International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 08 | Aug - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Understanding Bitcoin and Blockchain

Shivani Sugurushetty,
BE in CSE.

Abstract

Blockchain is the technology that enables the existence of cryptocurrency. Bitcoin is the name of the most recognized cryptocurrency, the one for which blockchain technology, as we currently know it, was created. A cryptocurrency is a medium of exchange such as the US dollar, but is digital and uses cryptographic techniques and its protocol to verify the transfer offunds and control the creation of monetary units.

Keywords: crypto, digital currency, blockchain, bitcoin.

1. Introduction

Blockchain is a new technology, which is known as distributed ledger Technology (DLT). A distributed database, which is shared over a computer network. Anything of value can be tracked and traded on the blockchain network. Blockchain stores information electronically in a digital format to make transactions secure. With the help of blockchain technology, currency as well as anything can be converted into digital format and stored.

Blockchain is database which is used to manage the data in blocks and are linked through a chain. These blocks cannot be hacked. Blockchain technology aims to keep documents digitally secure.

2. Properties of Blockchain

- **Smart contracts:** Auto execution of digital contracts.
- **Secured:** All records are individually encrypted.
- **Trusted:** Data is decentralized and managed by multiple participants.
- **Consensus:** All network participants agree to the validity of each of the records.
- **Time-stamped:** A transaction timestamp is recorded on a block.
- **Immutable:** Any validated records are irreversible and cannot be changed.
- **Distributed:** All trusted participants have a copy of the ledger for completetransparency.

Blockchain allows digital information to be recorded and distributed. Blockchain is an irreversible record of transactions, which cannot be changed, deleted or destroyed. In the year 2009, blockchain was used in bitcoin. Bitcoin was invented in 2008 by Santoshi Nakamoto an unknown person. Use of bitcoin as a currency began in 2009. Bitcoin is a cryptocurrency which is built on the basis of block technology. Blockchain has since been used in the creation of various cryptocurrencies, decentralized finance application, non-fungible tokens and smartcontracts.

3. Cryptocurrency

A cryptocurrency is a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it. For example, Bitcoin uses a method called "Elliptic Curve Cryptography" to ensure that transactions involving bitcoin are secure. Elliptic curve cryptography is a type of public-key cryptography that relies on mathematics to ensure the security of transactions with cryptocurrencies, even if part of the network is compromised, the rest will continue to be able to verify transactions correctly. The pure digital asset is anything that exists in a digital format and carries with it the right to use it. Currently, digital assets include digital documents, motion picture and so on. The market in fact evolved since its inception in 2009, with the first digital asset "Bitcoin". For this reason, we call the cryptocurrency the "first pure digitalasset.

4. Working

Cryptocurrency is a medium of exchange, created and stored electronically on the blockchain, using cryptographic techniques to verify the transfer of funds and an algorithm to control the creation of monetary units. Bitcoin is best known example.

Cryptocurrencies like bitcoin are conducted on peer-to-peer network structure. Each peer has a complete history of all transactions, thus recording the balance of each account. For example, a transaction is a file that says "A pays X bitcoin to B" that is signed by A using its private key. This is basic public-key cryptography, but also the building block on which cryptocurrencies are based. After being signed, the transaction is broadcast on the network. When a peer discovers a new transaction, it checks to make sure that the signature is valid. If the verification is valid then the block is added to the chain; all other blocks added after it will "confirm" that transaction. For example, if a transaction is contained in block 402 and the length of the blockchain is 407 blocks, it means that the transaction has 5 confirmations.

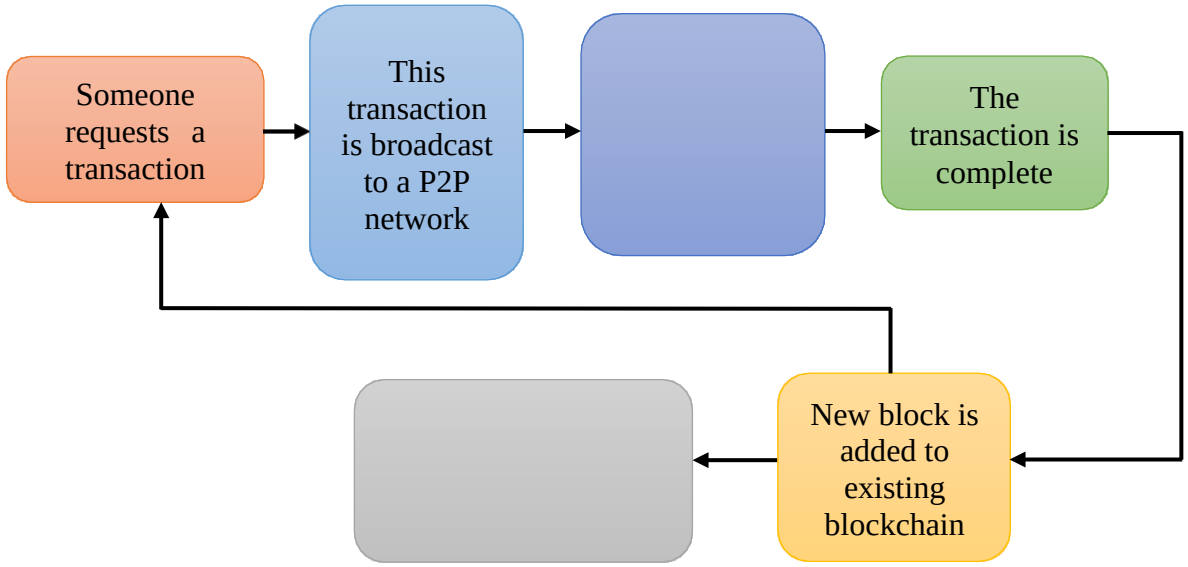

Fig. 1: Workflow of Blockchain Transaction

5. Advantages and Disadvantages of Blockchain Technology

Advantages:

- **Open:** One of the major advantages of blockchain technology is that it is accessible to all means anyone can become a participant in the contribution to blockchain technology, one does not require any permission from anybody to join the distributed network.

- **Verifiable:** Blockchain technology is used to store information in a decentralized manner so everyone can verify the correctness of the information by using zero-knowledge proof through which one party proves the correctnessof data to another party without revealing anything about data.

- **Permanent:** Records or information which is stored using blockchain technology is permanent means one needs not worry about losing the data because duplicate copies are stored at each local node as it is a decentralized network that has a number of trustworthy nodes.

- **Tighter security:** Blockchain uses hashing techniques to store each transaction on a block that is connected to each other so it has tighter security. It uses SHA256 hashing technique for storing transactions.

- **Efficiency:** Blockchain removes any third-party intervention between transactions and removes the mistake making the system efficient and faster. Settlement is made easier and smooth.

- **Cost Reduction:** As blockchain needs no third man it reduces the cost for the businesses and gives trust to the other partner.

Disadvantages:

- **Immaturity:** Blockchain is only a couple-year-old technology so people do not have much confidence in it, they are not ready to invest in it yet several applications of blockchain are doing great in different industries but still it needsto win the confidence of even more people to be recognized for its complete utilization.

- **Energy consuming:** For verifying any transaction a lot of energy is used so it becomes a problem according to the survey it is considered that 0.3 percent of the world's electricity had been used by 2018 in the verification of transactionsdone using blockchain technology.

- **Time consuming:** To add the next block in the chain miners need to compute nonce values many times so this is a time-consuming process and needs to be speed up to be used for industrial purposes.

- **Storage:** Blockchain databases are stored on all the nodes of the network creates an issue with the storage, increasing number of transactions will require more storage.

6. Conclusion

Based on the study, it can be concluded that blockchain is the right technology for cryptocurrency in commercial transactions because it allows cryptocurrency to work without a central authority. This can reduce risk as well as transaction costs.

7. References

- https://blockchain.gov.in/Home/BlockChain?blockchain=blockchain#
- https://jfin-swufe.springeropen.com/articles/10.1186/s40854-021-00321-6#Sec59
- https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain- cryptocurrency.html
- https://en.wikipedia.org/wiki/Bitcoin#:~:text=Based%20on%20a%20free%20market,of%20its%20open%2Dsource%20implementation.
- https://www.geeksforgeeks.org/advantages-and-disadvantages-of-blockchain/
- https://ieeexplore.ieee.org/document/9609790