Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7923123

CONCEPT FOR SECURING MODERN FINANCIAL TRANSACTIONS USING BLOCKCHAIN AND SECTION AREA PASSWORD

Aakansha Mitawa[1] , Dr. Pawan Bhambu[2]
Research Scholar, Associate Professor
[1,2]Department of Computer Science Engineering
VGU University Jaipur

Abstract: In addition to its high growth, cryptocurrency is also subject to various drawbacks, including hacking and data leaks due to its digital nature. Using the concept of a block chain, we propose a solution for associating each cryptocurrency transaction and cryptocurrency purchased with a digital user identity. For the purpose of associating the user identity with the cryptocurrency transactions, we suggested the model in which, at the time of the purchase, we would use the concept of Digital Identity code of Currency, which is formed by combining the number of currencies purchased, the Blake2b-512 extract of the user who purchased it, the MD5 extract of the password of the user who purchased it, and the purchase code. A picture area-based text pattern formation concept is used to validate the users, which forms the text pattern based on the selected area. As a result, in each transaction that involves the exchange of currency, we will also utilize the digital identity code of the currency plus the date and time of the transaction, as well as the BLAKE2b-512 extract of the key.
Index Terms–Blockchain, Security, Cryptocurrency, Blake-2B.

1. INTRODUCTION

The term cryptocurrency can refer to any type of currency that exists carefully or fundamentally and uses cryptography to acquire trades. To record trades and issue new units, cryptocurrency relies on a decentralized framework rather than a central authority. It is a computerized payment framework that does not depend on banks to confirm trades. A common network enables anyone to send and receive payments wherever they are. Cryptocurrency parts exist essentially as computerized segments of electronic databases depicting express trades, rather than actual money that is transported around and exchanged in reality [1].

When you trade cryptocurrency, the trades are recorded in a public record. Cryptocurrency is handled by advanced wallets. Because cryptography is used to look at trades, cryptocurrency earned its name. This indicates advanced coding is involved in securing and transferring cryptocurrency data among wallets and public ledgers [2]. Until recently, the most well-known cryptocurrency was Bitcoin, which was set up in 2009. Students occasionally drive expenses skyward as a result of cryptocurrencies. Trading cryptocurrencies for benefit is a major part of the interest in cryptocurrencies.

A. Blockchain and Cryptocurrencies

The blockchain is a public record of all trades revived and held by holders of cryptocurrencies. Cryptocurrencies are created by mining, a process in which computer power is used to solve tangled mathematical problems to generate coins. Similarly, customers can purchase money-related structures from sellers, then store and spend them using cryptographic wallets. If you own cryptocurrency, you own nothing significant. What you own is a key that allows you to move data from one individual to another without seeking out a trusted third party [3].

As an information base, a blockchain stores information electronically in computerized setup. Blockchains are conveyed between two or more PCs. For the most part, blockchains are famous for keeping an auditable and decentralized record of exchanges in cryptocurrency frameworks, such as Bitcoin. Blockchains provide stability and security for information records and generate trust without the need for a trusted in pariah as a prerequisite. The first essential difference between a normal data set and a blockchain is the way in which information is organized. A blockchain assembles information in social events, called squares, that hold sets of information. Outlining a chain of information known as the blockchain, blocks have explicit storing limits and, when filled, are closed and linked to the as of late filled square. Upon completion, the chain will be updated with all new information that follows that recently added block, which is then organized into a square that has been formed. [3]

2. LITERATURE SURVEY

Tian, H. et al. (2021) [4] In this paper, Tian, H. et al. propose a distributed cryptocurrency trading scheme to solve the problem of centralized exchanges, which can accomplish secure cryptocurrency trading.In addition to implementing transactions between individual users, our scheme also allows transactions between multiple users. The scheme is implemented on an Ethereum blockchain and deployed on an Ethereum test network using smart contracts. Based on the experimental results, we can conclude that our scheme is affordable.

Aktepe, S., Varol, C. and Shashidhar, N. (2020) [5] Cryptocurrencies are computerized monetary forms meant to supplant the standard greenbacks in our daily lives, especially in recent years. As a consequence of shaky qualities on the lookout, mining cryptocurrencies is one of the most popular ways of having them and making a profit. Aggressors are increasingly utilizing malware to hijack web clients' PC assets for mining cryptocurrencies, known as cryptojacking. This has become a major issue in the online world, prompting us to develop MiNo, an internet browser extension which can detect this malicious activity running without the user's consent or knowledge. MiNo offers protection and efficiency, boasting twofold layer security that sets it ahead of its competitors.

