ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

A survey on Blockchain based cryptocurrency & an e-wallet

Pranav Waikar [1], Pratik Deshmukh[2], Rohan Patel[3], Aditi Kulkarni[4], Sudam Pawar[5]

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India[1]

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India[2]

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India[3]

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India[4]

Professor, Department of Computer Engineering, SITS, Narhe, Pune, India[5]

ABSTRACT: The regular currency has grown to reveal many drawbacks such as unavailability; it‘s proneness to be stolen and the fact that it is regulated strictly by an authority. Cryptocurrencies bypass most of our regular currency‘s drawbacks. Cryptocurrencies have emerged as a boastful financial system. They depend upon secure distributed ledger data structure. Mining plays an important part in this system. Mining helps add records of all past transactions to the ledger known as blockchain, which in turn allows users to have a currency with secure, robust consensus for every transaction that occurs in that block. Cryptocurrencies lack a central authority since they are designed as a peer-to-peer system. And every transaction has a record of it stored on every block thus eliminating any misuse. Basically, our cryptocurrency is a distributed database which maintains a growing tamper-proof data structure blocks which hold batches of individual transactions. The verified blocks are then added to the chain in a linear and chronological order. This forms a blockchain which is the core part of our cryptocurrency. A blockchain is a linear chain of Cryptocurrencies are the need of the future and they are helping shape the future of banking, financial institutions and the advent of the Internet of Things.

KEYWORDS: Blockchain, cryptocurrency, distributed ledger, wallets.

I. INTRODUCTION

The blockchain is an appropriated and decentralized record that stores information as exchanges and that is freely shared over every one of the hubs of its system. Presently let see what is a record, Ledger is a record that stores all the exchange of an association. The record is conveyed in the system. Each duplicate of the record is put away in this exchange book.

Blockchain innovation backs up Bitcoin and different digital forms of money right up 'til today, however, there's been an ongoing groundswell of enthusiasm from an assortment of ventures in making appropriated record innovation work, particularly in business. Here's an introduction on what blockchain innovation is, the means by which it works, and where it is demonstrating the most guarantee in the business. By outline, a blockchain is impervious to change of the information. It is "an open, dispersed record that can record exchanges between two gatherings effectively and in an evident and perpetual way Once recorded, the information in some random block can't be modified retroactively without change of every consequent block, which requires an agreement of the system lion's share.

In spite of the fact that blockchain records are not unalterable, blockchains might be viewed as secure by outline and embody a circulated processing framework with high Byzantine adaptation to internal failure. Decentralized accord has subsequently been asserted with a blockchain. Blockchain was developed by Satoshi Nakamoto in 2008 to fill in as the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

general population exchange record of the digital currency bitcoin. The development of the blockchain for bitcoin made it the principal advanced money to take care of the double spending issue without the requirement for a confided in power or focal server. The bitcoin systems have motivated different applications, and blockchains which are coherent by the general population are broadly utilized by cryptographic forms of money. Private blockchains have been proposed for business utilize. Some advertising of blockchains has been designated "a snake oil".
Paper is organized as follows. Section II describes background and current work. The Section III describes the problem definition in detail. Section IV describes the design & methodology for suggested problem definition with UML diagrams. Finally, Section V presents conclusion.

II. LITERATURE SURVEY

Sr no	Paper title	General idea	Advantages & limitations
1	Blockchain and Cryptocurrencies: Model, Techniques, and Applications [2018]	A survey of current cryptocurrencies to understand blockchain & its different types.	**Advantages:** Provides different incentive models, ecosystem & applications of the blockchain. Explains blockchain in a layered architecture. **Limitations:** Does not provide any solid architecture for its stated application.
2	A Brief Survey of Cryptocurrency Systems[2017]	It evaluates the strengths, weaknesses, and possible threats to all major mining strategy. It outlines how Cryptocurrencies mine, where they have comparable performance and assurance, and where they have unique threats and strengths.	**Advantages:** 1. Currently, major Cryptocurrencies use Proof of Work, Proof of Stake or a combination of the both for mining. 2. A combination of the both is found to be effective. 3. Typically memory-intensive hash functions have been found to be faster mining algorithms. **Limitations:** A majority of hash algorithms are CPU-intensive and the others are memory intensive. 2. While Proof of Work is resource intensive, Proof of Stake cannot act independently. 3. Cryptocurrencies are still experimenting with their mining protocols and algorithms to optimize their performance. No full proof algorithm has been found yet.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

