. 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), 2017. IEEE, 887-892.

Ahmed, K. D., Askar, S. (2021). Deep Learning Models for Cyber Security in IoT Networks: A Review. International Journal of Science and Business, 5(3), 61-70

Al Majeed, S., Askar, S., Fleury, M. (2014). H.265 Codec over 4G Networks for Telemedicine System Application. UKSim-AMSS 16th International Conference on Computer Modelling and Simulation (UK), Cambridge (pp. 292-297), doi: 10.1109/UKSim.2014.59.

ALEXOPOULOS, N., DAUBERT, J., MÜHLHÄUSER, M. & HABIB, S. M. Beyond the hype: On using blockchains in trust management for authentication. 2017 IEEE Trustcom/BigDataSE/ICESS, 2017. IEEE, 546-553.

Ali, K., Askar, S. (2021). Security Issues and Vulnerabilities of IoT Devices. International Journal of Science and Business, 5(3), 101-115.

Askar S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Evaluation of Classified Cloning Scheme with self-similar traffic. 3rd Computer Science and Electronic Engineering Conference (CEEC), Colchester, 2011, pp. 23-28, doi: 10.1109/CEEC.2011.5995819.

Askar, S. (2016). Adaptive Load Balancing Scheme For Data Center Networks Using Software Defined Network. Journal of University of Zakho, Vol. 4(A), No.2, Pp 275-286,

Askar, S. (2017). SDN-Based Load Balancing Scheme for Fat-Tree Data Center Networks. Al-Nahrain Journal for Engineering Sciences (NJES), Vol.20, No.5, pp.1047-1056

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Service differentiation for video applications over OBS networks. 16th European Conference on Networks and Optical Communications, Newcastle-Upon-Tyne, pp. 200-203.

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). A novel ingress node design for video streaming over optical burst switching networks. Optics Express, Vol. 19 (26), pp. 191-194

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Adaptive Classified Cloning and Aggregation Technique for Delay and Loss sensitive Applications in OBS Networks. in Optical Fiber Communication Conference/National Fiber Optic Engineers Conference 2011, OSA Technical Digest (CD) (Optical Society of America, 2011), paper OThR4.

ATLAM, H. F., ALENEZI, A., ALASSAFI, M. O. & WILLS, G. 2018. Blockchain with internet of things: Benefits, challenges, and future directions. International Journal of Intelligent Systems and Applications, 10, 40-48.

BAHGA, A. & MADISETTI, V. K. 2016. Blockchain platform for industrial internet of things. Journal of Software Engineering and Applications, 9, 533-546.

BANAFA, A. 2017. IoT and blockchain convergence: benefits and challenges. IEEE Internet of Things.

BASHIR, I. 2017. Mastering blockchain, Packt Publishing Ltd.

BISWAS, S., SHARIF, K., LI, F., NOUR, B. & WANG, Y. 2018. A scalable blockchain framework for secure transactions in IoT. IEEE Internet of Things Journal, 6, 4650-4659.

BRUNEO, D., DISTEFANO, S., GIACOBBE, M., MINNOLO, A. L., LONGO, F., MERLINO, G., MULFARI, D., PANARELLO, A., PATANÈ, G. & PULIAFITO, A. 2019. An iot service ecosystem for smart cities: The# smartme project. Internet of Things, 5, 12-33.

CHRISTIDIS, K. & DEVETSIKIOTIS, M. 2016. Blockchains and smart contracts for the internet of things. Ieee Access, 4, 2292-2303.

DAI, H.-N., ZHENG, Z. & ZHANG, Y. 2019. Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6, 8076-8094.

DATTA, S. K., HAERRI, J., BONNET, C. & DA COSTA, R. F. 2017. Vehicles as connected resources: Opportunities and challenges for the future. IEEE Vehicular Technology Magazine, 12, 26-35.

DORRI, A., KANHERE, S. S. & JURDAK, R. 2016. Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187.

