Journal of Theoretical and Applied Information Technology
15th August 2019. Vol.97. No 15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A VISION OF BLOCKCHAIN TECHNOLOGY AND ITS INTEGRATION WITH IOT: APPLICATIONS, CHALLENGES, AND OPPORTUNITIES; FROM THE AUTHENTICATION PERSPECTIVE

F.A.HADI[1] , AHMED RAISAN HUSSEIN[2], JABAR RAHEEM RASHED[3], NAWAR SAAD ALSEELAWI[4], HASANAIN ALBEHADILI[5]

Department of Electrical Engineering, Faculty of Engineering

University of Misan/ IRAQ

E-mail: [1]electric.eng18@gmail.com, [2]alhusseinahmed70@uomisan.edu.iq, [3] dr.jabar72@uomisan.edu.iq , [4] nawar.alseelawi@uomisan.edu.iq , [5] mrhasanain14@gmail.com

ABSTRACT

The Internet of Things (IoT) is used in our daily lives, thus this type of technology greatly affects various environments such as smart home, smart cities, and industrial systems. Through IoT, daily objects will be able to interact and interconnect to gather information and automate specific tasks. An IoT framework is a group of guiding rules, protocols, and standards. The implementation of IoT applications depends on the characteristics of the IoT environment especially the security issue and the mechanisms implemented for this purpose, where security and privacy are pivotal. This paper maps the research landscape in two ways. The first describes the blockchain technology, the principles of using the blockchain technology, and the different areas of its applications. The second highlights the capabilities and challenges of blockchain, the most famous applications of IoT used in blockchain, and the opportunities of using blockchain together with IoT in the present and future. Finally, the recommendations and future research directions are discussed.

Keywords: *IoT, Blockchain, Authentication, Digital Identity, Authorization.*

1. INTRODUCTION

By 2020, the growth in IoT devices is predicted to be about 26 billion, which is 30 times the estimated number of devices used in 2009. This is more than the 7.3 billion smartphones, tablets, and PCs that are expected to be in use by 2020. Meanwhile, the growth in Machine-to-Machine (M2M) connections is predicted to be four-fold in the near future (from 780 million in 2016 to 3.3 billion by 2021). This may cover a wide range of applications such as defense, transportation, home automation, augmented realities, and public safety [1]. IoT, which is the abbreviation for Internet of Things, enhances the sharing and control of data between objects due to the connection of things through the internet. However, there are some privacy and security issues of IoT such as infringement of privacy, malicious attacks, and data tampering. All of these could occur when data is being shared between objects over the internet [2]. Therefore, using blockchain instead of a central database is one of the ways to achieve high security because in terms of data storage and management, it can prevent damages caused by attacks on the database. Furthermore, when blockchain is used in an area that requires data disclosure, its transparency attribute plays an important role. Hence, all these strengths promote the use of blockchain in the environment of the Internet of Things (IoT). The use of blockchain is expected to continue to grow and emerge in diverse areas such as the financial sector [3]. The real world of cyberspace will be reflected in IoT applications in the nearest future, thereby leading to authorization and privacy leaks due to the rapid growth in this area of information technology. Therefore, we need to investigate and discuss the most secure technology that can be used to achieve these requirements. Moreover, authentication is crucial in user and other areas of IoT like machines and vehicles that utilize IoT services. This is important and lead us to an important question, are the transactions or services provided in the IoT world

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

protected? If they are not protected, privacy and authorization information will be accessed illegally by criminals; these criminals will also be able to obtain IoT services, leading to serious consequences. Thus, to avoid such a risk, the identity of the user and other parts of IoT need to be validated. This work also answers some other questions such as, what are the blockchain capabilities? What is the ability of blockchain to integrate with IoT for security purpose? What are the challenges faced by the developer while implementing the blockchain in IoT applications?

This work contributes to the security of IoT-based blockchain technology, where there are various components of security incorporated in the design of the security system through the blockchain technology. The most popular blockchain platforms, the blockchain capabilities, the challenges of blockchain, the future of blockchain with IoT, and the opportunities implemented in IoT are also reviewed in this paper. This paper is organized into ten sections. Section 1 provides the basic information on IoT and the way this technology has been developed. Section 2 gives the definition of blockchain and its most famous platforms. Section 3 explains the opportunity of implementing blockchain with IoT. Section 4 lists the state-of-the-art implementation of the blockchain in IoT. Section 5 shows the blockchain capabilities in different applications within various fields. Section 6 lists the most famous application based on the blockchain that has been integrated with IoT. Section 7 presents the expected future of blockchain with IoT. Section 8 shows the challenges and prospects of blockchain. Section 9 discusses the finding and limitations of this study and highlights the important remarks. Finally, Section 10 provides the conclusions and recommends future research direction.

2. BACKGROUND OF BLOCKCHAIN TECHNOLOGY

In the world of revolutionizing technology, blockchain is regarded as second to the internet because it is changing the way people live and work [4]. A blockchain can be described as a mechanism for data storage. This mechanism is an open and distributed peer-to-peer data storage mechanism, which is tailored to record transactions between two parties efficiently. These transactions which are recorded, are verifiable and permanent [5][6]. In a situation where there is no means of verifying or auditing information systems, then the issue of trust becomes a complex issue, particularly when sensitive information is being handled such as economic transactions involving virtual currencies. In 2008, two radical concepts with great implications were introduced by Satoshi Nakamoto. The first concept, known as Bitcoin, is a virtual cryptocurrency that maintains its value, and is independent of support from any financial entity or centralized authority. Here, a decentralized P2P network of actors which constitute a network that can be verified and audited, collectively and securely hold the coin. The second concept is known as blockchain and it is even more popular than cryptocurrency itself.

