IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.67

Volume 5, Issue 8, March 2025

Blockchain Unlocked : A Complete Learning Guide

Sagar Laxman Bhor, Omkar Sampat Naykodi, Dipak Vilas Shelkande
Shubham Rohidas Mindhe, Jay Santosh Maskare, Siddhi Ashok Kokane
Shankarrao Butte Patil B.Sc. IT College, Junnar, Maharashtra, India

Abstract*: Blockchain technology has revolutionized digital transactions, data security, and decentralized applications. This review explores the fundamental aspects of blockchain, including its structure, consensus mechanisms, and real-world applications. Blockchain's decentralized and tamper-proof nature has made it a key technology in finance, healthcare, supply chain, and other industries. This paper provides insights into the benefits, challenges, and latest trends in blockchain adoption, making it a valuable resource for understanding its impact and future potential.*

Keywords: Blockchain, Decentralization, Distributed Ledger, Cryptocurrency, Smart Contracts, Consensus Mechanism, Security, Transparency, Peer-to-Peer Network, Immutability

I. INTRODUCTION

Blockchain technology is a revolutionary system that has transformed digital transactions, data security, and decentralized applications. Understanding its core principles is essential for anyone looking to explore its vast potential. For this research, the team focused on blockchain's fundamental aspects, including its structure, working mechanism, and real-world applications. Blockchain has gained immense popularity due to its transparency, security, and decentralized nature. Traditional systems rely on central authorities, whereas blockchain operates through a distributed ledger, making it tamper-resistant andtrustless.

For beginners, key aspects of blockchain technology include ease of understanding, security features, and practical use cases. The team gathered insights from various sources, including research papers, technical blogs, books, and industry reports. Below is an overview of blockchain technology, its types, and its significance in different fields.

Basics of Blockchain

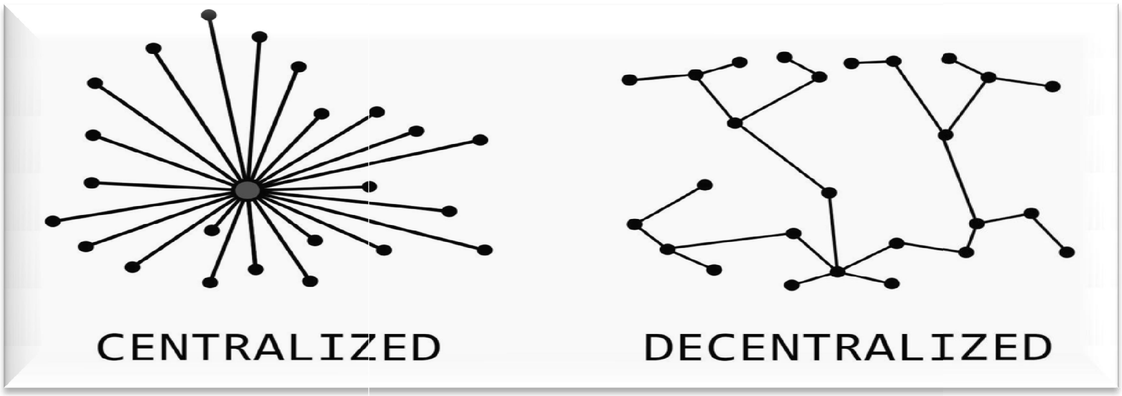
What is a Blockchain?

A blockchain is a distributed database or ledger shared across a computer network's nodes,also it is a Decentralized system .They are best known for their crucial role in cryptocurrency systems, maintaining a secure and decentralized record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry immutable—meaning it cannot be altered.

A Blockchain is defined as a series of blocks in which each block contains transaction information. a blockchain has as many blocks as transactions, and each block refers to the previous block; these are called blockchains. For example, normally in an office all the computers are connected to one common server. However, with blockchain technology the computers are linked to many different devices and processors. Within this database there is an ever-growing list of blocks. Upon entry, each block is time-stamped and 'attached' to the previous block to create a 'record'

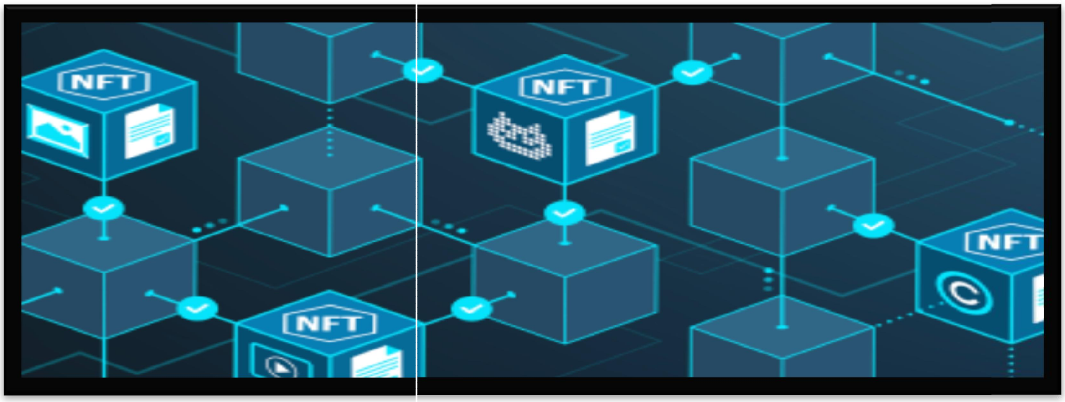
ISSN 2581-9429 IJARSCT

DOI: 10.48175/568



What are the blocks ?

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain.This iterative process confirms the integrity of the previous block, all the way back to the initial block, which is known as the genesis block (Block 0).To assure the integrity of a block and the data contained in it, the block is usually digitally signed.



History of Blockchain

Cryptographer David Chaum first proposed a blockchain-like protocol in his 1982 dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups". Further work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. They wanted to implement a system wherein document timestamps could not be tampered with. In 1992, Haber, Stornetta, and Dave Bayer incorporated Merkle trees into the design, which improved its efficiency by allowing several document certificates to be collected into one block. Under their company Surety, their document certificate hashes have been published in The New York Times every week since 1995.

