Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

A Comprehensive Study on Blockchain Technology

Sunil Kumar Dewangan

Assistant Professor, Computer Science & Engineering Shri Shankaracharya Institute of Professional Management & Technology, Raipur, India sunil.raipur@gmail.com

Astha Pathak

Assistant Professor, Information Technology Shri Shankaracharya Institute of Professional Management & Technology, Raipur, India
a.pathak@ssipmt.com

Vaishali Raheja

Undergraduate, Information Technology Shri Shankaracharya Institute of Professional Management & Technology, Raipur, India
vaishaliraheja03@gmail.com

Harshal Shende

Undergraduate, Information Technology Shri Shankaracharya Institute of Professional Management & Technology, Raipur, India Harshal.shende5555@gmail.com

Chaitanya Verma

Undergraduate, Information Technology Shri Shankaracharya Institute of Professional Management & Technology, Raipur, India
chaitanyaverma453@gmail.com

Sambhav Jain

Undergraduate, Information Technology Shri Shankaracharya Institute of Professional Management & Technology, Raipur, India
sambhavjn68@gmail.com

Article Info
Page Number: 462-469
Publication Issue:
Vol. 72 No. 1 (2023)

Article History
Article Received:
15 October 2022
Revised: 24 November 2022
Accepted: 18 December 2022

Abstract

Blockchain can be demarcated as a shared or distributed, immutable archive that provides the process of recording transactions. This innovation has given an important turn to the business environment. Keeping record of facts and details about transactions are vital part. Generally, those fact and data are passed through a trusted third party which increases both time and cost on business. Instead of this lengthy process Blockchain provides much faster process for transaction, which helps in saving money and time without the need of any third party. It assures data clarity, integrity and security as it is cannot be tampered. Blockchains are famous for their important role in cryptocurrency systems, like Bitcoin. Blockchain technology also has some other applications in healthcare, Business management, supply chains, banking

and Finance. The impartial of this paper is to study about what blockchain technology actually is, how does it work and its various underlying features and applications.

Keywords: Blockchain Technology, Bitcoin, Ledger

I. Introduction

The idea of Blockchain Technology was acquainted by Stuart Haber and W. Scott Stornetta in 1991. Further, the theory of distributed blockchains was intellectualized by Satoshi Nakamoto in 2008.[1] A blockchain has the ability to handle, process and store data without any need of centralized administration. Blockchain collects data in groups which holds set a of information also known as blocks. Blocks have some storehouse requirements and, when fulfilled are linked to the block which was previously filled and are closed, forms a chain or sequence of data or blocks generally referred as the blockchain. All new data which tails that recent block is collected in to a lately build block which will also be affixed to the chain formerly full.

A record usually structures the data into tables, but blockchain assemblies the data into blocks or chunks that are threaded together. When a block is completely occupied, it is set and then converts a member of this timeline. An exact timestamp is given to each block in the chain when it is added.

The main aim of blockchain technology is to permit cardinal data to be distributed and recorded, but unedited. Thus,

blockchain is the support for unassailable ledgers or data of transactions that can't be obliterated or altered. Hence, blockchains are also called a DLT (Distributed Ledger Technology).

It is more important to accentuate that Blockchain is a very new technology which has confirmed to be a feasible solution in creating trust in ecosystem without central authority and a proven example of this could be the Bitcoins.

There are many forms of blockchain technology and they are classified as permissionless blockchains and permissioned blockchains. In Permissioned blockchains access to network is restricted it authorize limited number of writers and readers. They're controlled by a central authority which decides whether the individual can write or read. Whereas Permissionless blockchains is accessible to anyone. Bitcoin is an example of permissionless or open blockchain. They are decentralized and the information is readable by users.[3]

II. Literature Review

One of the greatest cyber-security problems faced by an individual, business or an organization is data theft, because it threatens an individual's privacy. To deal with this issue many techniques have been suggested and several of them were proved unsuccessful. The rearmost addition is the Blockchain Technology.[3] It generates an audit trail that passes the derivation of an asset at each step or in other words it produces a record that cannot be

rehabilitated and is encrypted end-to-end. Blockchain technology eliminates the issue on several levels.

