IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008181|

New Way to Secure Your Cryptocurrency

Muskan khandare[1], Ayusha Jadhav[2]

Student, Department of Information Technology, B. K. Birla College of Arts, Science and Commerce (Autonomous), Kalyan, Maharashtra, India[1]

Student, Department of Information Technology, B. K. Birla College of Arts, Science and Commerce (Autonomous), Kalyan, Maharashtra, India[2]

ABSTRACT: Cryptocurrencies like Bitcoin, Litecoin, Ethereum are the digital payment systems which does not depends on banks to verify their transactions. Cryptocurrencies are based on Blockchain technology where every transaction is recorded in "blocks" and timestamped. In concern with the security issues cryptocurrencies are still hackable. In this paper, we have proposed a new approach to secure your digital wallets. We can protect your hardware in a more secure way using multi-factor authentications(MFA). In this,three ways to login are introduced,which includes knowledge, possession, inherence.

KEYWORDS: Cryptocurrency, bitcoin, hardwarewallets, Multiple Factor Authentication

I. INTRODUCTION

Cryptocurrency like Bitcoin is a decentralized digital currency, without a central bank or single administrator,that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.The cryptocurrency was invented in 2008 by an unknown person or group of people using the name Satoshi Nakamoto.The currency began use in 2009when its implementation was released as open-source software.The study till date says that cryptocurrencies are based on blockchain technology.The blockchain keeps the records of the transactions in units of blocks.Each block includes a unique ID, and the ID of the preceding block. Any miner may add a valid block to the chain by simply publishing it over the network to all other miners that are connected by p2p network[1].A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.Each block in the chain contains a number of transactions,and every time a new transaction occurs on the blockchain,a record of that transaction is added to every participant's ledger.The decentralized database managed by multiple participants is known as Distributed Ledger Technology(DLT).

Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a hash.

The Bitcoin is the purely digital currency that has no physical existence.The issues related to the security of the currency are the center of the discussion from the beginning. The efforts are made to make the currency as well as its transaction and mining secure but there are still some threats exist in front of this virtual currency.The mining process as well as transaction is not fully secure and colluding users can take the advantage of the flaws in the process.There are some services that provide the facility of online digital wallet for the clients and thus can be the target of hacking attacks.Even the exchange services can also be the target for the attackers. Some of the major harmful attacks or threats on this cryptocurrency are discussed here[1].

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008181|

Fig.1 Evolution of authentication methods from SFA to MFA [2]

Today, MFA is expected to be utilized in scenarios where safety requirements are higher than usual. According to SC Media UK, 68 percent of Europeans are willing to use biometric authentication for payments. Consider the daily routine of ATM cash withdrawal. Here, the user has to provide a physical token(a card) representing the ownership factor and support it with a PIN code representing the knowledge factor to be able to access a personal account and withdraw money[2]. This system could be easily made more complex by adding the second channel like, for example, a one-time password to be entered after both the card and the user password were presented. In a more interesting scenario, it could be done with the facial recognition methods. Moreover, a recent survey discovered that 30 percent of enterprises planned to implement the MFA solution in 2017,with 51 percent claiming that they already utilize MFA,and 38 percent saying that they utilize it in “some areas” of operation.This evidence supports the MFA as an extremely promising direction of the authentication evolution.

II. RELATED WORKS

Hangyu Tian, KaipingXue, ShaohuaLi, JieXu, JianqingLiu, Jun Zhao have scheme which has intermediates in between who acts as a communication channel. It talks about Single and multiple user transaction scheme which has Payer, Payee, Intermediary, Blockchain. Also, there is contract implementation for intermediary and for transaction. But the whole process is dependent on intermediary who’s responsible for viable transactions. The security can be improved more [4].

Hossein Rezaeighaleh and Ciffe.Zou has suggested the method which uses “ELLIPTIC CURVE DIFFIE. HELLMAN (ECDH). Inthis, bothparties’ “A” and “B”, use their private and public key, both parties share their secret public key with the other party, in process the private key of A is multiplied with public key (which is result of multiplication of B’s private key with generator point G) of B, and same on other hand, but the problem here is “Man-In-The-Middle” attack. Hacker replaces the public key of one party and can’t be distinguish byother. To solve this problem, they employ side-channel user visual verification, where the wallet displays a verification code in its trusted screen (smart card) and user confirms it (by pressing button on screen). Hence, there is no steal of master seed (private key) and backup is stored on backup wallet [3].