This mechanism involves the verification of transactions by a group of untrustworthy actors. Through this mechanism, a ledger that is immutable, secure, transparent, and auditable is provided. Blockchain gives room for open and full consultation, thereby enabling access to previous transactions, since the first transactions are performed by the system. Any entity can validate and collate the transaction regardless of time. In the blockchain protocol, information is structured in a chain of blocks with a set of previous bitcoin transactions which were performed at a certain point in time are stored in each block. Through a reference to the past block, blocks are connected together to form a chain [7]. As seen in Figure 1, all participants within the network are allocated a part of the block of data, with the aim of building a ledger that represents the transaction history. This ledger is used for all participants during the authentication operation and thus, it requires no third parties or central point authentication; this concept is called decentralized authentication

A blockchain model does not require the storage of information with third parties because the records are stored on different interlocked computers with identical information. The computer rejects breached blockchain updates. Security and privacy can be further strengthened with the use of multi-signature (multisig) protection or more than one key for the authorization of a transaction process. A hacker will find it difficult to penetrate a network or access transaction information because in blockchain protocol, several identical and redundant copies of the same ledger is stored globally. The advantage of this protocol is that there are many backups of information, even if one is breached. In other words, in blockchain, data is stored in several computers that are interlocked,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

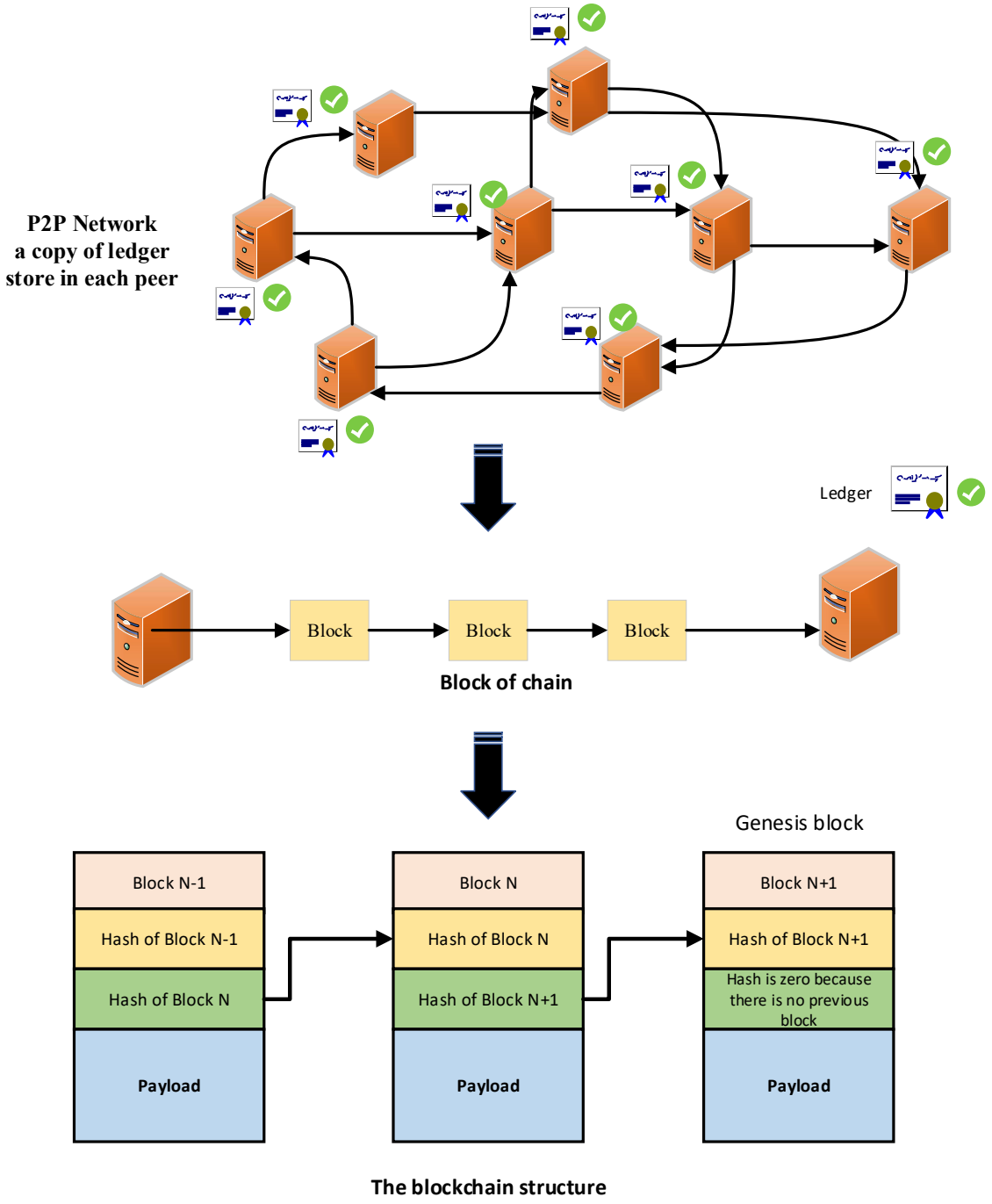

Figure 1: How The Block of Data Is Distributed Among All Participants in The Network

thereby making it difficult for an attacker to gain access to information. For hacking efforts to be successful, more than 50% of the systems in the network need to be hacked [8]. Many organizations have come up with their own blockchain platforms. Most of the development work of these platforms is open-source, and they have come up with interesting use-cases that go beyond just cryptocurrency. As security is a very critical issue in IoT, it is considered the backbone of IoT work. Therefore, it is a motivation to present this work and highlight the importance of using blockchain technology with IoT and implement new decentralized architecture in IoT application. Some of the popular blockchain platforms are shown in Table 1.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: The Popular Blockchain Platforms

