AAYUSHI INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (AIIRJ)
ISSN 2349-638x (Peer Review and Indexed Journal) IMPACT FACTOR 7.367
Devgiri Nagar, Ambejogai Road,Latur
Tq. Latur, Dist. Latur. Pincode 413512.
State Maharashtra, India.
Email ID's: editor@aiirjournal.com , aiirjpramod@gmail.com
Website: www.aiirjournal.com

Certificate of Publication

Awarded to

Siddika Nawab Patel

For Contributing Research Paper

" A Study on Blockchain Technology "

In the

AAYUSHI INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (AIIRJ)

Online Monthly Peer Review & Indexed Journal with ISSN 2349-638x (Impact factor 7.367)

for the month of **May 2023 with Special Issue No. : 126**

Pramod Prakashrao Tandale
(Chief Editor)

A Study on Blockchain Technology

Siddika Nawab Patel
DCC, Latur

Abstract

Blockchain technology is an advanced database mechanism that allows transparent information sharing within a business network. A blockchain database stores data in blocks that are linked together in a chain. The data is chronologically consistent because you cannot delete or modify the chain without consensus from the network. As a result, you can use blockchain technology to create an unalterable or immutable ledger for tracking orders, payments, accounts, and other transactions. The system has built-in mechanisms that prevent unauthorized transaction entries and create consistency in the shared view of these transactions.

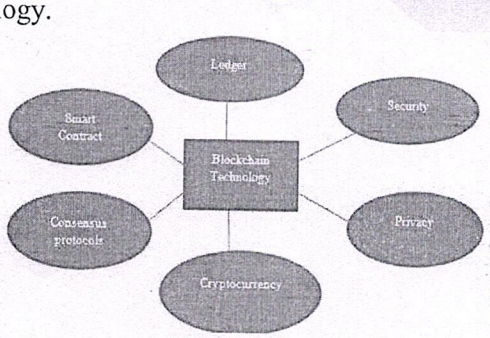
Blockchain is a one of emerging technology for decentralized and sharing of transactional data across a large peer to peer network, wherenon-trusting members can interact with each other without an intermediary, in a verifiable manner. In this paper, we review the basics ofBlockchain, its applications, types, and working of Blockchain. Behind this innovative technique, the security, privacy issues and Consensus mechanisms of this technology are also important and are a matter of concern. The problems associated with Blockchain technology are also discussed in this paper.

Introduction

All traditional transactions depend on the centralized trusted party,which gives many problems of transaction cost, efficiency, andsecurity. To solve these problems and to achieve secure, faster and transparent transactions we need to introduce the concept of Blockchain technology.

Blockchain technology, which was introduced by Satoshi Naka-moto. Bitcoin defines as one of the applications of BlockchainTechnology in the financial field. The blockchain is nothing but adistributed ledger technology. It will process the transactions be-tween the individuals and organizations without the need for thirdpartyinvolvement.

Fig.1: General Architecture of Blockchain Technology.



The above figure shows the Architecture of the Blockchain Technology.

Blockchain as a Service (BaaS) is a managed blockchain service that a third party provides inthe cloud. You can develop blockchain applications and digital services while the cloud providersupplies the infrastructure and blockchain building tools.

AWS Blockchain services provide purpose-built tools to support your requirement. You can usethem to build everything from a centralized ledger database that maintains an immutable recordof transactions to a multi-party, fully managed blockchain network that helps eliminateinter mediaries

EVALUATION OF blockchain TECHNOLOGY

Blockchain technology has its roots in the late 1970s when a computer scientist named RalphMerkle patented Hash trees or Merkle trees. The technology has continued to evolve over these three generations:

First generation – Bitcoin and other virtual currencies

In 2008, an anonymous individual or group of individuals known only by the name **SatoshiNakamoto** outlined blockchain technology in its modern form. Many of the features ofBitcoin blockchain systems remain central to blockchain technology even today.

Second generation – smart contracts

A few years after first-generation currencies emerged, developers began to consider blockchain applications beyond cryptocurrency. For instance, the inventors of Ethereum decided to use blockchain technology in asset transfer transactions. Their significant contribution was the smart contracts feature.

Third generation – the future

As companies discover and implement new applications, blockchain technology continues to evolve and grow.