A blockchain can be explained as a shared database comprising information or a ledger that keeps records of all the transactions and events, executed and distributed between the concerned parties. Information entered cannot be erased and transactions are verified. Each transaction executed had a verifiable record. Blockchain is updated constantly which makes it efficient for the users to modify and access information whenever they want to. It is a shared database which in sense means that identical copies of data are spread across the network and stored securely. In real time when you update one record it updates every other copy. Blockchain has verified data. Because of some cryptographic techniques it doesn't allow tampering of data hence data is secured. Blockchain Technology is used in both fiscal as well as non fiscal sectors.

III. Characteristics of Blockchain

III. 1. Privacy: -

Traditional/old banking systems frequently bear much information and documents to create an account. However, with public blockchain system there is no limitation on how many accounts that you can create and you don't have to pay any amount for building an account hence, does not need any identity verification. Ethereum and bitcoin are presently the most famous public blockchain networks. When you send Ether on Ethereum platform, the correspondent and recepients are both just hold location, public key. Each operation will be transmitted on the main net.[4]

Zero-Knowledge Proof - Public blockchain network use some mechanisms to protect an idividual's address from being traced and hide some transactions. ZKP (Zero-knowledge proof) is a proof which permits to prove that no information is disclosed during a process of transaction except for sharing some acquaintance of an undisclosed to both the verifier and prover. Verifier should not obtain any information after corroboration and before corroboration. There are two types of ZKP first one is interactive and the second one is non-interactive ZKPs. Interactive ZKP requires intervention among individualities to prove their knowledge and validates individual for proof. They are kind of intuitive.[5] It formerly has numerous requests in the communication sector, and this classification needs both a stable and nonstop communication channel. Whereas Non-interactive ZKP doesn't requires any of that, it takes lower time and only one communication is enough.

Permissioned Blockchain Network: - It generally includes a consortium of associations who vindicates the transition history rather than asking miners to share in the removal process.[6] Approved blockchains are frequently prevalent in the organizations that depends on digital information, like manufacturing industry, supply chain management. These organizations consider data privacy, data security and role definition very seriously and are keen to pursue advanced efficiency.

III.2. Security: -

Proof of Work (PoW): - It is a harmony algorithm /strategy of Bitcoin. In computer science a consensus algorithm is defined as a process which is used to attain an agreement on single data value between shared systems.[7] PoW is commonly known as a secure harmony algorithm. This mechanism depends heavily on cryptographic hash function and computing power.[1]. In PoW hash value of block header is premeditated by each node. The header consists of a time being and miners which could change the time being continuously to get dissimilar hash values. The agreement need premeditated value should be identical or less than the given value. When a node meets the goal value, it transmits the block to other nodes and all other nodes should authorize that the hash value is correct or not. If the block is verified then other nodes add this block to their own blockchain. This is generally cast-off by disseminated systems. It elucidates that in the ultramodern computing period, how multiple servers can work with each other and with great levels of security and a smaller number of errors. In further detail, some servers may not be reliable in other conditions for example, while being hacked, Thus, consensus algorithms should be flexible and fault free. This is the core part of a blockchain network.

Proof-of-Stake (PoS): - In PoS miners are incentivized to prove the ownership of the currency which they contributed. Here miners are asked to bet tokens so that they can take part in new block generation. PoS is much simpler, hoards more vigor and is much effective than PoW. Peercoin was the first one to discuss this concept in 2012[8]. and had later become a famous discussion among many cryptocurrencies. If you stake more, you will highly be able to influence on determining the next block. It is assumed that high staking nodes or people with more currencies are less likely to lie or attack the network because if they do, they will suffer with high losses. Consortium Consensus model and Chain-based stand recently two types of Proof of Stake consensus. [9]. Chain-based Proof-of-Stake selects accessibility over consistency. In this algorithm, throughout each time slot it randomly selects a validator. Then Validators are allowed to generate a sole block and then points it back to the prior one. Consortium Consensus Model chooses consistency over availability. In this every node counts proportionally to the stake it bets during each voting procedure.

