Table of Contents

LIST OF FIGURES

BLOCKCHAIN TECHNOLOGY AND THE INTERNET OF THINGS (IoT)

Today's world is becoming more digital/online like everything is connected to the Internet and most of the fields are related to the internet named the Internet of Things (IoT). It makes life easy but at the same time causes risks and issues to its users. For example, in business, the information is transferred between parties or companies and the risk of this confidential information being hacked causes troubles. Different steps were taken, and a technique named Blockchain technology helped a lot in this regard. Blockchain technology is a scheme/structure that protects the information of the system in such a way that it can't be accessed and is difficult to change and hacked. It is something like coding and decoding of information and the only targeted company/party can access it and read the information transferred. So, the risk of hacking transferred confidential information through the internet has been reduced to a great extent but with more ease comes several different problems as well. Blockchain technology faced some challenges that need to be accounted for and solved. This report highlights IoT, Blockchain, the relationship of IoT & Blockchain technology, and the issues and the steps/ protocols used for dealing with these issues along with different literature review has been proposed.

1. Blockchain:

1.1. What is Blockchain and how it is formed?

Currently, it was estimated that cryptocurrency (peer-to-peer money) is becoming more popular in every field of life, and the highest rated P2P money used these days is Bitcoin. Bitcoin is obtained from blockchain technology because the first bitcoin transaction was made by blockchain technology. Like, we never heard about this concept before that it would be possible to transfer or withdraw money with online wallets, banking systems, and any third-party involvement. The concept of blockchain was obtained from different issues faced by people/users. For example, if person A wanted to send money to another person B, he failed to do so sometimes due to some technical issues of the banking system, or account transfer limit exceeding issue, or the transfer chargers and the most important issue is the account hacked by someone else. Hacking is the common issue these days as the world is becoming more and more digital and online, risk of cybercrimes has increased at the same rate.

To solve the above-mentioned problems, the concept of cryptocurrency came into being. Cryptocurrency is a type of electronic or computer-based currency that is obtained from a technology called the blockchain. Now if someone A wants to send money to another person B, he will send the bitcoins and whenever when a person sends a bitcoin, its information is encrypted in a block. Similarly, each block is linked to other blocks and has information about the previous and future blocks also and all these blocks make a book or record (ledger). So, a BLOCKCHAIN is a technology that forms a dispersive ledger or book of information, and that information is encrypted in such a way that no one can hack it. The reason why hackers can't hack the information in blockchain technology is that each connected block has a unique encrypted algorithm and the sender or user has a copy of that particular block which he named as Invalid, so no one can get its information except the receiver [1]. Figure 1 shows the architecture of blockchain technology that shows the concept of blocks. Figure 1 presented three blocks i-1, i, and i+1 that are linked with each other and are coded using hash functions. Block i has all the information of block i-1 and block i+1 has all the information of block i.

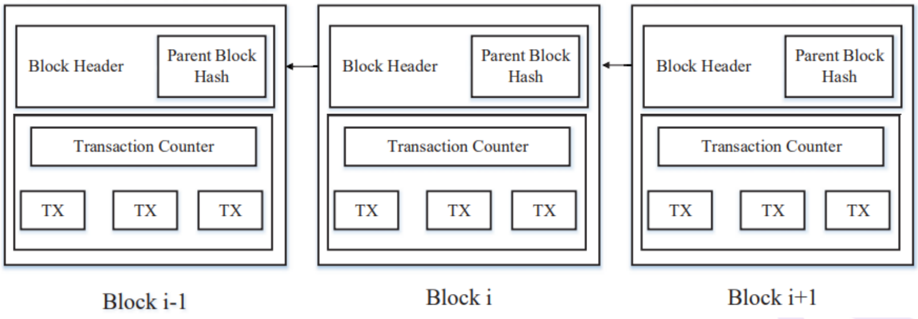

Figure 1: Architecture of Blockchain Technology| source: [1]

Blockchain technology contains two important keys that are public key and private key and the types of blockchain technology are public, private, and corporate. The public type or key allows any person to access the information, but it causes the privacy issues. Private keys or types gives access to limited persons only with high privacy whereas corporation type blockchain technology give access to some selected organizations/companies to approach the information and they have to operate at only one single node [2]. Figure 2 below represents the types of Blockchain technology [3].

