

# Blockchain Technology for Agriculture Development

VINAY A

*Computer Science Student, VVIET, Mysore*

-----\*\*\*-----

**Abstract** - This study aims to figure out the meaning of Blockchain. Why it is one of the booming technology in the modern world. The blockchain is not only a technology its a trend nowadays in every part of the sectors. Its the technology beyond the Bitcoin. To know whether it can be used beyond what we are thinking it can do. The main intention of this study is to learn about the signing and Verification process in Blockchain. How can we make use of this technology in agriculture and other sectors in India? Everything in the world will be having its drawbacks in the same way to study the drawbacks of Blockchain technology.

## INTRODUCTION

This study aimed to focus on the use of Blockchain in the Indian agriculture sector.so what is Blockchain? This technology was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008. A blockchain is essentially a distributed database of records or public ledger of all synchronized across networks. This will help the multi-organizational companies to share their data behind firewalls.

But blockchain has four key characteristics which make it different:

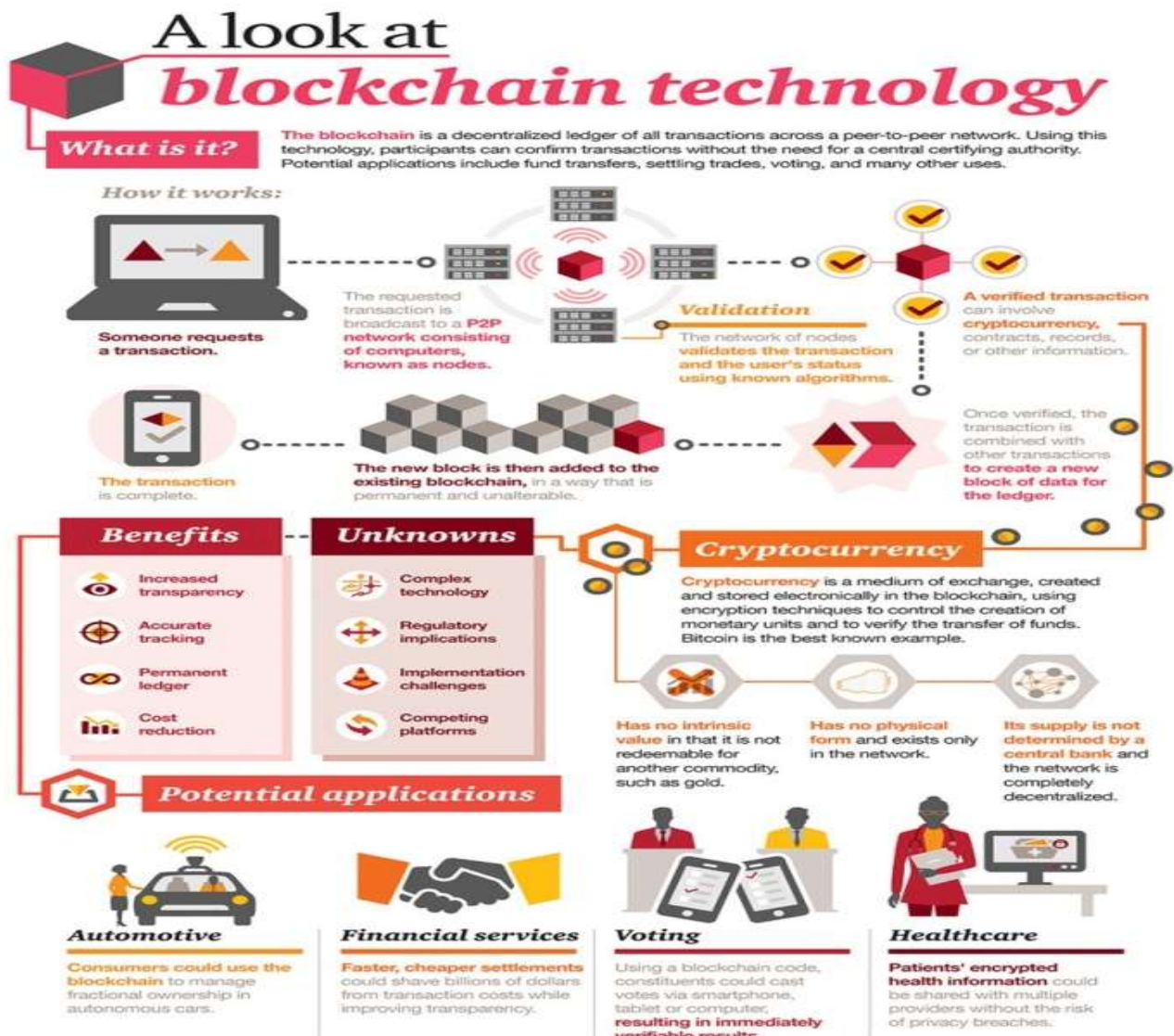
1. It is designed to be distributed and transactions or digital events that have been executed and shared among participating parties. This means its a block of data that is shared among every party in the network. The main hypothesis is that the blockchain establishes a system of creating a distributed consensus in the digital online world.

We now know the meaning of the Blockchain. Let us know why it is booming in the modern world. The cybercrime becomes the major threat due to this Trust and integrity are the major terms the modern online world lack and these are the things needed by every individual who is in the search of safety of his/her transactions in the network. But this technology provides trust and integrity which is needed. The core problem to be solved by the blockchain is achieving and maintaining integrity in a purely distributed peer-to-peer system that is comprised of an unknown number of peers with unknown reliability and trustworthiness.

2. Data cannot be manipulated easily. The types of transactions one can carry out are agreed between participants in advance and stored in the blockchain as "smart contracts.

3. Before one can execute a transaction, there must be an agreement between all relevant parties that the transaction is valid. This process is known as "consensus" and it helps keep inaccurate or potentially fraudulent transactions out of the database.

4. Immutability of the data. Once you have agreed on a transaction and recorded it, it can never be changed



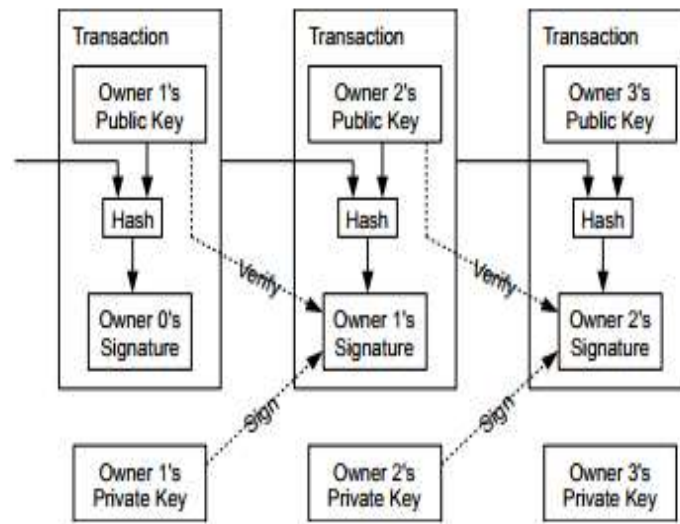
### Signing and Verification process in Blockchain

Hashes are used in blockchains to represent the current state of the world. The input is the entire state of the blockchain, meaning all the transactions that have taken place so far and the resulting output hash represents the current state of the blockchain.

The first hash is calculated for the first block or the Genesis block using the transactions inside that block. The sequence of initial transactions is used to calculate a block hash for the Genesis block. For every new block that is generated afterward, the previous block's hash is also used, as well as its own transactions, as input to determine its block hash. This is how a chain of blocks is formed, each new block hash pointing to the block hash that came before it. This system of hashing guarantees that no transaction in the history can be tampered with because if any single part of the transaction changes, so does the hash of the block to which it belongs, and any following blocks' hashes as a result. It would be fairly easy to catch any tampering as a result because you can just compare the hashes. This is cool because everyone on the blockchain only needs to agree on 256 bits to represent the potentially infinite state of the blockchain. The Ethereum blockchain is currently tens of gigabytes, but the current state of the blockchain, as of this recording, is this hexadecimal hash representing 256 bits

In asymmetric encryption systems, users generate something called a key pair, which is a public key and a private key using some known algorithm. The public key and private key are associated with each other through some mathematical relationship. The public key is meant to be distributed publicly to serve as an address to receive messages from other users, like an IP address or home address. The private key is meant to be kept secret and is used to digitally sign messages

sent to other users. The signature is included in the message so that the recipient can verify using the sender's public key. This way, the recipient can be sure that only the sender could have sent this message. Generating a key pair is analogous to creating an account on the blockchain, but without having to actually register anywhere. Pretty cool. Also, every transaction that is executed on the blockchain is digitally signed by the sender using their private key. This signature ensures that only the owner of the account can move money out of the account.



## DRAWBACKS

The main disadvantage of the Blockchain is the high energy consumption. The consumption of power is needed for keeping a real-time ledger. Every time the new node is created and at the same time, it communicates with each and another node. In this way, transparency is created.

The signature verification is the challenge of the Blockchain because each transaction must be signed with a cryptographic scheme, the big computing power is necessary for the calculation process to the sign. It is one of the reasons for high energy consumption.

The next problem of the Blockchain is the opportunity to split the chain. The nodes, which are operating to the old software, won't accept the transactions in the new chain. This chain is creating with the same history as the chain, which is based on the old software. Another problem of the Blockchain is the balance between the nodes' quantity and the favorable costs for users. Now there are the nodes are lacked for the Blockchain correctly and powerful work. In this case, the costs are higher, because the nodes received higher rewards; but the transactions completed more slowly because the nodes do not work-intensive

## CONCLUSION

The blockchain has been and will continue to be the subject of further improvements and developments such as variations in its implementation, improving efficiency, improving scalability, and conceptual advances. It is necessary to keep exploring the Blockchain development and application in the different areas for the nearest future because this new technology can help to solve many difficult problems, which are disturbing and preventing correctly systems work. In the next part we will be knowing how it can be implemented.

## REFERENCES

1. <http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>
2. <https://www.ibm.com/blogs/cloud-computing/2017/04/11/characteristics-blockchain/>
3. <https://www.beingcrypto.com/why-is-blockchain-important-for-business/>
4. <https://www.linkedin.com/pulse/what-blockchain-why-so-important-mark-van-rijmenam>

5. <https://bc.itrc.ac.ir/sites/default/files/blockchain%20basics%20a%20non-technical%20introduction%20in%2025%20steps%20also%20viewed.pdf>
6. [https://www.researchgate.net/publication/330028734\\_The\\_Advantages\\_and\\_Disadvantages\\_of\\_the\\_Blockchain\\_Technology](https://www.researchgate.net/publication/330028734_The_Advantages_and_Disadvantages_of_the_Blockchain_Technology)
7. <https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/>
8. <https://www.wired.com/story/guide-blockchain/>