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. 8, Issue 5, May 2019

A Blockchain based Cryptocurrency & the Development of 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 blockchain technology underlying the cryptocurrencies have the potential to be the future of finance. It can revolutionize the way all transactions works today. The underlying blockchain technology can provide a solid base for a fully autonomous system that could govern. Its potential is not just about the transactions with the cryptocurrency but can extend far beyond that. cryptocurrencies are cryptographically secure, publically owned by user & highly available. The regular currency has grown to reveal many drawbacks such as unavailability, Cryptocurrencies bypass most of our regular currency's drawbacks. They depend upon a secure distributed ledger data structure. Mining helps add records of all past transactions to the ledger known as the blockchain, which in turn allows users to have a currency with secure, robust consensus for every transaction that occurs in that block. Our cryptocurrency is a distributed database which maintains a growing tamper-proof data structure blocks which hold details 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.

KEYWORDS: Blockchain, cryptocurrency, distributed ledger, e-wallets.

I. INTRODUCTION

The blockchain is a transaction database which has information about every transaction ever executed in the past and works on the Bitcoin protocol. It creates a digital ledger of transactions and allows all the participants on the network to edit the ledger in a secure way which is shared over a distributed network of the computers For making any amount of changes to the block of data, all the nodes present in the network run algorithms to evaluate, verify and match the transaction information with its history. If the majority of nodes agree in favor of the transaction, it is approved and a new block gets added to the existing chain. In this, we are using (SHA-256) genetic algorithm to secure the chain. Every block contains a hash of parent block in its own header and the sequence of hashes linking individual block with their parent block creates a big chain pointing to the first block called Genesis block. The term private blockchain (permissioned ledger) refers to Blockchain that requires authentication of participant identities and authorization of participant's permission-level of access on the Blockchain This writing will use Private Blockchain to refer to Permissioned Ledger as well. The term public blockchain (permissionless ledger).Mining validates transactions and adds them to this public ledger. When a new transaction takes place, the miner checks if the currency belongs to the payer, or if the payer is trying to double spend. The resource-intensive task can be any of the following: Proof of Work, Proof of Stake, or Proof of Retrievability.

Paper is organized as follows. Section II describes related work. Section III describes the problem definition. Section IV describes the implementation. Section V describes the testing and result. Finally, Section VI presents the conclusion.

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. 8, Issue 5, May 2019

II. RELATED WORK

no	Paper title	General idea	Advantages	Limitations
1	Blockchain and Cryptocurrencies: Model, Techniques, and Applications [2018]	A survey of current cryptocurrencies to understand blockchain & it's different types.	Provides different incentive models, ecosystem & applications of the blockchain.	Does not provide any solid architecture for its stated application.
2	Blockchain: Future of Financial and Cyber Security[2016]	This paper explains the concept, flows, need for Blockchain and Bitcoin works.	The decrease in device cost and Increases computing power.	If an attack was done by an attacker then there will be a loss of all bitcoins.
3	Bitcoin: A Peer-to-Peer Electronic Cash System[2008]	A distributed peer to peer system working under the blockchain framework.	Cryptocurrency without any central authority.Successful POW mechanism.	The cost of the POW consensus protocol will keep increasing as more people join the network.
4	Trust Your Wallet : a New Online Wallet Architecture for Bitcoin [2017]	It introduces a wallet which is highly secured by Multiple signatures.	The scalability of the disaster recovery center.	If we lost one of the keys then we are not able to recover that key.
5	A survey on the security of blockchain systems [2017]	Detail survey of the security issues in current systems and existing solutions.	A careful comparison between bitcoin and ethereum. Different aspects of system vulnerability.	Cryptocurrency will need more methods to achieve security and privacy.

Table 1. 1: A Literature review [1]

The table above represents the literature review. It explains the paper name with its general idea with some advantages and limitations derived.

III. PROBLEM STATEMENT

To create crypto-currency with proof-of-authority but without a central point of failure by creating generalized public blockchain API with a hybrid consensus protocol for blockchain as well as a secure and high available e-wallet for easy to facilitate transactions. [1]

IV. IMPLEMENTATION

The Blockchain: The fig below represents the flowchart for the operation of the blockchain based systems. At the time of the creation of blockchain, the first block ie genesis block is added into the chain. To add subsequent blocks, new data accepted from the user. The last block of the chain is acquired & hash & difficulty fields are extracted from it. The default nonce value is zero. The current timestamp is then acquired. The SHA256 hash is generated taking data, nonce, difficulty, last hash, timestamp as an input. The condition for POW consensus protocol is the generated hash value should have a prefixed number of zeros equal to the difficulty level. The POW is like solving the computational puzzle. Till the desired condition is achieved, the nonce & timestamp changes & every time a new hash value is generated. After a successful attempt, the value is stored as a hash of that block & block is added at the end of the chain. Refer to figure 1.1.

