International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 08 | Aug 2020 www.irjet.net p-ISSN: 2395-0072

SECURE BANK TRANSACTION USING BLOCKCHAIN

Swathi H.C[1], Dr. H.P Mohan Kumar[2]

[1]*Student, Dept. of MCA, PES College of Engineering, Mandya, Karnataka, India*
[2]*Professor, Dept. of MCA, PES College of Engineering, Mandya, Karnataka, India*

Abstract - *Blockchain is a modern technique that enables transactions between parties simpler and safer. Most frauds now threaten the banking sector. The key goal of this work is to resolve banking transaction difficulties. As the current team can automatically traverse the network, it can focus on one point which is the server computer. The database server infrastructure would be removed and the information decentralized through the blockchain to minimize the possibility that a server will be compromised. We use SHA256 algorithm to generate 256-bit unique hash value and proof of work consensus algorithm to generate authenticated blockchain.*

Key Words:**Wallet, Public/Private key, Consensus algorithm, SHA256, Proof of Work.**

1. INTRODUCTION

The key purpose of the proposed program is the creation of a new technology to provide more security for banking transactions. The Blockchain, a platform for the exchange of leader schemes, can be used in a wide number of programmes. Blockchain technology typically has key decentralization, longevity, openness and data authenticity [5]. We provide a specific concept of decentralized conditional confidential payment, acknowledging the value of law, and defining the related safeguard criteria. The platform enhances information management and guarantees effective and secure communication. Confidence is improved when performing banking transactions between parties using Blockchain as it decreases the risk of fraud and creates records of operations automatically. This provides an automatic context tracking of all device users. Blockchain offers transparency because of its decentralized nature and decreases the risk when negotiating a client agreement with a non-known or unknown entity.

2. LITERATURE REVIEW

The popularity of blockchain is partially attributable to its decentralizing and anonymous characteristics. The framework holds the history of transactions between most nodes in a peer-to-pair network to avoid "double expenditure." To hold tradition, a consensus-based system called proof of work is used [1]. The different ways and methods in the application of the POW (proof of work) to a blockchain can be regarded as consensus. With this algorithm, different parties decide whether a transaction can be added to the corresponding blockchain or not. It makes it more difficult to solve the cryptographic puzzle, and the total number of leading zero in the cryptographic puzzle can be made more difficult to solve. [2]. How peer-to - peer electronic cash can help users send cash from place to place without involvement of third parties. And the use of Ethereum blockchain was also introduced to the corresponding blockchains network. Explains further how digital signatures and digital certificated organizations help and question the centralized structures that already exist [3]. Compared to a central data storage, Blockchain technology has better privacy security, as the server has no inaccessibility. And if we were to hack the entire blockchain network, we need 51% access to the network, so it can't be done at all. And several active nodes in the open blockchain blockchain network. The encryption token with intelligence string information used. This refers in general to the growth, transfer and storage of cryptocurrencies. The cryptographic token refers generally to the data string which actually shows the information with the first data. [4]. The work must be checked successfully by all nodes of the network to act as proof-of - work for cryptocurrencies. The primes, such as record breaks, should not be too that. It then precludes Mersenne primes and results in the use of the main chain as the function of the primary coin, since it is exponentially harder to locate the primary chain (with our present theoretical and algorytic understanding) [6].

3. PROPOSED METHODOLOGY

Blockchain technology refers to any electronic exchange of digital properties. This technology is used in this case to ensure safe banking transactions. blockchain is a decentralized distributed ledger, making it easy to verify all transactions and preventing any backup of the ledger from being updated. Fig(1) demonstrates transactions conducted in blockchain technology.

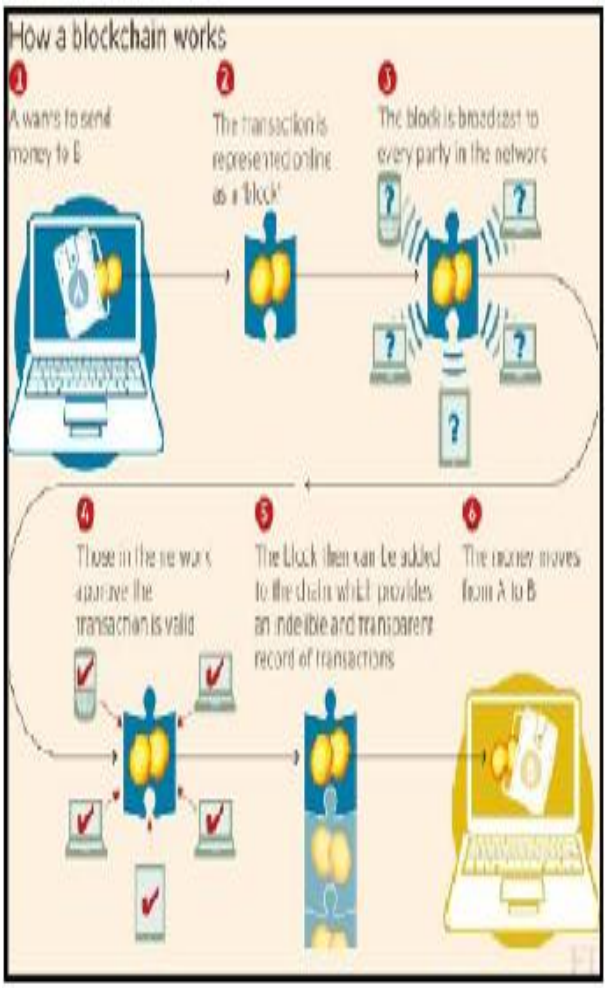

Figure 1. Transaction in blockchain

3.1 BLOCK CHAIN

For all participants in a business network, Blockchain has the potential to share a storage device. This replicated mutual leader would have consensus, provenance, immutability and intent about the transition of assets into the business network. The effect will be a decreasing of costs, complexity and time. In fig(2) Every block carry a hash of the previous block.

