Review Paper on IoT Devices using Block chain

Mohan Vishal Gupta
College of Computing Sciences and IT,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India

ABSTRACT: ***This was the new technology that emerged in the market block chain started as bitcoin technology but it's uses cases expands very fastly that include finances in many other regions the internet of things, surveillance and so on. Now a day's technology is used both for public and private matter and people are using it in both public and private sector. In addition to this we are also trying to develop such application and hardware IoT facilities are used on large scale so they must communicate with each other and synchronize there are conditions also such as where the thousands of IoT devices are available. Everyone expect the latest services client model to be used when in synchronization and then their drawbacks and different can be used when through we are trying to proper to create an IoT frame work with block chain that can manage IoT devices and change them into block chain key that used free accessible, crypto systems.***

KEYWORDS: ***Block chain, Devices, Ethereum, Key Management, Smart Contract***

INTRODUCTION

Nowadays, we are surrounded by a large number of IoT (Internet of Things) devices and sensors. These devices are designed to make life easier and more comfortable. Block chain technology, especially its mass application, is becoming a term number one. Adoption of block chain into enterprise networks still has a few challenges that need to be tackled. Utilizing block chain can bring increased security and efficiency of network maintenance. The key feature of the block chain, immutability, brings resistance to unauthorized modifications. The whole history of device configuration changes is stored in the block chain, hence recovery after incidents is very straightforward. Internet of Things (IoT) is an object used to connect various devices in a network to get data through the internet that is used in various intelligent applications with the help of embedded systems, sensors, software, and artificial intelligence. IoT can be said to be a major development in the field of information technology. Initially, blockchain technology was used by Satoshi to avoid double spending on a transaction.

The rapid development of IoT led to the emergence of various problems, one of which was the vulnerability to cyber-attacks. One way that can be done to strengthen IoT security is to use blockchain technology. Several studies have been conducted by researchers regarding blockchain technology use on IoT. One of them is research conducted by Oscar Novo where blockchain is used for distributed control access management. There is also research conducted by Singh et al. about using blockchain to secure data on IoT. In a study conducted by Singh et al., it was explained that one of the challenges faced in realizing IoT was in terms of security. However, security on this IoT can be strengthened using blockchain technology. The study also explained that there are four ways to strengthen IoT security, namely using blockchain technology for secure communication, authentication of users, discovering legitimate IoT, and configuring IoT. In that research, there was no implementation and testing of the methods mentioned above. Therefore, this paper will conduct research on implementation and testing from one of the methods to strengthen IoT security to prove the usefulness of blockchain technology for IoT security. This research focuses on making secure communication between IoT devices. The research was carried out by making communication simulations of two IoT devices without and using blockchain technology. The blockchain platform used is Ethereum because the implementation of the smart contract will be used. Then, a simulation of attacks on the two IoT systems was carried out and compared the results of both. In addition, an analysis of the security aspects of the hash function and encryption algorithm used is also carried out, namely avalanche effect.

This paper extends our previous studies. We are introducing an improved architecture for management and monitoring of IoT devices using a private block chain. Many people bet or speculated on Bitcoin since Bitcoin appeared in 2008. While the market, philosophical, and Bitcoin itself not all these revolutions may be of technical interest without blockchain possible, distributed ledger is a Bitcoin's pivotal part. After Bitcoin's success, several more cryptocurrencies that apparently are designed above appeared in technology blockchain. Not just disaster, but also adapting blockchain is another area. And Bitcoin, too[1]. It has some limits, has been a huge success first and foremost, the time of block generation is about 10 minutes and transactions take relatively slow to produce. Secondly, it can be preserved tracking UTXO

(Unspent Transaction) transactions it cannot use loops outputs) and support scripting. In it's not complete, in other words, Turing. In mind constraints, Ethereum is playing. for Ethereum it makes developers about 12 second block intervals write an intelligent contract. We may set up IoT devices with Ethereum. To authenticate, control public key infrastructure. The way ethereum may be used for computers to upgrade their behavior. As many realms are adapting to the IoT since the IoT era began.

Locations that involve more than 100 devices related as factories try to use these application technologies. However, there are a few concerns. First of all, provided they are interconnected over hundreds of computers, both systems must be synchronized. Secondly, almost as if the server is vulnerable, any server-client model devices are in difficulties depending on. Using blockchain, but IoT devices can sync with other devices easily on IoT due to the ledger circulated. Using the consensus, too. It is difficult to fake blockchain or algorithm data perform denial of service attack (DOS) unless innate problems like OPCODE problem so we offer the use of Ethereum for IoT devices management. We can write a code using the intelligent Ethereum contract that sets IoT system behavior. Will have access to the public smart contract primary facilities for such malicious assailants. The management system at Ethereum cannot be managed. We start a principle proof that includes the beginning few Raspberry Pi and smartphone IoT devices are available. Once upon a time we're finishing the blueprint, we want to develop an absolutely ethereum system of IoT.

DISCUSSION

Block chain used in IoT:

Block chain can be used to track the sensor data measurements and prevent duplication with any other malicious data. Deployments of IoT devices can be complex, and a distributed ledger is well suited to provide IoT device identification, authentication and seamless secure data transfer.

