Survey on Cryptocurrency Wallet

Pragya Jain[1], Sunandani Gupta[2], Sandali Bhise[3], Sneha Shelke[4]

Students, Department of Computer Engineering[1,2,3]

Assistant Professor, Department of Computer Engineering[4]

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 [1]. 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 [1]. 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 batchesof individual transactions [1].*

Keywords: *Cryptocurrencies, Blockchain, Transaction, Secure, Innovations*

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.[1]

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.[2]

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.[1]

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 [3].

II. KEY CONCEPT

2.1 Blockchain

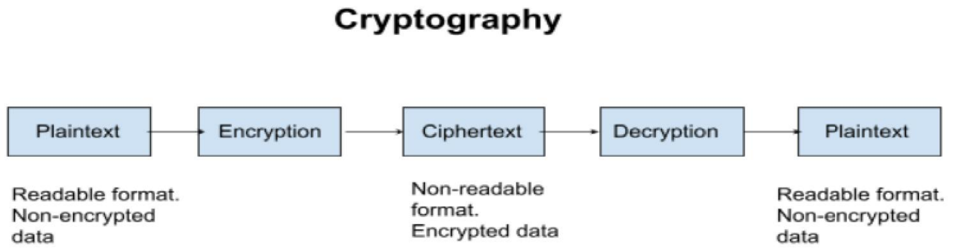
A blockchain is a publicly accessible type of record between technology nodes in the network. A blockchain serves as a digital database for storing data in digital form. The most well-known use of blockchain technology is for preserving a secure and decentralized record of transactions in cryptocurrency systems like Bitcoin [6]. 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.[7] 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

DOI: 10.48175/IJARSCT-7528

placed into them cannot be changed. This implies that payments done using Bitcoins are publicly visible and forever recorded.[6]

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.[7]


Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data
Non-readable format. Encrypted data
Readable format. Non-encrypted data

There are two types:

- Asymmetric: A public key and a private key are needed, one for encryption and the other for decryption.
- Symmetric: For both encryption and decryption, a single key is all that is necessary.[8]

III. LITERATURE REVIEW

The literature review conducted prior to this assessment provides insight into the blockchain innovation's concept as well as the distribution of outputs within designated areas [1]. The analysis shows that the areas mentioned in more detail—blockchain as an innovation capability, clever contracts, plans of action, innovative probabilities and obstacles, and cryptocurrency as a universally beneficial breakthrough—lack in-depth treatment. The author is talking about how a few of the outstanding issues and weaknesses are addressed by Currency's activity outside of the blockchain. Blockchain standards and promises related to cryptocurrencies do not meet FinTech's needs for security and privacy, from transaction throughput to primitives [2,7]. The issue of cryptographic agreement is tackled in this research via block - chain. Additionally, if there is a way to guarantee that certain databases will be used to store economic action and deal operations without the interference of the central authority It examines the key technology and design facets of blockchain and offers scenarios in which blockchain applications may be used [3,8].The author talks about how some of the outstanding issues and weaknesses are addressed by Bitcoin's activity outside of the blockchain. The specifications and assurances of cryptocurrency blockchains do not meet the security and privacy demands of FinTech, from transaction throughput to primitives [9]. It examines the distributed databases' security procedures and makes a blockchain-based suggestion on how to overcome the difficulties associated with maintaining information privacy in them. Without mining and tokens, the mechanism for preserving the secrecy and accuracy of knowledge regarding bank transactions, according to the authors, would be considerably disrupted by blockchain [10].In the paper,Blockchain and Cryptocurrencies: Model, Techniques, and Applications byY. Yuan, S. Member, and F. Wang [11] Blockchain has received a lot of attention in recent years as a new decentralised architecture and distributed computing paradigm that underpins Bitcoin and other cryptocurrencies. The main advantage of this technology is that it allows for the creation of secure, trusted, and decentralised autonomous ecosystems for a variety of scenarios, particularly for better utilisation of legacy devices, infrastructure, and resources.In the paper, Blockchain Technology and Cryptocurrencies by Siddharth Rajput, Archana Singh, Smiti Khurana, Tushar Bansal, Sanjukta Shreshtha [12],A blockchain can be referred to as a collection of open records that are shared with others parties. Each and every transaction that is included is first confirmed by each party to the transaction. Once the blockchain records the data, it can never be revised or modified. This paper includes history of bitcoin, a few literary reviews, working of the blockchain and its application. In the paper,

Blockchain: Future of financial and cyber security by Sachchidanand Singh, Nirmala Singh [4], This paper describes the concept, characteristics, and need for Blockchain, as well as how Bitcoin operates. It aims to highlight the significance of Blockchain in defining the future of banking, financial institutions, and Internet of Things adoption

(IoT).Blockchain is a decentralised ledger that is used to securely exchange digital currency and conduct business operations. Each network member has access to the most recent encrypted ledger copy in order to validate a new transaction. A blockchain ledger is a record of all Bitcoin transactions that have occurred in the past.

IV.CONCLUSION

The two most popular and valuable cryptocurrencies in existence today are Bitcoin and Ethereum. They are 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.

V. ACKNOWLEDGMENT

We would like to extend our gratitude to Project staff at the Sinhgad Academy of Engineering, Department of Computer Engineering and all other interns at the lab for their support and help without which this work could not have been accomplished. Additionally, we would like to give Prof. Sneha Shelke our project guide, our profound gratitude for leading us through the process.

REFERENCES

[1]. M. Marchesi, "'Why blockchain is important for programming designers, and why programming building is crucial for blockchain programming (Keynote),"' 2018 International Workshop on Blockchain orientating software system Engineering (IWBOSE), Campobasso, 2018, pp. 1-1.

[2]. Decisions in Economics and Finance (2021) 44:781–787 https://doi.org/10.1007/s10203-021-00366-3

[3]. D. Chaum, "Untraceable electronic main, return addresses, and digital pseudonyms," in Communications of the ACM, vol. 24, no. 2, pp. 84-88, February 1981

[4]. L. Law, S. Sabett, and J. Solinas, "How to make a mint: the cryptography of anonymous electronic cash," American University Law Review, vol. 46, no. 4, pp. 1131-1162, 1996

[5]. C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in 12th Annual International Cryptology Conference, pp. 139- 147, 1992

[6]. https://academy.binance.com/en/glossary/blockchain?utm_campaign=googleadsxacademy&utm_source=googleadwords_int&utm_medium=cpc&ref=HDYAHEES&gclid=Cj0KCQiA4OybBhCzARIsAIcfn9n89I1kLXkG3xGrl_de1LMQ_URuPjuuLV6ngZgCnjjPGzyST2EnnV0aAnYaEALw_wcB

[7]. WIKIPEDIA

[8]. https://www.geeksforgeeks.org/cryptography-in-blockchain/#:~:text=Cryptography%20is%20a%20method%20of,main%20concepts%20cryptography%20and%20hashing.

[9]. Eyal, I. (2017). Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities Computer MDPI AG 2. Popova, N.A., Butakova, N.G. (2019).

[10]. 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.

[11]. Y. Yuan, S. Member, and F. Wang, —Blockchain and Cryptocurrencies: Model, Techniques, and Applications, ‖ IEEE Trans. Syst. Man, Cybern. Syst., vol. PP, pp. 1–8, 2018.

[12]. Rajput, Siddharth, et al. "Blockchain technology and cryptocurrencies." 2019 Amity international conference on artificial intelligence (AICAI). IEEE, 2019.

[13]. U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, —A Brief Survey of Cryptocurrency Systems.

[14]. S. Singh, — Blockchain: Future of Financial and Cyber Security, ‖ pp. 463–467, 2016.

[15]. S. Nakamoto, —Bitcoin: A Peer-to-Peer Electronic Cash System, ‖ Www.Bitcoin. Org, p. 9,2008.