IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12669

INTRODUCTION TO BLOCKCHAIN TECHNOLOGY AND ITS APPLICATIONS

Rajat Pangantiwar[1], Mrs.Nidhi Damle[2]

Student, P.E.S. Modern college of Engineering, Pune[1]

Professor, P.E.S. Modern college of Engineering, Pune[2]

Abstract: Blockchain, the foundation of Bitcoin, has received extensive attentions recently. Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. However, there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome. This paper presents a comprehensive overview on blockchain technology. We provide an overview of blockchain architecture. Furthermore, technical challenges and recent advances are briefly listed. We also lay out possible future trends for blockchain.

Keywords: Blockchain, decentralization, transaction, scalability

I. INTRODUCTION

Nowadays cryptocurrency has become a buzzword in both industry and academia. As one of the most successful cryptocurrencies, Bitcoin has enjoyed a huge success with its capital market reaching 10 billion dollars in 2016[1]. With a specially designed data storage structure, transactions in Bitcoin network could happen without any third party and the core technology to build Bitcoin is blockchain, which was first proposed in 2008 and implemented in 2009[2]. Blockchain could be regarded as a public ledger and all committed transactions are stored in a list of blocks. This chain grows as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency.

The blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these traits, blockchain can greatly save the cost and improve the efficiency. Since it allows payment to be finished without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment. Additionally, it can also be applied into other fields including smart contracts, public services, Internet of Things (IoT), reputation systems and security services. Those fields favor blockchain in multiple ways. First of all, blockchain is immutable.

Transaction cannot be tampered once it is packed into the blockchain. Businesses that require high reliability and honesty can use blockchain to attract customers. Besides, blockchain is distributed and can avoid the single point of failure situation. As for smart contracts, the contract could be executed by miners automatically once the contract has been deployed on the blockchain.

Blockchain transactions are transparent, meaning they can be viewed by anyone on the network. Once a transaction is recorded on the blockchain, it is extremely difficult to alter or tamper with it due to cryptographic hashing and consensus mechanisms. This immutability ensures the integrity of the data stored on the blockchain.

Although the blockchain technology has great potential for the construction of the future Internet systems, it is facing a number of technical challenges. High integrity of transactions and security, as well as privacy of nodes are needed to prevent attacks and attempts to disturb transactions in Blockchain. In addition, confirming transactions in the Blockchain requires a computational power.

The rest of the paper is organized as follows. Section II literature Survey of blockchain technology. In Section III shows blockchain architecture. Section IV shows types blockchain and technology. Section V shows Transaction of blockchain. Section VI Applications of blockchain technology.

Section VII Advantages and Disadvantages of Blockchain technology. Section VIII concludes the paper.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12669

II. LITERATURE SURVEY

Satoshi Nakamoto [3] (born 5 April 1975) is the name used by the presumed pseudonymous person or persons who developed bitcoin, authored the bitcoin white paper, and created and deployed bitcoin's original reference implementation.

The Author [4] defined as bitcoin is a chain of digital signatures. The chain of ownership can be verified using signatures.

The author [5] discussed in his paper was that Blockchain is a new technology and used in applications like artificial intelligence, human enhancement, and smart contract etc.

The author [6] explained the characteristics of Bitcoin, related concepts like proof of work and technical review on distributed currencies.

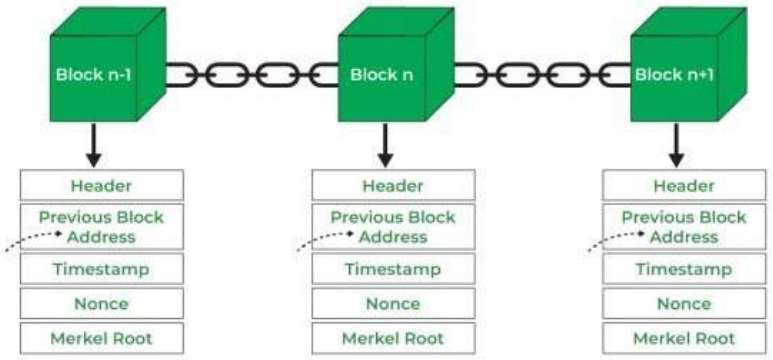
The author [7] proposed a model for exchange of bitcoins using elliptic curve cryptography

The author [8] mainly focused on Byzantine agreement and concept of the ledger in a distributed environment. The author discussed in his paper that transactional privacy in a decentralized smart contract system.

