A Systematic Literature Review on Blockchain-based Solutions for IoT Security

Ala Ekramifard[1], Haleh Amintoosi[2,*] and Amin Hosseini Seno[3]

[1, 2, 3] Computer Engineering Department, Faculty of Engineering,
Ferdowsi University of Mashhad, Mashhad, Iran
{ekramifard,amintoosi,Hosseini}@um.ac.ir

Abstract. Nowadays, we are facing an exponential growth in the Internet of Things (IoT). There are over 8 billion IoT devices such as physical devices, vehicles and home appliances around the world. Despite its impact and benefits, IoT is still vulnerable against privacy and security threats, due to the limited resources of most IoT devices, lack of privacy considerations and scalability issues, thus making traditional security and privacy approaches ineffective for IoT. The main goal of this article is to investigate whether the Blockchain technology can be employed to address security challenges of IoT. At first, a Systematic Literature Review was conducted on Blockchain with the aim of gathering knowledge on the state-of-the-art usages of Blockchain technology. We found 44 use cases of Blockchain in the literature from which, 18 use cases were specifically designed for the application of Blockchain in addressing IoT-related security issues. We classified the state-of-the-art use cases in four domains, namely, smart cities, smart home, smart economy and smart health. We highlight the achievements, present the methodologies and lessons learnt, and identify limitations and research challenges.

Keywords: Internet of Things, Blockchain, Security, Privacy

1 Introduction

Internet of Things represents a collection of heterogeneous devices that communicate with each other automatically. It has been widely used in many aspects of human life, such as industrial, healthcare systems, environmental monitoring, smart city, building and smart home, etc. IoT devises create, collect, and process privacy-sensitive information and send them to cloud via Internet, generating mass of valuable information that can be targeted by attackers. Moreover, most IoT devices have limited power and capacity, making the usage of traditional security solutions computationally expensive. In addition, most well-known security solutions are centralized and are not compatible with the distributed nature of IoT. Hence, there is a vital demand for a lightweight, distributed and scalable solution to provide IoT security.

Blockchain is a distributed ledger that is used to provides electronic transactions security, and at the same time guaranteeing the auditability and nonrepudiation. In Blockchain, cryptography is used to provide secure ledger management for each node without needing a central manager. Blockchain can help to develop decentralized applications running on billions of devices. It has prominent features such as security,

* Corresponding Author

immutability and privacy, and therefore can be a useful technology to address the security challenges of many applications.
In this paper, we performed a systematic literature review on the state-of-the-art to investigate the possibility of leveraging Blockchain to provide security and privacy for IoT applications in four categories: smart cities, smart home, smart economy and smart health.
The rest of the paper is organized as follows. The main structure of IoT and Blockchain as well as the research goal and research questions of the systematic review and its process are expressed in Section 2. Section 3 presents an overview on the Blockchain-based security solutions for IoT, according to the above-mentioned categories and the results obtained from the literature review. Section 4 presents the conclusion and open challenges.

2 Research Design

2.1 IoT Security and Privacy

IoT contains heterogeneous devices with embedded sensors interconnected through a network, which are uniquely identifiable and mostly characterized by low power, small memory and limited processing capability. The gateways are deployed to connect these devices to the cloud for remote provision of data and services to users [1].
IoT applications have very different objectives, from a simple appliance for a smart home to equipment for an industrial plant. Generally, IoT operations include three distinct phases: collection phase, transmission phase, and processing and utilization phase. Sensing devices, which are usually small and resource constrained, collect data from environment. Technologies for this phase operate at limited data rates and short distances, with constrained memory capacity and low energy consumption. These collected data transmit to applications with transmission technologies that are more powerful. In last phase applications process collected data to obtain useful information and take decisions to controlling the physical objects and act on the environment [2].
Due to development of hardware and network facilities, the use of IoT is expanding rapidly in everyday life. Hence, providing security and privacy in this field is very important. Security and privacy are fundamental principles of any information system. Security is the combination of integrity, availability, and confidentiality that can be obtained by authentication, authorization, and identification. Privacy is defined as the right that an individual has to share his information [3].
There are three main challenges in IoT that make traditional security solutions ineffective. First, most IoT devices have limited bandwidth, memory and computation capability which makes them inefficient for complex cryptographic algorithms. Second, IoT is subject to scalability challenge since there may be billions of devices connecting to a cloud server that may result in bottleneck problem. Third, devices normally report raw data to the server, resulting in the violation of users' privacy. Therefore, new security technologies will be required to protect IoT devices and platforms. To ensure the confidentiality, integrity, and privacy of data, proper

encryption mechanisms are needed. To secure communication between devices and privileged access to services, the authentication is required. Various mechanisms need to guarantee availability of services and prevent denial-of-service, sinkhole, replay, and others attacks. Various components of IoT like applications, framework, network, and physical devices have specific vulnerabilities and variety of different solutions have been implemented. A comprehensive review on security issues in IoT has been presented in [1].

