INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

Decentralized secure money transfer using blockchain

Suganya T.
suganya.t@skct.edu.in
Sri Krishna College of Technology, Coimbatore, Tamil Nadu

Vignesh A.
skct.15tucs250@gmail.com
Sri Krishna College of Technology, Coimbatore, Tamil Nadu

Vignesh Kumar N.
15tucs251@skct.edu.in
Sri Krishna College of Technology, Coimbatore, Tamil Nadu

Vivin Kumar D.
15tucs260@skct.edu.in
Sri Krishna College of Technology, Coimbatore, Tamil Nadu

ABSTRACT

A block chain is just a chain and a list of blocks. Each block, in the block chain, will have its own digital signature. Each block doesn't just contain the hash of the block, but its own hash in part, calculated from the previous hash Calculating and comparing the hashes allow us to see if a block chain is invalid. We create a system that Allows users to create wallets and Provides wallets with public and private keys using Elliptic-Curve cryptography. Secures the transfer of funds, by using a digital signature algorithm to prove ownership and finally allow users to make transaction your block chain

Keywords— *Blockchain, Netbeans, MySql*

1. INTRODUCTION

Block-chain is the backbone Technology of Digital Crypto-Currency Bit-coin. The block-chain is a distributed database of records of all transactions and digital events that have been executed and shared among the participating users. Each transaction is verified by the majority of participants of the system. It contains, every single record of each transaction. Bit coin is the most popular crypto-currency an example of the block-chain. The bitcoin is a crypto-currency and it is used to exchange digital assets online. Bit-coin uses cryptographic proof instead of third-party trust for two parties to execute transactions on the internet. Each transaction protects through digital signature.

There is no Central Server or System which keeps the data of Block-chain. The data is distributed over Millions of Computers around the world which are connected with the Block-chain. This system allows checking of Data as it is present on every Node and is publicly verifiable. A block is a data structure that contains all the necessary metadata about the block (Block Header) itself and contains the transactions. The first block in a block-chain is called genesis block.

The Block chain may be defined as a chain of the block that contains the information. This technique is intended to timestamp digital documents so that it's not possible to backdate them or temper them. The block chain is used for the secure transfer of items like money, property, contracts, etc without requiring a third-party intermediate like bank or government. Once the data is recorded inside a block chain, it is very difficult to change it. Block chains could not be run without the Internet. The node is a computer connected to the Block-chain Network. A chain of blocks that contains some metadata about the block, some transactions and joined to the block by the previous block's hash value.

Node gets connected with Block-chain using the client. Client helps in validating and propagates transaction on to the Block-chain. When a computer connects to the Block-chain, a copy of the Block-chain data gets downloaded into the system and the node comes in sync with the latest block of data on Block-chain. The Node connected to the Block-chain which helps in the execution of a transaction in return for an incentive is called Miners.

2. LITERATURE SURVEY

The purpose of this paper is to create a list of blocks each block to connect the previous block to some previous key to connect to find the next key to-do the transaction. V Dinh, Tien Tuan Anh, et al. "Untangling block-chain: A data processing view of block-chain systems.

"IEEE Transactions on Knowledge and Data Engineering 30.7 (2018): 1366-1385.
This project highlights some public versus private block-chains to create some multiple nodes it is not fully trusted. Some global states are modifying the states. The block-chain is to connect to the previous block-chain.

Dinh, Tien Tuan Anh, et al. "Block bench: A framework for analyzing private block chains." Proceedings of the 2017 ACM International Conference on Management of Data. ACM, 2017.
This project about the public block chain like some bitcoin and

highlights ethereum this public block chain enable peer to peer application.

Untangling Blockchain: A Data Processing View of Blockchain SystemSystems. Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang∗, Member, IEEE, Gang Chen, Member, IEEE, Beng Chin Ooi, Fellow, IEEE, and Ji Wang 2018.

In recent years block, chain concept has played had played a major role in improving security. In this world we cannot trust anyone to set and maintain the global states, in this paper s surely on the state of art and focusing on private block chain is done.

3. EXISTING SYSTEM

Since the traditional banking services provide technology which is lagging behind the pace of technology. The upcoming banking technologies are simply laid upon this technology to support providing banking services online or through mobile devices.

