International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 5, Issue 04, April-2019

An overview of Blockchain Technology and utilization of blockchain for transformation in India

Neha Shah

School of Engineering, P. P. Savani University,

***Abstract*— blockchain is the immutable blocks that are distributed over a network, which allows a transaction to take place in a decentralized manner. These distributed ledgers are secured with hash and consensus algorithm. Nowadays blockchains are widely used for different applications and use of blockchain is also increasing in numerous fields like bank, IOT, energy, etc. This paper provides a broad overview of blockchain technology, the architecture of blockchain, consensus algorithm. Moreover, applications of blockchain in different fields and future use of blockchain.**

***Keywords*— cryptocurrency, Blockchain, Smart Contact, consensus, distributed ledger**

I. INTRODUCTION.

Today cryptocurrency is the buzzword in the market. In 2016, Bitcoin cryptocurrency reached up to 10 billion dollars in the market [1]. Core technology behind building bitcoin was blockchain where transaction can happen without any centralized authority, this was first suggested in 2008 and used in 2009. Blockchain can be treated as a distributed database and all the transactions are stored in blocks. This chain grows as a new block added to the chain. All these blocks are secured with the help of encryption and consensus algorithm. The blockchain contains chain of blocks that storing information. Blockchain is a distributed database that is open to all with a property that once blocks are written they are very difficult to change. Each block in this chain contains some data, hash function for that block and hash of the previous block. Block data depends on the type of blockchain. Once data is written, the hash will be calculated for that block, and if block data is updated then the hash will again change. The third element in blockchain is the hash of the previous block, which is how one block can be connected to another block.

Due to encryption data is safe, but only hashing cannot prevent the block from tempering, here comes the consensus algorithm called as proof of work. In blockchain, this algorithm is used to confirm transactions and to create a new block. This makes it very difficult to tamper with the block. Because if you tamper with one block then you will need to calculate a proof of work for each and every block.

So, the security in blockchain comes from the use of hashing and proof of work. In addition to this, they are distributed, not stored on any centralized machine. Blockchain uses peer to peer network and anyone can join the network. When someone joins the network, he/she will get a full copy of blockchain. When a new block is created it will be sent to everyone on the network. Each node will verify the block to make sure that has not tampered.

The rest of this paper is organized as follows. Section II covers blockchain architecture. Section III introduces consensus algorithm and section IV elaborates how blockchain can be used to transform India.

II. THE BLOCKCHAIN ARCHITECTURE

Blockchain is a decentralized distributed ledger in P2P network. This network consists of many computers but the data within block cannot be altered without consensus of whole network. The architecture of blockchain is a list of blocks with transactions. Two data structures used in blockchain are: 1. Pointers- variable which is pointing to another variable. 2. Linked list- a node containing data and link to another same node in a list.

Blockchain is a sequence of blocks that holds an entire list of transaction records like regular public ledger [3]. Fig. 1 elaborates structure of a blockchain. Block header contains hash of previous block, a block has only one parent block. It is worth noting that uncle blocks (children of the block's ancestors) hashes would also be stored in Ethereum blockchain [4]. The first block of a blockchain has no parent block. Fig.2. shows simplified blockchain structure.

The internals of blockchain are:

Blockchain internals:

A. Block

A block consists of block header and block body. Block header includes block version, hash of all the transactions in the chain, time in seconds, and limit of valid block chain, hash of all transactions in the chain called as merkle root, hash of previous block.

