IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

Survey on Blockchain Cryptocurrency Wallet

Prof. M. S. Kale[1], Ayush Gimekar[2], Zuveriya Tamboli[3], Vaishnavi Patil[4], Abhay Pawar[5]
Professor, Department of Information Technology[1]
Students, Department of Information Technology[2,3,4,5]
Sinhgad Academy of Engineering, Pune, Maharashtra, India

Abstract: *Normal cash has developed and appears numerous downsides such as inaccessibility. It is inclined to burglary and is intensely directed by government offices. Cryptocurrencies have risen as a egotistic money related framework. They depend upon secure disseminated ledger data structure. Mining plays a critical portion in this framework. Basically, our cryptocurrency could be a conveyed database that keeps up tamper-proof information structure pieces containing his bunches of person exchanges. Blockchain innovation can be a widely emerging approach to data innovations. Bitcoin as a cryptocurrency has made several considerations since it was one of its earliest implementations. They discuss the key elements driving the development of sophisticated cryptocurrencies alongside Ethereum, a blockchain implementation with a focus on informed contracts. In its most basic form, our cryptocurrency may be thought of as a distributed database that keeps track of tamper-proof data structure blocks comprising batches of individual transactions.*

Keywords: Cryptocurrencies, Mining, Bitcoin, Ethereum, transactions, Hashing

I. INTRODUCTION

New dimensions of computer science and information technology are commencing to emerge thanks to bitcoin and blockchain innovation. The necessity for a distributed currency was previously more of a theoretical idea, but in the last ten years, it has become a reality owing to Satoshi Nakamoto's well known article from 2008, which introduced Bitcoin and Blockchain Technology. In terms of a viewpoint that is strongly tied to blockchain development, Bitcoin is the most popular option. It's also the least likely to be completely accurate because it enables a market of ambiguous exchanges worth billions of dollars that is unregulated. Accordingly, it must handle various bodily issues while working with national governments and financial connections. Since they blatantly displayed flaws in the traditional maintaining an account framework around the world, financial crises were one of the main motivations behind the creation of bitcoin. The purpose of the invention of the bitcoin was to promote global monetary interchange at the lowest cost possible. However, Bitcoin's journey never proceeded exactly as planned.

When discussing bitcoin and blockchain, there are many myths out there. In order to distinguish between the two, it should be noted that bitcoin is a kind of money and that it uses the blockchain to monitor and execute transactions. There are a number of applications for the blockchain technology that may be used in various industries. The financial back and keeping money areas are where Blockchain has the most significant potential

II. KEY CONCEPT

2.1 Blockchain

A blockchain is a publicly accessible type of record between technology nodes in the network. A blockchain serves as a digital database for storing data in digital form. The most well-known use of blockchain technology is for preserving a secure and decentralized record of transactions in cryptocurrency systems like Bitcoin. The novelty of a blockchain is that it fosters confidence without the necessity for a reliable third party by ensuring the integrity and security of a record of data. Blockchains are a specific kind of common ledger that vary from conventional databases as in manner they gather information. Blockchains hold data in blocks that are subsequently connected via cryptographic. Cryptocurrency is utilized in the context of Bitcoin in a decentralized manner, allowing all users to jointly maintain control rather than any one individual or organization. Since decentralized crypto currencies are unchangeable, the data

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

placed into them cannot be changed. This implies that payments done using Bitcoins are publicly visible and forever recorded.

2.2 Cryptography

Data security using cryptography prevents illegal access. As was already said, the two primary ideas in a cryptocurrency are cryptographic and hashing. Cryptography is employed in the blockchain to safeguard transactions between two nodes in a blockchain network.

