Mediterranean Smart Cities Conference (MSCC 2024)
2-4 May, 2024, Martil, Morocco

A lightweight blockchain architecture for IoT based on delegated nodes

Yassin Elgountery
Department of Computer Science, GLISI teams
FST Errachidia, Moulay Ismail University
Errachidia, Morocco
y.elgountery@edu.umi.ac.ma

Meryem Lasaad
Department of Computer Science, GLISI teams
FST Errachidia, Moulay Ismail University
Errachidia, Morocco
meryemlasaad@gmail.com

Mohamed Oualla
Department of Computer Science, GLISI teams
FST Errachidia, Moulay Ismail University
Errachidia, Morocco
m.oualla@umi.ac.ma

Abdeslam Jakimi
Department of Computer Science, GLISI teams
FST Errachidia, Moulay Ismail University
Errachidia, Morocco
ajakimi@yahoo.fr

Hassain Sadki
Department of Computer Science, GLISI teams
FST Errachidia, Moulay Ismail University
Errachidia, Morocco
h.sadki@umi.ac.ma

Abstract—**Blockchain for the Internet of Things (BCoT) is a new technology enabling the combination of Blockchain and IoT. BCoT aims to store transactions among IoT nodes in real time based on a decentralized, distributed and public ledger. BCoT architecture refers to the design of a system that combines these two technologies to enable secure and efficient communication and management of IoT data. However, implementing blockchain for IoT faces a variety of challenges due to the resource limitations of IoT devices. This paper proposes a lightweight architecture based on delegated nodes to avoid direct integration of blockchain into IoT systems. To enhance data trust, a proof of authentication (PoAh) consensus mechanism and smart contracts are deployed in the blockchain network.**

Keywords—Blockchain, Internet of Things (IoT), consensus, delegated node, lightweight architecture.

I. INTRODUCTION

The Internet of Things (IoT) is a collection of devices that can communicate via the internet. Generally, these devices are equipped with sensors capable of analyzing data from their physical environment [1]. Although the IoT has potential benefits, there are several issues that need to be resolved in order to fully take advantage of it. These issues include significant concerns related to security and privacy, especially when collecting and sharing sensitive information between different entities [2]. Data integrity, reliability, and non-repudiation of exchanged data are other problems [3]. For example, the question of trust in sensor data arises in a context such as a smart hospital, where treatment decisions are based on this data.

The blockchain (BC) is considered a solution to these problems [4]. Due to its decentralization, the BC eliminates the need for a third party to verify the integrity, reliability, and non-repudiation of data. Furthermore, the BC does not have any distinct failure points. It is a distributed technology that allows members to verify transactions, including potentially dishonest transactions. A set of data called blocks, which record the details of each transaction made by users, is stored in the BC, which functions as an immutable chain register. A valid block is connected to the last block in the chain once it is assembled [5].

The IoT benefits from several advantages of blockchain. Through automated communication between devices, it significantly reduces administrative management costs and cloud storage [6]. The system's reliability is improved by guaranteeing the absence of a single point of failure, which is achieved through device interconnection and transaction replication across the blockchain. While automatically establishing trust through cryptographic protocols, blockchain provides enhanced security against malicious intrusions, such as distributed denial of service. Lastly, it adds a layer of privacy that is not present in centralized IoT architectures by ensuring data security and protection against tampering [1].

The advantages of decentralizing the IoT network include improved security and privacy, as well as reduced maintenance costs. However, due to the limitations of IoT devices in terms of computing capacity, power, and storage, the energy efficiency and implementation of these features in the IoT remain uncertain [1]. Therefore, IoT devices are generally not connected to the blockchain network. These limitations prevent them from fully

participating in the blockchain network, which would require tracking network transactions and locally storing a complete copy of the blockchain. Although there are cost-effective solutions that rely on other nodes and do not require full local storage of blockchain data [7][8].

The problems related to the application of blockchain technology in the context of the IoT have been addressed in a variety of research [9]. However, most of these writings have shortcomings in one or more of the following areas: data trust, transparency, moderate consensus, use of smart contracts, and Oracles.