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. 8, Issue 5, May 2019

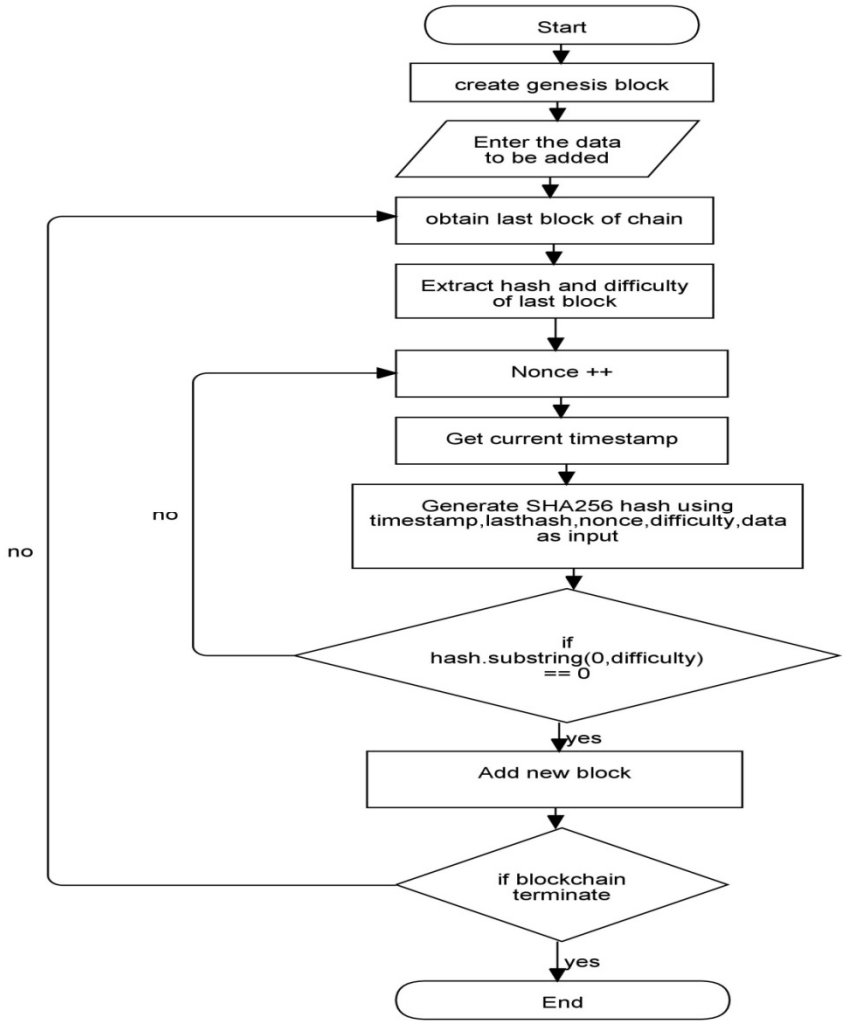

Fig 1.1: Blockchain flowchart

The cryptocurrency: The cryptocurrency model uses the blockchain technique to store & manipulate the data of transactions. The cryptocurrency model facilitates the creation & mining of transactions. The model allows sharing the transaction with multiple miners so that they could try to mine simultaneously & the one who wins will receive the reward. Also, the transaction data is shared between multiple nodes among those.

Creating a transaction: The algorithm is used to create a new transaction or update an existing transaction. The fig below shows the flowchart for the same. The balance is calculated first to verify the user has needed appropriate balance. If the balance is not enough then the transaction is not created. If the balance is enough then it is checked whether transaction already exists or not. If a transaction already exists then it is updated & updated transaction is broadcasted into the network. If the transaction does not exists then a new transaction is created with its UUID, the remaining balance is calculated and added as data of the transaction. The sender & recipient address, balance, amount & signature data used to create a new transaction. The transaction is broadcasted to the network using the transaction pool. Refer to figure 1.2.