Azman, M. and Sharma, K. (2020) [6] It offers us captivating highlights that can give way to a safe and secure money related exchange environment. The existing system provides a great opportunity for growth, and can be viewed as a foundation to build upon. HCH DEX, or Hot-Cold Hybrid Decentralized Exchange, proposes an approach of storing Cryptocurrency Wallet information on individual devices and engaging with exchanges between two devices without relying on any central storage database or server system to act as a broker or service provider;

it allows any authorized Local Broker to work with an exchange in the Blockchain and register it in the distributed ledger. Moreover, it is proposed that the card be cleverly designed and not much thicker than what we use today. This is based on a strong two-way authentication framework which enables secure handshaking processes between e-Wallets and Lightweight DLT Nodes as local facilitators. It could possibly be a small step towards a fair and equitable financial system, insulated from fraudulent and exploitative practices at every stage.

Ghorbanian, M. et al. (2020) [7] The purpose of this paper is to provide recommendations on how to effectively use digital cryptocurrencies in today's and future smart power systems, to meet the challenges of this new technology. In this paper, existing issues and challenges of smart grids in the presence of blockchain-based cryptocurrencies are presented and some innovative approaches for efficiently integrating and managing blockchain-based cryptocurrencies in smart grids are proposed. Several recommendations are made to improve the efficiency of smart grids in the presence of digital cryptocurrencies, as well as some directions for future research.

Lazo, J. G. L. et al. (2019) [8] It proposes a system to aid decision-making in the venture capital industry, embracing a modest speculation position that should reduce risk and increase profit. The strategy utilizes the genuine cost of cryptocurrencies to assess the likelihood of making a benefit, and to set up logical levels. It investigates Markov chains, which are coordinated into different decision trees, with a specific end goal to recognize which cryptocurrency has the most noteworthy potential return when sold either inside one or two periods from procurement. To guarantee exactness of the outcomes, they are compared against true information and the system's proficiency in helping speculation choices for cryptocurrency portfolio administration is confirmed.

3. PROBLEM STATEMENT AND OBJECTIVES

The use of blockchain is to identify and back track the transaction entry which is crucial in the case of the cryptocurrency. In the case of the cryptocurrencies the emphases are one the cryptocurrency as an entity. But with the concept which we are suggesting, will associate the user with the cryptocurrency and the digital code identity of the cryptocurrency with the user identify, will help to uniquely track each individual unit , directly via Digital Code Identity. In the research work we work on more secure. In the digital world of today and super sonic world which is coming on, we require the faster cryptographic hash functions for the purpose of the crypto-currencies so , due to this reason we are focusing on BLAKE2b is an excellent cryptographic hash that is extremely fast. The proper testing concepts and techniques are also required for the purpose of the examination of the strength of the blockchain generated for the cryptocurrency.

The proposed research work objectives are as follows.

- To identity the problems which are in the current cryptocurrency’sframework , where the user identity is not associated with the cryptocurrency.

- To find the methodology for make the cryptocurrency more secure, back track each of the transactions. For that we are like to work with BLAKE2b hash in combined with the MD5 hash generated Digital code for Currency.
- To propose the model of the cryptocurrency which will associate the currency individually with the user identity so that each of transaction the digital identity code can uniquely trace out the currency transact.
- Overcoming the various hacking attacks on cryptocurrencies.

The aim of this study is problems and solutions required in the field of securing the cryptocurrencies.

4. PROPOSED ALGORITHMS

The working for the Digital Identity based cryptocurrency will start for the user registration for the purpose of trading of cryptocurrency.

