IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

# Blockchain: Basics, Applications, Benefits, and Opportunities

**Mr. Aakash Haribhau Kondhalkar**
Student
Bharati Vidyapeeth, Navi Mumbai, India

**Abstract:** *Blockchain has played a major role in financial, sales, medical, cryptocurrency, gaming, and other areas or fields. blockchain comes into focus mainly due to the bitcoin cryptocurrency. and now blockchain has been used in the development of various applications to help make records such as files, audio, video, paintings, gaming nfts secured and provide greater transparency, improved traceability, efficiency, and speed, and reduced cost. in this paper, we will be looking at what blockchain is, what is blockchain consists of, its structure, framework, and how blockchain works in a distributed network environment.*

**Keywords:** Nonce, Hash Value, Consensus, Crypto

## I. INTRODUCTION

Blockchain is a shared ledger technology allowing any participant in the business network to see the system of record and provide a secure and distributed mechanism to record transactions. Blockchain considers a decentralized architecture consisting of blocks containing immutable transactions. Blockchain was first proposed in 2008 by a person named Satoshi Nakamoto and implemented in 2009. Blockchain stores all committed transactions in a chain of blocks. The chain grows continuously as each block gets appended to it. Blockchain saves time, and cost and improves efficiency. Bitcoin application is based on blockchain. Although blockchain is very famous in the cryptocurrency area blockchain is not limited to cryptocurrency. Blockchain can be used in other areas as well such as financial service, gaming, online payment, education, etc. Even though blockchain technology has great potential for future internet systems. It still has several challenges to resolve. Such as scalability interoperability, privacy, costs, etc.

## II. BLOCKCHAIN ARCHITECTURE

Blockchain consists of blocks connected in a sequence. With each block connected to the pre- previous block (via hash value) called the parent block. In Blockchain architecture single block is made up of two parts, firstly header which stores the metadata about a block, and the second body which stores the list of all transactions. (fig. 1)

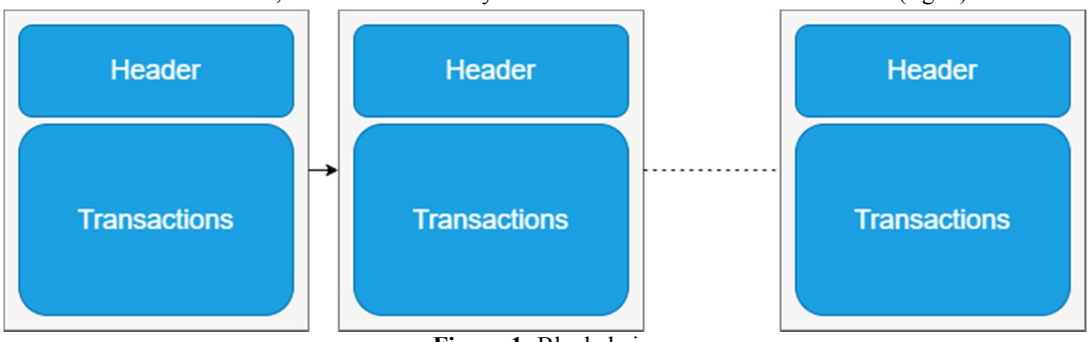


**Figure 1:** Blockchain

The header consists of the following metadata

- **Version -** the current version of the block structure
- **Previous Block Hash -** the reference value of the parent block in the current block
- **Merkle Root Hash -** a cryptographic hash of all of the transactions.
- **Timestamp -** the time when the block was created

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

- **nBits -** the current difficulty that was used to create this block
- **Nonce ("Number Used Once") -** a random value that the creator of a block is allowed to manipulate however they so choose

Apart from headers, the rest of the block consists of transactions.

