A Review on the Integration of Blockchain and IoT

Alia Al Sadawi
Engineering Systems Management
American University of Sharjah
Sharjah, United Arab Emirates
g00047863@aus.edu

Mohamed S. Hassan
Electrical Engineering
American University of Sharjah
Sharjah, United Arab Emirates
mshassan@aus.edu

Malick Ndiaye
Industrial Engineering
American University of Sharjah
Sharjah, United Arab Emirates
mndiaye@aus.edu

***Abstract*— The Internet of things (IoT) is a rapidly growing technology that enhances people's interaction with each other and with their surroundings. It is also a key player behind the advancements in different sectors including healthcare, smart city, and logistics in addition to many other fields. In order to meet their design requirements, IoT uses various types of sensors, smart meters, RFIDs, and actuators resulting in networks of growing size and complexity. This comes at the price of raising scalability, security, authenticity, and reliability issues. Therefore, it is vital to thoroughly address the expected issues not to hurdle further evolution of IoT deployment. This is where blockchain fits. The emersion of blockchain technology promises to solve many IoT related issues. Blockchain's unique features of transparency, reliability, traceability, and security nominate it to play a pivotal role in improving IoT networks, resolving their issues, and facilitating their expansion. This paper explains the main problems facing IoT-based systems and the role of blockchains in addressing them. Additionally, it briefly surveys the current work in the literature on researches discussing the integration of IoT with blockchain.**

Keywords*— blockchain, IoT, challenges, integration, enhance, performance.

I. Introduction

The term "Internet of Things" (IoT) was first introduced by Kevin Ashton in 1999 [1]. In essence, IoT is where the physical and virtual worlds meet. It is the major enabler of the digitally connected world where data collected from devices and sensors are exchanged through the Internet such that objects can be remotely monitored and controlled without human intervention [1]. IoT emerged as a result of the distinguished advancements in electronics, network technology, and wireless communications. It was facilitated by Wireless Sensors Networks (WSN), Radio Frequency Identification (RFID), and other smart devices and actuators that are capable of sensing and communicating through network infrastructures [2]. However, the IoT as a paradigm increased the complexity of cloud networks and is expected to continue doing so especially with the expected growth in its size and complexity. It is estimated that the number of connected IoT devices and sensors will reach 20 to 50 billion by the year 2020 [3].

IoT enabled societies to interact with their environment in a better way, therefore, IoT is expected to play a major role in the development of smart cities where connected devices are becoming increasingly common in daily life. For instance, IoT is used in applications such as environmental, healthcare, sports, entertainment, defense, agriculture, and others [1, 4].

Furthermore, The successful and growing implementation of IoT in diverse sectors along with its inherent huge complicated and scattered size resulted in many challenges. Unfortunately, such issues could diminish the deployment of IoT and limit its application. They could also lead to emerging problems in existing networks.

Although the challenges facing the IoT paradigm differ in nature, they are correlated to a certain extent. These challenges vary from complex security and privacy challenges to basic network structure issues. Therefore, the evident need to understand those challenges and addressing them has motivated different studies to explore and suggest proper solutions. A leading and emerging technology that demonstrated itself as a vital solution to IoT issues is blockchain. Blockchain as a disruptive innovation has already proved itself in many fields and gained great interest as a decentralized, trusted, and transparent network of peers. Many researches proposed the integration of IoT with blockchain to eliminate challenges and enhance the performance of IoT-based applications. However, surveying related work in literature, it was obvious that IoT-blockchain integration is still a new topic highlighting the fact that it needs further exploration and understanding. Also, it was found that current studies have discussed some challenges facing IoT and presented blockchain to solve part of them. However, this does not cover all issues related to the IoT paradigm nor reveals the full potential of blockchain and its capability to elevate IoT-based systems. Therefore, this paper is an attempt to fill the gap by providing brief, yet comprehensive, research that contributes to the body of knowledge in the following ways:

- Demonstrate the various issues facing IoT especially with its growing network complexity and size whereas other reviews in literature concentrated on some challenges that are mostly security related.
- Propose blockchain's characteristics and explain its architecture as a revolutionary technology that shall

978-1-7281-6535-6/20/$31.00 ©2020 IEEE

enhance the performance of IoT applications while addressing the challenges they face.

