MITIGATING IOT SECURITY AND PRIVACY CHALLENGES USING DISTRIBUTED LEDGER BASED BLOCKCHAIN (DL-BC) TECHNOLOGY

Anil Lamba[1], Satinderjeet Singh[2], Balvinder Singh[3], Natasha Dutta[4], Sivakumar Sai Rela Muni[5]
Department of Computer Science, Charisma University, Turks and Caicos Islands

Abstract: ***The internet of things (IoT) enabled a common operating picture (COP) across the various applications of modern day living. The COP is achieved through the advancements seen in wireless sensor network devices that were able to communicate through the network thereby exchanging information and performing various analysis. In IoT, the exchange of information and data authentication is only done through the central server there by leading to the security and privacy concerns. Chances of device spoofing, false authentication, less reliability in data sharing could happen. To address such security and privacy concerns, a central server concept is eliminated and blockchain (BC) technology is introduced as a part of IoT.***
This paper elaborates the possible security and privacy issues considering the component interaction in IoT and studies how the distributed ledger based blockchain (DL-BC) technology contribute to it. Applications of BC with respect to focused sectors and category were clearly studied here. Various challenges specific to IoT and IoT with BC were also discussed to understand blockchain technology contribution.
Keywords: The Internet of Things; IoT Security; Challenges in IoT; Blockchain Technology, Applications of Blockchain Technology; IoT-BC; Central Server in IoT; Anomaly based algorithm; Classification algorithms; Data communication; Denial of service attack; Intrusion detection; Cyber Security; Cloud Security; Network ; Cyber; Cyber Threats; Threat Analysis ; Information Security; Data security.

Citation: Anil Lamba, 2017."MITIGATING IOT SECURITY AND PRIVACY CHALLENGES USING DISTRIBUTED LEDGER BASED BLOCKCHAIN (DL-BC) TECHNOLOGY", International Journal for Technological Research in Engineering, Volume 4 Issue 8, pp.5687-5691, 2347-4718.

I. INTRODUCTION

The Internet of Things (IoT), an evolutionary technology that raised and gained huge scope in the science and engineering applications solving problems without the intervention of human-human work force. It enables mostly smart work force i.e. creating an interaction between human to machine, machine to machine. The internet of things (IoT) enabled a common operating picture (COP) across the various applications of modern day living1.The COP is achieved through the advancements seen in wireless sensor network devices that were able to communicate through the network thereby exchanging information and performing various analysis1.

From this point one must clearly understand that IoT is not a single technology, it is a combination of multiple technologies that would work for the smart ness achievement2-4. These technologies include communication technology, information technology, electronic sensor and

actuator technology, and the trending advancements in computing and analytics. The integration of all such technologies could make it complex and difficulty in handling when working on wider and large application point of view2-5. The complex scale of device integration, network interconnection, and distributed nature of the things in IoT gives a scope for central server concept where all the things or the devices would compulsory relay on it for authentication.

In this case the interconnection between the devices would become unreliable allowing the data sharing with false authentications or allowing device spoofing leading to insecure data flow. For clear understanding of the problem concerned with IoT, one can refer to the views of Gartner expressed in 2016 and International Telecommunication Union reports of 20156,7. These two reports suggest that in future i.e. by the end of 2020, twenty billion physical things could connect to the internet and operate as a single network under IoT6,7.

This statement suggests that IoT could be become much more complex in the coming future by connecting to a Network of Plentiful Things (NPT) making a provision for digital access. In such cases, the NPT devices could obtain enormous amount of information from the inclosing boundaries or the application or focus environment. These devices must communicate with the network and software defined computing and analytics platform, and this process is completely done through internet and leading to a point of central server storage. This communication results in the rich interactions between the things and network IoT architecture giving a scope for huge data generation allowing the reliable and trustworthy services over the wide area network of things through the Centralized Data Management Servers (CDMS).

Here, reliability and trustworthiness in providing services could not be done in fully secure manner. Chances of security and privacy issues with the data is possible and it is due to the due to the sensitive ness of the things that are interconnected among them as well as the network. More

provision and chances exist for reveling the sensitive aspects of the data to outside world (outside of the communicating network or NPT) through the false authentications, device spoofing. This leads to the various security and privacy issues in IoT making it as a challenge to encounter8,9.

