Blockchain: A Game Changer for Securing IoT Data

Madhusudan Singh
Yonsei Institute of Convergence Technology
Yonsei University
Songdo South Korea

Abhiraj Singh
Department of Mechanical Engineering
IIT-Roorkee,
Roorkee, India

Shiho Kim
School of Integrated Technology,
Yonsei University,
Seoul, South Korea

***Abstract*—Internet of Things (IoT) is now in its initial stage but very soon, it is going to influence almost every day-to-day items we use. The more it will be included in our lifestyle, more will be the threat of it being misused. There is an urgent need to make IoT devices secure from getting cracked. Very soon IoT is going to expand the area for the cyber-attacks on homes and businesses by transforming objects that were used to be offline into online systems. Existing security technologies are just not enough to deal with this problem. Blockchain has emerged as the possible solution for creating more secure IoT systems in the time to come. In this paper, first an overview of the blockchain technology and its implementation has been explained; then we have discussed the infrastructure of IoT which is based on Blockchain network and at last a model has been provided for the security of internet of things using blockchain.**

***Index Terms*—Internet of things, Blockchain, Security, Devices, Network.**

I. INTRODUCTION *(HEADING 1)*

Blockchain technology is now getting too much of attention from software scientists since it has been cre- ated. Fig 1 shows the basic pillars of blockchain technology in internet world. Actually, it has the ability to revolutionize and optimize the global infrastructure of the technologies connected with each other through internet. It has mainly two fields that are going to be influenced by it which are:

- By creating a decentralized system, it removes the indulgence of central servers and provides peer-to-peer interaction.
- It can create a fully transparent and open to all database, which could bring transparency to the governance and elections.

Blockchain technology basically has 4 pillars, first, Consensus, which provides the proof of work (PoW) and verifies the action in the networks, second is ledger, which provides the complete details of transaction within networks. Third, Cryptography, it makes sure that all data in ledger and networks gets encrypted and only authorized user can decrypt the information and fourth is smart contract, it is used to verify and validate the participants of the network.

IoT is maturing very fast and making its presence felt in almost every field of technology. However, with its rapid evolution, it has made itself more prone to cyber-attacks. Now there is an urgency to make IoT more secure [1].

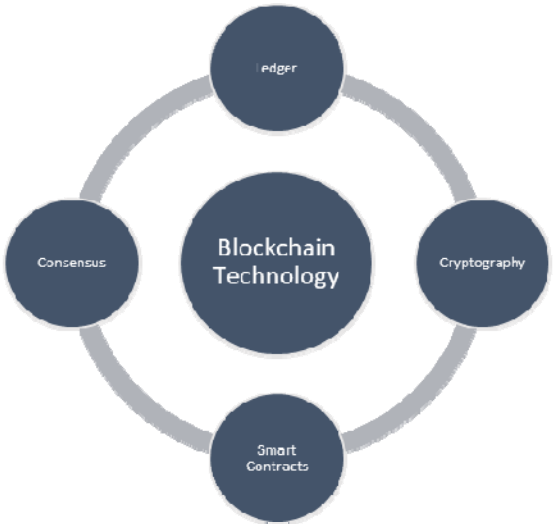

Fig. 1. Pillars of Blockchain Technology

Internet-Of-Things (IoT) refers to a loosely coupled, a system of multiple heterogeneous and homogeneous devices having the power of sensing, processing, and network capabilities [2]. Internets of Things have been discussed aptly with semantic touch in the IoT vision [3].The current scenario for making a safe and secure car is to lock your car automatically or manually. We become sure of its safety and security [4]. Our future generation cars would be having all sensors based devices and at the same time connected in to the system [5]. The cars with these devices make our car smart but are they safe? This is the pertinent question which compels us to write a more safe architecture for making our cars based on IoT devices safe and secure and connected to the Internet every time[6].

The purpose of this research paper is to provide guidance for the use of blockchain technology, through cases to make a more secure and trustable IoT model.

