International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A Review on Blockchain Technology

Pooja B[1], Dr. Ganavi M[2]

[1] VIII Sem student, Department of CSE, JNN College of Engineering

[2] Asst. Prof., Department of CSE, JNN College of Engineering

1. poojab3112@gmail.com 2. gaanavi4@jnnce.ac.in
Corresponding author: poojab3112@gmail.com

Abstract

Blockchain technology has emerged as a disruptive force with the potential to revolutionize various industries by offering decentralized, secure, and transparent solutions for data management and transactions. Initially conceptualized as the underlying technology for cryptocurrencies like Bitcoin, blockchain has evolved into a versatile tool applicable across diverse domains such as finance, supply chain management, healthcare, and government services. This paper provides an overview of blockchain technology, its fundamental principles, and key components. It explores the decentralized consensus mechanisms, cryptographic techniques, and data structures that underpin blockchain networks, ensuring immutability, transparency, and integrity of recorded transactions. Furthermore, the paper examines the challenges and opportunities associated with blockchain adoption, including scalability, interoperability, regulatory concerns, and environmental impact. Through a comprehensive review of existing literature and case studies, this research elucidates the potential benefits of blockchain technology, such as increased efficiency, reduced costs, enhanced security, and improved trust among participants. Additionally, it highlights ongoing developments, innovations, and future directions in blockchain research and implementation, emphasizing the need for interdisciplinary collaboration and regulatory frameworks to realize the full potential of this transformative technology.

Keywords :

IOT, blockchain, cryptocurrency, smart contracts, consensus algorithms, internet of things.

1. Introduction

Blockchain technology is a revolutionary concept that has garnered significant attention across various domains. At its core, blockchain is a decentralized, distributed ledger technology that enables secure and transparent recording of transactions in a tamper-resistant and immutable manner [1]. It operates on a peer-to-peer network where each participant, or node, maintains a copy of the entire ledger, ensuring redundancy and resilience against single points of failure [2]. The cornerstone of blockchain's robustness lies in its cryptographic principles and consensus mechanisms, which facilitate trust and integrity among participants without the need for intermediaries. Transactions are grouped into blocks, cryptographically linked in a chain, and appended to the existing ledger through consensus algorithms such as Proof of Work (PoW) or Proof of Stake (PoS).

Blockchain's potential extends far beyond its original application in cryptocurrencies like Bitcoin [3]. It has sparked innovation in various sectors, including finance, supply chain management, healthcare, and governance. Smart contracts, programmable code executed automatically when predefined conditions are met, further enhance blockchain's versatility by enabling self-executing agreements without third-party intervention and unlock the full potential of blockchain technology as shown in Fig 1.

2. Blockchain Technology

Blockchains are composed of blocks as shown in Fig.2. Blockchain databases maintain records in blocks in a distributed, fault-tolerant and shared manner. Even though blockchain users have access to all blocks, they cannot be deleted or altered. Blocks make up blockchain databases. Several verified transactions are in each block and it contains its hash value from the previous block.

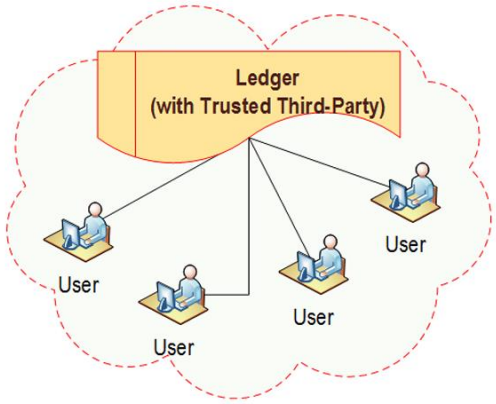

Fig 1. Traditional centralized ledger

A genesis block is the first block in a blockchain, and its hash value is entirely zero, since it has no parent block. Blockchains, as shown in Fig 3, are chronological sequences of blocks containing a list of all the transactions. Linked lists use the hash value of the previous block to reference each subsequent block, also known as parental blocks. The genesis block does not point to any other blocks in a Blockchain. There is a block header (metadata) and a block body (list of transactions). In addition to block version, parent block hash, Merkle tree root hash, timestamps, and nonce, the metadata includes. Nonce is an arbitrary number that is used to communicate cryptographically between users. Each participant digitally signs the block body and it contains data, records, or transactions [4].