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008181|

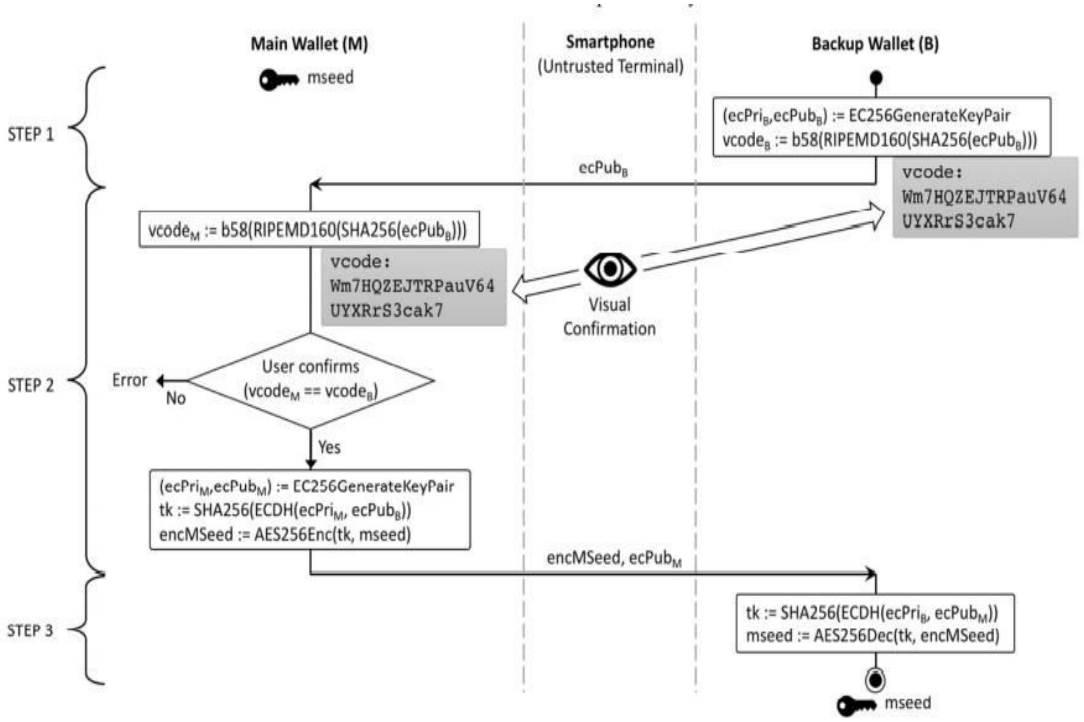

Fig. 2. Proposed secure backup mechanism to transfer master seed (mseed) from the main wallet (M) to the backup wallet (B) through an untrusted terminal. (The gray boxes illustrate the vcode that displayed on hardware wallets' screen for user verification. The values shown on the two wallets should be identical.)

Fig.2,3. [3]

Acronym	Meaning
mseed	Master Seed
$ecPri_x$	Elliptic-Curve Private key of wallet X
$ecPub_x$	Elliptic-Curve Public key of wallet X
b58	Base-58 encoding algorithm
$vcode_x$	Verification code of wallet X (displayed on the hardware wallet screen)
ECDH	Elliptic-Curve Diffie-Hellman algorithm
tk	Transport Key
encMSeed	Encrypted Master Seed

Shuangyu He, Qianhong Wu,Zhi Lang,Haibin Zheng,Yanan Li,Dawei Li, Xizhao Luo,Hanwen Feng discusses firstly on all the possible potential risks for wallets: 1.Key Storage in Local Storage 2.Password protected wallet 3.offline storage wallet 4.Password derived wallets 5.Hosted wallets, which were having certain disadvantages due to which they are unfit to use.So,the team proposes a new model comprising of User Management device, Proxy and central server [5].They performed a security analysis so that attacker cannot directly access to any information from wallet management database. It proposes an identity-based-key-insulated key which runs for minimum time. Although the team proposed an effective, usable and secure cryptocurrency wallet management system but it entirely depends on the trusted management team or we can say trusted network of people [5].

