A Survey of Blockchain Applications in IoT Systems

Diaa A. Noby and Ahmed Khattab
Electronics and Electrical Communications Engineering Department
Faculty of Engineering
Cairo University, Giza, 12613, Egypt
eng.diaa.elnoby@gmail.com, akhattab@ieee.org

***Abstract*—This paper presents an extensive study of the different ways the Internet of Things (IoT) applications exploit the recently developed blockchain technology. Even though the blockchain technology was originally presented as a security mechanism, its numerous benefits such as decentralization, immutability, persistence, anonymity and auditability can be used by IoT systems in different ways. More specifically, we classify the ways IoT systems exploit blockchain into three categories: resource management, decentralized information sharing, and IoT security. The comprehensive study of the applications of the blockchain technology in the different IoT domains presented in this paper sheds the light on the future research directions in the integration of the two technologies.**

***Index Terms*—Blockchain, Internet of Things (IoT), Distributed Systems**

I. Introduction

Recently, the Internet of Things (IoT) has become prevalent in our modern societies. IoT refers to the network of physical objects that are connected to the Internet as defined by ITU [1]. The IoT structure is composed of **(1) Things**: which are uniquely identifiable nodes, most often are sensors and actuators, that communicate without human intervention using various connectivity methods. **(2) Gateways**: which are network nodes used to connect two different networks protocols, thereby acting as intermediaries between the network nodes and the cloud. **(3) Network Infrastructure**: which are a set of devices that provide the connections between nodes and secure the data flow (e.g., repeaters, aggregators, and routers). **(4) Cloud Infrastructure**: which refers to the computational tools available to the IoT network. Such resources can be either software programs and user interfaces or hardware components such as virtual servers and storage. In the upcoming years, a massive evolution of the IoT is expected according to Gartner [2]. Therefore, there is a need to provide confidence and security in these devices considering the huge amount of incoming information.

In 2008, the concept of blockchain has been introduced by Satoshi Nakamato [3]. It was originally proposed for the electronic currencies such as Bitcoin[1] as a distributed public ledger technology. As a paradigm shift that transforms the centralized network topology into a peer-to-peer (P2P) topology in distributed data networks, blockchain has recently received much attention [4]–[7]. By enabling distributed environments, the blockchain technology transforms the major IoT application areas in which trusted transactions in an unknown society is needed. Combining the blockchain technology with IoT systems has numerous benefits such as providing robustness against threats and attacks, reducing the operation cost, and managing the resources in a decentralized manner.

This paper focuses on the relationship between the blockchain technology and IoT systems, investigates the challenges in integrating blockchain with IoT applications, discusses the current IoT and blockchain applications and focuses on the benefits of combining them. We accordingly classify the most relevant researches to demonstrate the various ways to improve IoT applications through the use of blockchains.

The organization of the rest of the paper is as follows. The basics of the blockchain technology and the blockchain structure are explained in Section II. In Section III, we classify the various blockchain applications in IoT systems. Section IV presents our conclusions.

II. Blockchain Integration In IoT

A. Blockchain Technology

Blockchain recently emerged as a new technology that transforms the way of decentralized information sharing. It provides a trustful environments over distributed networks without the intervention of authorized third party "service provider". This has the prospect to change many industries and applications, including IoT. Blockchain is defined as "an open, distributed ledger that is effectively and verifiably capable of recording the transactions between two parties in a permanent way" [3]. For instance, bitcoin emerged as the first digital currency that does not suffer the double-spending problem without using a central server or a trusted authority [3].

B. Blockchain Structure

A blockchain is defined as an expandable list of records. These records are referred to as blocks. Successive blocks are linked through the use of blockchain cryptography. A block is composed of (1) its own cryptographic hash, (2) the cryptographic hash of the preceding block, a time stamp, and a merkle tree root hash the contains the transaction information as shown in Fig.1. The blockchain technology stores transactions across several computers, thereby creating a public digital ledger that is distributed and decentralized in nature. Any involved block in the blockchain cannot be retroactively

[1]A digitally encrypted currency that adjusts the generation of units and provides a secure verification of the transfer funds independently from a central bank.

