**Issues in Information Systems**
Volume 23, Issue 4, pp. 170-182, 2022

DOI: https://doi.org/10.48009/4_iis_2022_115

# Challenges and solutions to blockchain-based management of IoT devices in smart cities

**Joshua Murphy,** *Robert Morris University, jxmst637@mail.rmu.edu*
**Sushma Mishra,** *Robert Morris University, mishra@rmu.edu*

## Abstract

The rapid development of urban cities has created a need for smart infrastructure and services which utilize the capabilities of internet of things devices. As the number of devices in an IoT ecosystem increases, there will become a tipping point when devices generate an extensive amount of data and become too resource-constrained to effectively enforce security and data privacy policies. Therefore, a distributed system such as blockchain must be used to manage the data and security of these devices. The following work discusses the importance of implementing blockchain for IoT security, privacy, and device management. Additionally, it reviews some of the current solutions regarding blockchain implementation with information heavy IoT devices, as well as suggests future topics of research to indicate areas of improvement.

**Keywords**: Blockchain, Internet of Things (IoT), Security, Device Management, Smart City.

## Introduction

In recent years, new developments in the Internet of Things (IoT) have enabled cities to adopt smart technologies to improve the quality of life, safety of all citizens, and overall efficiency of limited resources. As urban communities continue to adapt to the ever-increasing amount of technology available in order to handle both existing and upcoming obstacles, the more apparent it has become that the Internet of Things is most equipped to handle such challenges. Smart cities can use sensors and other IoT devices to manage energy and water needs more efficiently. Data gathered can also be used to decrease environmental pollution and better handle various weather conditions, as well as enhance transportation to generate faster traffic patterns for both public transit and citizens, while also improving parking lots by actively recording the number of available spaces (Arasteh et al, 2016). Smart cities also provide a higher level of safety through the implementation of a surveillance system (Bhushan et al, 2020). Due to the reliance on these devices in smart cities, it is necessary to prove data integrity and security in all domains.

IoT aims at creating a smart environment where devices are interoperable and can share gathered data with other devices and software systems. An IoT platform can consist of numerous physical objects usually controlled by a central system (Ashton, 2009). This centralized architecture is at a higher security risk due to it being a single point of failure. The problem created by a centralized server is the increased risk of security flaws, such as the release of sensitive information or the need for multiple management authorities. The immense amount of data produced from IoT devices must be secure to protect people's privacy.

Combining blockchain architecture with a peer-to-peer storage system can ensure privacy and the absence of a single point of failure (Conoscenti et al, 2016). In this framework, blockchain has the role of authenticating all actions performed on the confidential information of IoT devices such as the creation, modification, and deletion of data. Additionally, access controls can be implemented and enforced by the blockchain which could prevent abuse from unauthorized parties.

While there has been extensive research conducted into blockchain technology and smart cities, a majority of these studies focus on one aspect rather than the combination of both. Furthermore, studies that do analyze the relationship between blockchain and IoT mostly focus on a few characteristics instead of all facets of implementation. To bridge the connection between studies in separate realms of blockchain and IoT, this paper presents the challenges to implementation, as well as leading solutions to said challenges that highlight a successful blockchain network. Successful implementation of blockchain in IoT could prove beneficial to the safety and efficiency of civil services aided by technology in smart cities.

This paper is designed as a systematic literature review to study current research and applications of blockchain in IoT frameworks. I present a review of blockchain's role in addressing IoT weaknesses such as peer-to-peer communication, Thing management, data storage, and access controls. Furthermore, this paper identifies potential challenges to adopting a blockchain platform for IoT due to blockchain's inherent properties and provides possible solutions to these challenges. Section II explains background information on theories used in the literature including blockchain structure, the internet of things, and smart city architecture. Section III identifies common challenges with blockchain integration and IoT device management. The architectures and frameworks proposed to solve these challenges from various studies are presented in section IV. The key points from the reviewed papers are discussed in section V. Following in section VI is the conclusion paired with topics for future research. This literature review is based on the collection of 52 articles from leading publishers such as the Institute of Electrical and Electronics Engineers (IEEE), Association for Information Systems (AIS), and Association for Computing Machinery (ACM). Through searching for articles multiple topics were covered such as lightweight blockchain, access controls, smart cities, IoT device management, and IoT security.

