International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Blockchains – A Strong Promise to the Future

Anupama Kaushik[1], Ashana Sachdeva[2], Parul Kashyap[3], Saransh Negi[4]

[1,2,3,4] *Dept. of Maharaja Surajmal Institute of Technology, New Delhi, India*

Abstract - *The following paper gives a brief and concise information about the technology – Blockchains. With research work over a significant time duration, the paper has been written to give a short description of the core of this technology. Blockchains is a technology that came into the picture with its ability to produce secure and transparent applications. It brought the concept of decentralization and hence increased the level of security far more than earlier. It is used to make DAPPS (decentralized apps) with the inclusion of encryption and decryption using public and private keys. One of the many products produced by using this technology is the 'bitcoin'- the revolutionary cryptocurrency. With the huge success of products like bitcoin, etc. blockchains promise to bring an all new revolution in the 'finance sector'.*

The prevailing process of KYC among B2C entities is cumbersome and takes minimum T+2 settlement time. As a proof a concept, this work aims to offer these businesses an innovative approach to tackle the conventional KYC problem using Blockchains.

***Key Words*: Blockchains, Decentralized application, Distributed Ledger, Mining**

1. INTRODUCTION

BLOCKCHAINS - the word in itself gives a glimpse of what it actually is. It can be broken into two parts, "block-chain" which implies the existence of a 'chain of blocks'. In the most basic terms, we can say that it is a group of interconnected systems that are fully open and transparent to each other. The fundamental use of this technology is to make 'decentralized' applications.

In simpler terms, it could be called a network of computers possessing an identical copy of the database and changing its state (records) by a common agreement based on pure mathematics.

This makes the need for any central server or agent to trust completely redundant. The blockchain is the technological foundation for all those names in cryptocurrency like Bitcoin, Hyperledger, Ethereum.

The blockchain exists as a peer-to-peer network that stores data that is written by certain members, read by certain members and has an extremely hard mechanism to modify or delete the historical records.

To be conclusive, blockchains can be defined as a way to produce 'decentralized' apps with the convenience of being transparently distributed among various systems of the network, yet not being copied by anyone.

Section 2 describes the basic terminology related to blockchains.

Section 3 talks about 'Distributed Ledger' which is a shared database and is synchronized across the network.

Section 4 describes the different types of blockchains that exists in today's world.

Section 5 explains the properties and features of blockchains in detail.

Section 6 talks about our contribution in this field and the major commands involved in the blockchain process.

Section 7 describes future aspects of the work done.

2. TERMINOLOGY

2.1 Transactions

The literal meaning of a transaction is 'an instance of buying or selling something'. Here, the word transaction is used to depict a small action performed by a node in the blockchain. The term transaction holds its literal meaning and depicts a transfer of currency between users in the context of cryptocurrencies such as Bitcoin.

A blockchain can record transactions between two parties in a verifiable and permanent way by acting as an open, distributed, decentralized ledger. A peer-to-peer network manages a blockchain by following a certain set of rules to validate new blocks.

A 'transaction fee' is charged for certain transactions in blockchains. This fees initially serves as an incentive and is consequently given as a reward to the 'miner' that performs that transaction. Therefore, the transaction is computed and performed first by the most powerful computer and thus, rewarded with the transaction fees.

2.2 Nodes and Miners

Nodes are the important members of a blockchain that have the access and view of it. In simpler terms, a node is any member of the group of computers associated with the blockchain. A node is just like any other system of this network that stores a copy of the information and is aware of all the transactions that occurred in that blockchain.

The Bitcoin Blockchain environment acts like a network of duplicated databases where each copy contains the exact list of the previously occurred bitcoin transactions. Validators or nodes are responsible for passing around transaction data (payments) and block data (additions to the ledger).

On the other hand, a 'miner' is a node in the blockchain that does a transaction. Whenever a new block of transactions is created, it is added to the blockchain, resulting in an increasingly lengthy list of all the transactions that ever took place on the network. A constantly updated copy of the block is kept and is given to everyone who participates so that they are aware of the current status.

2.3 The Process of Mining

The process in which the transaction history is stored in the shared ledger is known as Mining. It is the distributed computational review process that is performed on each "block" of data in a "block-chain". In an environment where neither party knows or trusts each other, mining allows for achievement of consensus. Mining takes an ingenious approach to successfully achieve a previously unachieved feat: Distributed Trust.

In Bitcoin Blockchain ecosystem, the security and validity of the Bitcoin network are controlled by Bitcoin mining along with release of new coins into circulation while releasing reliance on centralized networks. During this process, new bitcoins are released from the remaining *unmined* pool of 21 million total bitcoins.