978-1-7281-5260-8/19/$31.00 ©2019 IEEE

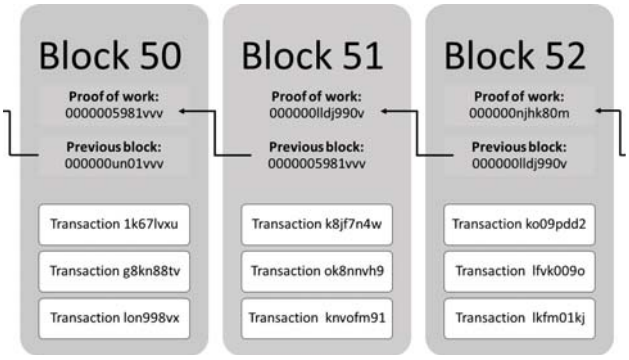

Fig. 1. Blockchain structure.

changed without causing changes in all the subsequent blocks. The main components of blockchain are:

1) **Blocks**: Each contains the cryptographic hash of the preceding block in order to link them together. Blocks linked in this manner form a chain that trace back to the original genesis block.
2) **Hashing**: It is a process through which data of a fixed size is generated given an input data of arbitrary size through a mathematical procedure. Some algorithms use cryptographic hash functions to have a consensus protocol.
3) **Proof of Work (PoW)**: Encourages mining nodes to receive a little reward of cryptocurrency, in addition to the fees that the nodes generating the transaction pay. In order to make a new block, the mining nodes compete by attempting to answer a PoW puzzle.
4) **Decentralization**: The decentralized or peer-to-peer (P2P) blockchain solves the problem of single point of failure. It uses ad-hoc message passing and distributed networking.
5) **Openness**: Blockchain is publicly open. However, physical access is still needed in order to view its content. In fact, open blockchains are more user-friendly compared to other legacy ownership records.

Figure 2 illustrate how does the blockchain work. Starting from someone requesting a transaction, this transaction is disseminated to the entire P2P network to be validated for creating a new block in the chain. The hash is calculated once a new block is created. Any change in the block data causes the hash to change. A newly created block is appended to the blockchain and ordered in a network of anonymous peers. Recall that each block contains data in addition to both its own cryptographic hash as well as the cryptographic hash of the preceding block.

C. Challenges of Blockchain in IoT

Merging the blockchain into IoT is challenging. Blockchain was initially designed to use powerful computers for the purpose of the Internet scenario, which is far from the IoT limited-resource nature. The transactions in a blockchain network are signed in a digital form. Therefore, it is necessary to equip the IoT devices operating the blockchain with this features. The main challenges of using blockchain in IoT are:

1) Storage Capacity and Scalability: One of the main challenges is the capacity and scalability limitations of IoT applications which make the integration with blockchain more challenging. It seems that the blockchain is inappropriate for the IoT because of the resource limitations of the IoT nodes. However, such limitations can be overcame through various ways as shown in [8].

2) Security: Due to the openness of blockchain, the security problems have to be taken into consideration. In addition, the set of properties that characterize IoT applications, such as wireless communications, mobility, lightweight and scale of the network, affect the security.

3) Data Privacy: Data privacy is considered as the solution for identifying, authenticating and authorizing nodes/users. However, some IoT applications may need to guarantee the social anonymity. The issue of data privacy has already been addressed in public blockchain. However, IoT is not limited to collecting the data. It is now used in the communication and application levels, which is more difficult in preserving the data privacy. The ability to conceal the person's identity when sending private information protects the privacy of users.

4) Legality: As a virtual currency, blockchain has sparked much controversy over legality. The blockchain provides the opportunity to use different blockchain manners such as private, permitted and consortium blockchain network topologies to manage the network elements based on the user needs.

5) Consensus: One of the most IoT challenges is how to the make the IoT device with its limited resource nature to participate in consensus processes such as PoW.

III. Blockchain Applications in IoT

Blockchain applications in IoT can broadly be classified into three categories as shown in in Fig. 3.

A. Resources Management

1) Data Storage: A typical data storage system often has various data sources. This data in most instances are valuable. The protection of sharing this personally identifiable information is one of the main important challenges in IoT. The authors of [9] presented technique that is called "Searchain" which searches for a keyword in distributed storage systems. Such a private keyword technique is composed of two elements: the first element is the nodes generating the transactions in a P2P network and the second component is a blockchain that represents the entire blocks appropriately ordered. The proposed strategy guarantees the user privacy and accountability.

2) Cloud Computing: IoT data storage and processing are typically implemented on distributed cloud platforms. Data centers consuming a significant power every day with the rush of the requested computations. This is an attractive challenge for researchers given the energy efficiency dilemma.

The resource management problem of energy in cloud data centers is investigated in [10] by considering the unpredictable capacity of green energy. The authors proposed a robust decentralized blockchain-based framework for resource management

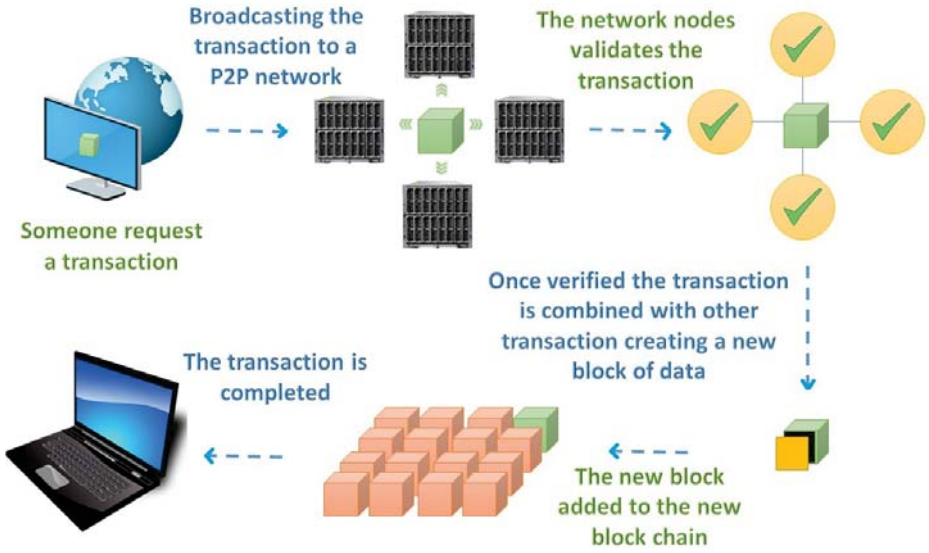

Fig. 2. A graphical illustration of how a blockchain works.

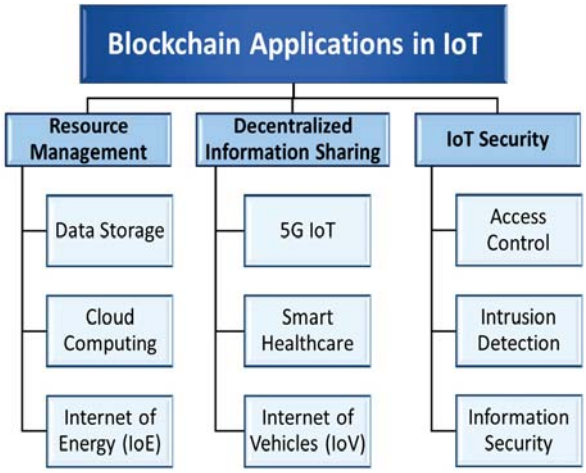

Fig. 3. Classification of the blockchain in IoT systems.

that reduces the huge power consumption by the request scheduler.

Meanwhile, the authors of [11] use public blockchain networks to investigate price-based computing resource management. The main goal is to enable the offload of the mining tasks to the cloud and/or the fog providers in consensus protocols that are based on the proof of work. Alternatively, the authors of [12] considered deploying an edge computing service for resource allocation for the mining process to support blockchain in IoT Systems. More specifically, the authors adopted a game-theoretic approach to investigate the relationship between the miners and the cloud and/or fog service providers in blockchain networks that are PoW-based. Consequently, they presented a lightweight PoW-based blockchain infrastructure in which the computationally exhaustive processes of the consensus are offloaded to the cloud and/or the fog.

3) Internet of Energy: Using the consortium blockchain based on the Stackelberg game, the energy blockchain was introduced in [13] maintaining the security of the energy trading in the Industrial Internet of Things (IIoT).

On the other hand, a P2P energy trading system, called PETCON, was initially introduced by [14], to plug-in hybrid electric vehicles connected to smart grids. The PETCON idea is based on the fact that the public auditing and sharing of transaction records is possible without supporting a trusted centralized entity.

B. Decentralized and P2P Information Sharing

1) 5G IoT: In the era of 5G, all mobile devices will be fully connected, and we here talk about billions of linked objects [15]. The authors of [16] solve the problem of pre-saving privacy in the 5G communication environment by presenting a privacy-protecting data exchange approach that exploits the blockchain technology. For more cooperation, [17] introduced a blockchain-based sincere incentive scheme to encourage users to cooperate in a dynamic distributed network. This cooperation will be helpful in the 5G heterogeneous communication environment, which provides a self-organizing and cooperating IoT devices for the more recent application social media data sharing, collaborative movies, electronic commerce, uploading data and forwarding files using sensor networks. The proposed scheme in [17] presents a pricing mechanism in which the intermediate network nodes gain rewards because of their participation in successful blockchain transactions defending against malicious collusion attacks.

