Internet of Things and Blockchain Integration

Subjects: Computer Science, Interdisciplinary Applications

Contributor: Yehia Ibrahim Alzoubi, Ahmad Al-Ahmad, Hasan Kahtan, Ashraf Jaradat

The Internet of things model enables a world in which all of our everyday devices can be integrated and communicate with each other and their surroundings to gather and share data and simplify task implementation.

Keywords: BC ; BIoT ; challenge ; integration ; trend

1. Introduction

Academics, researchers, and entrepreneurs are all interested in the Internet of things (IoT) these days because of its ability to provide novel services across a wide range of applications such as COVID-19 [1] and intelligent healthcare [2]. The IoT connects diverse things and devices to establish a physical network where processing, sensing, and communication activities are automatically managed without human intervention [3]. In the last decade, there has been significant growth in the number of IoT devices on the market. The number of IoT devices on the market is nearing 25 billion, with predictions that this number will rise to 50 billion by the end of 2025 [4]. To achieve such massive development, new arrangements are required, such as following the centralized IoT–cloud approach. The organization's system for cloud computing and data processing is referred to as IoT–cloud architecture. Here, the cloud manages and visualizes data flows from IoT devices while processing and analyzing them [5]. Although this approach may work well today, the projected development indicates that new approaches will be required in the future [6][7] due to several challenges of the centralized IoT–cloud approach. The following are some of the problems that a centralized IoT–cloud architecture faces [8][9][10][11][12]: (1) if the centralized server fails, the entire network system is at risk of being paralyzed and interrupted; (2) data fraud makes it difficult for IoT devices owners to trust partners who have oversight and access to the collected data; (3) data maintained in centralized clouds lack accountability and traceability because they depend on a trusted third party to store and retain data; (4) the central architecture is no longer robust enough to handle vast amounts of data and end-to-end interactions as a result of the rapid growth of IoT applications. Furthermore, due to the variety of smart devices on the market, maintaining and updating these devices are almost impossible; (5) since transparency is critical for promoting security and trust when designing next-generation IoT solutions, open-source techniques should be considered; (6) because most safe cryptographic methods need a large amount of processing power and energy, the encryption process is a big barrier due to the heterogeneity and limited compute capacity of IoT devices; (7) due to the constantly increasing number of IoT devices number, relevant IoT ecosystems must accommodate future network development while also processing a huge volume of data exchanged in a high-performance manner. The abovementioned challenges cannot be achieved in centralized IoT–cloud architecture. These problems necessitate a rethinking of the IoT's structure. Although decentralized systems for enormous peer-to-peer (P2P) wireless sensor networks have been developed in the past to overcome the drawbacks of the centralized IoT–cloud architecture, security and privacy requirements were lacking until the advent of Blockchain (BC) technology [13].

BC can carry out, organize, and monitor transactions provided by several devices without the need for a centralized cloud. To validate a transaction, BC is a decentralized system that does not require trust among participants. Its origins can be traced back to the cryptocurrency Bitcoin system [14]. The integration of BC and IoT (BIoT) may result in several benefits [15][16][17][18] for IoT security. Firstly, it provides a P2P framework that does not require a middle layer such as a third trusted party. Secondly, BC technology has no single point of failure, and, when it is used with smart contracts, it enables more secure transactions, which protects against various scams since smart contracts provide access control and improve stability, confidentiality, and authentication. By ensuring the data are cryptographically encrypted and signed by the rightful sender, BC ensures data confidentiality and authentication. Thirdly, the capacity of the entire network can be expanded due to its P2P nature. Fourthly, BC enables transactions to be performed quickly. Once built and attached to the BC network, each IoT device will get symmetric key pair, eliminating the need for key management and delivery in the BC network. As a consequence, lightweight authentication protocols can be used. The need for computing and memory capacity in IoT devices can be met and organized by these lightweight protocols. Fifthly, the immutability of IoT using data

logs stored on BC ensures traceability and transparency. Lastly, due to its tamper-proof design and safe storage, BC may enable the secure release of software updates to IoT devices.