This means that the huge share of the money goes to the operational status of these systems and not to introduce innovations. This while the old technologies are still operating and creaking with age. Block chain allows different parties that do not trust any other to share information without requiring a central administrator. Transactions are processed by a network of users serving as a consensus mechanism so that everyone is creating the same shared system of record simultaneously

The Principle of Block chain of the virtual currencies created over the recent decade, bitcoins are arguably the most popular worldwide.

4. PROPOSED SYSTEM

4.1 Preparing a Wallet

In crypto-currencies, coin ownership is transferred on the Block chain as transactions, participants have an address which funds can be sent to and from. In their basic form wallets can just store these addresses, most wallets, however, are also software able to make new transactions on the Block chain.

4.2 Transactions and signatures

Each transaction will carry a certain amount of data. The public key of the sender of the fund. The public key of the receiver of the fund.The value/amount of funds to be transferred. Inputs which are references to previous transactions that prove that the sender has some funds to send.Outputs, which shows the number of relevant addresses received in the transaction.A cryptographic signature, that proves the owner of the address is responsible for sending this transaction and that the data is not changed. (for example: preventing no rights for the third party from changing the amount sent).

4.3 A block chain is a chain of blocks connected to each other.

4.3.1 Hash and Previous Hash: A hash is a function that converts an input of letters and numbers into an encrypted output of 64-bit combination. A hash is created using an algorithm, and it is essential to block chain management in crypto currency. Hashing means taking an input string of any length and giving out an output of a fixed length (64 bit). In the context of crypto currencies like Bit coin, the transactions are taken as an input and run through a hashing algorithm (Bit coin uses SHA-256) which gives an output of a fixed length.

Hashing method requires processing the data from a block through a mathematical function, which results in an output of a fixed length. Using a fixed length output increases security since anyone trying to decrypt the hash not be able to tell how long or short the input is simply by looking at the length of the output.

4.3.2 Cryptographic hash functions: Cryptographic hash function is a special function which uses a hash function method and its various properties of ideal view of cryptographic. There are certain properties that use a cryptographic hash function method that needs to have secure considerations.

It means that there is no matter how many times you parse through a particular input through a hash function that you will always get the same result every time. It is very critical because if you get different hashes single time it is impossible to keep track of the input. A small change in your input will be reflected in the hash with huge changes in the result. It is tested with SHA-256. The first alphabet of the input will totally affect the output hash. This is a critical function because this property of hashing leads to one of the greatest qualities of the block chain, its immutability (more on that later). The two different inputs A and B are H(A) and H(B) which are respective their hashes, it is infeasible for H(A) to be equal to H(B). It means is that for the most part of each input will have its own unique hash.

4.3.3 Timestamp: Timestamps will displays that the blocks are connected in chronological order. It stores the time for every single transaction on the block chain. The process of keeping tracking of the creation securely and modification the document and it is an indispensable tool used for the business world. It allows the interested parties to know about the document, without having a doubt, which a document question exists at a particular date and time. Bit coin transaction includes a date and time, which held on the Block chain. It includes a cryptographic digest of a file which you can later certify the data existed at that time. Place the timestamp, block chain and its tamper-proof. Timestamp plays to the role a notary, and it's more credible than a traditional one. A timestamp is considered as valid input that if it is greater than the median timestamp of previous 11 blocks, and less than the network-adjusted time is + 2 hours. As a result, block timestamps will not be exactly accurate, and it must not need to be in order. Block times are accurate only within an hour. Whenever a node is connected to another node, it will get a UTC timestamp from it, and it stores the offset from node-local UTC. The network-adjusted time is the node-local UTC plus that the median offset is connected to all the nodes. Network time will not be adjusted more than 70 minutes from local system time. Bit coin uses an unsigned integer for the timestamp.