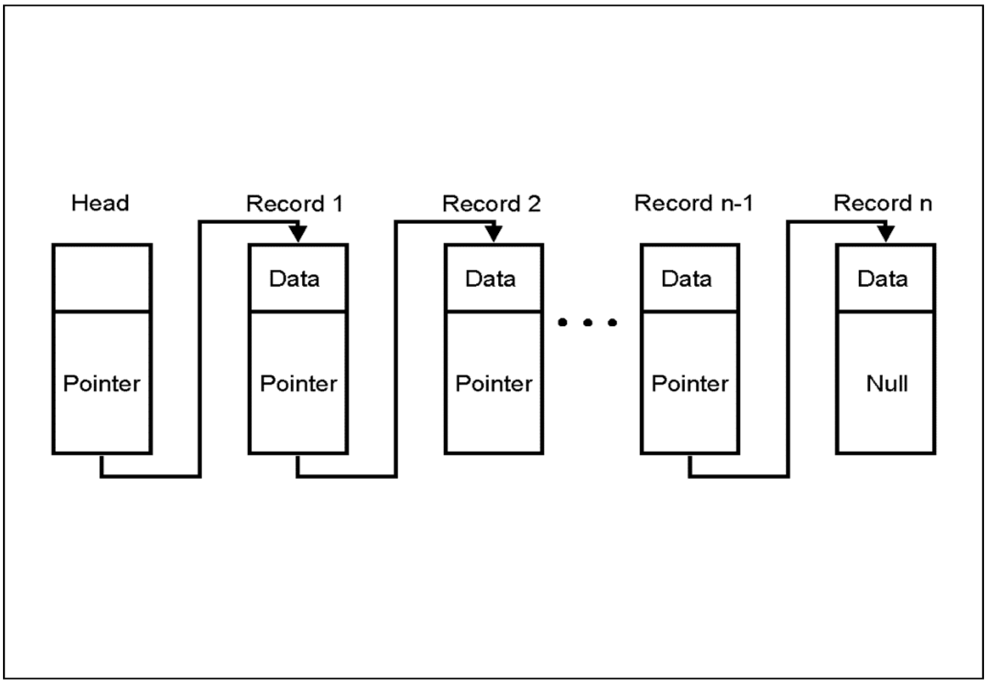

Fig. 1. Example of blockchain

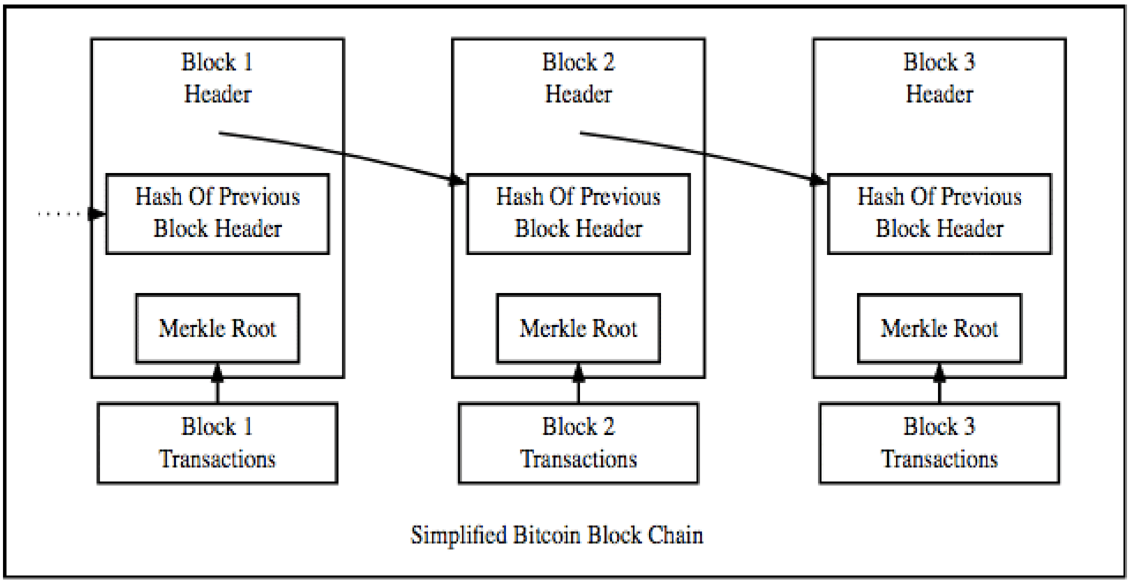

Fig. 2. Simplified blockchain

B. Cryptography

In blockchain each user is provided with private key and public key. The private is the confidential and it is used to sign the transactions. Then this digitally signed transactions are distributed throughout the network.

C. All blockchain structures fall into three categories:

There are three main types of Blockchain platforms—public, private and consortium. Organizations utilize these stages depending on their particular needs

- **Public blockchain architecture**

  A public blockchain will be available to all the user. User have open access to data. (E.g. Bitcoin, Ethereum, and Litecoin blockchain systems are public). Public Blockchain, the true platform for cryptographic money, is a decentralized structure that enables anybody to add themselves to the system, read transactions, exchange resources and partake in the agreement procedure utilizing PoS, PoW or different components.

- **Private blockchain architecture**

  In contrast private blockchain architecture are open to specific user form the organization or authorized user who are having invitation to participate in blockchain. Private Blockchain, conversely, is to a great extent brought together in nature and carefully consent, permitting just a pre-affirmed set of individuals to use and send transactions and participate in the consensus procedure. Usually worked to oversee inner hierarchical capacities, specifically for review purposes. Speed and execution are among the main points of interest of private

Blockchain. Since it is set up in a controlled situation with a limited number of nodes, transactions are executed a lot quicker.

- **Consortium blockchain architecture**
  Consortium Blockchain is a combination of public and private Blockchain stages. It use the decentralized idea of the open Blockchain and the consent ability of the private Blockchain. Similarly, as with any consortium, the whole system, alongside approval principles and strategies, is characterized and represented by individuals. They control each part of the Blockchain, including approval of transactions, the expansion of blocks, and so on.

III. CONSENSUS ALGORITHMS

Consensus is created by all the nodes in the network. It is an agreement which includes information about which blocks are valid and which are not. Invalid blocks will be rejected by other nodes in network. In blockchain, there is no centralized node that guarantees records on distributed nodes are all the same. A few conventions are expected to guarantee records in various nodes are reliable.

One of the approaches is the poW (proof of work) is a consensus strategy used in the Bitcoin network [2]. Once the block is transmitted using peer to peer communication to all other nodes, the same is included in the blockchain and any tentative transactions are rolled back [7].

IV. APPLICATIONS OF BLOCKCHAIN FOR TRANSFORMATION IN INDIA

1. Agriculture

Agribusiness is 16% of the all-out Gross domestic product in India.12 corer farmers are straightforwardly associated with horticulture. There are numerous farmers who kill themselves regularly. Why they kill themselves? Since it is possible that they need equipment's to get yields going. They possess the land which is extremely little or at some point, they don't have their own property or at some point because of defilement in the framework their properties are not individually named on the record. So they won't get the loan from the administration. They take it from other individuals. How a blockchain can help farmers? Blockchain can create a fractional ownership. Group of farmers can own one tractor. Same can be done with the costlier farming equipment's also, so there will be no compelling reason to purchase equipment's for the poor farmers. They can share them and can diminish the budgetary burden.

Governments everywhere throughout the nation are presently endeavoring to digitize the land. Be that as it may, security of such online information is less as anybody can change the quantities once they have the authority for. Additionally by digitizing the information government can follow information of current client as well as past client. It is hard to know the historical backdrop of the land by using traditional system. Like Who the land belonged before? To fathom this issue blockchain can help. Andhra Pradesh began to move all the farming information to the blockchain. As information in blockchain is hard to hack or temper.

Smart contracts can likewise can an imperative job in agriculture. The little grounds can be associated with one another through the blockchains, cultivating equipment can be obtained through the fragmentary proprietorship and the benefit can be disbursed between the approved farmers. Nobody can change the information once the blockchains are composed. There by less shot of getting less benefit than they get.

2. Energy

For us in India, power is the centralized thought. Power plants can create power and from that power can be transmitted to different parts. It works actually well in urban communities yet towns regard Lesly faces issues. People can transmit power with particular advancement. They can make them monetarily appropriate. People in towns can utilize solar or wind control plant, tidal power plant and they can trade power to the locales where it is required. Again fractional ownership can be used to diminish the budgetary load of the beginning installation. The idea of cryptocurrency can be used to get money. Money can be traded from where the power is transmitted to and the part where produced is produced.

3. Healthcare

The general vision for blockchain is to create a common database of health information that doctors can access irrespective of what electronic medicinal framework they utilized. Blockchain provides higher security and protection, less administrator time for specialists so there's more opportunity to spend on patient care instead of knowing the history of patients and better sharing of research results to encourage new medication and treatment therapies for the disease.

Not only could blockchains encourage new drug development by making patients information even more commonly accessible with the patient's consent, but it could also help diminish the fake drug proposals that cost pharmaceutical companies $200 billion in mishaps consistently.

4. Education

E-transcripts in training is an agonizing procedure for the understudies to get a new job or to get affirmation in the new school. Customary procedure in the schools is a very tedious procedure. Rather than this obsolete way universities can utilize the blockchain to store information safely and furthermore to send transcripts and cash to peer-peer organize. Information put away in blockchains are secured on account of specialized disappointments like failures.

Digital degrees and certifications- counterfeit degrees are much simple also fashion with talented falsifiers growing new procedures continually to ensure that produced degrees are imperceptible. Blockchains can be utilized issue one of a kind computerized resources that confirm the accreditations of scholarly degrees and affirmations. This would make it a lot simpler for potential managers to veri0fy the degrees to spare time.

5. Transportation

New Blockchain-enabled permits easy exchange of data that is shared on the distributed database making physical paperwork highly unnecessary. By utilizing smart contracts, endorsements and custom clearance can be quicker and progressively productive lessening handling times for merchandise at checkpoints. Organizations need new, secure and real information for decision making. Blockchain guarantees reliable information over the transportation since the whole system adds to information approval. The simply refrigerated shipment generally goes through many associations, requires many separate correspondences. Any hiccup in these could make the container be held up or lost. With Blockchain, these steps can be recorded safely and permanently in the system. With the rising enthusiasm for same-day and one-hour delivery traditional system won't scale. Blockchain development gives a versatile, brief response for solicitation following and confirmation With Blockchain,

V. Future Applications of blockchain

In future blockchain can be used in voting system [5], smart contracts [6], banking system, media and entertainment sector, government sector, Ecommerce sector, automotive sector, smart cities [7] and so on.

References

[1] "State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: http://www.coindesk.com/ state-of-blockchain-q1-2016/

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

[3] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed. Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc: eee: monogr:9780128021170.

[4] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, 2014.

[5] Ashish Singh, Kakali Chatterjee, "SecEVS : Secure Electronic Voting System Using Blockchain Technology", Computing Power and Communication Technologies (GUCON) 2018 International Conference on, pp. 863-867, 2018

[6] N. Szabo, "The idea of smart contracts," 1997.

[7] Charles Shen, Feniosky Pena-Mora, "Blockchain for Cities—A Systematic Literature Review", Access IEEE, vol. 6, pp. 76787-76819, 2018.