2. Blockchain Structure and Architecture

Distributed ledger technology (DLT) and directed acyclic graph (DAG) are revolutionizing the way information is shared [19]. DLT is a P2P network that maintains a decentralized database [20]. The ledger is validated and copied by each node. The BC is one kind of DLT. The BC divides data into blocks, which are subsequently chained together (connected) using an append-only structure. Although it is far from the only DLT data format, the chain-based block structure is the most widespread [21]. DLT may also be implemented using other data structures such as DAG. DAG, like BC, may store transactions. Nodes connected to at least one, but possibly many additional transactions describe these data transactions. Links, on the other hand, are precisely directed, pointing from a previous transaction to a current one. It is also worth noting that because DAGs are acyclic, they do not allow loops [22]. There are no blocks in DAGs, and no mining is conducted, compared to BC. While transactions may authenticate one another, they cannot validate themselves. Furthermore, while entering the DAG, at least one prior transaction must be authenticated before a new transaction may be created. Each new transaction must refer to the previous one [22]. The hashes of the parent transaction are signed by the new transaction, which then integrates them into the new transaction [23]. DAG and BC technologies are combined in hybrid DLTs. Bexam is a hybrid DLT that combines flexible chains with hierarchical nodes to give the security of BC, generating roughly 40 million transactions per second. Bexam is highly scalable and simple to incorporate into large-scale systems. Furthermore, processing resources and power consumption are low. Token technology is also used by Bexam to create transactions [23].

BC is a distributed and mutual ledger that keeps track of a constantly expanding list of blocks that are connected and guarded with cryptography. It is necessary to understand BC elements before diving into the activities of BC. The BC employs a decentralized architecture, with the user and data access permissions separated. The security problems associated with central controls are eliminated with BC-based applications [24]. To maintain data privacy and security, all processes are registered [25]. The BC, in a typical Bitcoin structure, is made up of three technical elements: a cryptographic hash function, a Merkle tree, and a BC. Hash functions are mathematical formulas that produce a lengthy sequence of characters as inputs. All of the previous inputs are combined into a single Merkle Tree, which links all of the transactions into the BC [26]. The block header is made up of the Merkle tree, the block stamp, and the preceding block header, which is a special ID. As a result, the BC uses the block header to track previous record history. The Merkle tree is a data structure for storing key-value pairs that are encrypted.

The Bitcoin BC system creates a secure public data reading process dependent on anonymity. Both nodes can instantly and safely validate and share data inside the device without any interference, thanks to agreements and protocols. The data in the BC system are encrypted and anonymized to different degrees. The most widely used hash functions in BC and cryptocurrencies are the SHA-256 series. There is no requirement to reveal or check each node's identity or relevant information unless lawfully necessary. Before being written into the BC, data must be checked with a timestamp (used to assure the uniqueness of the transactions). All can write and read data and nodes with maintenance functions in the BC system, which is free and transparent. Via open interfaces, anybody can query BC data and create similar applications.

When any participant or node in the network makes a transaction, it is broadcasted to all nodes in the network after a so-called signing process, which involves two steps: hashing and encryption to generate a digital signature. The process starts by hashing the transaction with some hash function, such as SHA-256, which yields the hash value. Then, the sender's private key encrypts the transaction, resulting in a digital signature. After that, the transaction, as well as the digital signature, are transmitted to the entire network [27][28]. A BC validator/miner is in charge of checking transactions on the network. After collecting a series of transactions, miners can begin the validation process by performing the following steps to ensure they are legal (i.e., no malicious transactions or double spends) [29]: (1) miners decode the digital signature using the sender's public key, resulting in a decrypted hash value; (2) the miners use the same hash function to generate a new hash value from the received address; (3) if the current hash value meets the decrypted hash value, the transaction has not been tampered with, and the integrity, verification, and non-repudiation requirements have been met; (4) each miner creates a block of authenticated transactions, and that the validation process is accordingly finished [29][30].

The hardware layer, data layer, network layer, consensus layer, incentive layer, contract layer, and application layer are the seven major layers in a basic BC architecture [21][22][31][32]. The elements of each layer are depicted in **Figure 1**.