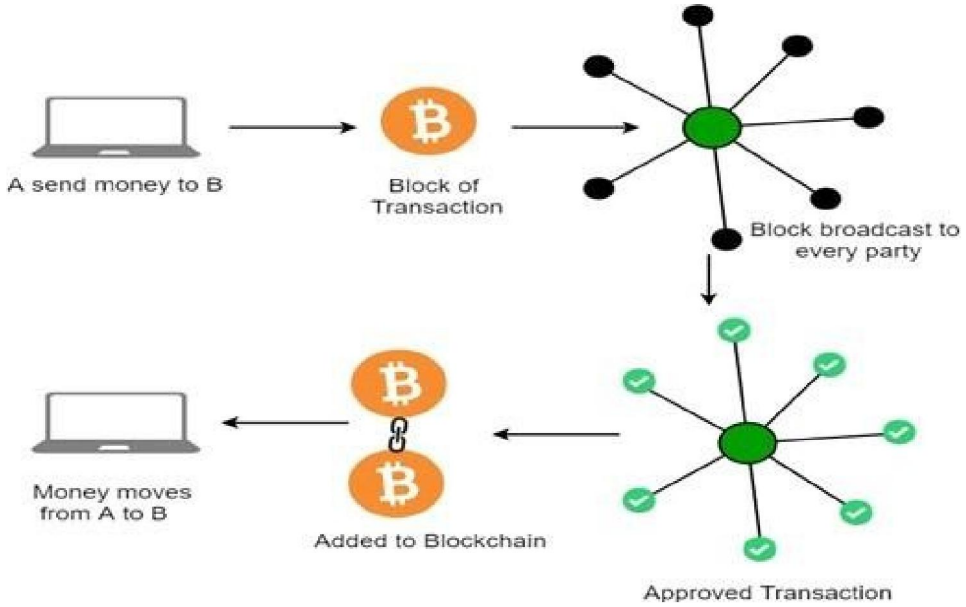

Fig.1. Transaction in blockchain

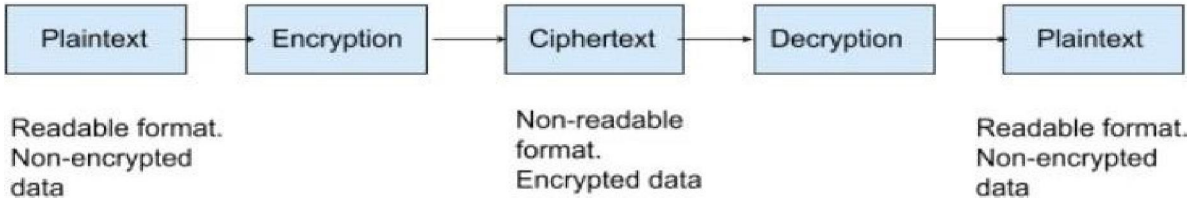

Fig.2. Working of cryptography

- **Encryption:** Conversion of normal text to a random sequence of bits.
- **Key:** Some amount of information is required to get the information of the cryptographic algorithm.
- **Decryption:** The inverse process of encryption, conversion of a Random sequence of bits toplaintext.
- **Cipher:** The mathematical function, i.e. A cryptographic algorithm which is used to convert plaintext to ciphertext(Random sequence of bits).

2.3 Cryptocurrency Wallet

Crypto wallets hold the user's private key and information, while public keys are located on the blockchain. With the combination of public and private keys, a crypto wallet can enable a secured operation to validate a balance and send or receive cryptocurrency transactions

2.4 Cryptocurrency wallet types

Hardware wallets With a hardware-based crypto wallet, the private key for the user's cryptocurrencybalance is stored on a physical medium, which is typically a USB drive. Because it's a secured device that

Paper wallets. A paper wallet is truly a low-tech solution, whereby the user writes down the public andprivate key information on a piece of paper.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

Within the hot wallet category are three types:

- **Online (web) wallets**. Perhaps the most common and widely used form of crypto wallet is found in online services. With an online wallet, an online service such as a crypto exchange holds the user's public and private keys. Users access the wallet by logging in to the online service.
- **Desktop wallets**. With a desktop wallet, the cryptographic keys are stored in an application on a user's desktop system.
- **Mobile wallets**. A mobile app can be used to store a user's public and private keys foraccessing and using cryptocurrency

III. LITERATURE SURVEY

A blockchain can be referred to as a collection of records or open records that can be shared among the participating parties. Every transaction that gets incorporated is first verified by all participants of that transaction. Once the data gets recorded by the blockchain can never be rewritten or changed. Thus blockchain can be termed as record book of all transactions held Cryptocurrencies, the decentralized bitcoin or say Ethereum which can be termed as peer-to-peer computerized cash also uses the blockchain technology. This paper proposed by Siddharth Rajput and Archana Singh includes history of bitcoin, a few literary reviews, working of the blockchain and its application.

[2] The paper proposed by Zhou Jian, Qu Ran, Sun Liyuan in Securing Blockchain Wallets Efficiently Based on Threshold ECDSA Scheme Without Trusted Center proposes a blockchain wallet protection scheme against single point failure based on threshold elliptic curve digital signature without trusted center. In this scheme, participants cooperate to generate public and private keys and sharing private key without the participation of trusted center. The participants who exceed the threshold number can sign the transaction by constant rounds, which can effectively resist single point attack and ensure the security of wallet.

