CZ4171: Internet of Things – Networks and Communications

Sofia Ingrid Rodriguez Granqvist

N2202550J

Blockchain for IoT

Table of Contents

1. Introduction

Blockchain and Internet of Things (IoT) are two of the most ground-breaking and disruptive technologies of our time. IoT has transformed the way the physical and digital worlds interact, facilitating the collection and analysis of large amounts of data. Blockchain technology has enabled a secure and transparent way to store and transfer value. The integration of blockchain and IoT has the potential to provide enhanced security, privacy and efficiency, among other benefits, for IoT applications.

This paper will give an introduction to the blockchain and IoT architectures, and the need for the convergence of these two technologies. It will cover the challenges faced by IoT applications and how the implementation of blockchain can address these issues and provide efficient solutions for them. The paper will also cover technical aspects of its implementation such as smart-contracts for blockchain-based IoT applications, the interoperability of blockchain and IoT protocols, and decentralized data storage in this context. We will also discuss some use cases of blockchain-based IoT applications such as supply chain management, healthcare and smart grids.

Finally, we will discuss the scalability, potential and challenges that result from blockchain in IoT and explore the future directions for research and growth of this technology.

2. Literature Review

2.1. Introduction to Blockchain Architecture

Blockchain, at its core, refers to a decentralized, distributed ledger, designed to provide a secure and transparent way to store and transfer value, without the need for intermediaries or trusted third parties. It is designed as a sequence of blocks, linked together in a chronological order, to form a continuous chain (Ali Syed et al., 2019).

Nodes are the individual devices or computers that participate in the network by verifying and storing the data. In most blockchain networks, each one has a copy of the entire ledger, which is being constantly updated.

Each block in the chain consists of a block header and a block body. The block header contains a hash that identifies it and points to the previous block on the chain. The block body is composed of transactions and a transaction counter. These transactions have to be validated by the majority of the nodes in the network through distributed consensus algorithms, before being added to a block, and appended to the chain. This makes altering or manipulating the chain very difficult, ensuring its integrity. In addition, asymmetric cryptography is used to ensure the consistency and security of the blockchain).

Finally, blockchain facilitates the execution of programs, called smart contracts that codify rules, conditions, and business logic among two or more parties without the need for a trusted party (Yánez et al., 2021). The code of the smart-contracts is stored on the blockchain and is triggered by a transaction that meets the specifications and requirements of the contract. This is a feature of some blockchain architectures that can provide benefits such as increased transparency, efficiency and security (Zheng et al., 2017).

Some blockchain applications include cryptocurrencies, supply chain management, Decentralized Finance (DeFi), digital identity, energy trading, etc.

2.2. Introduction to IoT Architecture

Internet of Things (IoT) refers to a network of Internet-connected devices that are empowered with computing capability. IoT devices need to communicate with each other, collect and share data, and perform tasks without the need for physical contact. IoT devices can be sensors, smart appliances or wearables, among others, and has applications throughout various industries such as transportation, manufacturing and healthcare. At its core, IoT architecture includes a physical layer, a network layer and an application layer.

The physical layer is composed by sensors and actuators that interact with the physical world. They are responsible for capturing data from the environment and converting the physical signals into digital data, that will then be transmitted and analysed.

The network layer, also known as the middleware layer, is responsible for the transmission of the data between the physical layer and the application layer. This layer ensures the safe and reliable transmission of the data through various protocols, gateways and cloud services, facilitating the interaction between devices and the cloud.

Finally, the application layer, or service layer, is responsible for the analysis of the collected data through analysis and machine learning algorithms. The algorithms are used to detect patterns or anomalies and make predictions to provide meaningful insights and make decisions on the collected data. The application layer is also responsible for providing a user interface to interact with the IoT devices and control them remotely.

Additionally, IoT makes use other technologies to ensure scalability, reliability and security of the system. Some of these technologies include cloud computing, edge computing, big data analytics, cybersecurity measures, etc.