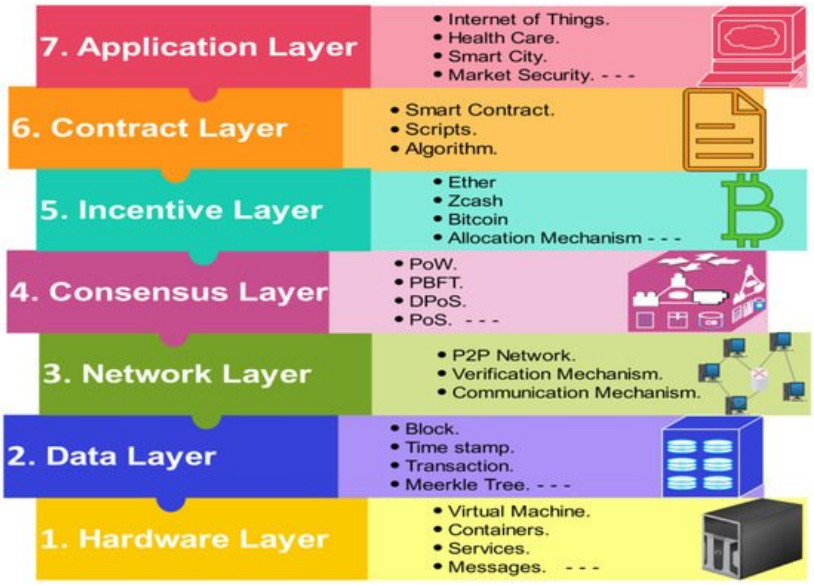

Figure 1. BC layered architecture.

(1)Hardware layer: Actuators, sensors, smart devices, controllers, and edge/fog nodes are all represented in this layer. The IoT is made up of these devices connected by a variety of wireless and wired communication protocols.

(2)Data layer: Blocks, transactions, the hash function, the digital signature, and the Merkle tree are all part of this layer. This layer collects IoT data from the lower layer in the form of transactions and encrypts it using asymmetric cryptographic methods, hashes, and digital signatures.

(3)Network layer: This layer serves as a P2P network on top of the communication layer. Only a network architecture that allows peers to trade resources without the participation of a third party allows for decentralization. While all P2P participants can operate as both a requestor and service providers, they can be divided into categories on the basis of the support services they provide, such as database, routing, and mining.

(4)Consensus layer: The distributed consensus necessary to verify a block's trustworthiness and guarantees that all peers have an accurate ledger copy are managed by this layer. However, owing to network failures, communication delays, or malevolent nodes, agents and nodes may end up with various perceptions of the system's status (i.e., forks). As a result, avoiding such forks is one of the problems of a consensus method.

(5)Incentive layer: The incentive layer is the heart of the BC network since it includes economic factors such as Ether (ETH) (a cryptocurrency that was created as a result of the confirmation of transactions on the Ethereum), Zcash (a protocol that provides a decentralized cryptocurrency, to store funds and generate a new private key for every new account [29]), and allocation methods to incentivize nodes to give their time and effort to data verification.

(6)Contract layer: This layer is in charge of digital money, as well as the design and management of smart contracts. Algorithms, smart contracts, and scripts are applied to allow more sophisticated transactions.

(7)Application layer: This layer offers services across a wide range of industries, including logistics, healthcare, IoT, and smart cities.

3. Blockchain Platforms

In general, two major categories can be identified for BC: permissionless and permissioned [20][21][22].

(1)Permissionless: This form of BC, also known as public BC, permits transactions to be viewable to all nodes. To authenticate a transaction, every node in the network can participate in BC consensus. The node does not require authorization, and it may be unknown to the rest of the network. Nodes in a permissionless network support and collaborate on a large scale. Each transaction is associated with a processing fee, which offers an incentive for peers looking to add additional blocks to the BC [33]. Because altering the contents of the permissionless BC would be prohibitively costly, it is immune to hacking. Each transaction comprises an incentive (i.e., transaction fees) to the peer that approves the transaction into a new block because the decentralized consensus involves hundreds of other peers [32]. Bitcoin is the most well-known permissionless cryptocurrency. Another well-known permissionless BC is Ethereum.

(2)Permissioned: This type of BC network may be classified as either private or consortium BCs.

- Private: These BCs are generally located in the heart of a single company that can verify transactions. Transactions may be read by the public or authorized parties. Private BCs operate without the need for money or tokens, and their transactions are fee-free [34]. Because blocks are broadcasted by surrogate nodes, a private BC is not as impenetrable to tampering as a public BC, but the firm may roll back its BC at any point in time. Multichain is an example of a private BC. Multichain is a Bitcoin fork with several features, including rights management, rapid setup, and data streams [35].

