International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 07 | July 2020 www.irjet.net p-ISSN: 2395-0072

Blockchain based Peer to Peer Money Transfer using Cryptocurrency Digital Wallet

Shashidhar M.R

4th sem M.Tech, SJBIT, Poornima M Associate Professor Department of CNE, SJBIT

ABSTRACT - Peer to Peer money transfer in Application with blockchain architecture is a general approach to transfer money within a small group of peers who lend, completely and transfer money from one person to another in e-wallets. Money transfer in the blockchain is inescapable soon as it entails non- repudiation, security, transparency, preserves anonymous of users with Homomorphic encryption and the inherent tamper-proof nature of the distributed ledger of the blockchain makes it more resilient and robust. The transactions of all the peers are recorded in distributed ledger stored in real-time cloud database Firebase with Homomorphic encryption.

Digital money deals with various issues in physical cash, for instance, the broad fake banknotes. Also, to build stock to utilized money significantly less complex, in this paper, we propose and send an Ethereum combination oversight system called blockchain put together disseminated money move subordinate concerning to blockchain development with database item stores. The basic initial outcomes by methods for the remarkable certain automated wallet of Testnet Ethereum show the proposed blockchain-based conveyed money move can cost-sufficiently assemble portion and manage the trades among clients and products executed NFC-engaged Application.

I. INTRODUCTION

Blockchain, a decentralized architecture with a tamper-proof, append-only log of transactions, non-repudiation has gained immense popularity and is a disruptive technology for all Fintech operations that involve transactions. With a blockchain, clients can put down passages into an account of data, and a network of clients can control how the record of data is changed and refreshed. The dispersed database made by blockchain innovation develops as the quantity of exchanges increments and is cryptographically secure. The most unmistakable and significant highlights of blockchain technology. Authentication and approval, crucial to advanced exchanges, are set up since they are the quintessential component of blockchain innovation.

The transactions by blockchain are slow and are nowhere near the VISA which handles 50,000 transactions per second, but this android app can be suited for small peer to peer members who do transactions like the women self-help groups, where the need for ledger maintenance is considerably reduced here every participant keeps an entire copy of the blockchain.

It is a trustless, decentralized network with the transparency of transactions. The usage of cloud application (third-parties) i.e. Firebase a real-time database, as part of our blockchain implementation, might be vulnerable to attackers, and data mining operations of sensitive data might be carried out by third-party cloud service providers. To avoid this data to be stored in firebase is encrypted using homomorphic encryption. Double Spending of digital currency is one of the major concerns in blockchain Transactions. This violation may take down the entire blockchain and may lead to the forking of blocks. Since blockchain is a blooming-technology which is still in its proof of Concept and pilot stages, there is no assurance for refunding of digital money. By chronologically ordering the transactions and validating them, the double-spending attack has been cleverly avoided in our proposed method. Since Mobile nodes are limited to performance constraints, it takes high time to do everything with peer-to-peer technology. Blockchain-based peer to peer money transfer for exchanges among clients and product stores who utilize the inescapable Ethereum computerized wallet. All trade nuances can be cost-reasonably got a good deal on Cloud Database straightforwardly after clients utilize their NFC empowered android wireless application to buy RFID named items in-stock store. Clients and shippers can survey these trade nuances lacking bothers referenced before the standard budgetary framework.

