SECURITY ISSUES OF A DECENTRALIZED BLOCKCHAIN-BASED MESSAGING SYSTEM

1st Christian Elías Cruz González
ICT Engineering
ITSOEH
Mixquiahuala, Mexico
cecruz@itsoeh.edu.mx

2nd Francisco Javier Cuadros Romero
ICT Engineering
ITSOEH
Mixquiahuala, Mexico
fcuadros@itsoeh.edu.mx

***Abstract*—This paper presents a decentralized messaging system based on blockchain technology. This system allows their users to securely send and receive digital messages in the network. Since the messages stored in a conventional blockchain could be easily read by everyone in the network, under the proposed approach these messages are previously encrypted using public-key cryptography, while the sender and recipient remain anonymous. The proposed system incorporates a browser-based user interface that enable their users to interact seamlessly in a peer-to-peer fashion.**

***Index Terms*—Blockchain, Decentralized messaging, Cryptography, Distributed system, Blockchain network**

I. Introduction

With the advent of the internet, people rely on it for a wide range of applications like sending emails, chatting, trade, etc. The above applications and all personal and sensible information of their users depend upon centralized systems, which are susceptible to failure. In 2019 for more than 14 hours, the Facebook "family" of apps stopped working, causing 2.3 billion people—users of the platform at the time—to be unable to chat, post and interact with their Facebook's favorite apps [1]. This is a notorious example among others that illustrate the fact that a failure in a centralized system propagates to all its end users whose images, chats and in some cases business information is compromised.

Centralized systems are not only prone to failures inherent to their architecture, but they are also susceptible to malicious attacks such as wiretapping, masquerading, DoS and DDoS [2].

Nowadays, the data on the internet is maintained mostly on centralized, private servers owned by a number of major corporations, which is now referred to as the "cloud." These systems are run by Google, Amazon, Microsoft, and a few other enterprises, and they serve as the backbone for both their own services and those of others [3]. These companies rely on centralized systems because the modern internet was developed in large part on centralized networks that interconnect legacy systems yet still in use.

An alternative to address the disadvantages of centralized systems is to use decentralized and distributes systems. The fundamental idea behind these options is to extend the cloud concept beyond servers and instead use laptops, phones, and even smart appliances available around the world, resulting in a peer-to-peer architecture in which data is dispersed and stored largely among billions of devices.

An example that this paradigm shift is possible is the blockchain technology, of which there is a vast variety of tangible examples. For instance, Nestle uses blockchain to implement QR codes in a coffee brand to provide information related with the product [4]. Another relevant case is the government of India, which raised the use of a blockchain to regulate pharmaceutical drugs [5].

The development of blockchain technology in the past few years is already quite impressive. This suggests that the blockchain-based systems might be the future of a world free of centralized systems prone to security violations, mainly because blockchain provides three groundbreaking benefits: (1) it is decentralized, hence no central point can take control over it and cause any harm to the system, (2) it is impervious to hack or any other malicious attacks, and (3) it is a public ledger, thus anyone can ensure that the transactions have been recorded accurately [6].

In this paper, we propose a messaging system implementation based on blockchain technology. It provides a browser-based user interface that enable their users to interact seamlessly in a peer-to-peer fashion with all the underlying benefits of a decentralized network that make it possible to own a real self-sovereign identity in the network.

The rest of the paper is organized as follows: Section II describes another blockchain-based messaging systems. Section III starts explaining a general view of the process followed to analyze and understand the issues. Subsections III.A - III.H explains some general terms to understand in detail the problem posed. Finally, the paper is concluded in section IV.

II. Existing blockchain-based messaging systems

According to Status App's website, Status is a secure messaging app, crypto wallet, and Web3 browser built with state-of-the-art technology [7].

The Status Network Token is based on the Ethereum network and it is used as a free cryptocurrency in the Status

978-1-6654-0221-7/21/$31.00 ©2021 IEEE

network. In this network, messages are encrypted and cannot be read but the metadata/flow of information is public and can be read by anyone.

The main disadvantage of this alternative is that Status uses the Ethereum blockchain technology and holds your data on the network. Users of this app also report that the application is a battery hog, and, according to the displayed information, the user interface is a little complex and hard to navigate.

In [8] a chat application is proposed. It implements immutability, efficiency, and decentralization, providing a more secure environment for chatting and resource sharing. The authors mentioned that this app is suitable for all kinds of decentralized applications, especially those that rely on the blockchain. Nevertheless, it is not a fully decentralized application, considering that it requires a centralized backend to store messages.