- Consortium: This type of BCs is managed by a small cluster of users from outside the group who are not allowed to confirm transactions. While the whole public may view transactions, only members of a limited group can write them. HLF is the most widely used and well-known federated BC. There are two sorts of HLF nodes: validating peers and nonvalidating peers. Validating peers are in charge of verifying transactions, establishing agreements, and keeping the ledger up to date. Nonvalidating peers can examine and verify transactions [32][36].

Due to the benefits that this technology provides, BC systems and implementation have recently arisen from a wide range of fields such as IoT, transportation, finance, eHealth, and energy applications. In the sections below, researchers survey some of the most widely used BC platforms. Since there are many platforms and they are constantly changing, it is difficult to study them all; thus, only the most common and most appropriate IoT domain platforms are surveyed (i.e., Bitcoin, Ethereum, HLF, and Multichain) [37]. Because investing in a specific BC technology is a mid- to long-term commitment, these are quite high levels of support. Some current systems are supported by a large number of individual developers, while others are supported by companies. The Ethereum Foundation, for example, is a nonprofit organization established in Switzerland, while the Bitcoin project has a large open-source development community [37]. IBM and the Linux Foundation support HLF. It is worth noting here that different authors refer differently to the specifications of the four platforms. The summary in the table is based on what was reported in [10][13][38][39][40].

Since many C platforms are built on Bitcoin BC, they share features such as using the proof-of-work (PoW) consensus protocol, not having specific hardware to generate new blocks, and being written in C++. All platforms use smart contracts, except for Bitcoin which does not use smart contracts. All the platforms do not use special hardware preparations, while only HLF and Multichain provide ID and key management, enable data confidentiality, and require trusted validators to validate the transactions.

It is essential to discuss the concept and functions of the smart contract in the context of BC platforms because they are a requirement of many BIoT platforms [41]. A smart contract is defined as a computerized protocol that implements a contract's terms [42]. A smart contract's ability to implement or self-execute contractual clauses is one of its most important characteristics [43]. Furthermore, smart contracts have greatly added to the energy of BC, and this integration has resulted in the second generation of BCs (i.e., BC 2.0). In a trustworthy environment, a mix of automatically executed contracts and no centralized oversight has the potential to revolutionize the way business is conducted today [43]. In essence, the smart contract code is stored on the BC, and each contract is known by a unique address, which users may access by sending a transaction to [23]. The BC consensus protocol ensures that the contract is executed correctly. Smart contracts provide several benefits, including cost savings, speed, accuracy, performance, and openness, which have prompted the development of a slew of new applications in a diversity of fields [44]. While Bitcoin includes a simple scripting language, it has proven inadequate, prompting the development of modern BC systems that provide Smart contract features [45].

Ethereum, the most common smart contract BC network, is a BC with a Turing-complete programming language that enables smart contracts and dispersed applications to be defined. Ethereum contracts are written in a stack-based bytecode language at a basic level called ‘‘Ethereum Virtual Machine (EVM) code” [46]. Financial smart contracts also require details about current events and states in the real world. The so-called oracles have this information. These institutions are essential for the efficient incorporation of smart contracts into the real world, but they add to the challenge by requiring authentication, confidentiality, and oracle trust [47].

The fact that all four most common BC platforms are open-source is a major factor in their success. While HLF and Multichain can provide high scalability and authentication, Bitcoin can provide low levels of authentication and scalability, and Ethereum can provide medium levels of scalability and authentication. Both Bitcoin and Ethereum are linked to a 51% attack level, while this value is 33% for HLF and Multichain. The security level provided by Bitcoin and Ethereum is low since the data are accessible to the public; however, the level is medium for HLF and high for Multichain. The privacy level is high when using HLF and Multichain, but low for Ethereum and Bitcoin since there is no authentication applied and they are publicly accessible.

