International Journal of Trend in Research and Development, Volume 5(2), ISSN: 2394-9333
www.ijtrd.com

Blockchain Technology in Financial and Banking Sector

[1]Ameya Dixit, [1]Blaze Rodrigues, [1]Kaustubh Yadav, [1]Thomas Chacko and [2]Dr. Lata Ragha,
[1]Students, [2]Professor and Head,
[1,2]Department of Computer Engineering, Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai, India

Abstract: Conventionally, money and other transactions are made through an intermediary entity or organization and we have to rely on them and assume that they would carry out the transactions in a neutral or unbiased manner. This involves a lot of risk as we have to blindly place our trust on them.

Blockchain is a technology which has the potential to revolutionize the finance and banking sector by introducing a peer to peer decentralized transaction system.

Blockchain is a type of distributed ledger or distributed database which keeps a record of digital transactions. Instead of having a centralized database system, here the database is replicated and distributed across the network and synchronized via the internet.

Keywords: *File Storage, Distributed consensus, Cryptography, Block, Ledger, Proof of work.*

I. INTRODUCTION

BLOCKCHAIN, a seemingly unassuming data structure, and a suite of related protocols, have recently taken the worlds of Finance and Technology by storm through its groundbreaking application in the modern crypto-currency, the Bitcoin, and more so because of the disruptive innovations it promises. While Bitcoin has been the most talked about application of the Blockchain technology to date, new applications such as Smart Contracts have tried to exploit more abstract nature of the platform. Blockchain Technology relies heavily on fundamental tools from Cryptology and Data Security, especially in terms of transaction authentication targeted towards tamper-evidence and tamper-resilience. In its most abstract form, a Blockchain may be described as a tamper-evident ledger shared within a network of nodes, where the ledger holds a record of transactions between the nodes.

In this paper we try to describe the underlying mechanisms and technology that make blockchain possible. [1]

II. BASIC ELEMENTS OF BLOCKCHAIN TECHNOLOGY

A. Distributed Consensus

Because any entity, individual, or party can submit information to the blockchain (that is to say, try to add information to the database), it is necessary for the distributed operators of the blockchain to evaluate and agree on all addenda before they are permanently incorporated into the blockchain (the database). Because we cannot be sure of the author's trustworthiness, it is vital that all new information must be reviewed and confirmed before being accepted. This review results in the 'consensus'. [2]

The concept of consensus incorporates 3 basic principles:

- The common acceptance of laws, rules, and norms
- The common acceptance of institutions(nodes) that apply these laws and rules
- A sense of identity or unity, so group members accept that they're equal in respect to the consensus.

In distributed ledgers, a consensus mechanism is the way in which a majority (or, in some mechanisms, all) of network members, the nodes, agree on the value of a piece of data or a proposed transaction, which then updates the ledger.

There are 2 major methods for consensus:Proof-of-work (PoW) and Proof-of-stake (PoS).

Proof of work mechanism is shown in figure 1:

1. Transactions are bundled together into a block
2. Miners verify that transactions within each block are legitimate by trying to solve a mathematical complex problem.
3. The miner solving the problem first is rewarded.

Verified transactions are then stored in the public blockchain. This entire process is known a mining. Proof of work essentially relies on computing power to secure the network; in order to take over the network one needs to have more than 50% computing power of all the other parties as a whole in the network and this is very unlikely to happen.

Proof of Stake (PoS) method will pick the Validator by the amount of stake a validator has and the respective age of the stake. Unlike PoW, this process is known as forging.

Our proposed system uses the proof-of-work technique to establish distributed consensus using SHA256 hash function.

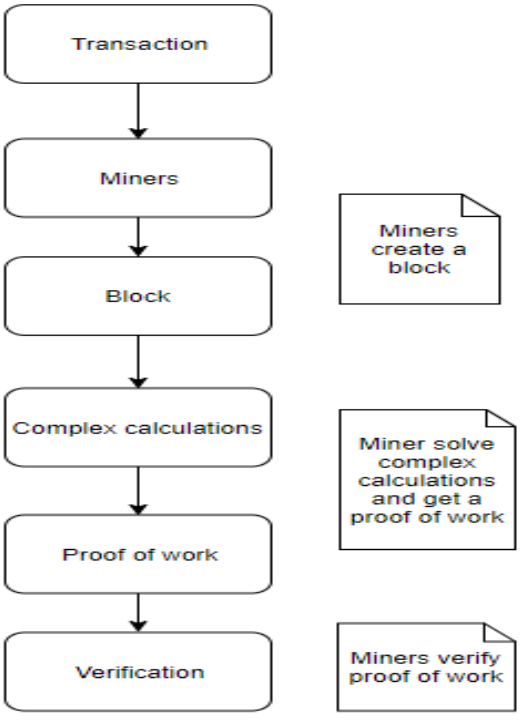

Figure 1: Proof of work

B. Working of Blocks

The blockchain is seen as the main technological innovation of Bitcoin, since it stands as proof of all the transactions on the network. A block is the 'current' part of a blockchain which records some or all of the recent transactions, and once completed goes into the blockchain as permanent database.