To address the security and privacy issues in IoT, we can eliminate centralized maintenance of the NPT produced data and thereby introducing the new Distributed Ledger -based technology called, a blockchain technology. This paper focuses on the blockchain technology in IoT by analyzing the possible data interruptions and security concerns during the IoT component interaction. The organization of this article is structured in four sections. In section-2, various possible issues and challenges in IoT are identified. In section-3, a study of blockchain is undertaken to identify whether it could address these issues in IoT or not. Finally, the article is concluded with the outcomes of BC in IoT and future scope of BC in various possible ways is briefed.

II. ISSUES AND CHALLENGES IN IOT

Even though, IoT has several benefits and able to solve wide range of problems in various sectors, still the challenges exist. These challenges might be in the form of overcoming the security issues, privacy concerns etc. This section briefly explains the various possible issues by considering the study on the IoT component interaction.

2.1. Challenges in IoT

Mostly the challenges in IoT are related to the security and privacy concerns. Apart from these, few other challenges are interoperability, lack of standards, legal challenges, regulatory issues, rights issues, emerging IoT economy issues, and other developmentalissues10.A report on IoT issues and challenges by The Internet Society (ISOC) prepared by Karen Rose et al. 2015 suggests various possible issues and how they were raised11. Summary of these issues and challenges were described in Table 1.

2.2. Security and Privacy Issues in IoT: A View from IoT Component Interaction

In IoT chances of arising issues in seven different ways were clearly stated in Table 1. The resulting challenges of such issues are also stated. Here, to make it clearer on the various issues related to security and privacy aspects, IoT component interaction study is considered11, 12. Three major components of IoT are the Things with Networked Sensors and Actuators (TNSA), Raw Information and Processed Data Storage (R-IP-DS), Analytical and Computing Engines (ACE). The interaction between these three IoT components were studied briefly to point out the chances of arising security and privacy issues.

Fig. 1 shows the schematic interaction view between TNSA, R-IP-DS, and ACE. From the interaction point of view, data flow will start from the data collection unit i.e. typically some things with networked sensors and actuators to information processing and storage unit i.e. typically raw information processing and data storage in the form of report states. During this process chances of losing, mishandling of the data occurs making the data flow process not 100 %.

This data must flow through the internet with some protocols and chances of misleading or misinterpret the protocols with the help of external influence is highly possible, for example, hackers can control the data process flow. During the second interaction between the R-IP-DS and ACE, the computing engines can be hacked or taken control by external users. In this case chances of analysis interruptions exists.

The third interaction is between the ACE to TNSA, here the feedback as per the computing algorithms must be sent and accordingly the things to should act.Here also chances of hacking and negative control over feedback loop is possible. Apart from interactions between these three components, in each individual component also chances of losing the data occurs by means wrong protocols12. Hence, there is huge scope for the security and privacy concerns in IoT, this even might be a serious problem in large scale IoT implementation.

Table 1. Issues and challenges in IoT

Issues	Challenges	Research
Security issues	Design practices	Lack of resources in train future generations about secure IoT design
	Cost vs. security trade-offs	Lack of informed decisions over cost-benefit analysis of IoT
	Standards & metrics	Lack of standards and metrics to identify the security in IoT devices
	Confidentiality, authentication &control	Lack of optimally controlled role in IoT device communication models to prevent threat of hijacking and cyber attacks
	Field upgradeability	No sufficient information on maintainability and upgradability issues. This is based on the expected life of IoT devices in a network
	Shared responsibility	Could IoT security is achieved with shared collaborations
	Regulation	IoT device or software developing without the security laws
	Device obsolescence	Limited implications on replacing the old and undesirable devices
Privacy concerns	Fairness in data collection and use	Lack of exact rules against data collection and use
	Transparency, expression & enforcement	Lack of multi party models that enable transparency, expression and enforcement
	Wide ranging privacy expectations	Lack of privacy protection models for IoT and inability to recognize the privacy expectations of users
	Privacy by design	Limited resources to develop IoT devices integrating with trusted privacy principles
	Identification	Lack of protection against the data collected by IoT devices
Interoperability issues	Proprietary ecosystem& consumer with	Lack of closed ecosystem concept in data collection format and reuse as per user choice. Individual security keys and protocols could be implemented.
	Technical and cost constraints	Limitations to the technical resources and investments
	Schedule risk	Chances of imposing the interoperability standards
	Technical risk	Less awareness over the technical design risk protocols
	Device bolstering body	Lack of documented standards for best design practices
	Legal system	Standard legal systems for manoeuvringIoT device compatibility
	Configuration	Lack of standard configurations for interfacing large number of IoT devices
IoT standards issue	Proliferation of standards efforts	Less efforts in developing standards and protocols
Legal, regulatory, rights issues	Data protection & cross border flow	Less developments in data sharing and trust policies, laws, and regulations
	Dissemination in data	Lack of laws on using the IoT data in discriminatory way
	Aid to Law enforcement & public safety	Lack of laws on the IoT data for using to fight against the crime
	Device liability	Laws against the liability issues of IoT devices.
	Device prohibitions as per legal actions	Confederation of complex liability during IoT device operation
Emerging economy issues	Investments	Limited investments in IoT research and developmental activities both in developed and developing countries
Developmental issues	Infrastructure resources	More burden or pressure on internet and communications infrastructure across the globe. Limited activities on strengthening the internet and communication infrastructure
	Technical and industrial developments	Limited study to evaluate the technical and economic benefits of IoT in emerging economic countries
	Policy and regulatory co-ordination	Less awareness on the policy plans with the consensus of growth of IoT