References

1. Elbasi, E.; Topcu, A.E.; Mathew, S. Prediction of COVID-19 risk in public areas using IoT and machine learning. Electronics 2021, 10, 1677.
2. Thakur, N.; Han, C.Y. Indoor localization for personalized ambient assisted living of multiple users in multi-floor smart environments. Big Data Cogn. Comput. 2021, 5, 42.
3. Alzoubi, Y.I.; Osmanaj, V.H.; Jaradat, A.; Al-Ahmad, A. Fog computing security and privacy for the internet of thing applications: State-of-the-art. Secur. Priv. 2021, 4, e145.
4. Fernández-Caramés, T.M.; Fraga-Lamas, P. A review on the use of blockchain for the internet of things. IEEE Access 2018, 6, 32979–33001.
5. Ismail, S.; Almayouf, R.; Chehab, S.; Alghamdi, S.; Almutairi, A.; Alasmari, B.; Altherwy, R. Edge IoT-cloud framework based on blockchain. In Proceedings of the 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 13–15 October 2020; pp. 1–7.
6. Powell, W.; Foth, M.; Cao, S.; Natanelov, V. Garbage in garbage out: The precarious link between IoT and blockchain in food supply chains. J. Ind. Inf. Integr. 2022, 25, 100261.
7. Al-Ahmad, A.S.; Kahtan, H. Cloud computing review: Features and issues. In Proceedings of the 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Shah Alam, Malaysia, 11–12 July 2018; pp. 1–5.
8. Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. Electronics 2022, 11, 630.
9. Bala, K.; Kaur, P.D. Changing trends of blockchain in IoT: Benefits and challenges. In Proceedings of the 2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 27–28 January 2022; pp. 324–329.
10. Brotsis, S.; Limniotis, K.; Bendiab, G.; Kolokotronis, N.; Shiaeles, S. On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance. Comput. Netw. 2021, 191, 108005.
11. Al Sadawi, A.; Hassan, M.S.; Ndiaye, M. A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. IEEE Access 2021, 9, 54478–54497.
12. Hu, S.; Huang, S.; Huang, J.; Su, J. Blockchain and edge computing technology enabling organic agricultural supply chain: A framework solution to trust crisis. Comput. Ind. Eng. 2021, 153, 107079.
13. Bhushan, B.; Khamparia, A.; Sagayam, K.M.; Sharma, S.K.; Ahad, M.A.; Debnath, N.C. Blockchain for smart cities: A review of architectures, integration trends and future research directions. Sustain. Cities Soc. 2020, 61, 102360.
14. Nakamoto, S.; Bitcoin, A. A peer-to-peer electronic cash system. Bitcoin 2008, 4, 2.
15. Li, X.; Lu, W.; Xue, F.; Wu, L.; Zhao, R.; Lou, J.; Xu, J. Blockchain-Enabled IoT-BIM Platform for Supply Chain Management in Modular Construction. J. Constr. Eng. Manag. 2022, 148, 04021195.
16. Rayes, A.; Salam, S. The Blockchain in IoT. In Internet of Things from Hype to Reality; Springer: Berlin/Heidelberg, Germany, 2022; pp. 277–303.
17. Alzoubi, Y.I.; Al-Ahmad, A.; Jaradat, A. Fog computing security and privacy issues, open challenges, and blockchain solution: An overview. Int. J. Electr. Comput. Eng. 2021, 11, 5081–5088.
18. Khan, N.S.; Chishti, M.A. Security challenges in fog and IoT, blockchain technology and cell tree solutions: A review. Scalable Comput. 2020, 21, 515–542.
19. Arslan, S.S.; Jurdak, R.; Jelitto, J.; Krishnamachari, B. Advancements in distributed ledger technology for internet of things. Internet Things 2020, 9, 100114.
20. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of blockchains in the internet of things: A comprehensive survey. IEEE Commun. Surv. Tutor. 2018, 21, 1676–1717.
21. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Commun. Surv. Tutor. 2019, 21, 2794–2830.
22. Zafar, S.; Bhatti, K.; Shabbir, M.; Hashmat, F.; Akbar, A. Integration of blockchain and Internet of Things: Challenges and solutions. Ann. Telecommun. 2022, 77, 13–32.
23. Tsang, Y.; Wu, C.; Ip, W.; Shiau, W.-L. Exploring the intellectual cores of the blockchain–Internet of Things (BIoT). J. Enterp. Inf. Manag. 2021, 34, 1287–1317.