2.2 Blockchain

Blockchain is a decentralized, distributed, and immutable database ledger that stores transactions and events in a peer-to-peer network. It is known as the fifth evolution of computing, the missing trust layer for the Internet. Bitcoin was the first innovation that introduced Blockchain. It is a decentralized cryptocurrency, which can be used to buy and exchange goods [3].

Blockchain is chained blocks of stored data transactions that are validated by miners. Each block includes a hash, time stamped sets of recent valid transactions, and the hash of the previous block. When a user requests a transaction, first it is transmitted to the network. The network checks it for validation and the valid transaction is added to the current block and then chained to the older blocks of transactions [5].

Blockchain provide immutability and verifiability by mixing hash functions and Merkle trees. Hash is the one-way mapping function, which transforms data of any size into short, fixed-length values. Merkle tree takes many hashes and squeezes them to one hash. To construct a new Merkle tree, leaf nodes that contain data are hashed and parent nodes combine pairs of hashes to calculate a new hash node. This process is continued until the root of the tree is constructed. Each block in Blockchain contains the root of this tree as well as all transactions within the block [5, 6].

Blockchain can be built as a private network that can be restricted to a certain group of participants, or public network that is open for anyone to join in like Bitcoin [1]. Blockchain does not have a central authority. In public Blockchain, when participants are anonymous, a malicious attacker may want to corrupt the history of data. Bitcoin for example, prevents this by using a consensus mechanism called proof of work (PoW) which is the Byzantine problem solving. Every machine that stores a copy of the ledger tries to solve a complex puzzle based on its version of the ledger. The first machine who solves the puzzle wins and all other machines update their ledgers with winner [5].

Blockchain has some advantages over existing electronic frameworks like transparency, low or no exchange costs, network security and financial data assurance [3]. In addition to cryptocurrencies applications, public ledger and a decentralized environment can be used in various applications like IoT, smart contracts, smart property, and digital content distribution [7]. When information has been written into a Blockchain database, it is nearly impossible to remove or change, so it leads to trust in digital data. Therefore, data is reliable and we can transact business online.

2.3 Research Goal and Questions

The goal of this research is to investigate whether and to what extend the Blockchain technology is able to address the security and privacy issues of IoT. At first, a Systematic Literature Review was conducted on Blockchain with the aim of gathering knowledge on the state-of-the-art usages of Blockchain technology. To do so, we considered the following research questions:

- **RQ1:** How does Blockchain address the security and privacy issues of IoT in the domain of smart home?
- **RQ2:** How does Blockchain address the security and privacy issues of IoT in the domain of smart city?
- **RQ3:** How does Blockchain address the security and privacy issues of IoT in the domain of smart health?
- **RQ4:** How does Blockchain address the security and privacy issues of IoT in the domain of smart economy?

2.4 Search Process

The searches were conducted on 25th October 2018 and we processed all studies that had been published up to this date. To obtain the collection of relevant studies, we selected the key terms "Blockchain" and "IoT" to search in IEEE Xplore, ScienceDirect, DBLP, and Google Scholar. The searches were run against the title, keywords and abstract. Duplicate studies were removed. The result was around 600 papers.

The results from these searches were filtered through the inclusion/exclusion criteria.

Inclusion Criteria are: 1) The paper must be an empirical study about usage of Blockchain in IoT applications. 2) The paper must emphasize on security. 3) The paper must have enough details about its approach.

Exclusion Criteria are: 1) Conference version of a study that has an extended journal version. 2) Non-English language papers.

The 'Abstract' of all 600 papers were read. After running the studies through the inclusion/exclusion criteria, 44 papers were remained for reading. These 44 papers were fully read and inclusion/exclusion criteria were re-applied, leaving 18 papers that specifically address the security issues related to the usage of Blockchain in IoT applications. It is worth mentioning that we conducted snowballing to make sure that no further papers were detected that met the inclusion criteria. (To be brief, snowballing refers to using the reference list of a paper or the citations to the paper to identify additional papers.)

