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 using blockchain

Dr. S. Gunasekaran
gunaphd@yahoo.com
Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu

Dr. G. Ravi Kumar
rgrtvr2007@yahoo.co.in
Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu

S. Nirmal Balaji
nirmalbalaji.cse@gmail.com
Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu

Gokul R.
gokulramalingam@gmail.com
Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu

R. Mahilan
mahilan022@gmail.com
Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu

Pooja M.
poojapamy@gmail.com
Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu

ABSTRACT

The blockchain is a decentralized transaction and managing the data. This technology introduced on the first for Bitcoin cryptocurrency which makes easier for the transaction. Blockchain technology has highly raised up in 2008. The main purpose of the Blockchain technology is to provide security, anonymity and data integrity without any third party organization in control of the transactions. This helps on improving in research areas especially from the perspective of technical challenges and limitations. In this research, we have conducted survive mapping study with the goal of presenting the Blockchain technology. The main objective of the researchers is to make the challenges in understanding the current research areas. This the future way to developing more and more on Blockchain technology. A blockchain is just a chain and list of blocks which secures the transfer of funds, by using a digital signature algorithm to prove ownership. Each block in the blockchain will have its own digital signature. We create a web page that contains the login and registration page. We create a key pair of each user that contains the private key and public key. Every time we check this blockchain is valid or not. The main reason for the paper is to research and focus on revealing and improving limitations of Blockchain from privacy and security perspectives. On the basis of this studying the blockchain we highly recommend the researchers to develop in the future.

Keywords— *Blockchain, Cryptocurrency, Transaction, Security, Data integrity, Anonymity, Peer-to-peer computing Ethereium*

1. INTRODUCTION

Currency transactions between persons or companies are often centralized and decentralized happens controlled by the miner in the organization. Whenever we make a digital transaction currency transfer requires a bank to complete the transaction. In addition, whenever there a money transaction there is some percentage of money goes to the bank like 2%. That single transaction causes a fee from a bank and if there is millions of transaction per day the bank earns lots of money through single clicks. This type of process applies also in several other domains, such as software, downloads etc. The transaction system is typically decentralized, all the data and information is not managed by any third party this leads to P2P.two principal entities involved in the transaction.

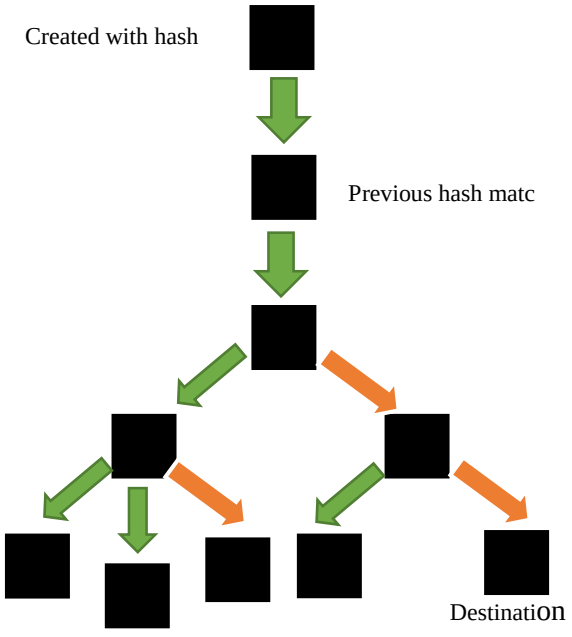

Fig. 1: Simple Blockchain transaction

The blockchain is a distributed database solution that maintains a continuously growing list of blocks that contains certain hash messages which the entire record of the block is confirmed and validated allows the nodes participating in it. The total blocks and data will be maintained by the public ledger it includes the information of each and every transaction until the process completes. The blockchain is a decentralized solution which does not depend on the miner or third party organization in the middle of a transaction.

The information of all the transaction is completed by Blockchain and shared available to all blocks. In addition, the blocks in Blockchain are all anonymous which is secured for other blocks to confirm the transactions. Bitcoin will generate a decentralized better environment for the cryptocurrency, where the parties can buy and exchange goods (give and take policy) with digital money.