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. 8, Issue 5, May 2019

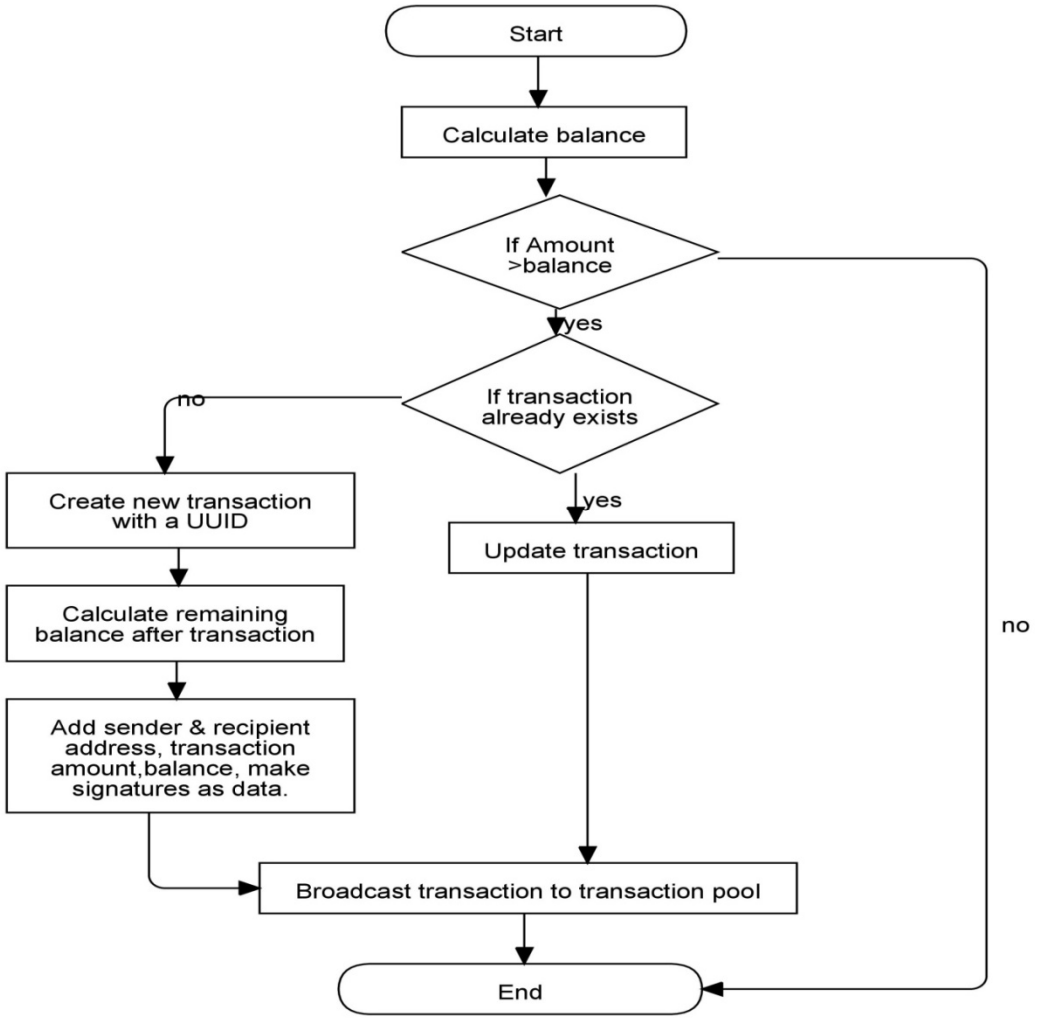

Fig 1.2: Transaction creation flowchart

Mining transactions: The algorithm is used to mine a transaction of the user from the transaction pool. The transaction is acquired from the transaction pool & the output amounts are calculated again for the validity. If invalid then it is rejected. If valid then the digital signature is checked for the correctness using the transaction data & public key of sender wallet. If invalid then the transaction is rejected. Mining starts using POW consensus protocol if valid.
After that reward transaction for a miner is created. All this information stored in the block then added to the blockchain. This newly added block is broadcasted over the network.

The wallet: This is the general flow of the wallet server. The wallet server first generates a proof-of-authority (POA) digital signature. The POA signature is then verified. If verification is successful wallet server is initialized otherwise terminated. In this way, the online wallet service will always be verified. After successful verification, the wallet server is started at the determined port. On that specific port, the server starts providing services to different clients. Refer to figure 1.3.