Table 1. Use Cases of Blockchain in IoT Security

Paper	Category	Usage of Blockchain
[9]	Smart City	Increase security and privacy in vehicular ecosystem
[10]	Smart City	Distributed transport management

[11]	Smart City	Secure data transfer in Internet of Vehicles
[8,15]	Smart City	Smart Energy Grid
[12,13]	Smart City	Trusted data sharing environment
[16,17,18]	Smart Home	Secure lightweight architecture
[19]	Smart Home	Self-management identity
[20]	Smart Home	Authentication and secure communication
[21]	Smart Health	Control and share health data in an easy and secure way
[22]	Smart Health	Securely share health data
[23,24]	Smart Health	Access control
[29]	Smart Economy	Reliable energy trading
[30]	Smart Economy	Anonymous energy trading

3 Review Results

In this section, we review the related articles related to each research question and discuss the results.

3.1 RQ1: Use Cases Related to Smart City

Smart City is aimed at improving the life quality of citizens by integrating the ICT services and urban infrastructures. There are a large number of smart city applications and technologies to realize complex interactions between citizens, third parties, and city departments and most of them heavily rely on data collection, interconnectivity, and pervasiveness. Despite the benefits, they are major threats to the privacy of citizens [8]. Common security and privacy methods that are used in smart city tend to be ineffective due to some challenges, such as single point of failure centralized communication model and lack of users' privacy. Hence, decentralized privacy preserving and secure Blockchain-based architecture can help to face these challenges.

Authors in [9, 10, 11] proposed architectures based on Blockchain technology with the aim of preserving the security and privacy of vehicular systems. The paper in [9] discusses the efficacy of the proposed security architecture in some smart city applications like wireless remote software updates. To provide integrity, all transactions contain the hash of the data. Similarly, to provide confidentiality, transactions are encrypted via utilizing asymmetric encryption.

Authors in [10] proposed a reliable and secure vehicle network architecture based on Blockchain to build the distributed transport management system. In this model, to achieve scalability and high availability of the vehicle network, there are three kinds of nodes: controllers that are connected in a distributed manner to provide the necessary services on a large scale, miner node, which handles request/response requests and vehicle nodes that are just ordinary nodes which send a service request message either to miner or controller nodes. Controllers process and compute the data (including a hash, a timestamp, a nonce, and a Merkle root) and share it to other nodes in a

distributed manner. All communications are encrypted using the public/private keys to secure the privacy of the client's data.

Communication between vehicles must be secure to prevent malicious attacks, and it can be achieved by authenticating all nodes before connecting to the network. An authentication and secure data transfer algorithm, was proposed in Internet of Vehicles using the Blockchain technology in [11]. Each vehicle is made to register with the Register Authority (RA) to prevent any malicious vehicle to become a part of the network.

Authors in [12] proposed a data-sharing environment for intelligent vehicles that is aimed to provide the trust environment between the vehicles based on Blockchain. To ensuring secure communication between vehicles, this mechanism provides ubiquitous data access based on crypto unique ID and an immutable database. They also proposed Intelligent Vehicle Trust Point (IV-TP) mechanism, which provides trustworthiness for vehicles behavior [13]. IV-TP is an encrypted unique number, which is generated by the authorized authority. To provide secure vehicles communication, it uses Blockchain as follows: each vehicle generates its private and public key, and then digitally signs messages to ensure integrity and non-repudiation. Receiver verifies the digitally signed message and decrypts it.

Authors in [14] introduced a Blockchain-based intelligent transportation system, which is a seven-layer conceptual model. It consists of a physical layer that encapsulates data of various kinds of physical entities such as devices and vehicles. The data layer produces chained data blocks by using asymmetric encryption, time-stamping, hash algorithms and Merkle tree techniques. The network layer is responsible for communication among entities, data forwarding and verification. Consensus Layer includes various consensus algorithms like PoW and PoS. Incentive layer includes issuance and allocation mechanisms of economic reward of Blockchain. Contract Layer controls and manages physical and digital assets. Application Layer includes application scenarios and use cases.

The article in [15] used Blockchain to recharge the autonomous electric vehicles in intelligent transportation systems. This system includes three parts: a particular charging station as server, vehicles as client, and a smart contract. Charging station and cars communicate with each other through the channel that is opened and prices are per unit of charging. Other parameters have been set in a Blockchain as contract.