## Background

### Blockchain

Before explaining the many architectures proposed in research, an overview of blockchain technology is needed to assist in later understanding the in-depth details and benefits of implementation in IoT frameworks. There are multiple definitions for blockchain but for this review, blockchain is defined as "a technology that enables immutability and integrity of data in which a record of transactions made in a system is maintained across several distributed nodes that are linked in a peer-to-peer network" (Viriyasitavat and Hoonsopon, 2019). In basic terms, a blockchain is a data structure similar to that of a linked list. The record of transactions created by the blockchain is called a ledger, which is shared with all participants of the blockchain network (Mendki, 2020). Transactions published to the ledger can be any exchange of information between two entities on the network (Novo, 2018). These participants of the blockchain are usually referred to as nodes or peers, whose job is to compute the complex cryptographic hashing algorithm of a new block of information to validate its integrity (Koteska et al, 2017). If the block is validated by a majority of the nodes on the network it is then appended to the blockchain making the information immutable (Casino et al, 2018).

Blockchain's decentralization assumes that the nodes in the network may be unreliable (Novo, 2018). Therefore, an essential function of blockchain is consensus, where peers on the network must mutually

agree on information to be added to the blockchain (Okada et al, 2017). Blockchain can be configured in two main different configurations, public and permissioned. The consensus protocol for a public blockchain is reasonably secure by nature, needing 51% of nodes to confirm a validation proposes that up to 50% of nodes can be malicious and still un-affect the system (Danko et al, 2019). However for permissioned blockchains where only authorized nodes can connect, a consensus of over two-thirds is needed to become trustworthy (Danko et al, 2019).

Voting-based consensus protocol has been established to provide the reliability of data and computation to systems despite malicious nodes acting on the network (Castro and Liskov, 2002). Permissioned blockchains use this same concept where it is assumed some nodes are controlled by bad actors. On this basis, a consensus can be achieved where there are $n$ nodes and at least $(2n -1) / 3$ number of nodes act honestly (Danko et al, 2019). In this context, devices acting honestly can be defined as providing the correct information to peers on the blockchain. Danko et al (2019) explain a blockchain concept where there are two different types of nodes called Leader and Validator. A randomly selected Leader will build a block of transaction information which is then distributed to Validator nodes for verification. Validators then check the integrity of the block, sign it, and distribute it to other Validator nodes. This process is repeated until Validators have gathered $n - 1$ versions of the block. If $(2n -1) / 3$ of the blocks are valid the Leader node then publishes the block to the blockchain.

Smart contracts are critical to many of the proposed blockchain architectures, due to their ability to create customized communication lines between devices and blockchain nodes. A smart contract is a transaction protocol intended to meet contractual obligations between two parties, which allows credible transactions without a third party (Novo, 2018). The smart contract is executed on a blockchain system when conditions are met to trigger it. Each participant adheres to the terms of the contract and automatically executes the script of the smart contract (Pesic et al, 2019). In a permissioned blockchain, smart contracts are only visible to the participant parties.

Business type blockchains are a contrast to previously mentioned configurations. This method is a newer smart contract-based blockchain that can be used in a variety of transaction types from ubiquitous devices, operation management, and intra-application data transfer (Biswas et al, 2019). For the adoption of this business blockchain, significant changes must be made to the generic blockchain protocol. Considering the necessity for changes to be made, a new permissioned blockchain has recently been developed called Hyperledger (Hyperledger, 2022). This new development introduces six new business frameworks of blockchain depending on technological requirements and the consensus algorithm needed (Cachin and Vukolic, 2017). Iftekhar et al (2021), presented a use case of Hyperledger Fabric to demonstrate managing access controls for IoT devices across separate organizations connected to the blockchain network.