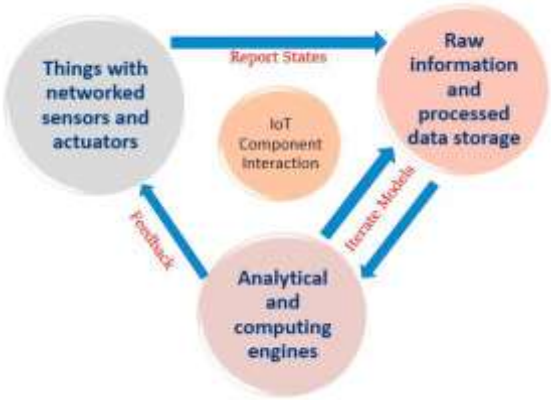

Fig. 1. IoT component interaction13.

III. COULD BLOCKCHAIN TECHNOLOGY CAN BE A REMEDY?

Yes. The blockchain technology would be one of the remedy for addressing the security and privacy issues in IoT. This is because, the blockchain technology eliminates the central server concept of IoT and allows the data to flow through the blockchain distributed ledger for each transaction with appropriate authentication.

3.1. Blockchain Technology

Blockchain technology evolved with the success seen in the cryptocurrency named Bitcoin. BC technology is behind the development of Bitcoin and is the key part. Blockchain is ledger-based tamper proof technology that allows various use cases in wide range of applications (refer to section 3.3). In general, the BC represents a continuously maintained and controlled database considering growing factors and collected data sample sets. The key elements of BC are participant created transactions, and the recorder blocks of such transactions. Here, the recorder block checks whether, transaction details were maintained in the correct sequence or not. This does not allow any tampering of the data available. If the recorded data must be maintained in sequential order, the need for chain approach arises. This maintained transaction was shared with the network of participated nodes. This eliminates the concept of central server by identifying each node that is participated in the transaction sharing process by using the cryptography. This allows the secure authentication8,9.

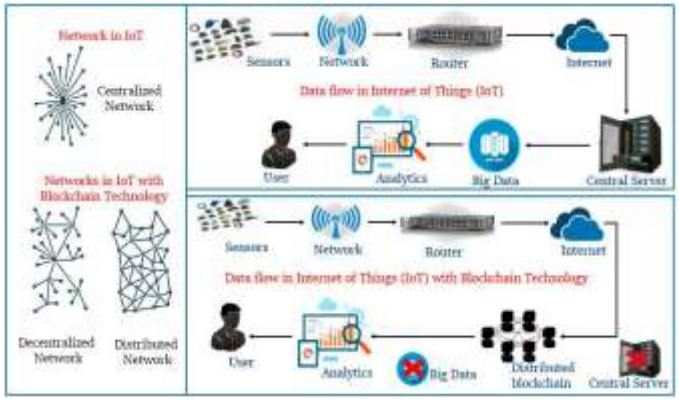

Fig. 2. IoT network types, data flow in IoT, data flow in IoT with blockchain technology

3.2. Blockchain Technology Solution to IoT

Blockchain technology would give better solution to the problems faced by IoT systems. In the growing scenarios of IoT systems, there are more chances for having increased number of interacting things or devices in it. These increased number of devices will try to interact with each making internet as a medium. This would lead to many hurdles because, in IoT systems, mostly the collected data is maintained in the central servers. If the devices want to access the data they have to interact using the centralized network and the data flow will happen through the central server, this process flow is clearly depicted in Fig. 2. But the growing needs of IoT and its applications were portraying IoT as large-scale systems with integration of advanced technologies. In such large-scale IoT systems, the centralized server will not be an effective approach7.