With no issue though Blockchain seems to be suitable for transactions by using bitcoin BTC or cryptocurrencies, leading a technical challenge and limitations that need to be proved. High integrity of transactions will provide the privacy to prevent attacks and attempts to disturb transactions in Blockchain. Blockchain has further computational power it conforms and validated. The resulted map of current research on Blockchain will help further researchers for identifying and finding out with the possible result. we take part in finding Blockchain research topics related to various technical areas, such as scalability, data integrity, performance privacy, and security. The main objective is to find and map all papers with technical viewpoints related Blockchain.

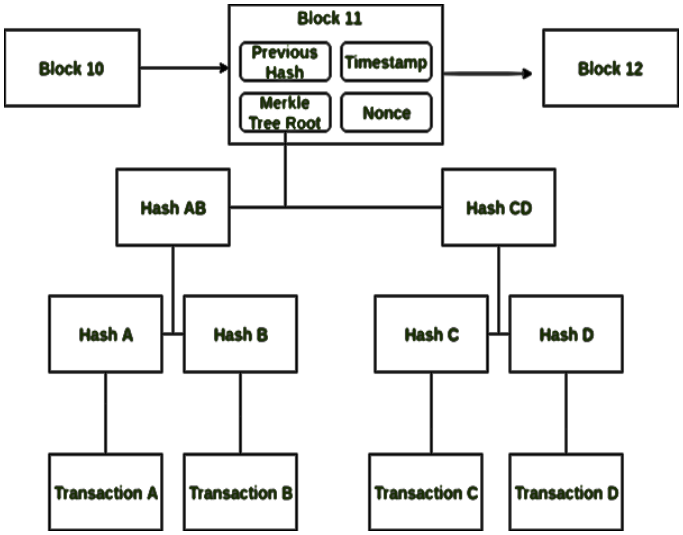

Fig. 2: Hash Key distributed transaction

2. EXISTING SYSTEM

Traditional financial services providers, banks, in particular, are lagging behind the pace of technology development. Newer computing technologies are simply laid on top of this foundation to support providing banking services online or via mobile devices. This means that the greater share of the money goes to support the operational status of these systems, and not to introduce innovations. But, the old technologies are still in operation, and creaking with age.

2.1 Disadvantage of the existing system

If the Hacker is aware of the pin in the traditional banking system, the risk of being hacked is comparatively higher. If the proper network is not provided or if the website crashes due to multiple issues, the accuracy and efficiency is not up to the mark and hence is not safe for transferring of large amounts of currency. The transfer, exchange, success, failure and other factors are all handled by a single organization which is a burden in the case of system failures.

2.2 Bitcoin

Bitcoin is the type of digital currency which is maintained by the new type of digital currency. Bitcoin is also known as the cryptocurrency. It's not maintained by a central bank or single organization it was done by user choice peer to peer bitcoin without any interconnected networks.