III. METHODOLOGY

This paper aims to propose a new secure approach which gives high assurance to secure your hardware wallets. Inthis, we have used MFA i.e., Multiple Factor Authentication that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008181|

Multi-Factor Authentication (MFA):
MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack.

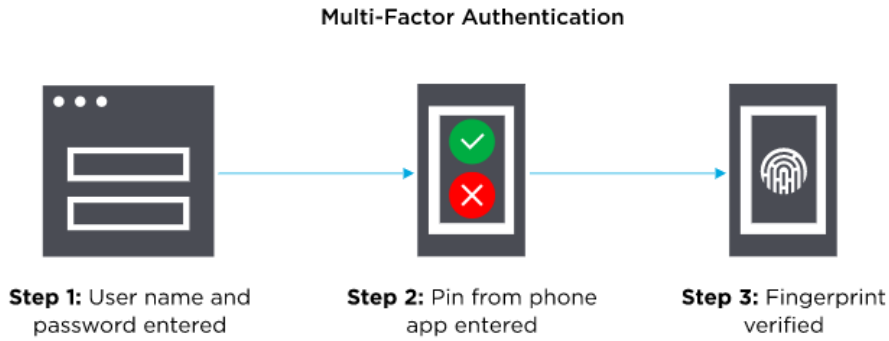

Fig.4 showing MFA process

MFA working:
MFA works by requiring additional verification information (factors). One of the most common MFA factors that users encounter is one-time passwords (OTP). OTPs are those 4–8-digit codes that you often receive via email, SMS or some sort of mobile app. With OTPs a new code is generated periodically or each time an authentication request is submitted. The code is generated based upon a seed value that is assigned to the user when they first register and some other factor which could simply be a counter that is incremented or a time value.

Three Main Types of MFA Authentication Methods:
Most MFA authentication methodology is based on one of three types of additional information:

- Things you know (knowledge), such as a password or PIN
- Things you have (possession), such as a badge or smartphone
- Things you are (inherence), such as a biometric like fingerprints or voice recognition

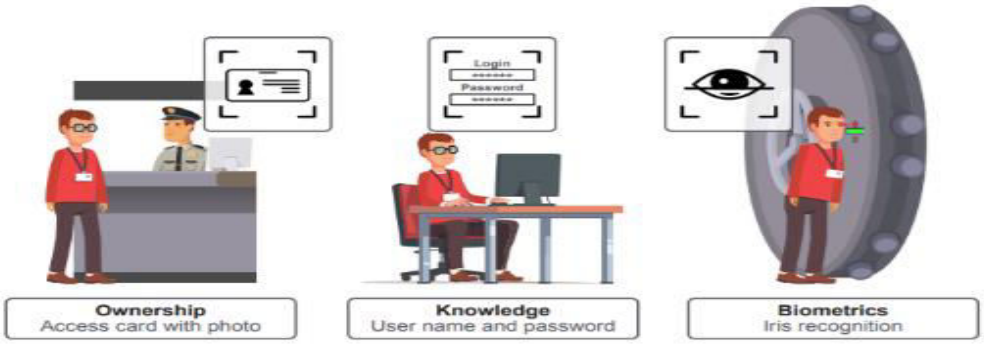

Fig.5 conceptual authentication examples

Password Protection: The conventional way to authenticate a user is to request a PIN code, password, etc. The secret pass-phrase traditionally represents a knowledge factor. It requires only a simple input device (at least one button) to authenticate the user.

OTP Generation: A user can begin to log into a secured service by entering an ID and password, but then must receive a one-time password (OTP) via SMS texting or a voice telephone call using a phone number associated with the account, with the idea that only someone who knows the correct account password and who physically possesses the required object can gain access to the account.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008181|

Fingerprint Protection: Fingerprint authentication or scanning is a form of biometric technology enables users to access online services using images of their fingerprint. The biometric scan commonly relies on mobile and other device native sensing technology, as this has all but eclipsed software, third-party biometric algorithms.

Though, user can gain access to account by simply hacking id and password. But due to biometrics is being used by variety of MFA frameworks, user fails to gain access to physical password (like fingerprints, facerecognition, voicerecognition, etc).

fig.6 how MFA works

IV. RESULTS

From the improvement perspective, Bitcoin can consider all the altcoins as a huge testing environment, from which it can borrow novel techniques and functionalities to address its weaknesses. At least in the recent future, the Bitcoin will be constantly evolving and will be in the under development phase, hence we now present our approach which uses Multiple Factor Authentication (MFA) that could be exploited in this direction.