Fares, N., Askar, S. (2016). A Novel Semi-Symmetric Encryption Algorithm for Internet Applications. Journal of University of Duhok, Vol. 19, No. 1, pp. 1-9

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. IEEE Internet of Things Journal, 6, 2188-2204.

Fizi, F., & Askar, S. (2016). A novel load balancing algorithm for software defined network based datacenters, International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom), Graz, 2016, pp. 1-6, doi: 10.1109/COBCOM.2016.7593506.

Hamad, Z., Askar, S. (2021). Machine Learning Powered IoT for Smart Applications. *International Journal of Science and Business, 5*(3), 92-100.

Husain, B. H., Askar, S. (2021). Survey on Edge Computing Security. International Journal of Science and Business, 5(3), 52-60.

JOSHI, N. 2017. Distributed cloud storage with blockchain technology.

Keti, F., Askar, S. (2015). Emulation of Software Defined Networks Using Mininet in Different Simulation Environments. 6th International Conference on Intelligent Systems, Modelling and Simulation, Kuala Lumpur, 2015, pp. 205-210, doi: 10.1109/ISMS.2015.46.

KHALID, Z. M. & ASKAR, S. 2021. Resistant Blockchain Cryptography to Quantum Computing Attacks. International Journal of Science and Business, 5, 116-125.

Khalid, Z., Askar, S. (2021). Resistant Blockchain Cryptography to Quantum Computing Attacks. International Journal of Science and Business, 5(3), 116-125.

KSHETRI, N. 2017. Can blockchain strengthen the internet of things? IT professional, 19, 68-72.

KUMAR, N. M. & MALLICK, P. K. 2018. Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132, 1815-1823.

KUMARI, S., KARUPPIAH, M., DAS, A. K., LI, X., WU, F. & KUMAR, N. 2018. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. The Journal of Supercomputing, 74, 6428-6453.

LEE, B. & LEE, J.-H. 2017. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. The Journal of Supercomputing, 73, 1152-1167.

LI, D., PENG, W., DENG, W. & GAI, F. A blockchain-based authentication and security mechanism for IoT. 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018. IEEE, 1-6.

LI, Z., KANG, J., YU, R., YE, D., DENG, Q. & ZHANG, Y. 2017. Consortium blockchain for secure energy trading in industrial internet of things. IEEE transactions on industrial informatics, 14, 3690-3700.

LIU, H., ZHANG, Y. & YANG, T. 2018. Blockchain-enabled security in electric vehicles cloud and edge computing. IEEE Network, 32, 78-83.

LUNDBAEK, L.-N., D'IDDIO, A. C. & HUTH, M. 2016. Optimizing governed blockchains for financial process authentications. arXiv preprint arXiv:1612.00407.

MAGYAR, G. Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management. 2017 IEEE 30th Neumann Colloquium (NC), 2017. IEEE, 000135-000140.

MERKLE, R. C. A digital signature based on a conventional encryption function. Conference on the theory and application of cryptographic techniques, 1987. Springer, 369-378.

MINOLI, D. & OCCHIOGROSSO, B. 2018. Blockchain mechanisms for IoT security. Internet of Things, 1, 1-13.

MOCRII, D., CHEN, Y. & MUSILEK, P. 2018. IoT-based smart homes: A review of system architecture, software, communications, privacy and security. Internet of Things, 1, 81-98.

Mohammed, C. M., Askar, S. (2021). Machine Learning for IoT HealthCare Applications: A Review. International Journal of Science and Business, 5(3), 42-51.

MOHANTA, B. K., JENA, D., SATAPATHY, U. & PATNAIK, S. 2020. Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 100227.

MOINET, A., DARTIES, B. & BARIL, J.-L. 2017. Blockchain based trust & authentication for decentralized sensor networks. arXiv preprint arXiv:1706.01730.

OUADDAH, A., ABOU ELKALAM, A. & AIT OUAHMAN, A. 2016. FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and communication networks, 9, 5943-5964.