Most of the IoT systems, that are implemented as of now are relaying on centralized server concept. In IoT systems, the sensor devices collect the information from the focused things and allow the data transmission to the central server by means of wired/wireless network refereeing as internet. From the centralized server, analytics were performed as per the user requirements and convenience. In similar, the large scale IoT system wishes to perform the analysis, processing capabilities of existing internet infrastructure may not support effectively8,9. For handling the huge data processed in large scale IoT systems, there is a need for increasing the internet infrastructure.

One best way to solve this is to have decentralized or distributed networks where “Peer-to-Peer Networking (PPN), Distributed File Sharing (DFS), and Autonomous Device Coordination (ADC)” functions could be capable9 . Blockchain can carry out these three functions allowing the IoT systems to track the huge number of connected and networked devices. BC allows the IoT systems to process transactions between the devices in co-ordination. BC will enhance the privacy and reliability of IoT systems making it to be robust. BC allows a peer to peer messaging in faster way with the help of distributed ledger as shown in Fig. 2.

The data flow process in IoT with BC technology is different from only IoT system. In IoT with BC, the data flow is from sensors-network-router-internet-distributed blockchain-analytics-user. Here, the distributed ledger is tamper proof which does not allow in misinterpretation, wrong authentications in data. BC complexly eliminates the Single Thread Communication (STC) in IoT making the system more trust less. With the adoption of BC in IoT, the data flow will become more reliable and secure14.

Blockchain technology have the following advantages for large scale IoT systems, they are as follows8,9,14:

- Tamper proof data.
- Trust less and peer to peer messaging possibility.
- Robust,
- Highly reliable
- More private data.

- Records the historic actions
- Records data of old transactions in smart devices.
- Permits the self-directed functioning.
- Distributed file sharing
- Elimination of single control authority
- Cost reduction in developing huge internet infrastructure
- Built in trust
- Accelerate transactions

Few of the works from the literature is discussed here to understand the role of blockchain in IoT:

MarcoConoscenti et al. 2016, conducted a systematic literature surveyfor investigating the possible case uses and applications of blockchain in IoT. Also identified the factors that affects the systems in terms of "adaptability, anonymity, and integrity". The study also suggested the applicability of BC in IoT as the scalability of cryptocurrency has seen growth in more secure way15.

Mayra Samaniego et al. 2016, have studied on the cloud and fog platforms to identify which platform would be better for the BC deployment in IoT. It was suggested that the deployment of BC will add a great value for the IoT systems to be realistic on a large scale. Also suggested a factor i.e. Network Latency (It is the identified to be dominant factor) that would help us to understand which platform to be used. Among the cloud and fog platforms, the fog platform seems to be outperforming16.

Seyoung Huh et al. 2017 proposed a new method for managing the networked IoT devices or things in BC computing platform using the Ethereum account17.

Ali Dorri et al. 2017, studied the applicability of blockchain in IoT for addressing the security and privacy concerns by considering a case study on smart home. They have discussed the applicability of BC in IoT by considering various procedures and transactions of components in smart home tier18.

3.3. Applications of Blockchain Technology

Similar to IoT, the blockchain technology has wider applications, and can be used in various sectors like agriculture, business, distribution, energy, food, finance, healthcare, manufacturing, and other sectors. Among these sectors, blockchain is used various cases that are clearly represented in Table 214,19,20.Category based applications of blockchain where it is used various cases that are clearly represented in Table 321.

3.4. Challenges in Blockchain Technology Integrated IoT

Even though blockchain technology when integrated with IoT could overcome the privacy and reliability concerns of IoT. However, the BC technology is also having some limitations making it as a challenge. These challenges include the limitation with the ledger storage facility, limited developments in technology, lack of skilled workforce, lack of proper legal codes and standards, variations in processing speeds and time, computing capabilities, and scalability issues. These challenges were clearly represented and described in Table 49.