IoT enables the collection and real-time analysis of vast amounts of data. This could result in improved operational efficiency, enable new business models, reduce costs and improve customer experiences, transforming industries and improving quality of

life. On the other hand, there are trade-offs and challenges that have yet to be dealt with, such as security and privacy concerns, interoperability issues, ethical concerns and need for regulations. (Islam et al., 2023)

2.3. The Role of Blockchain in Addressing the Limitations of IoT

IoT systems also have limitations that need to be overcome for the scalability of the technology and its implementation in certain industries. Some of these limitations include the security and privacy issues that arise in some IoT applications, as well as the interoperability and scalability of these systems.

The integration of IoT devices into the standard internet has introduced a variety of privacy and security challenges, owing to the fact that many traditional internet protocols and technologies were not originally designed to support IoT systems, and therefore, they might not be well-suited to meet their security and privacy requirements. Also, IoT devices usually have to work in harsh, erratic and even intimidating surrounding environments, where they are vulnerable to various security breaches (Krishna & Gnanasekaran, 2017). Furthermore, if information and data authentication are exclusively reliant on a central server for inter-device communication, the reliability of device interconnectivity is compromised. This can result in the sharing of erroneous authentications and enable device spoofing, ultimately leading to insecure data flow (Kumar & Mallick, 2018). By using cryptographic techniques to secure data, blockchain can enable users to control access to their data and ensure that it is only shared with authorized parties. It develops data privacy for clients connected to the framework by utilizing hashing procedures in information blocks. At the same time, the decentralized nature of blockchain ensures that all data transactions are recorded on a public ledger, providing a transparent and immutable record of all data exchanges. As a result, IoT devices would have the ability to function autonomously without relying on centralized servers, thereby mitigating the potential for downtime and augmenting the dependability and openness of IoT applications (Chi et al., 2020).

IoT networks are data-centric, where data are uploaded by a large number of end devices. This makes both data and devices be the targets of potential attacks on IoT. Sensory data in an IoT system can be personal or sensitive (Wang et al., 2019).

Furthermore, the implementation of blockchain can improve the interoperability of IoT systems by creating a standardized platform for data exchange. This standardized platform can facilitate seamless communication and interaction between different devices, regardless of their underlying technologies (Kumar & Mallick, 2018).

The framework’s goal is to provide safe data at the right place, in a suitable format, and real-time on a device. Blockchain will facilitate transaction processing, resolve or eliminate crises, and build a flexible environment for running physical things.

Overall, the role of blockchain in addressing the limitations of IoT is significant. The convergence of these technologies can extend company potential and introduce new marketplaces in which anybody or everything can connect in real-time in a decentralized device with authenticity, privacy, and security. Leveraging the interoperability and transparency benefits of blockchain has the potential to alter future IoT conversations.

2.4. Blockchain-enabled IoT Systems (BC-IoT): Overview and Challenges

The incorporation of Blockchain into IoT systems is not trivial and introduces several challenges. Some of the challenges involve storage capacity and scalability, security, smart contracts, and legal issues.

It is known that some current blockchain implementations can only process a few transactions per second. In IoT systems, devices can generate gigabytes of data in real time. This limitation could be a potential bottleneck in the integration of these two technologies (Reyna et al., 2018). This issue can be addressed with the use of techniques to compress and filter the large volumes of data generated by IoT devices, since the majority of times only a small part of it provides useful information.

Regarding the security of the system, Blockchain can ensure that data in the chain is immutable, making it tamper-proof. But this could introduce a reliability problem if the data generated by the IoT devices is corrupt before it is recorded on the ledger. Corrupt data can arise from many situations apart from malicious ones, since IoT devices can be located in harsh environments (Reyna et al., 2018).

Additionally, to incorporate smart contracts in these systems, there are some challenges that should be taken into account. IoT systems present some heterogeneity constraints that smart contracts should take into account. These systems are complex and often include a variety of devices and protocols, which may not be compatible with each other. Filtering and group mechanisms can be used to adapt the smart contracts to the context and requirements of the IoT system.

