Blockchain To Secure IOT And Its Applications: A Review

Dr.A.Nithya[1], Mrs.N.Paviyasre[2]
[1, 2] Assistant Professor,Dept of Computer Science (SF)
[1, 2] Kongunadu Arts and Science College, Coimbatore, India.

Abstract- *Internet of things and Blockchain are the two technologies which are gaining reputation since the time of their creation. In the near future, IoT is going to impact nearly every day-to-day particulars used by us. As the practice of this technology increases, the difficulty to misuse it also increases. Being technologies are not enough to deal with this. So, Blockchain has surfaced as an effective result for solving the security issues related to IoT. To address same security and privacy concerns, a central server concept is eliminated and blockchain (BC) technology is introduce as a part of IoT. This paper elaborates the potential security and privacy issues considering the component interaction in IoT and study how the distributed ledger based blockchain (DL-BC) technology supply to it. Applications of BC with respect to focused sectors and category were clearly considered here. Different challenges specific to IoT and IoT with BC were also discussed to understand blockchain technology.*

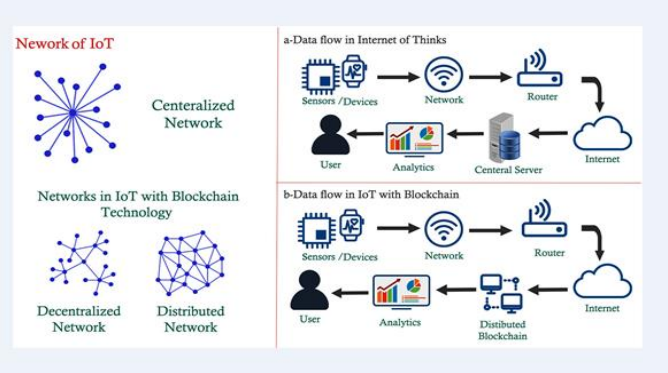
Keywords- IoT, Blockchain, Consensus, WSN

I. INTRODUCTION

Blockchain technology is now attracting a lot of attention. It can revise, optimize the global structure of the technologies linked with each other via the internet.[1] These two areas that are immense to be partial by it are :1)It develops a decentralized system and remove the indulgence of central servers and provides peer-to-peer interaction.2)It creates a total apparent and open to all record, which brings ambiguity to the governance and elections. This tools basically has four essentials.

- **Consensus:** Provides the evidence of work and verify the action in the networks.
- **Ledger :** Provides the entire details of operation within the networks.
- **Cryptography :** Makes sure that all data in ledger and networks gets encrypt and only authorized user can decrypt the information.
- **Smart contract:** It is used to authenticate and validate the participant of the network.

Blockchain offer a scalable and decentralized location to IoT devices, platforms, and its applications. Banks and Financial companies are doing PoC to authorize the blockchain technology.[2]-[3] Apart from financial institutes, a wide range of companies have planned to experience the blockchain's potential. On the other hand, the Internet of Things (IoT) opens up countless opportunities for businesses to run smart operations. Every device about us is now prepared with sensors, transfer the data to the cloud. Thus, connecting these two technologies can make the system proficient.



IoT refers to a insecured coupled system of multiple varied and identical devices which can be sense, process and network .The technologies on which the basics of IoT shows can have a number of bug. These issues should be solved, before implement the technology.

II. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

It is a decentralized database which records every transaction made on a network. It has a ledger distributed over a network of nodes. [4] This network can be public or private. Blockchain allows peer-to-peer transactions, eliminating the need of intermediaries.

Components of a Blockchain

Blockchain mainly has four elements.

1. **Network of Nodes :** All the nodes linked via the internet, maintains all the transactions through blockchain network collaboratively and the validity of a transaction is verified by a set of rules. When a new transaction occurs, its records are updated to the ledger of transaction which is known as 'mining'. Then the rest of the other nodes there on the network, verify the evidence of work.
2. **Distributed database system :** The database is divided into block of information and send to every node of the system. Every block has a file of transactions, a timestamp and the data which links to the previous block.
3. **Shared ledger :** The ledger is made publicly available and is corrupt when updating all the time a transaction happens.
4. **Cryptography :** Data is clear by a crypto mechanism which makes harder for illegal users to accessing or altering it.