III. BLOCKCHAIN ARCHITECTURE

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger [9]. Blockchain is a backlinked, decentralized and distributed-database of encrypted records. It's a data structure where each block is linked to another block in a timestamped chronological order. It's an append only transactional database, not a replacement to the conventional databases. Every node keeps a copy of all the transactions happened in the past which are secured cryptographically. All information once stored on the ledger is verifiable and auditable but not editable. Highly fault tolerant as there is no Single-point-of-failure.

Blockchain is a technology where multiple parties involved in communication can perform different transactions without third-party intervention. Verification and validation of these transactions are carried out by special kinds of nodes.



Header: It is used to identify the particular block in the entire blockchain. It handles all blocks in the blockchain. A block header is hashed periodically by miners by changing the nonce value as part of normal mining activity, also Three sets of block metadata are contained in the block header.

Previous Block Address/ Hash: It is used to connect the i+1th block to the ith block using the hash. In short, it is a reference to the hash of the previous (parent) block in the chain.

Timestamp: It is a system verify the data into the block and assigns a time or date of creation for digital documents. The timestamp is a string of characters that uniquely identifies the document or event and indicates when it was created.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12669

Nonce: A nonce number which uses only once. It is a central part of the proof of work in the block. It is compared to the live target if it is smaller or equal to the current target. People who mine, test, and eliminate many Nonce per second until they find that Valuable Nonce is valid.

Merkel Root: It is a type of data structure frame of different blocks of data. A Merkle Tree stores all the transactions in a block by producing a digital fingerprint of the entire transaction. It allows the users to verify whether a transaction can be included in a block or not.

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions. Digital signature based on asymmetric cryptography is used in an untrustworthy environment.

C. Key Characteristics of Blockchain Architecture

Decentralization: In centralized transaction systems, each transaction needs to be validated in the central trusted agency (e.g., the central bank), naturally resulting in cost and the performance jam at the central servers. In contrast to the centralized mode, a third party is not needed in the blockchain. Consensus algorithms in blockchain are used to maintain data stability in a decentralized network.

Persistency: Transactions can be validated quickly and invalid transactions would not be admitted by persons or miners who mining the crypto. It is not possible to delete or roll back transactions once they are included in the blockchain network. Invalid transactions do not carry forward further.

Anonymity: Each user can interact with the blockchain with a generated address, which does not disclose the real identity of the miner. Note that blockchain cannot guarantee perfect privacy preservation due to the permanent thing.

Auditability: Blockchain stores data of users based on the Unspent Transaction Output (UTXO) model. Every transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the position of those referred unspent transactions switches from unspent to spent. Due to this process, the transactions can be easily tracked and not harmed between transactions.

Transparency: The transparency of blockchain is like cryptocurrency, in bitcoin for tracking every transaction is done by the address. And for security, it hides the person's identity between and after the transaction. All the transactions are made by the owner of the block associated with the address, this process is transparent and there is no loss for anyone who is involved in this transaction.

Cryptography: The blockchain concept is fully based on security and for that, all the blocks on the blockchain network want to be secure. And for security, it implements cryptography and secures the data using the cipher text and ciphers.

IV. TYPES OF BLOCKCHAIN

[1] Public Blockchain:

A public blockchain is a concept where anyone is free to join and take part in the core activities of the blockchain network. Anyone can read, write, and audit the ongoing activities on a public blockchain network, which helps to achieve the self-determining, decentralized nature often authorized when blockchain is discussed. Data on a public blockchain is secure as it is not possible to modify once they are validated.

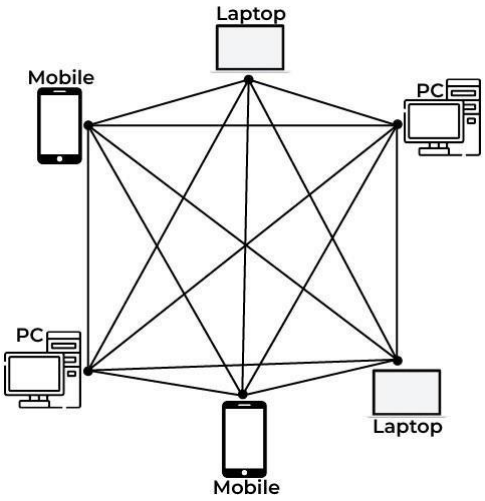
The public blockchain is fully decentralized, it has access and control over the ledger, and its data is not restricted to persons, is always available and the central authority manages all the blocks in the chain. There is publicly running all operations. Due to no one handling it singly then there is no need to get permission to access the public blockchain. Anyone can set his/her own node or block in the network/ chain. After a node or a block settled in the chain of the blocks, all the blocks are connected like peer-to-peer connections. If someone tries to attack the block then it forms a copy of that data and it is accessible only by the original author of the block.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