No.	Blockchain platform	Year proposed	Application	Definition
1	Bitcoin	2009	Cryptocurrency	The first cryptocurrency with decentralized p2p transactions and no central authority.
2	Ethereum	2015	DAPPs	Allow the building of decentralized applications (DApps) on top.Has a Turing-complete VM that DApps run on. Implementation of smart contracts is allowed. Conflicts that arise in the case of faster transaction times are resolved using GHOST protocol.
3	Monero	2014	Digital currency	It is an open-source, yet secure, private and untraceable mining algorithm that does not support ASICs.
4	Cardano	2015	Digital diplomas, cryptocurrency	Possesses a scientifically-proven secure consensus algorithm. Smart-contract capable platform. Faster transaction speeds, reliable and quantum resistant.
5	Ripple	2012	border payments	No miners exist; the 100 billion coins of XRP in existence, were created in 2012 when the network was launched. Based on a unique consensus algorithm
6	NEO	2014	Asset record keeping	Supports digital identities, digital assets and smart contracts. The implementation of Turing-complete smart contracts can be performed in the NeoVM, while smart contracts can be terminated using a “deterministic call tree”. Quantum crises is avoided through the introduction of lattice-based signatures and encryption technology.
7	NEM	2015	Automatic accounting, KYC, Logistics, Voting	Multigeniture transactions are supported. The use of Eigentrust++ is employed as a reputation system(that monitors previous behavior of nodes, taking note of the quality of work done).Through a powerful API interface, the functionality of NEM’s blockchain is revealed. The API is supported by any programming language, and not necessarily a particular “smart contract” language.
8	Hyperledger fabric	2015	Used to create DApps	The storage of ledger data is done in different formats. The switching in and out of consensus mechanisms is allowed. Supports different MSPs. Channels can be created using Hyper-ledger Fabric, the creation of a different transaction of ledger by a group of participants.
9	ZCash	2016	Cryptocurrency	Zero-knowledge proofs (zk-SNARKs)Fork of bitcoin is used in ensuring transaction privacy.
10	Intel Sawtooth	2014	For enterprise use	Highly Modular. The selection of transaction rules, per missioning and consensus algorithms which support specific business needs by applications, is allowed by Sawtooth’s core design.
11	Straits	2016	Identity management, supply chain management	End-to-end solutions are provided for the development, evaluation and implementation of native C# blockchain applications on the .Net framework

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

12	Waves	2016	Transfer custom tokens from person to person	Users are allowed to launch their custom cryptocurrency tokens. FIAT money alongside other cryptocurrencies are supported by Waves. Allows the use of POS which in turn results in rapid transaction rates, and this theoretically supports the execution of hundreds of transactions per second.
13	EQS	2017	DApps	A hosting platform which is smart contract enabled for the implementation of open-source projects and consumer-facing decentralized applications. This is similar to Ethereum Scalability is better than that of Ethereum ,Decentralization is achieved through the use of coin voting.
14	ICON	2017	Interconnect various blockchain communities	The connection of several blockchains around Nexus through portal is done using ICON. Nexus, which is a loop chain based blockchain, allows portals and different nodes to participate as a way of acknowledging decentralized governance. Conclusively, the purpose of the ICON Project is to ensure that all activities within a country are connected through its own blockchain, thereby allowing interaction between multiple communities without needing a third party.
15	Steem	2017	public content platform	It's a blockchain used as a database. It's an incentivized, blockchain-based, public content platform. Supports community building and social interaction with cryptocurrency rewards.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. OPPORTUNITY OF BLOCKCHAIN WITH IoT

Examining complex relationships and processes is possible using IoT. The major idea behind the IoT is a mutual relationship between the real/physical and the digital/virtual worlds: virtual representations and digital counterparts are possessed by physical entities. Here, things are aware of context, have the ability to sense, interact, and exchange data, information, and knowledge. Through IoT, business requirements are met while the introduction of novel services is done based on real-time data. IoT is the linking bridge between things from the physical and virtual realms. The connectivity between these things may not be private-owned and is accessible by all at a low cost. Since the protection of privacy is crucial, IoT can be protected against malicious attack and fraud through the use of blockchain technology. One of the major benefits of using blockchain-based user preference management scheme is that it plays a significant role in settling disputes between users and provider of IoT application [9]. The nature of blockchain, which is immutable, undeletable, distributed, and irreversible, makes it suitable for decentralized identity management and distributed credential storage [10].

The potentials of enhancing security are embedded in these properties of blockchain. Using blockchain with IoT enables the establishment of a genuine decentralized market [11]. The absence of a central point in the blockchain-based systems prevents failure, which often comes from a central point while providing a valid historical transaction log that is complete and transparent. Blockchain prevents disputes by ensuring that each party is responsible for its roles in the entire IoT transaction. More security could be provided to a system when the size of the network increases exponentially with authentication performed at no cost. Furthermore, blockchain is capable of playing a major role in tracing the sources of insecurity as well as solving the problem of security vulnerability. Blockchain-based identity and access management systems can solve major IoT security challenges like those related to IP spoofing [8].

Finally, the vision of Internet of Things (IoT) is to ensure that traditional devices become independent and smart. Technology advancements is turning the vision into reality, but some challenges need to be addressed, especially in the security domain e.g., authentication and data reliability. Thus, for IoT future potentials, it is important to make it trustworthy in the era of huge information source. As a major technology, blockchain is capable of transforming the manner in which information is shared in the world.