THEELEMENTS of Blockchain TECHNOLOGYARE:

[1] **Ledger**: Blockchain is a distributed ledger technology, means the copy of the record is same who are participatingin the network. There is neither central authority nor a trusted third party In the Blockchain

[2] **Consensus Protocols**: Transaction should be verified by all parties in a network. Creating a block and adding to its ledger is also a decentralized process.

[3] **Security**: Blockchain uses the techniques of digital signatures and public key cryptography in order toverify theidentityofthetransactionsinthenetwork.

[4] **Cryptocurrency(orcryptocurrency)**:itisdesign edasadigitalasset works as an exchange of medium for providingsecuretrans-actions usingcryptography.

[5] **Privacy**: All types of data can be stored in the blockchain. The privacy rules are applicable if sensitive data is processing-e.g.healthdataor citizenservice

[6] **Smartcontract:**Thesecontractsareactsasagreem entswitha facility of self-execute and self-enforced. These contractstake the data from external source, so that data should nottamper with thatacryptographicproofmustbeattached.

USES of Blockchain:-

Blockchain is an emerging technology that is being adopted in innovative manner by various industries. We describe some use cases in different industries in the following subsections:

Energy

Energy companies use blockchain technology to create peer-to-peer energy trading platforms and streamline access to renewable energy

Finance

Traditional financial systems, like banks and stock exchanges, use blockchain services tomanage online payments, accounts, and market trading.

Media and entertainment

Companies in media and entertainment use blockchain systems to manage copyright data. Copyright verification is critical for the fair compensation of artists

Retail

Retail companies use blockchain to track the movement of goods between suppliers and buyers.

FEATURES of Blockchain TECHNOLOGY

Blockchain technology has the following main features:

Decentralization

Decentralization in blockchain refers to transferring control and decision making from a centralized entity (individual, organization, or group) to a distributed network.

Immutability

Immutability means something cannot be changed or altered. No participant can tamper with a transaction once someone has recorded it to the shared ledger.

Consensus

A blockchain system establishes rules about participant consent for recording transactions. You can record new transactions only when the majority of participants in the network give their consent.

COMPONENTS of Blockchain TECHNOLOGY

Blockchain architecture has the following main components:

A distributed ledger

A distributed ledger is the shared database in the block chain network that stores thetransactions, such as a shared file that everyone in the team can edit. In most shared texteditors, anyone with editing rights can delete the entire file. However, distributed ledgertechnologies have strict rules about who can edit and how to edit. You cannot delete entries oncethey have been recorded.

Smart contracts Companies use smart contracts to self-manage business contracts without the need for anassisting third party.

Public key cryptography

Public key cryptography is a security feature to uniquely identify participants in the blockchainnetwork. This mechanism generates two sets of keys for network members. One key is a publickey that is common to everyone in the network. The other is a private key that is unique to everymember. The private and public keys work together to unlock the data in the ledger.

WORKING of Blockchain

While underlying blockchain mechanisms are complex, we give a brief overview in the following steps. Blockchain software can automate most of these steps:

Step 1 – Record the transaction

A blockchain transaction shows the movement of physical or digital assets from one party to another in the blockchain network. It is recorded as a data block and can include details like these:

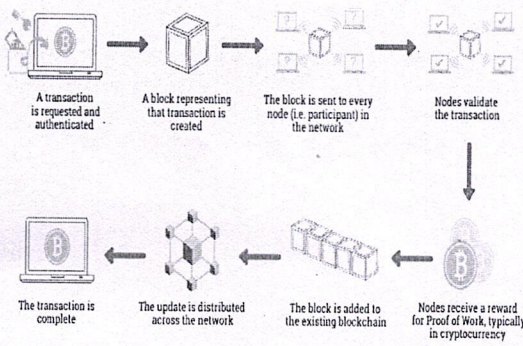
- Who was involved in the transaction?
- What happened during the transaction?
- When did the transaction occur?
- Where did the transaction occur?
- Why did the transaction occur?
- How much of the asset was exchanged?
- How many pre-conditions were met during the transaction?

Step 2 – Gain consensus

Most participants on the distributed blockchain network must agree that the recorded transaction is valid. Depending on the type of network, rules of agreement can vary but are typically established at the start of the network.