Symbol: ฿

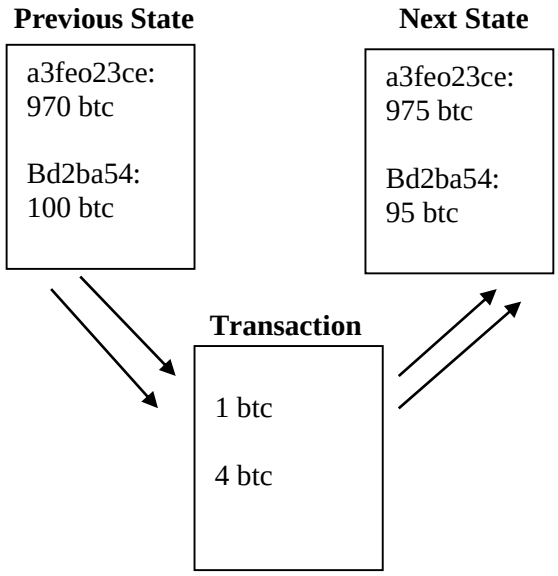

Fig. 3: BTC Transaction sender and Receiver

3. PROPOSED SYSTEM

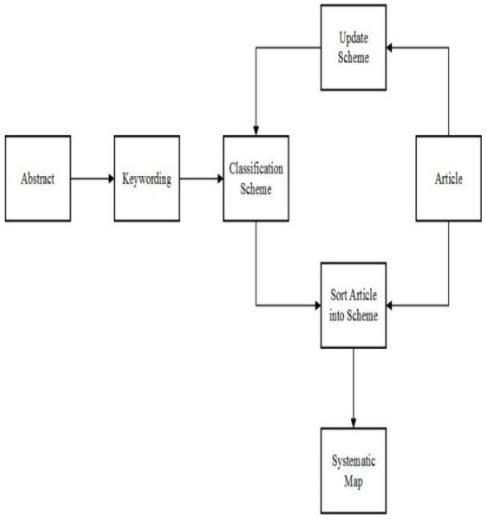

Fig. 4: Authentication updated

Users are allowed to create their own wallets so that they do not have to depend on third-party wallet providers. They provide digital wallets which are paid and have a limited period of usage. The newly created wallets are secured using elliptic curve cryptography and also contains public and private keys. Public keys are known to all the nodes in the network and private keys are held confidential and are given only to authorized nodes. The transfer of funds is secured by using this mechanism.

3.1 Advantage of the proposed system

It creates transparency by letting all other nodes in the network know about the transaction status and details. Provides enhanced security by the OTP (One-Time Password) authentication mechanism. The One Time Password is sent only to the authorized users to maintain confidentiality and security of online currency transfer. It provides zero development and maintenance cost.

3.2 Java IDE and glassfish server

Java is used in the server side. Entire blockchain process of creating a wallet to transaction added to blockchain are done in the back end.

Where in front end we make use of the JSP (java servlet programming).As registration cannot be decentralized using the

blockchain. we make use of JSP web application for registration. Where the details get stored in the SQL database. once a user is logged in server-side java program consisting of a class called Wallet is made a call. Then a wallet will be created for the particular user. He can check the balance and make a transaction by proving the receiving user name and amount to be transferred and he can also add some message. As soon as sender proceed an OTP will be randomly generated to the sender's email. The sender needs to provide that OTP to the application once the appropriate OTP is provided. The transaction takes place and the particular transaction block gets added to the blockchain. And an acknowledgement mail is been sent to both sender and receiver regarding the transaction and updated balance.

IDE used - net beans ,Server used - Tomcat / Glassfish

3.3 Nonce

Nonce stands for number only used once. A nonce is a random number. Thus nonce of a particular cryptocurrency blockchain has a particular difficulty level. Lite coin has a difficulty level around 442,592. The nonce is added to the block for performing rehashing of the particular block. After rehashing as per the difficulty, a particular number of zeros will be added in front of the hash that was before rehashed. Where in bitcoin after rehashing 32 number of zeros will be added in front of the old hash as per the difficulty level provided by the bitcoin. A Blockchain is a type of dairy or spreadsheet containing information about transactions. For each and every transaction generation of a hash takes place. Transaction orders are very much important. Nodes in the network can check for the hash to verify whether it has been changed or not. If any of the small change in the transaction may lead to complete creation of the new hash. The nodes can check the hash to notice if any change has occurred in the hash. If the majority of the nodes approve the transaction then it can be added into the block. Each and every block depends on the previous block hash value of the blockchain. The blockchain is very effective and efficient as it is spread across many numbers of computers, each and every computer will have a copy of the blockchain. The first block of the blockchain is known as the Genesis block because its previous hash value is set to zero. New block in the chain is linked with the previous block. It is impossible to tamper the data present in the blockchain system because their blockchain will be invalid until they make use of vast computation speed compared to all other nodes present in the blockchain network combined, For example, Quantum computers which we may expect in future.