In this paper, we propose a lightweight trust architecture that solves the challenges associated with integrating blockchain into the context of IoT. To improve accessibility for a variety of IoT scenarios with limited resources, our method uses delegated nodes instead of directly integrating blockchain technology into IoT devices. Delegated nodes allow communication with the blockchain network instead of IoT devices. Their functioning is based on smart contract, which reduces communication costs between them and simplifies the entire process on the blockchain network. The delegated nodes control the IoT devices based on smart contracts and an authentication consensus, ensuring trust in the data transmitted by these IoT devices. This topic has not been addressed by several works [5][10].

The rest of this paper is structured as follows: in section II, we present an overview of IoT and blockchain technology. Section III provides an overview of some suggested BCoT architectures. Section IV explains our contribution. In section IV, we detail the architecture we have developed. Finally, section VI summarizes the conclusions of the paper and perspectives.

I. Overview of Blockchain and IoT

A. Internet of things (IoT)

In September 2003, the Auto-ID Center presented its vision of a supply chain management that is automatically traceable, giving rise to the concept of the IoT. The IoT emerged from this advancement, leading to the creation of numerous small devices connected to the Internet for specific uses. It is considered a global infrastructure that connects many devices via the Internet [11]. Intelligent devices, capable of interacting and communicating with each other, are rapidly developing and have a significant impact on people's daily lives [12]. This category of devices includes sensors, actuators, mobile devices, and Radio Frequency Identification (RFID) tags, all of which have limited computing and communication capabilities. The remarkable decision of IPV6 to expand the addressing space leads to the creation of a fully functional IoT, capable of connecting billions of devices to unique addresses [13]. According to a survey by [14], smart devices, smart energy meters, wearable devices, connected cars, and smart healthcare devices are the most popular IoT applications. These devices are primarily useful in areas such as environmental monitoring, surveillance, smart cities, connected homes, and industrial equipment [15].

B. Blockchain

The blockchain is a distributed database based on distributed ledger technology (DLT). It consists of timestamped transactions that are managed by complex algorithms [16]. The transactions are stored in a peer-to-peer (P2P) network as successive blocks, and each participant, called a node, has a digital ledger. To reach a consensus, the nodes use a common algorithm [17]. There are numerous algorithms or consensus protocols used to perform transaction verification [18], and to add all blocks to the network [19]. Consensus algorithms are essential for achieving distributed agreements. They are designed to ensure the consistency, security, and reliability of data in the network [20]. Blockchain platforms use a decentralized P2P network to counter attacks, thus avoiding a centralized client-server architecture [21]. They integrate smart contracts to automate agreements, reducing costs and delays. These computer programs stored on the blockchain run automatically once the conditions are met, ensuring their immutability against any unauthorized modification [22]. Cryptography [23-24] is crucial for protecting blockchains, ensuring the integrity of contracts, access control, and preserving user privacy [25].

The blockchain is classified into three types: public, private, and hybrid/consortium [26]. The public blockchain is open to everyone, permissionless, enabling decentralized transactions. The private blockchain restricts access to authorized nodes for specific transactions [27]. The hybrid/consortium blockchain combines characteristics of public and private blockchains, offering semi-decentralization with multi-party consensus and oversight by a group of pre-established entities [28].

C. Integration of Blockchain with IoT (BCoT)

The recent development and emergence of new technologies have created multiple challenges in the field of the IoT. The distinctive characteristics of IoT have led to a variety of research problems. The diversity of IoT devices, communication protocols, and types of data (structured, semi-structured, and unstructured) are some of the aspects that demonstrate the heterogeneity of IoT systems. Additional challenges such as interoperability, privacy, and security stem from this heterogeneity [29]. The interoperability deficiency within IoT systems is exacerbated by the decentralization, diversity, complexity, and heterogeneity of IoT networks [30] [31]. Therefore, preserving data confidentiality is challenging [40]. Furthermore, the resource constraints of IoT devices compromise their security, making them vulnerable to malicious attacks [16] [29].

The use of blockchain technology can help overcome IoT issues such as heterogeneity, resource constraints, high vulnerability to adversarial attacks, and privacy concerns [25]. The blockchain strengthens the security of IoT devices by using encryption and cryptography to protect data, thus facilitating automatic software updates while preserving the security and confidentiality of information, thereby enhancing the resilience of IoT systems to compromises. Furthermore, it promotes the interoperability of IoT networks by recording information

about users and transactions, simplifying data processing and enabling secure communication between different IoT platforms or applications through its decentralized platform [33]. Blockchain technology enhances automatic interactions between IoT devices using smart contracts to strengthen security and reduce implementation costs [34]. It also ensures the reliability of Blockchain-IoT applications by ensuring the efficiency of the distributed network to authenticate information and maintain data integrity through the immutability of the blockchain [35]. Moreover, the traceability offered by the blockchain allows users to access, verify, and validate data at any time, monitoring each transaction to facilitate access to necessary information [36].