We proceed further to explain our article in following section VI section. Section II has describes need of security for IoT environment, Section III introduce the blockchain technology, section IV has mentioned the explanation of Internet of things structure based on blockchain technology. In section V shows the security strengths of blockchain for IoT architecture. In Section VI, we have conclude our article.

II. Concerns with Implementation IoT: IoT Security

IoT has numerous applications, for example: in making smart homes, Smart City, Improving Health, Autonomous Vehicles, etc. Some IoT devices are currently available in the market like Wearables, Smart Thermostat Systems, Air Conditioners, and refrigerators that use Wi-Fi for remote monitoring. Apart from all these benefits, IoT has some serious issues, which should be sorted out before it gets implemented, like the technologies on which the foundations of IoT have been established have several bugs, so if hackers get access to the system through these bugs then they can compromise the privacy of the customer or even can cause harm to them. Thus before implementing IoT, the security of these systems should be strengthened and made free from any bugs. Keeping the IoT device secure is one of the most difficult tasks to accomplish. In making these devices cheap, small and easy to use many security policies are compromised which increases the risk of security breach. In figure 2 shows the taxonomy of the IoT security.

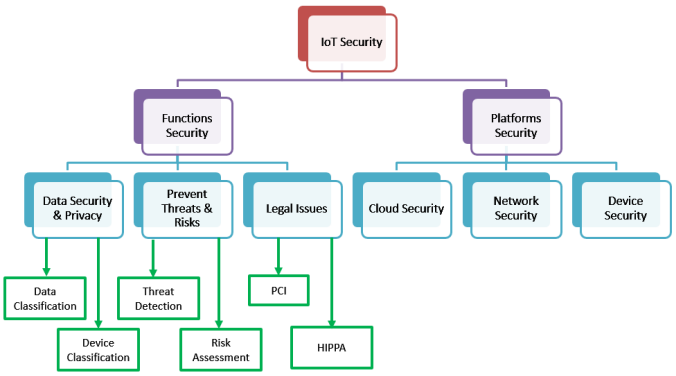

Fig.2. Taxnomy of IoT Security

III. Overview of Blockchain Technology

Blockchain is a kind of decentralized database, which keeps record of every transaction made on a network. Rather than having a traditional central database like that of banks or governments, it has a ledger distributed over a network of nodes. This network can be public, like the internet, which is accessible to any person in the world or it can be private, with accessibility given to only members of an organization. Blockchains decentralized cryptographic model allows users to trust each other and make peer-to-peer transactions, eliminating the need of intermediaries. This technology is not only affecting the way we use internet, but the global economy is also being revolutionized [2].

A. Components of a Blockchain

Blockchain mainly has 4 components which form its complete infrastructure. Fig.1 shows the component of blockchain.

1) *Network of Nodes:* All the nodes connected through the internet maintain all of the transactions made on a blockchain network collaboratively. The authenticity of the transaction is checked by the protocol, which eliminates the involvement of a trusted third party for validation purpose [3].
When a transaction is done, its records are added to the ledger of past transaction, this process is known as 'mining'. The proof of work has to be verified by the other nodes present on the network.
2) *Distributed database system:* The database, which is composed of blocks of information, is copied to every node of the system. Each block contains the following data in itself: A list of transactions; a timestamp; Information, which links it to the previous chain of the blocks.
3) *Shared ledger:* The ledger is updated every time a transaction is made. It is publicly available and is incorruptible which introduces transparency to the system.
4) *Cryptography*: It binds the data with the very strong crypto mechanism, which is not easy to track or tampered by unauthorized users.