II. SYSTEM DESIGN

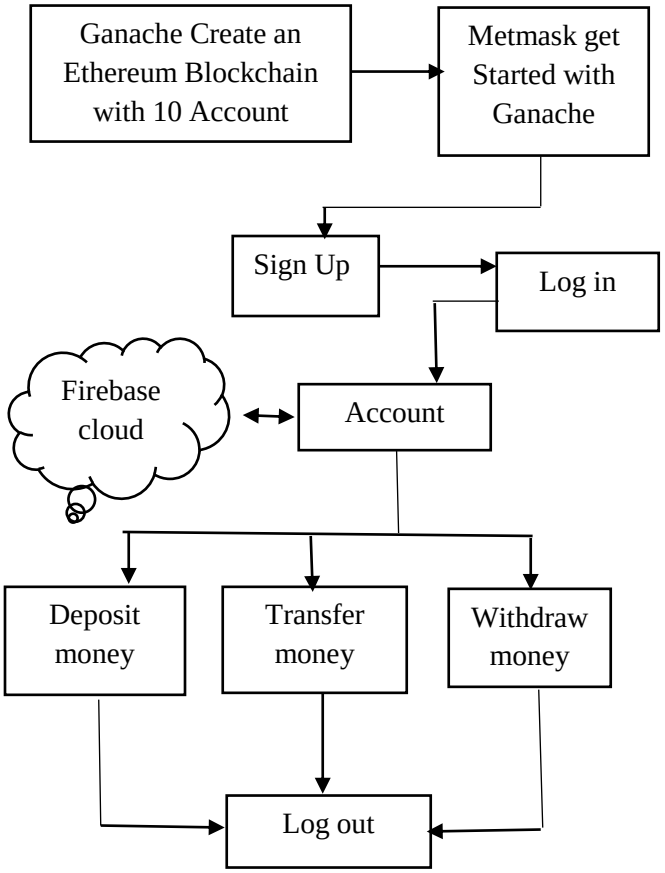

Figure: Block diagram of System Design

In this architecture depicts the block-chain based peer to peer money transfer using Ethereum currency, it's a secure way for the transaction in the above figure the user first log in using username, email, mobile number and they have to fill the account details also hereafter sign up he souses to login to the application. There they create an account he can deposit the money, withdraw can also possible and he can do transaction for another account after that he can log out from the application.

III. METHODOLOGY

Real-time database creation with Firebase The implementation is done in Firebase and Android Studio bundle 3.3. Google's Firebase which is a constant database has its information in JSON group and the information is shown, synchronized over the entirety of its customers, web customers, or versatile customers. The user of this app has to sign in and register their details like name, mobile number, and password. The login phase needs the user to log in to the details of the mobile number and pin number and login to the mobile application.

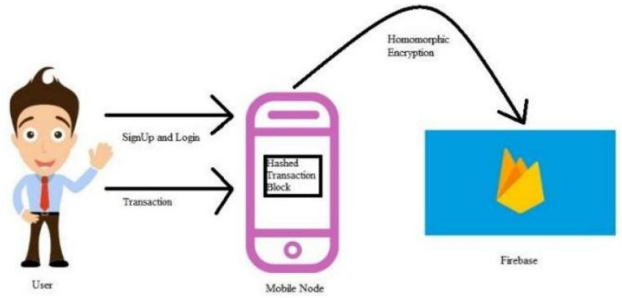

Figure: Firebase architecture

The blocks of each user, the number of users, and the transactions of the user are put away in the Google firebase, a real-time database Firebase, the cloud database has details of the group of users who wants to do their transactions in this Mobile-chain with the other registered users. The firebase has user details like his name, his phone number, and pin number. The user details are validated and entered or else the users are asked to enter proper values. The Digital signature is used for secure transactions in which every client has a couple of keys, the private key, and the open key. The sender node signs the transaction and broadcasts it to other users. The receiver node will sign with his private key to get the transaction details and also broadcast it to other users. Proof of work consensus mechanism is used which requires all the nodes to participate in block generation and verification process. The Mobile Wallet application, they contain four modules they are Signup module, Login module, edit Contactor updating of details module, and Transaction Module.

The square of every client with the hash evaluation of the square, Merkle root, the nonce, hash estimation of the past square, the time stamp appeared in a long number is illustrated. The Merkle root which has the hash of the considerable number of exchanges underneath, which will empower new clients to download the exchanges. If a new user downloads the Blockchain and if the transactions are broken during the download phase, the user can utilize the Merkle tree for downloading the transactions. Proof of work consensus is reached here where a transaction is validated by more than 51% of users in this peer to peer network. By chronologically ordering the timestamps of the transactions, the double-spending attack is carefully avoided, and thus forking of the chain is also prevented. There is no such implementation of the Meta mask wallet in Mobile Applications, so we have devised this method. Meta mask which is used for validating transactions in permissionless

blockchains (Ethereum) and decentralized applications has not been implemented in mobile applications.

The user details like the username, the mobile number of the user are encrypted and stored in firebase with our Android app. The number of transactions of each user, from whom they have got money and with who they have transacted money are also shown in encrypted form. Thus the anonymity of the payer and the payee are maintained by this app. The user details and the encrypted details are shown. The user validity of the chain is checked and shown in Log cat and the transaction details of a successful transaction, the public key of the user.

Homomorphic encryption is a form of encryption where the computation can be done in ciphertext that yields the same result as when it is done in normal data. The information that is put away in distributed storage by the clients can be put away utilizing homomorphic encryption that yields for security and protection saving highlights. If the cloud services provider or any anonymous person if he wants to perform data mining operations, he can do it in encrypted data and not in the real data. Thus it is a privacy-preserving decentralized application.

IV. IMPLEMENTATION

The working of block-chain based peer to peer money transfer using cryptocurrency it's a secure way for the transaction.

Implementation steps are:

1. First to sign up an account user must fill the following information like username, email, mobile number, adhar number, phone number and photo of user to open a new account,
2. After Signup, the user login to the account using the user Id and password.
3. After Sign in, the user enters to account and the user can deposit the amount to the account.
4. Once the user deposit user can log out or return to the account dashboard.
5. One more option is to withdraw can also possible,
6. Once user withdraw user can logout or return to account dashboard
7. The last option in this application is the transfer amount to another account also.
8. Every Transaction is viewed in the transaction field.
9. After his transaction user can logout from the account.

V. RESULTS

Figure: Signup-Collect All the Information Needed To Open A New Account

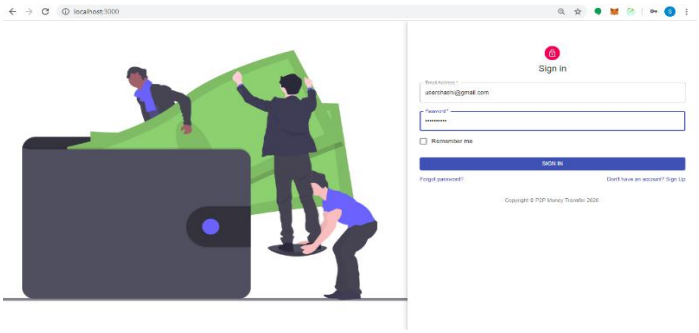

Figure: Sign-in-Login to the Account Using the User Id and Password.

