ACADEMICIA: An International Multidisciplinary Research Journal
ISSN: 2249-7137 Vol. 11, Issue 12, December 2021 SJIF 2021 = 7.492
A peer reviewed journal

A STUDY OF BLOCKCHAIN APPLICATION FOR DECENTRALIZED IOT DEVICE OWNERSHIP

Gulista Khan*

*Associate Professor,
Department of Computer Science, Faculty of Engineering,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, INDIA
Email id: gulista.engineering@gmail.com

DOI: 10.5958/2249-7137.2021.02627.6

ABSTRACT

Blockchain is a decentralized, publicly accessible ledger that records all transactions, both financial and non-financial. The Internet of Things (IoT) is also thought to be the next big thing. The techniques for peer-to-peer identification of ownership of IoT devices in a cloud context are discussed in this paper. The review paper goes over how a device is installed by its maker (also known as Genesis) and then transmitted to a user via blockchain technology. This paper also looks at how a similar blockchain method may be used to transfer device ownership from one user to another without the need for a third party. Because it depends on the strength of consensus of good nodes to operate effectively, the methods discussed in this paper are reasonably safe against all types of malicious attacks. Blockchain offers a fantastic alternative to modern-day authentication and device interaction.

KEYWORDS: *Blockchain, Decentralized, Device, IoT, Transactions.*

1. INTRODUCTION

Blockchain is a decentralized, publicly accessible ledger that records all transactions (digital events) between two clients. Because each transaction is confirmed by a majority of the clients participating in the system, the decentralized nature is feasible. Blockchain is a read-only ledger in which information recorded once cannot be deleted[1]. This guarantees that each transaction in a blockchain has been validated and approved as a legitimate transaction by the majority of clients engaged at the time. Because of blockchain's public availability, decentralized nature, and read-only nature, it is mathematically impossible to create a fraudulent transaction and have it added to the blockchain, making it a safe, secure, and reliable method of storing and executing transactions without the involvement of a third party. Bitcoin is one of the earliest and most widely used applications of blockchain technology, resulting in the development of a massive worldwide market for anonymous transactions that is unregulated and unaffected by government intervention[2]. This is very contentious, and it often necessitates a slew of political and regulatory changes to rein in such uncontrolled financial markets. Whereas Bitcoin has been seen as very contentious, the blockchain technology that underpins it has already been accepted and used in a number of fields. The Internet of Things (IoT) is one such promising sector. This paper uses blockchain technology to suggest a method in which IoT device ownership and transfer may be carried out in a decentralized manner.

However, Blockchain technology is now being effectively used to a variety of non-financial applications as well as financial markets. Many academics have seen blockchain's distributed peer-to-peer architecture as an innovation on par with the steam engine or the internet, with the potential to radically transform the world of business and beyond[3].

Another area where blockchain has found a surprising number of applications is the Internet of Things, often known as the next big paradigm change after the introduction of smart phones. The Internet of Things (IoT) is an emerging topic of social, economic, and technical significance that encompasses a wide range of consumer products, goods, vehicles, industrial components, sensors, and other everyday objects that, when combined with the Internet and powerful data consuming and analytics tools, will transform the way we all live, work, and play. On the other side, the introduction of IoT into the lives of a huge number of people has created major and critical difficulties that may prevent the IoT world from realizing its full potential. One of the most difficult tasks is determining who owns IoT devices in relation to the users who utilize them. The purpose of this paper is to provide a decentralized method for registering and assigning an IoT device to an owner. This system, which is mainly built on blockchain and its decentralized nature, aims to create a new system that assigns every IoT device to an owner and allows the existing owner to transfer ownership to any other user.

1.1. Blockchain and Bitcoin:

All Internet transactions now have a mediator or trusted party that validates and executes any electronic transaction[4]. They are in charge of securing, validating, and storing transactions. Third parties invest a lot of effort to prevent fraudulent transactions, which results in high transaction costs.