II. Related Work

Various research has been conducted on the integration of blockchain in the context of IoT. Fernandez-Carames et al. examined the current state of applications combining blockchain and IoT, while assessing the limitations related to the exploitation of blockchain in the field of IoT applications [9]. Furthermore, the blockchain, with the integration of smart contracts, has been implemented for various purposes. Choi et al. used blockchain smart contracts to enhance the security of IoT sensor control [37]. Novo et al. introduced an architecture for distributed IoT. This structure relies on the use of blockchain smart contracts to manage access permissions. It is based on a proof-of-concept consensus and a private blockchain to ensure information security [8]. However, it is important to note that the use of a private blockchain may restrict access to information of general interest to users. The study showed that waiting for access control information from the blockchain network introduces significant latency, leading to a deterioration in the overall system performance. Moudoud et al. proposed an architecture based on oracles and smart contracts, using a lightweight consensus characterized by reduced computational power, storage capacity, and latency [5]. However, the proposed solution relies on a single intermediary node, which may introduce a single point of failure.

A lightweight and scalable blockchain (LSB) specifically designed for the IoT was introduced in reference [38]. The block verification process of this blockchain utilizes a consensus algorithm tailored for IoT that incorporates a distributed trust mechanism. To strengthen end-to-end trust, Dedeoglu et al. proposed a layered structure that evaluates the reliability of data [10]. However, this work did not consider the use of smart contracts that utilize a formal model to establish a distribution of responsibilities among stakeholders, which is beneficial for the implementation of rules and policies. The study conducted by [39] proposes distributed trust methods. However, these approaches do not consider the auditability, transparency, and trust mechanisms specific to blockchain technology. In [40], Yan et al conducted a survey on IoT trust management mechanisms and their objectives. The survey revealed that blockchain-based applications require decentralization of trust and reputation management mechanisms. The researchers Lu and his team, in their study [41], introduced the concept of a system that verifies the reliability of messages from vehicle-related applications based on the reputation score of the involved vehicles. In their study [42], Kang et al. presented a model that relies on efficient reputation management and combines a consortium blockchain, smart contracts, and a subjective logical model. A distributed trust management model was proposed by researchers in the study cited in [7] to evaluate the credibility of messages exchanged in vehicle networks using blockchain technology by utilizing the reputation of observers as a reference criterion.

A systematic review of the literature on the use of blockchain in the context of the IoT was conducted by Conocenti et al. [43]. Their research identified several articles on the management of IoT device data. For example, [44] proposes a data authenticity verification system and [45] proposes a means to ensure the protection of data ownership created by IoT devices. Access control solutions for the IoT are examined in detail in reference [46]. This study focuses on the access control mechanisms currently used in the IoT and suggests that current Internet protocols are not suitable for all scenarios related to resource-constrained environments.

A. Discussion

In summary, some previous blockchain systems dedicated to IoT have encountered issues such as insufficient security levels, high management costs, and problems with monitoring transmission techniques and data trust [5][8][39]. Furthermore, due to the variety of cryptographic schemes and consensus algorithms used, the instant integration of blockchain technologies into IoT networks significantly increases computational complexity [46].

Current methods for ensuring trust in blockchain-based IoT applications generally focus either on improving trust in IoT data through the data capture process or on interactions between nodes participating in the blockchain network [10][40]. Therefore, they are unable to offer a lightweight architecture that does not integrate IoT devices into the blockchain and ensures overall data trust from source to validation in the blockchain.

To overcome these challenges, we propose a scalable lightweight architecture based on blockchain that takes into consideration the constraints of IoT devices and ensures data trust.

III. Proposed architecture principle

The article contributes to the creation of a lightweight architecture for the IoT using blockchain technology. Our method distinguishes itself from other solutions [10][47] due to its specific implementation to avoid direct integration of blockchain technology into IoT devices. Our solution is easier to use in many IoT scenarios characterized by limited capabilities with this method.

Unlike other solutions [5][8], our design uses delegated nodes that ensure trust in IoT device data. It uses authentication consensus to validate the data. It operates within a smart contract, simplifying the entire process within the blockchain network and reducing communication costs between nodes.

IV. LIGHTWEIGHT BCOT ARCHITECTURE

The integration of blockchain into an IoT system enhances the overall system security. All security and privacy features compatible with IoT are incorporated into the blockchain. The proposed lightweight architecture is depicted in Figure 1. This architecture consists of four layers, namely the perception layer, management layer, blockchain layer, and storage layer. Each layer of the proposed architecture is briefly described in the following subsections.

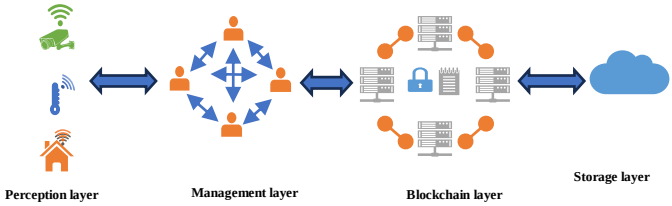

Figure 1: lightweight architecture to integrate blockchain into IoT.

A. *Perception layer*

In the proposed architecture, the perception layer consists of IoT devices such as sensors, surveillance cameras, RFID cards, etc. These devices are characterized by limited computing power, storage capacity, and energy autonomy. The IoT devices are not part of the blockchain network; they collect data and send it to a blockchain network through delegated nodes.

B. *Management layer*

Due to their significant limitations in terms of CPU, memory, and battery, IoT devices are not part of the blockchain network. Their ability to fully integrate with the blockchain network, which would involve locally storing a complete copy of the blockchain and keeping track of network transactions, is limited by these constraints. There are lighter alternatives that do not locally record all blockchain data and rely on other nodes [48], but these solutions remain too difficult to use for most IoT devices. Therefore, we have decided to use delegated nodes that allow connecting constrained IoT networks to the blockchain network. The delegated node registers IoT devices under its control, ensuring the trustworthiness of the data captured by these devices.

The delegated node is connected to a blockchain node. It translates messages from IoT devices into messages understandable by the blockchain node. Multiple IoT devices can register under the control of the same delegated node, and multiple delegated nodes can connect to the same blockchain node.

C. *Blockchain layer*

Public, consortium, and private ledgers make up the blockchain (BC) [49]. Public BCs allow anyone to join the network, and all members are responsible for validating transactions. Consortium BC is partially decentralized, with a number of members responsible for consensus, often created by multiple organizations. Finally, private BC is usually implemented by a single company or organization and limits access to network members only.

We present a lightweight architecture that integrates a private blockchain, for simplicity, characterized by a lightweight block creation process inspired by [50], adaptive block validation based on smart contracts, and authentication consensus among blockchain nodes.

- *Lightweight Block Generation*: In a private blockchain network, delegated nodes participate in block generation, block validation, and authentication consensus at the blockchain layer. We propose a lightweight block generation mechanism where blocks are generated at regular intervals by delegated nodes. The delegated node validates all associated sensor transactions after receiving and verifying them. Then, it creates a block of transactions containing observation data, the public key, and the data source's signature. The delegated node waits until it is ready to broadcast the block to other blockchain nodes for validation. The block generation delays of delegated nodes can be adjusted based on the sensor data throughput and the latency associated with data collection and generation.
- *Authentication consensus*: In distributed systems, consensus is a major challenge as it requires the mutual agreement of two or more agents on an important value for computational operations. Reliability has become essential, especially when some agents are no longer trustworthy. Blockchains use various algorithms to solve this problem, including proof of work (PoW), proof of stake (PoS) [51], proof of storage [52], proof of burn, and proof of capacity. In our proposed structure, we use "proof of authentication" (PoAh) to modify the blockchain. Figure 2 represents the operational scheme of the PoAh consensus algorithm [53].

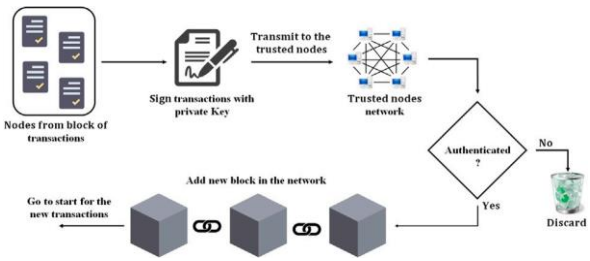

Figure 2: Authentication Consensus Algorithm [53].