**Internet of Things (IoT)**

The internet of things (IoT) is a concept of connected devices across large networks that possess a wide variety of functionality (Fan et al, 2018). These devices encompass more than just mobile phones or tablets, rather they can be CCTVs, drones, or any other smart device that has a level of processing or sensor capability (Alasbali, 2020). IoT is not solely defined by the connectivity of objects, but also by the interaction between these objects. One important aspect of IoT is the interoperability of a device. Interoperability is the capability of a system to work with or use other systems (Hatzivasilis et al, 2018). This capability is crucial for certain devices, for it allows devices to communicate with other devices outside their domain or from other manufacturers, which oftentimes is limited by middleware applications.
The rapid development of urban cities has created a need for infrastructure and services to provide essentials to citizens. Due to this need for improved infrastructure, there has been an emphasis on the use of digital

devices such as sensors, actuators, and smart objects. Integrating sensors and actuators, and the rapid development of wireless communication technologies have enabled low-cost objects to connect to the internet, resulting in increased deployment of IoT devices (Al-Turjman et al, 2019). Smart cities increase the quality of life for residents by using information technology and advanced data management. Infrastructure for smart cities includes interconnected systems and devices to benefit citizens in a variety of applications, such as healthcare, transportation, traffic systems, agriculture, and energy (Al-Turjman et al, 2019). Analyzing data from parking spaces and traffic patterns can produce decreased travel time through cities, while sensors for weather, water flow, and environmental pollution further enhance the ability of smart cities. With the assistance of the Internet of Things, governments are developing smart cities for their country's improvement in all sectors of life (Zhang et al, 2020). As more devices are implemented into smart cities, the data gathered from various sources grows rapidly. Storing this vast amount of information can be troublesome for developing cities, therefore IoT normally collaborates with large-scale processing and cloud technology to properly manage data storage (Xu et al, 2020).

Smart cities offer economic and social development to the public sector while indirectly improving the financial well-being and quality of life of city residents. A city incorporated with extensive IoT devices can store, sort, and exchange vast amounts of real-time data through interoperable devices. Data analysis of intelligent cities is expanding rapidly and can be used to control services, properties, and personnel while simultaneously enhancing city activities (Kumar et al, 2019). The communication between devices in smart cities is critical to the functionality of services and must be private and secured to limit the threat of misuse.

## Challenges

Through the review of literature, various challenges become apparent when analyzing blockchain designed for IoT devices. Several factors challenge adopting blockchain technology to improve IoT ecosystems like implementation cost, lack of resources, security threats, and many more described below.

### IoT Restrictions

As the number of devices in an IoT ecosystem increases, there will become a tipping point when the generated data will come from billions of devices that are too resource-constrained to enforce security and data privacy policies (Shammar et al, 2021). Therefore, adopting a distributed technology such as blockchain into IoT devices will provide an effective solution. Implementing a blockchain application to a large-scale system can be challenging as it requires technical expertise which can be costly (Wang et al, 2019). Furthermore, the adoption of these applications depends on the development of immense storage systems, wider bandwidth, and increased computational power (Dai and Vasarhelyi, 2017). The continuously increasing size of the blockchain is an issue. Current blockchain applications need large amounts of transactions to be processed which restricts system performance (Al-Jaroodi and Mohamed, 2019). Moreover, this large amount of data being processed requires extensive storage and computational resources (Dai and Vasarhelyi, 2017). As sensors and other edge devices have low computing power, additional nodes are needed to provide the necessary computational capabilities to execute blockchain processes (Lo et al, 2019). Another issue is latency, where a verified block is added to the ledger and each iteration increasingly becomes larger and more time-demanding (Wang et al, 2019).

### Security Issues

Although blockchain is regarded as a highly secure and immutable data structure, cyberattacks are still possible. Blockchain applications can be vulnerable to attacks such as data theft, spying, and denial of service (DOS) attacks (Al-Jaroodi and Mohamed, 2019). The most prominent attack against blockchain

systems is the 51% attack, in which a malicious actor gains control of more than 50% of the nodes on a blockchain and can then theoretically control the application and its future information (Wang et al. 2019). While this attack is close to impossible in large-scale blockchains with thousands of nodes, permissioned blockchains or architectures with lesser participants are more prone to this type of attack (Patel et al, 2017). One work conducted by Kouicem et al (2018) analyzed the security requirements for six major IoT applications. They provide approaches to security solutions with a multitude of technologies such as blockchain. The solutions are categorized into three realms of IoT described as confidentiality, availability, and privacy. The authors further defined privacy concerns into four categories: Data Tagging, Data Obfuscation, K-Anonymity Models, and Zero-Knowledge Proof. Contrarily, Frustaci et al (2018) described security threats against IoT devices using three distinct layers: perception, transportation, and application layers. Furthermore, they emphasized the security vulnerabilities of these layers using communication and network protocols. Authors from a separate work (Sengupta et al, 2019) take a different approach to defining IoT security. They classify attacks against IoT systems into four domains using the basis of attack technique: device, network, software, and data. Additionally, the authors link these attacks to one or more network layers in IoT architecture. Another vulnerability analysis was performed by Ling et al (2017) in their work featuring Edimax IP cameras. Through their analysis, multiple attacks were identified against these devices such as device scanning, brute force, and spoofing which would allow attackers to take control of cameras. With this control, attackers could obtain a vast array of information such as device passwords or MAC addresses.