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. 8, Issue 5, May 2019

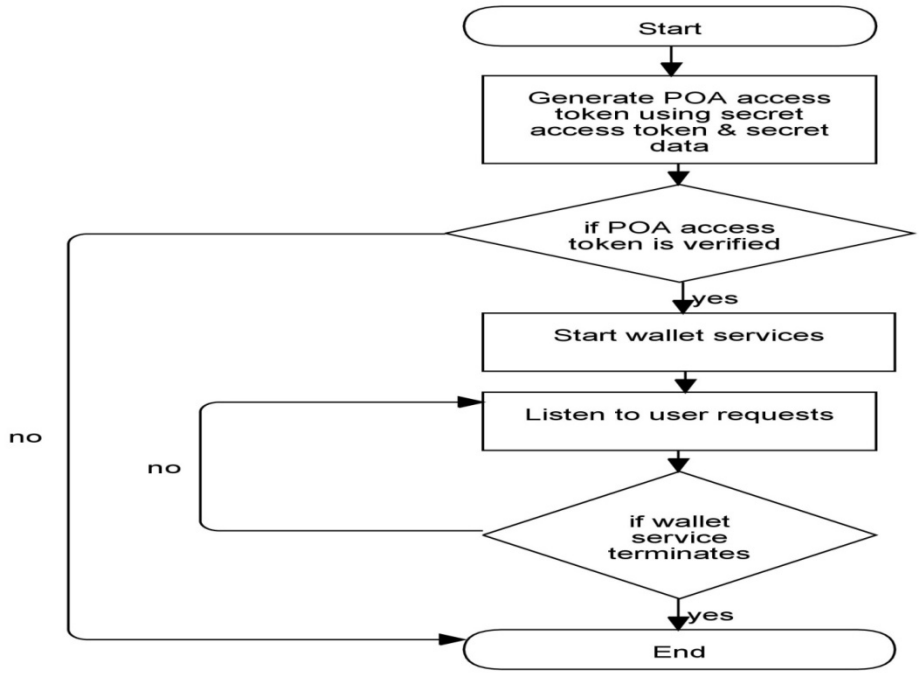

Fig 1.3: wallet flowchart

V. TESTING AND RESULTS

Performance testing: The memory space taken by each block affects performance as it is directly related to bandwidth parameters of the network. In this case each block measures around 100kb in size. It means each transaction upon adding into blockchain will consume 100kb space in memory over all the connected nodes. Another performance measure for a cryptocurrency is a number of transactions per second(TPS). Because of POW algorithm, TPS can be different for different machines. Refer to table 1.2.

Srno	Processor	RAM	TPS rate
1	Intel Core 2 Duo E7500	2 GB	100
2	Intel Core i3-8100	4 GB	106
3	Intel Core i3-6100	4 GB	103
4	Intel Core i7 7700K	8 GB	110
5	Intel Xeon E5-2686 v4 (Broadwell)	16 GB	119

Table 1. 2: Transaction rates

Acceptance testing: Acceptance testing can be done via various methods. Here online survey method is used. An online survey is a structured questionnaire that your target audience completes over the internet generally through a filling out a form.

The category of users: The figure below depicts that the majority of users entrusted with testing the system were naïve. A fair part i.e. about 24% was beginners and the remaining was fairly competent in using such software. Refer to figure 1.4.

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. 8, Issue 5, May 2019

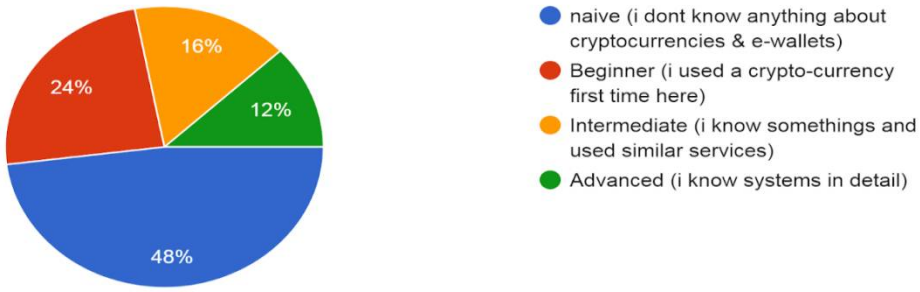

Figure 1.4: Category of users

Error occurrence in the system: The majority of users did not encounter any errors while navigating the system. 96% of users were satisfied with the experience of the system. Refer to figure 1.5.