Cong Li and Shihao Li [3], In this paper the authors have studied the security risks of Android-based cryptocurrency wallet and proposed the adversary model, analyzed the attack surface originated from the Android OS, and demonstrated several attack vectors by conducting experiments on multiple popular cryptocurrency wallets in Google Play Store. Finally, they have presented several security defense strategies in response to the security risks. Weiqi Dai, Jun Deng [4], In this paper, the analyst have designed a secure blockchain lightweight wallet based on Trust zone to protect SPV. It is more portable compared with the hardware wallet, and safer than the software wallet. Through the isolation, it can also protect the private key and the wallet's address from being stolen by the attackers no matter whether the Rich OS is malicious or not.Meanwhile, it can protect the verification process by verifying transactions in the secure execution environment (SEE), and keep the local block headers unreadable directly from the Rich OS through encryption. Shachi Mall et al. [13], Xu Wu et al. [14], N. Shelke et. al. [15] and S. L. Bangare et. al. [16-19], V. Durga Prasad Jasti et. al. [20], A. S. Ladkat et al.[21] have shown different methods for ML classification.

IV. FUTURE SCOPE

Blockchain in Cybersecurity: For apparent reasons, the future of blockchain technology is mostly in the area of cybersecurity. The data remains secure and verifiable despite the open and distributed nature of the Blockchain ledger. Cryptography is used to encrypt data in order to remove vulnerabilities like illegal data tampering

Blockchain in finance Industry: Blockchain technology has been successful in delivering its promise and demonstrated consistency regarding its objective of tracking financial assets. After seeing the potential and positive effects of this technology, several financial institutions made investments in it. Blockchain is able to address the flow and deals of black money flow because of its transparent ledger architecture.

Blockchain in Cloud Storage: Data loss, hacking, and human mistake are all serious risks associated with centralized systems. Blockchain technology can be used to improve cloud storage security and hacker resistance, similar to how it is used in cybersecurity.

Blockchain in Networking, IOT: blockchain technology is being adopted by businesses like IBM and Samsung to create a distributed network of IoT devices. The ADEPT concept attempts to eliminate the central site for the control of communication between devices for tasks like software updates, error handling, keeping track of energy usage, etc.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

Blockchain in Government Organizations: The idea of blockchain can also aid in the management of enormous amounts of data, which can be highly beneficial for government organizations. The adoption of Blockchain will result in an efficient data management system with the potential to enhance how these entities operate

V. CONCLUSION

The two most popular and valuable cryptocurrencies in existence today are Bitcoin and Ethereum. Theyare built on blockchain technology, which aims to support a done to assure in a peer-to-peer network based on the consensus of the majority of nodes. In this article, we present an overview of the foundations of blockchain technology, the most successful (or well-liked) blockchain applications, Bitcoin and Ethereum, as well as the early phases of the introduction of digital money. The expense of technology is the sole issue. Cost is what drives day-to-day company operations; thus, banks must carefully consider this before implementing this technology. When blockchain is used to power the banking system, it becomes more tolerant.

REFERENCES

[1]. Hossein Rezaeighaleh, Cliff C. Zou, Multilayered Defense-in-Depth Architecture for Cryptocurrency Wallet 2020 IEEE 6th International Conference on Computer and Communications.

[2]. Gokay Saldamli, Sohil S. Mehta, Pranjali S. Raje, Madhuri S. Kumar, Sumedh S. Deshpande. Identity management using blockchain, preprint, (2019)

[3]. N. Kshetri and J. Voas, ”Blockchain-Enabled E-Voting,” in IEEE Software, vol. 35, no. 4, pp. 95-99, 2018.

[4]. D. Mill operator, "’Blockchain and therefore the net of Things within the Industrial Sector,"’ in IT skilled, vol. 20, no. 3, pp. 15-18, May./Jun. 2018.

[5]. Popova, N.A., Butakova, N.G. (2019). Research of a possibility of using blockchain technology without tokens to protect banking transactions Proceedings of the 2019 IEEE Institute of Electrical and Electronics Engineers Inc.

[6]. T. N. Dinh and M. T. Thai, “AI and Blockchain: A turbulent Integration,"’ vol. 51, no. 9, pp. 48-53, Gregorian calendar month 2018.

[7]. L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, G. Linchao and H. Kai, "’A Multiple Blockchains design on Inter Blockchain Communication,"’ 2018 IEEE International Conference on software system Quality, responsibility and Security Companion (QRS-C), L’isbon, 2018, pp. 139-145.