V. CONCLUSION

Today, authentication matters more than ever before. In the digital era, most users will rely on biometrics in matters concerning systems security and authorization to complement the convention Cryptography 2018, 2, 1 19 of 31 passwords. Even though privacy, security, usability, and accuracy concerns are still in place, MFA becomes a system that promises the security and ease of use needed for modern users while acquiring access to sensitive data.

VI. ACKNOWLEGEMENT

We are truly thankful to B.K. Birla College Arts, Science and Commerce (Autonomous), Kalyan for providing us an opportunity to write a research paper as our academic performance. We also would like to thank Professor Swapna Augustine Nikale Madam for her constant assistance during the course of this research.

REFFRENCES

1. Chinmay A. Vyas and Munindra Lunagaria, Security concerns and issues for bitcoin, National Conference cum workshop on bioinformatics and computational biology, (NCWBCB-2014)
2. Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen and Yevgeni Koucheryavy, MultifactorAuthentication: Asurvey, on 6th November 2017
3. Hossein Rezaeighaleh and Ciffe. Zou, New secure approach to backup cryptocurrency wallets, University of central Florida Orlanda, USA
4. Hangyu Tian, KaipingXue, ShaohuaLi, JieXu, JianqingLiu, Jun Zhao, Enabling Cross-Chain Transactions: A decentralized cryptocurrency exchange protocol, arXiv:2005.03199v1(cs.CR) In (May 2020).
5. Shuangyu He, Qianhong Wu, ZhiLang, HaibinZheng, YananLi, Dawei Li, Xizhao Luo, Hanwen Feng, A Social Network Based Cryptocurrency Wallet-Management Scheme, IEEE ACCESS (Special section on Research challenges and Opportunities in security and privacy of Blockchain Technologies) in (January 2018).
6. Joseph J. Kearney, Carlos A. Perez-Delgado, Vulnerability of blockchain technologies to quantum attacks, Array 10 (2021)
7. Karthik C., Chandan M. N.,Abhinandan, Mohammad Rayan Baig, Blockchain for cloud backup system, International Journal of Advance Research, Ideas and Innovations in Technology

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008181|

8. Dr. Sunil Kumar, Dilip Agarwal, Hacking Attacks, Methods, Techniques and Their Protection Measures, International Journal of Advance Research in Computer Science and Management · May 2018.
9. Peter D. DeVries Professor of MIS University of Houston –Downtown, An Analysis of Cryptocurrency, Bitcoin, and the Future, International Journal of Business Management and Commerce Vol. 1 No. 2; September 2016.
10. Oliver Kattwinkel, Michael Rademacher, Exchange of Preparatory, Information for Secure and Usable Cryptocurrency transaction, IEEE 20thInternational Conference on Software Quality, Reliability and Security Companion (QRS-C) in (2020).
11. François R. Velde, senior economist, Bitcoin: A primer, the federal reserve bank December 2013 of Chicago number 317.
12. Paras Vishwakarma1, Mr. Zohaib Khan2, Dr. Taruna Jain, Cryptocurrency, security issues and upcoming challenges to legal framework in India, International Research Journal of Engineering and Technology (IRJET) (Jan-2018).
13. Iuon-Chang Lin and Tzu-Chun Liao, A Survey of Blockchain Security Issues and Challenges, International Journal of Network Security (Sept-2017)
14. Primecoin: Cryptocurrency with Prime Number Proof-of-Work, July 7th, 2013
15. Alex Greaves, Benjamin Au, Using the Bitcoin Transaction Graph to Predict the Price of Bitcoin.
16. Nallapaneni Manoj Kumara, Pradeep Kumar Mallick, Blockchain technology for security issues and challenges in IoT, International Conference on Computational Intelligence and Data Science (ICCIDS2018).
17. Le Lai, TongqingZhou, ZhipingCai, ZhiyaoLiang, Hao Bai, A Survey on Security Threats and Solutions of Bitcoin, Journal of Cyber Security in (Jan 2021).

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details