4.4 Overview

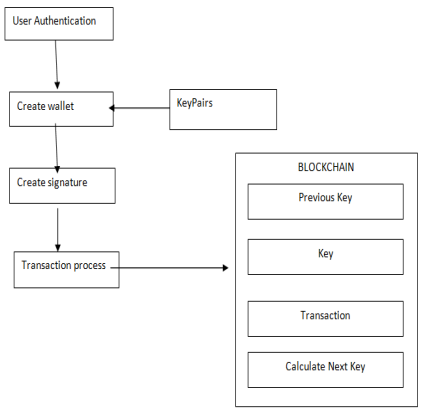

Fig. 1: Block diagram of the flow process

The block diagram explains the flow of the process in this paper. First, a ID is created to the user and the user is given with four key. While the user is undergoing into any transaction the user has to enter the four key. The movement from one key to another key is stored in the node of the first key. In this way, the four key get transferred and the transaction will get completed successfully.

5. BLOCK DIAGRAM

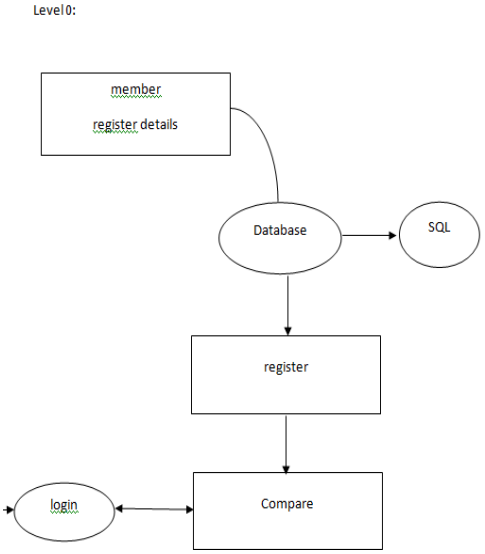

Fig. 2: Block diagram

6. OUTPUT AND EXPLANATION

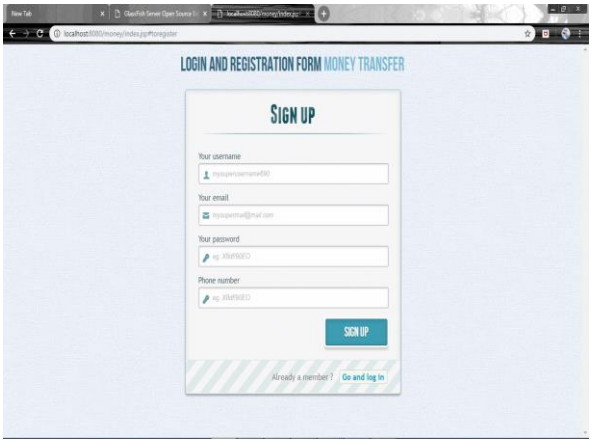

Fig. 3: Sign up page

It is used to get the information about the user and the user who register only have access to login in the sign in page. After signing up it automatically stores the information of the user in the database.

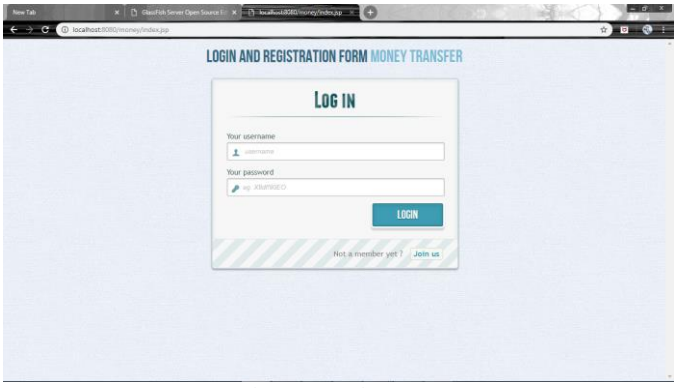

Fig. 4: Login page

Once the user gets registered in the sign-up, he gets access to login. And he user name and the password is verified with the database and when the user is registered user, then the user's account is signed in. When the user is not registered he cannot able to log in without registration. After getting the sign in login page welcome page will be displayed.

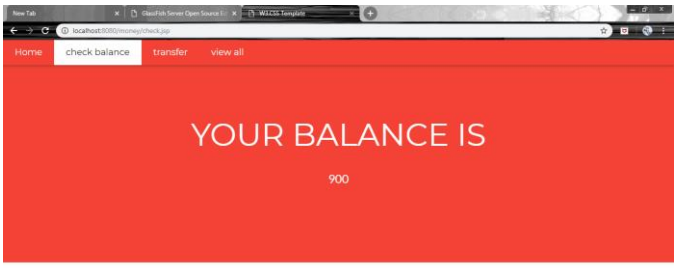

Fig. 5: Balance page

Once login in the page it shows the balance amount of the user that is stored in the wallet will be displayed in balance page.

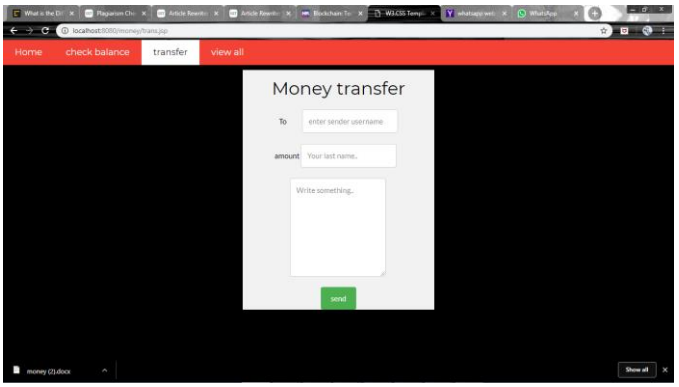

Fig. 6: Money transfer page

Once the user transfer the amount to another account the transaction process of the user gets converted into 64 bits and the money is transferred using block chain concept

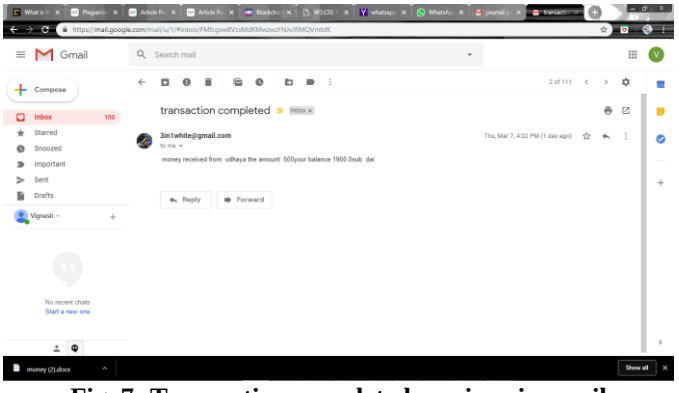

Fig. 7: Transaction completed receive via email

For additional security purposes an email is sent with OTP (One Time Password) this OTP is used for further transaction processes.

7. CONCLUSION AND FUTURE WORK

This project concludes that money transfer will be securely stored in the block chain. In this type of block chain, all user will know every transaction. It must be decentralized transfer No third party included in this transaction. The beautiful web page also is shown to the transaction of money. Block chain

technology provides the transformation of to the individual parties and entities, to transfers value of money to unassurance parties, by trusting the block chain technology. By using the block chain technology method, the participating parties can be confident about transferring amount at both ends of the agreement will be upheld and the transfer values will be agreed upon are attainable.

8. REFERENCES

[1] R. E. Anderson et al., "Experiences with Transportation Information System that Uses Only GPS and SMS," IEEE ICTD, No. 4, 2010.

[2] D. Risi, M. Teófilo, "MobileDeck: Turning SMS into a Rich User Experience," 6th MobiSys, No. 33, 2009.

[3] Kuldeep Yadav, "SMSAssassin: Crowdsourcing Driven Mobile-based System for SMS Spam Filtering," Workshop Hotmobile, 2011, pp. 1-6.

[4] J. Chen, L. Subramanian, E. Brewer, "SMS-Based Web Search for Low-end Mobile Devices," 16th MobiCom, 2010, pp. 125-135.

[5] B. DeRenzi, "Improving Community Health Worker Performance through Automated SMS," 5th ICTD, 2012, pp. 25-34.

[6] Raskin, Max, and David Yermack. Digital currencies, decentralized ledgers, and the future of central banking. No. w22238. National Bureau of Economic Research, 2016.