2) Smart Healthcare: An IoT device can also be used in healthcare providing electronic healthcare systems called ”e-

healthcare". Such e-healthcare systems exploit the medical data related to the patients and their family members, the patients' environment, and the healthcare providers. In [18], this data is referred to as the electronic medical records (EMRs) which are saved by the care provider. The authors proposed an IoT healthcare application based on a consortium blockchain scheme. The responsible healthcare provider creates a new block when new healthcare data is inserted and they are responsible for storing this EMRs. When the data stored is larger than EMRs, there are the electronic health records (EHRs) that has been introduced based on distributed online databases to enhance the transfer of the data of the patients. The Multiple-Authorities Attribute Based Signature (MA-ABS) approach has been introduced in [19] that maintains the patient privacy and keep EHRs stable. The authors of [20] used the blockchain network to insure the integrity protection in mobile healthcare applications.

3) Internet of Vehicles (IoV): IoV is a logical sequence for integrating vehicles into the new IoT era. The vehicles will be smarter and can communicate with one another, and with any other device in the environment. Like other applications, the blockchain technology was recently incorporated with the IoV. [21] proposed an ecosystem model based on blockchain called LNSC. This scheme is used for managing the charging of electric vehicles based on the decentralized security model. The electric vehicles hash functions and charging piles can be calculated using the elliptic curve cryptography (ECC) in the LNSC model.

The authors of [22] proposed the use of blockchain in vehicular communications via dynamic key management without backing to the central manager administration. The backup storage hash is also appended in the blockchain data.

The security-managing network authenticates the key transfer processes, and verifies the third party authorities based on a decentralized blockchain. A secured decentralized system based on blockchain technology has been introduced in [23] that preserves the privacy where overlay nodes manage the blockchain.

C. IoT Security

1) Access Control in IoT: Definitely, centralized access control systems are unable to efficiently handle increased loads. Meanwhile, most of the IoT nodes do not have enough resources to support the blockchain technology. For managing IoT devices, [24] proposed a new decentralized blockchain-based access control architecture for IoT system that arbitrates the permissions and the roles. This architecture solves the management problem of the scalability access to billions of IoT devices. Such an access control approach alleviates the problems related to managing the different constraints of the IoT devices.

The components of the proposed system are: 1) Physical sensors, 2) Agent nodes, 3) Network management nodes, 4) Blockchain, 5) Smart contracts, and 6) Hubs. The authors build a prototype for concept-proofing to demonstrate the ability of the system to provide a scalable access control that facilitates the management of the IoT nodes. More specifically, the advantages of such system are 1) Improving the mobility by using isolated administrative systems. The IoT nodes can be controlled by the administrative domains freely from the access management policies which are imposed through the blockchain regulations; 2) Enhancing the accessibility of the access control rules, and solving the problems that make the IoT system unable to directly access them such as using the sleeping patterns; 3) Concurrency by making the constrained IoT device that have multiple managers can be accessed concurrently. 4) Enabling the use of lightweight devices because there is no extra hardware or modifications to embrace such a system; 5) Increasing the scalability; 6) Transparency since the location of the IoT nodes and how to access them is concealed.

2) Intrusion Detection: Recently, the security challenge has become even more complicated. Educational and financial organizations are now extensively using the intrusion detection systems (IDSs). Intrusion detection is the process used to monitor the events in the network for any intrusion incidents. Essentially, IDS main functions can be described as follow: 1) Recording the information by monitoring the target objects and storing the information locally, then it can be sent to other authority for analysis; 2) Generating alerts to warn the security administrators of anomalies in the system. There are many techniques are used the IDSs process in the IoT networks. The authors of [25] discuss the integration of blockchain technology in an intrusion detection systems. The authors of [26] improve collaborative intrusion detection systems (CIDSs) by utilizing the blockchain technology to secure the exchange of alerts between the collaborating nodes. The authors of [27] emphasized that modern CIDS demands broad data sharing between the several entities. The modern CIDSs have to deal with the privacy concerns resulting due to the huge data exchange and cyber-attacks. This is the reason to apply the blockchain technology which implies that there is no need to have a central trustful entity to avoid the single point of failure problem.

3) Information Security: In order to provide better services in smart IoT environments, ICT information and communication technologies are used to monitor and control physical, social, and business infrastructures. The authors of [28] proposed a security framework based on a blockchain for enabling secure communication in a smart environment. The security framework is composed of three components: 1) Physical layer of IoT devices equipped with sensors (light, pressure, motion, etc); 2) Communication layer that uses different communication schemes such as Bluetooth, 6LoWPAN, WiFi, Ethernet, 3G, 4G and 5G to communicate while the blockchain technology to secure and provide privacy of the sent data; and finally 3) Database Layer which uses a type of distributed ledger blockchain with a decentralized database that stores the records consecutively including a time stamp and unique signature.

In IoT systems, attackers typically aim at retrieving the data from the IoT devices using some malicious codes. In [29], the authors proposed a framework based on consortium blockchain

named CB-MDEE to effectively detect the ill-natured pieces of code in malwares particularly in open source platforms such as Android. This framework consist of a consortium blockchain that detects the ill-natured pieces of code and extracts the corresponding evidences in IoT nodes, and a public chain that is shared by the users. In order to enhance the process of the malware detection and decreases the rate of false positives of malware variations, the CB-MDEE system supports comparison and marking functions. In order to shield an IoT system device, the authors of [30] introduced a firmware update approach that is based on Blockchain. The embedded devices in such an approach request firmware updates from the blockchain network nodes. The received response from the blockchain network determines whether or not the node's firmware is up-to-date, and accordingly download it if needed.

IV. Concluding Remarks

This survey paper has shed the light on the exploitation of the blockchain technology in the various IoT systems and domains. More specifically, the paper has provided a comprehensive study of the blockchain technology in different applications of IoT such as resource management, cloud, Internet of Vehicles, Internet of Energy, and security and have shown the advantages of this integration in many disciplines. We have classified the aspects by which the blockchain technology is exploited in IoT networks into three main categories, namely, resources management, decentralized applications, and security. There are still many challenging research directions of the blockchain technology in IoT applications that needs to be addressed in the future such as dynamic and adaptable security, social networks, trust management and vehicular cloud advertisement.

References

[1] U. internationale des télécommunications, *Measuring the information society report 2015*. International telecommunications union, 2015.

[2] M. Hung, *Leading the IoT*. Gartner, 2017.

[3] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[4] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, July 2018.

[5] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19 293–19 304, 2017.

[6] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[7] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts*, vol. 18, no. 3, pp. 2084–2123, 2016.

[8] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2016.

[9] P. Jiang, F. Guo, K. Liang, J. Lai, and Q. Wen, "Searchain: Blockchain-based private keyword search in decentralized storage," *Future Gener. Comp. Sys.*, 2017.

[10] C. Xu, K. Wang, and M. Guo, "Intelligent resource management in blockchain-based cloud datacenters," *IEEE Cloud Comput.*, vol. 4, no. 6, pp. 50–59, 2017.

[11] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, "Cloud/fog computing resource management and pricing for blockchain networks," *IEEE Internet Things J.*, 2018.

[12] Y. Jiao, P. Wang, D. Niyato, and Z. Xiong, "Social welfare maximization auction in edge computing resource allocation for mobile blockchain," in *IEEE International Conference on Communications (ICC)*, 2018.

[13] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, 2017.

[14] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, 2017.

[15] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, 2018.

[16] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5g," *IET Commun.*, vol. 12, no. 5, pp. 527–532, 2017.

[17] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A blockchain based truthful incentive mechanism for distributed P2P applications," *IEEE Access*, vol. 6, pp. 27 324–27 335, 2018.

[18] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, 2018.

[19] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11 676–11 686, 2018.

[20] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2017.

[21] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: a security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13 565–13 574, 2018.

[22] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, 2016.

[23] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, 2017.

[24] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, 2018.

[25] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: a review," *IEEE Access*, vol. 6, pp. 10 179–10 188, 2018.

[26] N. Alexopoulos, E. Vasilomanolakis, N. R. Ivánkó, and M. Mühlhäuser, "Towards blockchain-based collaborative intrusion detection systems," in *International Conference on Critical Information Infrastructures Security, Springer*, 2017.

[27] T. Cruz, L. Rosa, J. Proença, L. Maglaras, M. Aubigny, L. Lev, J. Jiang, and P. Simoes, "A cybersecurity detection framework for supervisory control and data acquisition systems," *IEEE Trans. Ind. Informat.*, vol. 12, no. 6, pp. 2236–2246, 2016.

[28] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *IEEE International Conference on High Performance Computing and Communications; IEEE International Conference on Smart City; IEEE International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2016.

[29] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium blockchain-based malware detection in mobile devices," *IEEE Access*, vol. 6, pp. 12 118–12 128, 2018.

[30] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," *J. Supercomput.*, vol. 73, no. 3, pp. 1152–1167, 2017.