[8]. Corina Sas and Irni Eliana Khairuddin, "Exploring Trust in Bitcoin Technology: A Framework for HCI Research" in, ACM, 2015.

[9]. Stanislaw Jarecki, Aggelos Kiayias, Hugo Krawczyk and Jiayu Xu, "Highly Efficient and Composable Password-Protected Secret Sharing (Or: How to Protect Your Bitcoin Wallet Online)" in , IEEE, 2016

[10]. Nelisiwe Peaceness DLAMINI, Mfundo Shakes SCOTT and Kishor Krish-nan NAIR, "Development of an SMS System Used to Access Bitcoin Wallets" in, IST Africa, 2017.

[11]. Miraje Gentilal, Paulo Martins and Leonel Sousa, "TrustZone-backed Bitcoin Wallet" in , ACM, 2017

[12]. Puneet Kumar Kaushal, Amandeep Bagga and Rajeev Sobti, "Evolu-tion of Bitcoin and Security Risk in Bitcoin Wallets" in, IEEE, 2017

[13]. Shachi Mall, Ashutosh Srivastava, Bireshwar Dass Mazumdar, Manmohan Mishra, Sunil L. Bangare, A. Deepak, “Implementation of machine learning techniques for disease diagnosis”, Materials Today: Proceedings, Volume 51, Part 8, 2022, Pages 2198-2201, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2021.11.274.

[14]. Xu Wu, Dezhi Wei, Bharati P. Vasgi, Ahmed Kareem Oleiwi, Sunil L. Bangare, Evans Asenso, "Research on Network Security Situational Awareness Based on Crawler Algorithm", Security and Communication Networks, vol. 2022, Article ID 3639174, 9 pages, 2022. https://doi.org/10.1155/2022/3639174

[15]. N. Shelke, S. Chaudhury, S. Chakrabarti, S. L. Bangare et al. “An efficient way of text-based emotion analysis from social media using LRA-DNN”, Neuroscience Informatics, Volume 2, Issue 3, September 2022, 100048, ISSN 2772-5286, https://doi.org/10.1016/j.neuri.2022.100048

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

[16]. S. L. Bangare, G. Pradeepini and S. T. Patil, "Brain tumor classification using mixed method approach," 2017 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 2017, pp. 1-4, doi: 10.1109/ICICES.2017.8070748

[17]. S. L. Bangare, G. Pradeepini, S. T. Patil, "Implementation for brain tumor detection and three dimensional visualization model development for reconstruction", ARPN Journal of Engineering and Applied Sciences (ARPN JEAS), Vol.13, Issue.2, ISSN 1819-6608, pp.467-473. 20/1/2018 http://www.arpnjournals.org/jeas/research_papers/rp_2018/jeas_0118_6691.pdf

[18]. S. L. Bangare, "Classification of optimal brain tissue using dynamic region growing and fuzzy min-max neural network in brain magnetic resonance images", Neuroscience Informatics, Volume 2, Issue 3, September 2022, 100019, ISSN 2772-5286, https://doi.org/10.1016/j.neuri.2021.100019

[19]. Sunil L. Bangare, Deepali Virmani, Girija Rani Karetla, Pankaj Chaudhary, Harveen Kaur, Syed Nisar Hussain Bukhari, Shahajan Miah, "Forecasting the Applied Deep Learning Tools in Enhancing Food Quality for Heart Related Diseases Effectively: A Study Using Structural Equation Model Analysis", Journal of Food Quality, vol. 2022, Article ID 6987569, 8 pages, 2022. https://doi.org/10.1155/2022/6987569

[20]. V. Durga Prasad Jasti, Enagandula Prasad, Manish Sawale, Shivlal Mewada, Manoj L. Bangare, Pushpa M. Bangare, Sunil L. Bangare, F. Sammy, "Image Processing and Machine Learning-Based Classification and Detection of Liver Tumor", BioMed Research International, vol. 2022, Article ID 3398156, 7 pages, 2022. https://doi.org/10.1155/2022/339815

[21]. Ajay S. Ladkat, Sunil L. Bangare, Vishal Jagota, Sumaya Sanober, Shehab Mohamed Beram, Kantilal Rane, Bhupesh Kumar Singh, "Deep Neural Network-Based Novel Mathematical Model for 3D Brain Tumor Segmentation", Computational Intelligence and Neuroscience, vol. 2022, Article ID 4271711, 8 pages, 2022. https://doi.org/10.1155/2022/427171