## Review

### Blockchain Architecture

To accommodate the limitations of IoT in regard to the processing power and storage capabilities, the blockchain architecture implemented to connect these devices must be lightweight and inconsequential to the overall resource allocation of devices. Biswas et al (2019) propose a lightweight blockchain architecture that creates a local peer network to allow the blockchain ledger to be scaled across all peers. This framework comprises a Certification Authority (CA) and a local peer, which groups devices based on their application scenario. The local peers work as peers inside the organization while interacting with an anchor peer in the global blockchain network. Anchor peers are interconnected on the global blockchain and every peer maintains a respective ledger and smart contracts. This structure increases the transaction rate of peers and the scalability of anchor peers (Biswas et al, 2019). This framework also promotes inter-organizational transactions through the global blockchain of anchor peers. Another proposal is from Michelin et al (2020) where the blockchain architecture consists of three layers: sensing, transportation, and storage. This framework uses SpeedyChain, a permissioned blockchain optimized for real-time data sharing, due to the capabilities of allowing multiple transactions to be appended in existing blocks, as well as giving each device its respective block, therefore, reducing the transaction processing time (Michelin et al, 2018). Gateways are deployed in the transportation layer and are responsible for video streaming, blockchain maintenance, and data integrity. In this method, the only latency to devices is during the hash calculation of the video metadata which includes framerate, position, and time duration to prove integrity. In a scenario with 32 cameras per gateway, the total latency is only approximately eight milliseconds (Michelin et al, 2020).

### IoT Security Solutions

Blockchain is a favorable solution to IoT security due to its decentralized and distributed nature. Using blockchain to manage IoT devices offers a higher level of security which could not be achieved otherwise (Ali et al, 2019). There are recent studies with proposed solutions for securing these devices by

implementing blockchain technology. Fitwi et al. (2019) describe a framework where a lightweight blockchain-based privacy protection scheme is used for smart surveillance at the edge of a cloud network. Users are assigned different levels of access privileges from smart contracts to allow access to the data broadcasted from the cameras. This system implements privacy-preserving smart contracts that define access controls for accessing the videos without compromising the privacy of individuals (Fitwi et al, 2019). This framework discourages the leaking of videos by embedding information specific to viewers into the videos and subsequently publishing a log reference to the blockchain (Fitwi et al, 2019).

One model of an efficient lightweight integrated blockchain (ELIB) system proved to retain the security and privacy of IoT devices while eliminating unnecessary overhead. Mohanty et al (2019) presented a model deployed in a smart home environment to illustrate its applicability in various IoT scenarios. This model operates on three separate levels: consensus algorithm, certificateless cryptography (CC), and distributed throughput management (DTM). The first level restricts the number of new blocks created by cluster heads, while the CC reduces the computational overhead when ensuring new blocks are appended to the blockchain. The DTM is used to alter system variables dynamically to ensure the throughput of the public blockchain does not vary significantly from the load in the network. This model was tested using 20 cluster heads, each comprising numerous nodes. Mohanty et al (2019) state that their proposed ELIB attains a total of 50% saving in processing time compared to the baseline method with a minimum energy consumption of 0.07 MJ. This model also has a minimum 4500kB packet overhead while communicating with 20 cluster heads. The outcome of their experiment shows that this model produces maximum performance under several evaluation parameters (Mohanty et al, 2019). Furthermore, its application in IoT ecosystems offers an efficient technique for security and privacy, as well as computational complexity, bandwidth, and overhead.