In distributed environments like IoT, trust-building without the need for authorities is a technological advancement that can be applied in several industries. In order to overcome the challenges of IoT since its introduction, disruptive technologies like cloud computing and big data have been used. In the next two decades, blockchain is assumed able to build trust in the IoT.

4. STATUS OF IMPLIMENTION OF BLOCKCHAIN IN IoT

According to previous researchers, a combination of blockchain and IoT has the probability of being powerful to transform many industries. For example, independent transactions are carried out by smart IoT devices through smart contracts. More significant outcomes in terms of data solutions may be achieved through the combination of blockchain and IoT with artificial intelligence. In organizations, IoT may constitute a big security challenge [8]. IoT can be described as an extension of extant interaction between people and applications through a new dimension of "Things" for communication and integration. Despite all the benefits of IoT, it is still very difficult to develop as it involves a complex process. The falsification of data records by means of arbitrary manipulation is prevented in blockchain distributed database [12]. The consistency of blockchain in IoT is not guaranteed through a distributed consensus protocol that involves the coming together of participants within an unreliable P2P network. Every transaction in the blockchain is encoded into a permanent record using cryptography; this record is difficult to modify without being detected. It is also easy to check and retrieve the complete history of transactions performed by any entity within the network without needing any extra security mechanism [13].

The interaction between physical and cyber worlds is one of the biggest achievements of IoT. The IoT covers daily use devices and devices that have great impacts on our lives. Therefore, the effective and successful interaction of all devices with little or no human support can be achieved through the development of a novel trust model. In this model, real world actions should be included, transactions should be enabled through, it and it should support novel compensation and mechanisms of accountability [14]. However, blockchain is a Peer-to-Peer network; therefore, in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

order to utilize the full benefits of the network, nodes from different parties are required. This implies changing of the "blockchain is a decentralized database system" to "blockchain is a distributed record of data" mindset. Through this change of mindset, a number of consortia have been created in different domains since early 2018. Some examples of such domains include financial transaction, trade, and the Intelligent Healthcare Networks.

5. BLOCKCHAIN CAPABILITIES

High level security in different applications within various fields can be achieved through blockchain technology. Some of the capabilities are discussed in the following section as shown in Figure 2.

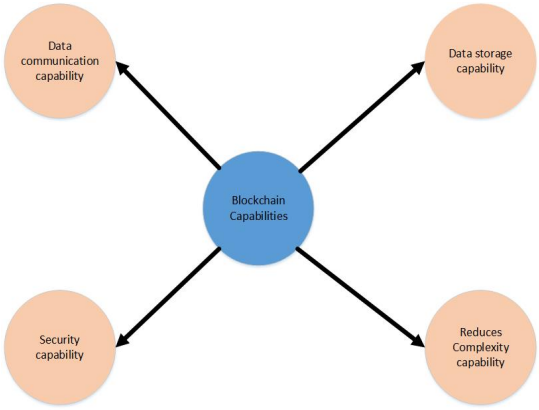

Figure 2:Shown The Capapbilities of Blockchain

5.1 Data Storage Capability

The use of blockchain can enhance security compared to the storage of all data within a central database. In terms of data storage and management, a database can be protected from damage caused by an attack. Data transparency is provided by blockchain, especially when used in an area where data disclosure is required; this transparency is provided because of the open nature of blockchain. Such strengths owned by the blockchain technology makes it usable in different areas including the financial sector. It is forecasted that the Internet of Things environment as well as its applications will expand further [3] where the immutable, distributed, undeletable, and irreversible nature of the blockchain makes it appropriate for decentralized identity management and distributed storage of the credential [9]. Therefore, this technique is suitable for securing storage in different systems.

5.2 Data Communication Capability

From the various kinds of attack, it is observed that authentication, security, data privacy, robustness against attack, self-maintenance, and easy use are required from blockchain [1]. An important advantage of blockchain technology is its ability to prevent double spending between customers in bank transaction [9] and to achieve best communication among customers. This is because the blockchains have the capability of allowing two or more entities to perform transactions using digital asset (the coin). The mapping in real life relies on each specific application (for instance, it is possible to translate a coin into real money, domain name or even to an actuation like energy transfer from one device to another. Moreover, a relationship of trust is established using smart contracts, without depending on a widely trusted entity. In other words, this relationship can be reliably and deterministically enforced by the blockchain when required [13]. This scheme can be regarded as the ultimate and ideal system [14]. Additionally, network dependability is enhanced by blockchain.

5.3 Security Capability

The blockchain can be a key player in the monitoring and tracking of sources of insecurity within a supply chain, and it is capable of addressing and dealing with crisis situations such as recalling of product in case of security vulnerability. Blockchain-based identity and access management may be capable of addressing major IoT security problems like those related to IP spoofing [8][15]. Blockchain manages data by keeping a record of data information in the block. In addition, problems of security vulnerability of data management system of extant IoT platforms like Sybil attack, IP spoofing, and single point of failure are solved by blockchain through its security properties such as data integrity, authentication, and non-repudiation [16].

5.4 Reduces Cost and Complexity Capability

Blockchain can reduce the complexity and cost during transactions where conflicting agents are made to engage in transactions that are cryptographically secured, and it can also interact without a governing body or centralized platform due to the distributed software architecture

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

provided by blockchain technology. These attributes reduce the cost of micro transactions, enable the sharing of information in lemon markets, and reduce the complexity that comes with writing contracts. In order to resolve conflicts within this scope, blockchains provide a record of past transactions [11]. With blockchain, business processes can be automated without requiring expensive and complicated centralized IT infrastructure. This technology will facilitate the building of trust between devices and users, eliminate the involvement of middlemen, reduce falsification risk and cost, as well as reduce the time required for transaction settlement [17].