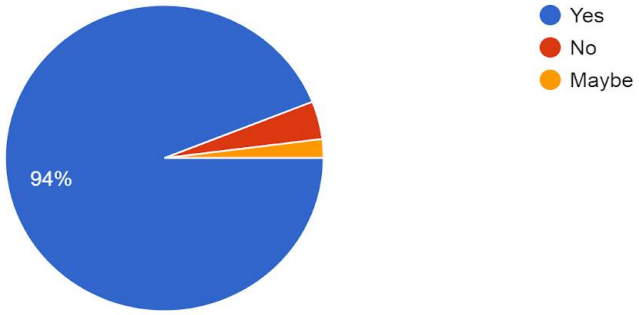

Figure 1.5: Error occurrence

Preferred key management policy: As expected, a majority of users chose the automatic KMS policy. While a fair share chose to have a recoverable passphrase for their operations. A minority of users opted to not save private key any form. Refer to figure 1.6.

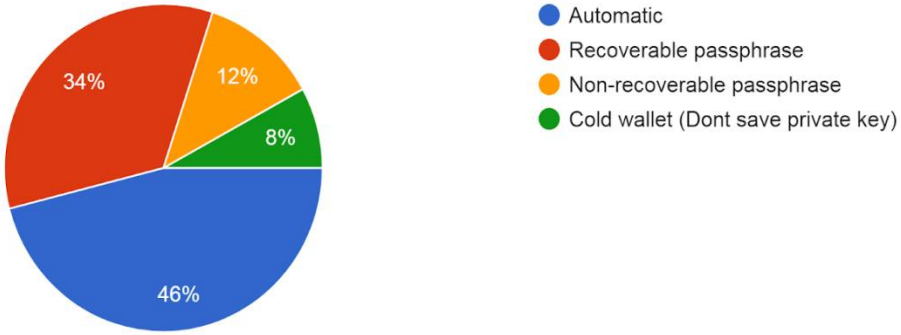

Figure 1.6: Preferred KMS

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. 8, Issue 5, May 2019

Ease of use: A whopping 94% of users found the website very easy to use. Refer to figure 1.7.

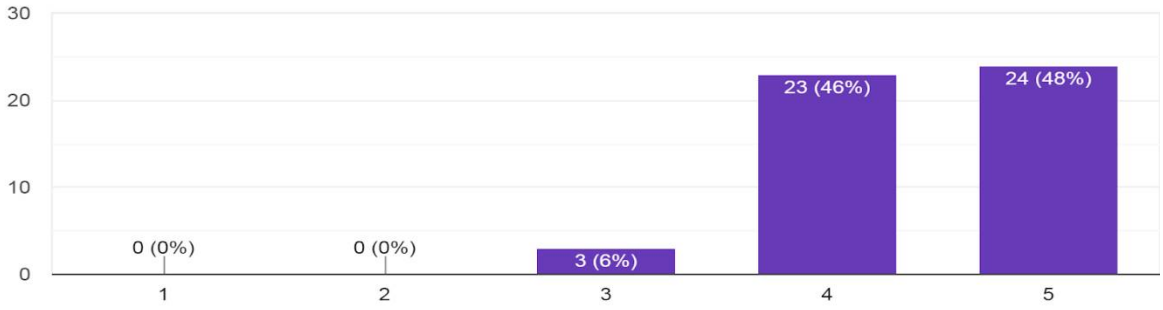

Figure 1.7: Ease of use

Overall satisfaction: Almost all the users were satisfied with their experience when using the website. Refer to figure 1.8.