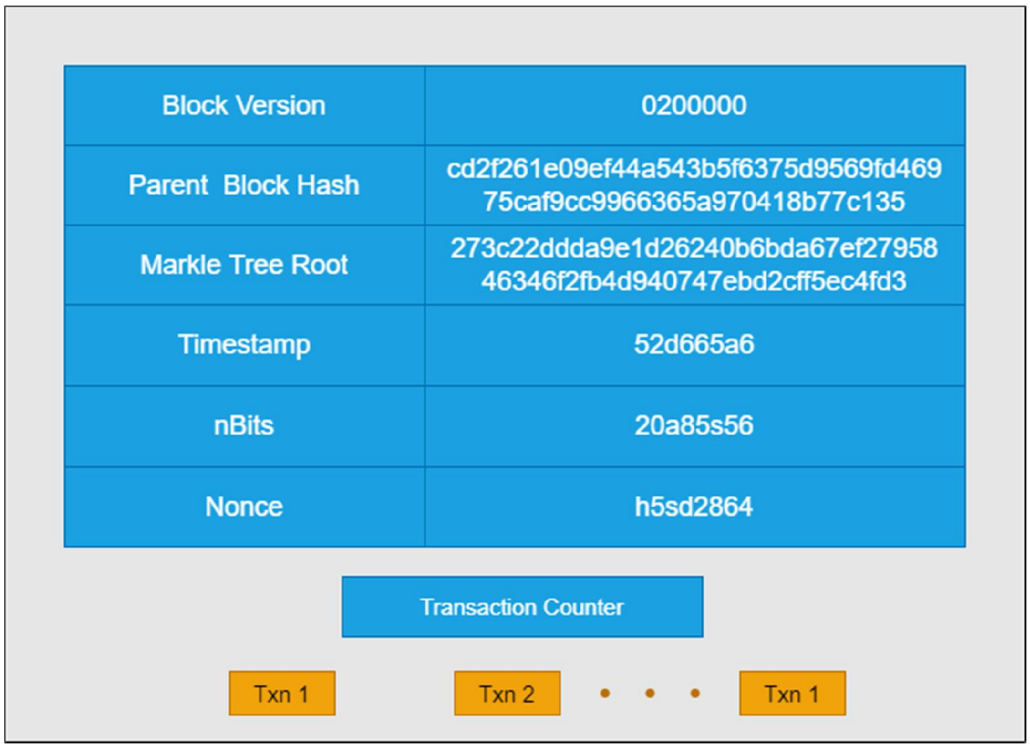


**Figure 2:** Block

## III. BLOCKCHAIN FRAMEWORK

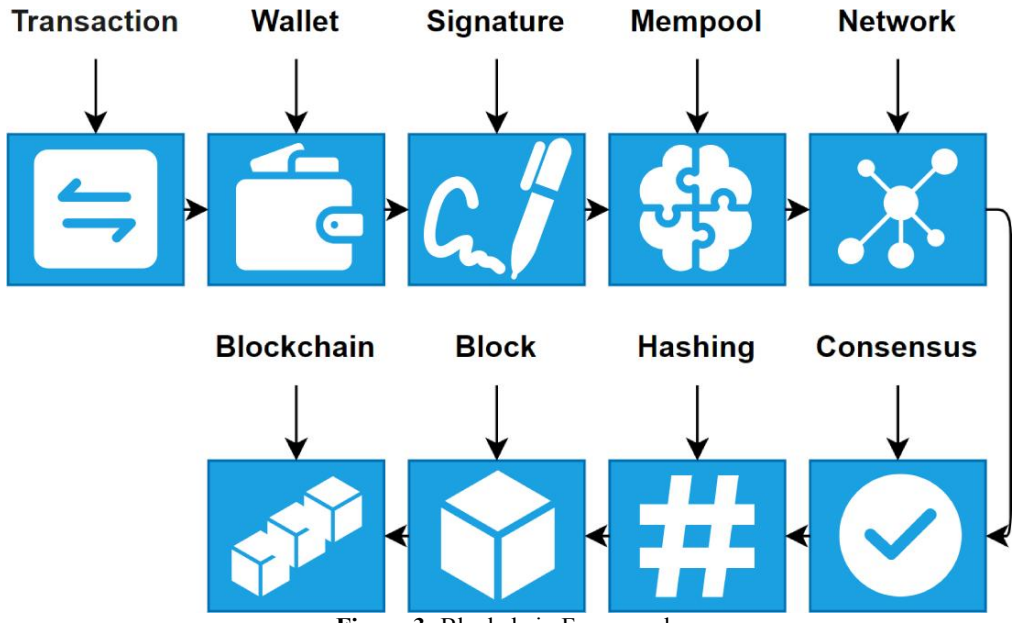


**Figure 3:** Blockchain Framework

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

1. **Transaction:** A blockchain transaction is the transfer of cryptocurrency from one address to another.
2. **Wallet:** A blockchain wallet is a digital wallet that allows users to manage, store, and transfer bitcoin and any other cryptocurrency
3. **Signature:** The signature is the main building block of the blockchain, used to validate or authenticate transactions, transaction must be signed by use be- fore transfer to the network by using his/her private key
4. **Mempool:** Mempool is an area where all unverified and newly added transactions are stored before it is verified and added to block in blockchain by miners.
5. **Network:** Blockchain work in a p2p dis- tributed network where all user is connected to each other called nodes and each user has access to the blockchain.
6. **Consensus:** It's an algorithm that validates the block on a network e.g., PoW (Proof of Work) and PoS (Proof of Stake)
7. **Hashing:** Hashing is used to encrypt the transactions on the block, in blockchain SHA256 algorithm is used to encrypt the block data, also hashing is used on the private key to generate a public key using the elliptic curve digital signature algorithm (ECDSA) Algorithm
8. **Block:** A block is a single unit in blockchain that consists of metadata about block and transactions info.
9. **Blockchain:** Block connected with hash value form a chain.

## IV. HOW BLOCKCHAIN WORK

Suppose Alice wants to send money to Bob, then Alice first opens his bitcoin wallet and searches or copies bobs address and enters the transferring and handling fee amount. After that block is created which represents the transaction created by Alice. After which transactions are sent and wait in the mining pool where all newly created and unverified transactions are waiting for the miner to handle. Miners then choose these newly created transactions and mine. After successful mining miner broadcast the block to every node in the network. Other nodes confirm the block legitimacy and transaction correctness. Nodes receive a reward for Proof of Work (PoW). The block is added to the existing blockchain. The transaction is now finished, and the amount is now transferred from Alice to bob's wallet.

## V. KEY BENEFITS

- **Time savings-** Transaction time is reduced from days to minutes. transaction settlement is faster because it doesn't need verification by a central authority.
- **Cost savings-** Blockchain networks need less oversight because the network is self-monitored by network participants. also, no need for Intermediaries required to exchange cryptocurrency.
- **Security-** Blockchain protects transactions against tampering, fraud, and cybercrime.