A Smart Energy Grid technology was proposed in [8] to improve the energy distribution capability for citizens in urban areas. The proposed method uses the Blockchain technology to join the Grid, exchange information, and buy/sell energy between energy providers and private citizens. *From review the literature in the domain of smart city, we conclude that the Blockchain can improve security in smart city specifically in two ways: secure data transfer in vehicular ecosystem and autonomous electric charging. Moreover, via Blockchain, the need for centralized companies to entrust users' data is eliminated.*

3.2 RQ2: Use Cases Related to Smart Home

Smart home is equipped with a number of IoT devices including a smart thermostat, smart bulbs, an IP camera and several other sensors. Smart devices should be able to store data on storages to be used by a service provider. Collection, processing and dissemination of data may result in the revealing of private behavior and lifestyle patterns of people [16].

Several works have addressed the challenges in ensuring security and privacy for smart home. A secure lightweight Blockchain-based architecture for smart home has been proposed in [16, 17, 18] that eliminates the concept of POW and the need for coins, to decrease the overhead of Blockchain. This architecture consists of three main tiers namely: smart home, overlay network, and cloud storage. Each smart home is equipped with a high resource device called "miner" that is responsible for handling all communication within and external to the home [17]. Nodes in the overlay network are grouped in clusters, to decrease network overhead and delay. Devices can store their data in the cloud storage, so that a service provider can access this data and provide certain smart services [16]. This work mostly focuses on data store and access control, in IoT devices. Data storage and access transactions have been stored as transactions in the Blockchain. The public keys are fixed with the cluster head. The proposed model has been analyzed against DDOS and linking attacks and the overhead of using their model over traditional message exchange models has been measured.

To overcome the problems of centralized identity management systems which are built basis on third-party identity providers, authors in [19] have proposed a Blockchain-based Identity Framework for IoT (BIFIT) in smart home. It provides self-management identity for devices in IoT environment, and helps casual users without technical expertise to manage and control them. This framework includes an autonomic monitoring system that relies on digital signature to control appliance behavior in order to detect any suspicious activities. In addition, it develops a unique identity for each device to correlate with its owner for the sake of ownership and security management.

The paper in [20] proposed an authentication and secure communication scheme in smart home based on Extended Merkle Tree and Keyless Signature Infrastructure (KSI). It provides authentication with a public key-secret key structure and generates integrity of the message by KSI's distributed server using the global timestamp value. It improves efficiency by eliminating the structure of the existing PKI based certificate system. *To conclude: Blockchain can be used for secure authentication, access control and communication in the domain of smart home. The main challenge, however, is the scalability issue due to the large size of Blockchain and cryptographic solutions which is not suitable for IoT devices with limited resources.*

3.3 RQ3: Use Cases Related to Smart Health

Sharing healthcare information makes healthcare systems smarter and improves the quality of their services. The analysis and storage of healthcare data must be done in a

secure way and should be kept private from other parties, as it may be used maliciously by attackers. To overcome these challenges, a Blockchain-based Healthcare Data Gateway (HDG) storage platform was proposed in [21] to enable patients to own, control and share their own data in an easy and secure way without violating privacy. It consists of three layers. The Storage layer stores data in the private Blockchain cloud and protects data with cryptographic techniques thus ensuring the medical data cannot be altered by anybody. The data management layer works as a gateway and evaluates all data accesses. The data usage layer includes entities that use patient healthcare data. Authors in [22] propose a secure healthcare system that is aimed at sharing health-related between the nodes in a secure manner. It contains two main security protocols: an authentication protocol between medical sensors and mobile devices in a wireless body area network and a Blockchain-based method to share heath data.

The work in [23] proposed a decentralized electronic medical records (MedRec) management system that was aimed handling secure information while managing security goals such as authentication, confidentiality and data sharing. It uses Ethereum as smart contract and stores information about ownership, permissions and integrity of medical records. It also uses cryptographic hash of the data to prevent tampering.

A secure, scalable access control mechanism for sensitive information has been proposed in [24]. It is a Blockchain-based data sharing method that permits data owners to access medical data from a shared repository after their identities and cryptographic keys have been verified. This system consists of three entities: users that want to access or contribute data, system management composed of entities responsible for identification, authentication and authorization process, and cloud-based data storage.