Step 3 – Link the blocks

Once the participants have reached a consensus, transactions on the blockchain are written into blocks equivalent to the pages of a ledger book. Along with the transactions, a cryptographic hash is also appended to the new block. The hash acts as a chain that links the blocks together. If the contents of the block are intentionally or unintentionally modified, the hash value changes, providing a way to detect data tampering. Thus, the blocks and chains link securely, and you cannot edit them. Each additional block strengthens the verification of the previous block and therefore the entire blockchain.



Working of Blockchain

Step 4 – Share the ledger

The system distributes the latest copy of the central ledger to all participants.

TYPES OF blockchainNETWORKS:

There are four main types of decentralized or distributed networks in the blockchain:

1. Public blockchain networks

Public blockchains are permissionless and allow everyone to join them. All members of the blockchain have equal rights to read, edit, and validate the blockchain. People primarily use public blockchains to exchange and mine cryptocurrencies like Bitcoin, Ethereum, and Litecoin.

2. Private blockchain networks

A single organization controls private blockchains, also called managed blockchains. The authority determines who can be a member and what rights they have in the network. Private blockchains are only partially decentralized because they have access restrictions.

3. Hybrid blockchain networks

Hybrid blockchains combine elements from both private and public networks. Companies can set up private, permission-based systems alongside a public system. In this way, they control access to specific data stored in the blockchain while keeping the rest of the data public. They use smart contracts to allow public members to check if private transactions have been completed.

4 Consortium blockchain networks

A group of organizations governs consortium blockchain networks. Preselected organizations share the responsibility of maintaining the blockchain and determining data access rights. Industries in which many organizations have common goals and benefit from shared responsibility often prefer consortium blockchain networks.

Blockchain PROTOCOLS

The term blockchain protocol refers to different types of blockchain platforms that are available for application development. Each blockchain protocol adapts the basic blockchain principles to suit specific industries or applications. Some examples of blockchain protocols are provided in the following subsections:

Hyperledger fabric

Hyperledger Fabric is an open-source project with a suite of tools and libraries. Enterprises can use it to build private blockchain applications quickly and effectively. It is a modular, general- purpose framework that offers unique identity management and access control features. These features make it suitable for various applications, such as track-and-trace of supply chains, trade finance, loyalty and rewards, and clearing settlement of financial assets.

Ethereum

Ethereum is a decentralized open-source blockchain platform that people can use to build public blockchain applications. Ethereum Enterprise is designed for business use cases.

Corda

Corda is an open-source blockchain project designed for business. With Corda, you can build interoperable blockchain networks that transact in strict privacy..

Quorum

Quorum is an open-source blockchain protocol that is derived from Ethereum. It is specially designed for use in a private blockchain network, where only a single member owns all the nodes, or in a consortium blockchain network.

BENEFITS OF BlockchainTECHNOLOGY

Blockchain technology brings many benefits to asset transaction management. We list a few of them in the following subsections:

Advanced security

Blockchain systems provide the high level of security and trust that modern digital transactions require. There is always a fear that someone will manipulate underlying software to generate fake money for themselves. But blockchain uses the three principles of cryptography, decentralization, and consensus to create a highly secure underlying software system that is nearly impossible to tamper with. There is no single point of failure, and a single user cannot change the transaction records.

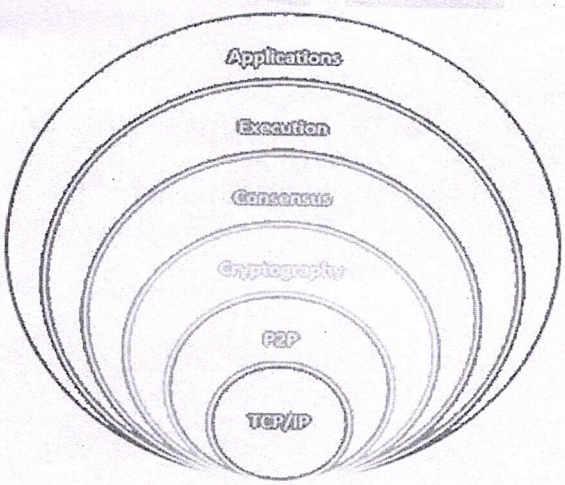
Improved efficiency

Business-to-business transactions can take a lot of time and create operational bottlenecks, especially when compliance and third-party regulatory bodies are involved. Transparency and smart contracts in blockchain make such business transactions faster and more efficient.

