Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 8 (2017) pp. 2449-2456

http://www.ripublication.com

A Review on Blockchain Application for Decentralized Decision of Ownership of IoT Devices

Poonam Ghuli*, Urvashi Priyam Kumar* and Rajashree Shettar*

** Departement of Computer Science and Engineering, R.V. College of Engineering, Bengaluru, India.*

Abstract

This paper describes a unique method for peer to peer identification of ownership of IoT devices in a cloud environment. The described methodology consists of device being added by it's manufacturer (also referred to as Genesis) & then being transferred to a user based on blockchain technology. This paper also introduces how similar blockchain mechanism can be used for the transfer of ownership of a device from one user to another, without the involvement of any third party and the benefits of using the same whereas serial K-means++ achieves 85-89% accuracy for same sampled dataset.

Keywords: Blockchain, Internet of Things(IoT), Peer to Peer, /cloud computing.

1. INTRODUCTION

Blockchain is a distributed, publicly available ledger for all transactions (digital events) that were executed & processed between two clients. The decentralized nature is possible as each transaction is verified through a consensus of a majority of the clients participating in the entire system. Blockchain, is a readonly ledger, where once entered information can never be erased, this also ensures that each transaction present in a blockchain was verified and accepted as a valid transaction by a majority of clients involved at that period of time. The public availability, decentralized and readonly nature of blockchain makes it mathematically impossible to create a fraudulent transaction and get it added to a blockchain, making it a safe, secure and reliable method to store and execute transactions, without the involvement of any third party.

Bitcoin is one of the first and most popular application of blockchain technology, which has resulted in creation of a huge global market of anonymous transactions which is unregulated and outside of any government control. This in turn is quite controversial and often warrants for a large number of governmental and regulatory reforms to keep such unregulated financial markets in check. Where, Bitcoin has been considered as hugely controversial, the underlying blockchain technology has already been adopted and applied in a variety of areas. One such potential area is the world of IoT. This paper utilizes the blockchain technology to propose a system, where, the ownership of IoT devices and the transfer of same, can be executed in a decentralized way.

However, Blockchain technology is currently being successfully applied to both financial markets as well as quite a few non-financial applications. Since the adevent of blockchain many researchers have considered the distributed peer to peer model for blockchain as an invention comparable to steam engine or the internet, having the capability to completely alter the world of commerce and beyond [3].

The Internet of Things, also considered as the next major paradigm shift since advent of Smart Phones, is another area which has found a remarkable number of applications of blockchain. IoT being an emerging topic of social, economic & technical significance, includes a wide variety of Consumer products, goods, verhicles, industrial components, sensors and other daily use objects which after being combined with the Internet and the powerful data consuming and analytics tools are going to transform the way all of us live, work or play.

However, on the other hand, the advent of IoT into lives of a large number of people has raised significant and important challenges that could stand in the way of achieving the true potential of the IoT world [5]. One of the major challenges is defining ownership of IoT devices with respect to the User who uses them. This paper proposes a de-centralized system, to register and assign an IoT device to an owner. This system primarily based on blockchain and its decentralized nature focuses on developing a new system which assigns any IoT device to an owner and can also be utilized by the current owner in turn to transfer the ownership to any other user.

2. BLOCKCHAIN and BITCON

In the current scenario, all Internet transactions have a mediator or a trusted party who verifies and processes any electronic transaction. Their role is to safeguard, validate and store transactions. To avoid fraudulent transactions the third parties puts in many resources, which in turn results in high transaction costs.

2.1 How does it work

For two willing parties to conduct any transaction over the internet a cryptographic proof is provided by each one. Instead of trusting a third party, Bitcoin uses cryptography and certificates to sign each request sent by any party. Each party has a set of "public key" and a "private key". A public key as the name explains, is publically available and can be viewed by anyone, whereas a private key is meant to be secured by the client and not shared with anyone. In order to perform a tansaction the owner of bitcoin needs to provide a proof of ownership of the "private key". For this purposes digital signatures are used. Any transaction is signed using a hash between the private key and the transaction id. This hash if re-hashed with the public key, will give back the correct transaction id. This way any other client can verify the proof of ownership of the "private key" of any client as shown in figure 1.

Due to this peer to peer communication for any transaction to succeed, information about each transaction is transmitted to every node in the network and is recorded publically in an immutable ledger, which is known as blockchain. Each and every is transaction is verified for validity by a consensus of a majority of nodes before recording it into the blockchain ledger. Two major things need to be taken care of by the verifying nodes are as follows:

- Verification of digital signature of sender – Sender owns the private key for that bitcoin
- Spender has sufficient balance in his/her account to spend the amount: As Blockchain maintains history, this makes it easier, as every single transaction is compared.