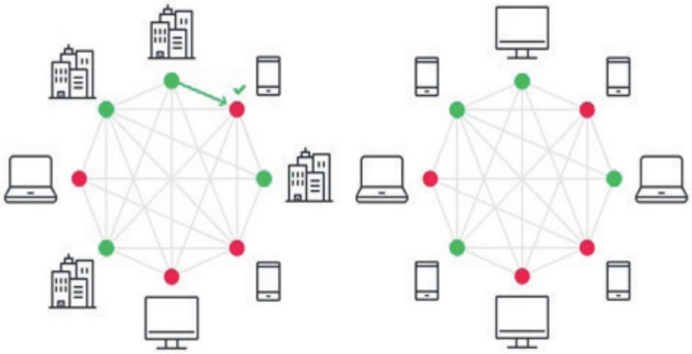

Figure 2: Types of blockchain technology, (a) public, (b)private |source: [3]

How the Blockchain technology Worked:

Blockchain technology worked in a distributive manner. Like, if there are 2 or more users or persons in a network and the information is being shared among them so everyone has access to that information/data. When a hacker tries to attack the information, then as the blocks are linked to each other, so one block is attacked by the hacker because of this attack the hash code of that specific block was changed and similarly the other connected linked blocks hashes also changed. The other user predicted that change as it is mentioned earlier all the blocks are linked with each other in blockchain technology and inform the user and in this way the information was recovered or prevented before hacker get access to data. Figure 3 shows the working of blockchain technology [4].

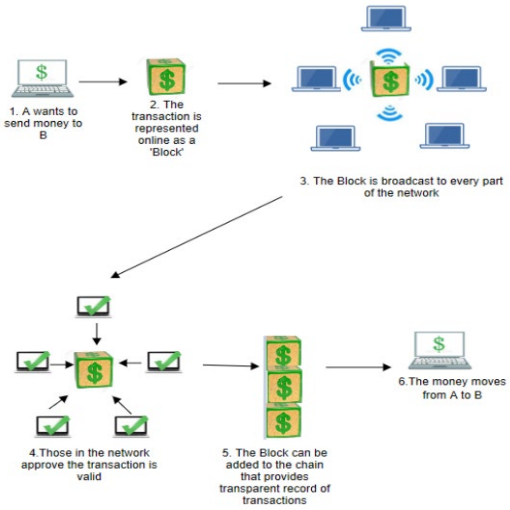
1. A wants to send money to B
2. The transaction is represented online as a 'Block'
3. The Block is broadcast to every part of the network
4.Those in the network approve the transaction is valid
5. The Block can be added to the chain that provides transparent record of transactions
6.The money moves from A to B

Figure 3: Working of Blockchain technology |source: [4]

1.2.Security Vulnerabilities and risks associated with blockchain adoption:

As it is mentioned earlier that every new technology added some challenges in the system also. So, blockchain technology faced some issues after it is adopted by the world. Some of the challenges are highlighted in this report. The major challenge was security or privacy problem because system having a private key may be stolen by any of the person because that private key is saved in the memory of the system and today's hacker can access it. This problem of security was solved by a method named color spectrum method that used a hash function for coding the information without using any private key. This steps consists of several authentication factors or steps when hacked by someone, so the system security issue has been resolved to a greater extent [2]. In the same way, the security problem was resolved by mixing multiple or different blocks and then sending information to other person in the form of same multiple blocks. In this way, hacker didn't get access to the actual block. Another way of dealing was proposed that hide the identity of the sender as well receiver along with the information being transferred and the approach was named as zero-knowledge proof [1].

Another challenge faced by blockchain technology was extensibility. This issue arises due to the cause that transactions or deals were increasing at rapid pace and the size of blockchain or the blocks that store the information was not that much larger to store such heavy amount of data. The blocks must save every information to check and restrain the system from any unethical hack. But it could only operate 7 deals or transaction in 1 second, so it was very difficult to handle millions of transactions in real time. This problem was sorted out by several efforts that were further classified into two types. The first effort was cache optimization/improvement that considered to process all the transactions/deals without the problem of scalability by removing previous data after the arrival of new data/information. In this way, the problem was solved but that was not the effective method as someone needs previous data at some point then what will he do to get it? The second type of effort was reshaping of blocks. In this method, the future generation bitcoin blocks were divided further into two parts. One stores all the previous information and the other processed all the present or incoming information/transactions. Egocentric and Inflexible mining/excavate was another issue that highlighted blockchain technology is not as secure as it is considered [1].

These challenges caused a threat for the blockchain technology that it may not be secure for dealing with hackers. But different steps were considered in the literature that are highlighted in the report also. Also, some of the agreements were made to implement this technology in every field in future.

1.3.Role of blockchain Consensus:

As the blockchain technology is a digital system with no other entity involved in it and it provides secure and unchangeable data/information transferred from A to B. So, it is required that some of the agreements are needed that highlights only valid transactions or deals/information are considered or not. These agreements/protocols helped in preventing the system from different cybercrime attacks and based on various algorithms. These algorithms are proof of work, proof of stake, practical byzantine fault tolerance algorithm, delegated proof of stake, ripple-based algorithm, and tender mint algorithm. Mostly, to store the information, one of the users should be selected in localized system. Before the consensus protocols, random selection was done that presented that due to random selection of nodes, system is more vulnerable to cyberattacks. So, different algorithms were addressed. Role of each of these protocols are discussed in detail next in this report.

1.3.1 Proof of Work Protocol: In this algorithm, each node must do some of the computer calculations. The computer calculations mean each user in the network must calculate the has number of each block linked to each other in transferring the information. A threshold was set in this case, and it was reported that value must be equal to or less than the predefined threshold value. The user who calculates that value faster is dominant in this case.

1.3.2 Proof of Stake: POS protocol is different from POW as the selection is currency-based. In this algorithm, the richest user will be more dominant and selected as that user who can store the information. In this case, a lesser value of hash along with stake size is considered in this protocol. Later, it was reported that mostly the blockchains first considered proof of work protocol and then shifted to proof of stake protocol.

1.3.3 Practical Byzantine fault tolerance algorithm protocol: This algorithm give permission to dispersive system to detect the cybercrime attacks even with small number of users present in the network. In this algorithm, there are three steps to be followed by the blockchain that includes customer sending a request for information, system performed different steps and transfer the data, customer received the information. Every user/node get the dominating effect in this protocol.

1.3.4 DPOS protocol: In this algorithm, shareholder selected one node as their representative and then that representative store the information of the block. The size of the block and the timespan of the block was also selected by the delegation selected by the shareholders.

1.3.5 Ripple-based protocol: In ripple-based protocol, the node is classified into two types, one is dependent that participated in all the process of consensus and the other is customer that only work in shifting the funds amount.

Different types of consensuses blockchain protocols were highlighted and discussed and it's a sure thing that everything has some pros and cons. The disadvantages of the above discussed protocols are that practical byzantine fault tolerance algorithm protocol required the ID of each node to select one primary node that is difficult for providing. Whereas the other algorithms freely join the networks and selected the primary node. Similarly, Proof of Work (POW) required each user to work means computer calculation which required energy to do this work and make the system more complex [1], [5].

It was also reported that practical byzantine fault tolerance algorithm (PBFT) and tinder mint protocols are categorized as private protocols whereas Proof of Work (POW) and Proof of Stake (POS) as public protocols.

