Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 6, Issue 3, March-2019

ANONYMIZE AND SECURE DECENTRALIZED TRANSACTIONS IN BITCOIN-LIKE DIGITAL CASH SYSTEM USING BLOCKCHAIN

Mrs.D.Murugeswari[1], Gayathri.M[2], Sandhya.B[3],Gayathri.M.S[4]
1.Asst professor , 2.UG Scholar, 3.UG Scholar, 4.Asst professor

Abstract- A pure peer-to-peer version of electronic money would sanction online payments to be sent directly from one party to another without going through a financial institution like bank. Digital signatures provide part of the solution, but the main benefits are disoriented if a trusted third party is still required to avert double-spending. To avoid double-spending and lack of time, Block chain technology is used. Main aim is to cover the security and privacy aspects of bit coin.

Keyword:Blockchain,Bitcoin,cryptocurre-ncy,Ethereum,Network formation, Bitcoin transfer, Tracking system.

I. INTRODUCTION

Commerce on the net has come back to believe nearly completely on monetary establishments serving as trusted third parties to method electronic payments. While the system works to a tolerable degree for most transactions, it still suffers from the inherent weaknesses of the trust primarily based model. Completely non-reversible transactions aren't very potential, since money establishments cannot avoid mediating disputes. Merchants should be cautious of their customers, has sling them for a lot of data than they'd otherwise want. A certain share of fraud is accepted as in escapable.

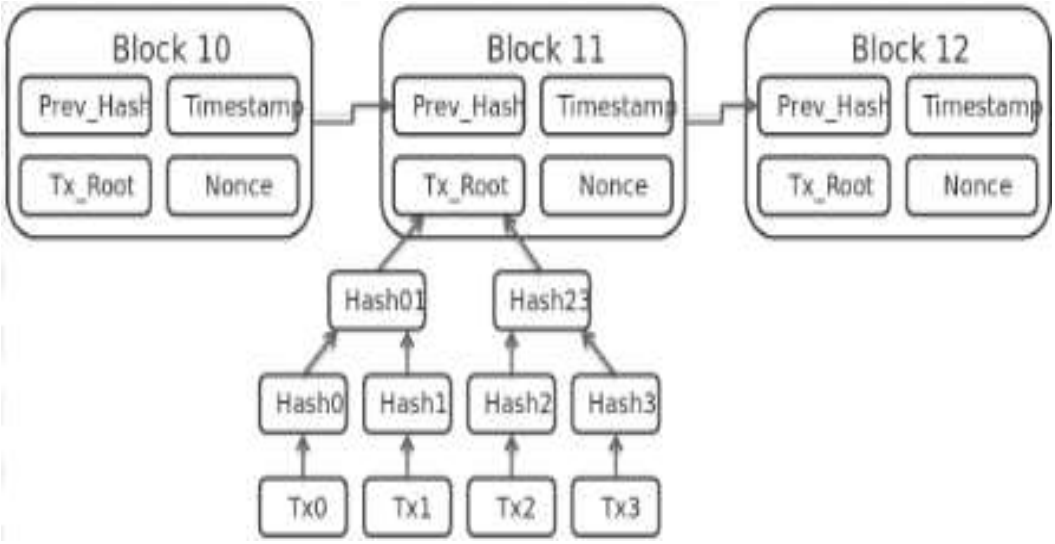
In this paper, we have a tendency to propose an answer to the double-spending drawback employing a peer-to-peer distributed timestamp server to get procedure proof of the written account order of transactions. The system is secure as long as honest nodes put together management a lot of electronic equipment power than any cooperating cluster of aggressor nodes.

II. LITERATURE SURVEY

Satoshi Nakamoto projected the network timestamps transactions by hashing them into an current chain of hash-based proof-of-work, forming a record that cannot be modified without modifying the proof-of-work. JonathanChiu,ThorstenKoeppl planned a general equilibrium financial model is developed to study the optimum design of a cryptocurrency system supported a block chain. The model is then graduated to bitcoin transaction data to perform a quantitative assessment of the scheme. We tend to formalize the critical parts of a cryptocurrency. Alex Kroeger planned bitcoin could be purely on-line virtual currency, single-handed by either physical commodities or sovereign obligation; instead, it depends on a mix of cryptographical protection and a peer-to-peer protocol for witnessing settlements.

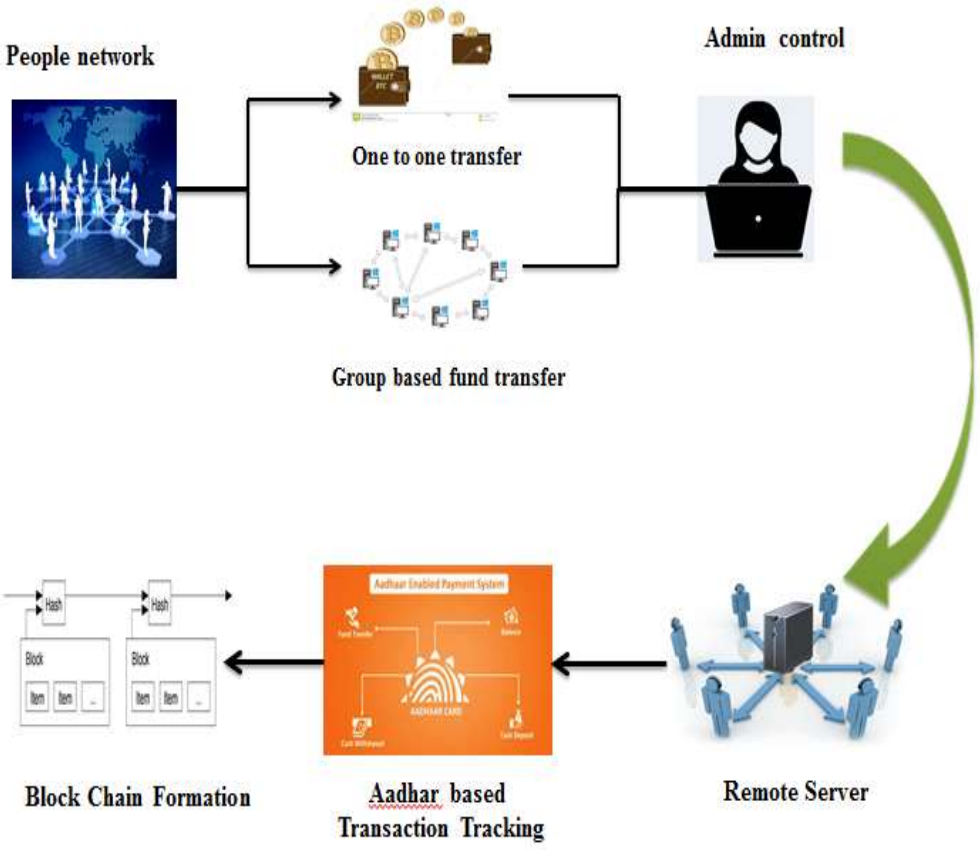
III. TECHNIQUES

- Blockchain is a platform with a scripting language that can explain many use cases other than simple digital forms of money. This property of Blockchain prompted brilliant contracts, an advancement introduced by the cryptographic money known as Ethereum.
- The development of the Blockchain for bitcoin made it the primary computerized money to unravel the twofold spending issue without the need of a confided in power or focal server.
- A worldwide system of PCs utilizes Blockchain innovation along with the information that records Bitcoin exchanges.
- That is, Bitcoin is directed by its framework, and no central master.
- Decentralization implies the system works on a consumer (or distributed) premise.



IV. PROPOSED SYSTEM AND BLOCK DIAGRAM

Digital cash will be transferred through cryptocurrency called Bitcoin. We implement Block chain technology for the implementation of cryptocurrency. Every transactions will be monitored by the Remote Server.



A. MODULES

1. GROUP FORMATION

- In this module Group construction is formed and members are registered in the network.
- Group Admin is assigned to monitor the entire activity of the group.
- One to one Bitcoin based money transformation is processed through this group. The group formation is done by using SHA-256 and Ethereum tools.
- Group leader holds the complete control of the group.
- New member addition or Removal of existing member will be processed by the Group admin only after the approval from all the group members.

- If group admin wants to exit from the group then admin has to assign one another member as Group admin and then that Group Admin is allowed to exit from the group. Unique private keys are generated for every registered participants.

2. Group Governance

- The group admin initially creates the group with username and passwords with the constants “admin”. The admin only has the privilege to govern the backend by using MySQL.
- New user can be introduced by any member, request is processed by the admin and finally that member is added after getting approval from all the members.

- If suppose member A wants to transact digital cash to member B, then member A is required to specify sender A's private key.
- At the receiver end B, the encrypted data will be decrypted using A's public key by B. Entire activity can be parallelly goverened by the remote server.

3. Banking Registration

- All the members will be registering their Bank details for banking purpose.
- All these recorded are stored in the network database securely.
- None of the users can view the banking details of the other users.

4. Digital cash Transfer

- Every exchange is resolved with its hash value speaking to an exchange identifier and a lot of information sources and yields.
- Each yield of the exchange must be utilized once as a contribution to the whole blockchain
- The endeavor of referencing a similar yield twice prompts the twofold spending issue and is illegal in the system. On the off chance that the yield of the exchange hasn't been referenced previously, it is called an unspent exchange yield (UTXO), and on the off chance that it has been referenced, it is known as a spent exchange yield (STXO).
- An exchange can have numerous inputs and just up to two yields. Numerous information sources can be utilized to join littler measures of coins being exchanged, and yields can be either a sum sent to the next gathering or the change that is sent back to the sender.
- All the details will be stored dynamically in the Database Server.

5. Tracking System

- In this module, Banking system is completely tracked through the centralized main server.
- This server holds complete control of the banks of all the users in that network.
- Search by address or by transaction ID. Complete money based Bitcoin transaction is tracked through this module.

V. CONCLUSION

Bitcoin and Ethereum today are the most known and important digital currencies. They depend on blockchain innovation that is proposed to advance a trust instrument in a distributed system dependent on the accord of most of the hubs.Thus the project infer that in the existing system tracking bitcoin transaction is challenging one.So we use blockchain to secure the transaction details.

REFERENCES

[1]Bitcoin: A Peer-to-Peer Electronic Cash System,Author: Satoshi Nakamoto.
[2]The Economics of Crypto currencies Bit coin and Beyond,
Author:Jonathan Chiu,Thorsten Koeppl.
[3]Essays on Bitcoin ,Author: Alex Kroeger.
[4]A Fistful of Bitcoins: Characterizing Payments Among Men with No Names
Author:SarahMeiklejohn Marjori..
[5] SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies
Author: Joseph Bonneau_yz, Andrew Millerx, Jeremy Clark, Arvind Narayanan_, Joshua A. Kroll_, Edward W. Felten.

[6]Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, Kyung-Hyune Rhee," A Critical Review of Blockchain and Its Current Applications", published in International Conference on Electrical Engineering and Computer Science (ICECOS) 2017.
[7]Fthi Arefayne Abadi_, Joshua Elluly and George Azzopardi," The Blockchain of Things, Beyond Bitcoin: A Systematic Review", published in Conference Paper · July 2018.
[8]Rainer Böhme, Nicolas Christin,Benjamin Edelman, and Tyler Moore,"Bitcoin: Economics, Technology, and Governance", published in Journal of Economic Perspectives—Volume 29, Number 2—Spring 2015.