24. Huang, J.; Kong, L.; Chen, G.; Wu, M.-Y.; Liu, X.; Zeng, P. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Trans. Ind. Inform. 2019, 15, 3680–3689.
25. Sharma, P.K.; Park, J.H. Blockchain based hybrid network architecture for the smart city. Future Gener. Comput. Syst. 2018, 86, 650–655.
26. Ouaddah, A.; Abou Elkalam, A.; Ouahman, A.A. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In Europe and MENA Cooperation Advances in Information and Communication Technologies; Springer: Cham, Switzerland, 2017; Volume 520, pp. 523–533.
27. Alzubi, J.A. Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare. Comput. Commun. 2021, 170, 200–208.
28. Rahulamathavan, Y.; Phan, R.C.-W.; Rajarajan, M.; Misra, S.; Kondoz, A. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, India, 17–20 December 2017; pp. 1–6.
29. Qatawneh, M.; Almobaideen, W.; AbuAlghanam, O. Challenges of blockchain technology in context internet of things: A survey. Int. J. Comput. Appl. 2020, 175, 14–20.
30. Lu, Y. Blockchain and the related issues: A review of current research topics. J. Manag. Anal. 2018, 5, 231–255.
31. Jo, B.W.; Khan, R.M.A.; Lee, Y.-S. Hybrid blockchain and internet-of-things network for underground structure health monitoring. Sensors 2018, 18, 4268.
32. Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. IEEE Commun. Surv. Tutor. 2019, 21, 1508–1532.
33. Abdellatif, A.A.; Samara, L.; Mohamed, A.; Erbad, A.; Chiasserini, C.F.; Guizani, M.; O'Connor, M.D.; Laughton, J. MEdge-Chain: Leveraging edge computing and blockchain for efficient medical data exchange. IEEE Internet Things J. 2021, 8, 15762–15775.
34. Berdik, D.; Otoum, S.; Schmidt, N.; Porter, D.; Jararweh, Y. A survey on blockchain for information systems management and security. Inf. Process. Manag. 2021, 58, 102397.
35. Chang, Z.; Guo, W.; Guo, X.; Chen, T.; Min, G.; Abualnaja, K.M.; Mumtaz, S. Blockchain-Empowered drone networks: Architecture, features, and future. IEEE Netw. 2021, 35, 86–93.
36. Yuan, P.; Zheng, K.; Xiong, X.; Zhang, K.; Lei, L. Performance modeling and analysis of a hyperledger-based system using GSPN. Comput. Commun. 2020, 153, 117–124.
37. Yang, H.-K.; Cha, H.-J.; Song, Y.-J. Secure identifier management based on blockchain technology in NDN environment. IEEE Access 2018, 7, 6262–6268.
38. Rizzardi, A.; Sicari, S.; Miorandi, D.; Coen-Porisini, A. Securing the access control policies to the Internet of Things resources through permissioned blockchain. Concurr. Comput. Pract. Exp. 2022, 34, e6934.
39. Kuo, T.-T.; Zavaleta Rojas, H.; Ohno-Machado, L. Comparison of blockchain platforms: A systematic review and healthcare examples. J. Am. Med. Inform. Assoc. 2019, 26, 462–478.
40. Paulavičius, R.; Grigaitis, S.; Igumenov, A.; Filatovas, E. A decade of blockchain: Review of the current status, challenges, and future directions. Informatica 2019, 30, 729–748.
41. Lone, A.H.; Naaz, R. Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review. Comput. Sci. Rev. 2021, 39, 100360.
42. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. 2018, 88, 173–190.
43. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.-Y. Blockchain-enabled smart contracts: Architecture, applications, and future trends. IEEE Trans. Syst. Man Cybern. Syst. 2019, 49, 2266–2277.
44. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. 2018, 42, 130.
45. Ghandour, A.G.; Elhoseny, M.; Hassanien, A.E. Blockchains for smart cities: A survey. In Security in Smart Cities: Models, Applications, and Challenges; Hassanien, A.E., Elhoseny, M., Ahmed, S., Singh, A., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 193–210.
46. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for internet of things. Comput. Commun. 2019, 136, 10–29.
47. Fotiou, N.; Siris, V.A.; Polyzos, G.C. Interacting with the Internet of Things Using Smart Contracts and Blockchain Technologies. In Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2018;

Wang, G., Chen, J., Yang, L., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2018.