6. APPLICATION OF BLOCKCHAIN INTEGRATED WITH IoT

The most widely known blockchain-based platform for running smart contracts despite its ability to run other distributed applications and interact with more than one blockchain is Ethereum. Ethereum is Turing-complete, a mathematical term which indicates that any other language can be simulated using Ethereum's programming language. Details on the functionality of smart contracts are not provided because they are beyond the scope of this paper. Apart from smart contracts and cryptocurrencies, blockchain can be used in several other areas as illustrated in Figure 3. The applications of IoT are used in such areas as data storage, sensing, identity management, management, smart living application, time-stamping services, mobile crowd sensing, intelligent transportation systems, and security in mission-critical scenarios.

Many researchers have made attempts to improve these kinds of application by integrating blockchain with IoT. The aim of this integration is to improve the authentication operation. In the next section, some of such studies that have integrated blockchain with IoT will be reviewed. The applications have been classified based on their categories.

6.1 To Provide Energy Using Smart Meters

In [2], Zero-knowledge proof was used in proposing a smart meter system to prove without disclosing information such as public key. IoT data is stored in the blockchain, thereby preventing the authentication of IoT device and data tampering. The use of Zero-knowledge proof is employed so that third parties are prevented from going through the user's original data using block retrieval.

6.2 In The Field of Telecommunication

Numerous applications have been applied in telecommunication using blockchain technology where in the study [11], blockchain was used to propose a scheme that authenticates mobile devices so that the resource information of the mobile devices in the (MRM) resource pool can be trusted. Using the proposed scheme, which is the Secure Authentication Management human-centric Scheme (SAMS), blocks that are based on the master node's hash value within the MRM and the resource information hash value in the subordinate client node are created. With this scheme, hash values and blocks are created and connected when client nodes are added. The performance of SAMS was assessed by applying it to the MRM, and artificial attempts were made to connect unauthorized devices. Since the field of telecommunication has recently become a vital field which requires high level of security, the study [18] focused on the introduction of a new ID as a service (IDaaS) to manage digital identity using the blockchain technology. One practical example of describing the proposed blockchain-based ID as a service (BIDaaS) is to show that the proposed BIDaaS works as an infrastructure for the management of identity and authentication for mobile users of a mobile telecommunication company. The study conducted by [19] presented an architecture that makes sensor data complex by hashing it; here, only hashes are retained at the enterprise level. Weights in CIMA are assigned manually or automatically to the value of sensor data. A lightweight engine on the mobile device, or an auditable and searchable context ledger can be used at the cloud or enterprise level to implement the architecture. However, the processing limitation does not allow peer-to-peer applications to use CIMA.

In study [20], a scheme authenticating access was designed and implemented to focus on providing anonymity and accountability efficiently and simultaneously without depending on any trusted party. The scheme proposed in this study was inspired by the current emergence of Bitcoin techniques such as CoinShuffle protocol and coloured coins. Through cloud radio access network (C-RAN), which is the scheme proposed by this study, thousands of terminal devices are interconnected so as to support Internet of Things (IoT) in the area of 5G area.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

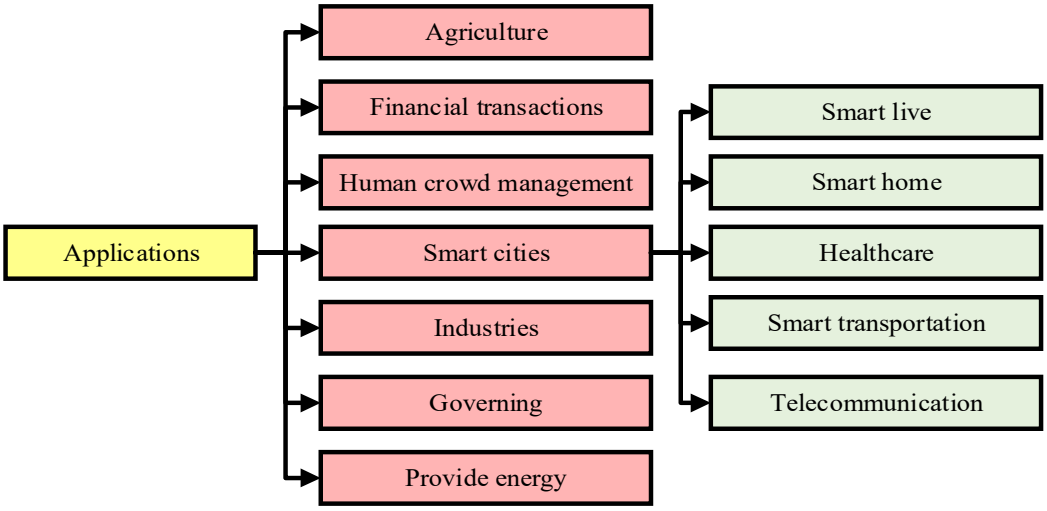

Figure 3: Blockchain Technology Applied In Different Areas

However, the operating and capital expenditure of network incurred by this scheme is high because the access authentication of each terminal is centralized and conducted in the mobile core network. The conventional C-RAN is not capable of providing a genuine mechanism that guarantees credibility of device, service security, and low cost accessing of resource. In study [21], a blockchain-based trusted authentication (BTA) architecture was proposed for 5G with blockchain-based anonymous access (BAA) scheme in cloud radio over a fiber network. The SDN test bed was used in evaluating the efficiency and feasibility of the authentication architecture with the aim of enabling blockchain as a service. User authentication in social network communication is an important issue which requires more support, thus in study [22] an efficient algorithm which preserves privacy of information on social networks was proposed.