Faster auditing

Enterprises must be able to securely generate, exchange, archive, and reconstruct e-transactions in an auditable manner. Blockchain records are chronologically immutable, which means that all records are always ordered by time. This data transparency makes audit processing much faster.

Six Layers of Blockchain Technology



The Blockchain technology is built upon 6 main layers that are:

1. **The TCP/IP network**
2. **Peer-to-Peer protocols**
3. **Consensus algorithms**
4. **Cryptography algorithms**
5. **Execution (Data blocs, Transactions, …)**
6. **Applications (Dapps, smart contracts …)**

The actual TCP/IP network

The first layer in the Blockchain is the TCP/IP protocol in simple words, the internet we all know, and the way it simply works with all its protocols. Without the internet, the concept of distributed apps or even the Blockchain will never exist.

Peer-to-Peer protocols

On top of the internet layer, we the Peer-to-peer protocols also known as P2P. The P2P protocol was developed to give end-users the ability to communicate with each other without the need for a central server.

The P2P protocols can be divided into two main types:

Structured P2P

In structured peer-to-peer systems, network connections are fixed, and peers keep track of the resources (e.g., shared material) that their neighbor peers have.

Unstructured P2P

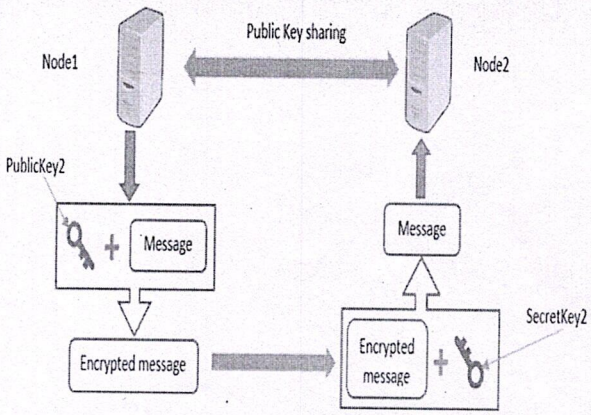
The unstructured P2P is the type used in Blockchain technology as the links are randomly established and all the data is stored in each node contrarily to the

Cryptography algorithms

I think what made all this concept available is the advancement in cryptography algorithms. The Blockchain technology was built on multiple cryptography algorithms and the most popular ones are:

Public/Private key encryption

When this field has started to first show up in the community of mathematicians, the only type of encryption that was known, was the symmetric encryption. This concept is based on having one shared key between two people to encrypt and decrypt the sent message.



Hash function

Hash functions are another essential cryptography concept in the Bitcoin processes. Hash functions are algorithms that can transform a large data into a small unique portion with a specific number of bytes. Those functions are used precisely in checking the integrity of the sent information. Moreover, the hashing algorithms represent the key concept in the PoW mechanism used by Bitcoin.

Here is a list of the most popular hash functions:

- MD5
- SHA256
- SHA-512

Digital signature

The digital signature concept is also a key element in Bitcoin technology and it is used in signing transactions sent by users.

Consensus algorithms

Consensus algorithms are the result of a famous problem discussed and researched for a long time ago called the Byzantine generals problem. This problem was first introduced by M. Pease, R. Shostak, and L. Lamport.

The Byzantine general's problem is defined as multiple generals trying to attack a city at the same moment to win the war. The problem is that they need to agree on the timing even if one of them is not loyal.

Consensus algorithms can be divided into two main categories:

Proof-based consensus mechanisms

This setup necessitates nodes competing in a leader-election lottery, with the winner proposing the ultimate value. To earn the privilege to propose the next block, the method requires proof of some effort as well as the ownership of some authority or tokens.

Traditional fault tolerance-based

This form of consensus method is based on a basic strategy of nodes publishing and verifying signed messages in stages. After a given number of messages have been received across a particular number of rounds (phases), an agreement is established.

Here is a list of some of the most popular consensus algorithms:

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Proof of Deposit (PoD)
- Proof of Importance (PoI)

Future Scope of Blockchain Technology

The paradigm move to cryptocurrency has swept the world of finance and changed the way the world looks at money. With the onset of Bitcoin, blockchain technology has risen to new popularity and significance. Blockchain is an irreversible, impenetrable digital database that permanently and verifiably records transactions.