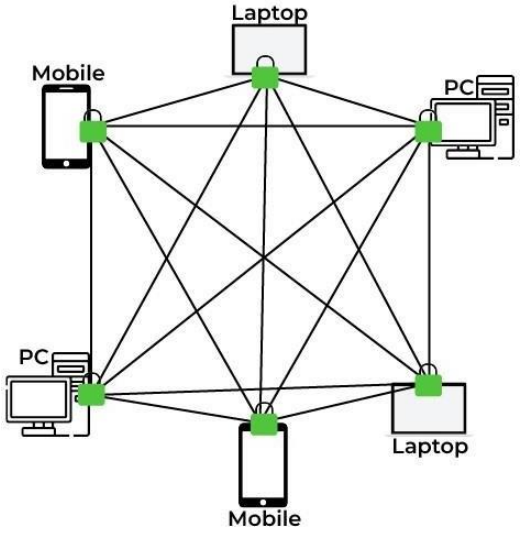
DOI: 10.17148/IJARCCE.2023.12669



[2] Private Blockchain

Miners need permission to access a private blockchain. It works based on permissions and controls, which give limit participation in the network. Only the entities participating in a transaction will have knowledge about it and the other stakeholders not able to access it.

By it works on the basis of permissions due to this it is also called a permission-based blockchain. Private blockchains are not like public blockchains it is managed by the entity that owns the network. A trusted person is in charge of the running of the blockchain it will control who can access the private blockchain and also controls the access rights of the private chain network. There may be a possibility of some restrictions while accessing the network of the private blockchain.



[3] Consortium Blockchain

A consortium blockchain is a concept where it is permissioned by the government and a group of organizations, not by one person like a private blockchain. Consortium blockchains are more decentralized than private blockchains, due to being more decentralized it increases the privacy and security of the blocks. Those like private blockchains connected with government organizations‟ blocks network.

Consortium blockchains is lies between public and private blockchains. They are designed by organizations and no one person outside of the organizations can gain access. In Consortium blockchains all companies in between organizations collaborate equally. They do not give access from outside of the organization’s consortium network.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12669

B. TYPES OF BLOCKCHAIN TECHNOLOGY

1. Digital Signature

Digital signatures are a fundamental building block in blockchains, used mainly to authenticate transactions. When users submit transactions, they must prove to every node in the system that they are authorized to spend those funds, while preventing other users from spending them. Every node in the network will verify the submitted transaction and check all other nodes‟ work to agree on a correct state. If Alice wants to send Bob 1 bitcoin, she must sign a transaction spending 1 bitcoin of inputs with her private key and send it to nodes on the network. The miners, who know her public key, will then check the conditions of the transaction and validate the signature. Once validity is confirmed, the block containing that transaction is ready for finalization by a validator/miner.

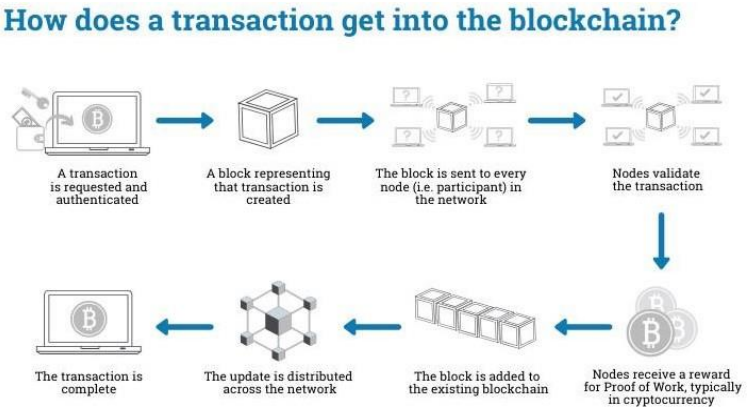
2. Encryption and Decryption:

In encryption, public and private key pairs will be used. The public key is used for encryption and the private key is used for decryption. Suppose there is a communication between Alice and Bob, Alice sends a message that is encrypted with Bob public key and then sends to bob. Bob decrypted the message with its own private key. To know the communication between Alice and Bob, the attacker must get both the private keys.