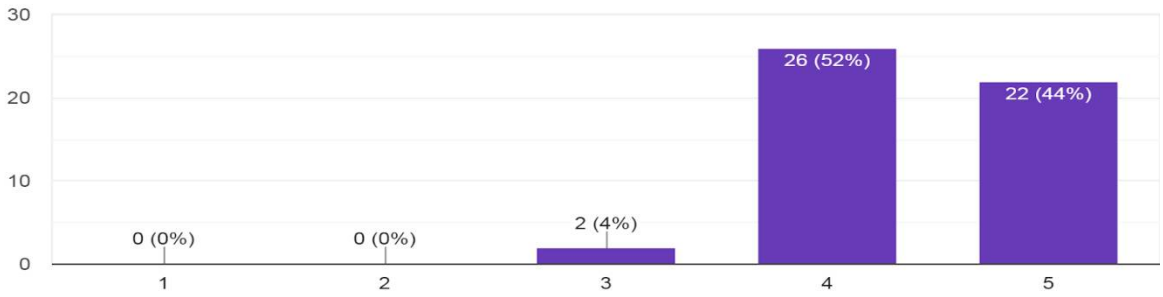

Figure 1.8: Overall satisfaction

Recommendation to other users: Among all the users who were entrusted with testing the website, a major part of them would happily recommend it to others. Refer to figure 1.9.

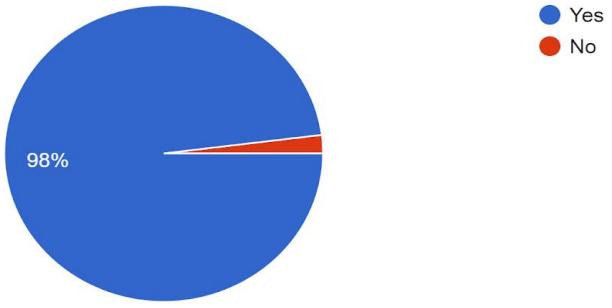

Figure 1.9: Recommendation to others

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. 8, Issue 5, May 2019

Outcome: The outcomes of the project are as following:

- A generalized blockchain API was created which could be used to create various project models like voting systems, cryptocurrencies, etc.
- A cryptocurrency model was created using the blockchain API with higher security, robustness, and availability.
- An e-wallet was designed with reference to the cryptocurrency model to access and control the currency transactions.
- The system was deployed over the cloud platform, which showcased reliable speed, performance, and scalability of the system.

VI. CONCLUSION

Thus, "A Blockchain based cryptocurrency & development of an e-wallet" project led to development on a generalized blockchain API, with the help of which a new cryptocurrency model was implemented along with the development of an e-wallet so as to access the said currency. The main objective of the project was to create a new blockchain based cryptocurrency model which was more secure, robust and faster than the current cryptocurrencies in the market. The cryptocurrency model was implemented along with a website acting as an e-wallet to access the currency. The users were then asked to review the website which revealed the usefulness of the address book and Key Management policies (KMS). This report is a detailed document of the methods used in the implementation of the project along with the relevant theory and practical. It also contains all the testing scenarios, their results, and relevant data. This document can be considered for improvement to the cryptocurrency models or the API's used to create them. Our cryptocurrency model is robust, faster, secure and adaptable compared to the current cryptocurrency models in the market which make it a highly viable alternative. The e-wallet with its KMS and address-book also will surely help even the naïve users to easily make effective use of the e-wallet.

REFERENCES

[1]P. Waikar, P. Deshmukh, R. Patel, A. Kulkarni, and S. Pawar, "A Survey on Blockchain based Cryptocurrency & an e-Wallet," pp. 10271–10277, 2018.
[2] 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.
[3] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, ―A Brief Survey of Cryptocurrency Systems.‖
[4] S. Singh, ― Blockchain: Future of Financial and Cyber Security,‖ pp. 463–467, 2016.
[5] S. Nakamoto, ―Bitcoin: A Peer-to-Peer Electronic Cash System,‖ Www.Bitcoin.Org, p. 9,2008.
[6] F. Zhu et al., ―Trust Your Wallet: a New Online Wallet Architecture for Bitcoin,‖ 2017.
[7] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, ―A survey on the security of blockchain systems,‖ Futur. Gener. Comput. Syst., 2017.
[8] R. Lai and D. LEE Kuo Chuen, Blockchain – From Public to Private, 1st ed., vol. 2. Elsevier Inc., 2018.
[9] http://www.wikiwand.com/en/Universally_unique_identifier
[10] https://hackernoon.com/types-of-consensus-protocols-used-in-blockchains-6edd20951899
[11] https://en.wikipedia.org/wiki/SHA-2
[12] https://en.wikipedia.org/wiki/Blockchain
[13] https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/
[14] https://coinsutra.com/future-of-bitcoin-cryptocurrency-india/
[15] https://github.com/pranavwaikar/cryptocurrency