International Journal of Future Generation Communication and Networking
Vol. 13, No.2s, (2020), pp. 1747–1757

Review on Blockchain contribution to the Internet of Things

Siddhant Dani, Priti P. Jorvekar
Department of Computer Engineering, NBNSinhgad School of Engineering,

Abstract

The Internet of Things became widely popular as a technology with the start of the fourth industrial revolution. IoT operates to gather confidential information remotely via a network of devices. IoT systems gather a huge amount of important and confidential information, often shared with external organizations for useful services. But such devices can be easily hacked, and the protection of these devices is therefore critical when IoT scenarios are implemented. Blockchain is a promising new framework to solve security and IoT trust challenges. This paper offers a summary of existing blockchain solutions for IoT networks. At first, it define the terms IoT and Blockchain and review current surveys dealing with blockchain technology implementations in IoT networks. Then, included a general overview of IoT architecture, classification of specific IoT attacks, and blockchain architecture. Moreover, This paper provide a taxonomy of state-of-the-art methods for stable and privacy-preserving IoT network blockchain applications in relation to the blockchain framework, basic security requirements, efficiency, constraints, machine complexity and communication overhead. Based on the present study, we stress the open barriers of research and potential future work directions in blockchain IoT technologies.

Keywords- *Blockchain, IoT, IoT security, Blockchain IoT, BIOT, IoT, Attacks on IoT*

I. INTRODUCTION

Internet of Things (IoT) is merely a network of small, lightweight devices or sensors which gather data from their surrounding environment, these devices can be connected to each other via internet and can communicate wirelessly. The data produced or gathered by these devices can contain very private or important information like phone records, daily schedule, banking information, etc. IoT devices have limited capacity in terms of computing power, storage, and battery capacity. Hence due to limited resources, high-level security algorithms cannot be applied to IoT networks. As these IoT devices are becoming more and more popular security, privacy and creditability of the data produced by these devices have become an important issue. Smart Home devices like Google Home, Alexa collect user data and share it with third party companies, which store and process this data. But while sharing the data with third party organizations the security and privacy of the user's data may get violated. And currently there aren't any particular methods or ways to handle this type of situations.

Nonetheless, IoT data protection problems listed above can be solved by applying the Blockchain technology to the IoT networks. Blockchain was first created in 2008 by Sataoshi Nakamoto for a Bit-coin crypto-currency. The blockchain platform serves as a non-centralized security system that can deliver feasible solutions to IoT protection and creditability problems. It provides a stable, distributed, and autonomous system that enables IoT devices to communicate securely with each other and to sign transactions without relying on a third party for processing and verifying transactions. A distributed ledger keeps a record of transactions which consist of blocks of transactions linked together cryptographically, known as a Blockchain.

This paper focuses on the various issues of IoT and various methods proposed to resolve these issues. The paper is structured as follows; Section II gives information about the studies related to our topic. Section III gives us a brief information about the concept of IoT and Blockchain. While in Section IV we discuss the integration of Blockchain and IoT. Section V discusses challenges and future work andin section VI we conclude the paper.

ISSN: 2233-7857 IJFGCN

II. Overview and Related Work

We found 8 studies that reviewed the integration of Blockchain and IoT. Table-1 lists out the names of authors of the study papers, their proposed methods, advantages and disadvantages of their proposed architecture.

Year of Publication	Author and Paper Name	Objective/Description	Proposed System/Methods	Advantages	Disadvantages/Challenges
2019	Dr K Prasanna Lakshmi, K Archana, Y Prasanthi, V Padma - A Study on Internet of Things with Blockchain Technology	The authors disscussed the application of Blockchain technology to an IOT network. The impact of the Blockchain on the IOT network.	Integration of Blockchain with IOT : This methodology helps in tracking massive devices available in IOT, is used for transaction processing and helps to eliminate failures in IOT functionality.	Decentralized Architecture. Trusted System. Reliability. Security.	The protocols used in designing IoT network should be efficient and the devices used must be light weight. A standard validation of the devices must be done in order to reduce vulnerabilities.
2019	MD Azharul Islam, Sanjay K. Madria- A Permissioned Blockchain based Access Control System for IOT	To develop a private permissioned blockchain based system that resolves access control and transaction requests faster.	Hyperledger Fabric : An open source implementation of a permissioned blockchain. ABAC(Attribute based Access Control) model for access control is implemented in this system.	Due to ABAC model, permissioned blockchain based scheme can serve IoT resource access request much faster by utilizing the low transaction latency in Hyperledger Fabric.	The transaction latency (around 4 seconds) of the ABAC policy evaluation algorithm can be reduced by optimizing the algorithm.
2019	Gero Dittmann, Jens Jelitto- A Blockchain Proxy for Lightweight IoT Devices	In this paper, a Blockchain proxy has been introduced as a service to light-weight IOT devices. The objective of the proxy service is to minimize the footprint of connecting an IOT device to permissioned blockchain.	Fabric Proxy for Hyperledger Fabric, a permissioned blockchain with pre-order execution and separate nodes (peers) for ordering and committing transactions, a Blockchain with PKI-based identity management.	The system delivers trustworthy readings without any tampering to the blockchain. IOT devices are able to save a significant amount of CPU time and communication bandwidth by using the proxy.	Supports a limited number of programming languages. System is prone to DoS attacks, malicious reordering and dropping of transactions. Excessive memory usage.
2019	Mohamed Ferrag, Makhlouf Derdour, Mithun Mukherjee- Blockchain Technologies for the Internet of Things: Research Issues and Challenges	This paper is a detailed survey of existing blockchain protocols for the Internet of Things networks.	Malware detection system based on the consortium Blockchain. Data protection framework based on distributed blockchain. Blockchain-based dynamic key management for vehicular communication systems.	Low-cost, accessible, reliable. Backward security and Forward security. Resistent to DoS attacks, Tampering attack, Overlay attack. Can be implemented as a cloud platform.	Authentication is not considered. Lacks resistance to Sybil Attacks. Location privacy is not considered. Lack of Privacy and Anonymity. System becomes less reliable.
2019	Houshyar Honar Pajooh, M. A. Rashid - A Security Framework for IoT Authentication and Authorization based on Blockchain Technology	To address the IOT creditability and high-security issues. This paper explains the application of a decentralized blockchain technology to address the IoT security problems.	A self-clustering method for IoT network is proposed to cluster the network into K-unknown clusters using Genetic Algorithms that optimizes the network lifetime.	System provides Multi-layer Security. Communication efficiency is improved through peer to peer nature of the communication blockchain. Computational load , network load and delay are reduced.	The scalability challenges can be classified into two part: 1) a large number of IoT devices, 2) a massively increased data traffic. Due to open environment, system is prone to various attacks.
2019	Asma Lahbib, Khalifa Toumi, Anis Laouiti, Alexandre Laub, and Steven Martin - Blockchain based trust management mechanism for IoT	In this paper, the authors have discussed the design and the implementation of a secure trust management system based on the Blockchain technology to collect trust evidences and to securely store and share them within and through the Blockchain network.	A novel trust-management system based on Blockchain technology, which will define and evaluate a trust score for each IOT device and securely store and share these scores with other devices in the IOT network guaranteeing their transparency, integrity, authenticity, and authorization.	Blockchain based trust management system provides tamper proof trust information. More reliable information integrity verification. Enhanced privacy and availability during sharing and storage. Low complexity for IoT applications.	Limited Areas of Application. Performance can be improved furthermore. Trustworthiness of other system entities such as miners is not considered.
2019	He Bai, Geming Xia, Shaojing Fu - A Two-Layer-Consensus Based Blockchain Architecture for IoT	This paper describes a two-layer consensus system aiming to make it possible to apply Blockchain technology in IoT.	A two-layer consensus system for Blockchain applying in IoT. The Base-Layer consensus reduces the difficulty of mining and reduces resource consumption. The Top-Layer consensus ensures that the Base-Layer blocks are randomly performed in a transparent manner.	System provides distributed consistency without losing scalability. Increased Transaction Processing Speed. Decentralized Structure.	Huge computing power consumption. System no longer guarantees security. System is prone to DDoS attacks, Modification attacks. False Reputation.
2019	Jun Lon IoT: Blockchain Driven Internet of Things with Credit-Based Consensus Mechanism	a moderate-cost creditbased PoW mechanism and an efficient access control scheme for power-constrained IoT devices.	blockchain, each entity is a node in the blockchain-based IoT system. It also uses PoW mechanisam.	Provides Good Performance.	

Table 1: Survey Review Table

paper focussed on the use of blockchain technology to develop a permissioned based private blockchain system for IoT networks. A further two papers discussed the development of the blockchain-based consensus system. One paper focussed on a consortium blockchain-based malware detection system. And one paper proposed a self-clustering method for IoT networks using blockchain.

Thus Table - 1 focuses on the major contributions of the previous studies conducted regarding theblockchain technology applied IoT networks. We can say that the above-mentioned papers have built a strong base for IoT blockchains, but our survey focusses on the following points:

- We review various issues related to security, privacy and different attacks on IoT networks.
- We review existing research on security, scalability and privacy in BIOT systems.
- We discuss the challenges and potential future directions for research in blockchain IoT area.

III. Internet of Things and Blockchain

A. Internet of Things

The internet of things is a stepping stone for turning entities in the physical world into intelligent entities. The method is to turn the physical world into a gargantuan web of knowledge with all activated machines called things connected to each other and communicating with each other. IoT can be built based on three so-called Internet-oriented, Things-oriented and Semantic-oriented orientations. Internet-oriented model deals with the design of IoT applications. Things-oriented model deals with the type of sensors, actuators used. While, Semantic-oriented model handles the data representation and reasoning with the shared data.

ISSN: 2233-7857 IJFGCN

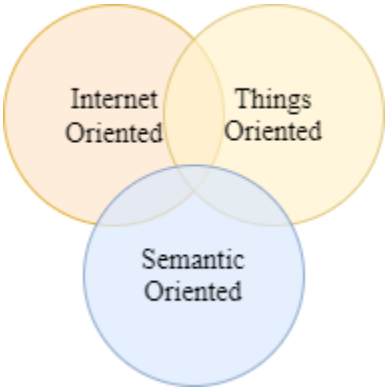

Fig.1 Three orientations of IOT

Architecture of IoT:

The Internet of Things links physical objects that can be static or movable with the space of the knowledge. Such entities have a heterogeneous dimension. Connecting such tools, extracting data from them, storing the collected data, analyzing that data and eventually producing the results involves an unbounded, autonomous architecture. The Service Oriented Architecture (SOA) operates on a concept of combining different elements, regardless of the suppliers, the products and the technologies used. SOA is thus ideally suited for the design of IoT applications.