Establishing secure connections between peer nodes and end-users is critical to distributed IoT applications. Therefore, a work proposed by Porambage et al (2014) explains a pervasive authentication protocol (PAuthKey) used in wireless sensor networks. This protocol obtains certificates from a cluster head and then establishes links between nodes and end-users. Through this, they claim that security is guaranteed in the application layer which ultimately protects against masquerade attacks or node compromise. Due to this protection, the proposed PAuthKey can defend against fake node injection attacks. Below, Figure 1 displays the challenges with blockchain implementation due to device capabilities, as well as possible implications. Figure 2 explains common security issues in IoT devices that can be reduced by using blockchain and their implications if not taken into consideration.

| Challenges | Literature support | Implications |
|---|---|---|
| Processing | Javaid et al, 2020; Pesic et al, 2019; | ● If IoT devices were to interact with the blockchain they would crash, cease communication, and be unable to function properly |
| Network Bandwidth | Xu et al, 2021; | ● Slow network performance, loss of data |
| Block Validation Latency | Majeed et al, 2021; Wang et al, 2019; Michelin et al, 2020; | ● Restrictions in the validation of data during the transaction process |
| Scalability | Alasbali et al, 2020; Biswas et al, 2019; Liang et al, 2017; | ● Could lead to centralization which would void the reason for implementing blockchain technology |
| Energy Consumption | Mohanty et al, 2019; | ● Increased costs to businesses that use immense IoT platforms and limitations in available energy |

**Figure 1: Device capabilities and blockchain implementation challenges and implications**

| Challenges | Literature support | Implications |
|---|---|---|
| Identity and Privacy | Majeed et al, 2021; Paul et al, 2019; Fitwi et al, 2019; Ali et al, 2019; | ● Attackers could obtain confidential information; data linking to specific individuals or devices |
| Fake Node Injection | Porambage et al, 2014; Xu et al, 2021; | ● Possibility of malicious actors inside of the network allowing access to data on the blockchain |
| DDOS Attack | Yin et al, 2018; Paul et al, 2019; Dorri et al, 2017; | ● Restricted access and downtime of devices. Could impose restrictions on block validation. |
| Sybil Attack | Airehrour et al, 2019; | ● Could incur a 51% attack, resulting in a malicious actor taking control of the blockchain network |
| Data Integrity | Liang et al, 2017; Danko et al, 2020; Michelin et al, 2020; Khan et al, 2020; | ● Restrict the ability to use collected data due to the possibility of corruption or compromise |

**Figure 2: Security issues and blockchain implementation challenges and implications**

## Discussion

Much of the reviewed literature uses blockchain's inherent properties to provide immutability and integrity to IoT devices and the data produced, while also leveraging the decentralized nature of blockchain along with smart contracts to manage Things and data.

Authors use blockchain infrastructure to resolve many of the challenges presented in IoT devices and communication. Firstly, as IoT devices generally have low computational and storage capabilities, there is a gap left for the heavy computations needed for block verification. Many solutions provided by studies use separate devices or servers to provide higher computational power for the blockchain. This infrastructure relieves the computational strain on Things and rather delegates specific devices to compute the hash algorithms. There is no single point of failure in this type of design, due to the computations and data being shared equally among devices in a peer-to-peer network that focuses on decentralization. One other solution provided is the delegation of smaller permissioned blockchain networks located within a parent blockchain network. Devices are grouped in smaller blockchains to limit the computation needed to validate blocks of information, while each smaller blockchain is linked to the global blockchain through an intermediary device (Biswas et al, 2019). Through this configuration resource requirements for validation decrease, and low-power devices are better suited for communication on blockchain networks.

Another use case of blockchain for IoT devices is enabling access controls across a large number of devices connected to the network. Authors implement access control policies and credentials through smart contracts based on the blockchain. In this way, devices do not need to be assigned individually and can autonomously configure access controls based on the smart contract distributed from the blockchain. Some studies use blockchain as Thing management, ensuring all devices are readily available and are in the same state as the blockchain. Ensuring all devices are in the same state promises integrity among all connected devices on the blockchain.

