Indian Institute of Information Technology, Vadodara

HS201 Term Report

Blockchain Technology

Archit Agrawal
202051213
B.Tech CSE Undergraduate

December 25, 2021

Table of Contents

Abstract

Blockchain is considered to be a disruptive core innovation. Albeit many researchers have realized the eminence of blockchain, the research of blockchain is still in its infancy. Consequently, this study reviews the important properties of blockchain technology such as decentralization, immutability, cryptographic hashing, consensus mechanism etc.

1 INTRODUCTION

A cryptographically secured chain of blocks, commonly called as a blockchain was first invented in 1991 by Stuart Haber and W. Scott Stornetta. A number of computer scientists researched on blockchains and its features. Nick Szabo worked on a decentralized digital currency known as 'bit-gold' in 1998. Stefan Konst published a theory on blockchains and gave his ideas for its implementation in 2000. The technology made a major breakthrough in 2008, when some developer or developers working under the pseudonym Satoshi Nakamoto published a white paper describing a digital cryptocurrency titled "Bitcoin: A Peer-to-Peer Electronic Cash System". In 2009, Nakamoto published the first blockchain for transactions made using Bitcoin by defining the genesis block of bitcoin.

In the last decade, researchers have separated the blockchain technology from digital currencies and explored the potential of the technology in various other sectors such as real estate, healthcare management, supply chain management, copyright protection etc. This phase of the technology is popularly known as Blockchain 2.0.

The growing emergence of blockchain can be assessed from the fact that currently there are nearly 8000 cryptocurrencies in the world which has severely increased from just a handful (nearly 70) in 2013. In September 2021, El Salvador became the first country to use bitcoin as legal tender.

This paper begins with a very easy to understand working of blockchain and its fundamentals. It also discusses the benefits of these features in different ways. Thereupon, it focuses on the various fields in which blockchain technology can or has already been implemented.

2 ANALYSIS

2.1 Blockchain

Consider an example of a bank. A bank has a ledger that stores the information about the transactions that occur throughout. To put it in simple words, a blockchain is nothing but a ledger that stores information depending on the use case. It is a chain of blocks where each block stores some information and a cryptographic hash code. This hash code is not just a random binary or hexadecimal code. The block also stores a hash of the previous block. All the data stored in the block along with the hash of previous block is used to create a hash of the current block.

The chain is the connection among these blocks. Every block contains a hash of previous block which can be used to trace the chain of blocks. The initial block that does not have any previous block hash is called the genesis block. In general, a blockchain is a type of database that only supports reading and appending.

2.2 Fundamentals of Blockchain

In this section, the fundamental features of blockchain are discussed briefly using easy examples for better understanding. The key features of blockchain technology are:

- **Decentralization**

  A blockchain is a decentralized, distributed peer-to-peer system of nodes each storing the whole blockchain or a part of it. Let us take the example of the bank used in the previous section. The bank holds the record of all the transactions, that is, a ledger which is not accessible to anyone. The account holders have to trust the bank, that is, they have to trust a central party. Blockchain Technology removes the requirement of a central party. This feature of blockchain is known as decentralization.

This architecture provides for the automatic distribution of software and other information across the network. Decentralization also reduces the possibility of a single point of failure and the reliance on a central authority that must be trusted.

This may aid in the reduction of corruption. Because the bank is the only one who has access to the ledger, they may make any modifications they want, and the clients may not even notice. However, in a decentralized system, every user has access to the ledger, so any modifications are more likely to be discovered.

Decentralization also minimizes the risk of data centers being hacked. Consider an online payment system. It will have a central server that will store all of its user information. If a hacker gains access to their servers, the data of all users is compromised. As there is no central server in a blockchain, no one can hack all of the data at once.

- **Cryptographic Hashing**

A chronological chain is generated by the hashed connection encoded in every block of a blockchain to the previous block. Hashing, in addition to the consensus method, assures that the entire chain, including the content, cannot be changed because a modification would influence one specific hash value, and from there, all subsequent hash values, rendering the chain invalid.

This adds another layer of protection. Data modification is now difficult itself. If someone wants to benefit, they must change the entire blockchain; otherwise, it will be invalid. Even if someone manages to modify the entire blockchain, all users linked to this network will be able to identify these changes.

- **Timestamping**

  Every record in a blockchain is chronologically timestamped. It provides consumers with full transaction history, traceability, and transparency. Timestamps combined with a cryptographic hash can be used as a Proof-of-Existence for specific information at a specific moment.

- **Immutability**

  The data added in a blockchain cannot be altered or deleted. This means that a blockchain can only be appended. This is ensured with the help of cryptographic hashing.

- **Proof of Work**

Consider the scenario where someone in the network, figured out a way of tampering with data without it being noticed by others. He/she can now think of tampering the data of whole blockchains. The concept of Proof of Work restricts such tampering of data. Proof of Work is a form of cryptographic proof in which one party proves to others that a certain amount of a specific computational effort has been expended.

Changing a block's hash requires some computational time. Changing the hash of a single block in Bitcoin takes 10 minutes to compute. As a result, changing the entire blockchain is not possible.

- **Consesus Mechanism**

  The layers of security in blockchains are not ended yet. One last layer is added by the use of consensus algorithms. Suppose, someone achieved the unthinkable, that is, someone changed the hash of all the blocks in the blockchain. Because the system is decentralized, each node in the network will vote for a specific change that is being implemented. If more than a certain percentage of nodes reported the change as invalid, it will be discarded. Consensus Rule is the name given to such a voting system.

2.3 Applications of Blockchain

The most widespread use of blockchain technology is in the field of digital currencies, commonly called as cryptocurrencies. Bitcoin, Ethereum, Ripple, PolkaDot are some most common cryptocurrencies. The use of cryptocurrencies has made transactions much efficient and cheaper. People in two different parts of the world can send and receive Bitcoin in minutes and with minimal transaction fees. Such transactions necessitate no currency conversions or third-party commissions, saving both time and money.

A blockchain supply chain can assist participants in recording price, date, location, quality, certification, and other relevant information in order to manage the supply chain in a better way.

The immutable nature of blockchain provides a history of ownership and creation that cannot be tampered. This property of blockchain is used in real estate. It functions as a digital notary system and keeps track of the entire history of real-estate properties. It can also be used in copyright protection or protection of intellectual property. It can also be used in healthcare management systems where the medical information of a person can be stored in blockchains.

3 CONCLUSION

The fundamental features of blockchain technology such as decentralization, immutability, timestamping, consensus algorithms etc. makes it exceptional and capable of revolutionizing different sectors such as healthcare, supply chains, digital transactions etc. It creates a permanent and immutable record of every transaction. Its decentralized structure eliminates the need for a central party, making it a trusted technology without trusting a central party.

The impenetrable digital ledger makes fraud, hacking, data theft, and information loss impossible. Companies such as Google, Walmart, Microsoft are some of the earliest adopters of this technology.

4 REFERENCES

[1] Leible, S., Schlager, S., Schubotz, M. and Gipp, B., 2021. A Review on Blockchain Technology and Blockchain Projects Fostering Open Science.

[2]IoT For All. 2021. How Blockchain Can Help to Protect Intellectual Property in the Age of the Internet of Things. [online] Available at: ¡https://www.iotforall.com/blockcha
intellectual-property-iot¿

[3]Deloitte United States. 2021. Using Blockchain to Drive Supply Chain Transparency and Innovation. [online] Available at: ¡https://www2.deloitte.com/us/en/pages/oper supply-chain-innovation.html¿

[4] Xu, M., Chen, X. and Kou, G., 2021. A systematic review of blockchain.