At the beginning of the procedure, delegate nodes create transactions with the collected data to create a block. After a private key is used by the delegate nodes to sign the transaction and broadcast it on the network. When a block is received in the network, trusted nodes search for the sender's public key to verify the signature.

After successfully verifying the signature, the MAC address is evaluated by trusted nodes and compared to the one received during the second evaluation step. Following authentication, trusted nodes broadcast the validated blocks with a PoAh identification. In order to add blocks to the chain, individual users in the network verify the PoAh information. Once a valid block is accepted, the block's hash is calculated to link it with the next block, and the hash of the previous block is recorded in the current block [53].

The PoAh approach uses a conventional blockchain working model with minor block verification [53]. To make the transaction process faster, it eliminates the reverse hash function used in the PoW approach. Therefore, blockchains can be effectively integrated into resource-limited devices in the Industrial IoT.

- *Smart contracts:* The use of smart contracts in the blockchain provides a transparent, secure, and decentralized way to manage data related to IoT devices. IoT devices use a smart contract for message transmission within the context of the blockchain. Authentication is done by applying a digital signature to the message using the owner's private key, ensuring the legitimate origin of the message. The possibility of "man-in-the-middle" attacks, replay attacks, and other types of attacks are eliminated in this method [54]. The smart contract defines all possible operations and permissions in our system, and they are triggered by blockchain transactions. The smart contract includes functions for recording, updating, and retrieving information from IoT devices. When an IoT device is added to the network, its information (such as unique ID, owner, manufacturing date, etc.) is recorded in the smart contract. The data recorded in the blockchain cannot be modified as it is immutable. This allows for complete traceability of the history of modifications made to the information of each device.

D. Storage layer

The cloud allows for the storage of raw data received from the network of delegated nodes. Each delegated node can allocate cloud space to store data from the devices it manages, accompanied by a Cloud public key. This process ensures proper data routing and enables reliable source identification. The hash of the received data can be stored on the private blockchain.

V. CONCLUSION

In this paper, we addressed the problem of integrating blockchain technology into IoT devices and ensuring trust in the data captured by these devices. The constrained nature of these devices remains a barrier to integrating blockchain technology into IoT systems. Therefore, a lightweight architecture must be designed to adapt to the scenarios of resource-limited devices. In this paper, we presented a blockchain architecture for IoT based on delegated nodes. This lightweight architecture demonstrates how IoT devices collect data, transmit it to a blockchain network via delegated nodes, and how this data is stored and validated on the blockchain network using authentication consensus. It should be noted that API interfaces can be used to allow developers to create applications for visualizing and interacting with IoT data stored on the blockchain network.

REFERENCES

[1] Pavithran, D.; Shaalan, K.; Al-Karaki, J.N.; Gawanmeh, A. Towards Building a Blockchain Framework for IoT. *Cluster Comput.*2020, *23*, 2089–2103

[2] [2] E. D. Ngangue Ndih, S. Cherkaoui, and I. Dayoub, "Analytic Modeling of the Coexistence of IEEE 802.15.4 and IEEE 802.11 in Saturation Conditions," *IEEE Communications Letters*, vol. 19, no. 11, pp. 1981–1984, Nov. 2015.

[3] A. Aris, S. F. Oktug, and T. Voigt, "Security of Internet of Things for Reliable Internet of Services," p. 36

[4] M. Conoscenti, A. Vetro, and J. C. D. Martin, "Blockchain for the ` Internet of Things: A systematic literature review," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Nov. 2016, pp. 1–6

[5] Hajar Moudoud , Soumaya Cherkaoui , Lyes Khoukhi , "An IoT Blockchain Architecture Using Oracles and Smart Contracts: the Use-Case of a Food Supply Chain" arXiv:2201.11370v1 [cs.NI] 27 Jan 2022

[6] Sun, J., Yan, J., Zhang, K.Z.: Blockchain-based sharing services:What blockchain technology can contribute to smart cities.Financ. Innov. 2(1), 26 (2016)

[7] A. Kchaou, R. Abassi, and S. Guemara, "Toward a distributed trust management scheme for vanet," Proceedings of the 13th International Conference on Availability, Reliability and Security, 2018, pp. 53:1-53:6

[8] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2,pp. 1184–1195, Apr. 2018.

