Secure Cryptography Key Management System for Web Based Wallet Management System

Garvit Chhajed, Hitesh Jethani and Anagha Pokharkar

April 16, 2020

Secure Cryptography Key Management System for Web Based Wallet Management System

1st Garvit Chhajed, Computer Science, Medi-Caps University, Indore, India, garvitchhajed87@gmail.com

2nd Hitesh Jethani, Computer Science, Medi-Caps University, Indore,India, hiteshjethani99@gmail.com

3rd Angha Pokharkar, Assistant Professor, Computer Science, Medi- Caps University, Indore, India, angha.pokharkar@medicaps.ac.in

***Abstract*— Cryptocurrencies are getting massive momentum in the last few years. Cryptocurrencies depend upon a secure distributed ledger called blockchain which stores blocks in a secure and chronological order. Although a large cryptocurrencies wallet management scheme has been proposed but they suffer from weak security. Thus effective cryptocurrency key management has become a much needed requirement for modern cryptocurrencies. In this paper, we propose a more effective, usable and secure cryptocurrency key management system named rashi that provides security enhanced storage, no password authentication. The performance analysis shows that our proposed system requires minimal additional overhead and has low time delays, enhanced security and efficient real - world deployment.**

Keywords— cryptocurrencies, wallet, blockchain, distributed ledger, secure, key management protocols.

I. INTRODUCTION

Cryptocurrencies have emerged as a popular medium of transaction. They are decentralized modes of transactions i.e. they do not have any single authority. A cryptocurrency wallet is much more secure than our regular means of transaction like cash and bank accounts. These wallets are based on blockchain technology. Each block in the blockchain represents a number of transactions and includes a cryptographic hash of the previous block.

Blockchain technologies, due to the success of bitcoin, have become famous all over the world. In blockchain architecture, payments are performed between two peers in the network. Every peer in the network is referred to by an unique address. Each address is associated with a public key and a private key. Normally if a key is lost, then there is no means by which the wallet can be accessed and all the amount is lost forever. Thus, managing cryptocurrency keys effectively and securely is one of the biggest challenges. Recently, some developers proposed a password-derived key, however they also have some disadvantages, password-derived key management relies on the security of password which is problematic because passwords can be hacked, also if passwords are forgotten, the user loses the whole of the amount forever.

To overcome this disadvantage, in our project , we have linked both the public and private keys with user ip-address and hence keys cannot be lost and more security is added as the wallet can be accessed through only one system. Therefore, proposing an effective and secure cryptocurrency wallet management system is our main aspect.

II. RELATED WORK

Key management is the art of managing cryptographic keys in a cryptosystem. This includes dealing with the generation of keys, their exchange, storage, use, crypto-shredding and replacement of keys. Key management basically concerns keys at the user level, either between users or systems. Successful key management is critical to the security of a cryptosystem because if the key is lost it cannot be retrieved and all the amount in the wallet is lost forever.

To overcome the problem of key management, developers have invested significant time and energy in implementing various key management tools.

One of the solutions was storing keys in a local storage. When a client wants to extract the key to execute a transaction, the local storage server can obtain the key files. This method is easy to implement but has its disadvantages because any malware can read and write the key files, if malware can tamper with key files, our wallet can be hacked.

Another idea to overcome the problem was a password protected wallet. These wallets prevented physical theft and security was based on strength of password but no effective mechanism was there to crack the password if the user forgets it.

Then came the idea of offline storage wallets which had enhanced security but they had a very clearly visible drawback as wallets stored offline took more time to spend funds because they are not available every time.

Another method of key management is to host the users' keys on a web service. The host service provider provides the servers to store the users accounts and assist users in key management and transactions. The users on these platforms can use the cryptocurrency system even when they have little knowledge about cryptocurrency. However, the hosted wallets are based on a very strong security assumption that the third-party service provider is trusted. However, accidents whereby hosted wallets are stolen by hackers or are lost by the host service provider closing down occur frequently. The statistical data show that there have been over 40 events involving hacking of wallets.

In our project, we have linked keys with unique ip addresses. The proposed key management mechanism provides a new innovation in making cryptography deployment practical, hence making cryptocurrency practical.

