IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Enhanced Security for IoT Devices using Blockchain Smart Contract

Ms. Sayali Parab
Department of Information Technology and Computer Science
Nirmala Memorial Foundation College of Commerce and Science
Mumbai, India

Mr. Chayan Bhattacharjee
Department of Information Technology Chikitsak Samuha's Patkar Varde College
Mumbai, India

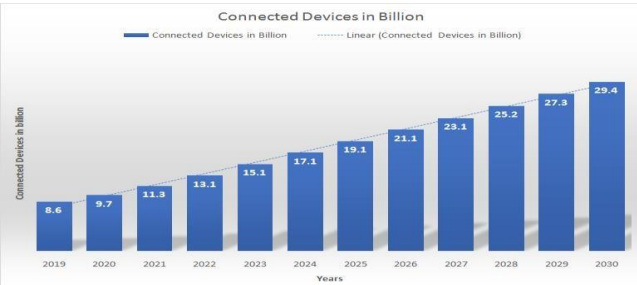
Abstract— Technological and Economical advancement leads to a tremendous boom in the Internet of Things industry which in turn leads to a rise in Smart devices used in various sectors of life. This strategy eventually improves people's lives but also puts their data and privacy at risk. Technological advancement does come at a cost of relinquishing data but this can be rectified by taking some precautionary measures. Blockchain is a technology that works on the basic concept of decentralization and hence proves to be efficient in security mechanisms. Blockchain can provide security support for the Internet of Things system due to its advantages of decentralization and immutability. Therefore, in this paper, any IoT device that is used in the home, industry, farming, etc. based on blockchain is proposed.

Keywords—IoT, internet of things, blockchain, smart devices, smart contracts, security.

I. INTRODUCTION

Smart devices are currently trending and are practically used in day-to-day life by many people across the globe. Smart devices usually refer to any device that can interact through the network and is an important application scenario of the Internet of Things. With continuous technological and Economical advancement, there has been rapid progress in the number of smart devices that are produced which eventually makes the industrial scale and market of smart homes, smart farming systems, etc. expand. Data from Statista shows the total number of Internet of Things (IoT) connected devices worldwide from 2019 (8.6 billion devices) to 2021 (11.3 billion devices) along with the forecasts up to 2030 (29.4 billion devices approx.) (Fig 1.1) [2].

Fig 1.1: Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts to 2030



IoT Technology and its massive popularity have resulted in the massive development of Smart Devices with diversified functions, intelligent products, and humanized services. However, user data security is one of the important criteria that need to be considered and poses a challenge in the development of Smart Devices. Firstly, smart devices become a very easy target for attackers since it collects a large amount of valuable data. Secondly, there is a constant threat to data confidentiality and Integrity following the traditional IoT architecture which include sensors and actuators on the perception layer, routers, and gateways on Network Layer, and cloud server on the Application layer (fig 1.2).

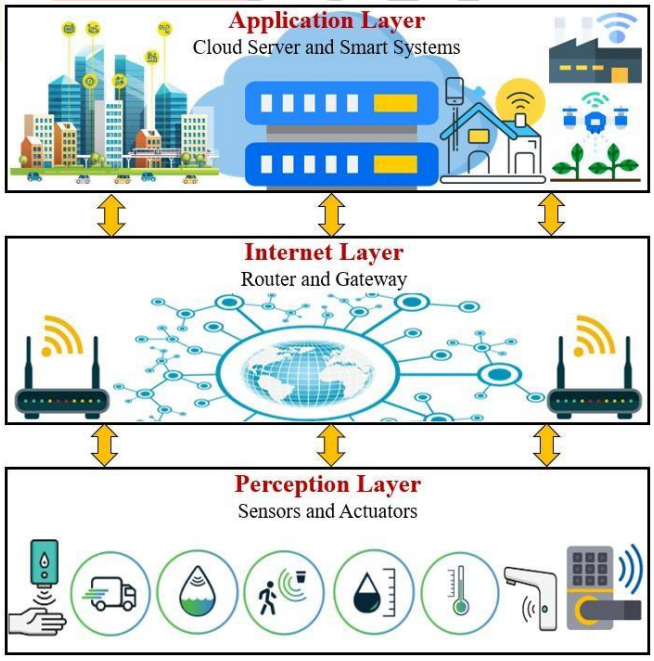


Fig 1.2: Traditional IoT Architecture

Thus, any attack on these layers can be troublesome for the smart device. In addition, most inter-device communication is happening through insecure networks like RFID (Radio-Frequency IDentifier) that uses the technology of NFC (Near Field Communication). Devices such as ceiling fans, windows,

doors, etc. which are made smart are prone to cause property damage and even personal safety.