These authors used recognition and non-tampering of the blockchain to store the user's public key while binding it to the block address, which is used in authenticating the sender's identity. The aim is to protect others from malicious users while their requests are being verified after they send a request. Mixed hash encryption was used instead of directly sending plaintext subsequent for authentication to ensure that only the matching degree is calculated rather than revealing specific information of the users. This was to prevent honest but curious users from illegally accessing information about others.

6.3 In Smart Cities Environment

Smart cities environment has attracted researchers' attention in the last decade as in a smart city, security is a critical issue while authentication of people and devices represent the corner stone in this environment. The blockchain technology is more suitable to perform this task according to the abilities of blockchain where the strength of evolving Software Defined Networking and blockchain technologies was taken advantage of by [17] who proposed a hybrid network architecture for a smart city. The architecture is divided into two parts: edge network and core network. In addition, the study [23] employed group key and key management that is based on multi-solution chain. Furthermore, a smart home environment was also proposed by the authors; this smart home environment is capable of reducing storage space via a secure and efficient Extended Merkle Tree and a KSI-based authentication alongside a communication with improved security strength. A Blockchain-based Identity Framework for IoT (BIFIT) was presented by [24]. In the study, the authors described how BIFIT is applied to IoT smart homes to independently extract the signatures of appliances and create identities that are based on blockchain for the owners of the appliances. Through this framework for smart homes, appliances signatures (low level identities) are correlated with the identities of their owners so that they can be used as authentication credential and used in ensuring that all IoT entities are functioning normally.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6.4 In Electronic Governance Environment

The electronic governance has been widely used in different countries and there are different application used in order to achieve the electronic governance goals. Several applications under this field used blockchain technology; for example, in electronic governance environment, although it is possible for an individual to supply certain information to anyone who requires it, this individual may choose to keep a copy of such information. As an example, when the owner of a verifiable passport number tries to retain a copy of the document; the assumed advantages of blockchain are compromised because enterprises are not required to keep their own copies of the document, thus exposing the documents to the risk of getting lost.

Blockchain technology is employed in various applications. In the property sector, blockchain is used to create digital property records that cannot be forged. This technology lowers transfer fees, enhances verifiability and transparency, and reduces disputes. In the food sector, blockchain technology is used to trace food movements and to address promptly the issue of food contamination [17]. Questions have been raised about the authenticity of information and documents placed on the chain because of individual control that is an attribute of some blockchain implementations. The major attributes of e-residency in terms of using blockchain for identity authentication and their implications from a multi-discipline perspective were explored in study [24]. Nevertheless, the use of blockchain for identity authentication has not been scientifically proven. Hence, questions have been raised about the accuracy of information and the implications of depending on such information as the legal implications can be complex. In another study [25], an ecosystem approach to digital identity was discussed, while the potentials of using blockchain technology to solve past and present challenges related to identity authentication and authentication in a Canadian context were also described in the study. Apart from that, blockchain has been widely employed in financial transactions, smart contract, and data forensics in IoT.

6.5 Smart Transportation Field

The focus of this area is the authentication of vehicles movement where in study [5] LNSC which is a decentralized security model that is based on the smart contract and lightning network in the blockchain ecosystem was proposed. The model which is a security model, focuses on registration, scheduling authentication, and charge phases. It is easy to combine the model with the present scheduling mechanisms to improve the security of trading between electronic vehicles EVs and charging piles. Meanwhile, in study [13] the use of blockchain was proposed for the purpose of tracking the certificate of each vehicle (revoked or valid) in distributed and immutable records. In the study, certificate verification was replaced with a lightweight blockchain-based authentication approach. Furthermore, the authors proposed a scheme that is a fully distributed vehicle admission/revocation scheme. The scheme was tested and found to improve the response time and the overall security of the system by eliminating computation overhead. Moreover, in study [26] this proposed system enables vehicles to make judgment about the received messages; they are able to judge the message as false or true using the reputation value of the sender. The calculation for reputation value is done based on the ratings of previous messages that a specific vehicle had broadcasted before. A temporary center node is required to obtain these ratings, and when the center node is obtained, it is validated by a majority of the cars after which it is stored in the blockchain. This means that the consensus of crowds on the reputation of each vehicle is represented by the ratings stored in the blockchain.

7. THE FUTURE OF BLOCKCHAIN WITH IoT

In the near future, there will be a great need for the optimization of blockchains for different applications. Blockchains are presently used with IoT systems in different fields. Thus, developing a mechanism for testing various blockchains is important because to integrate blockchain with IoT, the developer needs to know which blockchain fits their requirement. Two major phases are involved in optimizing blockchains for diverse applications: standardization and testing. The standardization stage involves having an understanding of the supply chains, products, markets, and services; an analysis of the requirements is then carried out and agreed upon. After a blockchain is created, the agreed criteria should be used to ensure that the blockchain is working as required in authentication. On the other hand, the testing phase involves the evaluation of different criteria carried out based on energy efficiency, security, privacy, latency, usability, and throughput [1]. Past studies have failed to define

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the most effective mechanism that can be used to facilitate the privacy of authentication operation while avoiding race attacks that may threaten the process of authentication [26]. Thus, a future potential will be the integration of designated verifier signature with the blockchain scheme to prevent malicious distribution of nodes' relationship certificates [27]. The global financial industry expected that the blockchain technology will grow to about USD 20 billion by 2020. This technology can be applied under IOT environment and its applications are expected to be expanded [3]. Lastly, the scalability and resistance against security attack of the model should be tested by the integration of blockchain and IoT. This testing is important as it enhances the discovery of the other capabilities of using blockchain in IoT research areas [28].

8. CHALLENGES AND PROSPECTS OF BLOCKCHAIN

Great concerns have been expressed over the challenges associated with blockchain technology despite its attractive authentication methods. The main challenges, which have been found to be associated with blockchain technology, are enumerated and discussed in the next section. References with more details are also provided. The challenges are classified based on their nature.

1.The cost of many IoT solutions is still high because of deployment and maintenance cost of server farms and centralized clouds. The cost is attributed to the middlemen and the infrastructure that is not created by the supplier. Moreover, when regular software updates have to be distributed to millions of smart devices, maintenance becomes a problem [1].

2. Many problems arise due to blockchain during a transfer transaction. Such problems have not been solved by previous studies. However, a majority of the past studies were focused on finding ways of protecting the personal key that is used in encryption. The security that is associated with the personal key is the crucial part of blockchain. In order to obtain the personal key which is stored in a peer's device for the purpose of hacking the bitcoin, an attacker attempts a "reuse attack" as well as other forms of attack [3].

3.Blockchain technology still has challenges in different areas such as query, scalability, high overhead cost incurred by consensus algorithms, and latency. Based on a non-technical perspective, researchers and practitioners are still unable to understand the implementation of blockchain protocol and evaluate the applicability of blockchain in potential use cases [11].

4.When a strong attacker that is capable of widely eavesdropping on the internet targets a system, the countermeasure using secret sharing becomes inadequate. By eavesdropping on the communication between the candidates for online storage servers and the user, the attacker can detect the target servers containing the data shared by the target user. This will enable the attacker to steal or delete the shared data [29].

5.It is important to consider the inherent security of networks and devices as well as those that may emerge in such integrations. Such important security issues are yet to be addressed by extant solutions [30].

6.In blockchain, it should be considered a serious authentication threat when an attacker is able to hack and change 51% of a participant's ledger [31].

9. DISCUSSION, REMARK AND LIMITATION

Different from previous works in the literature, this work focused on the most usable form of authentication used in IoT technology and the expected future of using blockchain-based IoT. There are a few studies discussing this topic but in different directions. The reviewed literature was selected from different fields, as shown in Figure 3. During the filtering stage of literature papers selection, unrelated papers were excluded. There are various motivations for using blockchain technology in IoT in order to provide high level security and privacy. Some of these motivations are related to the implementation and efficiency of blockchain where it reduces cost, reduces the transaction process time, and reduces the risk of counterfeiting, as well as eliminates the central point in the communication network as the trusted authority. Moreover, eliminating human intervention is a crucial concept in IoT environment. Another motivation is the high level of safety and security of the blockchain architecture compared to the central architecture, which has a critical privacy issue because all of the users' identities and data are disclosed to the central node.

Furthermore, the data storage using blockchain does not allow attackers to access and read the data since the data are converted into a new format called hash and the topology of the network distributed are P2P nodes. For security purposes, most of IoT environments use encrypted over SSL/TLS protocol, where TLS is used to achieve

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

confidentiality of data. If TLS is used to encrypt the communication between the device and the Message Broker, when the attacker learns the private key of an IoT device he will be able to read the secret data whereas when blockchain is implemented, the secret data are sent to the target as a block of hash. A serious security risk in blockchain architecture is when the hacker can penetrate 51% of the participants' ledger, which is very hard to accomplish. Finally, developers should also increase the internet infrastructure in order to deal with huge data in IoT environments, achievable through decentralized architecture that is based on blockchain technology. We expect that the blockchain will have a promising future with IoT and this study will be useful and thus, will be adopted by other researchers who are interested in developing the IoT security. However, the limitations of the study were the number of the source databases. The study had been focused on the most reliable and multidisciplinary databases. However, in order to explain and prove that blockchain is applicable and effective in such area, the studies focusing on the implementation of the blockchain technology in IoT for security purpose were selected while the other studies were excluded.

9. CONCLUSION AND FUTURE WORK

In blockchain, there is a guarantee for integrity because it is impossible to modify previous data; the immediate past block is cryptographically referenced, while a complete transcript is maintained by all nodes. There is a need to develop strategies of streamlining the issues of immutability and the continuous re-assertion of full chain during every transaction; otherwise, they will cause serious problems in the future. While the issue of scalability remains a big challenge to data scientists and organizations enjoying the propaganda, it is important to note that the idea has come thus far with so many industries trying to discover its potentials. Such industries include financial securities, cryptocurrencies, and property registries. Technological advancements of a global world that is internet-enabled have led to the rapid transition to a world that is data-driven; this transition has also been triggered by increasing completion for scarce resources and increasing societal challenges. A platform for the distribution of trusted information which disregard non-collaborative organizational structures can be provided to IoT by blockchain [1]. In this paper, an examination of blockchain technologies was carried out. The paper also discussed how this technology can be integrated with IoT for the purpose of authentication. Moreover, security features and resistance against pentation are highlighted as one of the critical issues plaguing IoT. The principle of blockchain technology, its capability, applications, opportunities of integrating blockchain with IoT in the present time, the future of blockchain, and the challenges related to blockchain were also examined in this paper. The authors of this paper believe that to integrate blockchain technologies into telemedicine, more research is needed. The application of blockchain in telemedicine will be easier in IoT as no central point and extra local hardware is required. Thus, the use of blockchain is suitable in-patient authentication. This paper is expected to be the starting point for more discussions and research on the employment of blockchain in Digital Identity in telemedicine in future work.

REFRENCES:

[1] T. M. Fernández-caramés and S. Member, "A Review on the Use of Blockchain for the Internet of Things," vol. 3536, no. c, pp. 1–23, 2018.

[2] C. H. Lee and K. Kim, "Implementation of IoT System using BlockChain with Authentication and Data Protection," pp. 936–940, 2018.

[3] J. Park and J. Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions," Symmetry (Basel)., vol. 9, no. 8, p. 164, 2017.

[4] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The Blockchain as a Decentralized Security Framework [Future Directions]," IEEE Consum. Electron. Mag., vol. 7, no. 2, pp. 18–21, 2018.

[5] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem," IEEE Access, vol. 6, no. c, pp. 13565–13574, 2018.

[6] A. H. Mohsin et al., "Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions," Comput. Stand. Interfaces, no. October, pp. 0–1, 2018.

[7] A. Reyna et al., "On blockchain and its integration with IoT . Challenges and opportunities," vol. 88, pp. 173–190, 2018.

[8] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecomm. Policy, no. June, pp. 1–12, 2017.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[9] S. C. Cha, J. F. Chen, C. Su, and K. H. Yeh, "A Blockchain Connected Gateway for BLE-based Devices in the Internet of Things," IEEE Access, vol. 6, pp. 24639–24649, 2018.

[10] J. G. Faisca and J. Q. Rogado, "Personal cloud interoperability Fully Decentralized Identity Management," WoWMoM 2016 - 17th Int. Symp. a World Wireless, Mob. Multimed. Networks, 2016.

[11] F. Hawlitschek, B. Notheisen, and T. Teubner, "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy," Electron. Commer. Res. Appl., vol. 29, pp. 50–63, 2018.

[12] H.-W. Kim and Y.-S. Jeong, "Secure Authentication-Management human-centric Scheme for trusting personal resource information on mobile cloud computing with blockchain," Human-centric Comput. Inf. Sci., vol. 8, no. 1, 2018.

[13] N. Lasla, M. Younis, W. Znaidi, and D. Ben Arbia, "Efficient Distributed Admission and Revocation Using Blockchain for Cooperative ITS," 2018 9th IFIP Int. Conf. New Technol. Mobil. Secur., no. i, pp. 1–5, 2018.

[14] G. C. Polyzos and N. Fotiou, "Blockchain-assisted information distribution for the internet of things," Proc. - 2017 IEEE Int. Conf. Inf. Reuse Integr. IRI 2017, vol. 2017-Janua, pp. 75–78, 2017.

[15] A. H. Mohsin et al., "Based medical systems for patient's authentication: Towards a new verification secure framework using CIA standard," J. Med. Syst., vol. 43, no. 7, p. 192, 2019.

[16] M. Y. Jung and J. W. Jang, "Data management and searching system and method to provide increased security for IoT platform," 2017 Int. Conf. Inf. Commun. Technol. Converg., pp. 873–878, 2017.

[17] P. K. Sharma and J. H. Park, "Blockchain based Hybrid Network Architecture for the Smart City," Futur. Gener. Comput. Syst., 2018.

[18] J. H. Lee, "BIDaaS: Blockchain Based ID As a Service," IEEE Access, vol. 6, pp. 2274–2278, 2017.

[19] J. Morrison, "Context integrity measurement architecture: A privacy-preserving strategy for the era of ubiquitous computing," 2016 IEEE 7th Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2016, 2016.

[20] Y. Niu, L. Wei, C. Zhang, J. Liu, and Y. Fang, "An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the Bitcoin blockchain," 2017 IEEE/CIC Int. Conf. Commun. China, no. Iccc, pp. 1–6, 2017.

[21] H. Yang et al., "Blockchain-based Trusted Authentication in Cloud Radio over Fiber Network for 5G," pp. 16–18, 2017.

[22] R. Yu et al., "Authentication with Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network," IEEE Access, vol. 5, pp. 24944–24951, 2017.

[23] G. J. Ra and I. Y. Lee, "A study on KSI-based authentication management and communication for secure smart home environments," KSII Trans. Internet Inf. Syst., vol. 12, no. 2, pp. 892–905, 2018.

[24] X. Zhu, Y. Badr, J. Pacheco, and S. Hariri, "Autonomic Identity Framework for the Internet of Things," Proc. - 2017 IEEE Int. Conf. Cloud Auton. Comput. ICCAC 2017, pp. 69–79, 2017.

[25] G. Wolfond, "A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors," Technol. Innov. Manag. Rev., vol. 7, no. 10, pp. 35–40, 2017.

[26] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Futur. Gener. Comput. Syst., vol. 82, pp. 395–411, 2018.

[27] C. Lin, D. He, X. Huang, M. K. Khan, and K. R. Choo, "A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-based Identity Management Systems," IEEE Access, vol. 4, no. c, 2018.

[28] S. Raju, S. Boddepalli, S. Gampa, Q. Yan, and J. S. Deogun, "Identity management using blockchain for cognitive cellular networks," IEEE Int. Conf. Commun., 2017.

[29] M. Fukumitsu, S. Hasegawa, J. Iwazaki, M. Sakai, and D. Takahashi, "A proposal of a secure P2P-type storage scheme by using the secret sharing and the blockchain," Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA, pp. 803–810, 2017.

[30] C. Lin, D. He, X. Huang, K. K. R. Choo, and A. V. Vasilakos, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," J. Netw. Comput. Appl., vol. 116, no. February, pp. 42–52, 2018.

[31] A. H. Mohsin et al., "Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication," Comput. Stand. Interfaces, 2019.