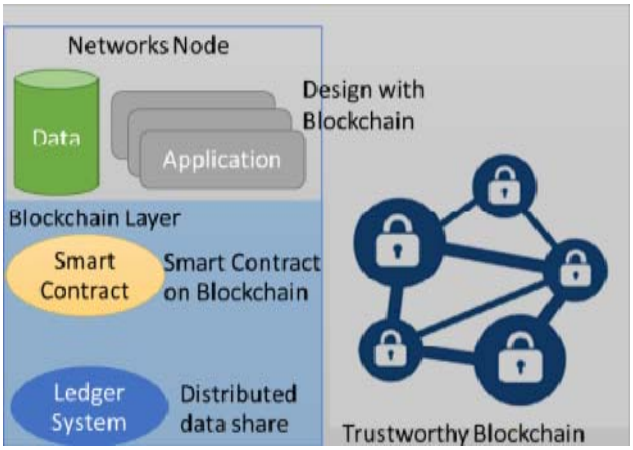

Fig. 3. Blockchain Networks and its Components

B. Constructing a blockchain

A new digital transaction is made which is then con- verted into a cryptographically protected block. Mem- bers of the blockchain network having high computation power (Miners) compete with each other to validate the transaction by solving difficult coded problems. First one to solve receives a reward (In case of bitcoin blockchain, the miner would get bitcoins). Then the validated block is timestamped and is added to the chain in chronological order. The acceptance of block by nodes is expressed when it creates another block in the chain, using the hash of the earlier accepted block [4].

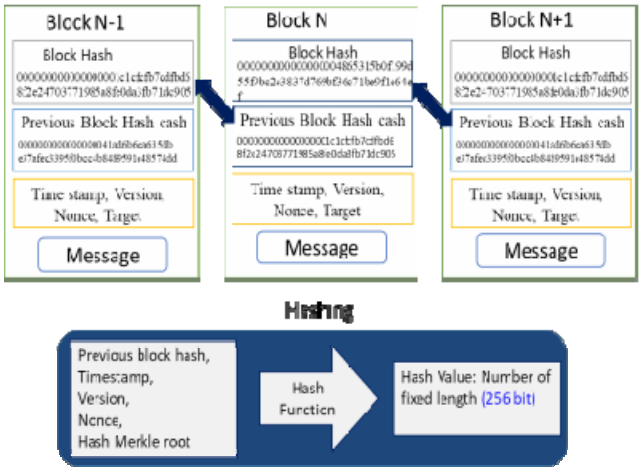

Fig. 4. Block Structure

C. Implementing a Blockchain

Blockchain can be mainly deployed in 3 domains [1].

1) *Public:* Un-permissioned area, each and every node can send or read transaction and can take part in the consensus process without the requiring any permission. Bitcoin and Ethereum come under this category.
2) *Consortium area:* It comes under partial permission, only defined nodes can take part in the consensus process. The permission to read or send may be made public or may be provided only to few authorized nodes.
3) *Private:* It is the permission area, only the organization to whom the network of blockchain belongs can write transaction to it. Reading of transaction may be public or restricted to few nodes depending upon the requirement. This type of system is generally deployed in industries.

IV. Blockchain Based Internet of Things

Before we can go into the security aspects of IoT using blockchain technology, let us first understand the pattern of IoT-based on blockchain technology.

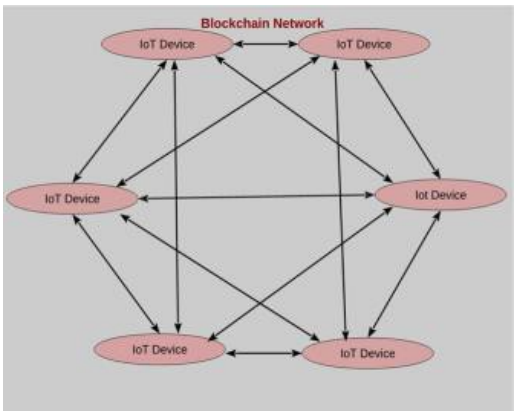

Fig. 5. Blockchain network for IoT

We have defined 3 of such patterns

A. Communication Model

In this model, mainly three of the fundamental functions of blockchain network are used.