According to a case study, a hacking happened where hackers, rather than gaining access to the vault of the unnamed establishment, were able to pinch the casino's highroller database after gaining access to its network via the smart thermostat in a fish tank in the lobby [3]. The attackers used the connected thermostat to get a foothold in the network. They then found the high-roller database and then pulled that back across the network, out the thermostat, and up to the cloud.

Blockchain, which was first proposed by Satoshi Nakamoto, is a typical data structure as represented in Fig 1.3. Blockchain includes several advantages such as decentralization, anonymity, non-repudiation, immutability, etc. IoT security can be enhanced in data assurance, trust, and decentralization sectors using blockchain. Integration of blockchain and smart devices has gained popularity and is been implemented on a large scale over the last decade.

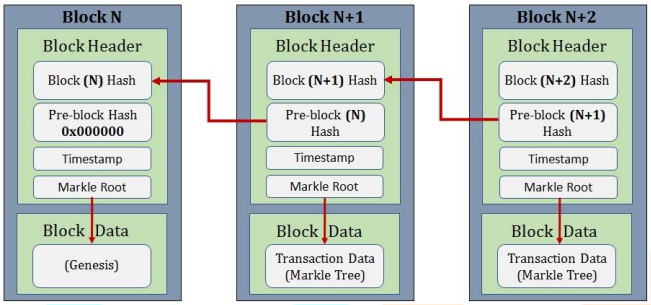


Fig 1.3: Typical Data Structure of Blockchain

II. Background Knowledge and Related Work

A. Blockchain

As the term suggests, Blockchain is a linked structure (chain) of nodes, which are referred to as blocks. It is a mechanism where using a specific type of algorithm, consent is taken from the block to accept or reject a block. These algorithms are known as consensus algorithms. Some of the prominent consensus algorithms include Proof of Work (PoW), Proof of Stake (PoS), Crash Fault Tolerance (CFT), Proof of time, Proof of Elapsed Time, Proof of Activity, Proof of Capacity, etc. PoW gained its popularity with the emergence of bitcoin and on the other hand, PoS was popularized by another cryptocurrency name Ethereum. PoS is the consensus algorithm that uses Solidity Programming to create smart contracts. Along with the likes of cryptocurrencies such as bitcoin, and Ethereum, the blockchain system also has an effective role in the formation of Hyperledger blockchain-based distributed ledger. Hyperledger can also be useful for securing smart devices using smart contracts which are referred to as Chain Code.

Blockchain Systems	Smart Contract	Language	Consensus Algorithm
Bitcoin	No	--	Proof of Work (PoW)
Ethereum	Yes	Solidity	Proof of Stake (PoS)
Hyperledger	Yes	GoLang, C++, etc	Crash Fault Tolerance (CFT)

Fig 2.1: Blockchain System Comparison

B. Smart Contract

Blockchain systems use smart contracts similar to traditional contracts, which are mostly used for legal documentation and in the technological domain and play an important role in the form of SLA (Service Level Agreements). A smart contract is a computer program that facilitates the exchange of money, shares, property, etc. The blocks/peers/nodes agree upon a set of terms and conditions which are the important components of a smart contract. This smart contract, without the need for a central authority, helps verify any anonymous network parties. The smart contracts working fundamentals include Pre-Defined Contracts, Events for which the contract is created, its execution, and the final settlement (fig 2.2).