- Then, summarize the work found in the literature that proposed integrating blockchain with IoT. Finally, our study provides a screening survey of the main architectural designs, schemes, and frameworks presented in the literature and discuss integrating blockchain with IoT.

The rest of this paper is organized as follows. Section II discusses the main challenges facing the IoT while Section III demonstrates the concept, structure, and characteristics of blockchains. Finally, Section IV discusses blockchain for IoT before a short survey is presented in section V and the conclusion provided in section VI.

II. Challenges facing IoT systems

The considerable spread and expansion of IoT applications in different fields brought in substantial issues which if not properly tackled might not only end up limiting further IoT deployment but will impact existing networks' performance, as well. Also, these issues are not totally independent but rather highly interrelated, therefore, an extensive study is required to recognize and overcome these challenges.

It is well known that IoT is based on the integration of various technologies such as communication and information technologies, electronic sensors, and computing in addition to data analytics in collaboration to establish smart systems [5]. The integration of such technologies resulted in increasing the complexity of IoT networks, especially for expanded and scattered ones. As a result, a central server architecture was adopted, which performs the task of authenticating all connected devices. This structure might cause unreliable interconnection between devices and allow data sharing with devices that have falsified authentication [6]. Therefore, it is also well-known that the centralized structure of IoT systems might have difficulty in fulfilling the trust factor.

Additionally, trusted information is essential to successfully and efficiently operate IoT systems [7] because sensors, meters, and other smart devices would interact depending on such information. Now, the question here is how far the information in the IoT system can be trusted and how to make sure it is not falsified. Data provided to IoT systems could be tampered with or modified according to the interests of certain entities, and then transferred throughout the network causing disruption to its performance [8]. Consequently, it is preferred that devices exchange data directly and autonomously. Therefore, a lot of efforts have been made to implement decentralized IoT platforms [9].

Also, IoT networks by nature generate a massive amount of data [6] that needs to be stored, communicated, and processed. This requires an extensive amount of energy and reliable connectivity [7]. This problem is inflated when implementing a centralized IoT structure where data is communicated through a central hub. The situation gets worse when data processing is also performed in the central server, which requires unavoidable upgrades in the server's infrastructure along with its capacity and computation capability [10].

Moreover, the IoT paradigm connects different types of devices serving diversified applications with different frameworks and different security mechanisms and requirements. This diversified ecosystem affects the success of IoT systems deployment [4]. Therefore, it is expected that more security and privacy challenges shall appear due to the expanded range of IoT applications. That is why it is recommended that security issues be thoroughly tackled because threats such as data manipulation or unauthorized control of IoT devices [4] could jeopardize the IoT system reliability.

Privacy and security issues are extremely important for data in transit or computation states [11]. Those challenges become critical due to the current trend of the Internet-of-Everything (IoE), which includes specific IoT applications such as the Internet of Medical Things (IoMT), Internet of Vehicles (IoV), Internet of Battlefield Things (IoBT), and so on. Many of these IoT-based systems such as IoMT and IoBT are data-sensitive, therefore, it is important to maintain the highest levels of data and devices security.

It is worth mentioning that security breaches could be due to a blunder in the adopted security measures, especially for application-specific IoT systems. For example, although IT team members have full control over IoT networks and devices, they are not fully acquainted with the specificity and functionalities of every single device. This may result in chaotic situations and security breaches simply because IT personnel was performing what looks like routine operations [11].

Lastly, IoT systems are increasingly utilizing cloud computing, which while providing upgraded and powerful analytical capabilities increases the privacy and security challenges as well as the ability to build a trusted environment compared to constrained IoT devices.

Based on the above, security and trust issues form considerable concerns affecting the reliability of IoT networks. Consequently, there is a significant need to verify data and ensure they have never been tampered with [8]. Therefore, blockchain technology was proposed as a solution for all the above challenges. In order to derive value from blockchain that shall serve the IoT paradigm, this emerging technology should be explored and understood.

III. Blockchain structure, and characteristics

Blockchain is a distributed and decentralized network containing immutable and timestamped data records shared securely yet privately between its nodes. Blockchain facilitates the interaction between non-trusting participants without the need for a trusted central authority [14]. Blockchain is the backbone of the cryptocurrency Bitcoin. However, it is applied successfully in other sectors such as digital identity, digital assets management, supply chain management, voting, healthcare services, IoT, and big data [14]. Blockchain is classified into public, hybrid, and private network [17].