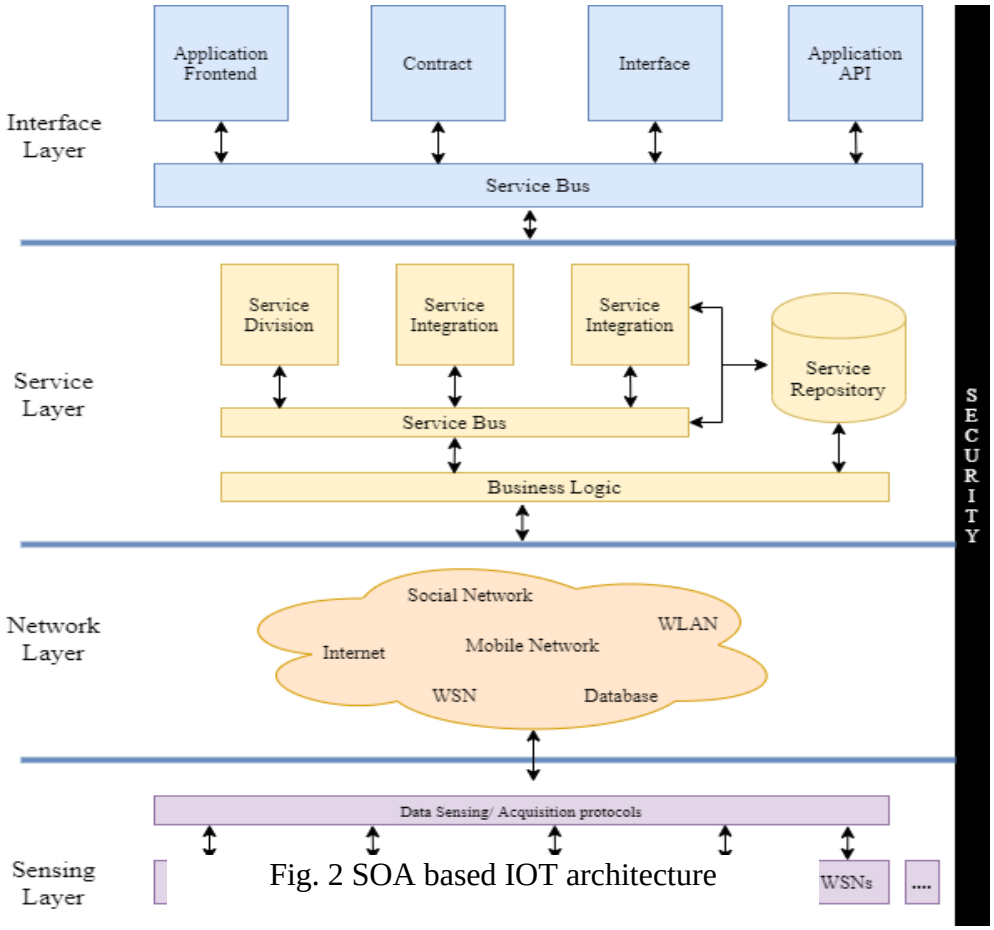

Fig. 2 SOA based IOT architecture

Fig. 2 shows the different layers of the SOA based IoT system architecture. The various protocols used in different layers of architecture are as follows:

1. Interface Layer - XML, HTTP, JSON

ISSN: 2233-7857 IJFGCN

2. Service Layer - MQTT, CoAP, AMQP, XMPP, SMQTT
3. Network Layer – Ipv6, TCP/UDP, RPL, 6LoWPAN
4. Sensing Layer – Zigbee, Bluetooth, Wi-Fi, NFC.

Security issues with IoT:

1. Data security: When the data generated by IoT devices passes across various layers or nodes, it has to be properly encrypted. Data encryption helps keep the data private. Due to its distributed architecture, the IoT Systems are vulnerable to attacks that pose data protection issues.
2. Availability: Denial of Service (DoS) or DDoS are the attacks on IoT devices which result in services not being readily available when needed.
3. Energy Efficient: IoT devices are lightweight, low powered, and have low capacity for storage. An assault on the system will increase the system's power consumption due to a flood of consumer's service requests in the network.
4. Trust: Number of IoT systems are used nowadays. Operating with these systems means building trust between the individuals involved in the sharing of data.

Attacks on IoT Systems:

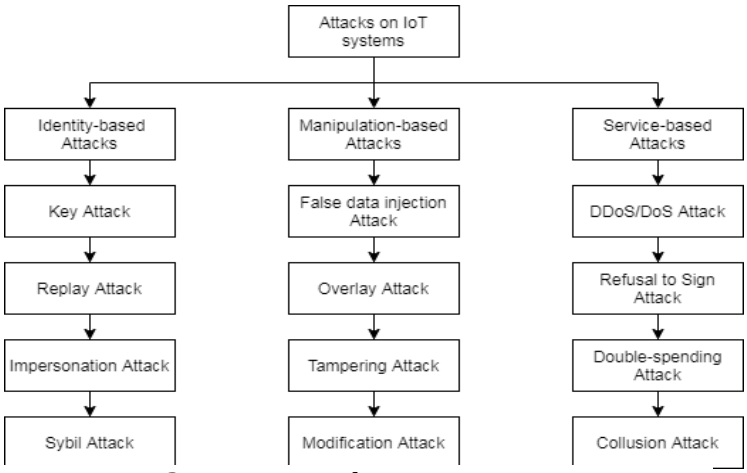

Fig. 3 various attacks on IoT systems

1. Identity-based Attacks: In this type, the attacks include manipulating identities of approved users to gain access to and exploit the network. There are four types of attacks under this category as follows:
   a. Key attack - It happens when an organization's private key has been used for long-term leaks, and the attacker uses it to impersonate the organization to gain access to the network.
   b. Replay attack - The purpose behind this attack is to spoof two parties identities, intercept their data packets and relay them to their destinations without alteration.
   c. Impersonation attack – An intruder attempts to impersonate a legitimate user to perform unauthorized operations.
   d. Sybil Attack: An attacker creates multiple false identities in this attack. And gains a wide impact within the group by conducting multiple interactions within the network.

2. Manipulation-based Attacks: Such attacks include unauthorized data access and manipulation. The attacks under this category are:
   a. False data injection attack: This attack is aimed at manipulating the data and undermining the system's data integrity to make it take wrong control decisions.
   b. Overlay attack.
   c. Tampering attack.
   d. Modification attack.

ISSN: 2233-7857 IJFGCN

3. Service-based Attacks: The aim of these attacks is to make a service unavailable or behave differently. Under this category, we can find the following attacks:
   a. DDoS / DoS attack: sending a large number of requests to cause network failure.
   b. Refusal to Sign Attack: A malicious agent will choose not to sign transactions in his favour. If an agent fails to sign the contract it will terminate the interaction.
   c. Double-spending attack: In this, the attackers are spending twice the same bitcoin to get extra numbers.
   d. Collusion attack: The nodes will collude with each other in this attack and act in a selfish manner to maximize benefit.

B. Blockchain

Blockchain a distributed public ledger technology was originally developed by Satoshi Nakamoto in 2008 for Bitcoin cryptocurrency. It was basically an accounting technique for handling the transactions of bitcoin cryptocurrency. Blockchain functions as a database that serves as a transaction ledger in a decentralized network where records of all existing transactions and transfers between the network entities are kept. Such transactions are held within the connected blocks. A block is a data structure that includes transaction records and stores them. A block consists of a message header and several records of transactions. In the blockchain structure of bitcoin, for example, the block header contains the hash value of the previous block, time stamp, Merkle root and other information. Block can be modified together because of the previous hash value, ultimately forming a chain called Blockchain.

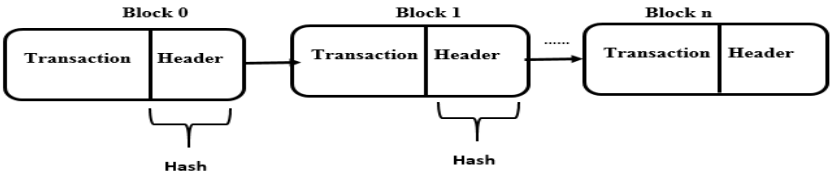

Fig. 4 Blockchain Structure

Mining is the process that creates blocks. In blockchain, the miners have to compete with each other to solve a computer problem with some level of difficulty, to create the blocks. The reason why blockchain needs mining is to maintain its decentralized structure. The blockchain keeps records of transactions between users of a P2P network. In general, a user has two keys: Public Key and Private Key. In blockchain system the private key is used to sign the transactions and the public key represents the unique address of user.

Initially, the user uses his private key to sign a transaction and broadcast it to his peers in the network. Upon receiving the transaction, the peers verify it and disseminate it over the network. The contract is collectively verified by all the involved bodies to reach a consensus agreement. The special node, called as miner, contains the correct transaction into a time stamped block until the consensus is reached. The block containing the transaction is then retransmitted back into the network. After the block that contains the transaction is validated and hash-matched with the previous block in the blockchain, the block that is broadcast is appended to the blockchain.

Blockchain's main aim is to free participants from the trust structures that both parties must sustain by exchanging their information with intermediaries. With cryptography, the blockchain system is able to prevent attacks that take over the network, since the network used and has no centralized control systems or a common storage system.