Stating conclusively, 'mining' is the process of adding and verifying new transaction records to the blockchain (distributed public ledger), which includes all past transactions.

2.4 Hash

When a block of transactions is created, it is done in a procedural manner by the miners. The data of the block is taken, and some mathematical formula is applied to it, turning it into something else, a third value. That value is a far shorter and probably a sequence of letters and numbers known as a "hash". This hash or the third value is stored along with the block, at the end of the blockchain at that point in time.

Hashes possess some interesting properties. Firstly, production of a hash from a collection of data is easy, but it's practically impossible to work out what the data was just by looking at the hash. Secondly, even though it is very easy to produce a hash from a large amount of data, each hash is unique. Even if just one character in a block is changed, its hash will change completely.

Apart from the transactions in the block, some other pieces of data are also used by the miners to generate a hash. Hash of the last block stored in the blockchain is also one of these pieces of data.

As each block's hash is generated using the hash of the preceding block, it becomes a digital version of a wax seal. It confirms that this block – and every block after it – is legitimate because if it has been tampered, everyone would know.

If one tries to fake a transaction by changing a block that had already been stored in the blockchain that block's hash would change. If the block's authenticity is checked by running the hashing function on it, the hash now found will be different from the one already stored along with that block in the blockchain. The block would be spotted as a fake instantly.

Any kind of alteration or tampering with a block would make the succeeding block's hash wrong. Each block's hash is used to generate the hash of the succeeding block. This would continue all the way to the end of the chain leading to a chaotic outcome.

Hence, the cryptocurrencies made using blockchains are free from 'double spend attacks', i.e., no person can fake a transaction, and the record of spending and earning of the currency cannot be altered by anyone.

3. DISTRIBUTED LEDGER

The term 'ledger' simply means a 'record' of anything. In technical terminology, it mainly describes a database. The ledger is considered to be the database itself that stores the data for a particular server. Thus, one can say that the distributed ledger is a collection or a database consensually shared and synchronized across network spread across multiple sites, institutions or geographies and is decentralized completely. Here the word 'consensually' refers to the process of agreeing to a fact or action by mutual consent. Hence, the distributed ledger is formed as a result of a common consent of the members of that group. The ledger can be of any type, be it any data or some media. Here, in the context of blockchains, we focus on the ledger of 'transactions' and that too a distributed and decentralized one.

3.1 Characteristics of Distributed Ledger

It allows transactions to have public "witnesses," thereby making a cyber-attack more problematic and difficult. Each and every node has a copy of the transaction records. Moreover, the hash of each block is stored with the block itself in the blockchain that can be used at any further point to check the validity of the transaction.

Once there is this consensus, the distributed ledger is updated, and all nodes maintain their own identical copy of the ledger. This architecture permits for a new dexterity as a system of record that goes beyond being a simple database.

4. TYPES OF BLOCKCHAINS

4.1 Public Blockchain

Blockchains can be 'public' in two senses: Anyone without permission can write data and anyone without permission can read data.

Usually, when people talk about blockchains, they refer to the public blockchains that are available for the use of everyone with no requirement of a permission from any other node.

4.2 Private Blockchain

A 'private' blockchain network is where each node is known and trusted i.e. each node participating in the blockchain is authentic and trusted. For example, a group of companies owned by an umbrella company. In such a system, all the nodes are the sub-companies of the umbrella company.

4.3 Test Blockchain

The test blockchain is a special case of public blockchain which is mostly used by the budding developers to get a hands-on for the public blockchain.

5. PROPERTIES AND FEATURES

5.1 Transparent and Incorruptible

The blockchain network lives in a state of consensus, one that automatically checks in with itself at regular intervals. It can be thought of as a self-auditing ecosystem of a digital value, every transaction that happens at particular intervals in the network is reconciled. Each bundle of these transactions is referred to as a "block". Consequently, two important properties arise from this:

Transparency: data, within the network, is embedded as a whole, and it is public by definition. There is a proper and well maintained transaction record of all the transactions at each node, hence making the system transparent.

It cannot be corrupted: In order to alter even a single unit of information on the Blockchain, one would require a huge amount of computing to override the entire network, which is practically impossible.

5.2 Durability and Robustness

Blockchain technology has a built-in robustness in it. As the information is stored in blocks in a blockchain and is identical across the complete network, it is observed that: No single entity can control the complete blockchain and no single point of failure exists.

For example, the invention of Bitcoin was observed in 2008. Since its inception, there has not been any significant disruption in the operation of Bitcoin blockchain. (To date, there have only been problems related to hacking and mismanagement with the bitcoin. In other words, these problems did not come with the flaws or shortcomings in the underlying concepts, rather they came from bad intention and human error only.)