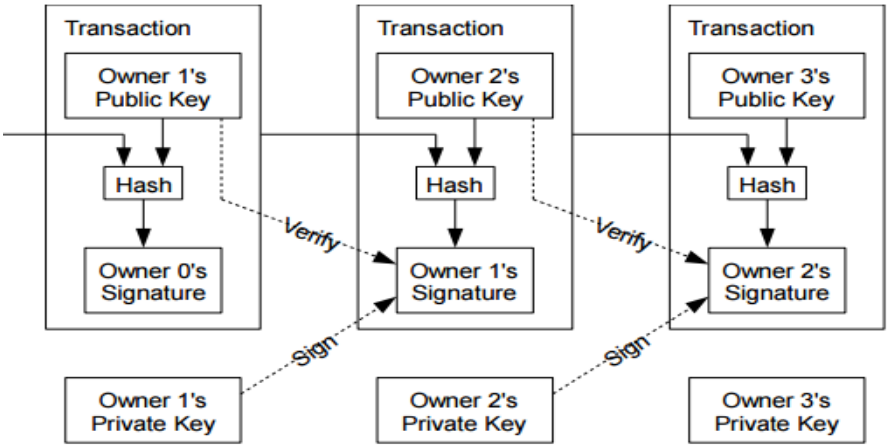

Figure 1 Transaction Flow between two Parties

2.2 Why Blockchain is Required

For any financial/transactional system to work, proper ordering of transactions is essential. As it prevents double spending as well as fraudulent transactions. As blockchain is a decentralized ledger, each transaction reaches a node at different points in time. The ordering of these transactions happens by grouping transactions happening over a certain time range in groups known as "blocks". Each block is linked to the previous one in the list, thus forming a chain like data structure, referred to as Block Chain.

One of the major problems to be handled for this type of addition of blocks is to maintain the order in which the blocks are added. Any node in the blockchain can collect fraudulent transactions and add them into a block. For instance, a faulty node creates a block with unverified transactions and then starts broadcasting them to the entire network. How does the entire network decide which block to add next in the blockchain. Due to difference in receipt time, at different points in the network, using a first come approach would become useless.

Blockchain solves this problem by introducing a proof of work concept: Each block will be accepted in the blockchain only when the owner of that block gives a proof of work being done [1, 3]. For instance, any node generating a block needs to give a solution for a specialized mathematical problem, which will require some usage of computing resources by the node. One such example is where; a client is required to find a "nonce" or a unique value, which when hashed with transaction ids and previous hash of block produces a hash with a certain fixed number of leading zeroes as shown in figure 2. The only way to solve this problem is through hit and trial method, which requires exponential time complexity, whereas verifying the result for it would require only one-step of computation, which would require only single hash to be computed [7].

Because of proof of work that needs to be done by all the nodes in order to add a block, it becomes mathematically impossible for fraudulent nodes to add blocks in the correct blockchain. For a fraudulent node to introduce an unverified transaction, it needs to mathematically race against the good nodes to generate all subsequent blocks in the correct order, which are being added, in parallel, by good nodes.

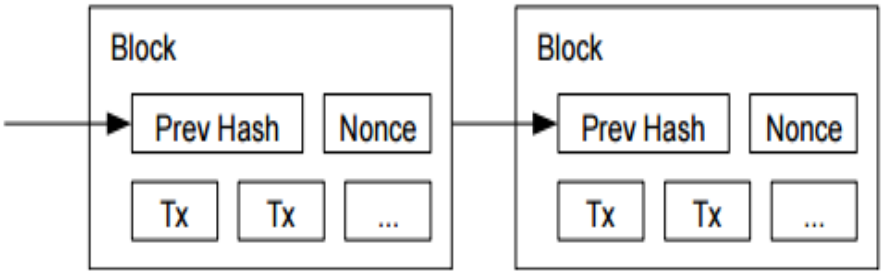

Figure 2 Proof of Work to Mitigate Double Spending

This is only possible, when the bad nodes are present in majority and are coordinating with each other, with millions of nodes in the network which is almost a impossibile task in reality.

3. DE-CENTRALIZED REGISTRATION & IDENTIFICATION SYSTEM

The subsequent section describes describes how to use a blockchain based system and apply it in de-centralized registration of IoT devices. The subsequent part of this section is organized as follows:

- First section provides description of various terminologies being used by the used by the proposed system
- Second section describes about the methodology being used and how it fits for the proposed problem.
- Lastly, use cases are discussed for the aforementioned system and compare it with existing systems, listing pros and cons of both

Firstly, this section introduces a Certificate Issuing Authority (CIA), this is an application or a node which can issue certificates(a set of public key and private key) to any requesting entity. The Certificate Issuing Authority, can also provide verification of a digital signature using the signing authority's public key. The verification is done using ECDSA (elliptic curve digital signature algorithm) [2, 4, 6], where when a certificate is requested, CIA service creates a pair of public key and private key, maintains the public key in a publically available storage while transferring the private key to the node, to be stored and kept securely. This allows the user and only the owner of the device to send digitally signed requests to the IoT device. These requests can be verified against the public key stored by the CIA. This mechanism, thus, serves as a source of peer-to-peer authentication. Where, CIA is nothing but a single-sign-on web portal that can be accessed by any app and is not owned by any single entity, similar to the DNS servers are used in the current day world wide web.