ISSN: 2233-7857 IJFGCN

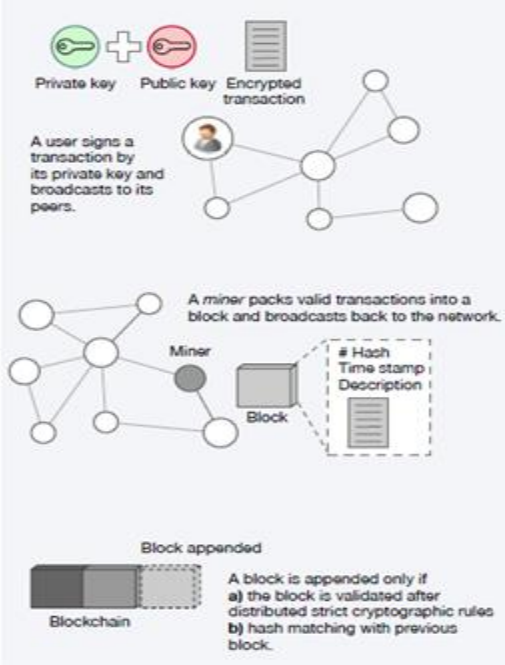

Fig. 5 Working of Blockchain methodology

Types of Blockchain:

1. Private Blockchain(Permissioned):
   A private blockchain network requires an invitation which must be validated by the network organizer. This places restrictions on who should participate in the network. No transaction costs for data recording and executing programs, since they are run by a group of authorities, are required in authorized blockchains. They can store and stream vast quantities of data or perform complicated calculations. Permissioned blockchains like the Hyperledger Fabric or Multichain are suitable for use with IoT.

2. Public Blockchain(Permission-less):
   A public blockchain network is open to everyone and anyone can participate in it. This network basically has a rewards mechanism which encourages more and more users to join the network. Bitcoin in one of the largest public blockchain mechanism available today.
   The drawbacks of public blockchains are:
   a. The amount of computational power needed to maintain the decentralized structure, more specifically to reach the consensus agreement.
   b. The openness of the system, which leads to no privacy for transactions and very little security in the network.

3. IOTA:
   It is a blockchain designed specifically for use in IoT. A DAG (Directed Acyclic Graph) is used to store transactions in place of blockchain. There are no blocks present, the DAG vertices represent transactions and the edges of the diagram represent transaction validation. This arrangement offers greater scalability, as there is no built-in maximum throughput.

Attempt to resolve IoT issues:

1. Data Privacy:
   The cryptographic techniques and consensus protocols used by blockchain technique provides data integrity and immutability. To achieve data integrity blockchain sacrifices confidentiality of data.

ISSN: 2233-7857 IJFGCN

2. Dynamic behaviour:
   After being implemented on a blockchain, smart contracts become permanent too. Smart contracts used to enforce access control in blockchain need to take into account the IoT network's complex behaviour, where new things can enter, old things can leave every time. If the dynamic behaviour of the system is out of the predefined rules, the smart contract should be able to help the adaptation of the access control.

3. Monitoring:
   The system can't support real-time monitoring due to the latency created by the consensus process in public blockchains. There is often a one-block interval delay until the state in the chain is changed and is publicly accessible to the users. If we want our system to support real-time monitoring, then use of private blockchain is desired. Use of private blockchain causes very less latency in the consensus process.

IV. Integration of IoT and Blockchain

In this section we review some of the existing systems that are designed to overcome the issues related to IoT systems, which have been discussed in the previous section. One of the ways to overcome the security and privacy issues of the IoT network is by using a private blockchain. As public blockchain provides almost no privacy for transactions and very less security to the system. The author of [1], has proposed a private blockchain based IoT access control system which uses attribute-based access control mechanism. The system is implemented by using Hyperledger Fabric. Hyperledger fabric is the open source implementation of a private blockchain technology. The system has two types of actors, one is Resource Provider and the other one is Requester. The system works on an ABAC model which includes attributes, policies and how the policies are evaluated based on the attributes.

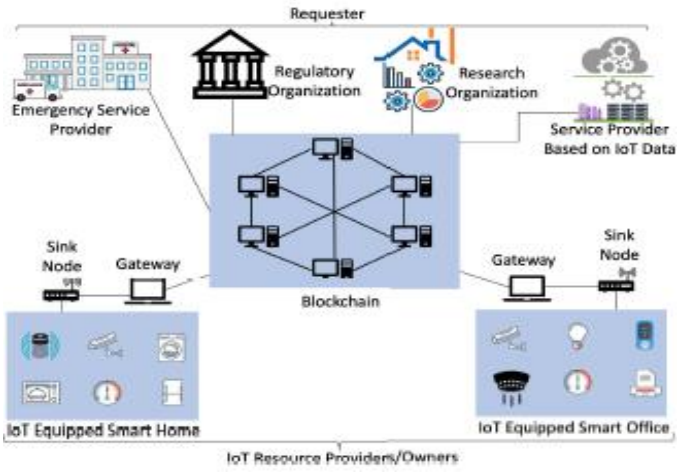

Fig. 6 System architecture for permissioned blockchain IOT network

The implementation of the ABAC mechanism in Hyperledger fabric involves forming a blockchain network. After that, creation of attributes and assignment, creation of policies and resource access request are done by sending transactions to the blockchain by the requester. The algorithm used for policy evaluation is NP complete. As private blockchain is used, the network can serve IoT access request much faster because of low latency offered by the blockchain. The transaction latency is around seconds, which can be improved by further optimizing the algorithm.