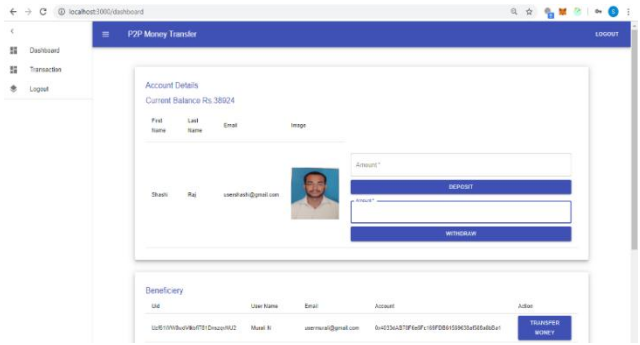

Figure: Account Dashboard

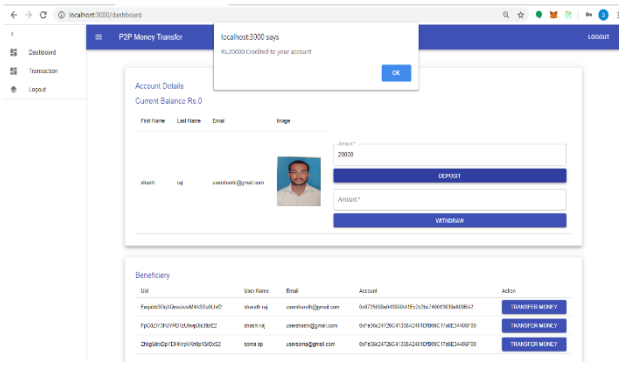

Figure: Deposit amount to Account

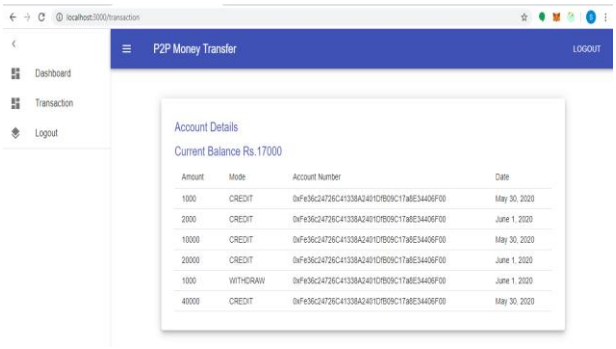

Figure: Transaction Details - of deposit, Withdraw and Transfer Money

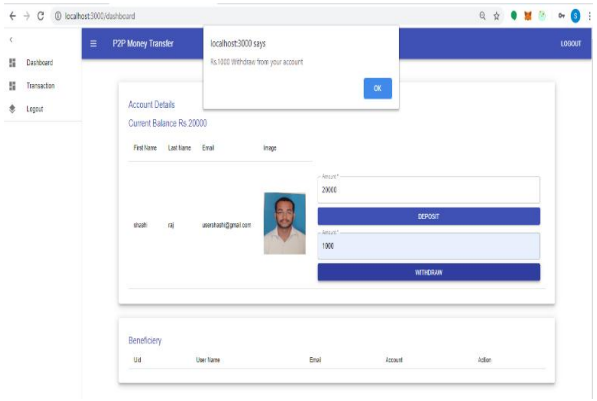

Figure: Withdraw -Amount Withdraw from Account

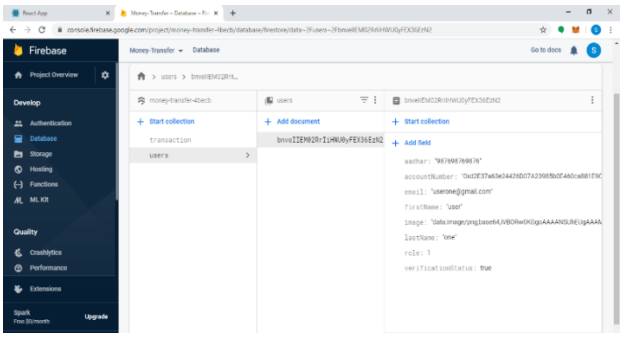

Figure: User Details in Firebase

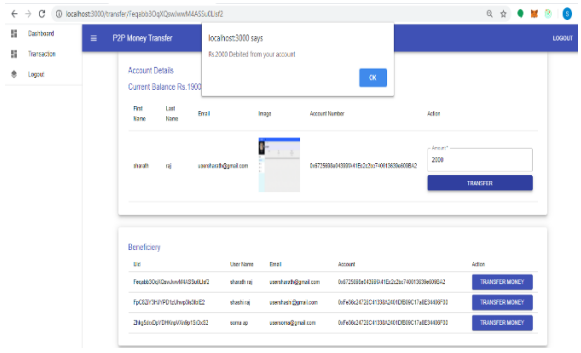

Figure: Transfer Money-Amount Debited from Account

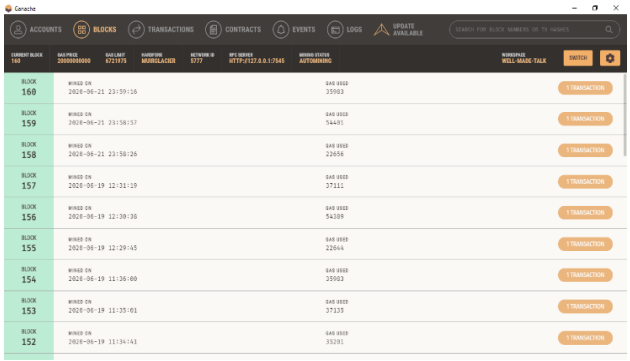

Figure : Data is Stored as Blocks in Ganache

Ganache makes a square on request, if you send in any event one exchange Ganache makes a square. That squares cannot be erase or adjust. If anyone attempt to change the square, adjust square is made as another square.

Blockchain stockpiling is a manner by which the information is put away in a square arrangement, which accesses the client's hard circle to search for space to store the information. This decentralized stockpiling structure was acquainted as an option with brought together distributed storage.

VI. CONCLUSION

In this Project blockchain-based shared cash move not just for clients and shippers who individually spend and win advanced money. Additionally, the underlying aftereffects of computerized cash exchange tests, utilizing the well-known general advanced wallet of cryptographic money and cloud databases, exhibit the protected cost-viability in computerized money exchanges and oversight among payer and payee in proposed blockchain-based distributed cash move. The proposed blockchain-based distributed cash move design additionally incorporates the accompanying qualities:

- Equipped for the following execution continuously thus bringing superb cost investment funds.
- Purchasers' exchange records can't be erased.
- Purchasers are as yet mysterious to guarantee the security of individual data.
- On the off chance that purchasers have inquiries regarding the exchange to request, they have to introduce the exchange receipt or demonstrate that entrance right of the location of the payee.
- All exchange data are open and straightforward.