2. Blockchain Applications in the Internet of Things (IoT):

As, every sector is becoming digital or online with the data synchronized with the internet and as a result the threat of hacking of all the information is increasing at the same rate that makes the users confused in implementing this advancement in future or not. But the future is totally dependent on online systems. Blockchain technology helped a lot by encrypting the information in the form of ledger, so no hacker can access the data at any time. Blockchain technology is working in almost each field like automotive sector, banking, and finance, in healthcare system, in media and industry sector, supply chain sector, telecommunication department and many more. The common thing in all these sectors is internet because all these sectors are interconnected through different devices with the internet to transfer and receive information. That transfer and receiving of information through internet is at risk of Hacking (cybercrime attacks) and blockchain technology helped a lot in these Internet of Things (IoT) based applications to prevent cyberattacks.

2.1.Internet of Things (IoT):

IoT is a very effective and appealing advancement in the field of information technology and telecommunication. IoT is the interconnection of different devices connected to the internet to transfer and receive information. A smart home is a perfect example of IoT. If a person forgets to turn off the air conditioner at home, then he needs not to return to home just to turn it off. He can turn it off through his mobile phone by connecting to the air conditioner. Internet of Things give ease to its users in this case that now the air conditioners are connected to internet also and a person can turn it on and off by only connecting its mobile phone [6]. From the past recent years, it is observed that different devices are connected to a single network. These devices include household appliances, electric and hybrid vehicles, mobile phones, tablets, TV, laptops, healthcare devices, electronic devices, street lightning system, traffic signals etc. It was reported that billions of these types of devices are connected to a single network and that amount will further increase by 2050 [7].

IOT devices are categorized in two types one is general devices and the other is the sensing devices. The general devices are all those mentioned above like household appliances, mobiles, tablets, vehicles etc. Whereas sensing devices are the actuators (servomotors, stepper motors etc.) and sensors that sense the parameters like temperature of the surrounding or the device, liquidity, and light intensity. These both devices are further connected to a cloud or a network through different gateways to record or store the information. Different wired and wireless devices like Bluetooth device, Wi fi, ZigBee, GSM etc. are used that provides connectivity of devices to the cloud [8].

2.2.Network topology in IoT and Network topology of IoT in Blockchain:

As, everything is connected to a network in IoT, so risk of hacking of information has been greatly increased. That’s why blockchain technology is used in IoT to prevent the devices or users from any unethical cybercrime attacks. The network topology of Internet of Things is defined as how different IoT elements interact with each other within an IoT cloud. Internet of Things network topology is categorized into four main types: Mesh configuration, Star configuration, Ring Configuration and Tip-to-Tip network configuration. In case of mesh configuration, three nodes are present named gateway node, sensor node and actuator node. Each node is in the range of at least one sensing device so, that information is not missed at any stage. Figure 4(a) represents the mesh network topology in IoT [9].

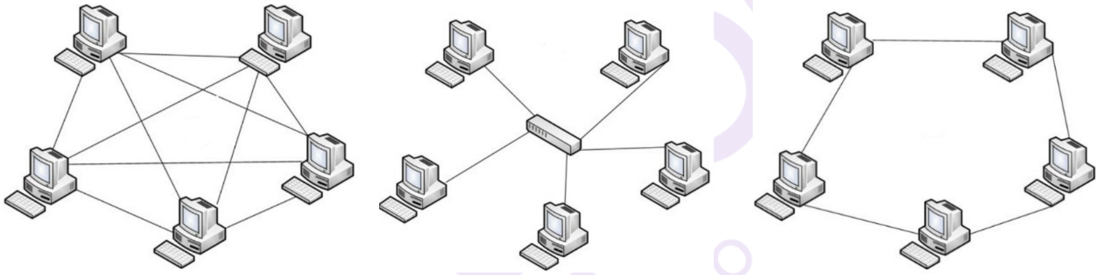

Figure 4: IoT network topologies, (a) mesh, (b) star, (c) ring |source: [9]