This literature review collected 52 articles from leading publishers such as the Institute of Electrical and Electronics Engineers (IEEE), Association for Information Systems (AIS), and Association for Computing Machinery (ACM), using a variety of keywords to search. These articles covered common topics such as lightweight blockchain, access controls, and IoT data management, although expanding the sample size of articles across more publishers and various topics could produce a more refined examination of blockchain's use in the IoT ecosystem. There were multiple limitations to this study, that if passed or resolved could produce improved results in the functionality of a blockchain platform used for IoT. The largest constraints throughout this study were the length of papers and the lack of availability in research journals and databases.

## Conclusion

This paper analyzed the current limitations presented by implementing a blockchain framework to better manage IoT devices in smart city ecosystems. The findings from this systematic literature review highlight the opportunities and challenges within the implementation of blockchain technology in IoT device platforms. The outcomes of this research improve understanding of smart city architecture to manage and secure IoT devices using blockchain. The main challenges to blockchain and IoT are privacy, lack of policy or standards, and Thing capabilities such as computational, storage, and interoperability. Efficiency and scalability are large issues to blockchain due to the large volume of data being gathered in pair with the low computational power of IoT devices. Taking these issues into consideration, a permissioned multi-layered blockchain rather than a public blockchain would be better suited for a smart city ecosystem. A permissioned blockchain will allow for better access controls to preserve authentication of data produced from IoT devices. While implementing a multi-layer system will assist in the computational requirements

of low-power devices by delegating validation tasks. Although blockchain technology is regarded as highly secure and presents promising use in all industries, there are unaddressed challenges that still lack sufficient research. Future empirical research should be conducted into the latency of communication between nodes in a large-scale solution, as well as the computational overhead in these strenuous scenarios. Research should also be done on the accessibility of end users under different access controls while on the blockchain, to ensure privacy and accessibility of data generated from IoT devices while eliminating possible misuse of the system. Blockchain offers promising use in managing IoT devices and improving security, which ultimately will create safer and more efficient smart cities.

## References

Airehrour, D., Gutierrez, J., & Ray, S. K. (2017). A testbed implementation of a trust-aware RPL routing protocol. 2017 27th International Telecommunication Networks and Applications Conference (ITNAC). https://doi.org/10.1109/atnac.2017.8215369

Alasbali, N., Azzuhri, S. R., & Salleh, R. (2020). A blockchain-based Smart Network for IOT-driven smart cities. *Proceedings of the 2020 2nd International Electronics Communication Conference*. https://doi.org/10.1145/3409934.3409957

Ali, J., Ali, T., Alsaawy, Y., Khalid, A. S., & Musa, S. (2019). Blockchain-based Smart-IOT Trust Zone Measurement Architecture. *Proceedings of the International Conference on Omni-Layer Intelligent Systems*. https://doi.org/10.1145/3312614.3312646

Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in Industries: A Survey. IEEE Access, 7, 36500–36515. https://doi.org/10.1109/access.2019.2903554

Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2019). An overview of security and privacy in Smart Cities' IOT Communications. Transactions on Emerging Telecommunications Technologies, 33(3). https://doi.org/10.1002/ett.3677

Arasteh, H., Hosseinnezhad, V., Loia, V., Tommasetti, A., Troisi, O., Shafie-khah, M., & Siano, P. (2016). IOT-based Smart Cities: A Survey. 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC). https://doi.org/10.1109/eeeic.2016.7555867

Ashton, K. (2009). That 'Internet of Things' thing. RFID J., 22(7), 99–114.

Bhushan, B., Khamparia, A., Sagayam, K. M., Sharma, S. K., Ahad, M. A., & Debnath, N. C. (2020). Blockchain for smart cities: A review of architectures, integration trends and future research directions. Sustainable Cities and Society, 61, 102360. https://doi.org/10.1016/j.scs.2020.102360

Biswas, S., Sharif, K., Li, F., Nour, B., & Wang, Y. (2019). A scalable blockchain framework for secure transactions in IOT. *IEEE Internet of Things Journal*, *6*(3), 4650–4659. https://doi.org/10.1109/jiot.2018.2874095

Cachin, C. (2017). Blockchains and consensus protocols: Snake oil warning. 2017 13th European Dependable Computing Conference (EDCC). https://doi.org/10.1109/edcc.2017.36

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, *36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

Castro, M., & Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems, 20(4), 398–461. https://doi.org/10.1145/571637.571640