IV . Types of Blockchains

	Public	Consortum	Private
Participants	Without permission Anonymous Could be malicious	Permissioned Identified Trusted	Permissioned Identified Trusted
Transaction approval frequency	Long Bitcoin: 10min or more	Short 100* ms	Short 100* ms
Consensus	Proof of work,	Multi-party	Multi-party

mechanism	Proof of stake,etc Large energy consumption No finality 51% attack	consensus algorithm or voting Lighter Faster Low energy consumption Enable finality	consensus algorithm or voting Lighter Faster Low energy consumption Enable finality
Network type	Decentralized	Partially decentralized hybrid between public and private blockchains	Partially decentralized
Benefits	Secure as the entire network verifies transactions	Efficient as relatively lesser nodes verify transactions	Efficient as verification is done by just owner of the blockchain

V. How does Blockchain works?

Blockchain is consist of three chief technologies:

1. Cryptographic keys

2. Peer-to-Peer network comprehending a distributed/ communal ledger

3. Means of computation, to stockpile records and the transactions of the network.[10]

These keys play an important part between two parties to perform a successful transaction. Each individual has these two keys, (i). Public key which is known to everyone and it is widely spread. (ii). Private key which is known only to the person whose private key it is. These two keys are used for generating a safe digital identity orientation. This secure digital distinctiveness is the pivotal facet of Blockchain. In the structure of crypto-currency, this secured distinctiveness is known as Digital Signature and is used for securing a document. Digital Signature is a mathematical technique used to authenticate the legitimacy and veracity of an information, software or digital conents.

A significant number of people who function as establishments use the identity or digital signature to acquire agreement on dealings, amid supplementary things. It is connected to a peer-to-peer network. A verified trade that has been authorized results in a safe and effective transaction between the two linked networks. Therefore, to execute various forms of digital communications via the connected network, Blockchain users make use of cryptography

keys.

The method through which Blockchain technology approves and confirms transactions is one of its main characteristics. Assume that if deuce parties want to complete a transaction using their respective public and private keys, the primary party will ascribe the transaction info to another party's public key. A block is created out of all of this absolute information. A timestamp, a digital signature, and other apposite data are encompassed in the block. The block does not contain information about the those involved in the transaction. The block is then sent to all of the system's nodes, and when the valid person uses his private key to verify that it matches the block, the transaction is successfully accomplished. The Blockchain can also contain transactional facts of vehicles, properties etc.

Every block in the Blockchain contains 4 main headers.

1. Previous Hash: The preceding block is located through this hash address.

2. Transaction Details: Contains minutiae about all the transactions that requires to transpire.

3. Nonce: This is a subjective number provided in cryptanalysis which is use to distinguish the block’s hash address.

4. Hash Address: All of the above are diffused through a hashing algorithm. This produces a 256-bit, 64-character span value, which is known as the exclusive ‘hash address.’ [10] Therefore, it is called the hash the block. The transaction is successfully completed when predefined conditions are met.

Blockchain technology secures data through encryption and hashing, relying on the SHA256 algorithm to do so. [10]

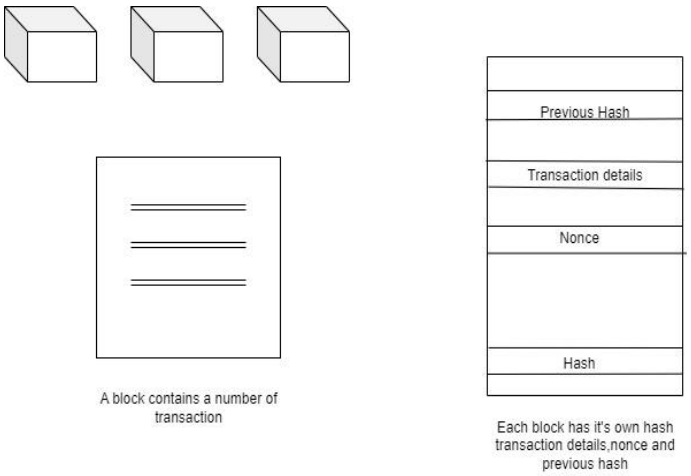

Figure 1: General architecture of a block in blockchain

The dispatcher's address, the beneficiary’s address, the transaction, and the recipient's private key information are all exchanged using the SHA256 method. After being verified, the hash-encrypted information is sent around the globe and added to the blockchain. The despatcher

and beneficiary's authentication is made simple by the SHA256 algorithm's near-impossibility to break the hash encryption.