Similarly, in star network topology presented in Figure 4(b), one node is common, and the remaining nodes are interconnected to that specific node whereas in tip-to-tip topology, there are only two users, and they have a direct relation with each other. Information is transmitted and received between these two users like a Bluetooth device has a direct connection to mobile phone. In case of ring topology presented in Figure 4(c), all the users are connected through a single cable and this network is efficient as compared to other networks as the information signal is strong and there is no limit of data but as the data is exceeding more speed of network becomes slow [10].

These network topologies have several challenges. The IoT networks are distributed in nature, so each user is at verge of disruption that exploit the whole system as a result cause cyberattacks. Another issue was that IoT framework is concentrated as shown in Figure 5, the network topology of IoT environment is presented. Apart from this, the issue of data of IoT devices is not confidential and authentic or accurate. As, the data is not secured in Internet of Things network, information may be hacked and can be used by hackers in an inappropriate way. Sensors may be damaged during the transmitting of information or even hackers can access the sensors for hacking of information and damaged the sensors. That’s why a technology named blockchain technology was introduced that helped to overcome all the above challenges faced by IoT network [10].

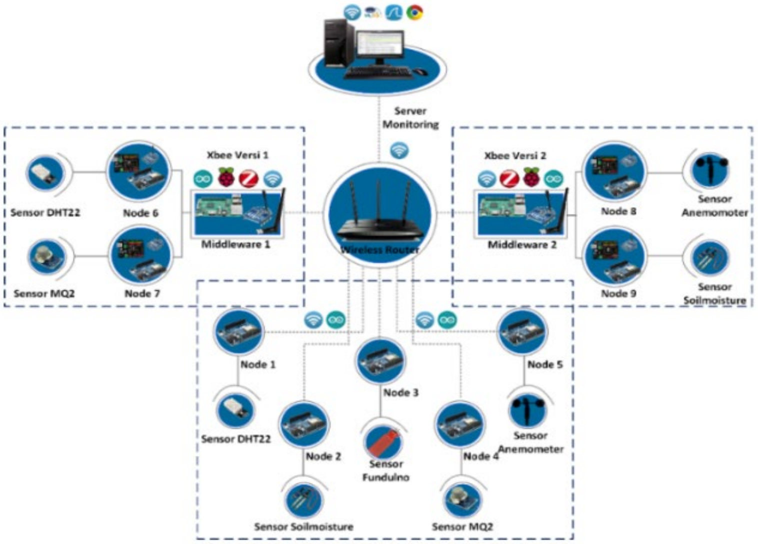

Figure 5: IoT environment network topology |source: [10]

Blockchain technology is used with IoT, and it makes a machine-to-machine configuration. As, blockchain technology is discussed in detail along with all the challenges, protocols etc. so next effort was blockchain with IoT. The problems of security faced by Internet of Things was solved by blockchain by forming a distributive ledger of information. The information transmitted or the transactions would become as every information is encrypted in a has code of different blocks and these blocks are further linked to each other. Figure 6 shows the network topology of blockchain technology implemented on IoT.

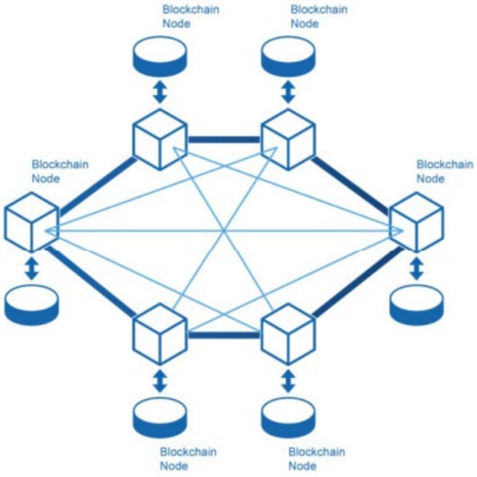

Figure 6: Blockchain technology on IoT |source: [2]