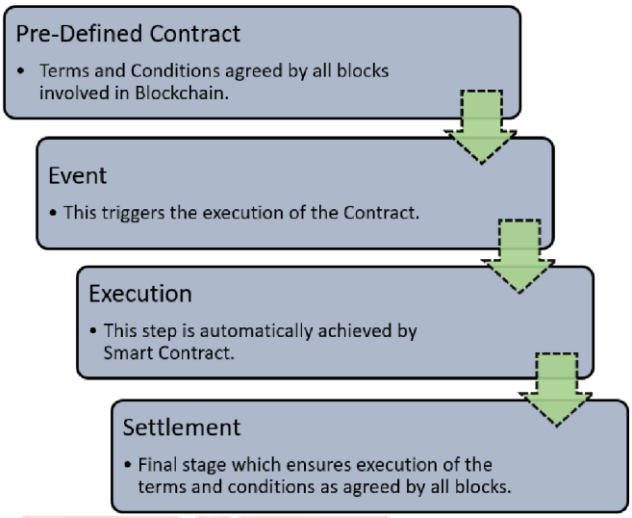


Fig 2.2: Fundamentals of Smart Contract

C. Smart Devices

Devices are often referred any electronic component which takes input signals and correspondingly gives output. In the case of the Internet of Things, where devices are not just any electronic components but also have the capability to connect to the network. These devices understand the simplest of commands used in day-to-day life. Some very common components such as watches, television, air-conditioner, fire sprinkler, etc. can easily be made smart with the simple integration of a controller system in the existing circuit design which brings in the capability to connect to the internet. Devices are getting smarter and so are the mechanisms to secure them hence using a simple implementation of a smart contract, a smart device can be easily secured.

Fig 2.3: Variety of Smart devices

III. Blockchain and Smart Contract-Based IoT System

Smart devices based on smart contracts are expected to be a scenario where all the IoT devices are assumed to be blocks and each one of them can communicate with each other without the intervention of any centralized authority, in this case, the human.

A. Smart contract on smart devices

- Algorithms that can be considered for implementing smart contracts on smart devices will comprise various conditions which initially start with adding the IoT Devices as a block in the blockchain.
- It will then check for various conditional statements which ensure the user's authorization.
- It will also notify the different blocks in the blockchain about unauthorized access.
- To add newer devices as a block, a consensus algorithm can be used to verify the block.
- Thus, a blockchain of IoT devices can be created for a specific sector where different types of devices can be connected and give a holistic environment.

B. Private and Public Blockchain

- IoT devices during their prototype design, determine about it being an open source or closed source hence after the added-on security feature using blockchain, whether it will be used along with public blockchain or should be kept in privation blockchain can be skeptical and may be determined by the organization implementing it.
- Permissionless blockchains that allow anyone to participate in the network are termed "Public Blockchain".
- Permissioned blockchain which is managed by a network manager and a participant who needs consent to join the network is termed as "Private Blockchain".

C. Application scenario

There are several sectors where IoT devices have made a significant impact and helped in the upgradation of their productivity. Some sectors include Residential uses, Industrial uses, Commercial uses, Agricultural uses, etc. Along with smart contract implementation that eventually increases the security and reliability of the system, the devices used in these sectors can be trusted.

IV. Proposed Architecture Principal

The implementation of an IoT environment is possible in simulation models and smart contracts can also be correspondingly created for the same.

A. Smart Home Access

- A traditional smart home system would comprise of motion sensor, Face recognition/biometric scanner, temperature sensor, smoke sensor, gas sensor, camera, light sensor, rain sensor, etc. which are ideally used to ensure that a smart home provides all the amenities and luxuries to the end user to give the best performance. All these sensors and their respective functionalities can be controlled and monitored by a mobile device. (Fig 3.1)
- A smart contract-based smart home system will be a system where conditions can be applied on camera for intrusion detection wherein if an intrusion is detected, along with notifying the user, the system will also notify the other blocks of the blockchain.
- It can also be applied on a gas detector for the detection of gas that can be combustible and subsequently buzz a buzzer but it can also broadcast the same to other IoT devices which are part of the blockchain.
- Thus, an algorithm can be formulated such as:

```
//NO Intrusion Detection  If (Smart
Camera Image == Owner)  then
Access Granted
  Unlock Smart Door

//Intrusion Detection
 If (Smart Camera Image != Owner)
then  Access Denied
 Send Alert Notification to Owner
 Broadcast Alert to other Blocks

//Smoke Detection  If (Smoke /
Flame == True)  then  Buzzer
alarm
 Turn ON sprinkler
 Broadcast Alert to other Blocks

//Grocery Stock Checker
 If (Grocery in Smart Refrigerator is less in stock)  then
 Smart Refrigerator will place an order according to  the
weekly Grocery list  Order invoice will be sent to the
Owner
```

Order Shipment details such as fertilizers and Preservatives used in the item, transportation time, temperature, humidity, Prize, etc. from the Production house to Wearhouse, Wearhouse to Grocery store, and Grocery store to Home will be sent to all the blocks.