Constructing a blockchain

The latest digital transaction is stimulated into a cryptograph protected block. Miners participate with each other to evaluate the transaction and then it is time stamped and are additional to the chain in sequential order. [5]The acceptance of block by nodes are expressed, if a new block is created in the chain, using the hash of the earlier accepted block.

Implementing a Block chain

There are three domains in which block chain can deployed:

1. **Public :** Bitcoin and Ethereum comes under this group. All the node can send or read transaction without requires any authorization. Consensus is open to all public.
2. **Consortium area :** It comes less than limited permission. The permission to read or send may be made public or may be provided only to few authorized nodes.
3. **Private :** Only the organization to whom the network of blockchain belongs can write transaction to it.

III. BLOCK CHAIN BASED INTERNET OF THINGS

Pattern of IoT based on blockchain: having three models.

A. Communication Model:

The three fundamental functions of blockchain network are :

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

Limitations :

1. Slow Processing
2. Small Storage

In this model, blockchain nodes are the members of the network. They can be personal computers, enterprise servers or also cloud- based nodes. Clients are the IoT devices. [6]-[7]Blockchain Clients and nodes interact with each other through APIs. Clients create transactions and these transactions are relayed to nodes for processing and storing the data into the distributed ledger.

Connecting multiple blockchain networks

In future, different Blockchains may serve different purposes. Blockchain network may be a home network, enterprise or the internet. If artificial intelligence is added to the IoT environment that is connected to a blockchain network it creates a Decentralize Autonomous organization that runs without human intervention.

IV. IOT SECURITY WITH BLOCKCHAIN TECHNOLOGY

For a secure application of IoT, the following points are to be considered

1. **Secure communication**

IoT devices have to communicate to exchange data required to process a transaction and to store it in a ledger. Ledgers can also be used to store encryption keys to make the exchanges more confidential. IoT device sends an encrypted message using the public key of the destination device, which is then stored in the blockchain 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.

2. **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. The digital signature work is described below:

- 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.

3. **Discovering legitimate IoT at large scale**

As soon as a new IoT device starts, it asks root servers to give a list of trusted nodes in the network. This device then registers itself in a node, and the exchange of information starts. DNSSec has to be implemented to secure name resolution of root servers by avoiding any spoofing attacks. Every communication made must be authenticated and encrypted efficiently. This can be done based upon:

- Credentials already installed on the device during setup.
- Credentials could be given by the owner of the IoT device.

4. **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 encrypted 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 download the latest and trusted configuration file after every fixed interval of time. 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.

Securing the network of IoT devices 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[8].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.

V. BLOCK CHAIN APPLICATIONS

Block chain have a significant impact across multiple industries:

1. Supply Chain and Logistics
2. Automotive Industry
3. Smart Homes
4. Sharing Economy
5. Pharmacy Industry
6. Agriculture
7. Water Management

1. Supply Chain and Logistics

A global supply chain network involves many stakeholders, such as:

1. Brokers
2. Raw material providers, etc.

It complicates the end-to-end visibility. The supply chain can also extend over months of time and consist of many payments and invoices. Due to the involvement of multiple stakeholders, delivery delays have become the biggest challenge [9]-[12].Therefore, companies are working on making the vehicles IoT-enabled to track the movement throughout the shipment process. Due to the lack of transparency and complications in the current supply chain and logistics, Blockchain and IoT combined can enhance the network's reliability and traceability.

Crisp details about shipments' status can be provided by IoT sensors, like:

1. Motion sensors
2. GPS

3. Temperature sensors
4. Vehicle information
5. Connected devices, etc.

Sensor information is then stored in the blockchain. Once the data is saved on the Blockchain, stakeholders listed in the Smart Contracts get access to the information in real-time. Supply chain participants can accordingly prepare for transshipment and run cross-border transactions.