The mixture of IoT and blockchain technology made the system totally autonomous, so there was no need for any concentrated or third person involvement. The users could continuously track the information and this combination offers several advantages to the community. Several challenges may appear in combining both technologies as blockchain is a distributed ledger and IoT is based on customer and server concept. That’s why IoT-blockchain technology is not common until now but it was reported that it will become effective and common by 2025. These challenges did not affect the advantages it offers and are discussed as follows:

1) Defending the information from alternation and disruption.
2) Storing the information that cannot be changed by any person other than the actual users.
3) Providing a facility of tracking the information any time [2].

2.3.Capabilities of Blockchain technology:

There are several attributes discussed about the blockchain in literature that highlighted that how blockchain technology prevent systems and IoT from different challenges. These attributes are decentralization or dispersion, durability, transparency, security, and privacy.

Decentralization: The IoT system was dependent on server and customer concept and was consolidated. Transfer of information in clouding atmosphere and telecommunication system required high value of cost as well it was reported that in traditional localized systems, there was a need for some other party or agency that confirmed the information before transferring it. Like, if someone wanted to send money to other person in traditional case, the third party would be a bank. A novel approach named blockchain technology based distributed network framework was proposed to overcome these challenges. The proposed approach was a distributed framework that gave advantages related to lesser cost, secured and demanding access to IoT networks. Blockchain then helped and as a result no involvement of third party was required [1].

Durability: This property of blockchain helped the data to become as efficient that it cannot be changed by any other hacker at any cost. In blockchain technology, as the blocks are interlinked to each other having hash values and they have complete information of its previous block, but it encrypted the previous block from the new block. A 51% attack occurred when some hackers tried to access and hack the blockchain blocks and tried to change the information in these blocks. As, mentioned earlier each block act as an individual entity block with different has values in each of them but they all are linked with each other to confuse the hacker which the block is having authentic information to target. This specific key in each block cannot be changed by anyone if someone tried to access it. This concept may be termed as private key as each block is protected by its own hash number. So, the problem in conventional systems that hackers accessed the data and then changed the record was solved by blockchain technology.

Transparency: Before the blockchain technology, Internet of Things networks were open to everyone in such a way that a small level of hacker could even access the system and made changes. But blockchain technology provides openness in a private manner. All the members of IoT network can approach the data in the blocks and checks what type of information present in the blocks. Similarly, the members of Internet of Things framework could provide the suggestions and ideas for any new update and versions to be added in the system or not. But this openness was not for the persons other than IoT community. Blockchain technology worked a lot in this field and provided a hash protected ledger that could only be approached by IoT people.

On the other hand, public blockchain provide access to all the public users if they wanted to open the information but they track the network continuously to check any unethical activity. A lot of work has been done presented in the literature related to transparency of blockchain technology in IoT frameworks. It was observed that detecting or tracking the data continuously led to transparency. Blockchain based detecting solutions were also proposed for different fields individually.

Security: Security is another capability of blockchain technology in IoT networks. In traditional systems or existing IoT systems, the addresses were visible to people that was termed as public addresses. Whereas private IDs were hidden. But the security issue arose when hackers tried to approach the private IDs with just smaller efforts. A lot of confidential data was at risk as it was accessed by anyone. Then blockchain technology helped the Internet of Things systems and encrypted the information and all the addresses. It guaranteed that no change of information would happen along with no data would become visible to any person other than the IoT community. Different authentication systems were mixed with blockchain technology to ensure the security of the system.

Privacy: Privacy is an important factor in online systems. Almost all the online systems, IoT networks were at risk. The applications people using, their data may be hacked, and the privacy would be lost. The problem of privacy issue was seen greatly in mobile phones connected to Internet when the data that was confidential become visible to hacker. This will lead to crimes. Different technologies in blockchain have been implemented that prevented these privacy issues. These approaches are protected socket layer approach, internet-based agreement security etc. Moreover, hardware based on cryptographic technique may helped a lot in this regard [1], [2].

2.4. Literature Review:

A lot of literature review has been presented in research papers that highlighted the solutions for the challenges faced by IoT networks regarding blockchain technology.

A blockchain technology based efficient contract was developed in 1994 that was a computer-based program. It had all the attributes like self-authentication, self-driven etc. This technology didn’t require any third person to involve in any of the data transfer and suggestion given. In the start, it was not given importance but after 2008, when bitcoin currency came into use, then it gained a lot of focus. Everything was automatic in efficient contract system, but the main issue faced by implementing it in future was the language it was programmed. Solidity was very top-level and extraordinary language and the coding obtained in this was not simple and understandable by all the IoT community members. Efficient city, efficient home, efficient travelling system etc. all depend on smart contract system technology. The challenges faced by efficient contract system leading to smart cities, homes etc. in Internet of Things environment was expandability, resilience, security issues etc. The reason was that the programming code in solidity language was publicly accessible [6].

Another approach was developed by researchers related to 51% attack in IoT networks. A security technique named Pirl-Guard was proposed based on the proof of work (POW) protocol. This algorithm worked in a way that when an attacker tried to attack the system, and approach towards the private blocks, then pirl-guard stopped the peer-to-peer based transactions immediately and penalize the blocks. The main work was that making the master node and then penalizing the attacker. The issue faced by this approach was that the penalty system was at continuous risk of 51% attack. Any attacker can attack the penalty system and caused security issues. Another approach was proposed related to the 51% attack prevention and was like pirl-guard technique termed as chain locks. This approach worked based on “first glimpse” policy. But the major limitations of this approach was that it only protect one transactions at a time [5]. Some other solutions were proposed related to blockchain and IoT environment. A novel approach was presented in 2014, a prototypical approach that let the sensing devices to change the data with the bitcoins. In this scenario, each bitcoin has a separate public key related to the node addresses. So, when a person demands data, IoT network provides him/her with that bitcoin’s public key. It was reported that this proposed approach was developed from the concept of another approach that was E-business model in Internet of Things network. The system was very complicated and when attacked by any hacker caused trouble. Separate layered based solutions were implemented to overcome the challenge of complexity.

Likewise, an efficient approach related to the blockchain based IoT environment cache system was proposed named as SAPPHIRE approach. The sapphire approach dealt with the major challenge faced by blockchain based IoT framework that was scalability. Due to this approach, system could easily deal with large chunk of data and decreased the high level of data entering the IoT environment. An enigma-based method was submitted by Guy Zyskind that helped in preventing privacy issues. The proposed approach was peer-to-peer framework-based approach and the problem of privacy was sorted by this method. But the problem was that an additional blockchain was used for controlling the network that made the system complex. A data storage-based solution was also presented based on the blockchain technology-based Internet of Things framework that was a secure and flexible method for storing and managing of data. One more solution was proposed by Li Shuling that was a smart and efficient city architecture. This solution was mixed with IOT, blockchain, large data sets and electricity-based internet connection to provide best solution in Internet of Things environment. But it faced challenges like less security, maintenance of equipment, difficulty in updating the network and high maintenance and operational cost etc. [7].

Most of the country’s system based on the energy and power systems are the main sources of providing the consumers they demand. From the last recent years, it was reported that cybercrimes were increasing at a greater rate in power systems and caused security and privacy issues. A lot of different solutions were proposed in literature to prevent power system from different cyberattacks. As the data of power system is connected to the internet connection because everything is monitored in real time and online, so it made a good example of IoT network. A microgrid based blockchain technology solution named LO3 energy technique was also suggested. This approach was the first ever step towards secure and reliable operation of power system. A device was implemented that examined the energy value of buildings (demand of customers) and send it to the Internet of Things environment. Everything was protected by blockchain technology based LO3 approach. Another solution related to IoT based blockchain technology protection system was proposed that was self-protected and flexible [11].