Finally, in addition to the technical issues that can arise in the convergence of IoT systems and Blockchain, there are some legal aspects that should be considered. In the context of IoT, the laws that deal with privacy and handling of data are still to be revised and improved, in order to implement this technology in areas that deal with personal and confidential data. The absence of a central authority in blockchain applications, such as Bitcoin, has generated a lot of disputes (Elwell et al., 2015). Legal implications in the context of currencies are an important concern, as they can directly and negatively affect blockchain applications (Reyna et al., 2018). As a result, the combination of these two technologies implies a big challenge in the context of anonymity, privacy and data protection.

3. Convergence Models for BC-IoT

Convergence models refer to the methods and architectures that can be used in the integration of blockchain technology with IoT systems. The approaches to the convergence of these two technologies can be broadly divided into three categories of architecture designs: IoT Peer to IoT Peer (P2P) (Fig 1. (a)), IoT Peer to Blockchain (P2B) (Fig 1. (b)) and a Hybrid Architecture (Fig 1. (c)).

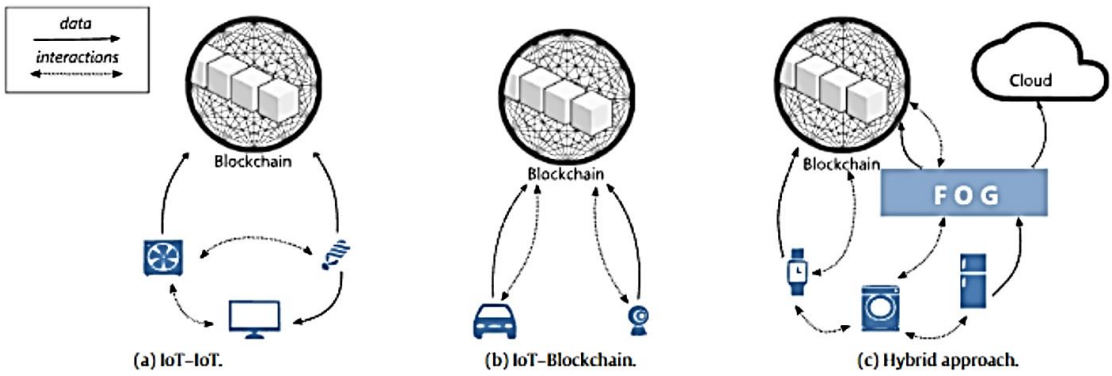

Figure 1. BC-IoT convergence models
(Reyna et al., 2018)

3.1. IoT Peer-to-Peer (P2P)

IoT Peer-to-Peer (P2P) architecture is a decentralized architecture that allows IoT devices to communicate directly with each other without the need for intermediaries such as cloud servers.

IoT sensors collect sensory data and interact with Blockchain services. This communication could be done through Blockchain agents. These agents will not take part in the Blockchain network. Instead, they will interpret the collected sensory data as transactions, and broadcast them into the network (Wang et al., 2019).

Blockchain technology is used to provide a secure and transparent way to store and share data generated by IoT devices. In this case, only the metadata of transactions between IoT peer devices is stored on the blockchain, while all other data is transferred between IoT peer devices directly (Nartey et al., 2021).

The P2P architecture provides a more scalable system as it enables IoT devices to communicate directly with each other. As a result, enabling this communication requires extensive routing and discovery techniques, to ensure that the data from one IoT peer device find its way to the other IoT peer device efficiently (Nartey et al., 2021). This convergence method is implemented in scenarios that require low latency and high performance, since it can work offline (Reyna et al., 2018).

In addition, it is most suitable for situations in which devices fall under a single domain or are located in the same area or network, as it would reduce the complexity of discovery and routing required.

3.2. IoT Peer-to-Blockchain (P2B)

In this architecture, IoT devices do not have a direct link or means of connection between each other, and all interactions and communications are done via the blockchain. This approach enables an immutable record of interactions, which makes them traceable, as their details can be queried in the blockchain, increasing the autonomy of IoT devices (Reyna et al., 2018).

The architecture consists of full nodes and light nodes. Full nodes store all the blocks on the blockchain, including block headers and block bodies, and are responsible for validating transactions and ensuring that the network rules are being followed, while light nodes store only the block headers and do not participate in block mining (Wang et al., 2019).

IoT devices would join the Blockchain network and be part of the core functions of Blockchain, such as generating transactions of raw sensory data, verifying transactions, and even mining blocks.