Digital Signature - Private keys and public keys are owned by each user. Transactions are signed using the confidential private key. Transactions digitally signed are transmitted to every computer in the network. There are usually two phases to the digital signature process: the signing phase and the verification phase [4].

A user such as Alice wants to send a message to a user Bob. Once Alice's data is signed with her private key, she encrypts the result with her private key and sends it to Bob encrypted as well. Bob verifies Alice's public key in the verification phase. Then Bob could easily see if there had been any alterations made to the data. The elliptic curve digital signature algorithm (ECDSA), the most commonly used digital signature algorithm in blockchains, is used [5].

Block : There are two parts to a block: a header and a body. It contains the following information: Blockversion, Merkle Tree Root Hash - A hash value associated with all transactions in a block, Timestamp, nBits - maximum number of bits in a valid block hash, Nonce - four bytes starting at 0 and increasing with each calculation.

Parent Block Hash - A hash value of 256 bits that identifies the previous block.

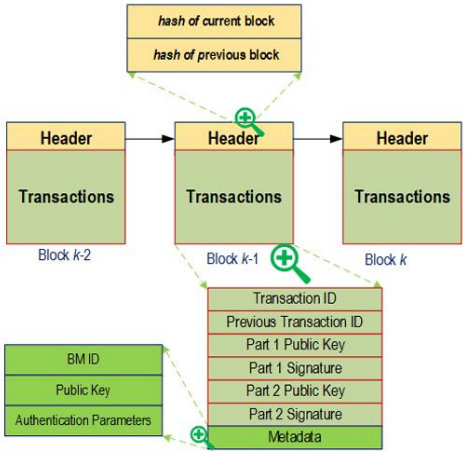

Fig.2. Blocks in Blockchain technology

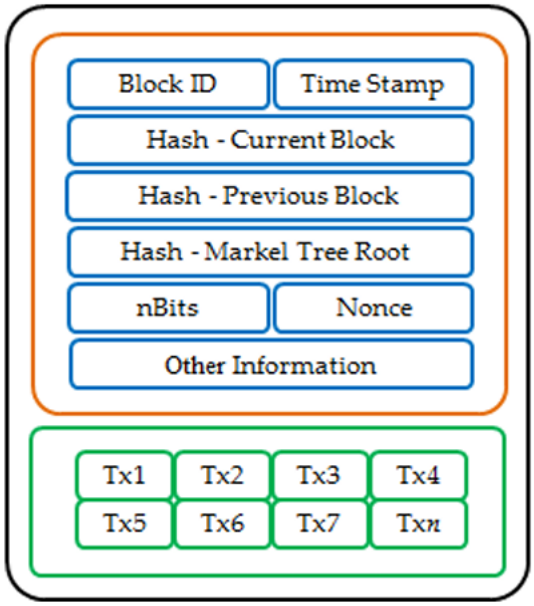

Fig.3. Block Structure

3. Types of Blockchain

Blockchain networks can be classified into four types: public blockchains, private blockchains, consortium blockchains, and hybrid blockchains.

3.1 Public Blockchain

In blockchain technology, public blockchains are the first type. Cryptocurrencies like Bitcoin emerged in this region, which contributed to the popularity of distributed ledger technology (DLT). By removing centralization's problems, including security and transparency, the entire process becomes more efficient. In DLT, information is distributed as a peer-to-peer network, not stored in any one place. A method

of ensuring data authenticity is required due to its decentralized nature. Essentially, it is a method of reaching consensus on the current state of the ledger by the participants in the blockchain. There are two common methods of reaching consensus: proof of work and proof of stake. A user can access both current and previous records and conduct mining activities, a complex computation used to verify and include transactions in the ledger.