A color spectrum-based solution was presented by Seong et al and his fellows that was related to Blockchain of IoT things on the Internet of Things Environment after continuous hacking issues in the system. This approach was based on the multi-algorithm, and it was something related to the one step verification and two step verification solutions presented in Facebook and other social media accounts. These algorithms stated that if someone unknown tried to access your account or data then a code will be generated and sent to you for verification, and if you didn't verify it then blockchain technology protect your data. So, in this color spectrum algorithm several multiple steps were added before accessing the data or any account/ID [2]. A large bunch of literature review related to the solutions of blockchain technology have been proposed. Some of the solutions are discussed in this report along with the challenges faced by these solutions.

According to my understanding, I think the solutions presented until now in different sectors have somehow positive impacts and the challenges faced by implementing them may be reduced by little efforts and update in these solutions. From the discussed solutions in this report, I considered color-spectrum solution as a best option because it's not as difficult and complex and we have observed it real time example in our social media accounts that its completely working and preventing our accounts and systems from any unethical hack.

3. Conclusion:

It is concluded that the report highlights all the features of the blockchain technology, what blockchain technology is how its working and how it prevents system from cybercrimes. Similarly, Internet of Things with blockchain technology was also discussed in the report along with the challenges faced by implementing the mixture of both and what solutions were proposed to overcome these challenges.

References:

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, pp. 557–564, 2017, doi: 10.1109/BigDataCongress.2017.85.

[2] S. K. Kim, U. M. Kim, and J. H. Huh, “A study on improvement of blockchain application to overcome vulnerability of IoT multiplatform security,” *Energies*, vol. 12, no. 3, 2019, doi: 10.3390/en12030402.

[3] P. K. Paul, “Blockchain Technology and its Types—A Short Review,” *Int. J. Appl. Sci. Eng.*, vol. 9, no. 2, 2021, doi: 10.30954/2322-0465.2.2021.7.

[4] H. Lakkis and H. Issa, “Understanding Blockchain Technology,” *Int. J. Technol. Hum. Interact.*, vol. 18, no. 1, pp. 1–14, 2022, doi: 10.4018/ijthi.297617.

[5] S. Sayeed and H. Marco-Gisbert, “Assessing blockchain consensus and security mechanisms against the 51% attack,” *Appl. Sci.*, vol. 9, no. 9, 2019, doi: 10.3390/app9091788.

[6] B. K. Mohanta, S. S. Panda, and D. Jena, “An Overview of Smart Contract and Use Cases in Blockchain Technology,” *2018 9th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2018*, pp. 1–4, 2018, doi: 10.1109/ICCCNT.2018.8494045.

[7] S. Li, “Application of blockchain technology in smart city infrastructure,” *Proc. - 2018 IEEE Int. Conf. Smart Internet Things, SmartIoT 2018*, pp. 276–282, 2018, doi: 10.1109/SmartIoT.2018.00056.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.

[9] Cicnavi, “Overview of Network Types and Topologies,” *Util. Wind.*, 2011, [Online]. Available: https://www.utilizewindows.com/overview-of-network-types-and-topologies/

[10] B. Purnama, Sharipuddin, Kurniabudi, R. Budiarto, D. Stiawan, and D. Hanapi, “Monitoring Connectivity of Internet of Things Device on Zigbee Protocol,” *Proc. 2018 Int. Conf. Electr. Eng. Comput. Sci. ICECOS 2018*, no. January 2019, pp. 351–356, 2019, doi: 10.1109/ICECOS.2018.8605225.

[11] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, “Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks,” *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3162–3173, 2019, doi: 10.1109/TSG.2018.2819663.