3	Blockchain: Future of Financial and Cyber Security[2016]	This paper explains the concept, characteristics, need for Blockchain and how Bitcoin works. It attempts to highlights role of Blockchain in shaping the future of banking.	**Advantages:** 1.The decrease in device cost 2.Increases computing power **Limitations:** 1. If an attack was done by an attacker then there will be a loss of all bitcoins, we can't recover it because the government is not involved in
4	Bitcoin: A Peer-to-Peer Electronic Cash System[2008]	A distributed peer to peer system working under the blockchain framework	**Advantages:** Cryptocurrency without any central authority. Successful POW mechanism. **Limitations:** The cost of POW consensus protocol will keep increasing as more people join the network.
5	Trust Your Wallet : a New Online Wallet Architecture for Bitcoin [2017]	It introduces a wallet which is highly secured by Multiple signatures.	**Advantages:** The scalability of disaster recovery center **Limitations:** If we lost one of the keys then we are not able to recover that key.
6	A survey on the security of blockchain systems [2017]	Detail survey of the security issues in current systems and existing solutions	**Advantages:** A careful comparison between bitcoin and ethereum. Different aspects of system vulnerability **Limitations:** Cryptocurrency will need more methods to achieve security and privacy.

Table 1.1: Literature review

The above table 1.1 describes the literature survey. The table describes about the details about the paper with the general idea of the paper with its advantages & limitations. It helps to understand the workings of the current system & the limitations of the system which are required to overcome for betterment of the system. The next section defines the solution for the limitations.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

III. PROBLEM DEFINITION:

Aim:
To create a de-centralized blockchain based cryptocurrency and an e-wallet to access currency.

Problem statement:
1. Creating a crypto-currency with proof-of-authority but without a central point of failure.
2. Generalized public blockchain API.
3. A hybrid consensus protocol for blockchain.
4. A secure and high availability e-wallet for easy to facilitate transactions.

Objective:
The objective of this project to create a de-centralized blockchain based cryptocurrency and an e-wallet to access currency. The project entails creating a generalized blockchain API which can later be used for further development in the blockchain field of applications. This blockchain API will be used to construct a cryptocurrency from scratch. Implement a new hashing function for the blockchain which will take data and create a fixed length output. Implementing a highly secure and personal e-wallet system to access and control the said cryptocurrency. This e-wallet system will let the user control and transact the currency efficiently. It provides the user with full authority over the token currencies. The aim is also to make the currency secure, easy to access, fast and as cheap to avail as possible.

IV. PROPOSED ARCHITECTURE

As shown in figure 1.1, suppose party A wants to transfer some currency over to party B. Then by the wallet interaction, party A can start the transaction over to party B. The transaction is represented online as a block.
The block is then broadcasted to every party in the network. The network as a whole will approve the transaction to be valid or invalid by using the distributed ledger. Then by some consensus protocol block will get added to the distributed ledger. In this way, the transaction for transferring money from A to B is completed successfully.

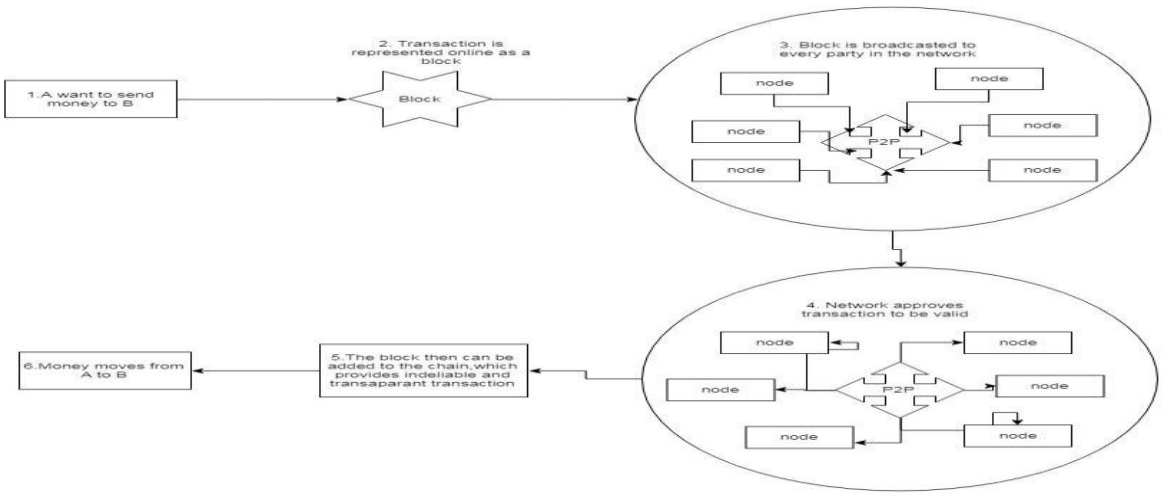

Fig 1.1 System architecture

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

Activity diagram:
In figure 1.2, user access wallet website and authenticate by referencing the database. After a successful login, the user can input transaction details and then start a transaction. The important details are verified with database and transaction is created in cryptocurrency network. The miners will then verify and validate the transactions. After that block gets added into blockchain. The changes are acknowledged by cryptocurrency model. The transaction details are recorded into the database. The result is displayed to the user by the wallet.