1.2. How does it Work:

A cryptographic proof is given by each willing party in order for two willing parties to execute any transaction via the internet. Bitcoin utilizes encryption and certificates to sign each request made by any participant, rather than relying on a third party. Each side has a “public key” and a “private key” for communication. A public key, as its name implies, is open to the public and may be seen by anybody, while a private key is intended to be kept private by the client and not shared with anyone. The owner of bitcoin must show evidence of possession of the “private key” in order to complete a transaction. Digital signatures are employed for this purpose. A hash between the private key and the transaction id is used to sign any transaction. If you re-hash this hash using the public key, you'll get the proper transaction id. As illustrated in Figure 1, every other client may verify the evidence of possession of any client's “private key.”

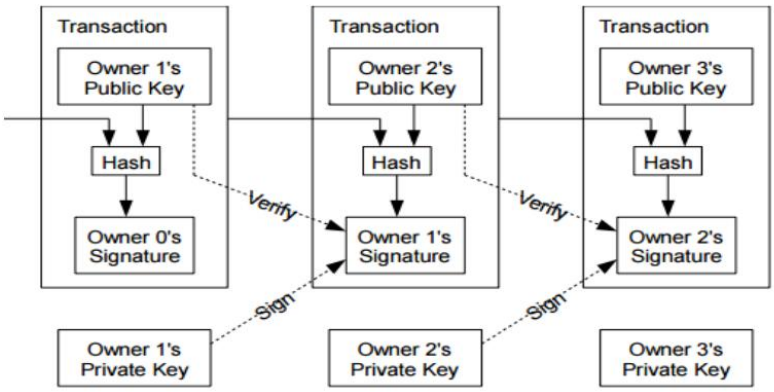

Figure 1: Transaction Flow between two Parties[5]

1.3. Why Blockchain is Required:

The correct sequencing of transactions is necessary for any financial/transactional system to function. Due to the fact that it prohibits both duplicate spending and fraudulent transactions. Each transaction reaches a node at a distinct moment in time since blockchain is a decentralized ledger. The sorting of these transactions is accomplished by grouping transactions that occur during a certain time period into "blocks." Each block in the list is connected to the one before it, creating a chain-like data structure known as Block Chain. Maintaining the order in which the blocks are added is one of the most difficult issues to solve for this kind of block addition. Fraudulent transactions may be collected and added to a block by any node on the blockchain. A malfunctioning node, for example, may generate a block of unconfirmed transactions and then broadcast them to the whole network. How does the blockchain's whole network select which block to add next? A first-come-first-served strategy would be ineffective due to differences in reception time at various locations in the network.

Blockchain addresses this issue by adding the notion of proof of work: Only when the owner of a block provides proof of work will that block be allowed into the blockchain. Any node producing a block, for example, must provide a solution to a specific mathematical problem, which will need the node's use of computer resources. One example is when a client must discover a "once" or unique value that, when hashed with transaction ids and the preceding hash of the block, generates a hash with a specified amount of leading zeroes, as illustrated in figure 2. The only option to address this issue is to use the hit-and-trial technique, which has exponential time complexity, while validating the result would only take one step of calculation and just one hash to calculate.

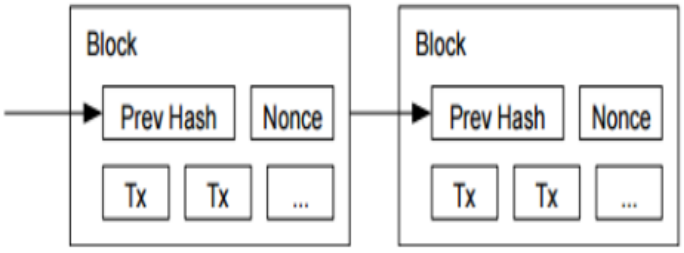

Figure 2: Proof of Work to Mitigate Double Spending[6]

Because all nodes must do proof of work before adding a block, it is theoretically impossible for fraudulent nodes to contribute blocks to the proper blockchain. To introduce an unverified transaction, a fraudulent node must mathematically race against good nodes to produce all future blocks in the proper sequence, which are being added by good nodes in parallel. This is only feasible when the bad nodes are in the majority and are coordinating with one another, which is almost impossible to achieve with millions of nodes in the network.

2. LITERATURE REVIEW

Dorri et al. go into more detail and describe the different basic components and functionalities of the smart home layer in their paper[7]. Each smart home is outfitted with a'miner,' an always-on, high-resource device that is in charge of all communication both inside and outside the house. A private and secure BC is also kept by the miner for regulating and auditing communications. They demonstrate the security of their proposed BC-based smart home system by carefully analyzing it in terms of the basic security objectives of confidentiality, integrity, and availability. Finally, they provide simulation results to show that the overheads imposed by their method are negligible in comparison to the security and privacy benefits it provides. The capacity to protect data and authenticate the identity of users of a service, according to Cresitello, is the most significant barrier to moving many services online[8]. The use of a password or, in rare cases, dual-factor authentication is used for online authentication. The issue with these techniques is that passwords are notoriously insecure, and dual-factor authentication often involves transmitting a code by SMS or a third-party service. The blockchain may be a solution to this issue. The ledger for a $10 billion USD currency is managed via the blockchain. Authentication, on the other hand, may use the same cryptographic techniques. Blockchain authentication prevents someone from intentionally changing a ledger by spreading it across all network users.

Fernández et al. conduct a comprehensive study of how to adapt blockchain to the particular requirements of IoT in order to create Blockchain-based IoT (BIoT) applications[9]. The most important BIoT applications are presented after the fundamentals of blockchain are explained, with the goal of highlighting how blockchain may affect conventional cloud-based IoT applications. The present difficulties and potential improvements for various areas of the design, development, and deployment of a BIoT application are then discussed. Finally, some suggestions are made in order to guide future BIoT researchers and developers through some of the problems that must be addressed before the next generation of BIoT applications can be deployed.

3. DISCUSSION

3.1. De-Centralized Registration & Identification System:

First, a Certificate Issuing Authority (CIA) is introduced in this section. A CIA is an application or a node that may issue certificates (a set of public and private keys) to any asking organization[10]. The Certificate Issuing Authority may also verify a digital signature using the public key of the signing authority. When a certificate is requested, the CIA service generates a pair of public and private keys, keeps the public key in a publicly accessible storage location, and transfers the private key to the node to be saved and maintained securely. This enables the user to submit digitally signed requests to the IoT device, and only the user and only the owner of the device may do so. These queries may be cross-checked against the CIA's public key. As a result,

this method may be used for peer-to-peer authentication. Whereas, CIA is nothing more than a single-sign-on web gateway that can be used by any program and is not controlled by any one organization, similar to how DNS servers are used today on the internet.

The different actors in the system are discussed in this section. First and foremost, the manufacturing unit or organization that produces IoT devices is discussed. In the realm of bitcoin, these companies are the equivalent of "miners." Manufacturing firms devote resources to improving the block chain's security and verifying transaction blocks for accuracy as miners. In turn, miners that participate in this system are rewarded with the ability to create genesis blocks for new devices. That is, every manufacturer has the ability to add new devices to the block chain and distribute them. Because adding new devices to the blockchain is a time-consuming operation owing to the proof-of-work scenario, the more resources a miner uses, the quicker its devices are added to the network. This also creates a rivalry between two miners (two IoT manufacturers). Finally, a user on the consumer end of these IoT devices is identified. A user is someone who purchases an IoT gadget from a manufacturer or a miner. The device's user/owner also has control over the device's ownership and may transfer it to any other user via this mechanism.

3.1.1. Genesis:

According to tradition, the first transaction in a block is a special transaction that adds a new device to the miner's current system. That is, before releasing a gadget to the market, the manufacturer must establish a block entry for that item. The maker must first contact the Certificate Issuing Authority (CIA) to get a private and public key pair for the device. The device's id is then put to the front of a block that is uploaded to the blockchain. This device addition is then propagated and confirmed over several nodes, resulting in the device being added with the miner as the owner. The miner must use a greater amount of resources in order to install devices at a quicker pace, thus supporting the security of the block chain. The connection between the blockchain and the miner may also be thought of as a symbiotic one, in which one's actions benefit the other.

3.1.2. Registration of Ownership:

In order to become the owner of an IoT device, the user must first make a physical payment to the IoT maker. Either the IoT maker or the User contacts the CIA to get a set of public/private keys before transferring the physical device. Where the public key is kept by the CIA and the private key is sent on to the user. The IoT manufacturer now starts a digitally signed transmission to the user using its own private key. Other nodes in the block chain verify this transfer, and it is added to the chain. The user becomes the owner of the IoT device once it is added. The user sends a digitally signed request to the gadget in order to interact with it. To confirm the request's origin, the device first calls the CIA to verify the signature using the user's public key; if the signature is valid, the device executes the request. As a result, the user may communicate with the gadget using any compatible protocol and third-party software, making them independent of the intermediary manufacturer.

3.1.3. Transfer of Ownership:

In this arrangement, any user may transfer ownership of a gadget to another user unilaterally. The receiving user must first have a CIA-registered private key and public key. After then, the

transfer of one user to another takes place in the same way as a regular blockchain transaction does, as previously explained. This eliminates the need for a central cloud to alter the ownership of a device.

3.1.4. Advantages over Current Scenario:

The user is signed up to the gadget with the aid of an intermediary cloud or a centralized authority in the present situation of ownership identification. Each manufacturing company has its own cloud for this reason, which makes the sign-up and owner identification procedure easier. This method eliminates the need for a centralized authority or cloud for the registration process, making it decentralized. Because there is no central cloud, the IoT device's identification of its owner becomes totally decentralized.

Interoperability between devices from various manufacturers is a major issue in the present IoT situation. The suggested solution does away with the need for a central cloud, making interoperability much easier. A device owner may easily manage their device by signing requests with their private key, which they can provide to any third-party app. As a result, this approach minimizes the reliance on any cloud and enhances the interoperability principle upon which IoT is founded. In the present situation, the user must rely on a 3rd party cloud or the manufacturer's cloud to securely connect with their device. As a consequence, protected user data and privacy may be jeopardized. The suggested solution is fully safe, since user data is only exchanged with the device and never with a third party.

4. CONCLUSION

Blockchain, being the first fully decentralized collection of transactions, has a wide range of applications in both financial and non-financial areas. Despite the fact that it has lately acquired favor among scientists, it should not be seen as a perfect answer to all problems. There are a few disadvantages to utilizing blockchain, as with any modern technology, in terms of wasted computing resources and increased storage requirements at the node level, but these issues are small and readily solved. Because it depends on the strength of consensus of good nodes to function effectively, the system discussed in this paper is reasonably safe against all types of malicious attacks. The problems with blockchain should be addressed and their remedies integrated into the implementation before creating a comparable system. A better type of registration and authentication procedure is required as the IoT environment grows and consumers become more techno and internet oriented. The tight connection between blockchain technology and modern-day cryptography allows for better kinds of identification and registration than current alternatives. As a result, blockchain offers a fantastic alternative to modern-day authentication and device interaction.

REFERENCES

1. V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaria, “To Blockchain or Not to Blockchain: That Is the Question,” IT Prof., 2018, doi: 10.1109/MITP.2018.021921652.

2. A. Urquhart, “The inefficiency of Bitcoin,” Econ. Lett., 2016, doi: 10.1016/j.econlet.2016.09.019.

3. Martin Garriga, M. Arias, Alan De Rensis, R. Li, and Y. Wu, “Blockchain based Academic

Certificate Authentication System Overview," Proc. Sample Conf., 2018.

4. H. Covington and Y. B. Choi, "Blockchain and Bitcoin," Int. J. Cyber Res. Educ., 2018, doi: 10.4018/ijcre.2019010103.

5. T. A. Sundara, I. Gaputra, and S. Aulia, "Study on blockchain visualization," Int. J. Informatics Vis., 2017, doi: 10.30630/joiv.1.3.23.

6. N. Shi, "A new proof-of-work mechanism for bitcoin," Financ. Innov., 2016, doi: 10.1186/s40854-016-0045-6.

7. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," 2017, doi: 10.1109/PERCOMW.2017.7917634.

8. B. Cresitello-dittmar, "Application of the Blockchain For Authentication and Verification of Identity," Int. J. Adv. Sci. Eng. Inf. Technol., 2016.

9. T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," IEEE Access. 2018, doi: 10.1109/ACCESS.2018.2842685.

10. J. Barclay, V. Kansara, E. Eswar, K. Elleithy, and L. Almazaydeh, "Efficient Approaches to Ensure Certificate Authenticity for Public Key Infrastructure," Inf. Technol. J., 2017, doi: 10.3923/itj.2017.79.84.