3. Cryptographic Keys

Cryptographic 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.

V. TRANSACTION ON BLOCKCHAIN TECHNOLOGY



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. Hash Encryptions

blockchain technology uses hashing and encryption to secure the data, relying mainly on the SHA256 algorithm to secure the information. The address of the sender (public key), the receiver’s address, the transaction, and his/her private key details are transmitted via the SHA256 algorithm. The encrypted information, called hash encryption, is transmitted across the world and added to the blockchain after verification. The SHA256 algorithm makes it almost impossible to hack the hash encryption, which in turn simplifies the sender and receiver’s authentication.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12669

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 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.

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.

VI. APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

1. Blockchain in Healthcare

Blockchain technology is being used to track and trace prescription medications throughout supply networks. Using this tool, it is possible to simply and swiftly prevent and regulate the distribution of counterfeit pharmaceuticals and recall ineffective and unsafe drugs.

2. Management of the Supply Chain

The unchangeable ledger of blockchain makes it ideally suited to activities like real-time tracking of commodities as they travel and change hands across the supply chain. Using a blockchain provides enterprises carrying these items with various possibilities. An entry on a blockchain might be used to prioritize supply chain tasks such as allocating freshly delivered commodities among numerous shipping containers.

3. Protection of Copyright and royalties

Many copyright and ownership regulations on music, films, blogs, and other internet content are required in today's world. Blockchain technology can make these regulations more secure and easy to apply. It also provides content creators and artists with real-time and genuine royalty distribution statistics. Any type of digital material download might be traced to guarantee that the artist or author gets their fair share.

4. Cryptocurrency

Cryptocurrency is one of the most prominent blockchain applications. Everyone is aware of bitcoin. One of the numerous benefits of adopting blockchain for cryptocurrencies is that it has no territorial boundaries. cryptocurrencies may be utilized for global transactions.

5. 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 financial system, money transfers between accounts can take days, while a blockchain transaction takes minutes. 6. 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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12669

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.

VII. ADVANTAGES AND DISADVANTAGES OF BLOCKCHAIN TECHNOLOGY ADVANTAGES

1. 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.

2. 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 correctness of data to another party without revealing anything about data.

3. 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.

4. Free from Censorship: Blockchain technology is considered free from censorship as it does not have control of any single party rather it has the concept of trustworthy nodes for validation and consensus protocols that approve transactions by using smart contracts.

5. 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 SHA 256 hashing technique for storing transactions.

DISADVANTAGES:

1. Scalability: It is one of the biggest drawbacks of blockchain technology as it cannot be scaled due to the fixed size of the block for storing information. The block size is 1 MB due to which it can hold only a couple of transactions on a single block.

2. 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 needs to win the confidence of even more people to be recognized for its complete utilization.

3. 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 transactions done using blockchain technology.

4. 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.

VIII. CONCLUSION

Blockchain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability Blockchains gives robust, distributed peer to peer systems and ability to interact with peers in a trustless and auditable manner. In this paper we discuss first about the blockchain technology. Then the architecture of blockchain and its characteristics. We then discuss about the types and technologies of blockchain. Furthermore, about the applications and finally discuss about advantages and disadvantages of the blockchain technology. In the future many processes will use blockchain technology.

REFERENCES

[1] "State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: http://www.coindesk.com/state-ofblockchain-q1-2016/
[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.[Online].Available: https://bitcoin.org/bitcoin.pdf
[3] Electronic Cash System. https://bitcoin.org/bitcoin.pdf.
[4] Swan M. "Blockchain thinking: The brain as a DAC (decentralized autonomous organization)", Texas Bitcoin

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12669

Conference. 2015: 27-29.
[5] FlorianTschorsch,BjörnScheuermann "Bitcoinand Beyond:ATechnical Survey on Decentralized Digital Currencies" 2016 ieeexplore.ieee.org/document/7423672.
[6] Huaqun Wang, DebiaoHe, Yimu Ji "Designated-Verifier Proof of Assets for Bitcoin Exchange Using Elliptic Curve Cryptography"2017.
[7] J.Garay, A.Kiayias, and N.Leonardos, The Bitcoin Backbone Protocol: Analysis and Applications, pp. 281–310, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.
[8] KosbaA, Miller A, Shi E, Wen Z, Papamanthou C. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts", 2016 IEEE Symposium on Security and Privacy,2016: 839-858.
[9] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed.Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc:eee:monogr:97 80128021170