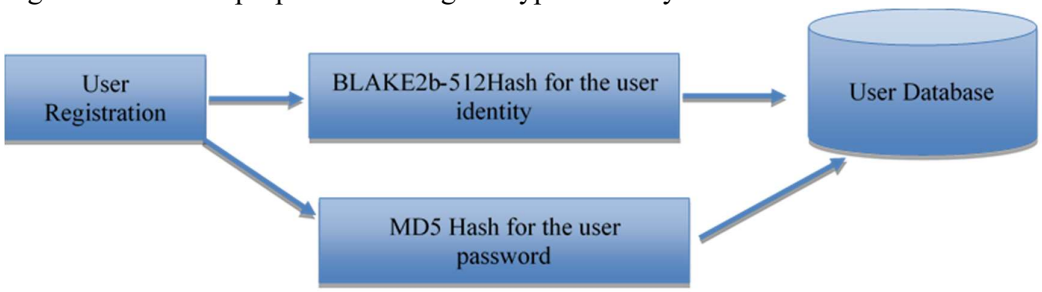

Fig 1 User Identification Process using BLAKE2b-512Hash

Now, at the time of the purchase we will use the concept like

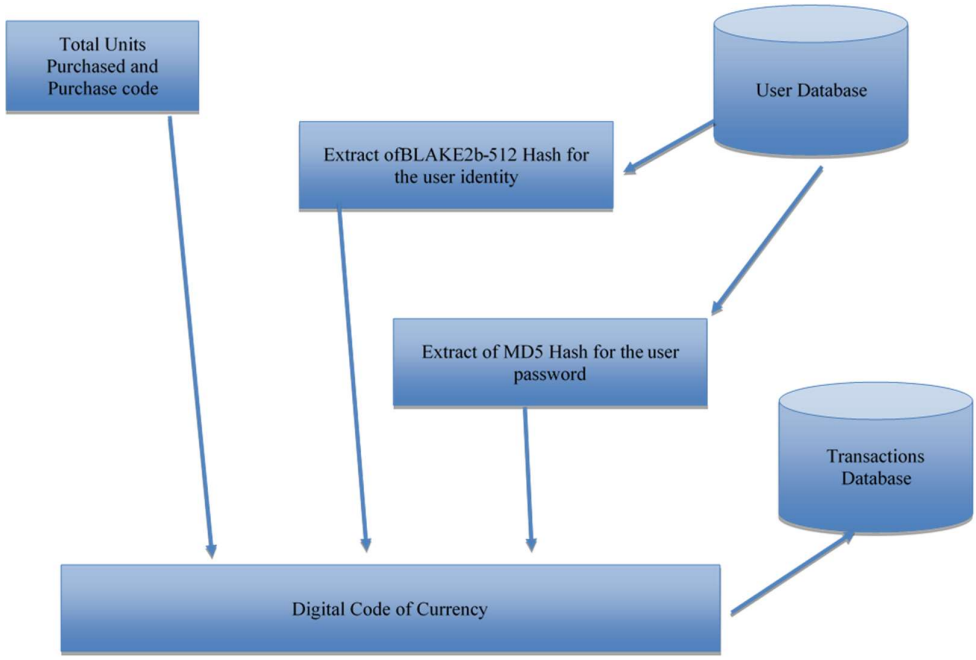

Fig 2 Digital Code of Currency Purchased

Thus, we can say the for the new purchase of the cryptocurrency we will store the,

Digital Identity code of Currency = Number of Currency Purchased , Purchase Code + BLAKE2b-512 Extract of UserName purchased it + MD5 extract of the password of User Purchased it

Similarly, in each of the transactions which are in exchange of the currency we will also make use of the digital identity code of currency + Date/Time of transaction+ BLAKE2b-512 extract of the key required for the transaction processing.

The formation of the user identity in the registration process will adopt the following process, where the user password or pattern will be formed as ,

The new concept which we can add-on in the authentication is the picture based string formation , where some 5-6 pictures are selected , in these pictures according to the coordinates area we have assigned some text corresponding to that area , so when the user click in the area we will associate that area and text in area in the pattern of authentication.

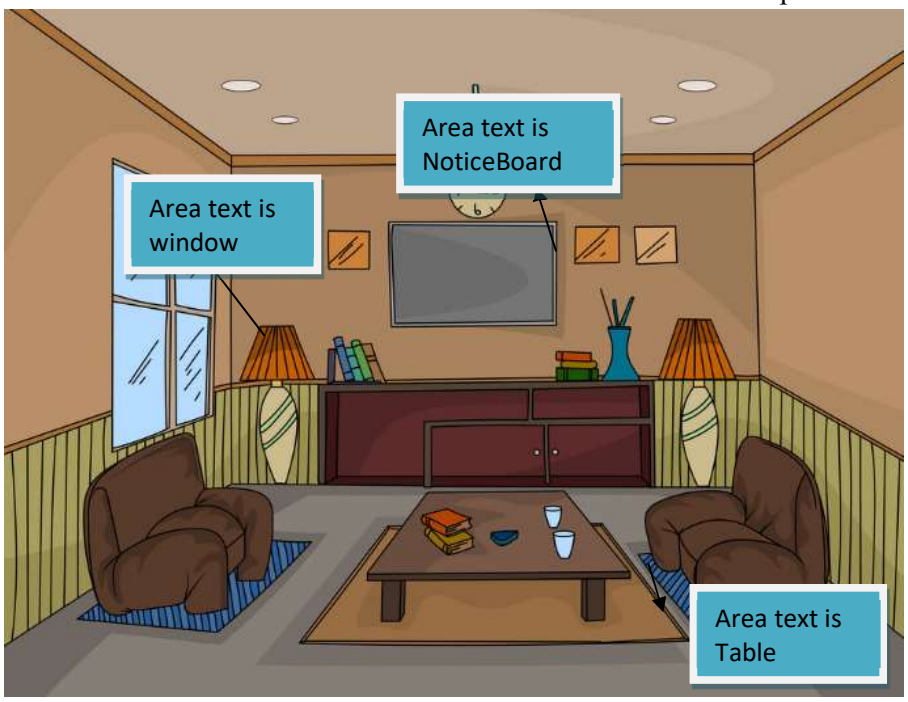

Fig 3 Picture Area Based Password Pattern

Now suppose user name Jack123 click over the following areas , noticeboard and table

So , pattern will be

Jack123_area1_noticeboard_area2_table will be the password pattern

We for the sake of example taken only three areas we can define multiple areas in the single picture on the basis of the coordinate's sections.