3.2 Private Blockchain

Blockchain networks that operate in restrictive environments, such as closed networks or those controlled by a single company, are called private blockchains. Despite being peer-to-peer and decentralized, this type of blockchain network is much smaller than a public blockchain. In contrast to public blockchains, where anyone with computing power can participate, private blockchains operate on a network of people inside an organization. Blockchains with permission and enterprise blockchains are also known as permission blockchains.

3.3 Hybrid Blockchain

Many organizations want to take advantage of both public and private blockchain technology at once, so they'll use hybrid blockchain, which combines elements of both technologies. By setting up a private permission system alongside a public permission less system, an organization is able to control what data in the blockchain is publicly accessible, as well as who can access it. A hybrid blockchain does not typically publish transactions and records, but can be verified through smart contracts when needed. It is still possible to verify the confidentiality of the information inside the network. The hybrid blockchain may be owned by a private entity, but it is not able to alter transactions.

3.4 Consortium blockchain

Supply chain Consortia blockchains, also called federated blockchains, have the characteristics of hybrid blockchains in that they combine private and public features. A decentralized network, however, allows multiple members of the organization to collaborate. Consortium blockchains are essentially private blockchains that can only be accessed by a particular group, eliminating the risks associated with just one entity controlling the network on a private blockchain. A consortium blockchain has nodes that control the consensus procedures. Transactions are initiated, received, and validated by a validator node. Any node in the system can initiate or receive transactions.

4. Consensus Algorithms

As one of the desired blockchain features, anonymity also poses a problem when it comes to trust. How can it be 100% ensured that anonymous users are honest when they add transactions to a ledger? The answer is to validate every transaction to be legal (not malicious, double-spending, etc.) and then put the transactions into a block. The agreement of adding a block to the blockchain is through consensus algorithms. These consensus algorithms take advantage of the fact that the majority of users on a blockchain have a common interest in keeping the blockchain honest.

A consensus protocol is essentially a set of rules to be followed by every participant. As a distributed technology without a universal trust, blockchain needs a distributed consensus mechanism for all participants to agree on the blockchain's current state. The blockchain's consensus is based on scarcity that controlling more of a scarce resource gives more control over the blockchain's operation. A number of unique consensus mechanisms have been designed for blockchains.

Thus, six consensus algorithms are further described below.

1. **Proof of Work (PoW)**: Majority of cryptocurrencies currently in circulation use Proof of Work consensus. Solving the mathematical problem may difficult. The solution can easily be verified to be correct. The next block generation is selected using this consensus algorithm. PoW is the consensus algorithm used by Bitcoin [3]. The idea behind this algorithm is to find an easy solution to a complex mathematical problem. A lot of computational power is required for solving this puzzle, so the node that solves it first gets to mine the next block.
2. **Proof of Stake (PoS)** : PoS is the second most prominent consensus method and requires fewer computations for mining than PoW. PoS solves time and electricity consumption problems that PoW has because the electricity requirement is associated with miners finding a nonce and this process needs to take some time, the creator will receive the transaction fees associated with that block.
3. **Delegated Proof-of-Stake (DPoS) :** In DPoS, all token holders can vote for a number of delegates and can also delegate to other users with their voting power. The more tokens that the token holder has, the more voting power the token holder has. Then the delegates are responsible for validating transactions and blocks to secure the network. Unlike the most computing power in PoW or the most tokens in PoS, token holders in

DPoS are allowed to vote on who to mine new blocks and reward only the best miners.

4. **Proof of Elapsed Time (PoET)** : Intel Corporation developed PoET to enable a different way to determine a winner to mine a block. In PoET, each potential validation node requests a random waiting time which is generated on a trusted computing platform, e.g., Intel's SGX.
5. **Practical Byzantine Fault Tolerance (PBFT) :** Byzantine Fault Tolerance (BFT) is to solve a famous general problem that some generals are dishonest but needs to reach a correct consensus. PBFT is a consensus algorithm that optimizes BFT. In PBFT, as long as the malicious or hostile nodes are less than one third of all the nodes in the blockchain system, the blockchain system will come to agree on the blockchain's current state.
6. **Proof of Burn (PoB)** : PoB validators do not invest in expensive hardware equipment, but rather send tokens to an unrecoverable address and will not be able to retrieve them. Validators earn mining privileges on the system through committing coins to an unreachable address based on a random selection process.