In IoT systems, devices with high computation capabilities (i.e., Raspberry Pi) can operate as full nodes while the resource-constrained devices (i.e., Arduino) can act as lightweight nodes. Specifically, the full nodes transmit the transactions from the lightweight nodes to the blockchain. The non-blockchain nodes are devices with limited capacity that cannot act as full or lightweight client and must connect to a trusted remote node (Yánez et al., 2021).

Overall, this approach is most suitable for systems that require network efficiency, since the communication between sensors and the intermediary server can be done using Wi-Fi or short-range radio, which reduces bandwidth consumption. It also provides low latency, since the data offload operation is done in the intermediary server, which is located in single-hop proximity to IoT devices (Yánez et al., 2021).

Finally, since the data is processed locally within the IoT network, there can be better control of the levels of security and privacy.

3.3. Hybrid Architecture

The hybrid approach of integrating blockchain technology with IoT systems combines the benefits of both IoT Peer-to-Peer (P2P) architecture and IoT Peer-to-Blockchain (P2B) architecture.

In this approach, only part of the interactions and data take place in the blockchain, while the rest are directly shared between the IoT devices. Fog computing can be used to complement the limitations of blockchain and the IoT system (Fig 1. (c)). It can help to reduce the energy consumption and computational load needed by IoT

devices. It can also help to alleviate some of the bandwidth and latency issues. It also provides a platform for AI algorithms to run, which can help to make critical decisions about these IoT peer devices (Nartey et al., 2021).

The strength of this design is that not all IoT interactions would go straight to the blockchain. This means all blockchain interactions would be done by the fog computing layer, as well as serve as nodes on the blockchain, which provides an extra source of redundancy (Nartey et al., 2021).

Overall, the hybrid architecture design enables the creation of a more robust and secure system by leveraging the strengths of both architectures and the power of technologies such as artificial intelligence and fog computing (Reyna et al., 2018)..

Finally, one of the challenges to take into account in this approach is choosing which interactions should go through the blockchain and providing the way to decide this in run time.

4. Applications of BC-IoT

Although the use of blockchain in the IoT is relatively recent, there are a number of areas where this technology is used in different ways to improve current IoT technology. BC-IoT can be widely used to support a number of industrial applications. Although there are many other applications, this paper discusses a few examples where these technologies can be used in, such as supply chain management, health care and smart grids.

A) Supply chain management

A product is often comprised of multiple components, sourced from various manufacturers which could be located in different geographical regions. Unfortunately, some forged or low-quality parts may infiltrate the supply chain, making it challenging to identify and prevent them. Implementing anti-fraud technologies across all components of a product can be costly. However, integrating blockchain and Internet of Things (IoT) technology can provide a viable solution. By assigning a unique ID and immutable timestamp to each component at the point of creation, it is possible to establish a tamper-resistant and traceable identification system for all components. This data can then be securely recorded in a blockchain (Ali et al., 2019).

Additionally, BC-IoT can be leveraged to reduce costs in post-sale services within the supply chain management process, as well as reduce the risk in the supply chain management (Kshetri, 2018).

B) Healthcare

IoT devices such as wearables, can be used to measure and collect healthcare data, such as heart rate, blood sugar, and blood pressure readings. This data can be accessed by healthcare professionals and teams from anywhere via healthcare networks, improving patient care. However, the storage and sharing of healthcare data raises concerns regarding privacy and security. Healthcare devices are vulnerable to cyber threats, and

healthcare networks are often heterogeneous, making it difficult to maintain privacy and security (Dai et al., 2019).

Incorporating blockchain technology into healthcare networks has the potential to address these challenges, since it enables a tamper-resistant and secure network for storing and sharing healthcare data (Dai et al., 2019).

In particular, blockchain technologies can be used to create decentralized data repositories that enable the secure and private storage of sensitive information, such as personal data. These repositories provide complete control to the data owner and follow strict standards like the Health Insurance Portability and Accountability Act (HIPAA) or the European Data Protection Directive (Ali et al., 2019).

Overall, the integration of blockchain technology into healthcare networks offers an innovative solution for ensuring the privacy and security of healthcare data (Griggs et al).