- Peer-to-peer messaging
- Distributed data sharing.
- Autonomous coordination with the device.

However, unfortunately, it has its own limitations, which make it problematic to implement:

1) *Slow Processing:* Generally, low-end CPU are available which makes it hard for processing, as computations in blockchain require high CPU and memory to work properly.
2) *Small Storage:* as more and more transactions are made the size of ledger goes on increasing.

However, companies such as IOTA [9], like block- chain tiny sensors, are proposing new approaches: results a decrease in hardware require requirements by simplifying the process of mining.

In this context, an architecture has been illustrated below: below (fig. 5), is a blockchain network with the implementation of technology: mining, ledger, encryption, etc.

Here, blockchain nodes are the members of the net- work, participating actively in the transaction process. They validate the transaction through mining; they can be personal computers, enterprise servers or also cloud- based nodes. Clients are the IoT devices; they do not store the distributed ledger. Blockchain client's block- chain nodes interact with each other through APIs. IoT devices create transactions and these transactions are relayed to blockchain nodes for processing and storing the data into the distributed ledger. mHTTP REST APIs can be used to establish communication between IoT and blockchain. They are specific for every blockchain node [5].

To avoid any "man-in-the-middle-attack" which can affect transaction details or can cause a double-spend, a complete trust must be established between clients and the nodes they are connected with. Messages that are exchanged between multiple IoT devices contain data, which are directly integrated in the transactions relayed by devices, which participate in exchanges, to block- chain nodes [10].

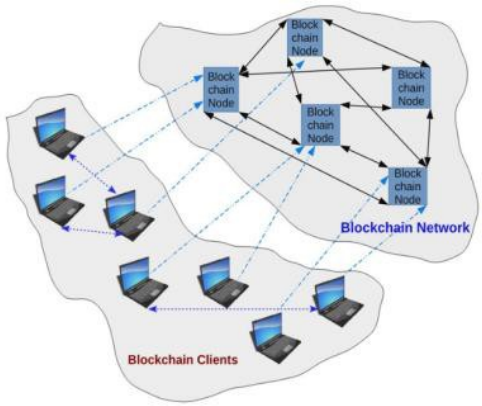

Fig. 6. Distributed data Share architecture

B. Connecting multiple blockchain networks

With the recent researches, it has been predicted that future is going to be constructed by multiple blockchains, with each having different features and providing different services. Here, Blockchain network may be a home network, enterprise or the internet. Message formats and communication protocols between devices are out of the scope of blockchain implementation: it refers to machine-to-machine communication [11]. If artificial intelligence is added to the IoT environment that is connected to a blockchain network it creates a Decentralize Autonomous Organization (DAO), DAO refers to an organization that runs without any human intervention [12].

V. Ways to Strengthen IoT Security with Blockchain Technology

Points that have to be considered to establish a secure IoT using technology. Fig. 7 shows the strength of blockchain those are built to secure IoT environment.

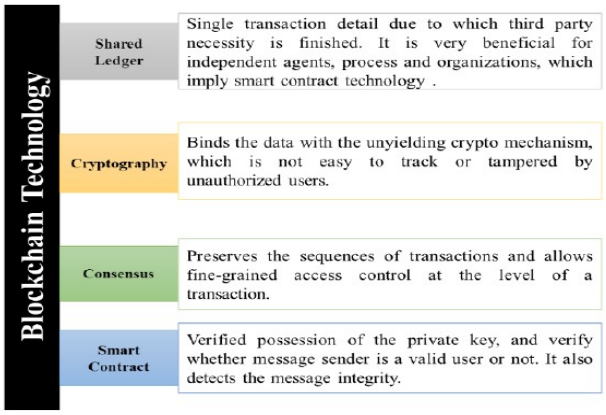

Fig. 7. Blockchain strengthen

A. Secure communication

In some cases, IoT devices have to communicate for the purpose exchanging data required to process a trans- action and to store it in a ledger.