Managing IoT Devices using Ethereum:

In this segment we deliver a rich-thin-client IoT approach based on the Ethereum blockchain. To address the above dilemma between minimal IoT system capital and unified architecture issues, we built an extensive customer architecture. The customers who communicate with users and gather IoT data can be treated as IoT devices with minimal resources; the customers are rich, Thin customers and total blockchain nodes can be known as devices have greater or equivalent resources than personal computers. We use an Ethereum private blockchain network as our underlying blockchain framework[2]. Not at all. It only supports intelligent contracts from which we can build reasonably complex interactions between various IoT devices, human and computer users, however even because the new block can be produced more rapidly than Bitcoin. We Often used the original method of consensus: PoW, and original method of encryption: Ethereum account[3].

A. Ethereum:

Ethereum is a public, suggested by Vatalik Buterin in 2013 distributed computing framework focused on blockchain. In comparison to previous Bitcoin blockchains, it can act as a machine amid the slowdown in efficiency of many existing PCs since it has an approximate transaction time of twelve sec. However, it has a language like its own soundness or Snake. It can write and compile a developer programme. It will function on Ethereum Virtual until compiled Motor. Much like anywhere else in the world, compiled code is converted into opcode until it's compiled and then binary, which is running in the Virtual Machine world of Ethereum. Therefore, Ethereum is specially combined with the cryptocurrency operating framework it's there. History since it provides developers with versatility to write a blockchain app that will run. It's going to be hard to hack or manipulate code, users. whoever depends on the written code is almost assured to comply as you foresee to.

B. Ethereum Model:

Unlike server-client architecture, Ethereum is a distributed computing network, which means all of contain pieces of blockchain from interested organisations etheria seems like a server client. The real model looks different in a way for simplicity; each blockchain contributing party requires a partial or full

blockchain. Rather than email to a computer, each transaction upgrade or render system involves ethericity.

C. Smart Contract:

One of Ethereum's most critical things is intelligent contract. The first definition that Nick Szabo developed the intelligent contract brought blockchain creativity. Ethereum uses an intelligent contract over the blockchain to on blockchain, developers can write a programme. That is to say, we can use Ethereum as a machine by means of a smart contract platform. Program languages like Solidity are available, ethereum Hydra, and LLL solidity is at this stage language and parser most frequently used. It's that high level language is compiled into byte codes until the language has been created. And byte codes on Ethereum have been deployed. Since byte codes are just a list of opcodes follow the codes as soon as you have the necessary instructions. True account contract is executed.

Key Management:

As all these arrangements are signed at Ethereum, IoT appliances like air conditioners or lamps should be supplied to recover both metre and regulation contract prices. On metre contract values they verify whether inputs are valid with a signature and public key. In reality, we are using the mobile and metre RSA algorithm the locked keys both with respect to the principles of political contracts check even if public key and signature inputs are correct. If the case in which the utilization of force exceeds policy regularly accumulating values, machines simply turn to energy mode to save. While Ethereum can be used. Reports as an infrastructure of public interest because they are focused on ECDSA, owing to fine granularity, we plan to use our own.

On Ethereum we have introduced intelligent contracts. Once upon a time, we began supplying inputs after encoding, deployed contracts. Once we change / report values successfully ethereum, we may find Ethereum values we find that others are in the process of growing ethereum block chain's vulnerabilities. Although first of all, it has approximately a 12 second transaction period, it is still not fast sufficient for those realms. It can be time-sensitive and hard to use technology such as this. Secondly, since light at this point, Ethereum Client is not sponsored either, you need a proxy or a big shop to save the whole the free Shuttle.

CONCLUSION

In this paper, we propose a way to manage IoT devices using Ethereum, block chain computing platform. We write smart contracts to save data coming from meter and smart phone. Using Ethereum account, meter constantly sends electricity use and smart phone sends policies for air conditioner and light bulb. And air conditioner and lightbulb constantly checks the values on Ethereum to update their devices. When necessary, they switch their mode from normal to energy-saving. As proof of concept, we are starting with small number of devices. Since we found that it is feasible to build such a system, in further studies, we would like to build fully-scaled IoT system which contains multiple of devices. With the start of this experiment, we hope to see improvements on IoT where users of the technology do not need to worry about synchronization and denial of service attacks while serving them efficiently and fast.

REFERENCES

[1] R. C. Pandey, M. Verma, and L. K. Sahu, "Internet of Things (IOT) Based Gas Leakage Monitoring and Alerting System with MQ-2 Sensor," *International Journal of Engineering Development and Research*, 2017.

[2] P. F. Martín Serrano, Payam Barnaghi, Francois Carrez Philippe Cousin, Ovidiu Vermesan, "IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps," *EUROPEAN RESEARCH CLUSTER ON THE INTERNET OF THINGS*, 2015.

[3] A. K. S. S. R. Giri, "Block Chain for Securing Internet of Things," *International Journal of Science and Research (IJSR)*, 2017.