Blockchains preserve data about financial transactions made with digital currencies. They also store data about product monitoring and other things. For instance, it is possible to follow cabs after the time they are reserved till they arrive at their location. This evidence can be useful if there is an outbreak of contamination since it makes it simple to identify the outbreak's origin. This is just one of the many methods blockchains may be used to hold important data for businesses.

VI. Applications of Blockchain Technology

1. Healthcare: Blockchain have a big wallop on healthcare using smart contracts in which between two parties a contract is made without needing any mediator. All the parties intertwined in the contract know the contract details and when the contract conditions are met the contract is automatically implemented. The Centers for Disease Control and Prevention to prevent security concerns uses this innovation to store Electronic Health Records (HER) on the blockchain network.[11] The FDA is keeping electronic clinical preliminary information, clinical records (emir) and hereditary information on a blockchain-based organization that is protected.

2. Supply chains: Blockchain technology provides a permanent and distributed record of each transaction which is created by distributed ledgers. To authorized participants all the recorded transactions are visible, can be traced within the ledger, irrevocable and immutable, which tells the increase in use of blockchains for sharing facts in supply chains. VeChain uses blockchain to monitor and track the logistic data for, regulated, translucent and safe data sharing. IBM also uses blockchain based data distribution solutions for supply chain.[1]

3. Finance and Banking: Generally speaking, blockchain allows the digitization of financial services by presenting a more open, transparent and secure data management system. HSBC use a blockchain-based framework to records its exchanges. Instead of conventional paper-based arrangements they use another decentralized vault framework. Barclays utilize blockchain to work on Know-Your-Customer (KYC) measures and monetary exchanges.[11]

VII. Conclusion

In this paper, we've introduced one of the most contemporary technologies. Any association or organization's first priority is actually cyber security. Blockchain technology offers sophisticated security features that are challenging to breach. We've looked at what blockchain technology is and why it's so popular right now. We have already covered some of the features of blockchain technology that make it so popular with cryptographers. Tetrad diverse kinds of blockchains are recognized as a result of blockchain networks, and we have also emphasised these in this chapter. The operation of blockchain technology is also covered. One of the well-known uses of blockchain technology, which we have focused on in this study along with a few other uses, is Bitcoin. Despite being the current day answer to

security problems, blockchain technology still faces significant difficulties.

VIII. References

1. Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: Research and Applications, 3(2), 100067. https://doi.org/10.1016/j.bcra.2022.100067
2. H.R Vyawahare, Blockchain Technology: A brief overview,2021
3. Karl Wst et al, Do you need a Blockchain?, Department of Computer Science ETH, International Association for Cryptologic Research, 2017
4. Conti M, Sandeep Kumar E, Lal C, Ruj S. A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys Tutorials. 2018
5. D RR, Adam S, Katerina S. Toward Non-Interactive Zero-Knowledge Proofs for NP from LWE. Journal of cryptology. 2021
6. Podgorelec B, Kersic V, Turkanovic M. Analysis of Fault Tolerance in Permissioned Blockchain Networks. IEEE,2019
7. Ferdous MS, Chowdhury MJM, Hoque MA, Colman A. Blockchain Consensus Algorithms: A Survey,2020
8. King S, Nadal S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,2012
9. Saleh F. Blockchain without Waste: Proof-of-Stake. The Review of financial studies,2020
10. Priyadarshini, Ishaani: Introduction to Blockchain Technology,2019
11. Nouman, M.; Azam, M.; Rehman Gill, A. A Systematic Review of Blockchain Technology in Current Epoch: Applications, Adoption Challenges, and Opportunities, 2022