These ledgers can also be used to store encryption keys to make the exchanges more confidential. IoT de- vice sends an encrypted message using the public key of the destination device, which is then stored in the block- chain network. The sender then asks its node to get public key of the receiver from the ledger. Then the sender encrypts the message using public key of the receiver, in this way, only the receiver will be able to decrypt the sent message using their private key [13].

B. Authentication of users:

The sender digitally signs the message before sending them to other devices. The receiving device then gets the public key from the ledger and uses it to verify the digital signature of the received message. We have describe the digital signature work at below:

- First, the sender calculates hash of a message that is then encrypted with its private key.
- The digital signature along with the message is transmitted.
- The receiver then decrypts the digital signature using the public key of sender stored in the ledger to obtain the hash value as calculated by the sender.
- The message is valid only if the calculated hash and the protected hash of the message are same.
- The trust on retrieved messages is improved if the digital signature of each message is stored into the ledger.

C. Discovering legitimate IoT at large scale

With potentially millions of IoT devices are to be connected on the same network, there is an urgent need to get the ability to discover devices at scale and to dis- cern legitimate and illegitimate nodes [14].

As soon as a new IoT device starts, it first asks root servers to give a list of trusted nodes in the network. Then this device registers itself in a node, and then the exchange of information starts. It receives information from other nodes and sends its information to other peers on network.

DNSSec has to be implemented to secure name resolution of root servers by avoiding any spoofing attacks.

In public network, this enrollment method can be easily applied without any specific constraints.

For private network, it has to be made sure that only the legitimate devices can be added to the blockchain network. For this, the root servers must authenticate the device before providing it the nodes list. To ensure integrity and confidentiality, every communication made must be authenticated and encrypted efficiently [15]. This can be done based upon:

- Credentials already installed on the device during setup: There should be a safe process, which could be a part of blockchain implementation, which could generate these credentials.
- Credentials could be given by the owner of the IoT device: It initializes the process of device enrolment into the security server to get the credential for IoT.

D. Configuring IoT

Blockchain technology helps a lot in establishing a trusted and secure configuration for IoT devices. Approaches that seem relevant here are:

- Properties of IoT like Configuration details and the last version firmware validated can be hosted on the ledger. During bootstrap, the blockchain node is asked to get its configuration from the ledger. The configuration is required to be en- crypted in the ledger to prevent the discovery of IoT network topology or its properties by analysis of the information stored in the public ledger.
- The hash value of latest configuration file for every device can be hosted in the ledger. Using a cloud service the IoT device will have to down- load the latest and trusted configuration file after every fixed interval of time (say every night). Then the device can use the blockchain node API to retrieve and match the hash value, which is stored in the blockchain. This would allow the administrators to remove any bad configurations regularly and reboot each and every IoT device in the network with latest and trusted configurations.

Example: A Use Case for the Blockchain based IoT Security Model:

Fig.7. shows a series of IOT devices interconnected with each other on a network. Securing them with a blockchain network makes the system decentralized, in which there is no single authority which can approve any transaction. Each and every device will have a copy of the ever growing chain of data. This means that whenever someone wishes to access the device and do some transaction, then all the members of the network must validate it. After the validation is done, the performed transaction is stored in a block and is sent to all the nodes of the network. All this make the system more secure and impossible for the un-authorized sources to breach into the security.