The first decentralized blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008. Nakamoto improved the design in an important way using a Hashcashlike method to timestamp blocks without requiring them to be signed by a trusted party and introducing a difficulty parameter to stabilize the rate at which blocks are added to the chain.The design was implemented the following year by Nakamoto as a core component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network. In August 2014, the bitcoin blockchain file size, containing records of all transactions that have occurred on the

ISSN 2581-9429 IJARSCT
DOI: 10.48175/568

network, reached 20 GB (gigabytes). In January 2015, the size had grown to almost 30 GB, and from January 2016 to January 2017, the bitcoin blockchain grew from 50 GB to 100 GB in size. The ledger size had exceeded 200 GB by early 2020.

The words block and chain were used separately in Satoshi Nakamoto's original paper, but were eventually popularized as a single word, blockchain, by 2016.

According to Accenture, an application of the diffusion of innovations theory suggests that blockchains attained a 13.5% adoption rate within financial services in 2016, therefore reaching the early adopters' phase. Industry trade groups joined to create the Global Blockchain Forum in 2016, an initiative of the Chamber of Digital Commerce. In May 2018, Gartner found that only 1% of CIOs indicated any kind of blockchain adoption within their organisations, and only 8% of CIOs were in the short-term "planning or [looking at] active experimentation with blockchain". For the year 2019 Gartner reported 5% of CIOs believed blockchain technology was a 'game-changer' for their business.

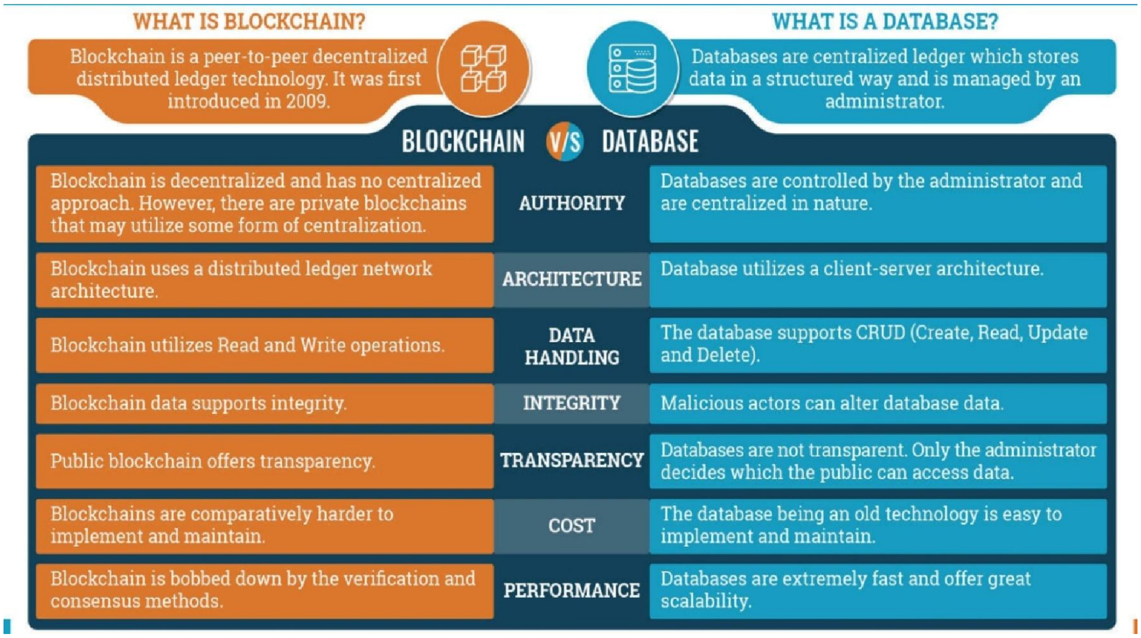
What are the benefits of blockchain?

The benefits of blockchain are increasing trust, security and transparency among member organizations by improving the traceability of data shared across a business network, plus delivering cost savings through new efficiencies.

Centralized Blockchain

Although most of blockchain implementation are decentralized and distributed, Oracle launched a centralized blockchain table feature in Oracle 21c database. The Blockchain Table in Oracle 21c database is a centralized blockchain which provide immutable feature. Compared to decentralized blockchains, centralized blockchains normally can provide a higher throughput and lower latency of transactions than consensus-based distributed blockchains.

Blockchain vs Database



WHAT IS BLOCKCHAIN?

Blockchain is a peer-to-peer decentralized distributed ledger technology. It was first introduced in 2009.

WHAT IS A DATABASE?

Databases are centralized ledger which stores data in a structured way and is managed by an administrator.

BLOCKCHAIN V/S DATABASE

BLOCKCHAIN		DATABASE
Blockchain is decentralized and has no centralized approach. However, there are private blockchains that may utilize some form of centralization.	AUTHORITY	Databases are controlled by the administrator and are centralized in nature.
Blockchain uses a distributed ledger network architecture.	ARCHITECTURE	Database utilizes a client-server architecture.
Blockchain utilizes Read and Write operations.	DATA HANDLING	The database supports CRUD (Create, Read, Update and Delete).
Blockchain data supports integrity.	INTEGRITY	Malicious actors can alter database data.
Public blockchain offers transparency.	TRANSPARENCY	Databases are not transparent. Only the administrator decides which the public can access data.
Blockchains are comparatively harder to implement and maintain.	COST	The database being an old technology is easy to implement and maintain.
Blockchain is bobbed down by the verification and consensus methods.	PERFORMANCE	Databases are extremely fast and offer great scalability.

II. TYPES OF BLOCKCHAIN

1. Public Blockchain

These blockchains are completely open to following the idea of decentralization. They don't have any restrictions, anyone having a computer and internet can participate in the network.

As the name is public this blockchain is open to the public, which means it is not owned by anyone.

Anyone having internet and a computer with good hardware can participate in this public blockchain.

All the computers in the network hold the copy of other nodes or blocks present in the network

In this public blockchain, we can also perform verification of transactions or records

Advantages:

- **Trustable:** There are algorithms to detect fraud. Participants need not worry about the other nodes in the network.
- **Secure:** This blockchain is large as it is open to the public. In a large size, there is a greater distribution of records.
- **Anonymous Nature:** It is a secure platform to make your transaction properly at the same time, you are not required to reveal your name and identity to participate.
- **Decentralized:** There is no single platform that maintains the network, instead every user has a copy of the ledger.