2. Automotive Industry

Nowadays, digitization is a competitive demand. Automotive industries are using IoT-enabled sensors to develop fully automated vehicles. Connecting Industrial IoT solutions in the automotive sector with the decentralized network enables multiple users to exchange crucial information easily and quickly.

The automotive industry is an exciting blockchain IoT use case, where the combined technology can disrupt:

1. Automated fuel payment
2. Autonomous cars
3. Smart parking
4. Automated traffic control

IoT sensors calculate the parking duration charges, and the billing takes place directly through the crypto-wallet.

3. Smart Homes

Smart IoT-enabled devices play a crucial role in our day-to-day lives. IoT blockchain enables the home security system to be managed remotely from the smart phone.

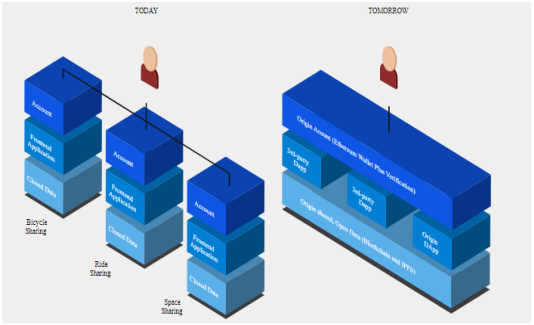
But the traditional centralized approach to exchange information generated by IoT devices lacks the security standards and ownership of data.

Blockchain could elevate the smart home to the next level by:

1. Solving security issues
2. Removing centralized infrastructure

4. Sharing Economy

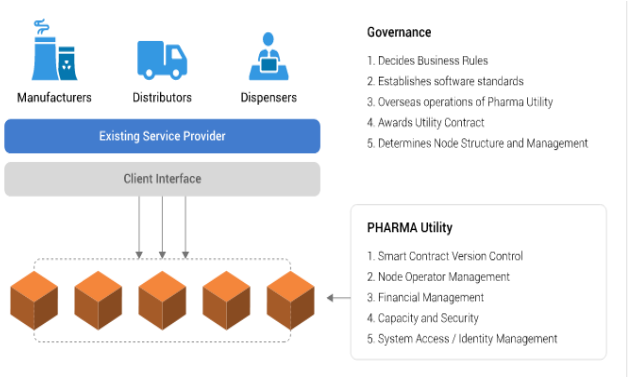
The sharing economy has become a widely adopted concept around the world. Blockchain could help create decentralized, shared economy applications to earn considerable revenue by sharing the goods seamlessly.



5. Pharmacy Industry

The issue of counterfeit medicines in the pharmaceutical sector is increasing with every passing day. The pharmacy industry is responsible for:

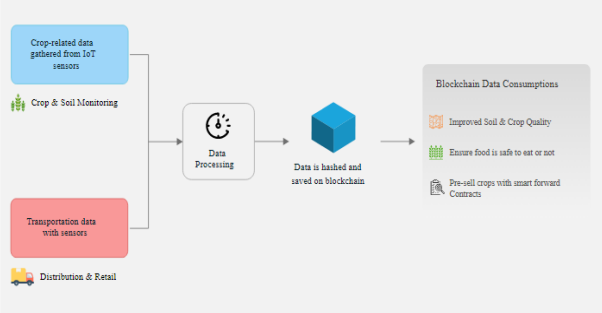
1. Distributing drugs
2. The data stored on the distributed ledger is immutable and timestamped, accessible to:
3. Manufacturers
4. Wholesalers
5. Dispensers
6. End-customers
7. Mediledger is a blockchain based platform, offering:
8. Simplified payment processes
9. Controlling users access
10. Stopping counterfeit drugs from invading the supply chain



6. Agriculture

For maximum customer satisfaction, it is essential to grow more food for the increased population while:

1. Minimizing environmental footprints
2. Ensuring transparency across the supply chain
3. Blockchain, coupled with IoT, has the potential to reshape the food production industry- from farm to grocery to home. Installing IoT sensors in the farms and sending its data directly to the blockchain can help enhance the food supply chain to a greater extent.