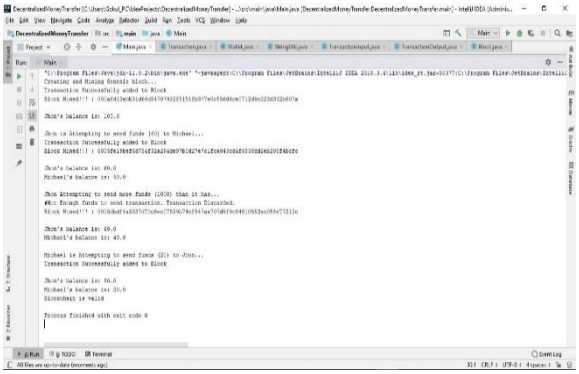

Fig. 5: Nonce backend output

3.4 Preparing a wallet

In the crypto-currencies, coin ownership will be transferred on the Blockchain as transactions, each and every participant are provided with an address using which funds can be sent to and from. In general form these wallets can be used to store these addresses, most of the wallets, however, are also software able to make new transactions on the Blockchain. Thus the private key is being used to signature the data that we don't want to be tampered with. The public key can be made use for verifying the signature. Generation of our private and public keys in a KeyPair. By making use of the Elliptic-curve cryptography to Generate our KeyPairs. Let us append a generateKeyPair() method to the program in the wallet class. Thus we can make use of the elliptic curve cryptography in java by importing a package of security. That is import java.security.* can provide the functionality of elliptic curve cryptography by making using of java.security.KeyPairGenerator package exactly. This algorithm can also be implemented using the BouncyCastle Application Programming Interface(API) in a simple manner. There are several differentiations in Elliptic-curve cryptography, for example, ECDH, ECIES, ECDSA, ECMQV. We make use of ECDSA. Where ECDSA stands for Elliptic Curve Digital Signature Algorithm.

Every transaction has a hash associated with it. All the transactions hashes in the block are themselves hashed in a block, all of those results in the Merkle root. In other words, the Merkle root is the hash of all the hashes of all the transactions in the block. The Merkle root always involves in the block header. With this scheme, it is possible to securely verify that a transaction has been accepted by the network by getting back data with just the tiny block headers and Merkle tree retrieves the entire blockchain is unnecessary. Currently, this is not used in Bitcoin, but it will be used in future.

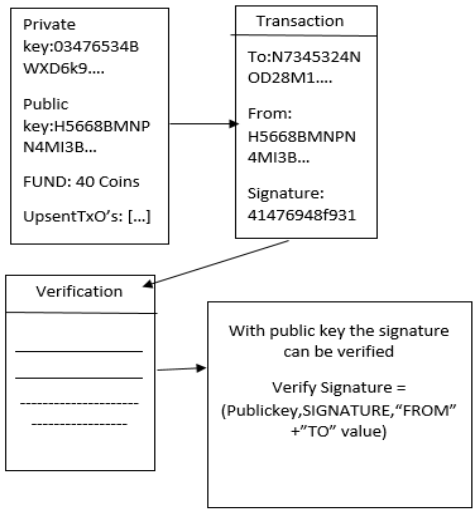

Fig. 6: Creation of Wallet

3.5 Elliptic curve digital signature algorithm

Bitcoin makes use of an algorithm called Elliptic Curve Digital Signature Algorithm or **ECDSA which** is a cryptographic algorithm for ensuring that funds as it is being used by the rightful owners. Where a private key is a secret number, which is known only to the person who generated it. Some firms and individuals are been in the hard journey are those who have fallen due to data manipulation and theft. It is now possible for creating data signatures and also promote data integration and validation. Firms no longer have to incur the data loss and manipulation warmth, now data is safe with Elliptic Curve Digital Signature Algorithm (ECDSA),. Elliptic Curve Digital Signature Algorithm (ECDSA) is a cryptographic algorithm which is used for the creation of **digital signatures** of data and give authentication.

Signature =
CreateSignature("Privatekey","FROM",+"TO","Value)

4. SYSTEM ARCHITECTURE

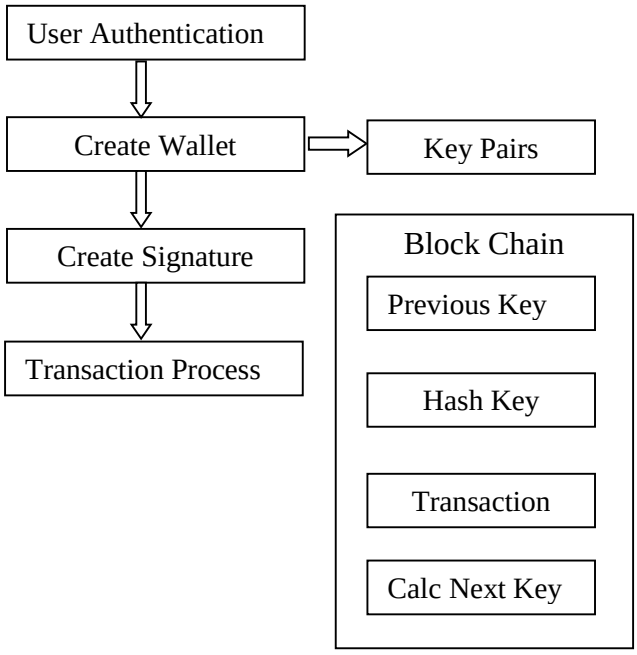

Fig. 7: System Architecture

The above figure states that User Authentication provides like OTP (One Time Password) and Email confirmation. After the Authentication, the page is diverted to create a wallet (whereas wallet is the storage) and create a pair of key and uses the Elliptic curve cryptography algorithm for the transaction process. Blockchain always depends on the previous hash key and moves to the transaction the record of the two parties of the transaction is efficiently verified in a permanent way.

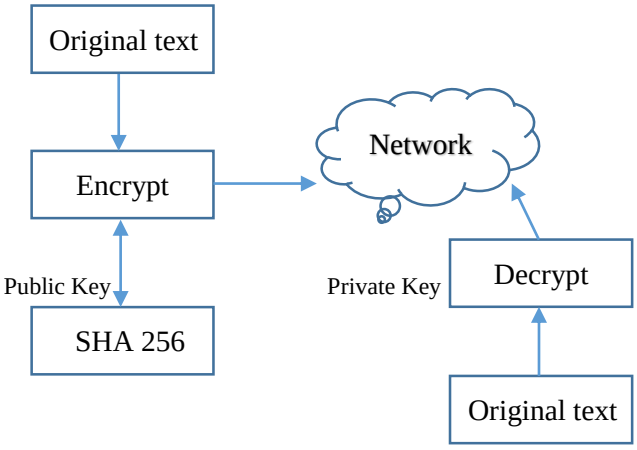

Fig. 8: Encrypt and Decrypt SHA 256

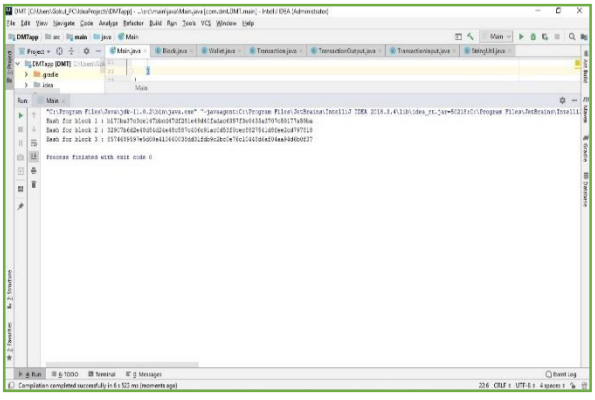

Fig. 9: SHA 256 Output

SHA 256 uses the encryption and decryption algorithm to separate the hash block.