A softwarized infrastructure for secure and privacy preserving deployment of smart healthcare applications was proposed in [25]. The privacy of sensitive patient data is ensured using Tor and Blockchain, where Tor removes mapping between user IP address and Blockchain tracks and authorizes access to confidential medical records. This prevents records from being lost, wrongly modified, falsified or accessed without authorization. *To conclude: the most important security challenges in Smart Health are privacy preserving health data sharing, authorized access to such data and preserving the integrity of health data, From reviewing the literature in the domain of smart health, it has been documented that Blockchain-based solutions are able to guarantee the security requirements of health data to a great extent, without the need to trust a third party.*

3.4 RQ4: Use Cases Related to Smart Economy

Blockchain has been widely applied for financial transactions, generally called cryptocurrency. However, it is not the only use of Blockchain in economy. Researchers are trying to identify new solutions in various economic aspects utilizing Blockchain benefits. In fact, integrating IoT and Blockchain may lead to excellent opportunities to develop distributed shared economy. Automatic payment mechanisms, foreign exchange platforms, and digital rights management are some of these applications [26].

Blockchain can also be used to digitally track the ownership of assets across business collaborations or to capture information about the product from participants across the supply chain in secure and immutable manner [27].
Smart contract is a computerized transaction protocol that is written by users to be uploaded and executed on the Blockchain, so to increase the need for trusted intermediaries between parties [1]. Authors in [28] describe the benefit of Blockchain, IoT and smart contract combination in automation of multi-step processes and marketing services between devices. ADEPT, Filament, Watson IoT platform, and IOTA are some other economic scenarios that are explained in [3]. ADEPT builds a network of distributed devices that transmit transactions to each other and perform maintenance automatically by use of smart contracts to provide security. Filament allows devices to interact autonomously with each other, for example to sell environmental conditions data to a forecasting agency. Watson platform provides a private Blockchain to push IoT devices data so that business partners can access them in a secure manner. IOTA is a cryptocurrency for selling the data that is collected from IoT devices [3].
A decentralized energy-trading platform, without reliance on trusted third party was implemented in [29]. It is a token-based private system and all trading transactions are done anonymously, and data is replicated among all active nodes to protect from failure. It uses Blockchain, multi-signatures and anonymity of users to provide privacy and security.
Using IoT devices as smart meters in Smart Grid can lead to energy trading without the need of third party. Authors in [30] have proposed a reliable infrastructure to transactive energy, based on Blockchain and smart contracts, which helps energy consumers and producers to sell to each other directly without the involvement of other stakeholders. Using Blockchain in this architecture leads to the increased reliability, higher cost effectiveness, and improved security. *To conclude: by utilizing the Blockchain applications such as cryptocurrency and smart contract, it is possible to improve the reliability of smart economy and add anonymous trading to economic systems.*

4 Conclusion

In this paper, we conducted a systematic literature review on the recent works related to the application of Blockchain technology in providing IoT security and privacy. The goal of our research is to verify whether the Blockchain technology can be employed to address security challenges of IoT. We selected 18 use cases that are specifically related to applying Blockchain to preserve IoT security and categorized them into four domains: smart home, smart city, smart economy and smart health. Due to the decentralized nature of Blockchain, its inherent anonymity afforded and the provided secure network on untrusted parties, it has been gaining great attention in addressing the security challenges of IoT. In fact, Blockchain technology facilitates implementation of decentralized Inter-net of things' platforms and allows secure

recording and exchanging information. In this structure, the Blockchain plays the role of the ledger, and all exchanges of data on the intelligent devices are recorded safely. However, despite all the benefits, the Blockchain technology is not without shortcomings. Encryption that is used in Blockchain-based techniques is time and power consuming. IoT devices have very different computing capabilities, and not all of them are capable to run the encryption algorithms at the appropriate speed. Since Blockchain has a decentralized nature, scalability is one of the major challenges in this area. Size of the ledger will increase over time, and usually this size of data is more than the capacity of most IoT nodes. Since there are many nodes in IoT scenarios, we need a large number of keys for secure transactions between devices. These issues introduce new research challenges. Moreover, with the increasing use of IoT devices in real world, the number of malicious attacks to these tools increases. Therefore, there is a need for extensive researches on vulnerabilities in current technologies and the identification and counteraction to attacks. Most recent works that rely on Blockchain just introduce models or prototypes, without dealing with real implementations. There seems to be a need for more research to examine the performance of new models and designs.

Conflict of Interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. M. A. Khan and K. Salah. 2017. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82, 395-411.*
2. B. B. Zarpelão, et.al. 2017. A survey of intrusion detection in Internet of Things. *J. of Network and Computer Applications, 84, 25-37.*
3. E. F. Jesus, et.al. 2018. A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. *Security and Communication Networks*.
4. A. Banafa. 2017. IoT and Blockchain Convergence: Benefits and Challenges. IEEE Internet of Things. *IEEE Internet of Things*.
5. T. Laurence. 2017. Blockchain for Dummies. *Hoboken, New Jersey:John Wiley & Sons.*
6. R. Chitchyan and J. Murkin. 2018. Review of Blockchain Technology and its Expectations: Case of the Energy Sector. *arXiv preprint arXiv:1803.03567*.
7. J. Yli-Huumo, D. Ko, S. Choi, S. Park and K. Smolander. 2016. Where is current research on blockchain technology?—a systematic review. *PloS one, 11(10).*
8. A. Pieroni, et.al. 2018. Smarter City: Smart Energy Grid based on Blockchain Technology. *International Journal on Advanced Science, Engineering and Information Technology, 8(1), 298-306.*
9. A. Dorri, M. Steger, S. S. Kanhere, R. and Jurdak. 2017. Blockchain: A distributed solution to automotive security and privacy. *IEEE Communications Magazine, 55(12), 119-125.*

10. P. k. Sharma, at.al. A distributed blockchain based vehicular network architecture in smart City. *Journal of Information Processing Systems, 13(1), 84.*
11. A. Arora and S. K. Yadav. 2018. Block Chain Based Security Mechanism for Internet of Vehicles (IoV). *3rd International Conference on Internet of Things and Connected Technologies, 267-272.*
12. M. Singh and S. Kim. 2017. Blockchain Based Intelligent Vehicle Data sharing Framework. *arXiv preprint arXiv:1708.09721*.
13. M. Singh and S. Kim. 2017. Intelligent Vehicle-Trust Point: Reward based Intelligent Vehicle Communication using Blockchain. *arXiv preprint arXiv:1707.07442*.
14. Y. Yuan and F. Y. Wang. 2016. Towards blockchain-based intelligent transportation systems. *Intelligent Transportation Systems (ITSC), 2663-2668.*
15. A. R. Pedrosa and G. Pau. 2018. ChargeltUp: On Blockchain-based technologies for Autonomous Vehicles. T*he 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, 87-92.*
16. A. Dorri, S. S. Kanhere and R. Jurdak. 2016. Blockchain in internet of things: challenges and solutions. *arXiv preprint arXiv:1608.05187*
17. A. Dorri, S. et.al. 2017. Blockchain for IoT security and privacy: The case study of a smart home. *IEEE Percom workshop on security privacy and trust in the internet of thing.*
18. A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram. 2017. LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy. *arXiv preprint arXiv:1712.02969.*
19. X. Zhu, et.al. 2017. Autonomic Identity Framework for the Internet of Things. *International Conference of Cloud and Autonomic Computing (ICCAC), 69-79.*
20. G.J. Ra and I. Y. Lee. 2018. A Study on KSI-based Authentication Management and Communication for Secure Smart Home Environments. *KSII Transactions on Internet & Information Systems, 12(2).*
21. X. Yue, H. Wang, D. Jin, M. Li and W. Jiang. 2016. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems, 40(10), 218.*
22. J. Zhang, N. Xue and X. Huang. 2016. A secure system for pervasive social network-based healthcare. *IEEE Access, 4, 9239-9250.*
23. A. Azaria, A. Ekblaw, T. Vieira and A. Lippman. 2016. Medrec: Using blockchain for medical data access and permission management. *2nd International Conference on Open and Big Data, IEEE, 22-24.*
24. Q. Xia, E. B. Sifah, A. Smahi, S. Amofa and X. Zhang. 2017. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information, 8(2), 44.*
25. M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib and F. Sallabi. 2018. Softwarization of internet of things infrastructure for secure and smart healthcare. *arXiv preprint arXiv:1805.11011.*
26. S. Huckle, R. Bhattacharya, M. White and N. Beloff. 2016. Internet of things, blockchain and shared economy applications. *Procedia Computer Science, 98, 461-466.*
27. How Blockchain Will Accelerate Business Performance and Power the Smart Economy. 2017. Accessed on June. 2018. [Online]. Available: https://hbr.org/sponsored/2017/10/how-blockchain-will-accelerate-business-performance-and-power-the-smart-economy
28. K. Christidis and M. Devetsikiotis. 2016. Blockchains and smart contracts for the internet of things. *IEEE Access, 4, 2292-2303*.
29. N. Z. Aitzhan and D. Svetinovic. 2016. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*.
30. F. Lombardi, L. Aniello, S. De Angelis, A. Margheri and V. Sassone. 2018. A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids. *Living in the Internet of Things: Cybersecurity of the IoT*. DOI: 10.1049/cp.2018.0042