1) Public blockchain: is a permissionless blockchain such as the cryptocurrencies network in which transactions are public but members' identities are kept anonymous [17].

2) Private blockchain: is a permissioned blockchain, which grants access to specific members [14, 17]. It is used by enterprises to transfer data between predefined users [12].

3) Federated or consortium blockchain: is a combination of a public and a private blockchain [13].

Based on IoT systems' characteristics and blockchains categories, it is deduced that consortium and private blockchains are more appropriate to be integrated with IoT than public blockchain which is available to all people whereas IoT systems are designed for specific groups or entities.

A. Blockchain Structure

Blockchain is a database containing all digital transactions shared among its nodes. Transactions records in each block are hashed and their hash is added to the successive block. This is how the chain of blocks is formed. Transactions get verified by a consensus mechanism among the majority of network members [9]. Data records authentication is the responsibility of special nodes called miners who solve a puzzle to verify a block. Then, data records encapsulated in a block becomes immutable and nodes update their databases accordingly [14]. The below "Fig. 1" demonstrates how blockchain is structured.

Blockchain is the enabler of the concept of smart contract, which is an application that resides on a blockchain. Various IoT-Blockchain integrated architectures use smart contracts to fulfill the goal of the integration and solve challenges facing IoT networks. The following section explores smart contract and its role in the proposed blockchain-IoT integration.

B. Smart contract and its potential for IoT-blockchain integration

A smart contract is defined as "a self-executing code that enables the system to enforce the clauses of a contract through certain trigger events" [15]. The main distinguishing feature of a smart contract is the ability to execute certain actions specified in its code when a pre-set term(s) occurs without human intervention [9]. A smart contract code has a unique address, so an IoT device can call and operate it by sending a transaction to its address. Every node in the blockchain will run as a virtual machine (VM) that executes the so-called smart contract independently, and the blockchain network will perform as a distributed VM [15]. Many blockchains facilitate smart contracts such as Ethereum, which is the first blockchain-based computing platform [16].

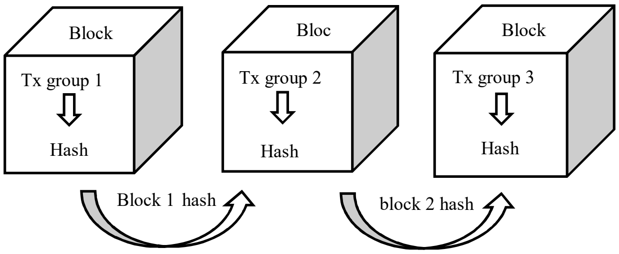

Fig. 1. Blockchain structure

Smart contracts are secured codes since they are executed and stored on a blockchain. Additionally, they reduce network performance costs and lower risks [15].

Smart contracts were utilized in the Blockchain-IoT integrated to pay for consumed IoT resources [17]. Also, smart contracts securely record all IoT interactions resulting in trusted actions. Therefore, smart contracts have the ability to model the logic behind IoT applications [18]. A good example is an experimental approach by the Finnish company Kouvola Innovation to connect pallets with shipping tasks, and willing carriers. Pallets are equipped with RFIDs and provided with shipping tasks and willing carriers. RFIDs communicate pallets' needs to be transported to potential carriers using a blockchain platform. When an offer is provided, the blockchain compares it with predefined contract terms and the smart contract gets executed automatically. Accordingly, pallets are moved visibly and traceably on blockchain thanks to RFIDs and sensors [19]. Therefore, smart contracts model the logic and the IoT devices send data whenever a transaction operates a smart contract [20].

C. Blockchain Characteristics

Blockchain has the following characteristics[13]:

1) Distribution: each node in the network posses a continuously updated copy of the ledger.

2) Decentralization: network operations and files' access is not controlled by a central server or authority.

3) Security: transactions encapsulated in any block within the chain can never be altered, erased, or tampered with.

4) Transparency: data in any block is visible to all participants.

5) Automation: performed by smart contracts where functions are automatically executed.

6) Traceability: blockchain network contains historical records of all transactions ever made.

7) Privacy: achieved using private/public keys where cryptography is used to keep users' identities autonomous.

8) Reliability: blockchains reliability stems from its firm structure.