The main trade information is noted by the blockchain advancement, with high-level constancy the de-united and the untampered information. The favorable circumstances of proposed a blockchain-based shared cash move are summed up as follows:

- For shoppers: The exchange information is open and straightforward, so the rights and interests of buyers are secured. Since the exchange is tenable and has a clear timestamp. At the point of purchasers required to offer their exchanges to their customer right, they can progressively successful and tenable evidence from the proposed framework.
- For Business: Businesses can do measurements and counts for their employment plans dependent on all digital exchange data. This can decrease the blunders in registering results from manual activity. The measurable information can be joined with stores stock administration to make merchandise and assets in expected parity, to additionally establish the employment in bookkeeping exactness and work cost.
- For Government: During the time spent settling the exchange contest, progressively tenable proof can be accommodated reference. The computerized exchange receipts additionally can take care of the issue of the paper getting dummy or lost.

Sooner rather than later, we will outfit usage of oversight capacities for Government monetary administrative part. Particularly, we require a practical method to upgrade safety and security insurance in getting to cloud databases for clients, stores, and a monetary administrative part.

VII. REFERENCES

[1] H. Kuzuno and C. Karam, "Blockchain explorer: An analytical process and investigation environment for Ethereum," APWG Symposium on Electronic Crime Research (eCrime), Scottsdale, AZ, Published on 2017, pp. 9-16.

[2] Tian, Feng. "An agri-food supply chain traceability system for China based on RFID & blockchain technology." Service Systems and Service Management (ICSSSM), International Conference on. IEEE, Published on 2016.

[3] Ali, Muneeb, et al. "Blockstack: A Global Naming and Storage System Secured by Blockchains." USENIX Annual Technical Conference, Published on 2016.

[4] Larimer, D., N. Scott, V. Zavgorodnev, B. Johnson, J. Calfee, and M. Vandeberg "Steem: An incentivized blockchain-based social media platform,". Published on 2016

[5] Buba, Zirra Peter,and Gregory Maksha Wajiga. "Cryptographic algorithms for secure data communication." International Journal of Computer Science and Security (IJCSS), Published on 2011, pp.227-243.

[6] Stapleton, Jeff, and Ralph Spencer Poore. "Tokenization and other methods of security for cardholder data." Information Security Journal: A Global Perspective 20.2, Published on 2011,pp 91-99.

[7] Swan, Melanie, "Blockchain: Blueprint for a new economy," O'Reilly Media, Inc.", Published on 2015.

[8] Szydlo, Michael. "Merkle tree traversal in log space and time," International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg", Published on 2004.

[9] Grinberg, Reuben. "Ethereum: An innovative alternative digital currency."Published on 2011.

[10] Gilbert, Henri, and Helena Handschuh. "Security analysis of SHA-256 and sisters", Selected areas in cryptography. Springer Berlin/Heidelberg, Published on 2004.

[11] Fox, Geoffrey. "Peer-to-peer networks." ,Computing in Science & Engineering , Published on 2001 pp. 75-77.

[12] Preibusch, Sören, et al. "Shopping for privacy: Purchase details leaked to PayPal," Electronic Commerce Research and Applications, Published on 2016, pp. 52-64.

[13] Antonopoulos, Andreas M, "Mastering Ethereum: unlocking digital cryptocurrencies," O'Reilly Media, Inc.", Published on 2014.

[14] Mathieu, Florian, and Ryno Mathee. "Blocktix: Decentralized Event Hosting and Ticket Distribution Network," (2017), https://blocktix.io/public/doc/blocktix-wp-draft.pdf

[15] Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine general's problem," ACM Transactions on Programming Languages and Systems (TOPLAS), Published on 1982, pp. 382-401.

[16] Gervais, Arthur, et al. "Is Ethereum a decentralized currency?" IEEE security & privacy 12.3, Published on 2014, pp. 54-60.

[17] Buterin, Vitalik. "Ethereum network shaken by blockchain fork." Ethereum Magazine 12 (2013).

[18] Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things." IEEE Access 4 (2016): 2292-2303.

[19] Buterin, Vitalik. "Ethereum white paper." (2013), https://github.com/ethereum/wiki/wiki/White-Paper

[20] Noether, Surae. "Review of CryptoNote white paper," http://monero.cc /downloads /whitepaper _review.pdf.

[21] González, Andrés Guadamuz. "PayPal: the legal status of C2C payment systems," Computer law & security review 20.4(2004): 293-299.

[22] Ortiz, C. Enrique. "An introduction to near-field communication and the contactless communication API," Oracle Sun Developer Network. Retrieved on Jun 30 (2008): 2010.

[23] Karame, Ghassan O., Elli Androulaki, and Srdjan Capkun. "Double-spending fast payments in Ethereum." ACM conference on Computer and communications security. ACM, Published on 2012.