- **Privacy-** Through the use of IDs and per- missions, users can specify which transaction details they want other participants to be permitted to view. Per- missions can be expanded for special users such as auditors who may need access to more transaction detail.

## VI. ADVANTAGE

- **Distributed -** Since blockchain data is stored on a distributed network of nodes. data is less prone to technical failure and cyber-attacks. There is no single point of failure as each node on the network is store a copy of the database. Even if one node goes offline does not affect the availability and security of the network.
- **Stability -** the block is very unlikely to be reversed once mined successfully. Once the data has been stored in blockchain, it is very difficult to alter the data or remove it. This is the reason blockchain is a great technology for storing financial records.
- **Trustless system -** In a payment system that we use today like GPay, BHIM UPI, PhonePe, etc. transactions not only involve sender and receiver but also an intermediary such as banks, and credit card companies. But when we use blockchain there is no third party involved as a node on the network verifies and validates transactions using a process called mining. For this reason, blockchain refers to a trustless system.
- **Transparency -** Blockchain transaction history is transparent everywhere, all the node in the network shares a copy of the transaction. any change that occurs in the transaction is visible to other nodes on the same network.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

## VII. DISADVANTAGES

- **Scalability-** The biggest disadvantage of blockchain technology is scalability as it cannot be scaled due to the fixed size of the block. Block can store up to 1MB of data onto it. Due to this, it can store a couple of transactions on a single block.
- **Trust-** About nearly 95 percent of cryptocurrencies are fake. People around the world are afraid to invest in cryptocurrency because it is so hard to identify which cryptocurrency is fake and which one genuine
- **Inefficient-** Blockchains especially those which work on PoW (Proof of Work), are highly inefficient. Since mining requires a lot of computational power it requires lots of servers and computer computers to do a lot of work to solve a complex mathematical problem. These computers and servers consume more energy than countries such as Nigeria and Ireland

## VIII. CONCLUSION

Blockchain is a promising technology and is highly appreciated and accepted for its peer-to-peer and deserialized infrastructure. blockchain has been changing how people do business as blockchain is designed to eliminate the in-intermediaries role, particularly in the financial transaction space. blockchain uses an algorithm for verifying transactions using a consensus mechanism that provides security.