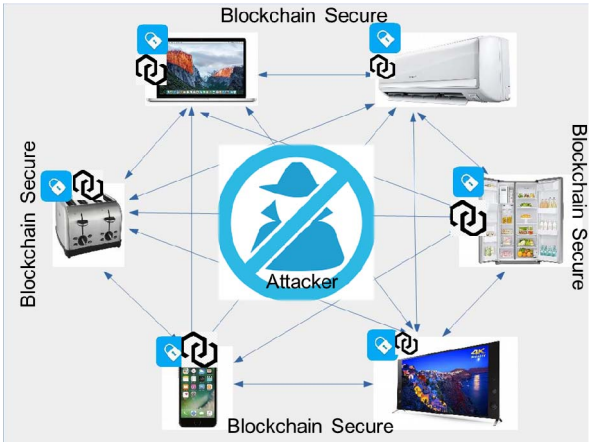

Fig. 8. Blockchain Secured IoT Devices

VI. Conclusion

In this article, we have provide guidance for the use of blockchain technology, through cases to make a more secure and trustable IoT model. Because of the high-end hardware requirements for the internet of things, we concluded that internet of things is not going to be a full member of a blockchain network. But internet of things is definitely going to be benefited from the functionalities introduced by the blockchain technology through the APIs offered by the nodes of the network or by any specialized intermediaries. Through these functionalities internet of things could be made highly secure.

We have discussed the new and emerging blockchain technology cybersecurity point. Blockchain technology mostly using and concentrating the finance area research work, as we know Bitcoin is a cryptocurrency which is based on blockchain technology. But in our article we try to introduce blockchain technology for internet of things to make secure data transmission between the internet connected devices. For this we have provide oview of blockchain technology, security issues on IoT environment and also discuss and propose blockchain is as a solution of IoT Security.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2017-0-00560, Development of a Blockchain based Secure Decentralized Trust network for intelligent vehicles)

References

[1] Singh, Dhananjay, Gaurav Tripathi, and Antonio J. Jara. "A survey of Internet-of-Things: Future vision, architecture, challenges and services." Internet of Things (WF-IoT), 2014 IEEE World Forum.

[2] Atzori, and Morabito, “The internet of things: A survey”, Computer Networks, 54(15), 2787–2805, 2010.

[3] Humayed, Abdulmalik, "Cyber-Physical Systems Security—A Survey." arXiv preprint arXiv:1701.04525 (2017).

[4] Meinel, Holger, and Wolfgang Bösch, "Radar Sensors in Cars." Automated Driving. Springer International Publishing, 2017. 245-261.

[5] Uden, Lorna, and Wu He, "How the Internet of Things can help knowledge management: a case study from the automotive domain," Journal of Knowledge Management 21.1 (2017).

[6] Sot iriadis, Stelios, Kostantinos St ravoskoufos, and Euripides GM Pet rakis, "Future Internet Systems Design and Implementation: Cloud and IoT Services Based on IoT-A and FIWARE." Designing, Developing, and Facilitating Smart Cities, Springer International Publishing, 2017. 193-207.

[7] http://www.informationsecuritybuzz.com/expert-comments/symantec-report-hijacked-iot-devices-ddos/

[8] On Public and Private Blockchains, “https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/,”2017

[9] IOTA http://iotatoken.com/

[10] Machine-to-Machine, https://en.wikipedia.org/wiki/Machine_to_machine

[11] Madhusudan Singh, “Perspective, Challenges, and Future of Automotive Security Enriched with Blockchain Technology”, IEEE Transportation Electrification Community Webinar-Abstract,06 Dec, 2017. https://register.gotowebinar.com/register/6157413934050745602

[12] Understanding Autonomous Organizations on the Blockchain https://www.linkedin.com/pulse/understanding-autonomous-organizations-blockchain-paul-kohlhaas

[13] C. Decker and R. Wattenhofer, “A fast and scalable payment network with bitcoin duplex micropayment channels,” In Stabilization, Safety, and Security of Distributed Systems pages 3–18. Springer, 2015

[14] Das, Manik Lal, "Privacy and Security Challenges in Internet of Things," Distributed Computing andInternet Technology. , pp. 33-48, 2015.

[15] Joseph Bonneau, “Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,” IEEE SECURITY AND PRIVACY (forthcoming May 2015), http://www.jbonneau.com/doc/BMCNKF15-IEEESP bitcoin.pdf.