Disadvantages:

- **Processing:** The rate of the transaction process is very slow, due to its large size. Verification of each node is a very time-consuming process.
- **Energy Consumption:** Proof of work is highly energy-consuming. It requires good computer hardware to participate in the network.
- **Acceptance:** No central authority is there so governments are facing the issue of implementing the technology faster.

Use Cases:

Public Blockchain is secured with proof of work or proof of stake they can be used to displace traditional financial systems. The more advanced side of this blockchain is the smart contract that enabled this blockchain to support decentralization. Examples of public blockchains are Bitcoin and Ethereum.

2. Private Blockchain

These blockchains are not as decentralized as the public blockchain only selected nodes can participate in the process, making it more secure than the others.

These are not as open as a public blockchain.

They are open to some authorized users only.

These blockchains are operated in a closed network.

In this few people are allowed to participate in a network within a company/organization.

Advantages:

- **Speed:** The rate of the transaction is high, due to its small size. Verification of each node is less time-consuming.
- **Scalability:** We can modify the scalability. The size of the network can be decided manually.
- **Privacy:** It has increased the level of privacy for confidentiality reasons as the businesses required.

ISSN 2581-9429 IJARSCT
DOI: 10.48175/568

- **Balanced:** It is more balanced as only some users have access to the transaction which improves the performance of the network.

Disadvantages:

- **Security:** The number of nodes in this type is limited so chances of manipulation are there. These blockchains are more vulnerable.
- **Centralized:** Trust building is one of the main disadvantages due to its central nature. Organizations can use this for malpractices.
- **Count:** Since there are few nodes if nodes go offline the entire system of blockchain can be endangered.

Use Cases:

With proper security and maintenance, this blockchain is a great asset to secure information without exposing it to the public eye. Therefore companies use them for internal auditing, voting, and asset management. An example of private blockchains is Hyperledger, Corda.

III. HYBRID BLOCKCHAIN

It is the mixed content of the private and public blockchain, where some part is controlled by some organization and other makes are made visible as a public blockchain.
It is a combination of both public and private blockchain.
Permission-based and permissionless systems are used.
User access information via smart contracts
Even if a primary entity owns a hybrid blockchain it cannot alter the transaction

Advantages:

- **Ecosystem:** The most advantageous thing about this blockchain is its hybrid nature. It cannot be hacked as 51% of users don't have access to the network.
- **Cost:** Transactions are cheap as only a few nodes verify the transaction. All the nodes don't carry the verification hence less computational cost.
- **Architecture:** It is highly customizable and still maintains integrity, security, and transparency.
- **Operations:** It can choose the participants in the blockchain and decide which transaction can be made public.

Disadvantages:

- **Efficiency:** Not everyone is in a position to implement a hybrid Blockchain. The organization also faces some difficulty in terms of efficiency in maintenance.
- **Transparency:** There is a possibility that someone can hide information from the user. If someone wants to get access through a hybrid blockchain it depends on the organization whether they will give or not.
- **Ecosystem:** Due to its closed ecosystem this blockchain lacks the incentives for network participation.

Use Case:

It provides a greater solution to the healthcare industry, government, real estate, and financial companies. It provides a remedy where data is to be accessed publicly but needs to be shielded privately. Examples of Hybrid Blockchain are the Ripple network and XRP token.

IV. CONSORTIUM BLOCKCHAIN

It is a creative approach that solves the needs of the organization. This blockchain validates the transaction and also initiates or receives transactions.
Also known as Federated Blockchain.
This is an innovative method to solve the organization's needs.
Some part is public and some part is private.
In this type, more than one organization manages the blockchain.

Advantages:

- **Speed:** A limited number of users make verification fast. The high speed makes this more usable for organizations.
- **Authority:** Multiple organizations can take part and make it decentralized at every level. Decentralized authority, makes it more secure.
- **Privacy:** The information of the checked blocks is unknown to the public view. But any member belonging to the blockchain can access it.
- **Flexible:** There is much divergence in the flexibility of the blockchain. Since it is not a very large decision can be taken faster.

Disadvantages:

- **Approval:** All the members approve the protocol making it less flexible. Since one or more organizations are involved there can be differences in the vision of interest.
- **Transparency:** It can be hacked if the organization becomes corrupt. Organizations may hide information from the users.
- **Vulnerability:** If a few nodes are getting compromised there is a greater chance of vulnerability in this blockchain

Use Cases:

It has high potential in businesses, banks, and other payment processors. Food tracking of the organizations frequently collaborates with their sectors making it a federated solution ideal for their use. Examples of consortium Blockchain are Tendermint and Multichain.

Comparative Analysis of Blockchain Types

Feature	Public Blockchain	Private Blockchain	Hybrid Blockchain	Consortium Blockchain
Access Control	Open to everyone	Restricted to specific participants	Limited to a group of organizations	Combination of public and private
Governance	Decentralized	Centralized	Semi-decentralized	Mixed governance structure
Transparency	High transparency	Low transparency	Moderate transparency	Variable transparency

ISSN 2581-9429 IJARSCT
DOI: 10.48175/568

Feature	Public Blockchain	Private Blockchain	Hybrid Blockchain	Consortium Blockchain
Scalability	Limited scalability	High scalability	Moderate scalability	High scalability potential
Security	High due to decentralization	Lower due to centralization	Moderate security	Variable security
Transaction Speed	Slower due to consensus mechanisms	Faster transactions	Faster than public, slower than private	Variable speed
Use Cases	Cryptocurrencies, decentralized apps	Enterprise solutions, data privacy	Supply chain, banking, collaborations	Various applications need flexibility

Top Blockchain Applications

- Money transfer
- Smart contracts
- Internet of Things (IoT)
- Personal identity security
- Healthcare
- Logistics
- Non-fungible tokens (NFTs)
- Government
- Media

Features of Blockchain

There are many features of Blockchain. Following are the main features

- **Decentralized :** The network is decentralized meaning a group of nodes maintains the network making it decentralized. This is one of the key features of blockchain technology. Blockchain puts us users in a straightforward position. As the system doesn't require any governing authority, we can directly access it from the web and store our assets there.
- **Immutability :** Immutability is something that can't be changed or altered. This one is the top Blockchain features that ensures that the technology will remain as it is a permanent, unalterable network. As it is distributed system, every node on the system has a copy of the digital ledger. When a transaction is added every node needs to check its validity. If the majority thinks it's valid, then it's added to the ledger. This promotes transparency and makes it corruption-proof. Without the majority consent from the nodes, no one can add any transaction blocks to the ledger.Once the transaction blocks added to the ledger, no one can change it. Thus, any user on the network won't be able to edit, delete or update it.
- **Enhanced Security :** As it gets rid of the need for a central authority, no one can just simply change any characteristics of the network for their benefit. Using encryption ensures another layer of security for the system. Every information on the Blockchain is hashed cryptographically. So, changing or trying to tamper

ISSN 2581-9429 IJARSCT
DOI: 10.48175/568

with the data means changing all the hash IDs. If someone wants to corrupt the network, he/she would have to alter every data stored on every node in the network. There could be millions and millions of people, where everyone has the same copy of the ledger.

- **Distributed Ledgers :** A public ledger will provide every information about a transaction and the participant nodes. Many people can see what really goes on in the ledger. The ledger on the network is maintained by all other users on the system. Distributed ledger responds really well to any suspicious activity or tamper. Nodes act as verifiers of the ledger. If a user wants to add a new block others would have to verify the transaction and then give the green signal.To make the blockchain features work, every active node has to maintain the ledger and participate for validation.

Benefits

1. Transparency and Security: The decentralized architecture of blockchain mitigates the vulnerability of centralized data storage, reducing the likelihood of data manipulation and hacking. By distributing information across a network of nodes, no single point of failure exists, enhancing data security. This decentralized nature fosters a transparent and tamper-resistant environment, instilling trust among participants. Industries with a critical emphasis on data integrity, such as finance and healthcare, find reassurance in blockchain's ability to provide an immutable and trustworthy ledger, ultimately bolstering confidence in the reliability of shared information.

2. Efficiency and Reduced Costs: Smart contracts, a cornerstone of blockchain technology revolutionize operations by automating processes. They eliminate the need for intermediaries, ensuring direct and secure execution of predefined contractual terms. This automation significantly accelerates transaction times, fostering swift and seamless interactions. Moreover, the efficiency gains extend beyond speed, encompassing cost reduction as manual processing requirements diminish. By cutting out intermediaries and automating workflows, smart contracts optimize resource utilization, enhance reliability, and ultimately contribute to a more cost-effective and streamlined operational environment.

Challenges:

1. Energy Consumption: Another challenge associated with blockchain implementation, particularly in the case of proof-of-work consensus mechanisms (commonly used in cryptocurrencies like Bitcoin and Ethereum), is the significant energy consumption. The process of validating transactions, known as mining, requires substantial computing power, leading to environmental concerns. As sustainability becomes a growing priority for businesses, addressing the energy consumption of blockchain networks is essential.

2. Interoperability: Blockchain technology exists in various forms, each with its unique features and protocols. Achieving interoperability — ensuring seamless communication and interaction between different blockchain networks or between blockchain and traditional systems — poses a challenge. The lack of standardized protocols can hinder the widespread adoption of blockchain, as interoperability is crucial for creating a unified and connected ecosystem.

3. Data Privacy and Security Concerns: Whileblockchainis lauded for its security features, concerns about data privacy persist. The transparent nature of the technology means that once information is recorded on the blockchain, it is immutable. Striking a balance between transparency and protecting sensitive data is a challenge, especially in industries with stringent data protection regulations.

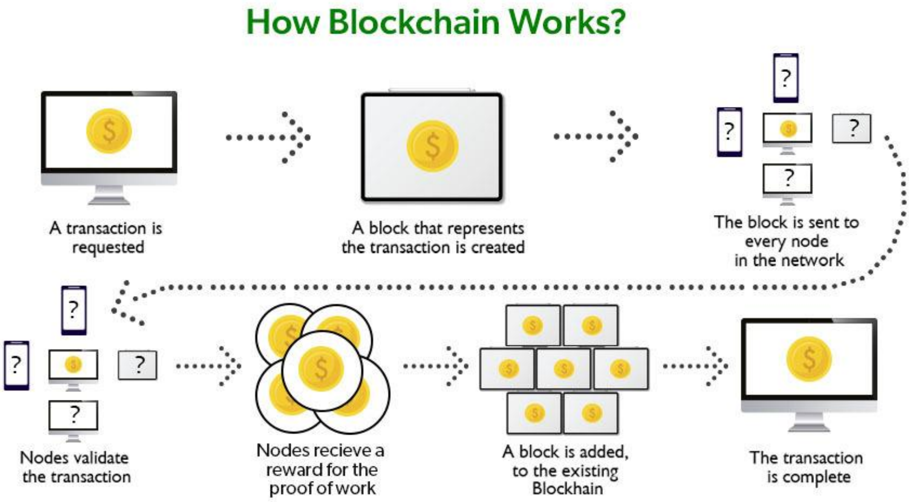
4. User Education and Adoption: Blockchain is a relatively nascent technology, and many potential users may not fully understand its intricacies. Implementing blockchain requires not only technical expertise but also a concerted effort to educate stakeholders about its benefits and functionalities. Overcoming resistance to change and fostering widespread adoption is a crucial aspect of successful blockchain implementation.

5. Cost of Implementation and Maintenance: While blockchain can lead to long-term cost savings through increased efficiency, the initial costs of implementing and maintaining a blockchain system can be substantial. Organizations need to allocate resources for technology upgrades, staff training, and ongoing maintenance to ensure the continued effectiveness of their blockchain solution.

While the benefits of blockchain technology are promising, organizations must navigate several challenges to successfully implement and integrate it into their operations. Scalability, regulatory uncertainty, integration complexities, energy consumption, interoperability, data privacy, user education, and implementation costs are all factors that require careful consideration and strategic planning. Addressing these challenges will be instrumental in unlocking the full potential of blockchain and ushering in a new era of transparency, security, and efficiency across industries.

How does the Blockchain Work?

A blockchain is a distributed database that stores information electronically in a digital format and is shared among the nodes of a computer network. A typical difference between a blockchain and a database is how data is structured. A blockchain is a shared, immutable ledger as the name suggests structures data into chunks or blocks, and a database structures data into tables. A blockchain is a chain of blocks. Once a block is filled with data it is chained to the previous blocks. Different types of information can be stored on the blockchain network but the most important is transactions.


How Blockchain Works?
A transaction is requested
A block that represents the transaction is created
The block is sent to every node in the network
Nodes validate the transaction
Nodes recieve a reward for the proof of work
A block is added, to the existing Blockhain
The transaction is complete

What Is a Peer-to-Peer (P2P) Service?

A peer-to-peer network is a simple network of computers. It first came into existence in the late 1970s. Here each computer acts as a node for file sharing within the formed network. Here each node acts as a server and thus there is no central server in the network. This allows the sharing of a huge amount of data. The tasks are equally divided amongst the nodes. Each node connected in the network shares an equal workload. For the network to stop working, all the nodes need to individually stop working. This is because each node works independently.

History of P2P Networks

Before the development of P2P, USENET came into existence in 1979. The network enabled the users to read and post messages. Unlike the forums we use today, it did not have a central server. It is used to copy the new messages to all the servers of the node.

1.In the 1980s the first use of P2P networks occurred after personal computers were introduced.

2.In August 1988, the internet relay chat was the first P2P network built to share text and chat.

3.In June 1999, Napster was developed which was a file-sharing P2P software. It could be used to share audio files as

DOI: 10.48175/568

well. This software was shut down due to the illegal sharing of files. But the concept of network sharing i.e P2P became popular.

4.In June 2000, Gnutella was the first decentralized P2P file sharing network. This allowed users to access files on other users' computers via a designated folder.

Types of P2P Networks

- **Unstructured P2P Networks:** In this type of P2P network, each device is able to make an equal contribution. This network is easy to build as devices can be connected randomly in the network. But being unstructured, it becomes difficult to find content. For example, Napster, Gnutella, etc.
- **Structured P2P Networks:** It is designed using software that creates a virtual layer in order to put the nodes in a specific structure. These are not easy to set up but can give easy access to users to the content. For example, P-Grid, Kademlia, etc.
- **Hybrid P2P Networks:** It combines the features of both P2P networks and client-server system An example of such a network is to find a node using the central server.

Features of P2P Network

These networks do not involve a large number of nodes, usually less than 12. All the computers in the network store their own data but this data is accessible by the group.

Unlike client-server networks, P2P uses resources and also provides them. This results in additional resources if the number of nodes increases. It requires specialized software. It allows resource sharing among the network.

Since the nodes act as clients and servers, there is a constant threat of attack.

Almost all OS today support P2P networks.

P2P Network Architecture

In the P2P network architecture, the computers connect with each other in a workgroup to share files, and access to internet and printer

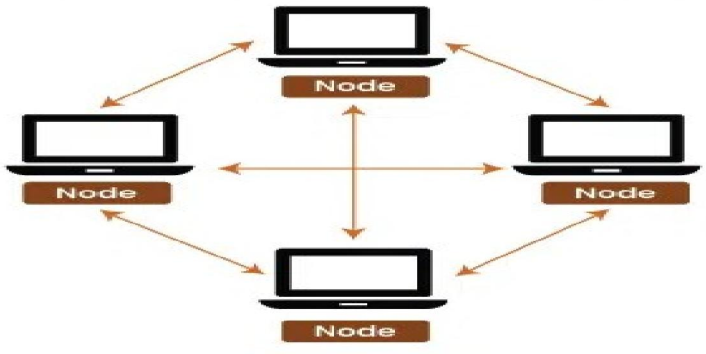
Each computer in the network has the same set of responsibilities and capabilities.

Each device in the network serves as both a client and server.

The architecture is useful in residential areas, small offices, or small companies where each computer act as an independent workstation and stores the data on its hard drive.

Each computer in the network has the ability to share data with other computers in the network.

The architecture is usually composed of workgroups of 12 or more computers.



DOI: 10.48175/568

How Does The Consensus Mechanism Work?

It achieves the agreement of most users on a single network. The consensus mechanism maintains the security of the blockchain by keeping a record of all legitimate transactions. Since crypto trading is a decentralised process, this becomes important to stop sellers from deliberately cheating a buyer.

To build trust for a blockchain, the consensus mechanism ensures that a transaction is reflected in the blockchain as soon as it gets validated. There are a variety of methodologies that are essential to ensure security and trust and achieve agreement across a blockchain network. Consensus mechanisms also ensure that all the transactions for a coin are rightly listed in the blockchain.

What Are The Types Of Consensus Mechanisms?

Several mechanisms are used as a consensus mechanism during coin trading. These mechanisms are as follows:

- **Proof of work :**'Proof' refers to the solution of a highly-complex problem, and 'work' refers to the process of solving the same. Crypto coin miners compete to solve the problem and gain the right to process the transaction. The fastest solver receives a mining fee from the traders of these coins.
- This mechanism tracks and verifies the creation and transactions across blockchain networks. It enables miners by allowing them to validate new transactions and is extremely secure. However, it has several cons, such as high electricity requirements and difficulty for individual miners.
- **Proof of Stake** :This mechanism randomly chooses a maximum coin owner to validate a transaction. It also allows the owner to create a block for the same coin. This mechanism requires comparatively less energy, transaction time and a lower fee. Coins like Etherium 2.0, Polkadot, Cosmos, Cardano, ThorChain, Nxt and Algorand use this mechanism extensively. There is a security risk as if an owner owns 51% or more coins of a particular coin, then that person will get sole ownership of its network.
- **Proof of Capacity** :The PoC mechanism heavily relies on free space available in the hard drive. This is because there are many solutions to a coin's hash problem that a trader needs to store. It is highly efficient as compared to PoW and PoC mechanisms. Coins such as Burst, Storj SpaceMint and Chia use these mechanisms.
- **Proof of Activity** :This mechanism is a combination of both Proof of Work and Proof of Stake. It has been designed to combine the best features of PoW and PoS. In the beginning, the Proof-of-Activity mechanism functions like PoW. Once a new block is completed, it starts to function like a Proof-Of-Stake mechanism. Coins such as DCR (Decred) use this mechanism.
- **Proof of Authority** :Different organisations and private companies created this unique mechanism. There are validators with approved accounts which authorise transactions and the creation of new blocks. These validators must disclose their true identity to get the right to validate a transaction.
- **Proof of Burn :**POB aims to improve the quality of blockchain so that it can be used easily and extensively as a tool for faster and more secured transactions. After PoW and POS, POB is designed to prevent fraud activities on a blockchain network. Cryptocurrencies such as Bitcoin use this mechanism to offer secure transactions to traders.
- **Proof of Elapsed Time** :Intel Corporation created this mechanism to permit blockchain to decide the person who will create the next block. It uses a lottery system to decide the next block creator. Thus, it gives a fair chance to all traders to create the next block. It is an efficient process involving utilising lesser resources and low energy consumption.

What makes blockchain immutable?

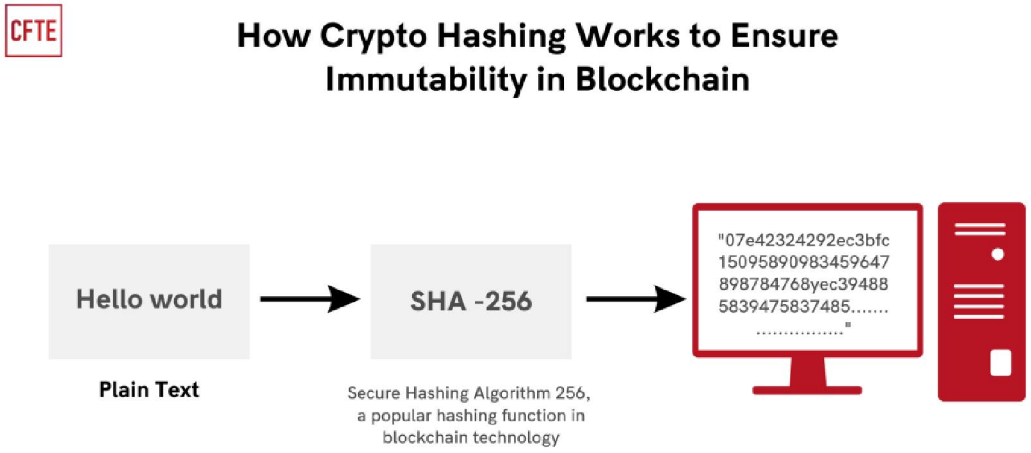
Blockchain's immutability arises from cryptographic algorithms that are used to secure information and data stored. All the data is stored in a block and contains a specific cryptographic hash representing its data. Crypto hashing is a process

ISSN 2581-9429 IJARSCT

DOI: 10.48175/568

in which the plaintext input creates a unique hash value as an output. The length of hashes remains constant irrespective of input properties.

For example, while using the Secure Hashing Algorithm 256 (SHA-256), the input is first converted to binary before undergoing encryption. If we input the word ‘Hello’ into SHA-256, the output generated will consist of 64 characters, which is the same length as the outputs for ‘Hello world’ and ‘Hello John.’


CFTE
How Crypto Hashing Works to Ensure Immutability in Blockchain
Hello world
Plain Text
SHA -256
Secure Hashing Algorithm 256, a popular hashing function in blockchain technology
"07e42324292ec3bfc
15095890983459647
898784768yec39488
5839475837485.......
................"

Source: upgrad

These blocks cannot be modified, as reversing the hashing algorithm is complex. The hash value acts as electronic identification or digital signature during data transactions across a network and is valuable for ensuring data accuracy.

IV. WHAT ARE SMART CONTRACTS?

Smart contracts are digital contracts stored on a blockchain that are automatically executed when predetermined terms and conditions are met.

Smart contracts are typically used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary’s involvement or time loss. They can also automate a workflow, triggering the next action when predetermined conditions are met.

What is Ethereum?

Ethereum is a decentralized blockchain technology that’s not owned or regulated by a third party such as a government or central bank.

Ethereum is used for building decentralized apps (dApps), holding and transacting cryptocurrency and other digital assets, and creating new cryptocurrencies.

Ethereum’s native cryptocurrency, called ether (abbreviated to ETH), powers Ethereum. Imagine ETH as the fuel and Ethereum as the engine.

How does Ethereum work?

The Ethereum network is like a large, powerful, decentralized computer.

Through computer code it can complete almost any task if it has enough time, processing power and instructions. This means a varied range of applications can be built on its blockchain, making Ethereum the rails on which many blockchain-based projects run.

DOI: 10.48175/568

How do Ethereum and Bitcoin compare?

The basic similarities between Bitcoin and Ethereum are:

They're not owned or regulated by a third party such as a central bankK

They both use blockchain technology to record and store transaction detailsK P They both have digital currencies (BTC and ETH) that can be stored in cryptocurrency wallets.

However, the main differences are:

Use case: Ethereum was created as a platform to facilitate smart contracts and dApps. Bitcoin was created as a currency alternative.

Supply: Ethereum has no limits on its total supply amount and instead uses its own supply and demand economics to define its scarcity. Bitcoin has a fixed total supply of 21 million.

How it works: Ethereum uses a proof-of-stake consensus algorithm, which means that users can earn rewards by holding ETH in their wallets and staking, or pledging, them to validate transactions. Bitcoin runs on a proof-of-work consensus algorithm, which involves people dedicating computing power to validate transactions (called mining).

What are Decentralized Apps (dApps) in Blockchain?

Decentralized apps are digital applications or programs that are based on Blockchain and fundamentally different from normal applications. Unlike normal applications that run on centralized servers that belong to the company which owns them, dApps run on a **decentralized peer-to-peer (P2P) network** that is baseon Blockchain.

What are Decentralized Apps dApp?

Decentralized applications or dApps are distributed, decentralized open-source software applications that run on a decentralized peer-to-peer network. Imagine the Twitter application that you have on your phone. You can post anything you want on Twitter but ultimately it's controlled by a single company that can delete your tweets if they violate community guidelines or some other reason. But if there was a Twitter-type dApp, then it would be decentralized and not owned by any one person. If you posted something there, nobody would be able to delete it including its creators.

Multiple people can create content and consume content on these applications that is free of any control and interference from one person. Below are some of the requirements of dApps:

1.Open Source: dApps should be open source and its codebase should be freely available for all. Any changes in the structure or working of the app should only be taken with the agreement of the majority.

2. Decentralized: dApps should be decentralized with all the information and operations stored on a public and decentralized Blockchain which would ensure security and transparency.

3.I ncentive: dApps should offer some sort of incentive to their users in the form of cryptographic tokens. These are a sort of liquid assets and they provide incentives for users to support the Blockchain dApp ecosystem.

4. Protocol: dApps should have a particular protocol to demonstrate proof of value. This means showing the value of a particular process in a way that caverified by others.

How Do DApps Work?

A DApp has a backend code running on a decentralized peer-to-peer network. It can also have a frontend code and a user interface that can be written in any language just as it is done for normal applications. The front end can be hosted on any decentralized server like IPFS. DApps work in a manner similar to normal applications except for the few differences that are discussed below:

The DApp working has the following features:

Decentralized: A DApp operates on Ethereum which is an open public decentralized platform.

Deterministic: DApps perform the same function irrespective of the environment in which they are executed.

Turing complete: DApps can perform any action given the required resources.

DOI: 10.48175/568

Isolated: DApps are executed in an Ethereum Virtual Machine which is a virtual environment that ensures that even if there is a bug in the smart contract, it won't hamper the normal functioning of the blockchain network.

What is a Hard Fork?

Now, as we get a deeper comprehension of soft fork vs. hard fork, let us understand the hard fork first. Consider this a process in which the creation of a new blockchain is imminent, with a few miners disagreeing to bring the upgrade. A hard fork is essentially the permanent divergence of a new side chain from the original one. The consensus of nodes and developers that agree to the new set of rules follow the newer version of the blockchain. The old blockchain no longer considers the newer one valid, meaning it is not backward compatible. A hard fork generally degrades the network's security and efficiency since the consensus between network validators and security breaks.

Why Do Hard Forks Happen?

Since hard forks can make the blockchain network vulnerable, why do the nodes even consider them? The answer is to move forward with the requirements of the nodes. There can be requirements related to new functionalities, security procedures, resolving a disagreement in the network, or even resolving some faulty transactions on the network. Sometimes they occur by accident, too, when two miners work on the same block and the blockchain splits due to different consensus results on the same block. The participants follow the old block, and the new one is called the orphan block.

What is a Soft Fork?

A soft fork is considerably simpler than a hard fork since there are no major changes to the consensus mechanism. It can occur when the majority of nodes or miners agree to smaller upgrades to the protocol without changing the original rules of the network. There is no requirement for all the nodes on the network to upgrade to the new version. An original singular chain with minor upgrades moves forward in the network, and the risk of 'double spending' goes away. Soft forks are backward compatible and can sometimes be used by hackers to manipulate the nodes and bring malicious changes to the chain.

What is a Soft Fork?

A soft fork is considerably simpler than a hard fork since there are no major changes to the consensus mechanism. It can occur when the majority of nodes or miners agree to smaller upgrades to the protocol without changing the original rules of the network. There is no requirement for all the nodes on the network to upgrade to the new version. An original singular chain with minor upgrades moves forward in the network, and the risk of 'double spending' goes away. Soft forks are backward compatible and can sometimes be used by hackers to manipulate the nodes and bring malicious changes to the chain.

Difference Between Hard Fork and Soft Fork

Characteristics	Hard Forks	Soft Forks
Authority level	They often make a change to the original protocol, thus requiring a stronger consensus of nodes and miners	It is backward-compatible, so attackers can reinstate earlier models by manipulating the nodes.
Split in the chain	The original chain splits into two.	There is no splitting as the original chain moves forward with minor upgrades.
Need for	All the users on the network need to	Only the ones that have the use of

upgradation	agree to the new chain in order to use it.	upgrades need to upgrade their network.
Vulnerability	It is not backward compatible. Hence hackers can take the majority consensus by manipulation and create a hard fork.	It is backward-compatible, so attackers can reinstate earlier model by manipulating the nodes.
Power Requirements	Hard forks require high computational power since a new side chain generates out of the original one.	Generally, 51% hash power is required for a soft fork.

What is an Initial Coin Offering (ICO)?

Initial Coin Offering (ICO) is a fresh way for businesses to generate funds using cryptocurrency. It is a way to launch a new coin by selling it to investors during a large period. For example, Coinbase is a crypto/fiat-based company that has recently launched its IPO(Initial Public Offering) i.e.; they are sharing some shares of their company in return for money and that money can be used to have fund some of their projects and anything else they need capital of. Just like Coinbase a coin or a token in the crypto world is called an ICO. A token creator can sell a bunch of digital tokens for a set price to get the token out into the market and raise capital for the creator or project.

Types of ICOs

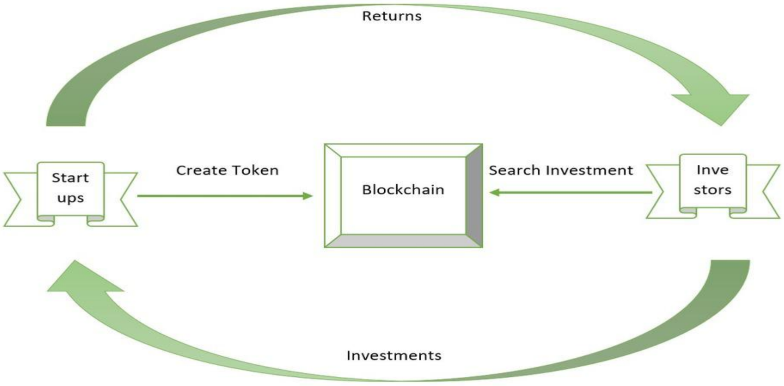
There are two types of ICO:

Private ICOs: In this ICO only a selected number of investors are allowed to participate. Since only a selected number of participants are there and the company requires a lot of money these participants are big institutions and high-worth individuals and a company can choose a minimum investment amount.

Public ICOs: In this type of ICO everyone can participate and it is targeted at the general public, due to some regulatory concerns the private ICO is becoming a more viable option for the companies. Since the general public can participate in the ICOs companies set the money cheaper so that most public can buy and they can make a lot of money for their project.

Working of ICO

An ICO is a process that requires deep knowledge of the technology. The main idea behind the ICO is to raise capital for the investment from an investor to the companies. Additionally, for raising funds in ICO the project organizer first determines its structure of it. There are generally three types of structures of ICO:



ISSN 2581-9429 IJARSCT
DOI: 10.48175/568

Static Supply and Static Price: In this type, the number of tokens and their price are fixed.
Static supply and dynamic Price: In this type, the number of funds received in the ICO will determine the price of the token
Dynamic supply and static price: In this type, the amount received determines the supply of ICO.

V. LATEST TRENDS IN BLOCKCHAIN TECHNOLOGY

What’s the Difference Between Web3 and Metaverse?

Basis	Web3	Metaverse
Definition	Web 3.0 will be based on a decentralized blockchain system that will not allow for centralized ownership of information, services, or platforms.	The Metaverse is a 3D interactive experience space that allows users to interact with 3D objects using augmented, virtual, and mixed reality.
The Application’s Scope	It’s applicable throughout the internet.	Currently, it’s in progress as it’ll take time to develop and some of the areas are still under scrutiny.
Target	Web3 targets blockchain-controlled and peer-to-peer controlled facilities.	Metaverse targets AR, VR, and MR/XR facilities.
Application	It applies to democratic internet systems and permissionless financial networks like Crypto. Web 3 leverages ML, AI, and blockchain to attain real-world human communication.	It applies in the virtual gaming world, 3D surgeries, peer-to-peer virtual meetups, etc.
Depiction	Individuals can own the internet and regulate it on their own accord.	Turning physical materials into virtual material in a virtual world.
Underlying technology	Blockchain, DeFi, NFTs, DAOs.	AR/VR, 3D Reconstruction, Internet of Things (IoT), Edge Computing & 5G, Blockchain.
Technical	Powered by DAO (Decentralized Autonomous Organization), AI, and Blockchain.	Powered by 5G communication, extended reality, brain-computer interfaces, cloud computing, blockchain, digital twins, creators economy, and artificial intelligence.

What Is a Central Bank Digital Currency (CBDC)?

A central bank digital currency (CBDC) is a form of digital currency issued by a country's central bank. It is similar to cryptocurrencies, except that its value is fixed by the central bank and is equivalent to the country's fiat currency.

ISSN 2581-9429 IJARSCT
DOI: 10.48175/568

Many countries are developing CBDCs, and some have even implemented them. Because so many countries are researching ways to transition to digital currencies, it's important to understand what CBDCs are and what they mean for society.

ACKNOWLEDGMENT

We extend our gratitude to the various sources, including research papers, industry reports, and technical blogs, that contributed to this study. Special thanks to our mentors, peers, and organizations that provided valuable insights and resources for understanding blockchain technology in depth.

DISCUSSION

Blockchain technology is a transformative innovation that eliminates the need for central authorities by enabling decentralized transactions and data management. This discussion delves into the working principles of blockchain, including its structure, transaction validation mechanisms, and security protocols. Additionally, it compares different blockchain types—public, private, hybrid, and consortium—and evaluates their advantages and limitations. The review also highlights real-world applications, such as smart contracts, decentralized finance (DeFi), and non-fungible tokens (NFTs), along with ongoing challenges like scalability, regulatory concerns, and interoperability.

VI. CONCULSION

Blockchain technology has emerged as a disruptive force across various industries, providing enhanced security, transparency, and efficiency. Its decentralized nature ensures trustless interactions, reducing dependency on intermediaries. However, challenges such as energy consumption, scalability, and regulatory compliance must be addressed for widespread adoption. As blockchain continues to evolve, integrating emerging trends like Web3, Layer 2 solutions, and Central Bank Digital Currencies (CBDCs) will play a crucial role in shaping the future of digital economies.

REFERENCES

[1]. https://www.investopedia.com/terms/b/blockchain.asp#toc-what-is-a-blockchain
[2]. https://www.w3schools.in/blockchain/introduction-to-blockchain-technology
[3]. https://www.etoro.com/wp-content/uploads/2018/10/A-beginners-guide-to-blockchain.pdf
[4]. https://en.wikipedia.org/wiki/Blockchain#Blocks
[5]. https://en.wikipedia.org/wiki/Blockchain#History
[6]. https://www.ibm.com/think/topics/benefits-of-blockchain
[7]. https://en.wikipedia.org/wiki/Blockchain#Centralized_blockchain
[8]. https://101blockchains.com/blockchain-vs-database-the-difference/
[9]. https://www.geeksforgeeks.org/types-of-blockchain/
[10]. https://builtin.com/blockchain/blockchain-applications
[11]. https://blockchain.gov.in/Home/BlockChain?blockchain=feature
[12]. https://skillfloor.medium.com/the-benefits-and-challenges-of-implementing-blockchain-technology-96ce7688faf4
[13]. https://www.geeksforgeeks.org/how-does-the-blockchain-work/
[14]. https://www.geeksforgeeks.org/what-is-p2p-peer-to-peer-process/?ref=lbp
[15]. https://cleartax.in/s/consensus-in-blockchain
[16]. https://blog.cfte.education/immutable-ledger-in-blockchain/
[17]. https://www.ibm.com/think/topics/smart-contracts
[18]. https://www.blockchain.com/learning-portal/tokens/ethereum-explained
[19]. https://www.geeksforgeeks.org/what-are-decentralized-apps-dapps-in-blockchain

ISSN 2581-9429 IJARSCT

DOI: 10.48175/568

[20]. https://shardeum.org/blog/hard-fork-vs-soft-fork/
[21]. https://shardeum.org/blog/hard-fork-vs-soft-fork/
[22]. https://www.geeksforgeeks.org/what-is-an-initial-coin-offering-ico/
[23]. https://www.geeksforgeeks.org/web3-vs-metaverse/
[24]. https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp

ISSN 2581-9429 IJARSCT

DOI: 10.48175/568