III. Problem Defination

Cryptocurrency wallets have become widely popular all over the globe. This is because of the various advantages they have over normal modes of transactions, for example, they involve no third party, they are decentralized, more immune to security threats and various other advantages. These widely used wallets must be user friendly and easy to use for them. We know that every cryptocurrency wallet has keys and keys play a major role in security of the wallet. Hence an effective cryptocurrency key management is must for modern cryptocurrency.

Although various cryptocurrency wallet-management schemes have been proposed but they are for one particular application and suffer from weak security. Modern public-key cryptography is not easy to use by the user because a private key is too long and complex. In case one forgets a key because of its complexity or loses it, the amount in the wallet will be lost forever. Various methods such as password protected wallets and password derived wallets have been proposed but the problem still arises that users will have to keep complex passwords for security of wallet and if he/she forgets password then also amount in wallet is lost forever.

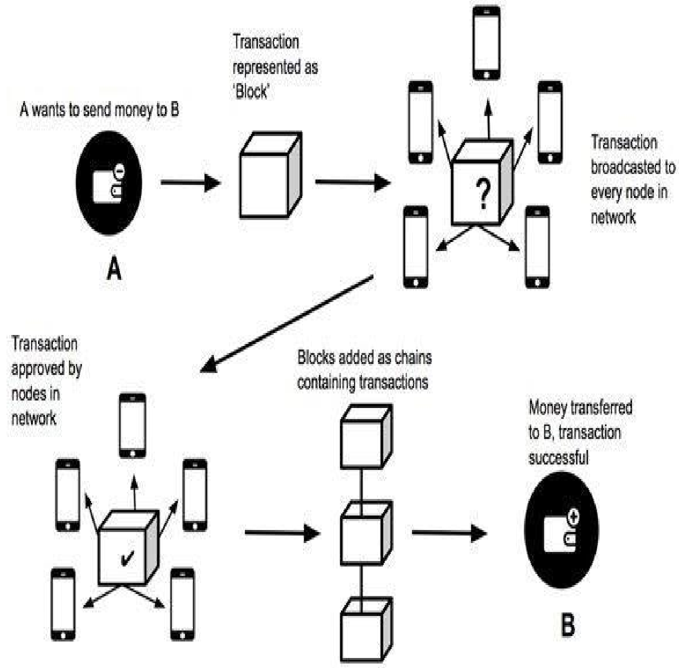
Hence there is an urgent need to improve the key management to make this widely popular cryptocurrency wallets more practical for users.

In our project, we propose a more effective, usable and secure cryptocurrency key management system. We have linked both the private key and public key with the user ip address and hence there will be no problem as the user does not have to remember complex private keys or any password and it also provides more security to our wallet. This is our step in making cryptocurrency wallets more practical.

IV. Proposed Solution

This system is proposed to have the transactions of cryptocurrencies between nodes without explicitly using complex public and private keys. Instead we added a minimal additional overhead of the ip address of the nodes by binding the public and private keys to the unique ip address of the nodes so that nodes can perform transactions without memorising the complex and large public and private keys. This provides a more secure key management system for the cryptocurrencies wallets.

This system overcomes the drawback of previous cryptocurrencies wallet systems by providing a better key management scheme. Because the keys play an important role in securing cryptocurrencies as if they are stolen or lost all the transaction details and cryptocurrencies may be lossed permanently. Thus to prevent the loss of cryptocurrencies we need a system which provides a secure cryptographic key management.


A wants to send money to B
A
Transaction represented as 'Block'
?
Transaction broadcasted to every node in network
Transaction approved by nodes in network
✓
Blocks added as chains containing transactions
Money transferred to B, transaction successful
B

As shown in figure 1.1, suppose node A wants to transfer some currency over to node B. There is a unique ip address associated with each node in the network and thus the user has not to remember the complex and large public and private keys. He has just to access the website using his own system(unique ip address) and then perform the transactions. When a transaction is performed it is represented as a block. The Block is then broadcasted to each and every node in the network. The network as a whole decides whether the transaction is valid or not and thus if it is a valid transaction it is added to the distributed ledger. In this way, the transaction from node A to B is performed successfully and securely.

Building Blocks

Block - block can be thought of as a page in a ledger that records the transactions between the nodes in a secure and chronological way linked using cryptography. It is like a record book of transactions. The individual block consist of the following several components :

Index
Timestamp
Transactions
Proof(Nonce)
Previous_hash

Blockchain - blockchain is a chain of data blocks which contains the verified(mined) block in a secure and chronological order linked using cryptography. Blockchain is unalterable i.e if once a block is added to the blockchain then it is not possible to remove the block from the blockchain .

Consensus Protocol - consensus protocol ensures that every block that is added to the Blockchain is the single version of the truth that is accepted by all the nodes in the Blockchain. Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire nodes in the network.

Mining - mining is the process of securing and verifying the cryptocurrencies transactions. It involves the miners who perform complex computation in proof of work(pow) consensus algorithm to add the block to the blockchain i.e verify the transaction and add it to the distributed ledger which cannot be thereby altered. Each miner is rewarded with some part of cryptocurrencies for performing complex computation and using resources for mining.

ENVIRONEMENTAL SETUP

Python modules that were used to develop the web based cryptocurrency wallet with secure cryptography key management system, Rashi are :

Hashlib - This module contains interfaces to various secure hashing algorithms like SHA1, SHA224, SHA256, SHA512 as well as RSA'S MD5 algorithm.

Flask - This is a framework in python used for building web applications.

Json - This module is used to handle the JSON data.

Time - This module is used for performing date time operations and getting the current system date and time.

SocketIO - This module is used for creating a client server communications and server for running the web application.

We have used Visual Studio as a development environment for developing the proposed system.

ALGORITHMS

Secure Hashing Algorithm(SHA) 256 - sha-256 is a one way function which takes as an input of any size and generates a string of fixed 256 bits. This algorithm is developed by National Security Agency and is a highly complex encryption algorithm which generates a unique hash value for each different data value and thus is used as a cryptographic hashing algorithm which is nearly impossible to be decrypted.

Proof Of Work(POW) - proof of work is the consensus algorithm used as a mining algorithm in our proposed solution. It is used to confirm the transactions and add new blocks to the chain. The miners compete against each other and perform a complex computation and the one who does first is given a chance to mine the block and add it to the chain and gets rewarded with some part of the currencies.

V. FUTURE SCOPE.

The system we proposed has a limitation of being used over a similar network because hitting the web url with specific unique ip address is much needed for system to work else if there is any network change the system will not work so as to overcome these limitation we can use the unique mac address of the nodes which allows to perform transaction over the same system over different networks.

VI. CONCLUSION

Thus with the rapid increase in the value of cryptocurrencies, there is an urgent need for a scheme that can manage the cryptocurrency transactions in a secure and efficient way. The main challenge is the effective and secure key management system which can be efficiently applied to real world scenarios. We propose an effective, usable and secure cryptocurrency wallet management system based on the key management using the unique ip address of the user. The system offers a much more security and easy key management by using an ip address instead of complex and large public and private keys. It also offers a security enhanced storage, no password authentication feature with some additional overhead to create an effective and secure cryptocurrency wallet management system.

VII. REFERENCES

[1] S. Nakamoto. (2012). Bitcoin: A Peer-to-Peer Electronic Cash System.
[Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[2] S. He et al., "A Social-Network-Based Cryptocurrency Wallet-Management Scheme," in IEEE Access, vol. 6, pp. 7654-7663, 2018.

[3] M. Guri, "BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1308-1316.

[4] A Survey on Blockchain based Cryptocurrency & an e-Wallet http://www.ijirset.com/upload/2018/october/17_A%20Surve y.pdf

[5] Hameed, Bashar. (2019). Blockchain and Cryptocurrencies Technology: a survey. JOIV : International Journal on Informatics Visualization. 3. 10.30630/joiv.3.4.293.

[6] Guri, Mordechai. (2018). BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets.

[7] Cryptocurrency Wallet Guide: A step-By-Step Tutorial. Retrieved from https://blockgeeks.com/guides/cryptocurrency-wallet -guide/

[8] A Simple Introduction to Blockchain Algorithms https://blog.goodaudience.com/a-simple-introduction-to-blockchain-algorithms-ca05b9bcc32f

[9] What is Blockchain Technology? A Step-by-Step Guide For Beginnershttps://blockgeeks.com/guides/what-is-blockchain-technology/