Understanding Blockchain:

Before we delve into the **scope of blockchain technology**, let us have a broad overview of **blockchain and its characteristics**. Blockchain, which is a digital ledger, allows for duplication and sharing over the entire network of connected computer systems. Every member of the Blockchain has access to the history of every transaction or modification made there.

Dissecting the Scope of Blockchain and Its Application in Various Industries:

The future of blockchain technology and its applications have enticed numerous organizations cutting across varied domains and fields. With the prospect of being accepted globally owing to its disruptive characteristics, blockchain technology has been included in numerous studies.

Finance Industry and the Future of Blockchain Technology

Blockchain technology has been successful in delivering its promise and demonstrated consistency regarding its objective of tracking financial assets. After seeing the potential and positive effects of this technology, several financial institutions made investments in it. Blockchain is able to address the flow and **deals of black money flow** because of its transparent ledger architecture.

Cybersecurity and the Future of Blockchain Technology

For apparent reasons, **the future of blockchain technology** is mostly in the area of cybersecurity. The data remains secure and verifiable despite the open and distributed nature of the Blockchain ledger.

Cloud Storage and the Future of Blockchain Technology

Data loss, hacking, and human mistake are all serious risks associated with centralized systems. **Blockchain technology** can be used to improve cloud storage security and hacker resistance.

Networking, IoT, and the Future of Blockchain Technology

Blockchain technology is being adopted by businesses like IBM and Samsung to create a distributed network of IoT devices. The ADEPT concept attempts to eliminate the central site for the control of communication between devices for tasks like software updates, error handling, keeping track of energy usage, etc.

Digital Advertising and the Future of Blockchain Technology

Business entrepreneurs are often plagued by the complexities of stiff competition. Owing to bad players publishers and promoters struggle with digital marketing, ineffective payment structures, domain fraud, etc..

Supply Chain Administration and the Future of Blockchain Technology

At each stage of the supply chain, the **usage of blockchain technology** can monitor employment, expenses, and releases while minimizing time delays and human errors. Blockchain can also guarantee the legality of products and the fair trade status of those products through traceability. Blockchain has the potential to stop revenue losses from illegal or grey market goods as well as reputational harm.

Governments' Use of National Digital Currencies

The year 2017 witnessed a massive increase in the value of Bitcoin which is relatively higher in comparison to other services and forms of money. Cryptocurrency has come to attain a significant position in the market as among the most valuable assets. Even with the fixed cap of 21 million units, the demand for Bitcoin will once again increase. Governments across the globe are likely to develop their own digital currencies and take part in an open market as a result. .

Government Organizations and the Future of Blockchain Technology

The idea of blockchain can also aid in the management of enormous amounts of data, which can be highly beneficial for government organizations. The adoption of Blockchain will result in an efficient data management system with the potential to enhance how these entities operate.

Future Blockchain Experts will be in High Demand

Blockchain engineers and specialists are in short supply on the job market, despite the technology being at the height of its popularity. Investing in Blockchain technology now will benefit you in the long run.

Conclusions

Blockchains gives robust, distributed peer to peer systems andability to interact with peers in a trustless and auditable manner.The government should provide consistent laws for this technolo-gy, and enterprise gets ready to hold blockchain technologies.Consensus mechanism is the core technology of Blockchain. In Future work, concentrate on algorithms based on consensus mech-anisms of Blockchain technology for differentscenarios. .

References

1. Electronic Cash System.https://bitcoin.org/bitcoin.pdf
2. Future Scope of Blockchain Technology www.careera.com
3. Blockchain feature ant types Data-flair.training.blogs
4. Components of Blockchain www.shiksha.com
5. www.getsecuredworld.com
6. www.techtarget.com
7. What is blockchain Technology. Aws.amazon.com
8. blockchain Technology www.euromoney.com
9. blockchain Technology www.ibm.com
10. Benefits of blockchain www.reseachgate.net
11. blockchain Technology www.hidawi.com
12. Blog.goodaudience.com
13. White paper on Applications of Blockchain technology to Bankingand Financial sector in India(2017)-IDRBT.
14. Blockchain in Banking: A Measured Approach (2016) Cognizant Reports.
15. Konstantinos Christidis and Michael Devetsikiotis (2016). Block-chains and Smart Contracts for the Internet of Things [Online].Available: ieeex-plore.ieee.org/iel7/6287639/6514899/07467408.pdf