IoT devices are very crucial source of information for business processes. Blockchain is a very promising platform for such processes where multiple entities are involved. Hence the author of [2], introduced the concept of blockchain proxy for network of IoT devices. The IoT devices will offload to this proxy service a significant part of their software footprint. The network is a blockchain with Identity Management based on PKI. The framework implemented is Fabric Proxy for Hyperledger

ISSN: 2233-7857 IJFGCN

fabric. It is an authorized or private blockchain with pre-order execution and separate transaction order and commit nodes. Every fabric customer makes, signs and sends the transactions to the endorsing peers. The endorsing peers execute the transactions and sends an acknowledgement containing the result of execution signed by the endorsing peer, back to client. The client collects enough endorsements to fulfil the endorsement policy in a transaction, signs it and sends it to orderers. The orderers arrange the transactions sequentially, group them in blocks and distribute them to the committing peers. Committing peers validate the transactions and commit valid transactions to their local copy of the ledger. The system uses a slim SDK of Go language without client identity and transaction signing for IoT devices and remaining SDK back end for Proxy. Both these parts are connected to each other by using MQTT protocol on top of TCP/IP used in IoT networks.

The system proposed in [2], delivers trustworthy data without any tampering to the blockchain. The IoT devices are able to save a lot of computing power and communication bandwidth by using the proxy. Although the system supports only a number of programming languages and is prone to attacks like DoS.

The dynamic and complex network environment of IoT requires a flexible solution which can quickly adapt to changes within a secure and distributed architecture. The distributed and decentralized structure of blockchain makes it a very feasible solution to address the communication security challenges of IoT networks.

The author of [3], proposed a multi-layer network security model for IoT networks to resolve security issues in 5G cellular systems. The proposed model solves the problems associated with blockchain technology by splitting the structure into a decentralized multi-layer architecture. Using evolutionary computation algorithms, the network is divided into K-unknown clusters in this model. Uses algorithms such as Genetic Algorithms (GA) and Particle Swarm Optimization (PSO). For authorizing and authenticating purposes within each cluster operated by a cluster head a local authentication mechanism is chosen. Blockchain's high security and authenticity offers an authentication mechanism for interaction between the cluster heads and base stations. Nodes are initially grouped together as clusters in the network, and an optimal selection procedure for the cluster head is performed. The aim of clustering is to achieve less overheads and network delays. GA and PSO are used for the process of cluster head selection as well as clustering.

The model in [3] provides multi-level security. By using the model described above, it can be observed that the computational load, network load and delay are reduced significantly in the network. Also, the communication efficiency is improved. But the system faces scalability issues due to large number of IoT devices and increased data traffic. The system does not provide tolerance against Sybil attacks, DoS/DDoS attacks and etc.

Security is one of the big obstacles for IoT scenarios to be applied and realized. To determine an entity's trustworthiness, it is necessary to share trust information in order to arrive at an accurate assessment. For this purpose, authors of [4] propose a stable trust management framework based on blockchain technology. The trust management system based on blockchain can provide tamper-proof data, more efficient integrity of trust information, and helps improve privacy and availability during sharing and storage. The main goal of this approach is to suggest a novel method of trust management. The system used in this model is designed to establish and evaluate a trust score for each device, and to store and exchange these scores securely with the other devices in the IoT network.

The system designed in [4], is made up of number of zones which contain some physical resources. In each sector, there is also an authentication manager who is responsible for authorisation decisions, system verification and tokens generation. The device is linked to a trust manager, who determines the degree of trustworthiness and calculates the final trust score for each system in the sector. A group of miners are then deployed to collect the trust data, build blocks of it and retransmit them back into the network. Every individual inspects the validity of transactions broadcast by the miners in the network and then arranges these checked transactions into a block that will be added to the distributed ledger. The system is developed by using Multichain blockchain technology and Round Robin (RR)

ISSN: 2233-7857 IJFGCN

algorithm as the consensus method for approving transactions. Although, the system has a limited number of areas of application and while assigning trust scores, trustworthiness of entities like miners is not considered.

Due to the immutable nature, Blockchain provides a decentralized solution to overcome security and privacy issues of IoT networks. But the integration of blockchain with IoT is limited by scalability and computing resources. So, the author of [5] proposed a two-layer-consensus based architecture of blockchain specifically designed for IoT requirements. The system is divided in two layers – Base layer and Top layer. Devices with low resources, users and other nodes form the base layer, maintaining a blockchain with full functionalities. Users or the other nodes can begin new transactions to other entities which can execute them, then the transactions are sent to the poll where they wait for getting packed in blocks. Hybrid consensus approach is used to allow more base-layer nodes to engage in blockchain maintenance. Special nodes that run a non-byzantine fault tolerance algorithm to evaluate the accounting rights form the top-layer of high-security blockchain. Top-layer does not really mimic any standard IoT cloud. The nodes in the top layer determine only the accounting rights, and never determine how or what to do. The top layer serves as a computer's RAM and hard disk, while the base layer serves as a CPU carrying out its functions.

The architecture proposed in [5], provides consistency without losing scalability and increased transaction processing speed. However, consumption of huge amount of computing power can be seen. Also, the system no longer guarantees security, which makes it prone to DDoS, Modification, and False Reputation attacks.

In certain instances, IoT systems are built by adopting the client-server architecture, which makes it exposed to single-point failures and malicious attacks. The author of [6], suggests a credit-based proof-of-work system for IoT devices to address such vulnerabilities. The framework is based on a blockchain formed by a Directed Acyclic Graph (DAG / IOTA). This increases the quality of transactions and enhances security. The system can be divided into two categories: full nodes, and light nodes. Light nodes are the power-constrained IoT apps, they do not store blockchain information because of their restricted existence. Full nodes are strong nodes namely gateways or servers, their main role is to maintain the network of blockchains, i.e. Tangling. Full nodes preserve the tangle by harvesting, transmitting, and synchronizing information about blockchain, and light nodes improve tangle stability by validating and uploading new transactions.

The working of the system described [6] is as follows, the manager i.e. PC initializes the gateways to setup the tangle network. The manager may then approve or disable the devices in the IoT network by updating the device list in the form of a transaction. In the next phase, the manager hands out the confidential key to IoT devices that store sensitive data. Before publishing the transactions, the IoT system must encrypt the data, using the secret key, which ensures data privacy. After that, the IoT system will collect tips before sending new transactions, to verify the transactions[17 18]. The IoT app bundles the new transaction with these two checked tips using the PoW algorithm when the transactions are validated, and submits it to the gateway.

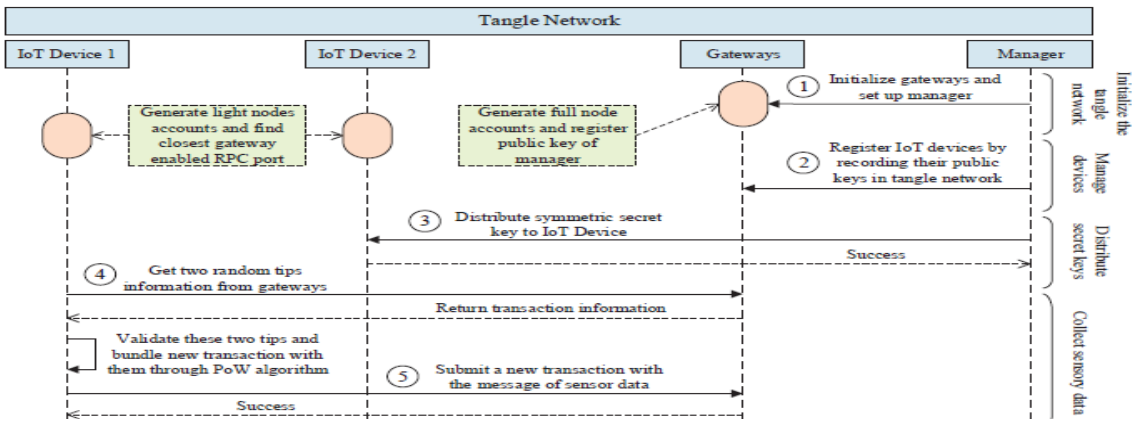

Fig. 7 interaction of devices, gateways and manager in credit-based consensus system

ISSN: 2233-7857 IJFGCN

Challenges and Future Work

1. Scalability
   Scalability issues in the existing blockchain solutions are a major drawback in acceptance and deployment of blockchains. The scalability issues can be classified in two categories: 1) a large number of IoT devices and 2) increased amount of data traffic. In existing blockchains, every node needs to maintain a copy of the blockchain, which is nearly impossible for resource constrained IoT devices. In an IoT network, as the number of nodes increases the amount of data generated is large, and the problem becomes more and more complex. Hence, Blockchain solutions remain out of scope for resource and storage constrained IoT devices.
2. Security and Privacy
   IoT devices are small sensors which collect a lot of sensitive data. For e.g. in home automation system the IoT sensors collect a lot of private and sensitive data of users. It is unacceptable that this data gets stored on some other nodes outside the home automation system. Another concern is communication security in IoT systems. IoT systems are already vulnerable to various attacks. Proper secure communication protocols must be applied to IoT networks in order to provide security and privacy. Along with security risks of IoT, blockchains bring their own set of risks. Some known risks of blockchain are smart contract program vulnerabilities, message leak, etc. Also, privacy leakage is another important issue in blockchains.
3. Storage Issue
   When you combine blockchain with IoT, the storage problem can be extremely severe. As compared to blockchain nodes, the majority of IoT devices have low storage capacity. Even a high storage capacity blockchain node can't handle the growing volumes of data. The heterogeneous IoT systems would complicate the storage issue, as systems with low storage space build network bottlenecks.
4. Dynamic and Adaptable Security Framework
   Inside the IoT network, which consists of low-powered devices as well as high-end servers, heterogeneous devices are deployed. So, as the number of resources is small, a single security protocol cannot be applied to the entire Blockchain-network. So how to build a complex and adaptable security framework for the entire Blockchain- IoT network should be one of the areas of potential enhancement.
5. Energy and Cost Efficiency
   The consensus algorithms used in mining process of blockchain technology like proof-of-work (PoS), require a lot of computational power to execute and consume a large amount of electricity. As the size of blockchain increases, we need more powerful miners to run these algorithms. Some energy efficient algorithms have been proposed in recent past. But energy and storage constrained IoT devices still cannot handle large amounts of data generated. Hence, design of a power efficient algorithm is still a challenge.
6. Stakeholders also assume that blockchain is only connected to cryptocurrencies and has no uses other than finance.
7. Large enterprises or MNC's have already spent a large amount of financial resources to upgrade their platform's to latest technologies, So it is not possible for them to spend another fortune to adapt to the blockchain technology, they need a cost effective solution.

Future Scope
Both IoT and Blockchain are new technologies. Blockchain is a reliable technology for securing the IoT networks. As there are a lot of areas still left unexplored, which can be explored in the near future. So, we will continue our investigation in the field of different applications of blockchain technology for IoT devices.

V. Conclusion

The use of blockchain technology in IoT networks is going to increase in the near future and it is going to benefit multiple sectors where automation of any kind is used. The existing IoT systems face many problems such as security issues, privacy issues, trust management, scalability, and storage

ISSN: 2233-7857 IJFGCN

issues. Through research we were able to list out various types of attacks that can affect the IoT systems.

In this paper, we carried out a survey to analyze how blockchain can be applied to IoT applications. We also reviewed some interesting state-of-the-art blockchain methods used to overcome the challenges faced by IoT systems. We overviewed different types of private blockchains such as Hyperledger Fabric, IOTA/DAG-structured, Multichain, etc. And we came to conclusion that private blockchain would be very useful for IoT applications, instead of public blockchain.

Based on our knowledge, we provided insights on different challenging areas of research such as scalability, privacy and security, storage, dynamic security framework, which should be further explored in the near future.

References

[1]M. D. Azharul Islam, Sanjay K. Madria, "*A permissioned blockchain based Access Control System for IOT*," in 2019 IEEE International Conference of Blockchain, IEEE, 2019.

[2] Gero Dittmann, Jens Jelitto, "*A Blockchain Proxy for Lightweight IoT Devices*," in 2019Crypto Valley Conference on Blockchain Technology, IEEE Access, 2019.

[3] Houshyar Honar Pajooh, M. A. Rashid, "*A Security Framework for IoT Authentication and Authorization based on Blockchain Technology*," in 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, IEEE, 2019.

[4] Asma Lahbib, Khalifa Toumi, Anis Laouiti, Alexandre Laube, and Steven Martin, "*Blockchain based trust management mechanism for IoT*," in 2019 IEEE Wireless Communications and Networking Conference, IEEE, 2019.

[5] He Bai, Geming Xia, Shaojing Fu, "*A Two-Layer-Consensus Based Blockchain Architecture for IoT*," in 2019, IEEE.

[6] Junqin Huang, Linghe Kong, Guihai Chen, Long Cheng, Kaishun Wu, Xue Liu, "*B-IoT: Blockchain Driven Internet of Things with Credit-Based Consensus Mechanism*," in 2019 IEEE 39th International Conference on Distributed Computing Systems, IEEE, 2019.

[7] Dr. K. Prasanna Lakshmi, K. Archana, Y. Prasanthi, V. Padma, "*A Study on Internet of Things with Blockchain Technology*," in 2019 Third International Conference on Trends in Electronics and Informatics, IEEE Xplore, 2019.

[8] Sunghyun Cho, Sejong Lee, "*Survey on the Application of BlockChain to IoT*," in 2019, IEEE.

[9] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras, Helge Janicke, "*Blockchain Technologies for the Internet of Things: Research Issues and Challenges*," in 2018, IEEE.

[10] Wattana Viriyasitavat, Li Da Xu,Zhuming Bi, Danupol Hoonsopon, "*Blockchain Technology for Applications in Internet of Things - Mapping from System Design Perspective*," in 2018, IEEE.

[11] Tejasvi Alladi, Vinay Chamola, Reza M. Parizi, Kim-Kwang Raymond Choo, "*Blockchain Applications for Industry 4.0 and Industrial IoT: A Review*," in 2019, IEEE Access.

[12] Quang Le-Dang, Tho Le-Ngoc, "*Scalable Blockchain-based Architecture for Massive IoT Reconfiguration*," in 2019 IEEE Canadian Conference of Electrical and Computer Engineering, IEEE, 2019.

[13] Hongyang Liu, Feng Shen, Zhiqiang Liu, Yu Long, Zhen Liu, Shifeng Sun, Shuyang Tang, Dawu Gu, "*A Secure and Practical Blockchain Scheme for IoT*," in 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, IEEE, 2019.

[14] Sin Kuang Lo, Yue Liu, Su Yen Chia, Xiwei Xu, Qinghua Lu, Liming Zhu, Huansheng Ning, "*Analysis of Blockchain Solutions for IoT: A Systematic Literature Review*," in 2019, IEEE Access.

[15] Mingli Wu, Kun Wang, Xiaoqin Cai, Song Guo, Minyi Guo, Chunming Rong, "*A Comprehensive Survey of Blockchain: from Theory to IoT Applications and Beyond*," in 2019, IEEE.

[16] Akshay Pillai, Sindhu M., Lakshmy K. V., "*Securing Firmware in Internet of Things using Blockchain*," in 2019 5th International Conference on Advanced Computing & Communication Systems, IEEE, 2019.

[17]Dhumane, A., & Prasad, R. (2015). Routing challenges in internet of things. CSI Communications.

[18] Dhumane, A. V., Prasad, R. S., & Prasad, J. R. (2017). An optimal routing algorithm for internet of things enabling technologies. International Journal of Rough Sets and Data Analysis, 4(3), 1–16.

ISSN: 2233-7857 IJFGCN