5. Limitations and Benefits

5.1 Limitations of Blockchain

Developing decentralized applications with blockchain technology has enormous potential. In order for blockchain technology to be used in mainstream applications, there are certain barriers as shown in Fig. 4

- Lack of Awareness : Blockchain is currently being discussed a lot, but people do not know how to utilize it in various situations.
- Limited availability of technical talent : Developers today are available in many different fields, and can do many things. Compared to other technologies, however, blockchain technology has fewer developers who have specialized knowledge of the technology. Because of this, blockchain development has been hampered due to the scarcity of developers.
- Immutable: Immutable means that we can never modify the records in any way.
- Key Management : In addition to the public and private keys that blockchain has as its foundation, it is built on cryptography. Private keys present one more risk: someone may regain access to your key if you have lost it.
- Scalability : Every participating node in a blockchain, like bitcoin, verifies the transaction. Blockchain networks can only handle a limited number of transactions. The bitcoin network was not designed to handle the high volume of transactions conducted by many other institutions.
- Complexity : It is the complexity of the network that makes blockchain so attractive. Blockchain is more effective when there are many parties involved in a transaction.
- High Energy Consumption : Every node that is part of the blockchain network must have around 200 GB of storage space. Additionally, a daily upload of 5GB and a download of 500MB are required.

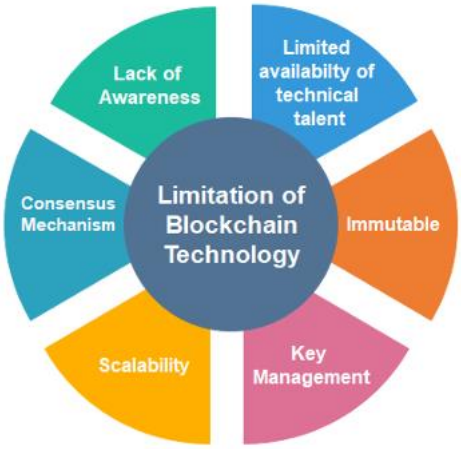

Fig.4: Limitations of Blockchain

5.2 Benefits of Blockchain

Trust in a network is one of the key issues that blockchain technology resolves. Organizations can focus on solving their problems by altering the key parameters, trust. Blockchain technology has also been embraced by governments and deemed important as shown in Fig. 5

1. Energy Sector Environmental Sustainability:

Blockchain helps to reduce the environmental impact of the energy sector. In addition to providing an efficient network for storing, producing, and distributing energy, it also deals with legacy efficiency problems in the energy sector.

- Reduced Costs: The energy sector suffers from a reduction of costs associated with infrastructure.
- Improved Transparency: Distributed ledger systems offer enhanced transparency.

2. Real Estate Tokenization:

The blockchain will enable tokenization of actions. A pre-defined code is used to rent out properties for a specified

period of time. In addition to adding any business logic, tokens can be used to secure transactions against fraud.

- Proper Tenant and Investor Identity: Creating digital identities that are easy to verify and use is beneficial to both investors and tenants. A proper identity management system will enable KYC/AML procedures to be streamlined. Additionally, sharing and accessing documentation will become easier.
- Property Sale: Smart contracts can automate the sale of property. By doing so, as long as a certain condition is met, legal agreements can be tracked and executed.
- Real-Time Accounting: The Blockchain enables real-time accounting.

3. Trade Finance Data Integrity:

In terms of data integrity, authenticity, and proper asset provenance, blockchain technology improves the trade finance industry.