C) Smart Grid

The emergence of distributed renewable energy resources has revolutionized the role of energy consumers, turning them into "prosumers" who can both consume and generate energy, particularly from renewable sources. Energy prosumers can sell excess energy to other consumers, which is known as P2P energy trading (Zhang et al., 2018). However, ensuring secure and trusted energy trading between two parties in a distributed environment is a challenge.

Blockchain technology has the potential to ensure secure and transparent P2P energy trading. For instance, a secure energy trading system based on consortium blockchains, where nodes from multiple organizations or enterprises govern the network with far more privacy (Zhong et al., 2020). This be used to enable trading parties to reach a consensus without a central broker, reducing trading costs (Li et al., 2017).

Furthermore, smart contracts can be used to automate the process of managing energy demand, which reduces the need for intermediaries and increases transparency (Pop et al., 2018).

Overall, the integration of blockchain technology into energy trading can provide a secure and cost-effective solution for P2P energy trading, enabling prosumers to monetize their excess energy and increase the use of renewable energy sources.

5. Future Research directions

While blockchain-based IoT applications have shown immense potential, there are still several research gaps that need to be addressed to fully realize their benefits. As a result, despite its major advantages, there are multiple challenges introduced in the adoption of Blockchain in the IoT. These challenges involve scalability, security and utilizing blockchains in scenarios involving devices with limited capabilities.

Scaling blockchains remains a huge issue in their implementation in digital finance and beyond, due to their high performance and networking overhead (Ali et al., 2019). As mentioned before, IoT devices generate large amounts of data, which results in a scalability issue for certain BC-IoT applications. Research is needed to adapt these systems to the scalability constraint introduced with blockchains.

Additionally, a key future research direction is to extend blockchains to the IoT edge. The challenge in this research direction would be to enable IoT devices and gateways to push transactions to the blockchain using light clients, without creating centralized block validation pools (Dorri et al., 2017). There is also a need for standards and protocols to ensure interoperability between different blockchain-based IoT systems, allowing them to exchange data and information seamlessly.

Furthermore, blockchain provides a tamper-proof system to store data, but the data could be previously corrupted during the collection process by the IoT devices. Also, there is a need to develop security standards for scripting smart contracts in such a way that there are no loopholes that compromise the security of the devices in the IoT network (Ali et al., 2019). As a result, research is needed to develop new security mechanisms to protect IoT devices and ensure the security of blockchain-based IoT systems.

Finally, another investigation area could involve the development of energy-efficient approaches to enable the convergence of these systems, since they require significant computational power.

6. Conclusion

This paper surveyed the basic architectures and applications of Blockchain Technology and IoT systems, and the integration of the two technologies (BC-IoT). IoT presents limitations, regarding scalability, security, privacy and centralized data storage, which can potentially be overcome with the implementation of Blockchain into these systems. This paper explains the role of Blockchain in addressing these issues, and categorizes the different convergence models for BC-IoT systems. These convergence models can be broadly categorized into three different approaches: IoT Peer to IoT Peer (P2P), IoT Peer to Blockchain (P2B) and a Hybrid Architecture. This paper then covers some use-cases of BC-IoT systems, such as its potential applications in supply chain management, healthcare and smart grids. Finally, the paper covers the challenges involving energy viable scalability, data consistency and interoperability, and legal concerns that emerge from the integration of these two technologies, and future research directions that need to be explored in order to achieve the full potential of IoT.

7. References

1. Ali Syed, T., Alzahrani, A., Jan, S., Siddiqui, M. S., Nadeem, A., & Alghamdi, T. (2019). A comparative analysis of blockchain architecture and its applications: Problems and recommendations. IEEE Access, 7, 176838–176869. https://doi.org/10.1109/access.2019.2957660

2. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, Consensus, and future trends. 2017 IEEE International Congress on Big Data (BigData Congress). https://doi.org/10.1109/bigdatacongress.2017.85
3. Islam, M. M., Nooruddin, S., Karray, F., & Muhammad, G. (2023). Internet of things: Device capabilities, architectures, protocols, and smart applications in Healthcare Domain. IEEE Internet of Things Journal, 10(4), 3611–3641. https://doi.org/10.1109/jiot.2022.3228795
4. Ghovanlooy Ghajar, F., Sikora, A., & Welte, D. (2022). Schloss: Blockchain-based system architecture for secure industrial IOT. Electronics, 11(10), 1629. https://doi.org/10.3390/electronics11101629
5. Qushtom, H., Mišić, J., Mišić, V. B., & Chang, X. (2022). A high performance two-layer consensus architecture for Blockchain-based IOT Systems. Peer-to-Peer Networking and Applications, 15(5), 2444–2456. https://doi.org/10.1007/s12083-022-01363-y
6. Yánez, W., Bahsoon, R., Zhang, Y., & Kazman, R. (2021). Architecting Internet of things systems with Blockchain. ACM Transactions on Software Engineering and Methodology, 30(3), 1–46. https://doi.org/10.1145/3442412
7. Chi, J., Li, Y., Huang, J., Liu, J., Jin, Y., Chen, C., & Qiu, T. (2020). A secure and efficient data sharing scheme based on blockchain in Industrial Internet of Things. Journal of Network and Computer Applications, 167, 102710. https://doi.org/10.1016/j.jnca.2020.102710
8. 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. https://doi.org/10.1016/j.future.2018.05.046
9. C.K. Elwell, M.M. Murphy, M.V. Seitzinger, Bitcoin: questions, answers, and analysis of legal issues, Congressional Research Service, 2013. Available on-line: https://fas.org/sgp/crs/misc/R43339.pdf. (Accessed 1 February 2018)
10. Krishna, B. V., & Gnanasekaran, T. (2017). A systematic study of security issues in internet-of-things (IOT). 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). https://doi.org/10.1109/i-smac.2017.8058318
11. Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IOT. Procedia Computer Science, 132, 1815–1823. https://doi.org/10.1016/j.procs.2018.05.140
12. Paredes, J. N., Simari, G. I., Martinez, M. V., & Falappa, M. A. (2021). Detecting malicious behavior in social platforms via hybrid knowledge- and data-driven systems. Future Generation Computer Systems, 125, 232–246. https://doi.org/10.1016/j.future.2021.06.033
13. Nartey, C., Tchao, E. T., Gadze, J. D., Keelson, E., Klogo, G. S., Kommey, B., & Diawuo, K. (2021). On Blockchain and IOT integration platforms: Current implementation challenges and future perspectives. Wireless Communications and Mobile Computing, 2021, 1–25. https://doi.org/10.1155/2021/6672482
14. Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for internet of things. Computer Communications, 136, 10–29. https://doi.org/10.1016/j.comcom.2019.01.006
15. Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2019). Applications of blockchains in the internet of things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2), 1676–1717. https://doi.org/10.1109/comst.2018.2886932

16. Kshetri, N. (2018). 1 blockchain's roles in Meeting Key Supply Chain Management Objectives. International Journal of Information Management, 39, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005
17. K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," J. Med. Syst., vol. 42, no. 7, p. 130, Jun. 2018. [Online]. Available: https://doi.org/10.1007/s10916–018-0982-x
18. Zhang, C., Wu, J., Zhou, Y., Cheng, M., & Long, C. (2018). Peer-to-peer energy trading in a microgrid. Applied Energy, 220, 1–12. https://doi.org/10.1016/j.apenergy.2018.03.010
19. 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, 1–1. https://doi.org/10.1109/tii.2017.2786307
20. Zhong, B., Wu, H., Ding, L., Luo, H., Luo, Y., & Pan, X. (2020). Hyperledger fabric-based consortium blockchain for Construction Quality Information Management. Frontiers of Engineering Management, 7(4), 512–527. https://doi.org/10.1007/s42524-020-0128-y
21. Pop, C., Cioara, T., Antal, M., Anghel, I., Salomie, I., & Bertoncini, M. (2018). Blockchain based decentralized management of demand response programs in Smart Energy Grids. Sensors, 18(2), 162. https://doi.org/10.3390/s18010162
22. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IOT security and privacy: The case study of a smart home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). https://doi.org/10.1109/percomw.2017.7917634