7. Water Management

Leaking water fixtures can result in one trillion gallons of wasted water per year in the USA. Aquai has built Puck, a smart water sensor that can:

1. Track how much water you use
2. Automate water shutdown if any leak is detected

VI. CONCLUSION

This paper deals with the various possible security and privacy issues in IoT. These were identified based on the observations in IoT component communication. Blockchain technology as recognized one of the solutions for addressing the issues and challenges in IoT. The scope for blockchain integration with IoT is explained in the paper. Also, the various possible applications of IoT with blockchain technologies were highlighted. As a final, challenges in IoT with blockchain technology are also acknowledged. Hope this paper would give basic idea to understand the need for blockchain in IoT. Advanced Consensus algorithm can be applied to wide range of services in all the fields of engineering. It provides improved flexibility in accessing of the data.

REFERENCES

[1] S. Singh, V. K. Verma, and N. P. Pathak, "Sensors augmentation influence over trust and reputation models realization for dense wireless sensor networks," IEEE Sensors Journal, vol. 15, no. 11, pp. 6248–6254, Nov. 2015, doi:10.1109/JSEN.2015.2448642.

[2] S.Sharma and V. K. Verma, "AIEMLA: artificial intelligence enabled machine learning approach for routing attacks on internet of things," The Journal of Supercomputing, vol. 77, no. 12, pp. 13757–13787, Dec. 2021, doi: 10.1007/s11227-021-03833-1.

[3] O. P. Yadav, "Internet of things (IoT) security issue in wireless sensor network (WSN) with radio frequency identification (RFID)," pp. 1–10, 2018.

[4] V. K. Verma, A. Sharma, K. Ntalianis, and K. Verma, "CTMRS: Catenarian-trim medley routing system for energy balancing in dispensed computing networks," IEEE Transactions on Network Science and Engineering, pp. 1–1, 2022, doi:10.1109/TNSE.2021.3140139.

[5] T. Nimi and P. Samundiswary, "Comparative analysis of ZigBee network with tree and mesh topology for different range of frequencies," in 2017 2nd International Conference on Communication and Electronics Systems (ICCES), Oct. 2017, pp. 560–564, doi: 10.1109/CESYS.2017.8321140.

[6] J. V. Hoof, G. Demiris, and E. J. M. Wouters, Eds., Handbook of smart homes, health care and well-being. Cham: Springer International Publishing, 2020.

[7] H. S. Yeotkar and T. V. Gaikwad, "IoT based human body parameters monitoring by using wearable wireless sensor network," International Research Journal of Engineering and Technology (IRJET), vol. 06, no. 07, pp. 2458–2466, 2019.

[8] A. A. Allahham and M. A. Rahman, "A smart monitoring system for campus using zigBee wireless sensor networks," International Journal of Software Engineering and Computer Systems, vol. 4, no. 1, 2018, doi: 10.15282/ijsecs.4.1.2018.1.0034.

[9] S. Pirbhulal et al., "A novel secure IoT-based smart home automation system using a wireless sensor network,"

Sensors, vol.17, no. 12, p. 69, Dec. 2016, doi: 10.3390/s17010069.

[10] Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey." International Journal of Web and Grid Services 14.4 (2018): 352-375

[11] Alam T, Benaida M. The Role of Cloud-MANET Framework in the Internet of Things (IoT). International Journal of Online Engineering (iJOE). 2018;14(12):97-111. DOI: https://doi.org/10.3991/ijoe.v14i12.8338

[12] Alam, Tanweer. "Fuzzy control based mobility framework for evaluating mobility models in MANET of smart devices." ARPN Journal of Engineering and Applied Sciences 12, no. 15 (2017): 4526-4538