Among its disadvantages are its inability to handle errors, such that if the chat application is not properly running, users will be unable to send messages. Also, it is not able to control the case when messages are sent but not delivered. Additionally, the chat application is susceptible to low throughput, which is a result of the limited confirmation rate inherent to the blockchain.

Another proposed scheme is presented in [9]. This relies upon a new blockchain called Blockchain-as-a-Service which presents an identity-based blockchain with the aim to provide an infrastructure for decentralized storage, computation, and messaging services.

Under this approach, the mobile network operator issues a digital certificate to the user's device during the application installation process. The main advantage of the proposed scheme is that the users can communicate with each other using a ratchet forward encryption mechanism. As counterpart, the above mentioned proposal it is not scalable to large-scale data, the data integrity is not guaranteed in systems with malicious nodes, and there is no way to prevent the mobile network operators from tampering the data.

III. Proposed messaging system

For research purposes, the first step was to generate a blockchain following the Bitcoin base [10].

In a blockchain-based system, the nodes perform their transactions by broadcasting them to the entire network. As described in Fig. 1, the nodes verify the transactions and apply the rules in the blockchain to verify the validity of the transactions. Once a transaction is verified, it will be applied to the blockchain and the nodes will start to work on the next transaction.

Each transaction in the blockchain is signed by the owner of the transaction using SHA-256, and verified by other nodes in the network. If two transactions conflict with each other, the nodes will decide which one is the valid transaction by applying the rules in the blockchain. In the blockchain, the rules are defined by the protocol. In this way, a decentralized blockchain-based system is more secure than a centralized system.

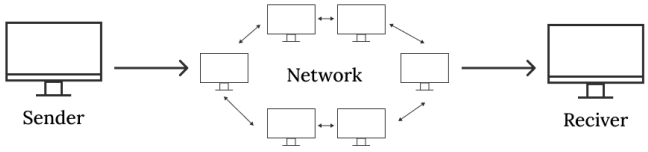

Fig. 1. Process to validate a transaction.

Once the network was created, the nodes had to be able to communicate with each other. Then, it was necessary to develop the messaging system using the API of the blockchain and the JavaScript programming language. With this app, we can send some messages stored in the data of each block.

Because network data is public, it is completely important to encrypt the data using public-key cryptography (the application uses SSH protocol to communicate) [11]. Then, we need to test and try to violate the security of the blockchain.

A. Implementation of the blockchain

The first step in the process is the creation of the blockchain. A blockchain should have a genesis block, which, basically, is the first block in the blockchain. The genesis block in this paper have hard-coded into it the information about the blockchain: The name of the currency, the reward for the generation of a block, and the address (in the blockchain) of the creator. This is the step that is the most important part of the whole implementation, because the blockchain without a genesis block is not a blockchain at all.

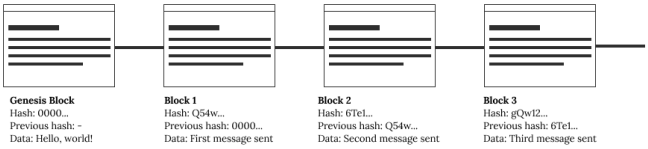

Fig. 2. Addition of a new block to the blockchain.

When all the blockchain is developed, miners begins to mine the new block on the blockchain. When a new block is mined, the miner can add the block as the next in the chain, as seen in Fig. 2. The miner will also get a reward for the new block.

Each block contains a message sent between two nodes of the network. The message should be encrypted with the public key of the receiver, as described in Fig. 3. Then, when the network accepts the block, the receiver can decrypt using the private key.

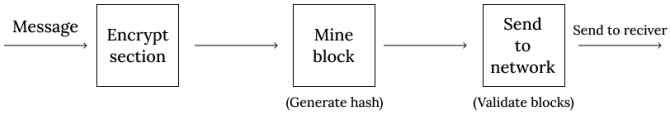

Fig. 3. Block diagram of the protocol.

B. Public-key cryptography

In this work, the algorithm to encrypt data is aes128-ctr, which is a quite secure algorithm and used by hundreds of web servers (applying SSH protocol). It provides the authenticity and confidentiality of the communication and helps users to establish secure connections between each other and encrypt data. This algorithm involves a pair of keys known as a public key and a private key, which are associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data [12]. Public keys are your ID in the blockchain, then, you can encrypt data to the message sent.

Users can obtain each other's public key through the registry, which is a central repository for all public keys. On the other hand, private keys are known only to their owners and are stored on their servers and computers. Private keys must be kept secret. These keys are used to decrypt data and verify the identity of the recipient of the message.