Chhina, S., Chadhar, M., Vatanasakdakul, S., & Chetty, M. (n.d.). Challenges and opportunities for Blockchain Technology adoption: A systematic review. *ACIS*. https://doi.org/https://aisel.aisnet.org/acis2019/81

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the internet of things: A systematic literature review. 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). https://doi.org/10.1109/aiccsa.2016.7945805

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, *31*(3), 5–21. https://doi.org/10.2308/isys-51804

Danko, D., Mercan, S., Cebe, M., & Akkaya, K. (2019). Assuring the integrity of videos from Wireless-based IOT devices using blockchain. 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW). https://doi.org/10.1109/massw.2019.00016

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IOT. Proceedings of the Second International Conference on Internet-of-Things Design and Implementation. https://doi.org/10.1145/3054977.3055003

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). LSB: A lightweight scalable blockchain for IOT security and anonymity. Journal of Parallel and Distributed Computing, 134, 180–197. https://doi.org/10.1016/j.jpdc.2019.08.005

Fan, L., Gil-Garcia, J. R., Werthmuller, D., Burke, G. B., & Hong, X. (2018). Investigating blockchain as a data management tool for IOT devices in Smart City Initiatives. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*. https://doi.org/10.1145/3209281.3209391

Fitwi, A., Chen, Y., & Zhu, S. (2019). A lightweight blockchain-based privacy protection for smart surveillance at the edge. 2019 IEEE International Conference on Blockchain (Blockchain). https://doi.org/10.1109/blockchain.2019.00080

Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating critical security issues of the IOT World: Present and future challenges. IEEE Internet of Things Journal, 5(4), 2483–2495. https://doi.org/10.1109/jiot.2017.2767291

Gao, Y., Li, Y., & Jia, Y. (2019). Video computing across trust domains based on Blockchain. *Proceedings of the ACM Turing Celebration Conference - China*. https://doi.org/10.1145/3321408.3326693

Hatzivasilisv, G., Askoxylakis, I., Alexandris, G., Anicic, D., Bröring, A., Kulkarni, V., Fysarakis, K., & Spanoudakis, G. (2018, November). *The interoperability of things: Interoperable solutions as an enabler for IoT and web 3.0*. IEEE Xplore. https://ieeexplore.ieee.org/document/8514952

Hyperledger Foundation. (2021, December 29). http://www.hyperledger.org/projects

Iftekhar, A., Cui, X., Tao, Q., & Zheng, C. (2021). Hyperledger fabric access control system for internet of things layer in blockchain-based applications. Entropy, 23(8), 1054. https://doi.org/10.3390/e23081054

Javaid, U., Aman, M. N., & Sikdar, B. (2020). Defining trust in IoT environments via distributed remote attestation using blockchain. *Proceedings of the Twenty-First International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*. https://doi.org/10.1145/3397166.3412801

Khan, P., Byun, Y.-C., & Park, N. (2020). A data verification system for CCTV surveillance cameras using blockchain technology in Smart Cities. Electronics, 9(3), 484. https://doi.org/10.3390/electronics9030484

Koteska, B., Karafiloski, E., & Mishev, A. (2017). *SQAMIA 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications*, *11*.

Kouicem, D.E.; Bouabdallah, A.; Lakhelf, H.; 2018. Internet of things security: a top-down survey. http://www.sciencedirect.com/science/article/pii/S138912861801208

Kumar, G., Saha, R., Rai, M. K., Thomas, R., & Kim, T.-H. (2019). Proof-of-work consensus approach in Blockchain Technology for cloud and fog computing using maximization-factorization statistics. IEEE Internet of Things Journal, 6(4), 6835–6842. https://doi.org/10.1109/jiot.2019.2911969

Liang, X., Zhao, J., Shetty, S., & Li, D. (2017). Towards data assurance and resilience in IOT using blockchain. MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM). https://doi.org/10.1109/milcom.2017.8170858

Ling, Z., Liu, K., Xu, Y., Fu, X. 2017. An end-to-end view of IoT security and privacy. IEEE Global Communications Conference, pp. 1-7.

Lo, S. K., Liu, Y., Chia, S. Y., Xu, X., Lu, Q., Zhu, L., & Ning, H. (2019). Analysis of Blockchain Solutions for IOT: A systematic literature review. IEEE Access, 7, 58822–58835. https://doi.org/10.1109/access.2019.2914675

Majeed, U., Khan, L. U., Yaqoob, I., Kazmi, S. M. A., Salah, K., & Hong, C. S. (2021). Blockchain for IOT-based smart cities: Recent advances, requirements, and future challenges. Journal of Network and Computer Applications, 181, 103007. https://doi.org/10.1016/j.jnca.2021.103007

Mendki, P. (2019). Blockchain enabled IOT edge computing. *Proceedings of the 2019 International Conference on Blockchain Technology*. https://doi.org/10.1145/3320154.3320166

Michelin, R. A., Dorri, A., Steger, M., Lunardi, R. C., Kanhere, S. S., Jurdak, R., & Zorzo, A. F. (2018). Speedychain. *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. https://doi.org/10.1145/3286978.3287019

Michelin, R., Ahmed, N., Kanhere, S., & Jurdak, R. (2020, May). *Leveraging lightweight blockchain to establish data integrity for surveillance cameras*. IEEE Xplore. https://ieeexplore.ieee.org/document/9169429/

Mohanty, S. N., Ramya, K. C., Rani, S. S., Gupta, D., Shankar, K., Lakshmanaprabu, S. K., & Khanna, A. (2019). An efficient lightweight integrated blockchain (ELIB) model for IOT security and privacy. Future Generation Computer Systems, 102, 1027–1037. https://doi.org/10.1016/j.future.2019.09.050

Novo, O. (2019). Scalable Access Management in IOT using blockchain: A performance evaluation. IEEE Internet of Things Journal, 6(3), 4694–4701. https://doi.org/10.1109/jiot.2018.2879679

Okada, H., Yamasaki, S., & Bracamonte, V. (2017). Proposed classification of blockchains based on authority and Incentive Dimensions. 2017 19th International Conference on Advanced Communication Technology (ICACT). https://doi.org/10.23919/icact.2017.7890159

Patel, D., Bothra, J., & Patel, V. (2017). Blockchain exhumed. 2017 ISEA Asia Security and Privacy (ISEASP). https://doi.org/10.1109/iseasp.2017.7976993

Paul, R., Baidya, P., Sau, S., Maity, K., Maity, S., & Mandal, S. B. (2019). IOT based secure smart city architecture using blockchain. 2018 2nd International Conference on Data Science and Business Analytics (ICDSBA). https://doi.org/10.1109/icdsba.2018.00045

Pešić, S., Tošić, M., Iković, O., Radovanović, M., Ivanović, M., & Bošković, D. (2019). Conceptualizing a collaboration framework between blockchain technology and the internet of things. *Proceedings of the 20th International Conference on Computer Systems and Technologies*. https://doi.org/10.1145/3345252.3345279

Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., Ylianttila, M. 2014. PAuthKey: a pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications. https://doi.org/10.1155/2014/357430.

Sengupta, J., Ruj, S., Bit, S. 2019. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. https://doi.org/10.1016/j.jnca.2019.102481

Shammar, E. A., Zahary, A. T., & Al-Shargabi, A. A. (2021). A survey of IOT and Blockchain Integration: Security perspective. IEEE Access, 9, 156114–156150. https://doi.org/10.1109/access.2021.3129697

Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, *13*, 32–39. https://doi.org/10.1016/j.jii.2018.07.004

Wang, H., Chen, K., & Xu, D. (2016). A maturity model for blockchain adoption. Financial Innovation, 2(1). https://doi.org/10.1186/s40854-016-0031-z

Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: A Systematic Literature Review and Research Agenda. *Supply Chain Management: An International Journal*, *24*(1), 62–84. https://doi.org/10.1108/scm-03-2018-0148

Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IOT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452–10473. https://doi.org/10.1109/jiot.2021.3060508

Xu, X., Han, M., Nagarajan, S. M., & Anandhan, P. (2020). Industrial internet of things for smart manufacturing applications using hierarchical trustful resource assignment. Computer Communications, 160, 423–430. https://doi.org/10.1016/j.comcom.2020.06.004

Zhang, R., V E, S., & Jackson Samuel, R. D. (2020). Fuzzy Efficient Energy Smart Home Management System for Renewable Energy Resources. Sustainability, 12(8), 3115. https://doi.org/10.3390/su12083115