Here, the various players involved in this system are discussed. First of all, manufacturing unit or the organization which manufactures the IoT devices is introduced. These organizations are an equivalent of "miners" in a bitcoin world. As a miner the manufacturing companies dedicate resources towards increasing the security of the block chain and validating transaction blocks for correctness. In turn the participating miners in this system, get incentives by getting a privilege of creating genesis blocks for new devices. That is, every manufacturer has the right to add new devices / release new devices to the block chain. As the rate of addition of new devices to the blockchain is a time of consuming process, posed due to proof of work situation described in section 2, the more resources some miner applies the faster the

rate of addition for its devices. This also introduces competition between two miners (two IoT manufacturers).

Finally, a user is identified who is on the consumer end for these IoT devices. The user is the person who buys an IoT device from the manufacturers or miners. The user/owner of the device also holds control over the ownership of the device and can transfer it to any other user through this system.

3.1 Genesis

By convention, the first transaction in a block is a special transaction that adds a new device to the current system owned by the miner who created the block. That is, the manufacturer before bringing a particular device to the market needs to create a block entry for that device. For this purpose, the manufacturer first contacts the Certificate Issuing Authority (CIA) to get a private & public key pair assigned to the device. Then the id for that device is added to the front of a block added to the blockchain. This device addition is then propagated and verified at various nodes, in the end, getting the device added with the owner as the miner itself.

In order for the miner to add devices at a much faster rate, the miner has to apply more number of resources, thus, supporting the security of block chain in turn. The relationship, between the blockchain and the miner can also be seen as a symbiotic relationship in which action of one supports another.

3.2 Registeration of Ownership

To become the owner of an IoT device the user first makes a physical payment to the IoT manufacturer, in turn, for the physical device. Prior to transferring the physical device, either the IoT manufacturer or the User itself contacts the CIA to get a set of public/private key. Where, the public key is retained in the CIA itself and the private key is transferred to the user.

Now, using its own private key the IoT manufacturer initiates a digitally signed transfer to the user. This transfer is verified by other nodes in the block chain and gets added to the block chain. Once added, the user becomes the owner of the IoT device. To communicate with the device, the user sends a digitally signed request to the device. To verify the origin of the request, the device first contacts the CIA to verify the signature through user's public key, if valid, the device then processes the request. This way the user can use any supported protocol and third party app to contact the device, thus being independent of the intermediate manufacturer.

3.3 Transfer of Ownership

In this system any user can independently transfer the ownership of one device to another user. First the receiving user needs to have a private key and public key registered with the CIA. After which, the transfer of one user to another user happens like a normal blockchain transaction as described previously. This reduces the dependency on a central cloud to change the ownership for a particular device.

3.4 Advantages over Current Scenario

- In the current scenario of ownership identification, the user is signed up to the device with the help of an intermediate cloud or a centralized authority. For this purpose, each manufacturing organization has its own cloud to facilitate sign up and owner identification process. This system removes the presence of centralized authority or cloud, for sign up process, making the registration process de-centralized. As there is no central cloud the identification of its owner by the IoT device becomes completely de-centralized.
- In the current IoT scenario interoperability between devices of different manufacturers is a huge problem. The system proposed eliminates the presence of any central cloud, thus making interoperability far more convenient. A user who is owner of a device can easily control the device just by providing their private key to any 3rd party app, for signing the request. Hence, this system reduces dependency of any cloud and further strengthens the principal of interoperability on which IoT is based.
- In the current scenario, to communicate with your device securely, the user has to depend on a 3rd party cloud or manufacturer's cloud. This can result in compromising of secure user data and privacy. The proposed system is completely secure, in which, the user data is only shared with the device and no intermediary.

4. CONCLUSION

Blockchain being first of kind completely decentralized collection of transactions, finds its application in a large number of financial & non-financial fields. Although, recently it has gained popularity among scientists, it should not be considered a perfect solution for all the issues. As with any present day technology there are a few drawbacks of using blockchain, in terms of computation resource wastage, more storage requirement at each node level, but all these problems are minor and easily solvable. The system defined in this paper is fairly secure to all kinds of malicious attack as relies on the strength of consensus of good nodes to work successfully.

Before implementing a similar system the issues with blockchain should be considered and their solutions incorporated in the implementation. As IoT environment further rises and users becomes more techno and internet centric, a better form of registration & authentication process is necessary. Blockchain technology and it's close relationship with modern day cryptography provides better forms of authentication & registration process than the contemporary solutions. Blockchain therefore provides a great alternative towards modern day authentication and interaction between devices.

REFERENCES

[1] Satoshi Nakamato, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf. (*references*)

[2] Ali Dorri, Salil S. Kanhere, Raja Jurdak and Praveen Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home".

[3] Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman. "BlockChain Technology : Beyond Bitcoin"

[4] Ben Cresitello-Dittmar, "Application of the Blockchain For Authentication and Verification of Identity".

[5] The Internet Of Things, An Overview, ISOC-2015

[6] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980

[7] W. Feller, "An introduction to probability theory and its applications," 1957.