IV. Blockchain for IoT

Most currently implemented IoT systems are large-scale centralized networks where a huge number of devices interact through servers performing different tasks such as data storing, authenticating, and analyzing. This network structure is not efficient which raises many issues that are added to existing challenges as demonstrated in section II.

Blockchain is capable of providing solutions to most challenges facing IoT. The following demonstrates how blockchain plays this role.

1) Elimination of central authority: blockchain eliminates the need for central servers. Transactions are stored in a decentralized way in a blockchain where identical copies of all records exist with each node within the network. Also, data authentication is performed using a consensus algorithm rather than through a central server. Furthermore, data analysis is carried on using smart contracts.

*2) Accelerated direct messaging between peers: s*ince blockchain is a peer to peer network, it facilitates direct messaging between devices which is faster than exchanging messages through central serves. This is achieved thanks to the decentralized and distributed structure of blockchain that eliminates intermediaries and facilitates direct data transmission and processing among nodes [21]. It is worth mentioning that data flow differs between centralized and decentralized systems and for the case of integrating blockchain with IoT, there are many forms of integration architecture.

3) Built-in trust: Trust is a basic feature of blockchain that emerged from its distributed architecture and the adopted consensus mechanism. Trust provided by blockchain is useful for IoT data where all peers guarantee that this information provided by IoT devices has never been tampered with. Simply, if all nodes have a copy of the data then they can verify. As a result, trustworthiness could be achieved [22, 23].

4) Security: cryptography is a major part of the structure of blockchain. Blocks are connected using a hash algorithm to form the chain where each block contains the hash of the previous block embedded in its header. This virtual chain granted blockchain its name. If any hackers want to alter the contents of any block, they need to recalculate its hash along with the hashes of all successive blocks which is almost an impossible task. Besides, hypothetically speaking, even if all the previously mentioned hashes where recalculated, the distributed data records among peers will reveal that one copy was altered and the peers will not reach consensus on the altered blocks and therefore the ledger will not be updated accordingly and altered blocks will not be added to the chain.[12]. Therefore, security is always guaranteed in a blockchain.

5) Privacy: Another part of the cryptographic structure of blockchain is the private/public key pair, which guarantees that only authorized participants can perform data transactions.

*6) Traceability: r*ecords of all data transactions are immutably saved in the blocks, and since blocks are chained together through hashing, every transaction could be traced back to the very first action.

7) Cost reduction in developing huge internet infrastructure: expanded and large-scale IoT systems need upgrading the supporting network infrastructure to increase its capability and connectivity which is a costly process. Blockchain as a decentralized technology eliminates this requirement and consequently saves cost.

8) Transparency: The technological advances have led to the introduction of cloud computing concepts which increased the ability to analyze and process IoT data and perform real-time responses. Unquestionably, cloud computing contributed to the development of IoT systems[24]. However, it acts as a black box when considering data transparency. Participants do not know where and how their data is going to be used [25].

9) Robustness and reliability: Since blockchain enhances privacy and security in IoT data by eliminating the need for central servers, the integration of blockchain with IoT is expected to result in a reliable combined system. Although IoT can support information digitization, the reliability of such information is still questionable [25]. Blockchain solved this challenge by increasing the reliability of a proposed combined system. Blockchain reliability along with its history of flawless implementation in many fields ensures high robustness [21].

The above demonstrates the role of blockchain in complementing the IoT paradigm by providing trusted and secured data and enhance latency and transparency. Furthermore, IoT is integrated with some computing infrastructures such as cloud computing to increase systems storage and processing capabilities[24].

V. Research Survey

The literature offers different contributions to the field of integrating blockchain with IoT systems. Researches such as [26] discussed a number of the challenges facing IoT and suggested blockchain as a useful solution. Other work focused on specific challenges facing IoT and proposed frameworks to address some of them [11, 27]. Further studies demonstrated advanced IoT network architecture by integrating blockchain and explained the benefits of this integration on IoT's performance[28]. However, there was no comprehensive review paper found in the literature that surveys all proposed IoT - blockchain integration designs as we did in this research.

The first architecture, to begin with, is an IoT EdgeABC model introduced by [29] to be implemented in smart homes, factories, and healthcare institutes. It consists of three layers: An IoT device layer, a distributed agent controller architecture based on blockchain, and hierarchical edge computing servers. The model integrates blockchain in the middle layer to ensure the integrity of transaction data. The research used smart contracts to implement task offloading and resource allocation. A security protocol and decentralized model based on blockchain were presented by [30]. Authors aim to provide cryptographic keys and trusted data storage for Wireless Sensor Networks which enables their components to authenticate data about every network peer. Also, [28] suggested a distributed blockchain-based cloud architecture utilizing fog computing and software-defined networking SDN. The model consists of three layers: IoT devices, SDN controller network based on blockchain for fog nodes, and distributed cloud-based on blockchain. The research aims to manage raw IoT data stream at the network edge and cloud level. The researchers in [31] explained the blockchain role for 5G-beyond networks and demonstrated their architecture for Blockchain of Things (BCoT). In this research, a blockchain- layer forms a middleware between IoT and industrial applications to hide the lower layers devices' heterogeneity while providing blockchain-based services. A hierarchical architectural model demonstrated by [32] integrated blockchain into more than one layer. The model comprising of a physical network layer, blockchain edge layer, and a blockchain network layer aims to improve authentication efficiency and data sharing between IoT platforms. In [33] a decentralized blockchain-based IoT management system was proposed to tackle gateway nodes' single-point failure issue. The proposed protocol aims at improving the security of the IoT management system by introducing blockchain and deliver all messages to all nodes accordingly. A study by [34] proposed a P2P network architecture involving blockchain and edge computing. The research aims at achieving high system performance and secured data storage. The architecture consisted of three layers: A cloud layer, an edge layer, and a device layer. Cloud resources could be configured as blockchain peers. Also, information authentication was fulfilled using a Proof-of-Space solution based on smart contracts. Another blockchain architecture including edge computing was proposed by [35]. Researchers suggested a blockchain-based data management scheme (BlockTDM) to protect sensitive data using matrix-based multichannel and smart contracts. As per [27], the Internet of Drones (IoD) could also benefit from blockchain's distinguishing characteristics. Researchers designed a blockchain-based access control scheme between any two neighbor drones and between a drone and its associated ground station server (GSS). Simulation results showed that the scheme increases communications security and helps to resist attacks.

The integration of IoT and blockchain is implemented in power systems as well. The research in [36] demonstrated structural applications incorporating blockchain with IoT in distributed generation systems, energy hubs, smart buildings, and management of residential electric vehicles. The study aims to utilize blockchain characteristics to tackle the problem of securely transferring, storing, and analyzing the generated data which results in enhancing the performance of the grid. Also, research by [37] integrated blockchain with IoT ecosystems trading platforms and demonstrated business linked scenarios in addition to a case study to trade IoT devices and their corresponding data in a trusted end to end environment. Trust was the center of the article by [38] which proposed an IoT secondary authentication scheme to control Wi-Fi network access. The design used smart contracts to identify IoT devices located within a certain range.

In a related context, an article by [39] analyzed the cost of integrating blockchain with IoT especially the cost associated with storing the data generated from IoT sensors on Ethereum. The researchers used smart contracts to addend new data or overwrite existing data. The study aims to enhance the implementation of blockchain and smart contracts in IoT applications. Furthermore, another study by [40] designed and tested a blockchain tokenizer that connects industrial machines to blockchain platforms. The research aims to enable diffusing blockchain in industrial applications by tokenizing industrial assets. Researchers used smart contracts to create the digital twin of machines and tested them on two industrial supply chain use cases. The work by [41] discussed how security and decentralization features of blockchain would benefit the integration with IoT, especially for shared economy applications. Integrating blockchain with industrial IoT was the center of another article by [42]. The research proposed a blockchain-enabled IoT framework. Smart contracts were used to control components interactions, and data storing and processing. Related research by [43] modeled and designed a blockchain-based self-organized IoT devices trading platform. The authors used game theory to model resource management and pricing between cloud providers and blockchain miners.

Moreover, many researchers aimed at optimizing IoT-blockchain integration architecture such as [44] who addressed blockchain consensuses management required to deal with highly dynamic IoT applications. The researchers proposed application-aware consensus management for software-defined intelligent blockchain as well as an intelligent scheme to analyze packets at the IoT application-layer. Also, [45] used interledger mechanisms and smart contracts to build a model that quantifies the performance of IoT devices in terms of reducing transaction delay and cost. Lastly, research by [46] utilized blockchain and Tangle technologies to model an optimization policy for IoT sensors sampling rate. The study aimed to minimize the age of information (AoI) experienced by end-users.

It is concluded from the screened researches that systems based on integrating blockchain and IoT demonstrate better performance compared to standard benchmark IoT systems with no blockchain integration [6]. Also, the reviewed articles did not only agree on the feasibility of the integration but presented a variety of designs to achieve it, as well. While some concentrated on the general architectural prospects needed for the integration; others focused on mitigating specific challenges. additionally, other researchers used integrated blockchain-IoT systems as a platform to deploy certain applications.

VI. Conclusion

The IoT is gaining popularity due to its ability in connecting people and increasing their awareness of their surrounding environment. Also, it supports the advancements of many fields and industries. Therefore, IoT systems witnessed a significant increase in size and complexity. This created various issues and challenges that could impact their further expansion and reliable performance. On the other hand, blockchain emergence as a revolutionary technology has widely opened the door for a comprehensive solution to many of the IoT issues. Blockchain features of transparency, security, decentralization, and trust form a strong base for its successful integration with the IoT paradigm. The idea of integrating blockchain with IoT called the attention of researchers who proposed different integration forms and architectures. This work discussed the main challenges facing IoT, explained the structure and characteristics of blockchain and its role in resolving IoT issues. It also surveyed the work on blockchain-IoT integration and demonstrated a summary of their work. Such a survey can assist in evaluating the position of the integration process and possible methods for practical implementation.

References

[1] S. Balaji, K. Nathani, and R. Santhakumar, "IoT Technology, Applications and Challenges: A Contemporary Survey," *Wireless Personal Communications,* vol. 108, no. 1, pp. 363-388, 2019.

[2] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," *Journal of Network and Computer Applications,* vol. 67, pp. 99-117, 2016.

[3] J. Rivera and R. van der Meulen, "Forecast alert: internet of things—endpoints and associated services, worldwide," ed: Gartner, 2016.

[4] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *Journal of Information Security and Applications,* vol. 38, pp. 8-27, 2018.

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems,* vol. 29, no. 7, pp. 1645-1660, 2013.

[6] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," *IT Professional,* vol. 19, no. 4, pp. 68-72, 2017.

[7] M. Amadeo *et al.*, "Information-centric networking for the internet of things: challenges and opportunities," *IEEE Network,* vol. 30, no. 2, pp. 92-100, 2016.

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

[9] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation,* vol. 2, no. 6-10, p. 71, 2016.

[10] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to Networking Cloud and Edge Datacenters in the Internet of Things," *IEEE Cloud Computing,* vol. 3, no. 3, pp. 64-71, 2016.

[11] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks,* vol. 4, no. 3, pp. 149-160, 2018.

[12] M. Swan, *Blockchain : blueprint for a new economy*. [Sebastopol, Calif.]: O'Reilly (in English), 2015.

[13] W. Mougayar, *The business blockchain : promise, practice, and application of the next Internet technology* (Online access with DDA: Askews (Economics)). Hoboken, New Jersey: John Wiley & Sons, Inc. (in English), 2016.

[14] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2009.

[15] Q. Tang and L. M. Tang, "Toward a distributed carbon ledger for carbon emissions trading and accounting for corporate carbon management," *Journal of Emerging Technologies in Accounting,* vol. 16, no. 1, pp. 37-46, 2019.

[16] V. Buterin, "A next-generation smart contract and decentralized application platform," *white paper,* vol. 3, no. 37, 2014.

[17] K. Wüst and A. Gervais, "Do you Need a Blockchain?," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 20-22 June 2018 2018, pp. 45-54.

[18] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access,* vol. 4, pp. 1-1, 2016.

[19] A. Kawa and A. Maryniak, *SMART supply network* (EcoProduction, 2193-4614). Cham, Switzerland: Springer (in English), 2019.

[20] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *Journal of Network and Computer Applications,* vol. 125, pp. 251-279, 2019.

[21] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Computer Science,* vol. 132, pp. 1815-1823, 2018.

[22] D. Kundu, "Blockchain and Trust in a Smart City," *Environment and Urbanization ASIA,* vol. 10, no. 1, pp. 31-43, 2020/08/28 2019.