The Bitcoin network orders transaction by putting them together into groups called blocks each block contains a definite amount of transactions and a link to the previous block.

In order to add next block to the blockchain, each blockmust contain the answer to a complex mathematical problem created using an irreversible cryptographic hash function. The only way to solve such mathematical problem is to guess random numbers that combined with the previous block content generate a defined result (usually a number below a certain value). It could take about a year for a typical computer to guess the right number and solve the mathematical problem. However due to the high number of computers in the network that are guessing numbers a block is solved on average every 10 minutes. The node that solves such mathematical problem acquires the right to place the next block on the chain and broadcast it to the whole network.

Every block within the blockchain is recognized by a hash, created with the SHA 256 cryptographic hash algorithm on the block header. The block header contains the following parameters :version, hash of the previous block, thus making a chain of block, timestamp, number of seconds since 1970-01-01 00:00, bits,a representation of the networks current difficulty, nonce, incremented when mining.

Every block also references a preceding block, referred to as the parent block. In other words, every block has the hash of its parent in its own header. The series of hashes connecting each block to its parent makes a chain going back to the first block, referred to as the genesis block**.**

Genesis Block: A genesis block is the first block of a blockchain. Modern versions of Bitcoin number it as **block 0**, though very early versions counted it as block 1. The genesis block is almost always hard coded into the software of the applications that utilize its blockchain. It is a special case in that it does not reference a previous block.

C. Storage

Nowadays storage services are provided by central authorities which charge a client on monthly basis for certain amount of storage space allocation. The risk again lies in the centralized nature of the system where the files are kept at the sole responsibility of the central party. If this party gets compromised the this may lead to the confidential files being in custody of malicious user. [3]

The decentralized system can be used for creating a hybrid file storage system where:

1) The files are divided into multiple small chunks and storing them at different nodes to increase the security. The attacker has to obtain the file chunks from all the nodes where the file is stored which is very difficult.
2) Using the principle of blockchain to establish authenticity and validation of the files and user

The first approach can be implemented by using a scheme where the metadata that contains information about different chunk's location is encrypted and is divided into pieces. After the restructuring of the metadata the file chunks are collected from the nodes and the file is reconstructed.

The second approach can be implemented by using an extended version to proof of work concept of blockchain like proof-of-storage and proof-of-replication which functions like requirement of nodes to prove they actually store the files and proving that some data has been replicated to that node's own physical storage.

III. PROPOSED SYSTEM

The proposed system shall consist of an application which would allow users to be a part of the blockchain and share data in the form of multiple blocks linked to each other forming a chain of blocks. It will also allow mining and exchange of cryptocurrency and thus users will be able to make monetary transactions. Figure 2 shows the flow of working of the proposed system.

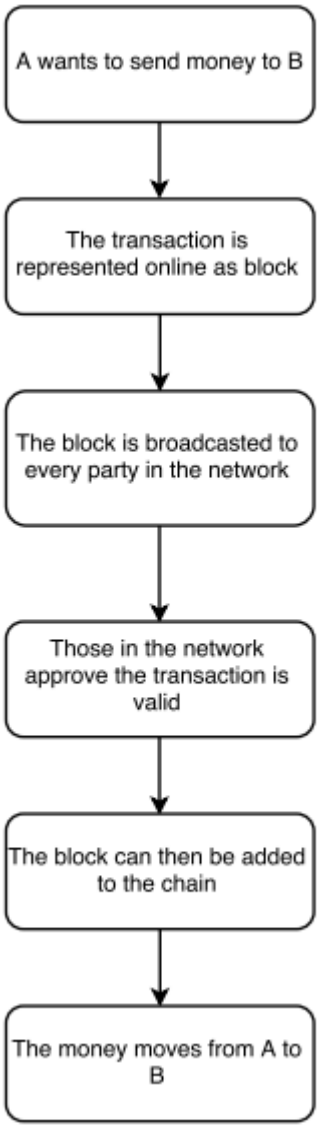

Figure 2: Proposed system

The software would have a graphical user interface that would consists of different options for the user to select such as checking the wallet, tracking the mining operation, perform transactions, etc.

1) Connecting the nodes

The software will implement the networking part for communicating with different nodes in the network.

Websockets API and HTTP interface would be used for this purpose. It will also use different algorithms for performing operations on hash functions.