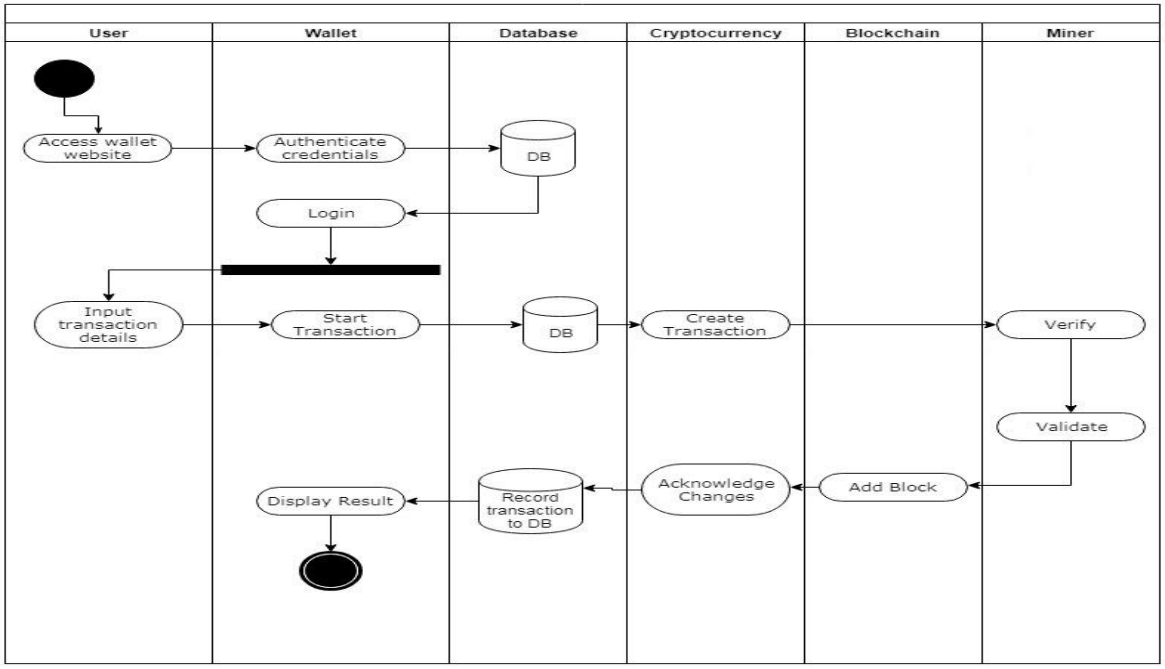

Figure 1.2 Swim lane activity diagram

Algorithms:

1. Secure Hashing Algorithm (SHA)-2:
The SHA version 2 provides various different hash functions with various output bit length & input. The SHA-256 is a novel hash function which works on 32bit words respectively. SHA-256 has ability work on x86 as well as x86-64 based architecture.

2. Consensus protocols:
The process of achieving single data value among the distributed or decentralized system is known as consensus protocol. The main goal is to achieve reliability in the system of unreliable nodes. These are also known as mining algorithms. The system will use a hybrid model of proof-of-work and proof-of-authority. The Proof-of-work uses a computational puzzle which needs to be solved by random guessing. Once the solution is found anyone can check the answer easily for authenticity. The proof-of-authority provides comparatively fast transaction through consensus mechanism of identity as a stake.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

3. Elliptic curve cryptography(ECC):
ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators, and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. [12]

4. Universally Unique Identifier (UUID):
UUID is also known as GUID. It is a 128-bit number used to identify information in computer systems. When generated according to the standard methods, UUIDs are for practical purposes unique, without depending for their uniqueness on a central registration authority or coordination between the parties generating them, unlike most other numbering schemes. While the probability that a UUID will be duplicated is not zero, it is close enough to zero to be negligible.[8]

5. Dynamic Difficulty mining algorithm:
Figure 1.3 shows the flowchart for dynamic difficulty mining algorithm. This algorithm is used to adjust the mining difficulty of the system automatically as per the specified mining rate. The difficulty parameter suggests how hard the hashing function should be for the proof-of-work algorithms.
The time difference between the last mined block and the newly mined block is compared with the specified mining rate. If the answer is less than the mining rate, the difficulty is increased. If the value is higher then the mining difficulty is decreased. This function is repeated for every new block inclusion into the system.

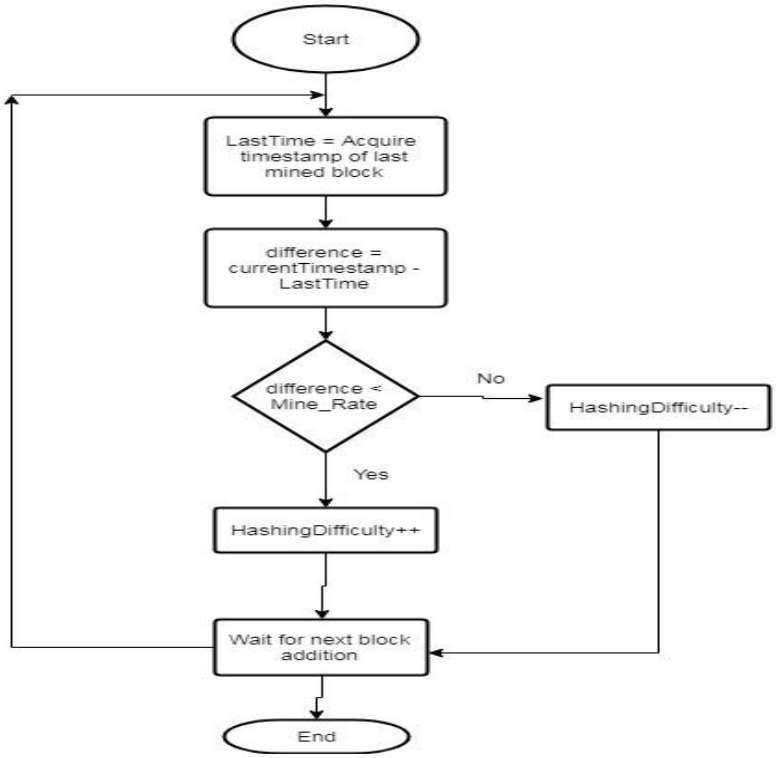

Fig 1.3: Dynamic difficulty mining

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

V. CONCLUSION

Thus, as we have already seen there is a need of a decentralized regulated transaction token or currency without a central point of failure. We have created a cryptocurrency from scratch which can be controlled using an e-wallet.
We have also created a generalized blockchain API which can further be used to develop applications in the blockchain domain. This purpose can be other than a cryptocurrency as well. A new hashing function was implemented to create fixed length output needed. The cryptocurrency is fast, secure and readily available. It implements a hybrid consensus protocol, meaning it combines two proofs to verify and validate transactions in the blockchain system, since PoW is expensive on the resources but not as good as PoS, PoA. Any transaction needs to be verified by miners like all the other prevalent cryptocurrencies. The difficulty of the function to be solved to verify transactions is set to be dynamic and is set such so that it does not cause either inflation or recession of the currency. The system is built as a peer-to-peer system, thus all the users depend on each other for the proper functionality of the system. An efficient data clean-up and detection mechanism has been implemented to improve the execution efficiency of blockchain systems. An e-wallet which is secure, fast and highly accessible has been implemented which can be used by the user to interact and control the cyrptocurrency. This e-wallet creates a public as well as private key bind to the user which can be used in various transactions over the currency.

REFERENCES

[1] 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.
[2] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, ―A Brief Survey of Cryptocurrency Systems.‖
[3] S. Singh, ― Blockchain: Future of Financial and Cyber Security,‖ pp. 463–467, 2016.
[4] S. Nakamoto, ―Bitcoin: A Peer-to-Peer Electronic Cash System,‖ Www.Bitcoin.Org, p. 9,2008.
[5] F. Zhu et al., ―Trust Your Wallet: a New Online Wallet Architecture for Bitcoin,‖ 2017.
[6] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, ―A survey on the security of blockchain systems,‖ Futur. Gener. Comput. Syst., 2017.
[7] R. Lai and D. LEE Kuo Chuen, Blockchain – From Public to Private, 1st ed., vol. 2. Elsevier Inc., 2018.
[8] http://www.wikiwand.com/en/Universally_unique_identifier
[9] https://hackernoon.com/types-of-consensus-protocols-used-in-blockchains-6edd20951899
[10] https://en.wikipedia.org/wiki/SHA-2
[11] https://en.wikipedia.org/wiki/Blockchain
[12] https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
[13] https://en.wikipedia.org/wiki/Cryptocurrency
[14] https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/
[15] https://coinsutra.com/future-of-bitcoin-cryptocurrency-india/