[23] M. J. Casey and P. Vigna, "In blockchain we trust," *MIT Technology Review,* vol. 121, no. 3, pp. 10-16, 2018.

[24] P. Wang, R. X. Gao, and Z. Fan, "Cloud Computing for Cloud Manufacturing: Benefits and Limitations," *Journal of Manufacturing Science and Engineering,* vol. 137, no. 4, 8/28/2020 2015.

[25] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems,* vol. 88, pp. 173-190, 2018.

[26] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Blockchain with Internet of Things: Benefits, challenges, and future directions," *International Journal of Intelligent Systems and Applications,* vol. 10, no. 6, pp. 40-48, 2018.

[27] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," 2020.

[28] P. K. Sharma, M. Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," *IEEE Access,* vol. 6, pp. 115-124, 2018.

[29] K. Xiao, Z. Gao, W. Shi, X. Qiu, Y. Yang, and L. Rui, "EdgeABC: An architecture for task offloading and resource allocation in the Internet of Things," 2020.

[30] A. Moinet, B. Darties, and J.-L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," *arXiv preprint arXiv:1706.01730,* 2017.

[31] H. N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A Survey," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8076-8094, 2019.

[32] S. Guo, X. Hu, X. Qiu, and F. Qi, "Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System," 2020.

[33] S. He, Q. Tang, C. Q. Wu, and X. Shen, "Decentralizing IoT management systems using blockchain for censorship resistance," *IEEE Transactions on Industrial Informatics,* vol. 16, no. 1, pp. 715-727, 2020.

[34] B. W. Nyamtiga, J. C. S. Sicato, S. Rathore, Y. Sung, and J. H. Park, "Blockchain-based secure storage management with edge computing for IoT," *Electronics (Switzerland),* vol. 8, no. 8, 2019.

[35] M. Zhaofeng, W. Xiaochang, D. K. Jain, H. Khan, G. Hongmin, and W. Zhen, "A Blockchain-Based Trusted Data Management Scheme in Edge Computing," 2020.

[36] H. Hosseinian, H. Shahinzadeh, G. B. Gharehpetian, Z. Azani, and M. Shaneh, "Blockchain outlook for deployment of IoT in distribution networks and smart homes," *International Journal of Electrical and Computer Engineering,* vol. 10, no. 3, pp. 2787-2796, 2020.

[37] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, "Trust chain: Establishing trust in the iot-based applications ecosystem using blockchain," *IEEE Cloud Computing,* vol. 5, no. 4, pp. 12-23, 2018.

[38] Y. Chen, X. Wang, Y. Yang, and H. Li, "Location-aware Wi-Fi authentication scheme using smart contract," 2020.

[39] Y. K. Peker, X. Rodriguez, J. Ericsson, S. J. Lee, and A. J. Perez, "A cost analysis of internet of things sensor data storage on blockchain via smart contracts," *Electronics (Switzerland),* vol. 9, no. 2, 2020.

[40] D. Mazzei *et al.*, "A Blockchain Tokenizer for Industrial IOT trustless applications," 2020.

[41] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of Things, Blockchain and Shared Economy Applications," *Procedia Computer Science,* vol. 98, pp. 461-466, 2016.

[42] S. Zhao, S. Li, and Y. Yao, "Blockchain Enabled Industrial Internet of Things Technology," *IEEE Transactions on Computational Social Systems,* vol. 6, no. 6, pp. 1442-1453, 2019.

[43] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, "Resource trading in blockchain-based industrial internet of things," *IEEE Transactions on Industrial Informatics,* vol. 15, no. 6, pp. 3602-3609, 2019.

[44] J. Wu, M. Dong, K. Ota, J. Li, and W. Yang, "Application-Aware Consensus Management for Software-Defined Intelligent Blockchain in IoT," *IEEE Network,* vol. 34, no. 1, pp. 69-75, 2020.

[45] V. A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, and G. C. Polyzos, "Decentralized authorization in constrained IoT environments exploiting interledger mechanisms," 2020.

[46] A. Rovira-Sugranes and A. Razi, "Optimizing the Age of Information for Blockchain Technology with Applications to IoT Sensors," *IEEE Communications Letters,* vol. 24, no. 1, pp. 183-187, 2020.