The durability of internet itself has now extended up to almost 30 years. The track record for blockchain technology also holds well now as it continues to be developed.

5.3 Decentralization

In Blockchains, no central authority has a right to control the other bodies of the network i.e. it is a decentralized technology. Here, each node is connected in a peer-to-peer fashion in a decentralized way. This is the primary reason why decentralized apps are made using blockchains, thus preventing itself from various cyber-attacks and database failures.

5.4 Enhanced Security

The risk of data being held centrally is eliminated, as the data is held across the blockchain network. Its network lacks centralized points of vulnerability that computer hackers can find and exploit.

Moreover, the technique of cryptography is used in the blockchains. This makes it more secure as compared to other platforms. The inclusion of the concept of 'public key' and 'private key' has made life much easier for the developers.

6. CONTRIBUTION

The Know Your Customer (KYC) systems will be revolutionized when the shared KYC system will be incorporated. It will save a lot of time and money of the banks and thus, will solve numerous problems regarding storage and maintenance of such extensive and delicate data.

This project work focuses on making the KYC system for the banks more efficient using Blockchains. This web application takes basic information required for KYC from the user and saves it over the blockchain that makes the complete system decentralized.

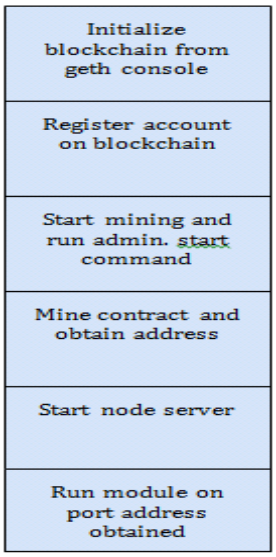

Fig -1: Flow of the Work

Fig.1 shows the process flow of work done. Geth is a command line tool developed to run Ethereum nodes. The steps followed are explained below.

6.1 Initialization of Blockchain

In order to initialize a blockchain we have to allot some space to it in our memory to store all private data, this is done by the creation of a genesis.json file.

geth --datadir "C:/minorProject/blockchain/DataDir" init C:/majorProject/blockchain/genesis.json

geth --fast --cache 512 --nodiscover --datadir "C:/majorProject/blockchain/DataDir" --identity "parul" js geth_mine.js

6.2 Geth Console

An active geth node is now connected to the blockchain. Through Geth console we enter an interactive environment.

pushd C:\minorProject\blockchain

sudo geth attach \\.\pipe\geth.ipc

6.3 Creating Coin Base

In order to make the node operational, a coinbase address is required. All the ether that is mined will be received at this node. While creating a new node, coinbase address is to be generated as it is initially undefined.

personal.listAccounts

personal.newAccount

personal.unlockAccount("0x9b67d04782b167958a6f99568869e4596a1508f9","parul",0)

6.4 Mining

For any transaction to be added to the blockchain, it has to be mined. Ether can be added to the coinbase address only by mining, in addition to directly adding it.

To start mining, the following command is to be run.

miner.start()

To start remote procedure call from the console,

admin.startRPC("localhost",8545,"*","db,eth,net,web3,admin,debug,miner,personal,ssh,txpool")

7. FUTURE ASPECTS

The future of blockchains seems to be pretty bright with the ever increasing demand for highly secured and decentralized applications. The technology has a made a great impact on the masses with its performance till now and promises to continue the same.

It is not wrong to say that in the near future blockchain will be the real 'backbone' of the finance sector. The influence of blockchain technology will be evident in the sectors such as crime, control, banks, industries, governments, etc.

8. CONCLUSION

A nice ending to the topic can only be given by quoting' "the time has come, fasten your seatbelts, this plane named 'blockchains is soon going to land you at a place called 'development'!"

The world is soon going to experience an all new BLOCKCHAINS' ERA.

REFERENCES

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, 2008.

[2] W. Dai, "b-money", http://www.weidai.com/bmoney.txt, 1998.

[3] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements", In 20th Symposium on Information Theory in the Benelux, May 1999.

[4] S. Haber, W.S. Stornetta, "How to time-stamp a digital document", In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[5] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping", In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[6] S. Haber, W.S. Stornetta, "Secure names for bit-strings", In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[7] A. Back, "Hashcash - a denial of service counter-measure", http://www.hashcash.org/papers/hashcash.pdf, 2002.

[8] R.C. Merkle, "Protocols for public key cryptosystems", In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[9] W. Feller, "An introduction to probability theory and its applications", 1957.

[10] CoinDesk, "A beginner's guide to bitcoin Technology", https://www.coindesk.com/information, 2017.

[11] Athena, "Future of Blockchain", https://www.shapingtomorrow.com/home/alert/665529-Future-of--Blockchain, September 2015