C. SHA-256

A cryptographic hash function can be informally defined as an easy to compute but hard to invert function which maps a message of arbitrary length into a fixed length (m-bit) hash value, and satisfies the property that finding a collision [13].

SHA-256 is a 256-bit hash algorithm designed to work on strings or other data that is either unstructured or has small, frequent changes. It is one of the most widely used hash algorithms for digital data in the world, and is used for a variety of purposes, such as blockchain mining.

This hash function is used to verify and store data. In general, they are used for the construction of digital signatures, so that they can be used to verify transactions.

D. Miners

Miners (peers) contribute to mining blocks and earning rewards. They are interested in mining as much as possible and receive as many rewards as possible. Miners are also responsible for adding blocks in the blockchain, and the order of the blocks in the blockchain is decided by the miners.

In this blockchain, the consensus on the blockchain is reached through a consensus algorithm. A consensus algorithm is designed to protect the security of the blockchain by avoiding forks.

Miners follow the longest blockchain chain and publish blocks according to their own interests. If one side wins the miner's vote, the blocks on the other side of the fork are discarded.

E. Proof-of-work

In Proof-of-work, each node is competing to find a nonce value to produce a hash that meets certain criteria. The difficulty of calculating such a nonce value can be calculated based on the criteria of the hash value. [14]

Proof of work includes the members solving the complex problem, As shown in Fig. 4, without having a particular need for the solution (except as evidence, of course), which absorbs a large number of resources in turn [15].

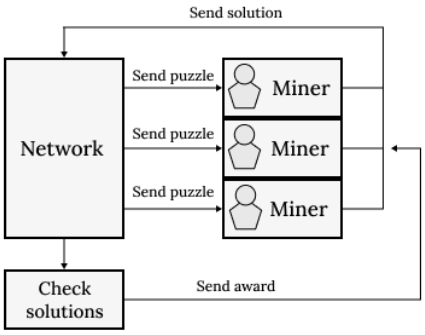

Fig. 4. In proof-of-work, miners want to find the solution.

The security of a decentralized blockchain-based messaging system is based on the security of blockchain. To maintain security, we must follow the laws and regulations of the blockchain. For this reason, it is necessary the proof-of-work, based on mathematical algorithms, to solve the problem of computational power and computational difficulty. These algorithms are used to generate a block in the chain.

F. 51% attack

According to [16] a 51% attack occurs when a single party accumulates enough hashing power to overwhelm the rest of the network. This allows them to prevent new transactions from being confirmed, meaning they can halt payments between users. They can also reverse transactions completed while they are in control of the network.

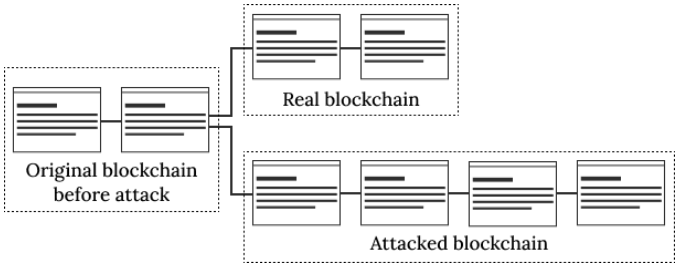

Fig. 5. Key idea of the 51% attack.

The attacker can also prevent new blocks from being added to the blockchain. In a 51% attack, the attacker can create their own blockchain which is longer than the original blockchain. This forces all other users to use the attacker's blockchain, as they will not receive any other communications, as described in Fig. 5.

The attacker can maintain a blockchain that will be longer than the true blockchain for as long as they have more hashing power than all other users combined. Once a user on the network has 51% hashing power, they can also use it to create an invalid transaction.

G. Double-spending problem

Double-spending is a major problem for digital currency users. It is a form of fraud that occurs when a person spends

the same digital currency twice, as presented in Fig. 6. This is often done without the permission of the spender.

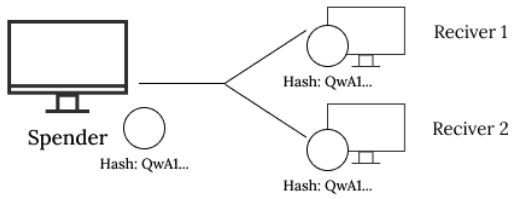

Fig. 6. A person spends the same asset.

This is possible because blockchain rely on a central database that records all the transactions that have ever been made. This is a database that is openly available to all users.

This allows anyone to take a look at the history of transactions made with the digital currency. It also allows them to undo transactions that have already been made.

H. Verification process speed

The blockchain is a public ledger that records transactions in chronological order, creating some blocks every ten minutes. This has been the standard since the beginning.

The problem is that this means that the blockchain is also public, which makes it slow. Also, there is a limit to how much data can be placed on the blockchain. The main issue with the blockchain is that it can only process so much data. There is a limit to the amount of data that can be stored on a block.

IV. Discussion

The blockchain technology is still in its infancy, and there are many limitations and important issues that need to be addressed. We have seen here that blockchain technology is an important new method to manage various types of transactions. However, it is still in development, and there are many improvements to be made before this technology can be used for mass adoption.

However, the future is still bright for blockchain technology. It is not only a promising and effective way to manage transactions, but it also has the potential to revolutionize the way we do business today.

The blockchain-based systems are vulnerable to various attacks. First, the blockchain is not secure against attackers that control a majority of the nodes in the network that can perform a 51% attack. This issue should be solved by adding nodes to the blockchain network and incentivizing the participants to run the nodes. At the same time, the network participants should be selected with care to reduce the risk of collusion.

Another issue in blockchain technology is the double-spending problem. This happens when the same digital token is spent in two different transactions. For this reason, in the blockchain core, it was added a verification for each token. The transactions are verified by using a validation of the hash. We can see that it was added a consensus protocol. This is the mechanism to reach a consensus between the nodes. The consensus protocol is used to validate the transactions and the blocks. So, the nodes are able to verify the transaction and prevent double-spending.

A limiting in the messaging system is caused by this verification of the transaction, the miners check the link between the sender and the receiver. This verification process is a quite slow process, and it is a hurdle to the mass adoption of blockchain technology.

For a blockchain, all the nodes in the blockchain must be honest and cannot cheat. If a node cheats, it can manipulate the data in the blockchain. This results in a message with no confidentiality and integrity. For potentials issues, it proposes solutions that can help achieve a secure messaging system.

The proposed solution por this problems is straightforward and easy to implement. It is applicable to any network, regardless of the type of blockchain.

References

[1] D. Lee. Facebook and instagram suffer most severe outage ever. [Online]. Available: https://www.bbc.com/news/technology-47562281

[2] I. Kantzavelou and P. A., "Issues of attack in distributed systems - a generic attack model," in *IFIP Advances in Information and Communication Technology*. Springer US, 1995, pp. 1–16.

[3] A. Lam. These technologists think the internet is broken. so they're building another one. [Online]. Available: https://www.nbcnews.com/tech/tech-news/these-technologists-think-internet-broken-so-they-re-building-another-n1030136

[4] M. del Castillo and M. Schifrin. (2020, Feb) Blockchain 50. [Online]. Available: https://www.forbes.com/sites/michaeldelcastillo/2020/02/19/blockchain-50/

[5] A. Roy. Blockchain: The india strategy. [Online]. Available: https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf

[6] M. Di Pierro, "What is the blockchain?" *Computing in Science Engineering*, vol. 19, no. 5, pp. 92–95, 2017.

[7] T. C. Contributors. (2021) Status. [Online]. Available: https://status.im/

[8] A. P. Takale, "Decentralized chat application using blockchain technology," *International Journal for Research in Engineering Application & Management*, 2008.

[9] R. Singh, "Blockchain-enabled end-to-end encryption for instant messaging applications," *arXiv*, 2021.

[10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Cryptography Mailing list at https://metzdowd.com*, pp. 1–9, 03 2009.

[11] R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Secure shell (ssh) traffic analysis with flow based features using shallow and deep networks," in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2017, pp. 2026–2032.

[12] IBM. Public key cryptography. [Online]. Available: https://www.ibm.com/docs/en/ztpf/1.1.0.15?topic=concepts-public-key-cryptography

[13] H. Gilbert and H. Handschuh, "Security analysis of sha-256 and sisters," in *Selected Areas in Cryptography*, M. Matsui and R. J. Zuccherato, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 175–193.

[14] X. Yang, Y. Chen, and X. Chen, "Effective scheme against 51% attack on proof-of-work blockchain with history weighted information," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 261–265.

[15] P. R. Nair and D. R. Dorai, "Evaluation of performance and security of proof of work and proof of stake using blockchain," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, 2021, pp. 279–283.

[16] S. Aggarwal and N. Kumar, "Chapter twenty - attacks on blockchain working model." in *The Blockchain Technology for Secure and Smart Applications across Industry Verticals*, ser. Advances in Computers, S. Aggarwal, N. Kumar, and P. Raj, Eds. Elsevier, 2021, vol. 121, pp. 399–410.