- Streamlined Process: With blockchain-based smart contracts and blockchain-based dApps, automation has also become a norm. The process efficiency was improved, including the ability to perform real-time settlements. Since intermediaries were not involved, the process was also error-free.
- Programmable: A blockchain platform enables organizations to code multiple business aspects such as identity management, data privacy, and governance.
- Market Reactivity: A trade finance organization can also make changes as needed by using digital security. The ability to customize is a major benefit.

Fig. 5: Benefits of Blockchain Technology

- Cost Reduction: Automating your network means reducing operational, infrastructure, and transactional costs.

4. Government Proper Identity Management:

- Identity management is a tool that can be used by the government for every citizen. Thus, they are able to manage transactions, credentials, and data in a simplified way. Fair Elections: As well as conducting transparent elections with no chance of fraud, they can also use the blockchain. Finance Management: Engage in more effective financial management. Also, budgets can be allocated in a transparent, efficient, and effective manner.

5. Healthcare Patient Profile Privacy:

Unified patient profiles are created when decentralized ledgers are used. A secure ledger allows patients to store and share all their papers online without carrying them. As patients are in control of who can see or use their data, it will also increase their privacy.

- Drug Traceability: Blockchain will also enhance drug traceability. The fact that everything is tracked in real-time in a decentralized network virtually eliminates any chance of its being compromised.

- Better Clinical Trials: A decentralized network secures and stores patient data. By using public health data, researchers can do better clinical trials and research, which could help develop drugs to treat different diseases.
- Electronic Health Records (EHRs): Electronic records can be easily managed by health organizations using blockchain.

6. Logistics Better Freight Tracking:

There is no way for anyone to alter the data available on the network, since blockchain offers a proper authentication channel, which also includes verification. In this way, all deliveries can be tracked and managed in real time. Better Carrier Onboarding: Blockchain is equipped to handle the situation; onboarding new drivers takes only minutes.

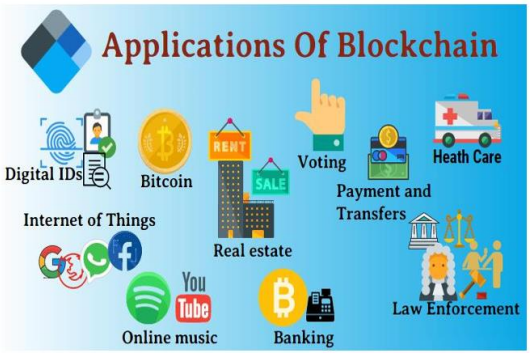

Fig.6: Applications of Blockchain

CONCLUSION

An overview of blockchain is presented in this paper. Blockchain technology has become increasingly popular around the world. Decentralized infrastructure and peer-to-peer nature make blockchain an excellent technology and highly valued and acclaimed. We investigate blockchain applications in various fields. Key characteristics and architecture are described. Discussed typical consensus algorithms of blockchain. More blockchain-based applications are emerging nowadays, so investigate blockchain-based applications extensively in the future.

REFERENCES

1. Karthik Kumar Vaigandla, Mounika Siluveru, Madhavi kesoju, Radha Krishna Karne, "Review on Blockchain Technology : Architecture, Characteristics, Benefits, Algorithms, Challenges and Applications", Journal of Intelligent Computing, pp 10-18, volume 3, 2023.
2. Mingyue Xie, Jun Liu, Shuyu "A survey on blockchain consensus mechanism: research overview, current advances and future directions", International Journal of Intelligent Computing and Cybernetics, pp. 24, volume 16, 2023.
3. Zhang Wenhua, Faizan Qamar, Taj-Aldeen Naser Abdali, Rosilah Hassan, "Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends", Journal of Electronics, pp. 54, volume 12, 2023.
4. Hamed Taherdoost, "Smart Contracts in Blockchain Technology: A Critical Review", International Journal of Science Applications, pp. 14, volume 117, 2023.
5. Kasula, Balaram Yadav, "The Role of Blockchain Technology in Securing Electronic Health Records", Journal of Transactions on Latest Trends in Artificial Intelligence, pp. 15, volume 4, 2023.