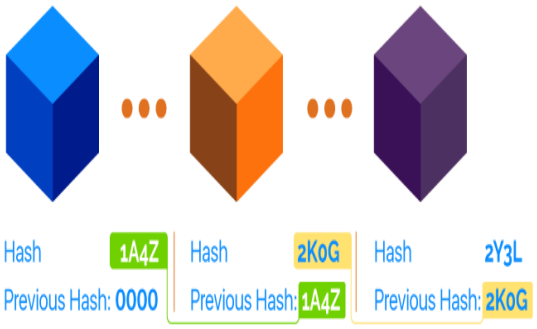

Figure 2.Blockchain

3.2 ALGORITHM

A. Proof of Work

In Blockchain this algorithm is used to confirm transactions and introduce new blocks. With POW, miners will participate and receive compensation for completing payment process. Digital tokens are sent in a network customer. A shared registry puts together all transactions. Payments should also be tracked and blocks carefully arranged. This duty is performed by special nodes called miners, which is called mining.

Working:

POW is used in the authentication of transactions and after confirmation, new blocks are recorded on the ledger. When each transaction is completed successfully new block is added to the blockchain ledger. It requires more computational capacity.

B. SHA256

One of the cryptographic hash functions is the Secure Hash algorithm (SHA). A hash cryptographic is like a data collection signature. It's like the data's biometrics. Although only one symbol is modified, there is another hash value to the algorithm. A fast-unique, 256-bit (32-byte) hash generated by SHA256 algorithm. Hash is defined as a feature in one way. This makes it ideal for protection of data integrity, hash encryption, antitampering, digital signatures and blockchain applications.

3.3 IMPLEMENTATION AND WORKING

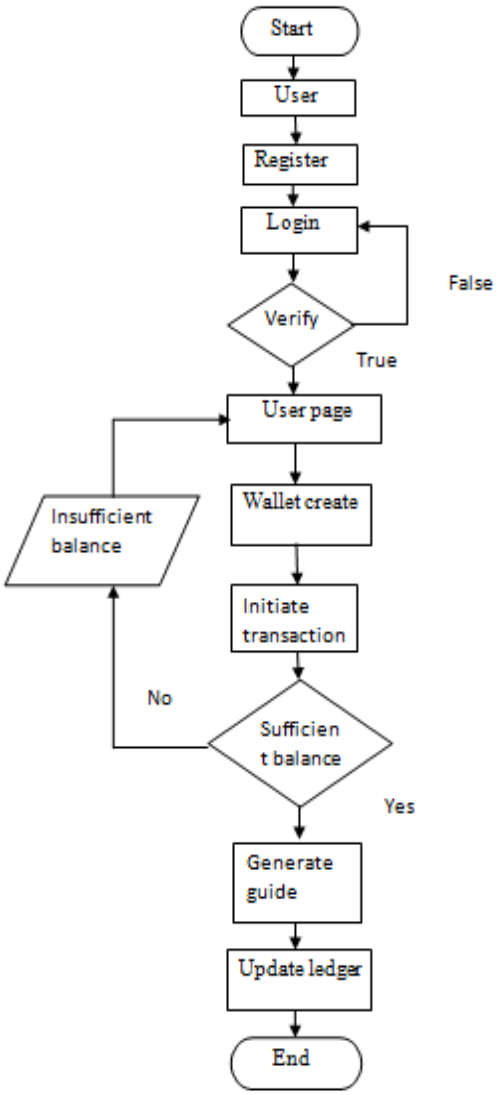

Figure 3. Flow chart of the system

The complete working of application is shown in the above flowchart Fig(3). At the beginning of the application's UI module, our system's front end UI has no blockchain storage. It displays transactions without blockchain i.e. by simply storing a database. It allows to user signup with system and create wallet by linking bank acoount. After creating wallet user will get a private key of the wallet through mail, by using the private key user can make transactions. This private key is generated by using SHA256 algorithm. During the transaction the public key will be sent to the reciever, which can be used to check the authenticity. Once users have made a transaction, a blockchain is built with a proof of work (mining) method. Every single block has its own cryptographic key. Once blockchain is determined, its validity can be checked by looping through blocks in blockchain, i.e. searching for the previous block is the same as the previous hash block and current hash with the newly found hash block. This is known as "Proof of Work".

4. CONCLUSIONS

There is a debate on the standard consensus algorithms in blockchain. The openness and immutability of Blockchain systems are frequently seen as added benefits. Keep a decentralized, public leader without direct control or regulation. There are significant challenges. In addition, private distributed ledgers and blockchains can be generated to deal with such issues. An person would be almost difficult to crack the device because it requires a massive volume of computing capacity that nobody has. Blockchain can speed up transactions by eliminating the steps involved in regular transactions. We are using blockchain technology in this case to securely transact banks.

AKNOWLEDEGEMENT

I would like to express profound gratitude to my guide Dr. H P Mohan Kumar, Professor & HOD, Department of MCA, PES College of Engineering, Mandya for his continues guidance and support to publish my research paper successfully.

REFERENCES

[1] "State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016.

[2]S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] Satoshi Nakamoto,Bitcoin:A Peer-to-Peer Electronic Cash System,.White paper.[2008]

[4] F. Tschorsch and B. Scheuermann, Bitcoin and beyond: a Technical Survey on decentralized digital currencies, IEEE [2016]

[5] Zibin Zheng, Shaoan Xie, Hong-Ning Dai and Muhammad Imran "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,6th IEEE International Congress on Big Data

[6] S. King, "Primecoin: Cryptocurrency with prime number proof-ofwork," July 7th, 2013.