[9] T. M. Fernandez-Caram ´ es and P. Fraga-Lamas, "A Review on the Use ´of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp.32 979–33 001, 2018

[10] Dedeoglu, V.; Jurdak, R.; Putra, G.D.; Dorri, A.; Kanhere, S.S. A Trust Architecture for Blockchain in IoT. In Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous), Houston, TX, USA, 12–14 November 2019; ACM: New York, NY, USA; pp. 190–199. [CrossRef]

[11] Da Xu, L., He, W., Li, S.: Internet of things in industries: a survey. IEEE Trans. Ind. Inform. 10(4), 2233–2243 (2014).

[12] Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. 54(15), 2787–2805 (2010).

[13] Foote K.: A brief history of the internet of things—DATAVERSITY.DATAVERSITY. https://www.dataversity.net/briefhistory-internet-things/(2016). Accessed 30 Aug 2019.

[14] Gsma.com. https://www.gsma.com/newsroom/wp-content/uploads/15625-Connected-Living-Report.pdf (2018). Accessed 30 Aug 2019

[15] Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Internet of things: vision, applications and research challenges. Ad hoc Netw. 10(7), 1497–1516 (2012)

[16] P. Patil, M. Sangeetha, V. Bhaskar, Blockchain for IoT access control, security and privacy: a review, Wirel. Pers. Commun. 117 (3) (2021) 1815–1834.

[17] Y. Wang, S. Cai, C. Lin, Z. Chen, T. Wang, Z. Gao, C. Zhou, Study of blockchains's consensus mechanism based on credit, IEEE Access 7 (2019) 10224–10231.

[18] S. Velliangiri, P. Karthikeyan, Blockchain technology: challenges and security issues in consensus algorithm, in: 2020 International Conference on Computer Communication and Informatics, ICCCI, IEEE, 2020, pp. 1–8.

[19] T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: A state of the art survey, IEEE Commun. Surv. Tutor. 21 (1) (2018) 858–880.

[20] A. Yazdinejad, G. Srivastava, R.M. Parizi, A. Dehghantanha, H. Karimipour, S.R. Karizno, SLPoW: Secure and low latency proof of work protocol for blockchain in green IoT networks, in: 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), IEEE, 2020, pp. 1–5.

[21] R.T. Frahat, M.M. Monowar, S.M. Buhari, Secure and scalable trust management model for IoT P2P network, in: 2019 2nd International Conference on Computer Applications & Information Security, ICCAIS, IEEE, 2019, pp. 1–6.

[22] T.M. Hewa, Y. Hu, M. Liyanage, S.S. Kanhare, M. Ylianttila, Survey on blockchain-based smart contracts: Technical aspects and future research, IEEE Access 9 (2021) 87643–87662.

[23] B.K. Mohanta, S.S. Panda, D. Jena, An overview of smart contract and use cases in blockchain technology, in: 2018 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT, IEEE, 2018, pp. 1–4.

[24] K. Yu, L. Tan, C. Yang, K.-K.R. Choo, A.K. Bashir, J.J. Rodrigues, T. Sato, A blockchain-based shamir's threshold cryptography scheme for data protection in industrial internet of things settings, IEEE Internet Things J. (2021).

[25] M. Al-Shabi, A survey on symmetric and asymmetric cryptography algorithms in information security, Int. J. Sci. Res. Publ. (IJSRP) 9 (3) (2019) 576–589.

[26] D. Dasgupta, J.M. Shrein, K.D. Gupta, A survey of blockchain from security perspective, J. Bank. Financ. Technol. 3 (1) (2019) 1–17.

[27] R. Andreev, P. Andreeva, L. Krotov, E. Krotova, Review of blockchain technology: types of blockchain and their application, Intellekt. Sist. Proizv. 16 (1) (2018) 11–14.

[28] X. Zhang, X. Chen, Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network, IEEE Access 7 (2019) 58241–58254.

[29] H-N. Dai, Z. Zheng, Y. Zhang, "Blockchain for Internet of Things: A Survey" , arXiv:1906.00245v3 [cs.NI] 1 Sep 2019.

[30] M. Chen, Y. Miao, Y. Hao, and K. Hwang, "Narrow Band Internet of Things," *IEEE Access*, vol. 5, pp. 20 557–20 577, 2017.