Blockchain showed its potential through cryptocurrency applications, but now blockchain is being used beyond the digital currency field. blockchain can be used across various domains, as this paper demonstrated in healthcare, media, energy, advertising and media, and many others.

Blockchain is a future of banking and finance, but blockchain facing some issues with scalability, security, and most important regulation. because there are no regulations and rules blockchain is being used for money laundering across the world. another problem with blockchain is that it is hard to find which blockchain is genuine and which one is fake. because of this people are afraid to invest in blockchain.

Another problem with blockchain is that blockchain needs a lot of energy to validate a transaction by solving complex math problems before adding to the block. this problem can be solved using the PoS (Proof of Stake) consensus mechanism over PoW (Proof of Work) which consumes a lot of energy. Ethereum runs on PoS whereas Bitcoin uses PoW.

## REFERENCES

**[1].** H. Kopka and P. W. Daly, A Guide to LATEX, 3rd ed. Harlow, England: Addison-Wesley, 1999.
**[2].** Abou Jaoude, J. and Saade, G.R. (2019). Blockchain Applications - Usage in Different Domains. IEEE Access 7.
**[3].** Adams, R., Glenn Parry, G., Godsiff, P., and Ward, P. (2017). The Future of Money and Further Applications of The Blockchain. Strategic Change, 26(5), 417- 422.
**[4].** Ahram et al. (2017). Blockchain Technology Innovations. IEEE Technology and Engineering Management Conference (TEMSCON).
**[5].** Buterin, V. (2015) On Public and Private Blockchains, https://blog.ethereum.org/2015/08/07/onpublic- and-private-blockchains/
**[6].** Foroglou, G. and Tsilidou, A-L. (2015) Further Applications of the Blockchain.
**[7].** Barcelo, J. (2014) User Privacy in the Public Bitcoin Blockchain.
**[8].** Zyskind, G., Nathan, O. et al. (2015) Decentralizing privacy: Using blockchain to protect personal data, Security and Privacy Workshops (SPW), 2015 IEEE, IEEE, pp.180184.
**[9].** Zheng, Z., Xie, S. and Dai, H., Chen, X., and Huaimin Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE 6th international Congress on Big Data, 557-564.
**[10].** White, G. (2017). Future Applications of Blockchain in Business and Management: A Delphi Study. Strategic Change, Vol. 26, No. 5, PP. 439- 451.
**[11].** Tran, T. (2018). Blockchain Technology and Potential Applications in Online Advertising. International Conference on Marketing in the Connected Age (MICA-2018), Danang City, Vietnam.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

**[12].** Perkinson, J. and Miller, R. (2016). Unimpeachable Blockchains: Could Blockchain Revolutionize the Accounting Profession. Chartered Accountants Australia and New Zealand.

**[13].** Puthal, D., Malik, N., Mohanty, S., Kougianos,E. and Das, G. (2018). Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems. IEEE Consumer Electronics Magazine, 6-14.

**[14].** Silvestre et al. (2020). Blockchain for power systems: Current trends and future applications. Renewable and Sustainable Energy Reviews 119.

**[15].** Smith, S. S. (2018a). Blockchain Augmented Audit - Benefits and Challenges for Accounting Professionals. The Journal of Theoretical Accounting Research, 14 (1), 117-137.

**[16].** Veuger, J. (2018). Trust in A Viable Real Estate Economy with Disruption and Blockchain. Facilities, 36, 103-120.

**[17].** Woodside, M. J., Augustine Jr, K. F., and Giberson, W. (2017). Blockchain Technology Adoption Status And Strategies. Journal of International Technology and Information Management, 26(2), 65-93.

**[18].** The banker (2018). Why Blockchain Can Revolutionize Trade Finance. Banker, 169, (1110).

**[19].** Treleaven, P., Brown, G.R. and Yang, D. (2017). Blockchain Technology in Finance. Computer Published by The IEEE Computer Society, 14-17

**[20].** Workie, H. and Jain, K. (2017). Distributed Ledger Technology: Implications of Blockchain For the Securities Industry. Journal of Securities Operations and Custody, 9 (4), 347-355

**[21].** Xia et al. (2017). MeDShare: Trust-less Medical Data Sharing Among Cloud Service Providers Via Blockchain. IEEE Access, 5, 14757 - 14767.