IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN AND CRYPTOCURRENCY: SIGNIFICANCE OF DISTRIBUTED COMPUTING

Dr. Shamsudeen E
Assistant Professor of Computer Applications
EMEA College of Arts and Science, Kondotty, Kerala, India

ABSTRACT:
Nowadays the cryptocurrency has been the hot topics for the entire world and its popularity of this decentralized electronic currencies known as has dramatically increased. Bitcoin cryptocurrency is implemented with the concept of distributed computing, signaled the emergence of a radically new form of digital money that operates outside the control of any government or corporation.With time, people began to realize that one of the underlying innovations of bitcoin, the blockchain, could be utilized for other purposes. The blockchain technology is a relatively new approach in the field of information technologies. Blockchain is a distributed public ledger technology that originates from the digital cryptocurrency, bitcoin. Its development has attracted wide attention in industry and academia fields. As one of its first implementations, bitcoin as a cryptocurrency has gained a lot of attention. This article is meant to give a brief introduction to these topics.

Kerywords: Distributed computing, bitcoin, blockchain, distributed ledger

1. INTRODUCTION

Distributed systems are becoming more and more used and has significance in the area of cryptocurrency. They are a sophisticated field of study in databases and its applications,especially decentralised.

A distributed system, also known as distributed computing[1], is a system with multiple components located on different machines that communicate and coordinate actions in order to appear as a single coherent system to the end-user. It does not reveal the existence of multiples systems. i.e., the user feels that all services are get done by the system which is located on his table.

The machines that are a part of a distributed system may be computers, physical servers, virtual machines, containers, or any other node that can connect to the network, have local memory, and communicate by passing messages[2].

If you have been following banking, investing, or cryptocurrency[3] over the last ten years, you may have heard the term blockchain, the record-keeping technology behind the Bitcoin[4] network.

All these above term are examples of a pure distributed system. That is the blockchain and bitcoin are the result of distributed computing.

2. THE DISTRIBUTED COMPUTING AND BLOCKCHAIN TRANSACTIONS

Distributed computing is one of the fundamental computing principles that drives blockchain[5]. But what exactly is distributed computing? Many people now have a basic understanding of a blockchain as a network of computers verifying transactions. However, for anyone interested in digging a little deeper, wondering how key encryption works, or finding out about distributed computing can lead to a better understanding of blockchain technology. Understanding how the technology works isn't just for the scientifically curious.

3. BLOCKCHAIN AND ITS PURPOSE

Blockchain is a chain of blocks that contains information. The technique is intended to timestamp digital documents so that it's not possible to backdate them or temper them. Without the central server the double records problem can be solved by the blockchain.

The blockchain is used for the secure transfer of items like money, property, contracts[6], etc. without requiring a third-party intermediary like bank or government. Once a data is recorded inside a blockchain, it is very difficult to change it.

The blockchain is a software protocol like SMT protocol is for email.interesting thing is that Blockchains could not be run without the Internet. It is also called meta-technology as it affects other technologies. It is comprised of several pieces: a database, software application, some connected computers, etc. Blockchain has the advantages of de-centralization, trustworthiness, anonymity and immutability. It breaks through the limitation of traditional center-based technology and has broad development prospect.

This decentralisation[7] is one of the things that makes blockchain so transformative. Unlike in a traditional, centralised database – where records are processed by one central administrator say, a company or government – the entire blockchain is transparent and data is verified by user consensus. Despite all this transparency, blockchains are incredibly secure. That is because of the fact that there is no one central point of attack for hackers to target.

The reasons why Blockchain technology is being used widely.

Resilience: Blockchains has decentralised architecture. So,the chain is survived even if in the case of a massive attack against the system.

Time reduction: By the use of blockchain technology the quicker settlement of trades as it does not need a lengthy process of verification, settlement, and clearance because a single version of agreed-upon data of the share ledger is available between all stack holders.

Reliability: Blockchain certifies and verifies the identities of the interested parties. This removes double records, reducing rates and accelerates transactions.

Unchangeable transactions: By registering transactions in chronological order, when any new block has been added to the chain of ledgers, it cannot be removed or modified.

Fraud prevention: The concepts of shared information and consensus prevent possible losses due to fraud.

Security: being Distributed Ledger Technology[8], each party holds a copy of the original chain, so the system remains operative when any fail happens.

Transparency: Changes to public blockchains are viewable to everyone. So blockchain provides transparency, and all transactions are immutable.

Collaboration – Blockchain technology allows parties to transact directly with each other without the need any mediator.

Decentralized: There are protocols rules on how every node exchanges the blockchain information. This protocol ensures that all transactions are validated, and all valid transactions are added one by one.

Blockchain can be either public or private,

Public: in this anyone can use a public blockchain network.here, ledgers are visible to everyone on the internet. It allows anyone to verify and add a block of transactions to the blockchain. Public networks have incentives for people to join and free for use.

Private: The private blockchain is within a single organization. It allows only specific people of the organization to verify and add transaction blocks. However, everyone on the internet is generally allowed to view.

3.1. Applications of blockchain

Because blockchain and Bitcoin are so inextricably linked, it took people a long time to realise that blockchain actually has much wider applications beyond cryptocurrency networks. In fact, blockchain's potential is so great that many people believe the technology will revolutionise the way we do business, just like the internet did before it.

Here are just a few examples of the wider applications of blockchain beyond Bitcoin and other cryptocurrencies:

- **Smart contracts.**The blockchain is great for facilitating digital transactions, but it can also be used for formalising digital relationships through smart contracts. With a smart contract, automated payments can be released once the contract terms have been fulfilled, which promises to save time and help to reduce discrepancies or solve disputes without a mediator.
- **Maintaining a shared, transparent system of record.** Blockchain is the fittest solution for maintaining a long-term, secure and transparent record of assets, for example, land rights, that all parties can access the data securely.

- **Auditing the supply chain.** Blockchain allows users to trace the records of ownership for goods.
- **Providing proof of insurance.** Nationwide insurance company is planning to use blockchain to provide proof-of-insurance information. This is a significant tool as far as police officers, insurers and customers and those who verify insurance coverage instantly, which definitely help to speed up the claims process.

4. BITCOIN CRYPTOCURRENCY: MOST POPULAR APPLICATION OF BLOCKCHAIN

A cryptocurrency is one medium of exchange like traditional currencies such as USD, but it is designed to exchange the digital information through a process made possible by certain principles of cryptography. A cryptocurrency is a digital currency and is classified as a subset of alternative currencies and virtual currencies.

Cryptocurrency is a bearer instrument based on digital cryptography. In this kind of cryptocurrency, the holder has of the currency has ownership. No other record kept as to the identity of the owner.

Blockchain is the technology that underpins Bitcoin and it was developed specifically for Bitcoin. So, Bitcoin was the first example of blockchain in action and without blockchain, there would be no Bitcoin. That's why the two names are so often used interchangeably.

But that doesn't mean that blockchain and Bitcoin are the same thing. Bitcoin is a decentralised digital currency, or peer-to-peer electronic payment system, where users can anonymously transfer bitcoins without the interference of a third-party authority like a bank or government. Bitcoin is just one example of a cryptocurrency, though; other cryptocurrency networks are also powered by blockchain technology. So although Bitcoin uses blockchain technology to trade digital currency, blockchain is more than just Bitcoin.

This experiment explores the problem of reaching consensus in a distributed system. "Consensus" is the problem of getting members of a network to agree on something, e.g. a value. In some systems, there is a centralized control unit who can decide on the value and then broadcast it to the rest of a network. In a distributed consensus system, members of the group have to collectively reach consensus without the benefit of a centralized unit. Further complicating the problem, some members of the group may be lying or otherwise manipulating the group to try and reach a consensus that favors them over the "true" value.

Bitcoin uses a process called mining to reach a consensus. Members of the network who choose to take part in the process of reaching a distributed consensus are called miners[9]. Mining involves forming a block containing a series of transaction records, then finding a valid proof of work for that block that satisfies certain rules. Specifically, miners increment a nonce until they find a value that gives the block's hash a certain number of leading zeros, thereby "finding" the next block in the blockchain. For example:Once a block has been "found", it is broadcast to all other nodes in the network, who validate the transactions it holds and accept the block if it is valid.

5. LIMITATIONS OF BLOCKCHAIN TECHNOLOGY

The following are the limitations of blockchain technology,

Higher costs: Nodes seek higher rewards for completing Transactions in a business which work on the principle of Supply and Demand

Slower transactions: Nodes prioritize transactions with higher rewards, backlogs of transactions build up

Smaller ledger: It not possible to a full copy of the Blockchain, potentially which can affect immutability, consensus, etc.

Transaction costs, network speed: The transactions cost of Bitcoin is quite high after being touted as 'nearly free' for the first few years.

Risk of error: There is always a risk of error, as long as the human factor is involved. In case a blockchain serves as a database, all the incoming data has to be of high quality. However, human involvement can quickly resolve the error.

Wasteful: Every node that runs the blockchain has to maintain consensus across the blockchain. This offers very low downtime and makes data stored on the blockchain forever unchangeable. However, all this is wasteful, because each node repeats a task to reach consensus.

6. THE KEY DIFFERENCES

To finish up, let's recap why blockchain and Bitcoin are two completely separate things:

Bitcoin is a cryptocurrency, while blockchain is a distributed database.

Bitcoin is powered by blockchain technology, but blockchain has found many uses beyond Bitcoin.

Bitcoin promotes anonymity, while blockchain is about transparency. To be applied in certain sectors (particularly banking), blockchain has to meet strict Know Your Customer rules.

Bitcoin transfers currency between users, while blockchain can be used to transfer all sorts of things, including information or property ownership rights.

▪

7. CONCLUSION

Blockchain is the technology that underpins Bitcoin and it was developed specifically for Bitcoin. Bitcoin is a decentralised digital currency, or peer-to-peer electronic payment system, where users can anonymously transfer bitcoins without the interference of a third-party authority like a bank or government. Bitcoin is the best example of cryptocurrency and worldwide payment system. The transactions done among the nodes are available on each node of the network. A consensus is being done among transactions inorder to reach a common decision. This leads to solve double spending problem. Here, also distributed computing is used as all the nodes communicate with their neighbor nodes in order to come to a particular decision.

This consensus protocol is implemented to get equal rights to all the nodes and their active participation in the transactions accomplished. This Consensus can establish trust within the peers in the blockchain. Interestingly, all the computations taking place in the blockchain can be termed as distributed system computing.

References

1. Birman, Kenneth. Reliable Distributed Systems: Technologies, Web Services and Applications. New York: Springer-Verlag, 2005
2. William Gropp, Using MPI: portable parallel programming with the message-passing interface, MIT Press, vol. 1, 1999.
3. S. King, “Primecoin: Cryptocurrency with Prime Number Proof-of-Work,” www.primecoin.org/static/primecoin-paper.pdf.
4. S. Nakamoto, 2009, “Bitcoin: A Peer-to-Peer Electronic Cash System”, www.bitcoin.com, unpublished.
5. Liu A D , Du X H , Wang N , et al. Research Progress of Blockchain Technology and Its Application in Information Security[J]. journal of software, 2018.
6. Gebert M . Application Of Blockchain Technology In Crowdfunding[J].New European, 2017.
7. Gray, J. and Reuter, A. Transaction Processing: Concepts and Techniques. San Mateo, CA: Morgan Kaufmann, 1993
8. Masood, Faraz & Faridi, A.. (2018). An Overview of Distributed Ledger Technology and its Applications. International Journal of Computer Sciences and Engineering. 6. 422-427. 10.26438/ijcse/v6i10.422427.
9. Ankalkoti, Prashant & Santhosh,. (2017). A Relative Study on Bitcoin Mining. "Imperial Journal of Interdisciplinary Research (IJIR).