5. CONCLUSION

The concept of the cryptocurrency which we have proposed , we will try to create an online framework for the cryptocurrency , where the user can register , purchase as well as transact our cryptocurrency. For the simulation purpose , we can make use of the Microsoft Visual

Studio framework for creating web application for the same.The blockchain which we have create for the purpose of the purchase as well as for the purpose of the transacting the cryptocurrency can be examined of its entropy and we can make use of various online as well as offline tools for the purpose of examination of the entropy of the blockchain generated..

REFERENCES

1. Almukaynizi, M. *et al.* (2018) "Finding cryptocurrency attack indicators using temporal logic and darkweb data," in *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, pp. 91–93.
2. Azman, M. and Sharma, K. (2020) "HCH DEX: A secure cryptocurrency e-wallet & exchange system with two-way authentication," in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*. IEEE, pp. 305–310.
3. Khadzhi, A. S., Zareshin, S. V. and Tarakanov, O. V. (2020) "A method for analyzing the activity of cold wallets and identifying abandoned cryptocurrency wallets," in *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. IEEE, pp. 1974–1977.
4. Tian, H. et al. (2021) "Enabling cross-chain transactions: A decentralized cryptocurrency exchange protocol," IEEE transactions on information forensics and security, 16, pp. 3928–3941.
5. Aktepe, S., Varol, C. and Shashidhar, N. (2020) "MiNo: The chrome web browser add-on application to block the hidden cryptocurrency mining activities," in *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE, pp. 1–5.
6. Azman, M. and Sharma, K. (2020) "HCH DEX: A secure cryptocurrency e-wallet & exchange system with two-way authentication," in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*. IEEE, pp. 305–310.
7. Ghorbanian, M. et al. (2020) "Methods for flexible management of blockchain-based cryptocurrencies in electricity markets and smart grids," IEEE transactions on smart grid, 11(5), pp. 4227–4235.
8. Lazo, J. G. L. *et al.* (2019) "Support System to Investment Management in Cryptocurrencies," in *2019 7th International Engineering, Sciences and Technology Conference (IESTEC)*. IEEE, pp. 376–381.
9. Lee, J.-H. (2019) "Rise of anonymous cryptocurrencies: Brief introduction," *IEEE consumer electronics magazine*, 8(5), pp. 20–25. doi: 10.1109/mce.2019.2923927.
10. Li, Z. *et al.* (2019) "A Landscape of Cryptocurrencies," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, pp. 165–166.
11. Liang, J. *et al.* (2019) "Towards an understanding of cryptocurrency: A comparative analysis of cryptocurrency, foreign exchange, and stock," in *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, pp. 137–139.
12. Rustem, M. *et al.* (2019) "Problems of criminal responsibility for illegal circulation of cryptocurrency," in *2019 12th International Conference on Developments in eSystems Engineering (DeSE)*. IEEE, pp. 996–999.

13. Sai, A. R., Buckley, J. and Le Gear, A. (2019) "Privacy and security analysis of cryptocurrency mobile applications," in *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*. IEEE, pp. 1–6.
14. Sukharev, P. V. and Silnov, D. S. (2018) "Asynchronous Mining of Ethereum Cryptocurrency," in *2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)*. IEEE, pp. 731–735.
15. Takahashi, H. and Lakhani, U. (2019) "Multiple layered security analyses method for cryptocurrency exchange servicers," in *2019 IEEE 8th Global Conference on Consumer Electronics (GCCE)*. IEEE, pp. 71–73.
16. Wimalagunaratne, M. and Poravi, G. (2018) "A predictive model for the global cryptocurrency market: A holistic approach to predicting cryptocurrency prices," in *2018 8th International Conference on Intelligent Systems, Modelling and Simulation (ISMS)*. IEEE, pp. 78–83.
17. Ghimire, S. and Selvaraj, H. (2018) "A Survey on Bitcoin Cryptocurrency and its Mining," in *2018 26th International Conference on Systems Engineering (ICSEng)*. IEEE, pp. 1–6.