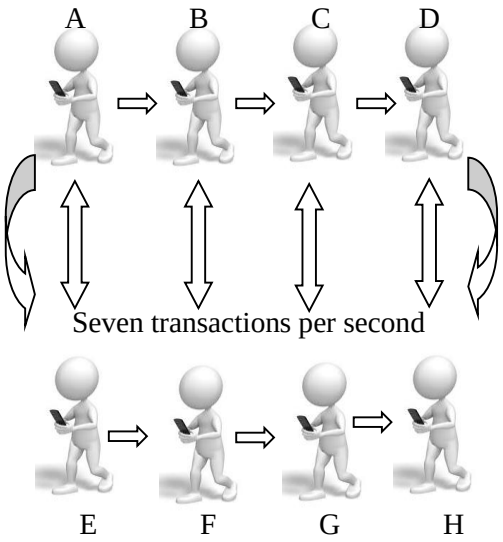

Fig. 10: Users Blockchain transaction

5. RESULT

Where the money transfer is done and there is no more charges by any of the organization or central bank.

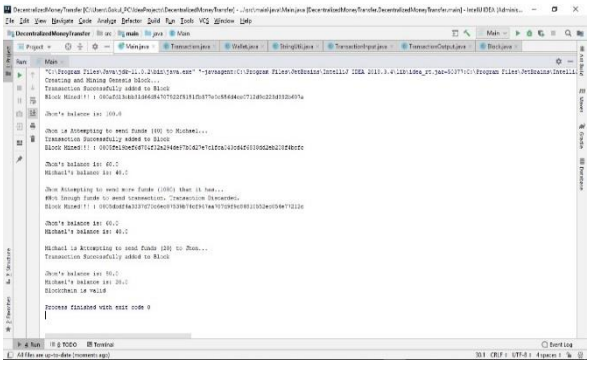

Fig. 11: Transaction completed using the blockchain

6. CONCLUSION

In summary, cryptocurrency mining can bring a massive change in the market. Blockchain technology runs on the bitcoin cryptocurrencies. It is decentralized and visible to everyone public ledger. The goal of the project is to bring the secure transaction, security and transparency to users. People who are mining in small and large-scale are enterprises have struggled a lot in the past year is evident. However, the fact remains that crypto mining plays an important role in the security validity and verification of transactions for the vast majority of Blockchains. Due to the massive challenges for miners, it's an opportunities to lead over in the future upcoming technology.

7. REFERENCES

[1] Swan M. Blockchain: Blueprint for a New Economy. [a] O'Reilly Media, Inc.º;2015.
[2] Kitchenham B, Charters S. Guidelines for Performing Systematic Literature Reviews in Software Engineering;
[3] Coinmarketcap, Crypto-Currency Market Capitalizations; 2016. Accessed: 24/3/2016. https://coinmarketcap.com/
[4] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Consulted. 2008; 1(2012):28.
[5] Kondor D, PoÂsfai M, Csabai I, Vattay G. Do the rich get richer? An empirical analysis of the Bitcoin transaction network. PloS one. 2014;9(2):e86197.doi:10.1371/journal.pone. 0086197 PMID: 24505257Where Is Current Research on Blockchain Technology? ĐA Systematic Review

[6] Herrera-Joancomart J. Research and Challenges on Bitcoin Anonymity. In: Garcia-Alfaro J, Herrera-Joancomart J, Lupu E, Posegga J, Aldini A, Martinelli data privacy management.

[7] Bitcoincharts; 2016. Accessed: 24/3/2016. https://bitcoincharts.com

[8] Housley R. In: Public Key Infrastructure (PKI). John Wiley & Sons, Inc 2004. Available from:http://dx.doi.org/10.1002/047 148296X.tie149.

[9] Double-spending; 2016. Accessed: 24/3/2016. https://en.bitcoin.it/wiki/Double- spending.

[10] Bitcoin wiki; 2015. Accessed: 24/3/2016. https://en.bitcoin.it

[11] Di Battista G, Di Donato V, Patrignani M, Pizzonia M, Roselli V, Tamassia R. Bitcoin view: visualization of flows in the bitcoin transaction graph.