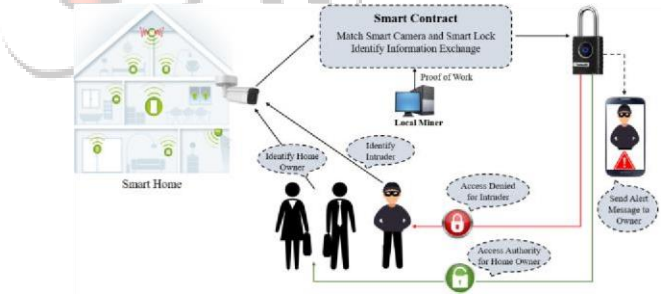


Fig 3.1: Smart Home with Smart Contract Mechanism

B. Smart Farming System

- Although smart devices have been available in farming for some time, merging smart contracts with these devices enhances the quality of food supply chain management and also maintains the confidentiality of farmer and customer data.
- A traditional smart farming system would comprise of soil moisture sensor, nutrient sensor, water level sensor, etc. which on detection of any abnormalities, will notify the user via mobile phone application or in some cases might automatically make the adjustment and convert the levels of those respective components which is suitable. (Fig 3.2)
- Thus, an algorithm can be formulated such as:

```
//Farm Animal detector
```

If (In Crop Section Animal == True) then Close the Smart Door
Turn on Electric fencing
Send notification to Farmer

//Water Level Checker
If(Water level in the soil is less)
then Check Crop type
Check Soil type
Turn on the Irrigation system to provide adequate water
Send notification to all Blocks.
//This information will be helpful to maintain the Irrigation schedule for that specific Crop.

//Bird or other predictor detectors If (In Crop Section Bird or Predator == True) then turn on Ultrasonic electronic repellent
Broadcast Alert Notification to all Blocks

- These devices are silent to humans but generate audible loud noise that scares animals It is highfrequency sound waves that repel wild animals.

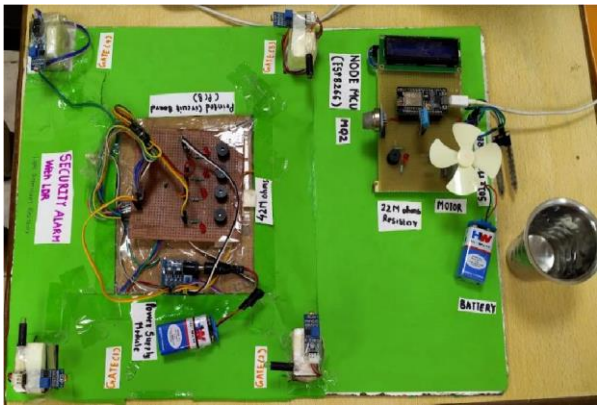


Fig 3.2: Smart Farming Prototype system

CONCLUSION

Smart contracts are beneficial in providing a security mechanism for a decentralized system but in the case of IoT based system, a central node is important. Hence the idea of this research is to bring all these central nodes into a peer-topeer decentralized network of blockchain where they can communicate with each other resulting in the smooth flow of events amongst all the devices.

REFERENCES

[1] Wentai Zhang and Huaizhi Yan 2021 J. Phys.: Conf. Ser. 1971 012049: "A blockchain-based access control scheme for smart home".

[2] Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts to 2030. https://www.statista.com/statistics/1183457/iot-connected-devicesworldwide/

[3] Criminal hacked a fish tank to steal data from a casino .https://www.forbes.com/sites/leemathews/2017/07/27/criminalshacked-a-fish-tank-to-steal-data-from-a-casino/?sh=775590132b96

[4] Nakamoto S. (2008) Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf.

[5] Cui P, Guin U, Skjellum A, and Umphress D. (2019) Blockchain in IoT: current trends, challenges, and future roadmap. *Journal of Hardware and Systems Security 3(4)* p:338-364.

[6] Sreelakshmi K K, Bhatia A and Agrawal A. (2020) Securing IoT applications using blockchain: a survey.

[7] Yiyun Zhou, Meng Han, Liyuan Liu, Yan Wang, Yi Liang, Ling Tian (2018) Improving IoT Services in Smart-Home using Blockchain Smart Contract. IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics.