A Through Fundamental Study of Blockchain Technology

1. **V. RAMYA, M. Sc., M. Phil.,**
Part-Time Research Scholar, University of Madras,
Assistant Professor in Computer Science,
Government Arts College for Men(Autonomous),
Nandanam, Chennai-600035**.** TamilNadu.

2. **Dr. M. SURIAKALA, M. Sc., M. Phil., P.hD.,**
Assistant Professor in Computer Science,
Government Arts College for Men(Autonomous),
Nandanam, Chennai-600035**.** TamilNadu

Abstract:

Blockchain is a technology that is developed using a combination of various techniques such as mathematics, algorithms, cryptography, economic models, and so on. Blockchain is a public ledger of all cryptocurrency transactions that are digitized and decentralized. Blockchain technology is a structure that stores transactional records, as the block, of the public in several databases, known as the "chain," in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a 'digital ledger'. Therefore, this study attempts to investigate and explore its Structure, types, process of transaction, and its technologies and applications of Blockchain. Thus, a large number of published studies were carefully reviewed and analyzed based on their contributions to the Blockchain's body of knowledge.

Keywords: Blockchain, Mining, Ledger, Cryptocurrency, Bitcoin, Applications.

Introduction:

A blockchain [1] is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Blockchains are best known for their crucial role in crypto currency systems [2], such as Bitcoin, mining for maintaining a secure and decentralized record of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.

A blockchain collects information together in groups, known as blocks that hold sets of information. Each block contains its own hash. Blocks have certain storage capacities and, filled blockchains are closed and linked to the previously filled block, forming a chain of data known as the blockchain. All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled.

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited because of hash value (hash value cannot be revered). In this way, a blockchain is the foundation for immutable ledgers, or records of transactions that cannot be altered, deleted, or destroyed.

Is Blockchain Secure?

Blockchain technology achieves decentralized security and trust in several ways. To begin with, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. After a block has been added to the end of the blockchain, it is extremely difficult to go back and alter the contents of the block unless a majority of the network has reached a consensus to do so. Because each block contains its own hash, along with the hash of the block before it, as well as the previously mentioned time stamp. Hash codes are created by a mathematical function that turns digital information into a string of numbers and letters. If that information is edited in any way, then the hash code changes as well.

Let's say that a hacker, who also runs a node on a blockchain network, wants to alter a blockchain and steal cryptocurrency from everyone else. If they were to alter their own single copy, it would no longer align with everyone else's copy. When everyone else cross-references their copies against each other, they would see this one copy stand out, and that hacker's version of the chain would be cast away as illegitimate.

Succeeding with such a hack would require that the hacker simultaneously control and alter 51% or more of the copies of the blockchain so that their new copy becomes the majority copy and, thus, the agreed-upon chain. Such an attack would also require an immense amount of money and resources, as they would need to redo all of the blocks because they would now have different time stamps and hash codes.

Architecture Diagram:

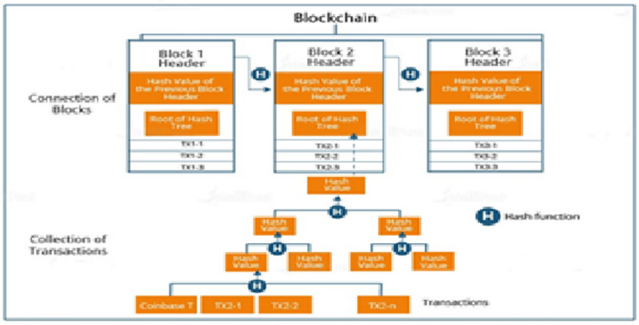

Fig: 1 Structure of Blockchain

A blockchain collects information together in groups, known as blocks that hold sets of information. Each block contains its own hash. Blocks have certain storage capacities and, filled blockchains are closed and linked to the previously filled block, forming a chain of data known as the blockchain. All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled.

Types of Blockchain:

There are four different types of blockchains [3]. They are as follows:

Private Blockchain Networks:

Private Blockchains operate on closed networks, and tend to work well for private businesses and organizations. Companies can use private blockchains to customize their accessibility and authorization preferences, parameters to the network, and other important security options. Only one authority manages a private blockchain network.

Public Blockchain Networks:

Bitcoin and other cryptocurrencies originated from public blockchains, which also played a role in popularizing distributed ledger technology (DLT) [4]. Public blockchains also help to eliminate certain challenges and issues, such as security flaws and centralization. With DLT, data is distributed across a peer-to-peer network [5], rather than being stored in a single location. A consensus algorithm is used for verifying information authenticity; proof of stake (PoS)[6] and proof of work (PoW)[7] are two frequently used consensus methods.

Permissioned Blockchain Networks:

Also sometimes known as hybrid blockchains [8], permissioned blockchain networks are private blockchains that allow special access for authorized individuals. Organizations typically set up these types of blockchains to get the best of both worlds, and it enables better structure when assigning who can participate in the network and in what transactions.

Consortium Blockchains:

Similar to permissioned blockchains, consortium blockchains [5] have both public and private components, except multiple organizations will manage a single consortium blockchain network. Although these types of blockchains can initially be more complex to set up, once they are running, they can offer better security. Additionally, consortium blockchains are optimal for collaboration with multiple organizations.

Process of Transaction:

One of Blockchain technology's cardinal features is the way it confirms and authorizes transactions. For example, if two individuals wish to perform a transaction with a private and public key, respectively, the first person party would attach the transaction information to the public key of the second party. This total information is gathered together into a block.

The block contains a digital signature, a timestamp, and other important, relevant information. It should be noted that the block doesn't include the identities of the individuals involved in the transaction. This block is then transmitted across all of the network's nodes, and when the right individual uses his private key and matches it with the block, the transaction gets completed successfully.

In addition to conducting financial transactions, the Blockchain can also hold transactional details of properties, vehicles, etc.

Here's a use case that illustrates how Blockchain works:

Hash Encryptions:

Blockchain technology uses hashing techniques[9] and encryption[10] to secure the data and information. The address of the sender (public key), the receiver's address, the transaction, and his/her private key are encrypted information, called hash encryption, is transmitted across the world and added to the blockchain after verification.

Proof of Work

In a Blockchain, each block consists of 4 main headers.

- Previous Hash: This hash address locates the previous block.
- Transaction Details: Details of all the transactions that need to occur.
- Nonce: An arbitrary number given in cryptography to differentiate the block's hash address.
- Hash Address of the Block: All of the above (i.e., preceding hash, transaction details, and nonce) are transmitted through a hashing algorithm. This gives an output containing a 256-bit, 64 character length value, which is called the unique 'hash address.' Consequently, it is referred to as the hash of the block.
- Numerous people around the world try to figure out the right hash value to meet a pre-determined condition using computational algorithms. The transaction completes when the predetermined condition is met. To put it more plainly, Blockchain miners attempt to solve a mathematical puzzle, which is referred to as a proof of work problem. Whoever solves it first gets a reward.

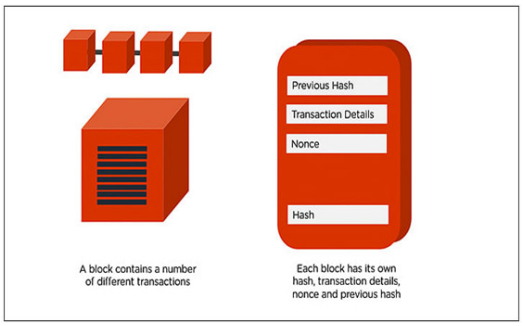

Fig: 2 Proof of Work

Mining

- In Blockchain technology, the process of adding transactional details to the present digital/public ledger is called 'mining.' Though the term is associated with Bitcoin, it is used to refer to other Blockchain technologies as well. Mining involves generating the hash of a block transaction, which is tough to forge, thereby ensuring the safety of the entire Blockchain without needing a central system.

Blockchain is a combination of three leading technologies:

1. Cryptographic keys
2. A peer-to-peer network containing a shared ledger
3. A means of computing, to store the transactions and records of the network

Cryptography keys consist of two keys – Private Key and Public key. These keys help in performing successful transactions between two parties. Each individual has these two keys, which they use to produce a secure digital identity reference. This secured identity is the most important aspect of Blockchain technology. In the world of cryptocurrency, this identity is referred to as 'digital signature' and is used for authorizing and controlling transactions.

The digital signature is merged with the peer-to-peer network; a large number of individuals who act as authorities use the digital signature in order to reach a consensus on transactions, among other issues. When they authorize a deal, it is certified by a mathematical verification, which results in a successful secured transaction between the two network-connected parties. So to sum it up, Blockchain users employ cryptography keys to perform different types of digital interactions over the peer-to-peer network.

Applications:

1. Money Transfers:

Money transfers using blockchain can be less expensive and faster than using existing money transfer services. This is especially true of cross-border transactions, which are often slow and expensive. Even in the modern U.S. financial system, money transfers between accounts can take days, while a blockchain transaction takes minutes.

2. Financial Exchanges:

Using blockchain for exchanges allows for faster and less expensive transactions. Moreover, a decentralized exchange doesn't require investors to deposit their assets with the centralized authority, which means they maintain greater control and security. Blockchain-based exchanges primarily deal in crypto currency, the concept could be applied to more traditional investments as well.

3. Lending:

Lenders can use blockchain to execute collateralized loans through smart contracts[11], built on the blockchain allow certain events to automatically trigger things like a service payment, a margin call, full repayment of the loan, and release of collateral. As the result loan processing is faster and less expensive and lenders can offer better rates.

4. Insurance:

A blockchain can provide greater transparency for customers and insurance providers. Recording all claims on a blockchain would keep customers from making duplicate

claims for the same event. Furthermore, using smart contracts can speed up the process for claimants to receive payments.

5. Real Estate:

Using blockchain technology to record real estate transactions can provide a more secure and accessible means of verifying and transferring ownership. That can speed up transactions, reduce paperwork, and save money.

6. Secure Personal Information:

Blockchain technology can be used to secure access to identifying information while improving access for those who need it in industries such as travel, healthcare, finance and education.

7. Voting:

Using blockchain technology can make sure that nobody votes twice, only eligible voters are able to vote and votes cannot be tampered with. It can increase access to voting by making it as simple as pressing a few buttons on your smartphone. At the same time, the cost of running an election would substantially decrease.

8. Government Benefits:

Another way to use digital identities stored on a blockchain is for the administration of government benefits such as welfare programs, social security and Medicare. Using blockchain technology could reduce fraud and the costs of operations. Meanwhile, beneficiaries can receive funds more quickly through digital disbursement on the blockchain.

9. Securely share medical information:

Keeping medical records on a blockchain can allow doctors and medical professionals to obtain accurate and up-to-date information on their patients. That can ensure that patients seeing multiple doctors get the best care possible. It can also speed up the system for pulling medical records, allowing for more timely treatment in some cases. If insurance information is held in the database, doctors can easily verify whether a patient is insured and their treatment is covered.

10. Artist Royalties:

Using blockchain technology to track music and film files distributed over the internet can make sure that artists are paid for their work. Since blockchain technology was invented to ensure the same file doesn't exist in more than one place, it can be used to help reduce piracy. A smart contract to distribute payments can provide greater transparency and the assurance that artists receive the money they're owed.

11. Non-fungible tokens:

NFTs are commonly thought of as ways to own the rights to digital art. Since the blockchain prevents data from existing in two places, putting an NFT on the blockchain guarantees that only a single copy of a piece of digital art exists. NFTs can have varied applications, and ultimately they're a way to convey ownership of anything that can be represented by data. That could be the deed to a house, the broadcast rights to a video, or an event ticket.

12. Logistics and supply chain tracking:

Using blockchain technology to track items as they move through a logistics or supply chain network can provide several advantages. It provides greater ease of communication between partners since data is available on a secure public ledger. It provides greater security and data integrity since the data on the blockchain can't be altered. That means logistics and supply chain partners can work together more easily with greater trust that the data they're provided is accurate and up to date.

13. Secure IOT networks

The Internet of Things (IOT) is making our lives easier; Blockchain technology can provide greater security by storing passwords and other data on a decentralized network instead of a centralized server. Additionally, it offers protection against data tampering since a blockchain is practically immutable.

14. Data Storage:

Adding blockchain technology to a data storage solution can provide greater security and integrity. Since data can be stored in a decentralized manner, it will be more difficult to hack into and wipe out all the data on the network, whereas a centralized data storage provider may only have a few points of redundancy. In some cases, using blockchain for data storage may also be less expensive.

15. Gambling:

The gambling industry can use blockchain to provide several benefits to players. One of the biggest benefits of operating a casino on the blockchain is the transparency it provides to potential gamblers. Since every transaction is recorded on the blockchain, betters can see that the games are fair and the casino pays out. By using blockchain, there's no need to provide personal Information , including a bank account, which may be a hurdle for some would-be gamblers.

Conclusion:

Blockchain Technology has high value and good prospects in resolving problems of data integrity, improving transparency, enhance security, preventing fraud, and establish trust and privacy. Blockchain Technology can bring revolution in the areas of Finance, Accounting, e-Government, insurance, entertainment, trading platforms, healthcare, internet-of-things, as well as law firms and others. Hence, Blockchain Technology has a huge potential in introducing innovative solutions, depending on the area or the sector of its implementation, since economic efficiency and social benefits can be achieved through technical innovation and applications.

In conclusion, more intensive research in this area of Blockchain Technology is necessary to advance the maturity of this field, since it is still in the exploratory stage and there are many legal and technical issues to be resolved. Therefore, this review offers a useful starting point for future research themes for the development of Blockchain application, and assist practitioners and researchers.

References:

1. Ackermann, J. & Meier, M.," The_next_generation_of_blockchain_systems [Accessed 12 10 2018]".
2. Paul J. Taylor a , Tooska Dargahi a , Ali Dehghantanha b , Reza M. Parizi c , Kim-Kwang Raymond Choo d "A systematic literature review of blockchain cyber security".
3. Anita.n , vijayalakshmi.m "Blockchain Security Attack: A Brief Survey "
4. Ateniese, G., Fu, K., Green, M., and Hohenberger, S. (2006)." Improved proxy reencryption schemes with applications to secure distributed storage. ACM Transactions on Information and System Security (TISSEC), 9(1):1–30".
5. Subhasis Thakur, John G. Breslin "Peer to Peer Energy Trade Among Microgrids Using Blockchain Based Distributed Coalition Formation Method".
6. Gusti Ayu Kusdiah Gemeliarana , Riri Fitri Sari "Evaluation of proof of work (pow) blockchains security network on selfish mining".
7. Wenting Li, S´ebastien Andreina, Jens-Matthias Bohli, and Ghassan Karame "Securing Proof-of-Stake Blockchain Protocols".
8. Jingkuang Liu, Lemei Yan, Dong Wang " A Hybrid Blockchain Model for Trusted Data of Supply Chain Finance".
9. Jinhua Fu , Sihai Qiao, Yongzhong Huang, Xueming Si, Bin Li, and Chao Yuan" A Study on the Optimization of Blockchain Hashing Algorithm Based on PRCA".
10. Sheping Zhai, Yuanyuan Yang, Jing Li , Cheng Qiu and Jiangming Zhao " Research on the Application of Cryptography on the Blockchain"
11. Survey on Blockchain based Smart Contracts: Technical Aspects and Future Research Tharaka Mawanane Hewa , Yining Hu , Madhusanka Liyanage , Salil Kanhare , and Mika Ylianttila.
12. https://www.sciencedirect.com/topics/engineering/blockchain
13. https://www.kaspersky.com/resource-center/
14. https://www.oracle.com/middleeast/blockchain/
15. https://www.investopedia.com/terms/d/distributed-ledgers/
16. https://www.sciencedirect.com/science/article/pii/
17. https://www.fool.com/investing/stock-market/market-sectors/financials/