Table 2. Sector wise applications and use of blockchain technology

Sector	Application area or the use
Agriculture	Soil data, processing records related to agriculture data, shipping of agro-products, sales and marketing data of agro-seeds, yields etc., growth.
Business	Import and export data, digital records by software industries, transaction processing data, and all other which has the value for finance.
Distribution	Transport records, storage records, sales records, marketplace, digital currencies, mining chips, used goods and sales.
Energy	Energy generation data, energy raw material data, resource availability, energy supplier and demand data records, tariff data maintenance, supply on demand, tracking of resources, condition maintaining of the utility.
Food	Food packing data, food delivery and shipping data records, food online ordering and transaction data, food quality assurance data.
Finance	Currency exchange, money deposit, money transfer, crowd funding, smart securities, smart contract, social banking, digital transaction assets, cryptocurrency.
Healthcare	Genome data, electronic medical records, digital case reports, digitalizing old medical data, prescription records, information system at hospital, healthcare costs, vital signs.
Manufacturing	Product assurance, product guarantee information, product warranty information, manufacturing management, robotics, sensors/actuators, product production data, packaging data, product delivery transaction data, supplier and components or raw material tracking.
Others	Digital content, economy sharing, artwork, ownership, jewels and precious metals, space developments, government and voting, virtual nations.
Smart city	Smart service offerings, energy management data, water management data, pollution control data, digital data, enabling digital transactions, smart data maintenance, smart transactions.
Transport and logistics	Transport records, good delivery and shipping data, logistics service identifiers, toll data maintenance, vehicle tracking, shipping container tracking.

IV. CONCLUSION

This paper dealt with the various possible security and privacy issues in IoT. These were identified based on the observations in IoT component interaction. Blockchain technology is identified as one of the solutions for addressing the issues and challenges in IoT. The scope for blockchain integration with IoT is explained in the paper. Also, the various possible applications of IoT with blockchain technologies were highlighted. As a final, challenges in IoT with blockchain technology are also identified. Hope this paper would give basic idea to understanding the need for blockchain in IoT.

This technology can be applied to wide range of services in engineering fields. But the exact implications for each technology has to be studied clearly. Blockchain provides better flexibility in accessing the data. Authors would bring up the studies related to the potentials implication in various fields with appropriate demonstrative models.

Table 3. Category based applications of blockchain technology

Category	Application area or the use cases
Attestation	In most cases, a proof is required to show whether a document is true or genuine copy. This act is mostly referred to attestation. Examples: Notarized copy, stamp provided documents.
Currency	In the process of creating digital currency. Example: Bitcoin, cryptocurrency.
Financial transactions	Financial transactions include the records of various activities where the term money is involved. Examples: Mutual funds, insurance records, stock, bonds, annuities, private equity, pensions, crowd funding, derivatives.
General	This include various other possible transactions that were not categorized into any of the others mentioned in the table 2. Examples: Third-party arbitration, escrow transactions, multiparty signature transactions, and bonded contracts.
Identification	It refers to a sensible act or the process of recognizing something with the help of the certain legal reports. Examples: Identity cards, passports, voter registrations, driver licenses.
Intangible assets	Assets which does not have any physical substance or nonexistence in any of the physical forms that supposed to be in nature. These include the intellectual property materials like trademarks, domain names, brand recognition, reservations, patents, copyrights, goodwill.
Physical asset keys	Physical assets include variety of objects or things that are necessary for human living. In the present era, these physical assets were locked for security and privacy concerns allowing access to the concerned authority or in person. Examples: Office rooms, deposit lockers, hotel rooms, homes, automobile etc.
Public and private records	These records are the quite opposite to the intangible assets. Here these records are having a physical form and they include land documents, property documents, business licenses, vehicle registrations, birth certificates, death certifications under the public records. The private records include contracts, loans, bids, signatures, trusts, assesses, and wills.

Table 4: Challenges in blockchain technology integrated with IoT[9]

Name of the challenge	Description
Limitation with storage facility	In IoT ecosystem, the storage capacity required for sensors and actuators is very less when compared to the ledger based blockchain technology. In IoT a single central server storage is facilitated, where as in BC, each ledger must be stored at the node on themselves. This increase the storage size with time when compared to the traditional storage seen in IoT devices.
Lack of skills in the field	Still the technology is new, many challenges are to be sought out to make it more convenient.
Lack of workforce (Skilled)	Skilled force on this technology is very much limited, this number is extremely less when it is integrated with the concept of IoT. That means skilled work force who are knowing about the blockchain integrated IoT concept is very less.
Legal issues	This technology does not have any legal codes to follow. This is one of most challenging issue to be tacked.
Variation in computing capabilities	As it is known fact that IoT systems are diverse and connected over vast network, this becomes much more complex when the blockchain technology is integrated with it. The need for running the encryption from all the things that are connected blockchain based IoT systems is essential. In such cases, all the algorithm for running the encryption may not have similar computing capabilities.
Processing time	When these computing capabilities are varying, the time required to perform the encryption would vary leading to the variations in processing time.
Scalability	This might lead to the consideration. If it becomes considered the technic behind the cryptocurrency like Bitcoin would be revealed.

REFERENCES

[1] Jayavardhana Gubbi, RajkumarBuyya, Slaven Marusic, MarimuthuPalaniswami (2013)"Internet of Things (IoT): A vision, architectural elements, and future directions."Future Generation Computer System29(7):1645-1660, https://doi.org/10.1016/j.future.2013.01.010.

[2] Nallapaneni Manoj Kumar, Archana Dash (2017) "The Internet of Things: An Opportunity for Transportation and Logistics." Proceedings of the International Conference on Inventive Computing and Informatics (ICICI 2017), pp. 194-197, Coimbatore, Tamil Nadu, India.

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, (2014) "Internet of Things for Smart Cities."IEEE Internet of Things Journal1(1):22-32, Feb. 2014. doi: 10.1109/JIOT.2014.2306328

[4] Nallapaneni Manoj Kumar, Karthik Atluri, SritejaPalaparthi (2018) "Internet of Things in Photovoltaic Systems." In Proceedings of IEEE National Power Engineering Conference (NPEC-2018), Madurai, Tamil Nadu, India.

[5] Nallapaneni Manoj Kumar, Archana Dash, Neeraj Kumar Singh (2018) "Internet of Things (IoT): An Opportunity for Energy-Food-Water Nexus." 2018 1st IEEE International Conference on Power Energy, Environment & Intelligent Control (PEEIC2018), 13th and 14th April, GL Bajaj, Greater Noida, India.

[6] Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015," http://www.gartner.com/newsroom/id/3165317.

[7] International Telecommunication Union (2015) "Measuring the Information Society Report." International Telecommunication Union (ITU), Report.

[8] Ben Dickson, Decentralizing IoT networks through blockchain, (2016) https://techcrunch.com/2016/06/28/decentralizing-iot-networks-through-blockchain/

[9] Ahmed Banafa (2017) "IoT and Blockchain Convergence: Benefits and Challenges." https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

[10] Ahmed Banafa (2017), "Three Major Challenges Facing IoT."IEEE Internet of things, newsletter, March 14, 2017 https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot

[11] Karen Rose, Scott Eldridge, Lyman Chapin (2015) "The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World."The Internet Society (ISOC), pp. 1-80. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf

[12] Celent, Interaction between the three components of internet of things.https://qph.ec.quoracdn.net/main-qimg-a1db8df2497ec1c595ca93deef7b25ca

[13] Nallapaneni Manoj Kumar, Pradeep Kumar Mallick (2018) "The Internet of Things: Insights into the building blocks, component interactions, and architecture layers" Procedia Computer Science.International Conference on Computational Intelligence and Data Science (ICCIDS 2018), Gurugram, India.

[14] David Snyder (2017), BLOCKCHAIN TECHNOLOGY for THE INTERNET OF THINGS, 42TEK, Inc., January 10.

[15] M. Conoscenti, A. Vetrò and J. C. De Martin (2016) "Blockchain for the Internet of Things: A systematic literature review."2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, pp. 1-6. doi: 10.1109/AICCSA.2016.7945805

[16] M. Samaniego and R. Deters (2016)"Blockchain as a Service for IoT."2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, pp. 433-436. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102

[17] S. Huh, S. Cho and S. Kim, (2017)"Managing IoT devices using blockchain platform."2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, pp. 464-467. doi: 10.23919/ICACT.2017.7890132

[18] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, (2017) "Blockchain for IoT security and privacy: The case study of a smart home."2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, pp. 618-623. doi: 10.1109/PERCOMW.2017.7917634

[19] Fujitsu Laboratories of America Technology Symposium (2016) http://www.fujitsu.com/us/Images/Fujitsu-Keynote-Shigeru-Sasaki.pdf

[20] Blockchain2.0. http://www.digitalmoney.or.jp/wp-content/uploads/2015/08/20150814_Blockchain2.0.pdf,
[21] Blockchain: Blueprint for a New Economy by Melanie Swan (2015)