[31] H.-N. Dai, H. Wang, G. Xu, J. Wan, and M. Imran, "Big data analytics for manufacturing internet of things: Opportunities, challenges and enabling technologies," *Enterprise Information Systems*, 2019.

[32] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, January 2017.

[33] M.H. Miraz, M. Ali, Integration of blockchain and IoT: an enhanced security perspective, 2020, arXiv preprint arXiv:2011.09121.

[34] J. Wu, F. Xiong, C. Li, Application of Internet of Things and blockchain technologies to improve accounting information quality, IEEE Access 7 (2019) 100090–100098.

[35] X. Lin, J. Li, J. Wu, H. Liang, W. Yang, Making knowledge tradable in edgeAI enabled IoT: A consortium blockchain-based efficient and incentive approach, IEEE Trans. Ind. Inform. 15 (12) (2019) 6367–6378.

[36] S. Wang, D. Li, Y. Zhang, J. Chen, Smart contract-based product traceability system in the supply chain scenario, IEEE Access 7 (2019) 115122–115133.

[37] S. S. Choi, J. W. Burm, W. Sung, J. W. Jang, and Y. J. Reo, "A Blockchain-based Secure IoT Control Scheme," in *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, Jun. 2018, pp. 74–78

[38] A. Dorri, S.S. Kanhere, R. Jurdak, and P. Gauravaram. "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy." Journal of Parallel and Distributed Computing (forthcoming), 2019. available online: https://arxiv.org/pdf/1712.02969.pdf

[39] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, Volume 76, 2015, pp146-164.

[40] Z. Yan, P. Zhang, A. V. Vasilakos, "A survey on trust management for Internet of Things", J. Netw. Comput. Appl., vol. 42, pp. 120–134, June 2014.

[41] Z. Lu, W. Liu, Q. Wang, G. Qu and Z. Liu, "A Privacy-Preserving Trust Model Based on Blockchain for VANETs," in IEEE Access, vol. 6, pp. 45655-45664, 2018.

[42] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang. "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks." IEEE Internet of Things Journal(2018).

[43] M. Conoscenti, A. Vetr, and J. C. D. Martin, "Blockchain for the Internet of Things: a Systematic Literature Review," *The Third International Symposium on Internet of Things: Systems, Management and Security (IOTSMS 2016)*, 2016.

[44] D. Wilson and G. Ateniese, "From Pretty Good To Great: Enhancing PGP using Bitcoin and the Blockchain." *CoRR*, vol. abs/1508.04868, 2015. [Online]. Available: http://dblp.uni-trier.de/db/journals/corr/corr1508.html#WilsonA15

[45] O. N. Guy Zyskind and A. S. Pentland. (2015) Decentralizing Privacy: Using Blockchain to Protect Personal Data.

[46] A. Ouaddah, H. Mousannif, A. A. E. Kalam, and A. A. Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," *Computer Networks*, vol. 112, pp. 237–262, 2017.[Online]. Available:http://dx.doi.org/10.1016/j.comnet.2016.11.007

[47] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, Z. Zou, A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things, https://doi.org/10.1016/j.jii.2020.100190 ; Accepted 29 November 2020, 2452-414X/2020 Elsevier Inc.

[48] "The Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT) system," 2015, [IBM]. [Online]. Available: https://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf

[49] Satoshi Nakamoto, A. Bitcoin, A peer-to-peer electronic cash system, Bitcoin (2008) URL: https://bitcoin.org/bitcoin.pdf

[50] A. Dorri, S.S. Kanhere, R. Jurdak, and P. Gauravaram. "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy." Journal of Parallel and Distributed Computing (forthcoming), 2019. available online:https://arxiv.org/pdf/1712.02969.pdf

[51] K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, "Deypos: Deduplicatable dynamic proof of storage for multi-user environments," *IEEE Transactions on Computers*, vol. 65, no. 12, pp. 3631–3645, Dec 2016.

[52] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20,2015, Proceedings, Part II*, 2015, pp. 585–605. [Online]. Available: https://doi.org/10.1007/978-3-662-48000-7 29

[53] Deepak Puthal, Saraju P. Mohanty, Proof of authentication: IoT-friendly blockchains, IEEE Potentials 38 (1) (2018) 26–29.

[54] Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media Inc, Newton (2015).