OUADDAH, A., ABOU ELKALAM, A. & OUAHMAN, A. A. 2017. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. Europe and MENA cooperation advances in information and communication technologies. Springer.

PANDEY, P. & LITORIYA, R. 2020. Securing and authenticating healthcare records through blockchain technology. Cryptologia, 44, 341-356.

PILKINGTON, M. 2016. Blockchain technology: principles and applications. Research handbook on digital transformations. Edward Elgar Publishing.

Qadir, G. A., Askar, S. (2021). Software Defined Network Based VANET. International Journal of Science and Business, 5(3), 83-91.

REYNA, A., MARTÍN, C., CHEN, J., SOLER, E. & DÍAZ, M. 2018. On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems, 88, 173-190.

RODRIGUES, B., BOCEK, T., LAREIDA, A., HAUSHEER, D., RAFATI, S. & STILLER, B. A blockchain-based architecture for collaborative DDoS mitigation with smart contracts. IFIP International Conference on Autonomous Infrastructure, Management and Security, 2017. Springer, Cham, 16-29.

ROY, S., ASHADUZZAMAN, M., HASSAN, M. & CHOWDHURY, A. R. Blockchain for iot security and management: Current prospects, challenges and future directions. 2018 5th International Conference on Networking, Systems and Security (NSysS), 2018. IEEE, 1-9.

Samann, Fady E. F., Zeebaree, S. RM, Askar, S. IoT Provisioning QoS based on Cloud and Fog Computing, Journal of Applied Science and Technology Trends, Vol. 2, No. 1, pp. 29-40.

SCEKIC, O., NASTIC, S. & DUSTDAR, S. 2018. Blockchain-supported smart city platform for social value co-creation and exchange. IEEE Internet Computing, 23, 19-28.

SRIVASTAVA, G., CRICHIGNO, J. & DHAR, S. A light and secure healthcare blockchain for iot medical devices. 2019 IEEE Canadian conference of electrical and computer engineering (CCECE), 2019. IEEE, 1-5.

Sulaiman, S., Askar, S. (2015). Invetigation of the Impact of DDoS Attack on Network Efficiency of the University of Zakho. Journal University of Zakho, Vol. 3(A) , No.2, Pp 275-280.

TESLYA, N. & RYABCHIKOV, I. Blockchain-based platform architecture for industrial IoT. 2017 21st Conference of Open Innovations Association (FRUCT), 2017. IEEE, 321-329.
WATANABE, H. 2018. Can Blockchain Protect Internet-of-Things? arXiv preprint arXiv:1807.06357.
XU, Q., JIN, C., RASID, M. F. B. M., VEERAVALLI, B. & AUNG, K. M. M. 2018. Blockchain-based decentralized content trust for docker images. Multimedia Tools and Applications, 77, 18223-18248.
YIN, W., WEN, Q., LI, W., ZHANG, H. & JIN, Z. 2018. An anti-quantum transaction authentication approach in blockchain. IEEE Access, 6, 5393-5401.
YUE, X., WANG, H., JIN, D., LI, M. & JIANG, W. 2016. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40, 1-8.
ZHANG, L., LI, H., SUN, L., SHI, Z. & HE, Y. Poster: towards fully distributed user authentication with blockchain. 2017 IEEE Symposium on Privacy-Aware Computing (PAC), 2017. IEEE, 202-203.
ZHANG, Y. & WEN, J. 2017. The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications, 10, 983-994.
ZYSKIND, G. & NATHAN, O. Decentralizing privacy: Using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops, 2015. IEEE, 180-184.

**Cite this article:**

**Shavan Askar, Zhwan Mohammed Khalid, Tarik A. Rashid** (2021). Blockchain For Securing IoT Devices: A Review. *International Journal of Science and Business, 5*(6), 209-224. doi: https://doi.org/10.5281/zenodo.5222704
Retrieved from http://ijsab.com/wp-content/uploads/757.pdf

# Published by

IJSAB International