2) Storage of Blocks

The ledgers/blocks will be stored in the hard-drive of all the individual peers in the network.

3) Validation of Transactions / Proof of work

The Machine node which calculates the block first will present this value to other nodes which can be easily verified by other nodes . This block is then accepted and used for calculating next block . The consensus is established by using the longest chain of blocks representing oldest transactions as a standard for validation.

Characteristics

- The system would be implemented as a peer-to-peer network.
- The system consists of a standalone software that needs to be installed on the target machine.
- These machines would act as nodes in the blockchain network that send messages at regular intervals to synchronize and update the ledgers.

IV. SCOPE

This proposed methodology is being implemented in order to overcome the drawbacks of a centralized banking system where we have to depend on a third party for carrying out the transactions, placing all our trust on them. Instead, we would try to use a peer to peer blockchain technology for the same purpose which would provide greater security to the transactions being done.

Purpose of work:

Blockchain technology in financial and banking sectors would implement a secure method to implement financial and banking transactions using the blockchain technology which is a peer to peer system.

Our main purpose is to stop relying on a central entity to conduct transactions. We would do so by using the peer to peer blockchain database system and this would also involve a cryptocurrency similar to bitcoin. [4]

In a peer to peer system, we shall be able to achieve a greater amount of security by incorporating the distributed consensus concept.

Deliverables:

The major output would be a secure system for carrying out financial transactions. We would also implement a cryptocurrency system.

Future scope:

We will implement secure financial transactions using blockchain and a cryptocurrency system. However, in the future this system can include additional features such as:

- Digital authentication using blockchain.
- Secure digital identity.
- Smart contracts.
- Digital decentralized notary service.

V. IMPLEMENTATION

The proposed method is split into different modules so that each module can be completed easily and the integration of all these modules would be done at a later stage. The system would be created first which would be tested extensively to find errors and bugs. After building a stable working backend, the GUI module (Apps) would be started to initialize the frontend development of the system. [5]

The modules can be broadly classified into 4 parts:

- Networking module
- Cryptographic module
- GUI module
- Storage and database module

The networking module is responsible for the communication among the peers. The cryptographic module (protocols) is responsible for functions like generating the keys, public address generation encryption of wallets etc.

The GUI modules form the front end part of the system which would contain a simple user interface for the user.

The storage and database module is used for storing the blockchain locally as well as in a distributed database system.

The tokens represent the digital assets that would be used for making transactions between nodes. Figure 3 shows implementation modules of the proposed system.

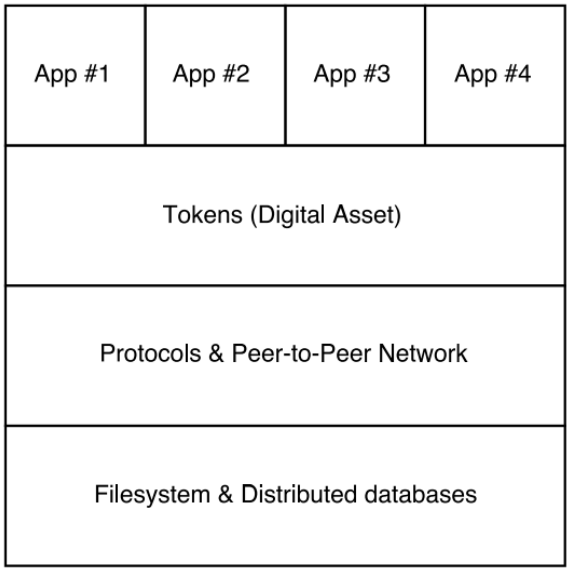

Figure 3: Implementation modules

CONCLUSION

The proposed system provides a means for the users to do financial transactions in a decentralized manner without involving the middle party or the central authorities for the record keeping purposes. The security measures of the blockchain ensure that the malicious intents of the attacker are very difficult to execute on a blockchain network. The security strength of blockchain increases exponentially as the time passes and more blocks are mined and store in the network making it practically infeasible to alter the transactions. This can be implemented at the national and international levels.

References

[1] "Application of Blockchain Technology to Financial and Banking Sector in India" by Institute for Development and Research in Banking Technology

[2] "Blockchain Technology", Berkeley Education, Sutardja Center for Entrepreneurship & Technology Technical Report by Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman.
[3] "A Proposal of a Secure P2P-type Storage Scheme by using the Secret Sharing and the Blockchain" by Masayuki Fukumits, Shingo Hasegawa, Jun-yaIwazaki, Masao Sakai, Daiki Takahashi. Published in 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA).
[4] "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto.
[5] "Tax, financial and social regulatory mechanisms within the knowledge-driven economy. Blockchain algorithms and fog computing for the efficient regulation" by N. N. Pokrovskaia. Published in 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM).