SPPU New Syllabus

A Book Of

BLOCKCHAIN TECHNOLOGY

For T.Y.B.Sc. Computer Science : Semester – V

[Course Code CS 3511 : Credits - 2]

CBCS Pattern

As Per New Syllabus, Effective from June 2021

Dr. Ms. Manisha Bharambe

M.Sc. (Comp. Sci.), M.Phil. Ph.D. (Comp. Sci.)

Vice Principal, Associate Professor, Department of Computer Science

MES's Abasaheb Garware College

Pune

Ms. Manisha Gadekar

M.C.A., (Science), UGC-NET

Assistant Professor, Annasaheb Magar College

Pune

NIRALI PRAKASHAN

~~Price: ₹ 130.00~~

Price: ₹ 155.00

NIRALI PRAKASHAN

ADVANCEMENT OF KNOWLEDGE

N5868

Syllabus ...

1. Introduction to Blockchain (7 Lectures)

- Foundational Computing Concepts (Client-Server Systems vs Peer to Peer Systems)
- Evolution of Blockchain
- Blockchain vs Database
- Essentials of Blockchain (Blockchain Generations, Types of Blockchain, Benefits and Challenges of Blockchain Usage)
- Types of Networks
- Layered Architecture of Blockchain Ecosystem
- Components of Blockchain
- Cryptography (Private and Public Keys, Hashing and Digital Signature)
- Consensus Mechanisms
- Cryptocurrency, Digital Currency Bitcoin and Ethereum
- Smart Contracts
- Blockchain Use Cases

2. How Blockchain Works? (5 Lectures)

- Understanding SHA-256 Hash
- Immutable Ledger
- Distributed P2P Network
- How Mining Works? (The Nonce and Cryptographic Puzzle)
- Byzantine Fault Tolerance
- Consensus Protocols (Proof of Work, Proof of Stake, Defense against Attackers, Competing Chains
- Blockchain Demo

3. Smart Contracts (6 Lectures)

- Ethereum Network
- What is a Smart Contract?
- Ethereum Virtual Machine, Ether, Gas
- DApps
- Decentralized Autonomous Organizations (DAO)
- Hard and Soft Forks
- Initial Coin Offerings
- Demo of Smart Contracts

■■■

Contents ...

1. Introduction to Blockchain 1.1 – 1.

2. How Blockchain Works? 2.1 – 2.

3. Smart Contracts 3.1 – 3.

CHAPTER 1

Introduction to Blockchain

Objectives...

- To learn Concepts of Blockchain
- To study Layered Architecture of Blockchain
- To learn Evolution of Blockchain

1.0 INTRODUCTION

- Blockchain technology has been called the one of greatest innovations of the 21st century. Blockchain based applications are fast growing up and can be used in financial services, education systems, healthcare, IoT, supply chain and many more.
- Blockchain is a peer-to-peer distributed ledger or public registry that permanently records transaction in a way that cannot be update.
- Blockchain combines the terms "block" and "chain" as explained below:
  - A **block** can be seen as a file that contains information about all the transactions that have been processed. Every transaction contains information about the sender and receiver and some form of identification that makes the transaction unique and connected to the others.
  - For a **chain**, the blocks are arranged in linear sequence.
- Blockchain is an emerging technology platform for advancing distributed applications and data storage, over and beyond its role as the technology underlying the crypto-currencies.
- The primary principle of Blockchain technology is that it allows to create a distributed and duplicate ledger of transactions and data generated through various IT processes with strong cryptographic guarantees of interfere resistance, immutability and sustainable.
- It is approximate that Blockchain will generate $3.1 trillion in new business value by 2030.
- Blockchain is essentially, provides the basis for a dynamic distributed ledger that can be applied to save time when recording transactions between parties, remove costs associated with negotiator and reduce risks of fraud and tampering.

- Blockchain technology has become widely popular because of it is use in the implementation of crypto-currencies such as Bitcoin, Ethereum etc.
- The technology itself carry much more agreement, in various areas such as recording of transactions, time stamping, logging of critical events in a system, trustworthy e-governance etc.
- Blockchain is a specific type of database which differs from a typical database in the way it stores information; Blockchains store data in blocks that are then chained together.
- As new data comes in it is entered into a new block. Once, the block is filled with data it is chained onto the previous block, which makes the data chained together in chronological order.
- Different types of information can be stored on a Blockchain but the most common use so far has been as a ledger for transactions.
- In simple words, a Blockchain is a chain of blocks which contain information. Each block in Blockchain records all of the recent transactions and once completed goes into the Blockchain as a permanent database. Each time a block gets completed, a new block is generated.
- Blockchain technology is a public ledger which is factually needed in distributed system that records all transactions that have be executed sharable among participating parties in distributed network.

1.1 FOUNDATIONAL COMPUTING CONCEPTS

- Computing involves process-oriented step-by-step tasks/operations to complete a goal-oriented computation. Normally we can say that a goal is a complex operation that is processed using a computer.
- Computation is any type of calculation that includes both arithmetical and non-arithmetical steps and which follow a well-defined model (e.g. an algorithm).
- Computing may encompass the design and development of software and hardware systems for a broad range of purposes - often structuring, processing and managing any kind of information.
- Blockchain technology is simply described, as a decentralized, distributed ledger that records the source of a digital asset.
- A blockchain has a decentralized and distributed style of network of computers.
- In decentralized computing the whole workload is distributed to the computing nodes so that each computing node has equal processing power.
- Distributed computing is concurrent processing of multiple processes at the same time over a computer network.

- Blockchain technology is combination of cryptography and computer networking. Computer networking is the application of the technology and architecture in which connect the nodes that is computer systems, hence established communication and resource sharing among these systems.
- Distributed computing methods are one of the basic computing principles that drive the Blockchain mechanism. Generally, distributed computing methods are like a network of computers working together as a single system.
- The usage of distributed systems and distributed computing technologies has vital roles in solving real-world problems.
- Blockchain technology considers the two computing systems/networks namely, Client-Server system and Peer-to-Peer system.

1.1.1 Client-Server Systems

- Client-server system/computing/network is architecture of distributed applications in which most of the resources and services consumed by users (clients) are managed and exhibited by a centralized server.
- The server is an entity that is purely responsible for offering services to the client; servers provide services like storage, data processing, deploying applications, etc.
- Clients are the individual entities which are connected in a network. Client sends a request/query to server and server responds accordingly.
- The server is more powerful than the client or user in terms of computing power, storage and authority.
- Now a days, most of the websites of the modern Internet use client-server architecture.
- Client-server system is a good example of a service-oriented system. Fig. 1.1 shows client-server system.

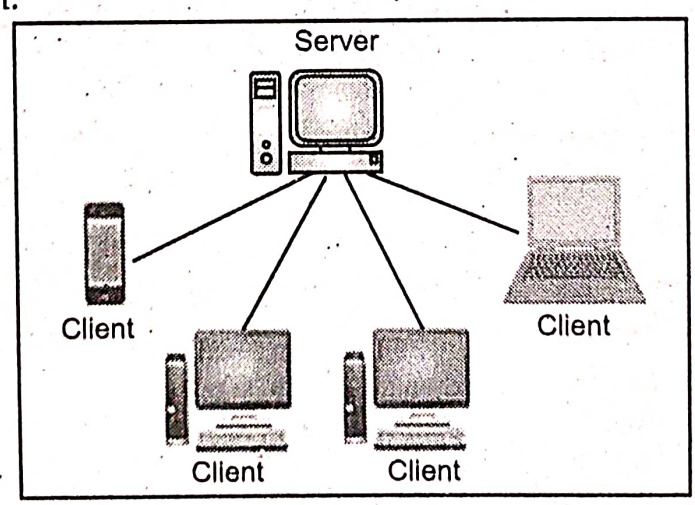


Fig. 1.1: Client–Server System

- Client-server system is a centralized system which has centralized control over system. In client-server system all the data is stored on server so it is easy to make a back-up of it.

- In client-server system new resources and systems can be added easily by jus upgrading the server. In client-server system rules defining security and access right can be defined at the time of set-up of server.
- Client-server system is not as robust means, if the server fails, the whole network goe down. Client-server system is very expensive to install.

1.1.2 Peer-to-Peer (P2P) Systems

- Peer-to-peer system/network is an architecture, that work is assigned equally to all system or nodes i.e., in the network and all nodes are considered to have the same authority.
- P2P system is a network of inter-connected systems in which they are capable of sharing resources and information. Every system connected to the network is referred to as a node or "peer".
- P2P system can be used in Blockchain technology, transportation services, education, e-commerce, banking and finance, etc.
- In Peer-to-Peer (P2P) network each of the participation workstation (computer) has same (equivalent) privileges, capabilities and responsibilities.
- Peer-to-peer networks are referred to as decentralized architectures. Peer-to-peer networks, nodes behave, as server and client both simultaneously.
- In peer-to-peer system, there is no centralized control or server to serve the requests, any node can act as a server and serve a request.
- These networks have a hierarchy with no single point of ownership, authority or control and hence no single point of failure.
- Blockchain networks are generally public peer-to-peer networks, i.e., anyone or any user can join them and as it is a peer-to-peer network no one owns or completely controls the network. This is the "decentralization of control" which Blockchains provide.
- In peer-to-peer networking, even if one peer gets down, the other peers are still working or alive, so nobody can take down the Blockchain.

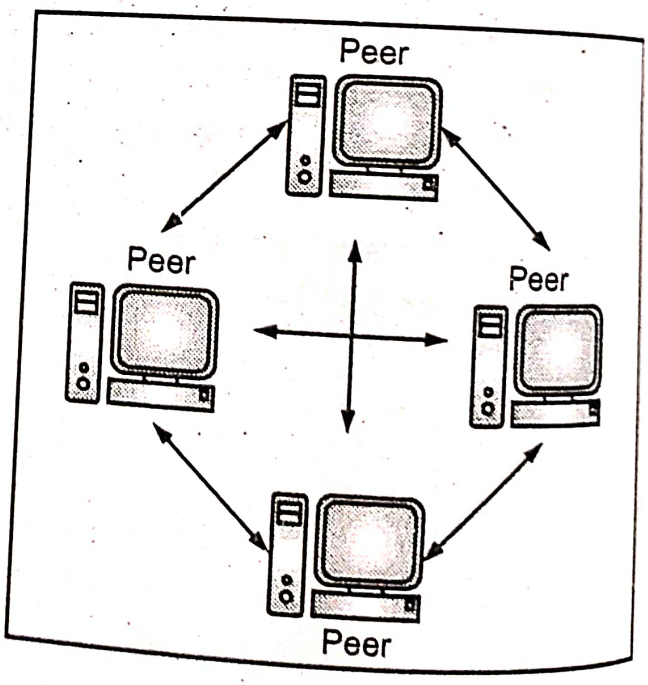


Fig. 1.2: Peer-to-Peer (P2P) System

- The peer-to-peer architecture of Blockchain allows all crypto-currencies to be transferred all over the worldwide, without the need of any middle-man or intermediaries or central server.
- Advantages of P2P system includes, P2P system can be easily configured and install. In P2P system if any single node goes down it will not affect the whole system. Maintaining P2P system is comparatively cost-effective.

- Number of P2P networks has very little security available to protect the information stored on individual peers. In P2P networks each direct connection between individual peers results in slower performance.

Difference between Client-Server System and Peer-to-Peer (P2P) System:

- In client-server system, the client nodes requests for services and server node responds with services. Whereas, in Peer-to-Peer (P2P) system, each node/peer can request for services and provide services.
- In client-server system, the client request for service and server respond with the service. In P2P system each node can request for services and can also provide the services.
- Peer-to-Peer networks provide more security compared to traditional client-server systems.
- The client-server system is centralized system while P2P is decentralized system. A client-server system is more stable and secure than a peer to peer system/network.
- A client-server system is expensive ti install while P2P system is less extensive to set up or install.

1.2 EVOLUTION OF BLOCKCHAIN

- Blockchain technology has massive innovations of the 21st century given the ripple effect; it is having on various sectors like banking, healthcare, supply chains, education and so on.
- Blockchain was introduced in the early 1990s, but its popularity started growing a few years back, a number of applications have cropped up all but underlining the kind of impact it is destined to have as the race for digital economies quickly grow up.
- The Blockchain has evolved early 1990s, starting with S. Haber and W. Scott Stornetta's work on cryptographically secure chain of blocks, the first work on a cryptographically secured block chain where no one tampered with time stamp of document.
- Then in 1992, the system was upgraded with the Merkle tree approach, which optimized and combined all tasks into a single one.
- In the year 2008 Blockchain gained relevance due to a group of people named Satoshi Nakamoto and is the accredited brain behind the digital ledger technology.
- The new concepts and approaches evolved into the Blockchain mechanism for transformation towards digital data/information utilization in the year 2009. In the beginning it was developed to support Bitcoin.
- Decentralized data using a decentralized database are the core components of Blockchain. The need for Bitcoin increased drastically so Blockchain made immediate changes to the Internet. The Russian-Canadian transferred money in form of Bitcoin scripting language.

- The decentralized nature of the Blockchain technology can make any language readable by computer rather than third party, which will generate smart contracts. The Ethereum projects are useful in efficient transaction management systems.
- A smart contract is simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum Blockchain.
- The security of transaction through the Blockchain methodology produces different digital transaction systems such as Bitcoin, crypto-currency, Ethereum and Lightcoin ripple which can handle huge numbers of transaction per second.
- In the years 2013-2015 the system developed to Ethereum development with version Blockchain 2.0. It provides for the recording of books as well as contracts. This can develop the decentralized application efficiently.
- In the year 2018 a new version of Blockchain evolved Blockchain 3.0. It supports the leveraging capabilities of Blockchain. The new Blockchain application is called NEO, which is an open source, decentralized application platform first developed in China.
- The base asset of the Neo (formerly Antshares)Blockchain is the non-divisible Neo token which generates GAS tokens (a separate asset on the network, can be used to pay for transaction fees).
- For further upgrades with the Internet of Things (IoT), IOTA was developed. It supports the IoT ecosystem for digital transactions.
- IOTA is an open-source distributed ledger and cryptocurrency designed for the Internet of things (IoT).
- IOTA is a distributed ledger developed to handle transactions between connected devices in the IoT ecosystem, and its cryptocurrency is known as mIOTA.
- Fig. 1.3 shows evolution of Blockchain technology.

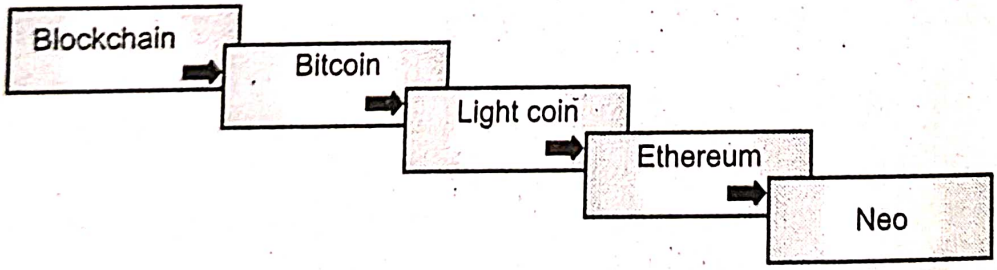


Fig. 1.3: Evolution of Blockchain Technology

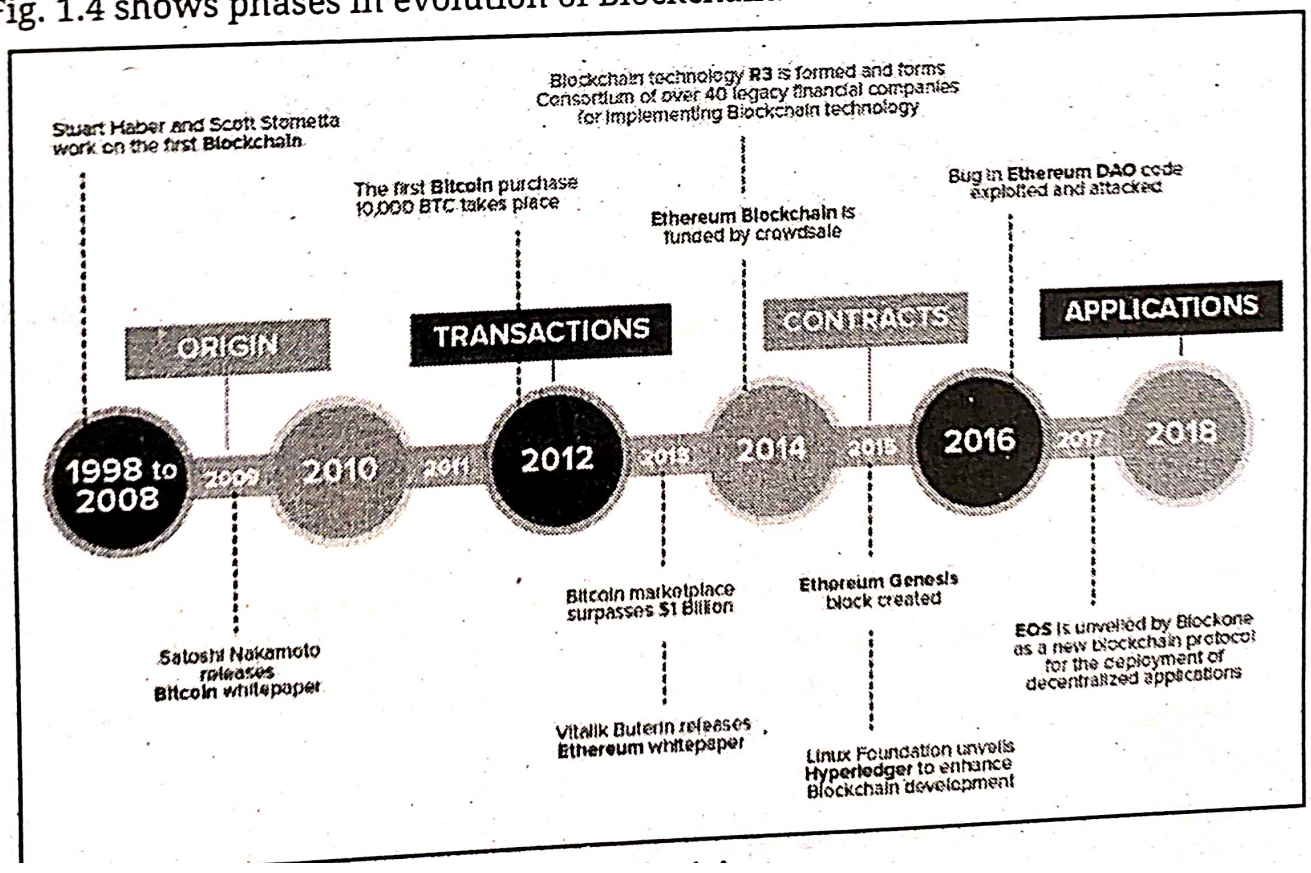
- Evolution of Blockchain technology in Fig. 1.3 is explained below:

1. **Bitcoin:** Bitcoin is first decentralized cryptocurrency uses peer-to-peer network without the need for intermediaries. The Bitcoin cryptocurrency was invented in 2008 by an unknown person or group of people using the name Satoshi Nakamoto. The bitcoin blockchain is a public ledger that records Bitcoin transactions. There are currently more than 18.5 million Bitcoin tokens in circulation, against a present capped limit of 21 million.

2. **Litecoin:** Litecoin was created in 2011 by Charlie Lee, a former employee of Google. He designed it to improve on Bitcoin technology, with shorter transaction times, lower fees, more concentrated miners.
3. **Ethereum:** Ethereum was launched in July 2015 by Vitalik Buterin. Ethereum is the currently holds the second-largest cryptocurrency after Bitcoin. Ethereum is a blockchain platform with its own cryptocurrency, called Ether (ETH) and its own programming language, called Solidity.
4. **Ripple:** Ripple is a type of cryptocurrency operates on an open-source and peer-to-peer decentralized platform that allows for a seamless transfer of money in any form like Litecoin or Bitcoin. Ripple is a blockchain-based digital payment network and protocol with its own cryptocurrency, XRP.
5. **NEO:** It is formerly called Antshares and developed in China, NEO is very aggressively looking to become a major global cryptocyrrency player. Its focus is smart contracts (digital contracts) that allow users to create and execute agreements without the use of an intermediary.
6. **IOTA:** Launched in 2016, IOTA stands for Internet of Things (IoT) application. Billions of devices were connected to the Internet by 2020. Within this Internet of Things (IoT) ecosystem, smarts devices can exchange data and payment information with multiple other devices in transactions conducted throughout the day. IOTA intends to become the standard mode of conducting transactions on smarts devices.

Phases of Evolution of Blockchain:

- Fig. 1.4 shows phases in evolution of Blockchain.



- Various phases in evolution of Blockchain are explained below:

Phase 1 (Transactions):

2008-2013: Blockchain 1.0 (Bitcoin Emergence)

- This is the first type of Blockchain that works with cryptocurrency in Bitcoin. It was introduced in 2008 by Shatoshi Nakamoto. The first version is known as 1.0. Internet-based financial transactions are enabled by Internet of Money or cryptocurrencies. This is the basic type works on 16-bit architecture.

Phase 2 (Contracts):

2013-2015: Blockchain 2.0 (Ethereum Development)

- Bitcoin is some limitations, so Vitalik Buterin started working on what he felt would be a fexible, blockchain that can perform various functions in addition to being a peer-to-peer network.
- Ethereum was born out as a new public blockchain in 2013 with added functionalities compared to Bitcoin, a development that has turned out to be a pivotal moment in Blockchain history.
- Vitalik Buterin differentiated Ethereum from Bitcoin Blockchain by enabling a function that allows people to record other assets such as trademark as well as contracts.
- The latest feature expanded Ethereum functionalities from being a cryptocurrency to being a platform for developing decentralized applications.
- In 2015, Ethereum blockchain has progress to become one of the biggest applications of blockchain technology given its ability to support smart contracts used to perform various functions.
- Ethereum blockchain platform has also succeeded in combining an active developer community that has seen it establish a true ecosystem.
- Ethereum blockchain developments, the most number of day to day transactions recall to its ability to support smart contracts and decentralized applications. It is market cap has also increased extremely in the cryptocurrency space.

2015: Hyperledger

- In 2015, the Linux Foundation exposed an Umbrella project of open-source blockchain.
- They are designated, it as Hyperledger, which until to date acts as collaborative development of distributed ledgers.
- Under the leadership of Brian Behlendorf, Hyperledger seeks to advance cross-industry collaboration for the development of blockchain and distributed ledgers.
- Hyperledger focuses on supportive, the use of blockchain technology to upgrade the performance and reliability of modern systems to support global business transactions.

Phase 3 (Applications):

2016-2018: Blockchain 3.0 (The Future)

- In late years, a number of projects have cropped up all leveraging blockchain technology capabilities.
- New projects have desired to address some of the failing of Bitcoin and Ethereum in addition to coming up with new features leveraging blockchain capabilities.
- A few blockchain new applications include NEO, billed as the first open-source, decentralized, and blockchain platform launched in China.
- NEO register itself, as the Chinese Ethereum having already received the backing of Alibaba CEO Jack Ma as it plots to have the same impact as Baidu in the country.
- The cryptocurrency platform is develop for the Internet of things ecosystem as it is make an effort to provide zero transaction fees and also unique verification processes.
- To accelerate the development of the Internet of Things, some developers, so it fit, to leverage blockchain technology and in the process came up with IOTA.
- Other Second-generation blackchain platform and IOTA and NEO are also having a ripple effect in the sector.
- Monero Zcash and Dash blockchains came into being as a scheme of addressing some of the security and scalability issues associated with the blockchain applications.
- Classify as privacy Altcoins, the three blockchain platform seek to provide high levels of privacy and security when it comes to transactions.
- Co-operation like Microsoft and Microsoft appear to have some guide when it comes to exploring blockchain technology applications emerging in what has come to be known as private, hybrid and federated blockchains.

2017: EOS.IO

- In being, 2017 EOS brainchild of private company block on the publishing of a white paper detailing a new Blockchain protocol powered by an EOS as the native Cryptocurrency.
- EOS tries to imitate attributes of actual computers including CPU and GPU. IO doubles up as a smart contract platform as well as a decentralized operating system.
- The main purpose is to stimulate the deployment of decentralized applications (dApps) through an autonomous decentralized corporation.
- The main purpose is to stimulate the deployment of decentralized applications through an autonomous decentralized corporation.
- DApps (decentralized application) has their backend code running on a decentralized peer-to-peer network.
- A dApp can have frontend Blockchain example code and user interfaces written in any language that can make a call to its backend, like a traditional Apps.

2020: The Future

- The future of Blockchain technology glance bright, because of the in many way governments and enterprises or many organizations are investing big as they seek to stimulate innovations and applications.
- The technology is already finding great use in supply management as well as in the cloud computing business.
- The technology should also find its way into basic items such as search engines on the internet in the future.
- Gartner Trend Insights expects at least one business built on blockchain to come into being valued at more than $10 billion by 2022.
- Due to the Blockchain Digital Transformation, the research firm expects the business value to grow to over $176 billion by 2025 and exceed the $3.1 trillion by 2030.

1.3 BLOCKCHAIN vs DATABASE

- As Blockchain is a ledger that stores information in blocks, it actually makes it a database. A database in the same way stores information in data structures named tables.
- Nevertheless, a Blockchain is a database, but a database is not a Blockchain. Both these structures should never be interchanged as both of them serve a different purpose.

Differentiation between Blockchain and Database:

Sr. No.	Blockchain	Database
1.	A Blockchain is a chain of blocks which contain information.	A Database is a collection of related data.
2.	A Blockchain stores information in data structures called 'blocks'.	Database store data using 'tables', in the form of rows and columns.
3.	A Blockchain is a P2P decentralized distributed ledger.	Databases are centralized ledger.
4.	Blockchain uses a peer-to-peer distributed network/system.	Database uses a client-server network/system.
5.	Blockchain uses Read and Write operations.	The database supports create, read, update and delete operations.
6.	Data in Blockchain are secured and supports integrity.	Data in database is less secured and can be altered/updated by anyone.
7.	Blockchains are harder to implement and maintain.	Databases are easy to implement and maintain.

contd. ...

8.	Blockchains are slower because of verification and consensus methods.	Databases are extremely fast and offer great scalability.
9.	Blockchains are decentralized in nature.	Databases are centralized in nature.
10.	Blockchain has a history of records and ownership of digital records.	Databases record current information only. They do not detect information that was previously recorded.
11.	A blockchain is immutable means, the data/information stored in a block cannot be changed/updated once it has been validated.	A database is mutable means, the data/information stored in database can be changed as per requirement.
12.	Every blockchain may be considered as a database.	Every database cannot be considered as a blockchain.

1.4 ESSENTIALS OF BLOCKCHAIN

- In this section we will study basic concepts in Blockchain like generations, types of Blockchain, benefits and challenges of Blockchain and so on.
- Blockchain is a decentralized, shared and trusted distributed ledger (or database) that consists of encrypted 'blacks' of information added to a chain of existing blocks of records.
- A Blockchain is an immutable public ledger for recording transactions. A blockchain ledger stores all of the transactions processed in peer-to-peer Blockchein network.
- Blockchain's transactions are called 'immutable' because once inserted in a block, they become permanent and cannot be modified retroactively, not even by the authors, without the alteration of all subsequent transactions.
- A formal definition of blockchain can be given as, "a blockchain is an immutable distributed ledger secured by cryptographic techniques and managed by a decentralised community over a peer-to-peer network through incentivisation"

Why Blockchain?

- Following are some of the reasons why we need to embrace Blockchain technology:
  1. **Automated Operations:** In Blockchain networks, operations are fully automated through software implications. Private companies are not needed to oversee the operations.
  2. **Open-source Technology:** Blockchain happens to be an open-source technology. All operations within a Blockchain network are carried out by the open-source community.
  3. **Secure:** It is impossible for anyone to tamper with transactions or ledger records present in Blockchain.

4. **Distributed Architecture:** Blockchain works in a distributed mode in which records are stored in all nodes in the network. If one node goes down, it doesn't impact the other nodes or records.
5. **Worldwide Adaptation:** Blockchain has been adopted worldwide and has the backing of many investors from both the banking and non-banking sectors.
6. **Flexible:** The Blockchain network can be programmed using the basic programming concepts. This flexibility makes Blockchain networks easy to operate on.

- Fig. 1.5 shows features/characteristics of Blockchain technology.

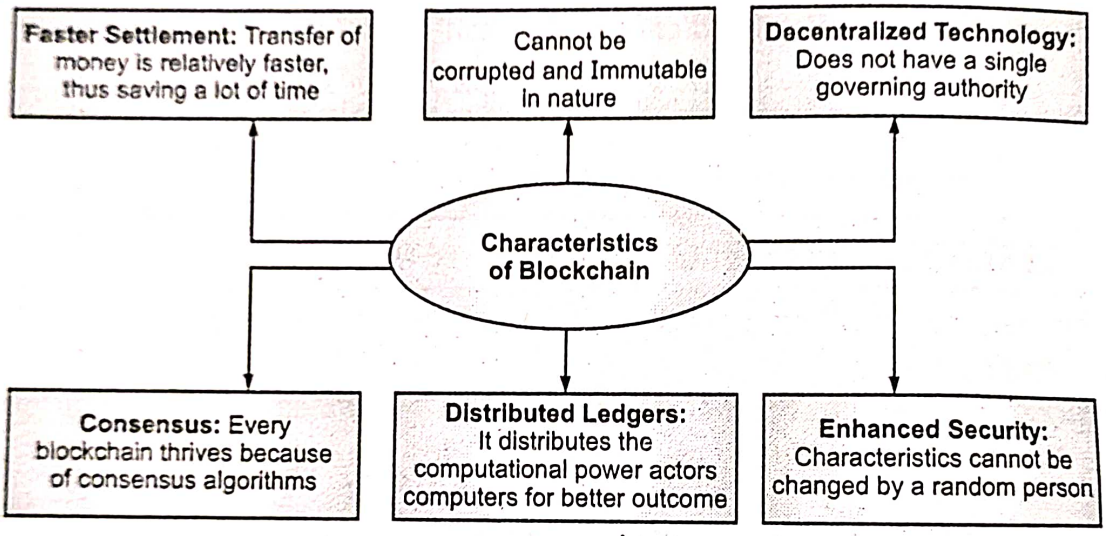


Fig. 1.5: Characteristics of Blockchain Technology

Concept of Blockchain Technology:

- Blockchain technology is probably the most attractive innovation since the emergence of the internet. Blockchain refers to an open distributed ledger spread across mid tipk computers that hold digitally recorded transactions in a much more efficient, transparent, and secure manner.
- A Blockchain consists of a number of blocks, each containing data relating to digital assets and a hash header that links it to the previous block in the chain.
- The blocks in a Blockchain are linked together, and new blocks can be added and removed, following a process of consensus.
- Also, those involved in the transactions can share the distributed digital ledger without needing a centralized intermediary.
- The structure of Blockchain technology is represented by a list of blocks that are ordered, with these blocks represented as transactions in a particular order.
- Fig. 1.6 shows structure of a Blockchain. In Fig. 1.6, the first block is represented in Black color.
- A genesis block/main block is the first block of the blockchain. It has the maximum number of blocks from the origin to the current block.

- The Grey color blocks form the main chain and the White color with Black border blocks are orphaned blocks outside the main chain.
- The nodes that complete the consensus mechanism process in the Bitcoin application are called miners. In consensus mechanism process, the transactions contained in a block are first verified and then the blocks are published.
- The Blockchain are decentralized systems, and provide safe and secure systems because transactions are encrypted before storage.

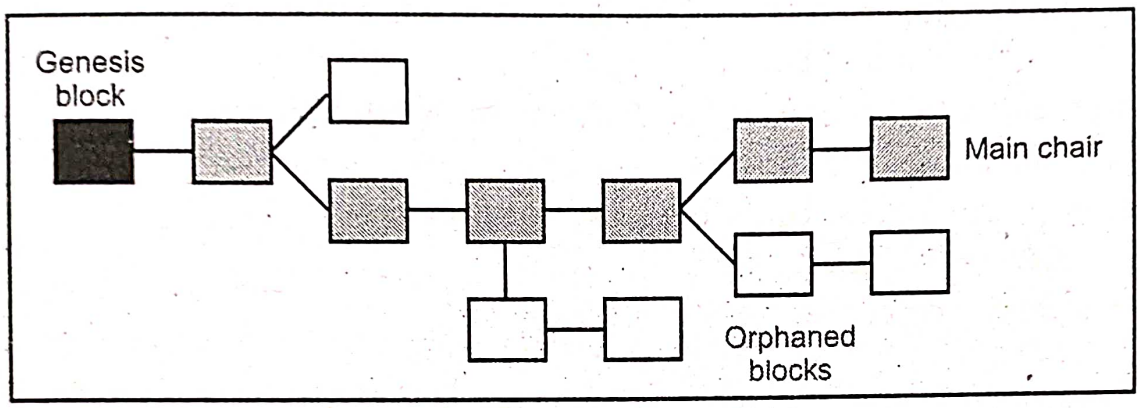


Fig. 1.6: Structure of Blockchain

Basic Terms used in Blockchain Technology:

1. **Block** is a data structure that stores/records a set of transactions that is then shared (distributed) among all nodes in the network. A block contains block header (metadata) and block data (list of validated and authentic transactions).
2. **Chain** is a term for a sequence of blocks arranged in a specific order.
3. **Transaction** refers to the smallest building block of a blockchain system, that is, the records and information stored in the block. Transactions in a Blockchain represents interaction between parties that is transfer the currency between two users. Each block in a blockchain can contain zero or more transactions; it consists of inputs and outputs, the inputs – assets that are to be 'transferred', and outputs – where the assets 'go'.
4. The cryptographic **hash functions** takes input data like text, image can be any size and returns outputs of a fixed size.
5. In Blockchain network used for **asymmetric-key cryptography** in secured systems. It consists of public key and private key of two pairs of key systems.
   The encryption key is public and decryption key is private key (anyone can encrypt the data, but decryption only done for intended receiver).
6. In Blockchain network, the **addresses** are used only once, using cryptographic hash function.
7. **Ledgers** is a collection of transactions, every user maintains their own copy of the ledger.

8. **Consensus** models determining the next block in the systems, verify and construct a valid block and add to chain, by computing a cryptographic block hash then generating new currency.
9. **A fork** (new branch of sequence of blocks) in Blockchain is to impart change in the previous version or divergence from the existing protocol of the Blockchain.
10. **Smart contracts** are the code and data deployed in the blockchain network.

Structure of Block in Blockchain:

- A Blockchain is comprised of a chronological (means every transaction happens after the previous one) chain of blocks.
- Blocks are the basic units of in the Blockchain. A block is a basic data structure in Blockchain for transaction distributed to other monetary control.
- The blocks in Blockchain contain a **block header** which verifies the validity of the block and **metadata** which describe the block.
- Fig. 1.7 shows structure of a block in Blockchain.

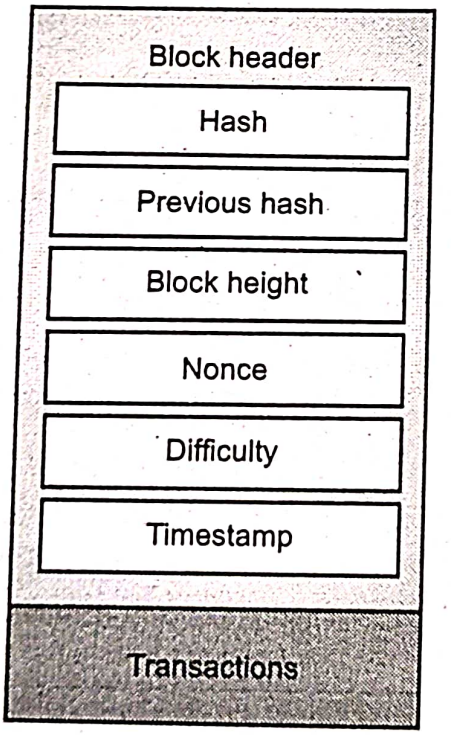


Fig. 1.7: Structure of Block in Blockchain

- A block in Blockchain consists mainly of the block header containing metadata and a list of transactions appended to the block header.
- The **block height** of a block is defined as the number of blocks preceding it in the Blockchain. It is calculated as the length of the blockchain minus one.
- A **nonce** is a random number the miners use to solve a mathematical puzzle in the mining process. A nonce is also known as Proof of Work (PoW).
- **Difficulty** in a block is a value that measures the degree of difficulty to find a hash value for a given target, which represents the difficulty of mining.

- A **timestamp** in a block is a sequence of characters or encoded information identifying when a certain event occurred, usually giving date and time of day. In **timestamping** each block is timestamped with each new block referring to the previous block using the cryptographic hash. Combined with cryptographic hashes, this time stamped chain of blocks provides an immutable record of all transactions in the blockchain.
- A **hash** (or hash value) is the result of a hash function. A hash function takes an input of any length, performs an algorithmic transformation and produces an alphanumeric value of a predetermined or fixed length. The purpose of the hash is for validation. Data on the Blockchain is "hashed" in each block and each block is linked with the previous block via the hash value.
- The **Merkle tree** also known as the hash tree. It encodes the Blockchain data in an efficient and secure manner. Every transaction occurring on the blockchain network is subjected to a hashing algorithm to produce a hash. The Merkle tree structure will enable the quick verification of Blockchain data and quick/fast moments of large amount of data from one computer node to the other on peer-to-peer Blockchain network. A Merkle root contains information about every single transaction hash that ever was on a particular block in a blockchain.

Working of Blockchain Technology:

- Fig. 1.8 shows an easier way to expalin working of Blockchain technology. In Fig. 1.8 person A, sending money to person B.
- Every transaction in Blockchain is represented as block, so when a person X sends money, the block is broadcasted to every node (peer) in the network.
- The block is always timestamped, so that users can verify the authority of the data. The hash value present in the block is very important information, when verifying transactions by nodes.
- Nodes can be any computers on the network participating in Blockchain. The nodes connects with each other in a P2P network and verify transaction.
- Nodes might be participating in Blockchain for various reasons and one important reason is mining, where the computers participating in blockchain solve a mathematical puzzle to participate in the transaction.
- If successful, they receive a share of the transaction. This process is called the Proof of Work (PoW), which can change depending on the technology used and vary from time to time.
- The nodes in Blockchain verify varied informaion contained in the block and make sure that the transaction is valid.
- The protocols used in PoW must be validated by each node. If the protocols are not met, then the transactions are denied by the node.

- Once, enough nodes approve the transaction, the transaction is then approved, and th block is added to the blockchain.
- The processing of a transaction might take from a few seconds to minutes or eve longer, depending on how the blockchain technology is set up.
- The hash value stored in each block is very important. In fact, it is critical, because thi is what helps maintain network security.
- In the digital currency world, when a hash is solved, it generates coins, so each computer participating in the blockchain network try to solve as many hashes a possible, so they can mine more currencies.
- But because of the proof of work, the balance of currencies mined in blockchain i maintained.

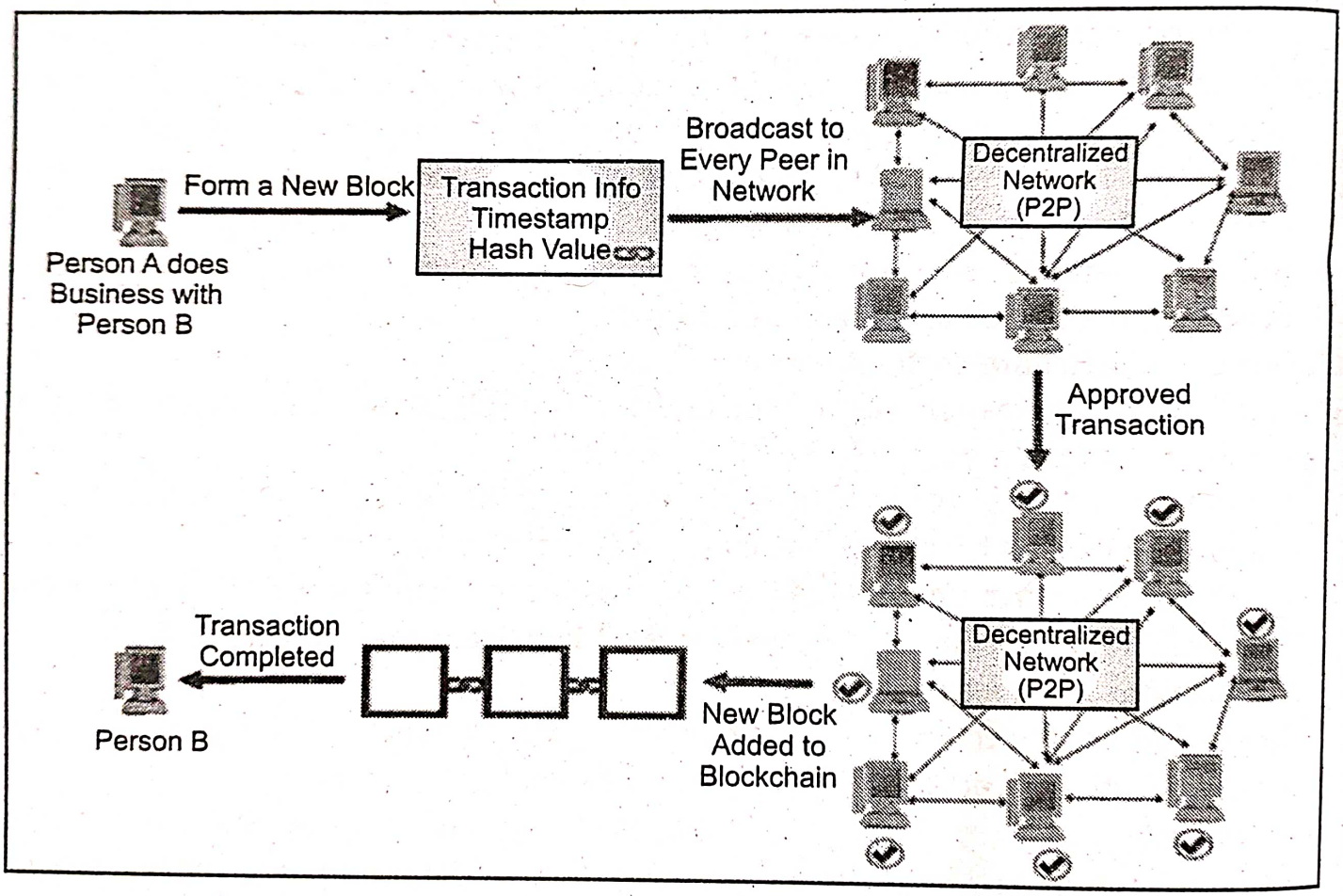


Fig. 1.8: Working of Blockchain Technology

1.4.1 Blockchain Generations

- Blockchain is commonly associated with Bitcoin and cryptocurrency and while that is a lot more to the technology than digital currency.
- To know and get and develop it, we are going through three blockchain generations. Fig. 1.9 shows generations of Blockchain.

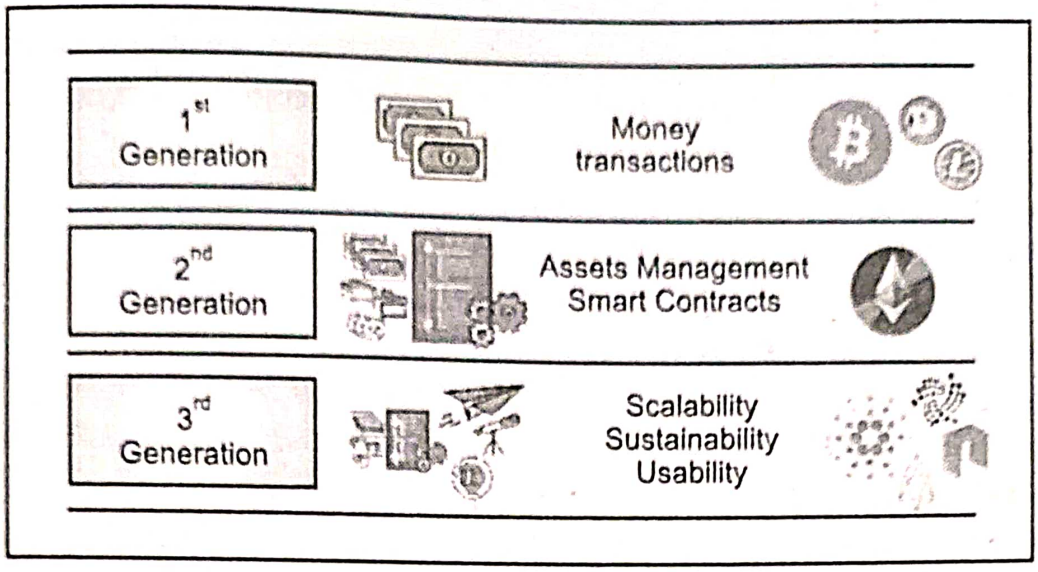


Fig. 1.9: Generations of Blockchain

- Let us see the three generations of Blockchain in detail.

First-Generation Blockchain: Bitcoin

- In the first generation, blockchain specifically Bitcoin was created which is a digital currency.
- By empowering people with the technology to perform with one another at a peer-to-peer level, they do not need to depend on centralized entities such as banks and any financial organization.
- Bitcoin and blockchain go together where, Bitcoin is the first real use case of blockchain technology and it is main purpose is as a financial application, any user can send Bill, digital money and there is security in that transaction.
- Bitcoin and blockchain both can strong privacy because the transaction is anonymous and they can take peace in knowing that the system is secure in the technology and the trust lies in the algorithm and not a centralized figure.

Second-Generation Blockchain: Ethereum

- In first generation of blockchain design allows, to send, receive and trade the transactions. But if any terms and conditions we want in our transactions. Bitcoin is simply can not server that, thus Ethereum introduced.
- Ethereum can be conduct two things, the innovative smart concept of smart contracts. These are very clever self-executing agreements made between two parties.
- A smart contract means that the parties involved draw up the conditions and once they are met, the contract triggers.
- For example, now Amar can deliver bill's of milk and when that is done, the digital payment will fire automatically.
- A smart contract is that it offers a faster, more secure way of executing agreements and it does not depend on an expensive intermediary to manage it because of decentralization.

- The ease of writing up a new cryptocurrency based on the Ethereum blockchain where developers could launch their own cryptocurrency project and applications which something was not as accessible before.
- Ethereum is actually behaves less like a cryptocurrency and more like an entire digital ecosystem that other cryptocurrency projects can operate on.
- It acts as a platform which developers can use to build on, like apps have iOS, Decentralized Apps (dApps) have Ethereum.
- Here, we get an impressive variety of functional uses including decentralized finance (DeFi), gaming, supply chain management, web browsing, identity management etc.

Third-Generation Blockchain: Cardano/Polkadot/Ethereum 2.0

- In first and second generation are exceptional in innovation, there are some fundamental growing problems.
- The main issue is that of scaling, basically, there are too many people trying to transaction and too little accessing space for it on the blockchain that it is the means "too many cooks and too little kitchen" problem.
- For example: As a startup, a company could get away with one birthday cake for the entire office. As the company grew, the number of people eating that cake increased, but the size of that one cake stayed the same. This means that more people are getting a smaller portion and they have to wait for it in a queue.
- Bitcoin scalability works the same, Bottle-necking problems emerge as too many people try to transaction at the same time. This means delays which is not sustainable for a financial system and high fees which present an obstacle for adoption, especially in developing countries.
- In Third generation blockchain applications are designed with this in mind and the technology automatically resolves issues of scaling if they emerge.
- Essentially, more cake is bought automatically when needed so that no one is waiting for their slice.
- Third generation blockchain applications are solve one more issue is interoperability.
- In the same way that we cannot charge an iPhone with a Samsung charger, the first iterations of the blockchain cannot interact with each other.
- The world relies on collaboration and systems where information and data can be shared across platforms is critical. Projects like Cardano and Polkadot introduced interoperability functions into their blockchain from the get go meaning they can work with other blockchains seamlessly.

1.4.2 Types of Blockchain

- There are four different major types of Blockchain technologies namely, Public Blockchain, Private Blockchain, Hybrid Blockchain, Consortium or Federated Blockchain.

- Fig. 1.10 shows types of Blockchain.

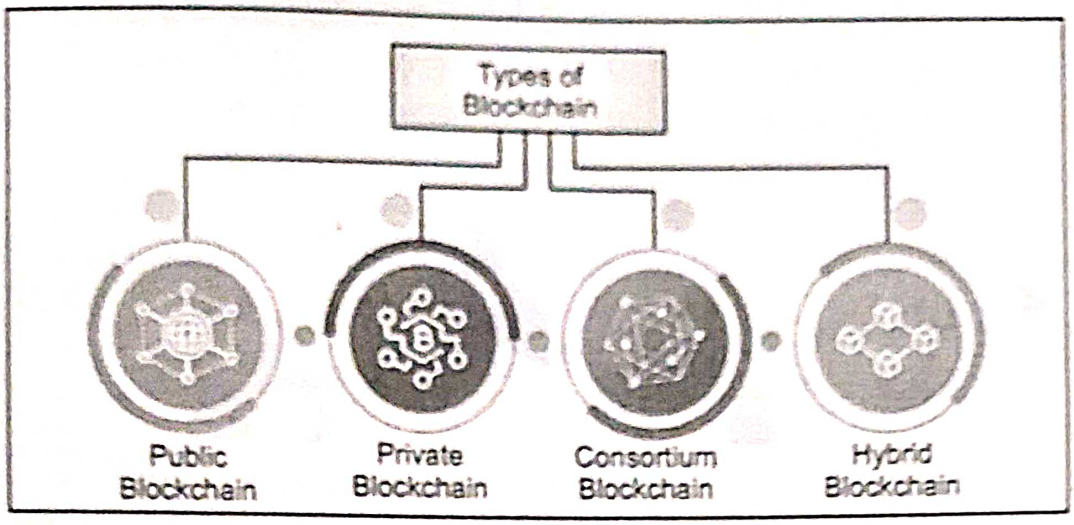


Fig. 1.10: Types of Blockchain

- Let us see various types of Blockchain networks in detail.

1. Public Blockchain:

- A public Blockchain is the permissionless distributed ledger technology where anyone can join and do their transactions.
- Public is a nonrestrictive version where each and every peer has a copy of the ledger. Also means that anyone can access the public Blockchain, if they have an internet connection to do transactions in a decentralized manner.
- In public Blockchain, the verification of the transactions is done through agreement methods such as Proof-of-Work (PoW), Proof-of-Stake (PoS), and so on.
- A user or node which is a part of the public Blockchain is authorized to access present ie current and past records, verify transactions or do proof-of-work for an incoming block, and do mining.
- Public Blockchains are basically used for mining and exchanging cryptocurrencies.
- Public Blockchains are primarily more secure if the users strictly follow security rules and methods. However, it is only unsafe when the participants do not follow the security protocols.
- **Example:** Bitcoin, Ethereum, Litecoin etc.

Advantages of Public Blockchain:

(i) Public Blockchains are good, however anyone can join the public blockchain.
(ii) It brings trust among the whole community of users.
(iii) Public Blockchain requires no intermediaries to work.
(iv) Public Blockchains are brings transparency to the whole network as the available data is available for verification purposes.

Disadvantages of Public Blockchain:

(i) Public Blockchain go through from a lack of transaction speed.
(ii) Public Blockchain is less scalability.

- **Use Cases of Public Blockchain:** The most common use case for public Blockchains is mining and exchanging cryptocurrencies like Bitcoin. However, it can also be used for creating a fixed record with an auditable chain of custody, such as electronic notarization of affidavits and public records of property ownership. The public Blockchain is ideal for organizations that are built on transparency and trust, such as social support groups or non-governmental organizations. Because of the public nature of the network, private businesses will likely want to steer clear.

2. **Private Blockchain:**

- A private Blockchain is a restrictive or limiting permission Blockchain operative only in a closed network.
- Private Blockchains are generally used within an companies and enterprises or organization where only selected ie authorize members are participants of a Blockchain network.
- Private Blockchains are similar in use as a public Blockchain but have a small and restrictive network because the private Blockchain have authorizations, level of security, accessibility, permissions is in the hands of the controlling organization.
- Private Blockchain networks are deployed for voting, supply chain management, digital identity, asset ownership etc.
- **Examples:** Multichain and Hyperledger projects (Fabric, Sawtooth), Corda, etc.

Advantages of Private Blockchain:

(i) There are less participants compared to the public Blockchain so the Private Blockchains are fast.

(ii) Private blockchains are more scalable, because, in a private Blockchain, only some nodes are authorized to validate transactions.

Disadvantages of Private Blockchain:

(i) Private Blockchains are not truly decentralized, this is disadvantages of private Blockchain so it goes against the fundamental, philosophy of distributed ledger technology or Blockchain in general.

(ii) Achieving trust is difficult in private Blockchain.

- **Use Cases of Private Blockchain:** The speed of private Blockchains makes them ideal for cases where the Blockchain needs to be cryptographically secure but the controlling entity doesn't want the information to be accessed by the public. Other use cases for private Blockchain include supply chain management, asset ownership and internal voting.

3. **Consortium Blockchain:**

- A consortium Blockchain is a semi decentralized type where more than one organization manages a Blockchain network.

- This is opposite to private Blockchain, where in which that is managed by only a single organization but in consortium Blockchain, more than one organization can act as a node and exchange information or do mining.
- Consortium Blockchains are typically used by government organization and banks etc.
- Examples of consortium Blockchain are; Energy Web Foundation, R3, etc.

Advantages of Consortium Blockchain:

(i) Consortium Blockchains are more secure and have better scalability.
(ii) Consortium offers better customizability and control over resources.
(iii) It is also more efficient compared to public blockchain networks.

Disadvantages of Consortium Blockchain:

(i) Consortium Blockchain is less transparent.
(ii) It is secure and also less anonymous compared to other types of Blockchain.
(iii) Regulations and restriction can have a more impact on network functionality.

- **Use Cases Consortium Blockchain:** Banking and payments are two uses for this type of Blockchain. Different banks can band together and form a consortium, deciding which nodes will validate the transactions. Research organizations can create a similar model, as can organizations that want to track food. It's ideal for supply chains, particularly food and medicine applications.

Public Blockchain vs. Private Blockchain vs. Consortium Blockchain:

Sr. No.	Public Blockchain	Private Blockchain	Consortium or Federated Blockchain
1.	Anyone can access set of nodes.	Not everyone can access a set of nodes.	Selected members can access a set of nodes.
2.	Not centralized.	Centralized.	Partial centralized.
3.	Low efficiency.	High efficiency.	High efficiency.
4.	Anyone can make transactions.	Not everyone can make transactions.	Selected members of the consortium can make transactions.
5.	Immutable.	Mutable.	Mutable.
6.	It is a permissionless block chain.	It is a permissioned block chain.	It is a permissioned block chain.
7.	Examples: Bitcoin, Ethereum, Litecoin etc.	Example: MONAX and Multichain.	Examples: EWF, r3.
8.	Low efficiency.	High efficiency.	High efficiency.
9.	Permissionless system.	Permissioned system.	Permissioned system.

4. **Hybrid Blockchain:**

- A hybrid Blockchain is a combination of the private and public Blockchain.
- Hybrid Blockchain uses the features of both types of Blockchains that is one can have a private permission based system and also a public permissionless system.
- A hybrid network, users or clients can control who gets access to which data stored in the blockchain, only where a selected section of data or records from the Blockchain can be allowed to go public keeping the rest as confidential in the private network.
- The hybrid system of Blockchain is flexible so that users can easily join a private Blockchain with multiple public Blockchains.
- A transaction in a private network of a hybrid Blockchain is usually verified within that network. But sometimes users can also release it in the public Blockchain to get verified.
- The public Blockchains increase the hashing and involve more nodes for verification. This enhances the security and transparency of the Blockchain network.
- In short, hybrid Blockchain means the combination of the two types of Blockchains i.e., private Blockchain and public Blockchain.
- By the combination of the best features of both public and private Blockchains, we can achieve more security and faster Blockchain solutions.
- Hybrid Blockchain architecture is entirely customizable. The hybrid Blockchain members can decide who can participate in the Blockchain or which transactions are made public.
- **Example:** Dragonchain, XinFin's Hybrid Blockchain etc.

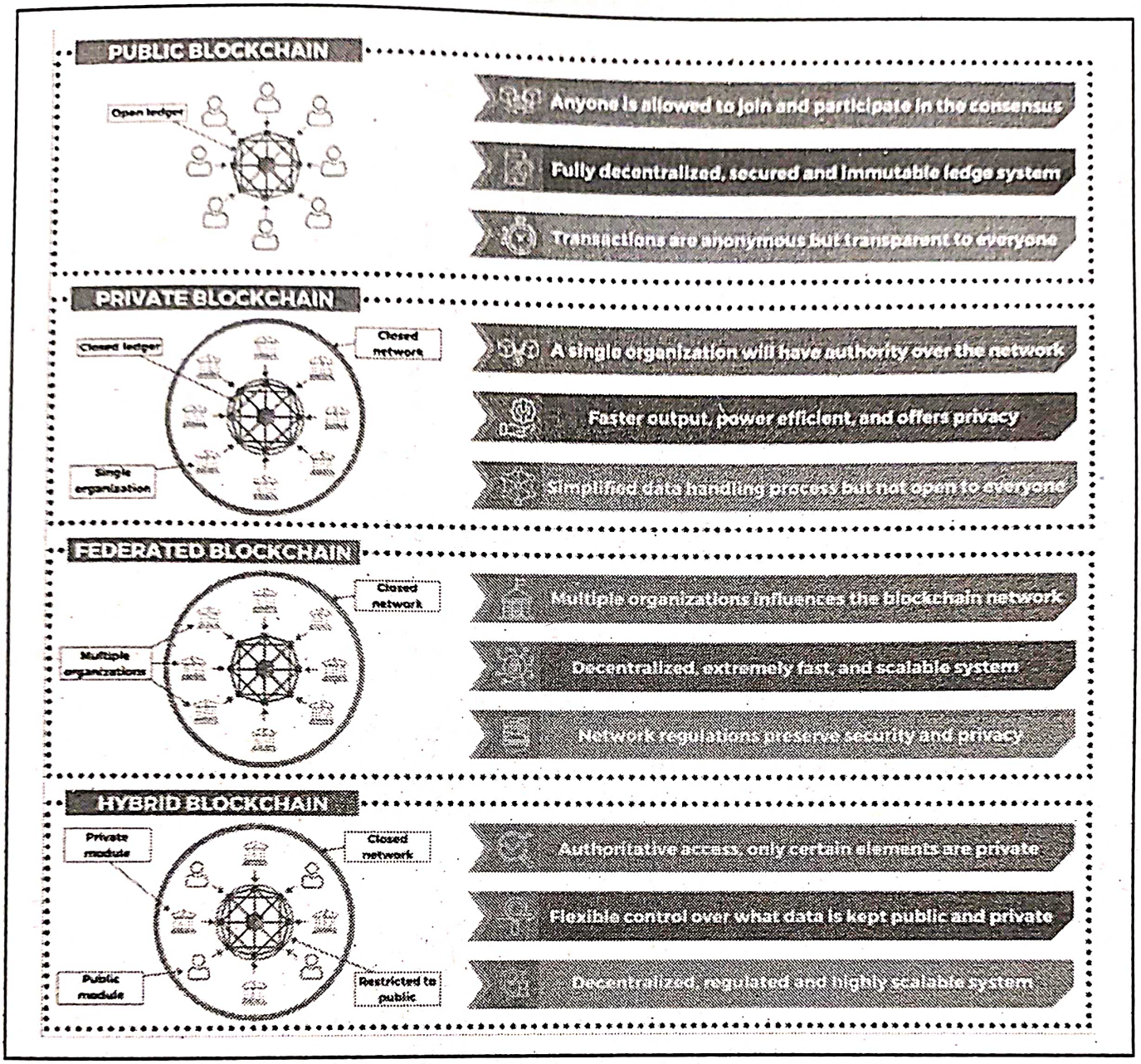
Advantages of Hybrid Blockchain:

(i) Rules can be changed according to the users needs.
(ii) Works in a closed ecosystem without the need to make everything public.
(iii) Hybrid offers good scalability compared to the public network.
(iv) Hybrid networks are also immune to 51% attacks.

Disadvantages of Hybrid Blockchain:

(i) Upgrading to the hybrid Blockchain can be a challenge.
(ii) Not completely transparent.

- **Use Cases of Hybrid Blockchain:** Hybrid Blockchain has several strong use cases, including real estate. Companies/organizations can use a hybrid Blockchain to run systems privately but show certain information, such as listings, to the public. Retail can also streamline its processes with hybrid Blockchain, and highly regulated markets like financial services can also see benefits from using it. Governments could also use it to store citizen data privately but share the information securely between institutions.



1.4.3 Benefits and Limitations of Blockchain

- The benefits of Blockchain technology are given below:
  1. **Digital Freedom and Decentralization**: The entire Blockchain network is a decentralized one as it gives every user its digital freedom. There is no central authority that controls all the other users in the network. Every node is independent in functioning.
  2. **New-age Technology Integrations:** Blockchain provides the universal infrastructure which is flexible to integrate with all sorts of old as well as new technologies. It has various applications in the domains of voting, banking, commodity trading, supply chain management, etc. In addition to this, the concept of blockchain, smart contracts, and distributed ledger system works perfectly well for the Internet of Things (IoT).

3. **Anonymity and Privacy:** The Blockchain network has tight security techniques for the transactions to take place securely. For users that use Blockchain for cryptocurrencies like Bitcoin, can do so anonymously (without revealing their real identity) keeping their privacy and security ensured.
4. **Security:** Blockchain technology is highly secured. The security method in the Blockchain is cryptography that ensures that hackers cannot change or tamper with the data records stored in the blocks of the Blockchain. Encrypted hash functions link all the blocks in the Blockchain and so it is impossible to do fraud or illegitimate transactions in the Blockchain network.
5. **No Intermediaries:** Due to the point-to-point nature of the Blockchain network, transactions take place directly between two nodes without a mediator. There is no need for an intermediary like Paypal, any bank, Visa, WesternUnion, etc. to facilitate transactions between two parties.
6. **Immutable Data:** One cannot change a data record or information that is once stored or added as a block in the Blockchain. The data in the Blockchain is immutable that is no one can make changes in it and it gets a permanent place in the Blockchain.
7. **Transparency:** The digital distributed ledger system provides a great deal of transparency to all those who are a part of the network. Each node in a network has its own copy of the ledger and has the right to verify transactions. Due to this, no one can hide their details and transactions from the other users ensuring fair trade.
8. **Low Transaction Cost:** As there are no intermediaries in a transaction within the Blockchain network, the transaction costs are also lowered. Transactions of millions of dollars can happen for around $1.00 or even less. If there are intermediaries involved, then they charge a heavy amount and your overall transaction cost increases.
9. **Consensus-Based:** The Blockchain concept is entirely consensus-based, that is, for every transaction that takes place between two nodes in a Blockchain, a request for its verification is sent to all the other nodes. After all the nodes verify a transaction, it goes into the memory pool to make a new block. The memory pool stores numerous such verified transactions.
10. **Faster Processing:** Blockchain technology speed of the transaction increased to a very high extent. Before this, the overall banking process takes around two to three days to resolve but after the introduction of Blockchain, the time reduced to nearly minutes or even seconds.
11. **Transparency and Trust:** As Blockchains are shared and everyone can see what is on the blockchain, this allows the system to be transparent and as a result trust is established.

- The limitations of Blockchain technology are given below:
  1. **Higher Costs:** The underlying cost of implementing Blockchain technology is huge. The transactions cost is also high.
  2. **Scalability:** Blockchains are not scalable as their counterpart centralized system. The transactions in Blockchain are completed depending on the network congestion means, the more people or nodes join the network, the chances of slowing down is more.
  3. **Immutable:** In Blockchain one cannot make any modifications/updations to any of the records. The data once written in a block cannot be removed or erased.
  4. **Private Keys:** To access the assets or the information stored by the user in the Blockchain, they need private keys. If a user who forgets its private key in Blockchain are eventually logged out of their wallet and no one can get it back.
  5. **Expertise Knowledge:** Implementing and managing a blockchain project is hard. It requires thorough knowledge from the business to go through the whole process.
  6. **Interoperability:** There are multiple types of Blockchain networks which work differently, trying to solve the problem in their own unique way which leads to interoperability issues where these chains are not able to communicate effectively.

1.4.4 Challenges of Blockchain

- Fig. 1.11 shows major challenges of Blockchain technology.
- The major hurdles are not just technical toward the adoption of Blockchain technology. There are also lack of standards and regulations.
- Blockchain requires thousands of hours of human manpower and money for design of software and back-end programming which is needed for integration of Blockchain to existing business networks.

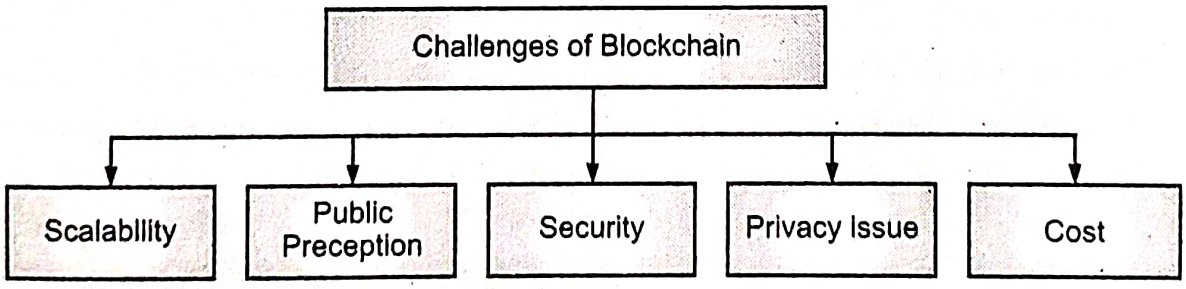


Fig. 1.11: Challenges of Blockchain Technology

- Major challenges which come in the way of acceptance of Blockchain technology are discussed below:

1. **Scalability:**

- Blockchains are having trouble effectively supporting a large number of users on the network. There is need to increase capacity of Blockchain.

2. **Public Perception:**

- Perception, Blockchain holds in the eyes of people is the biggest drawback in the way of its success.
  - People have not accepted it as a part of mainstream functioning.
  - Numbers of the people are sceptical about the longevity of this technology.
- The lack of governance and regulation, easy access to become a member of public Blockchain adds to the deterioration of image of Blockchain in the eyes of people. All these factors are the hurdles for the growth of Blockchain technology.

3. **Security:**

- The Blockchain maintains confidentiality to protect users from hackers and hence provides privacy. But the Blockchain network can be used for illegal activities and trade purposes.
- Users who make online transactions using Blockchain are not given Blockchain networks and newer cryptocurrencies are prone to 51% attacks.

4. **Cost:**

- The Blockchain technology does not come free. To validate transactions, Bitcoin uses the "Proof of Work (PoW)" system.
- The Bitcoin requires appreciable amount of computational power to validate transactions. This energy is far from free and costs money.

5. **Privacy:**

- The Bitcoin Blockchain is designed to be publicly visible. All the information pertaining to a transaction is available for anyone to view.
- While this feature may be important in some contexts, it becomes a liability if distributed ledgers are to be used in sensitive environments. For example, government data or financial data.

1.4.5 Applications/Usages of Blockchain

- Some common fields which use Blockchain technology includes:

1. **Banking:** Blockchain distributed-ledger architecture has the potential to enhance security, speed, and operational efficiency for banks in several business areas such as payments, asset management, loyalty, and loans.
2. **Cloud Storage:** Blockchain cloud storage allow for decentralised storage and for that reason are less prone to attacks which will cause systemic harm and extensive data loss.
3. **Voting:** Elections need authentication of voter identity, preservation of secure records to monitor votes and confidence counts to decide the winner. Blockchain tools could function as an integrated infrastructure for casting, tracking and counting votes, potentially reducing the need for counts by taking electoral fraud and dirty play off the table.

4. **Supply Chain Management:** With Blockchain, as products change hands in a supply chain from manufacturing to sales, transactions can be documented in a permanent decentralized register, which reduces delays, additional costs and human errors.
5. **Cryptocurrency:** Blockchain technology acts as the backbone of cryptocurrency systems like Bitcoin. Cryptocurrency is an encrypted digital currency that everyone can use as a medium of exchange in transactions.
6. **Healthcare:** With the help of blockchaining, we can store information about patients and drugs in a database securely. Doctors can access patient records and history to analyze a case better at a given point to ensure proper treatment.
7. **Smart Contracts:** Smart contracts in Blockchains are digital, self-executable contracts recorded and stored in a Blockchain once created. A smart contract is a programmed file containing all the terms and conditions of a contract between two parties and it automatically executes itself once all the conditions are met. This gives a 100% guarantee and prevents the deal from any fraud.
8. **Internet of Things (IoT):** Blockchain and smart contracts can prove to be useful for the implementation and workings if IoT systems. A smart contract can store software, sensors and other important details that will take care of the proper functioning of the electronic device and the network.
9. **Digital Identity Management:** With the digital revolution, the risks of fraud have also gone up significantly. More and more incidents of cybercrime and digital fraud are surfacing. This is due to easily hackable digital identities of people that hackers can use to do fraud and theft. To ensure the security of digital identities of people, Blockchain is the best solution.

1.5 TYPES OF NETWORKS

- A Blockchain network is a technical infrastructure that provides ledger and smart contract (chain-code) services to applications.
- A Blockchain is a decentralized ledger of all transactions across a peer-to-peer (P2P) network.
- Using Blockchain technology, participants can confirm transactions without a need for a central clearing authority.
- The Blockchain network is a peer-to-peer decentralized network. The peers (also known as nodes) are connected to this network in a synchronous way.
- The nodes can be a desktop, a laptop, a mobile phone, a mining rig, servers, or any other electronic devices. These nodes form the foundation of the Blockchain network.
- Nodes in Blockchain network views al the transactions processed. They provide computing resources like disk storage space to keep the network alive and to maintain its integrity and security, and they do so voluntarily.

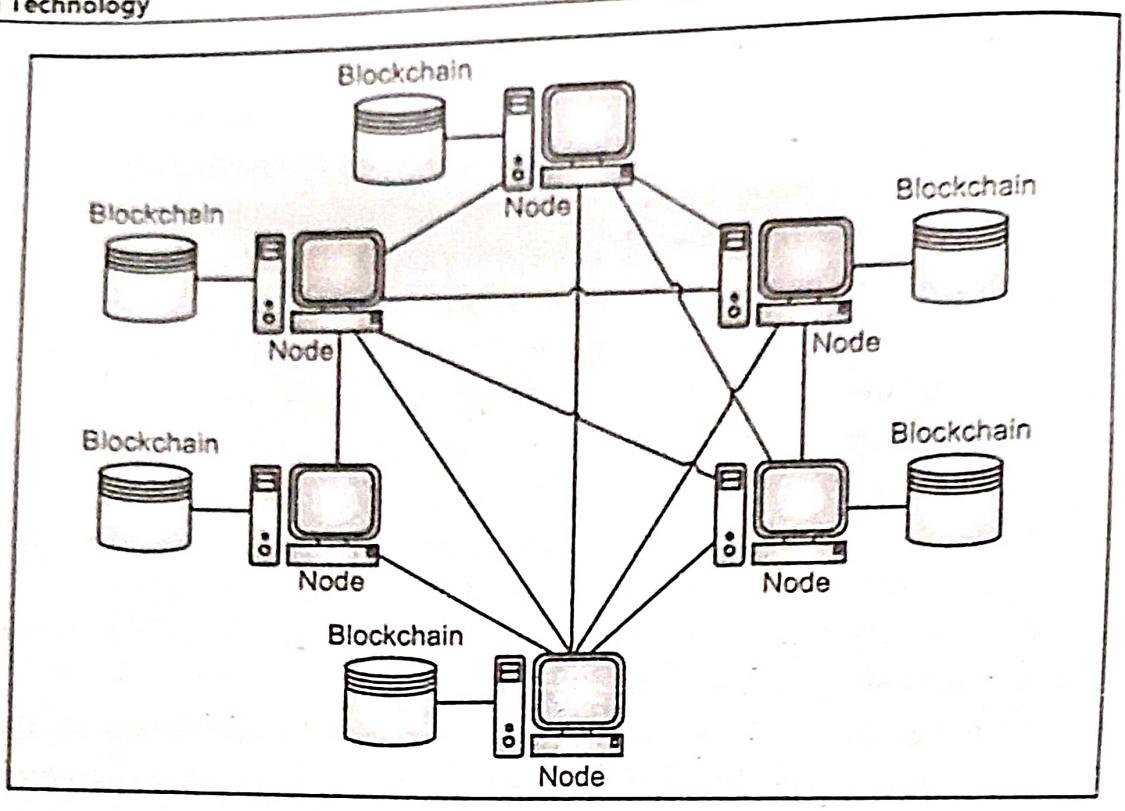


Fig. 1.12: Blockchain P2P Network

- Blockchain is an encrypted repository of digital information. A Blockchain has decentralized and distributed style of network of computers.
- Hence, its hosting on a distributed network of systems allows secure transactions occur across a Blockchain with little possibility of fraudulent activities.
- A Blockchain is a decentralized ledger of all transactions across a peer-to-pe network.
- Blockchain is a decentralized, immutable, and transparent distributed ledger t maintains a list of transaction records arranged in blocks in order.
- Every Blockchain consists of a cluster of nodes functioning on a peer-to-peer (P2 network system.
- There are four main types of Blockchain networks, each of which is suitable different purposes explained below:

1. **Public Blockchain Network:**

- As the name suggests, public Blockchains are accessible to and managed by t public. A public Blockchain is a very inclusive type of Blockchain network, which open for participation by any machine or node. Anyone can join and participate in t public Blockchain.
- The public Blockchain does not require permission and does not have a single contr server, every transaction is public and users can remain anonymous, so it is a ve reliable type of Blockchain.
- This type of Blockchain is highly democratic and transparent because every node h equal access to data on the network.

- The capacity of a public Blockchain is limited to the number of participating computers and individual capacity.
- The Bitcoin, Ethereum, Litecoin, etc. are examples of a public blockchain. Fig. 1.13 shows public Blockchain network.

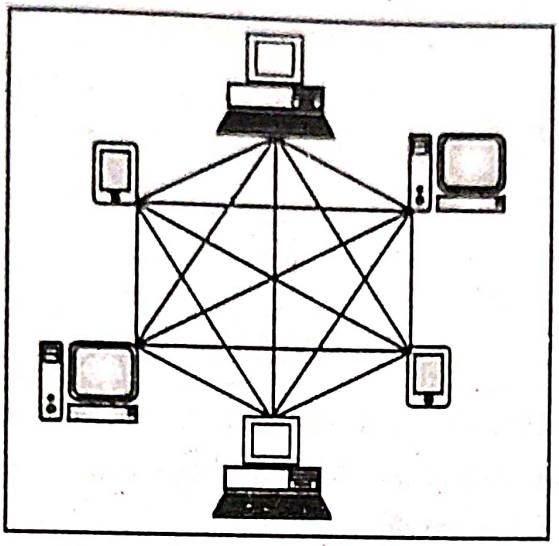


Fig. 1.13: Public Blockchain Network (an open network system where all the devices can freely access without any kind of permission. The ledger is shared and transparent.)

2. Private Blockchain Network:

- A private Blockchain is a network restricted to invited users and controlled by a single enterprise, which determines who can read the Blockchain, send transactions to the Blockchain, and participate in the consensus process.
- Users who join the private Blockchain network need permission to read write or review the Blockchain.
- Therefore, there are different levels of access rights and information can be encrypted to protect business secrets.
- Compared to public Blockchains that require a lot of time and resources to verify transactions, private Blockchains are faster, more effective, and more cost-effective.
- With the help of a private Blockchain, organizations can adopt distributed ledger technology without disclosing data. But this means that the technology lacks an important feature of Blockchain i.e, decentralization.
- However, this kind of Blockchain is completely centralized, so it is only suitable for use as a sandbox environment and cannot be used in actual production.
- Some critics believe that a private Blockchain is not a blockchain at all, but a centralized database using distributed ledger technology.
- The Multichain and Hyperledger projects (Fabric, Sawtooth), Corda, Quorum etc. are examples of private Blockchains.
- Fig. 1.14 shows private Blockchain network.

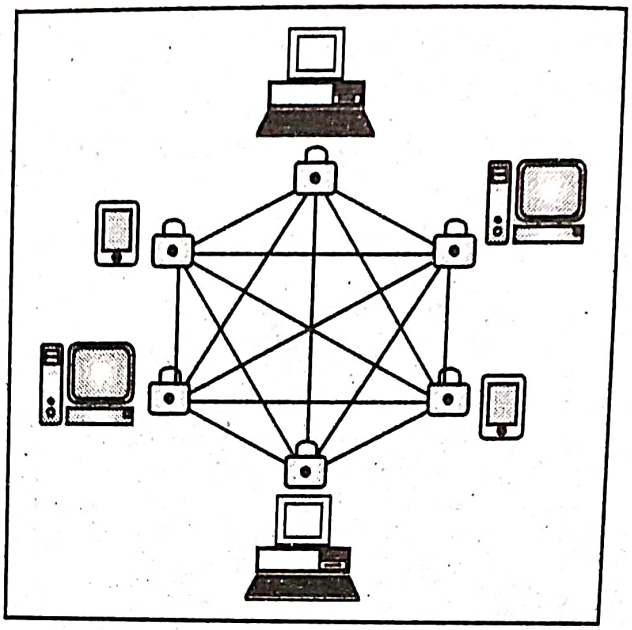


Fig. 1.14: Private Blockchain Network (a user has to be permitted by the Blockchain author before he/she could access the network. The user might join only if he/she gets an invitatio

3. Consortium Blockchain Network:

- A consortium Blockchain is a type of semi-decentralized Blockchain network but i permissioned too.
- Multiple companies/organizations or multiple individuals combine together to oper the node in a network.
- These groups are known as a consortium or federation and their combined natu helps in making decisions for the benefit of the entire network.
- A Consortium Blockchain or Federated Blockchain is a partially private Blockcha where instead of only a single organization, multiple organizations govern t platform.
- Companies/organizations that build private Blockchains will usually build consortium Blockchain network.
- Multiple organizations can share the responsibility of maintaining the Blockchai These pre-selected organizations determine who can submit transactions or acce data.
- When all participants need to obtain permission and share responsibility for th Blockchain, the consortium Blockchain is ideal for business.
- The Blockchain consortium provides many of the same benefits of the privat Blockchain (efficiency, transaction privacy, etc.), without consolidating power wit just one party.
- The Energy Web Foundation, R3, etc. are examples of consortium Blockchain.
- Fig. 1.15 shows the consortium Blockchain network.

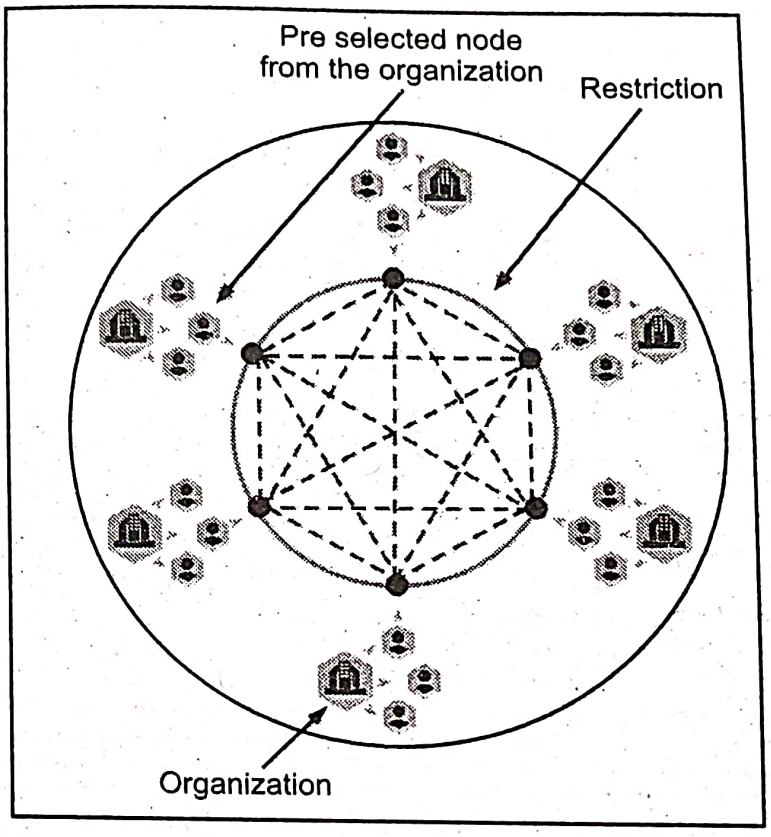


Fig. 1.15

4. **Hybrid Blockchain Network:**

- Hybrid Blockchain refers to a combination of the public and private Blockchains. Hybrid Blockchains is a type of Blockchain combines the strong features of both private and public Blockchains.
- The best way to describe hybrid Blockchain is using a public Blockchain where a private network is hosted.
- Hybrid Blockchain is a Blockchain network that consist the features of public and private Blockchain networks.
- A hybrid Blockchain network uses the features of both public and private Blockchains where, one can own a private permission-based system as well as a public permission-less system.
- The Blockchain hybrid system is flexible so that users can easily join a private Blockchain with multiple public Blockchains and can control who access to the data has stored in the Blockchain.
- Public and authorized Blockchains interoperate using the same easy-to-use smart contract language.
- The Dragonchain, IBM Food Trust™, etc are examples of a hybrid Blockchain.
- Fig. 1.16 shows the consortium Blockchain network.

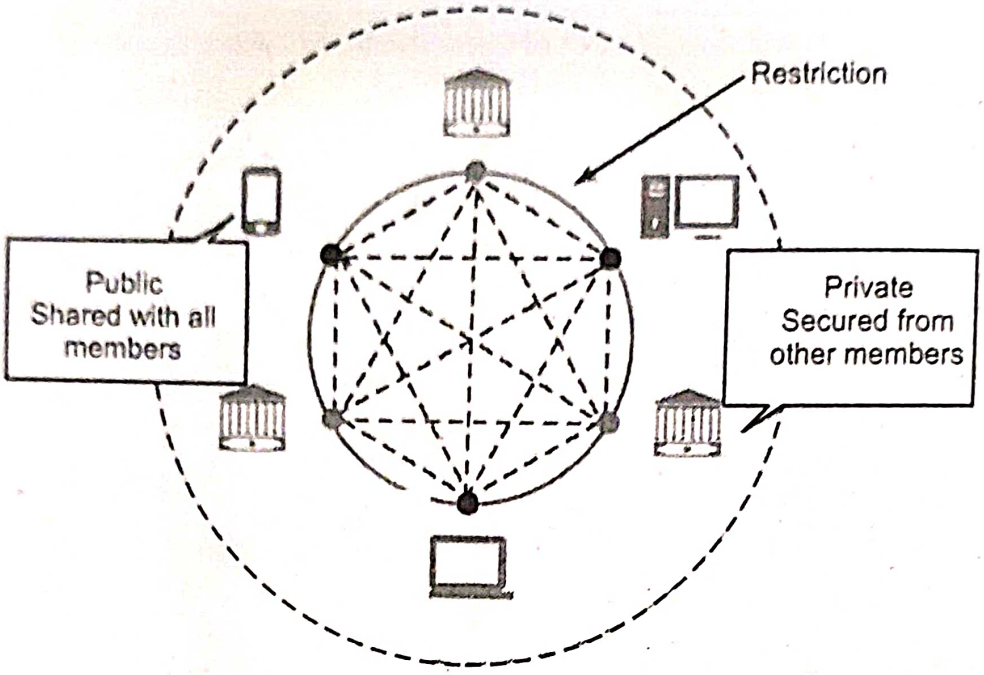


Fig. 1.16

1.6 LAYERED ARCHITECTURE OF BLOCKCHAIN ECOSYSTEM

- Blockchain ecosystem, we mean a group of elements that interact with each other t create an environment with special features.
- Ecosystems that use blockchain technology consist of a set of distributed nodes wher immutable transactions are replicated.
- The blockchain (or digital ledger) technology is built upon a layered architecture a shown in Fig. 1.17.
- The different layers of the blockchain technology include Hardware/Infrastructure layer, Data layer, Network layer, Consensus layer and Application and Presentation layer.

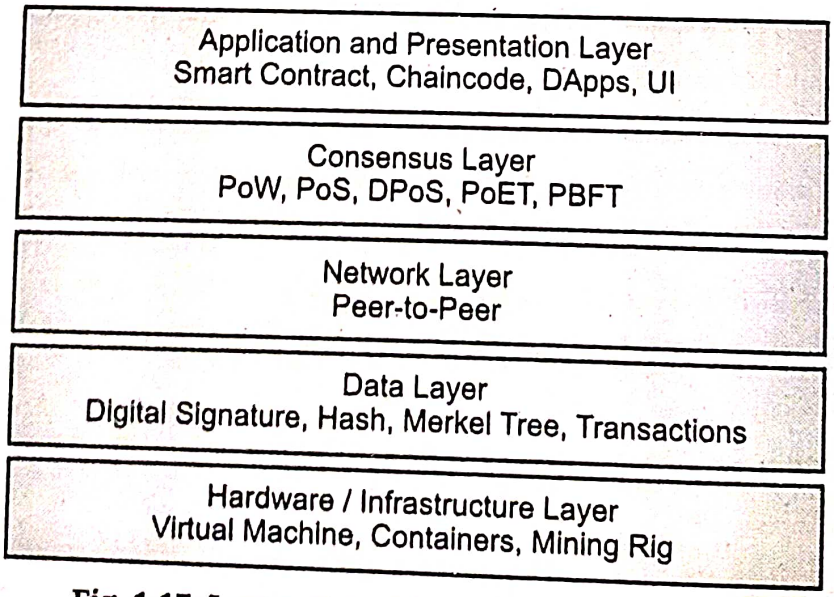


Fig. 1.17: Layered Architecture of Blockchain

- The Blochchain layers are explained below:

1. **Hardware or Infrastructure Layer:**

- The first layer of the Blockchain is the hardware or infrastructure layer. In the Blockchain the content is hosted in a server that resides in a data center.
- While browsing the web or using applications clients request data or content from application servers, commonly referred to as client-server architecture.
- Blockchain technology generally based on the Peer-to-Peer (P2P) network of computers that computes transactions, validates and stores them in an ordered form in a shared ledger.
- This results in a distributed database that records all the data, transactions and various relevant information.
- Computer in a Peer-to-Peer network is known as node. Nodes are accountable for validating transactions, organizing them into blocks, broadcasting them to the Blockchain network, and it keeps on.
- Reaching agreement, the nodes commit the block to the Blockchain network and update their local ledger copy. When a device gets connected to a Blockchain network then it is termed and used as a node.

2. **Data Layer:**

- Data structures of a Blockchain are represented as a linked list includes two primary elements i.e., pointers and a linked list of blocks where transactions are ordered.
- Pointers are the variable that refers to the location of another variable and linked list is a list of chained blocks where each block has data and pointers to the previous block.
- Merkle tree is a binary tree of hashes, in each block contains the hash of the Merkle root with information such as the hash of the previous block, timestamp, nonce, the block version number, and the current difficulty target.
- A Merkle tree provides security, integrity and irrefutability for the Blockchain technology.
- A hash tree or Merkle tree is a tree in which every leaf node is labeled with the cryptographic hash of a data block, and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes.
- Fig. 1.18 shows the connected list of blocks present in a Blockchain.

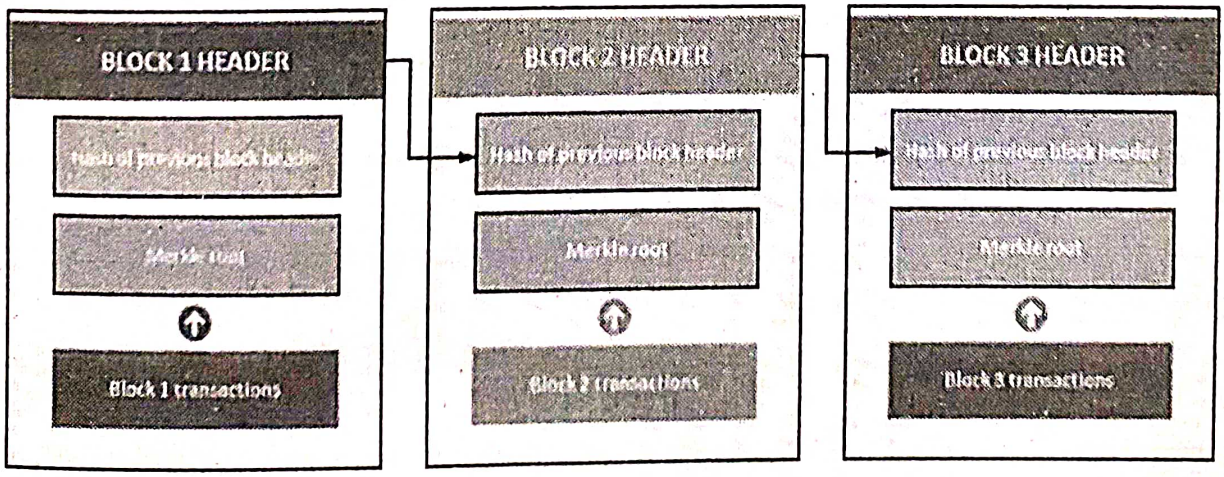


Fig. 1.18

- Transactions are digitally signed in Blockchain to assure that the integrity and secur and of the data stored into it.
- Transactions are signed using a private key and anyone having the public key c verify the signer.
- The digital signature checks for tampering of information, and also guarantee unity the data that is encrypted is also signed.
- As the data is encrypted it cannot be detected. Also a digital signature secures senders or owners identity as well.
- Data layer is responsible for the structure of the block in the Blockchain, (s Fig. 1.18).

3. **Network Layer:**

- The network layer is also known as the Peer-To-Peer (P2P) layer. It is the one that responsible for inter-node communication and also called propagation layer.
- Network layer takes care of block propagation, transactions, and discovery.
- Network layer ensures that nodes can reveal each other and able to communica synchronize and propagate with each other to maintain valid current state of t blockchain network.
- Peer-to-peer network is a computer network, where nodes are distributed and sha the networks workload to reach the end goal also nodes perform transactions in t blockchain.
- There are two kinds of nodes i.e full node and light node. Full nodes guarantee t validation and verification of transactions, enforcement of consensus rules ar mining. Whereas, Light nodes only keep the header of the Blockchain and can ser transactions.

4. **Consensus Layer:**

- The consensus layer is the essential to the existence of Blockchain platforms. Th consensus layer is the most crucial and critical layer for any Blockchain be Ethereum, Hyperledger or any other.
- Consensus layer is responsible for validating the blocks, ordering the blocks an ensuring everyone agrees on it.
- Consensus layer create a definite set of agreements between nodes across th distributed Peer-to-peer network.
- Consensus layer ensures that power remains distributed and decentralized.

5. ***Application Layer:***

- Application layer is divided into two sub layers i.e application layer and execution layer.
- Application layer comprise of the applications that are used by end users to interact with the Blockchain network.

- The application layer comprised of smart contracts, chaincode and dApps, scripts, APIs, user interfaces and frameworks. For these applications blockchain network is the back-end system and they connect with blockchain network via APIs.
- Execution layer is the sublayer which consists of chain code, smart contracts and underlying rules.
- A transaction travels from application layer to execution layer however the transaction is validated and executed at the semantic layer.
- Applications send instructions to execution layer which ensure the deterministic nature of the Blockchain and performs the execution of transactions.

1.7 COMPONENTS OF BLOCKCHAIN

- To understand Blockchain technology applications deeply it is necessary to understand the logical components of a Blockchain ecosystem and the duties of each component.
- Fig. 1.19 shows logical components of a Blockchain.

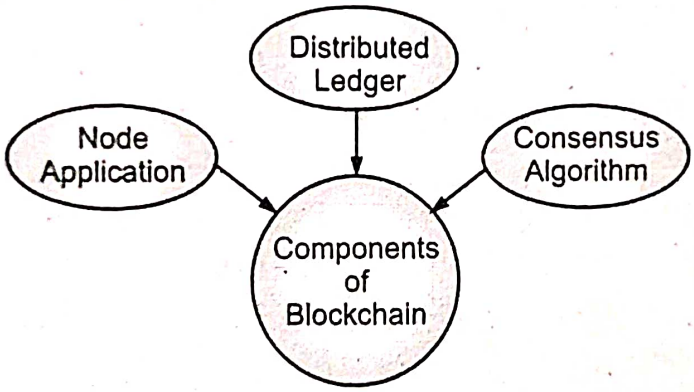


Fig. 1.19

- The main components (logical) of any Blockchain ecosystem are given below:

1. **Node Application:**

- A node application specify that every computer, connected to the internet, if its wants to participate in.
- Examples of node application are bitcoin wallet application and bankchain application.
- Node application not free from any restrictions, for example, in case of a Bankchain as a Blockchain ecosystem, only banks are allowed to participate.

2. **Distributed/Shared Ledger (Database):**

- The distributed ledger means the shared databases and contents accessible to the participants of a particular Blockchain system.
- The shared ledger lists down the rules or guidelines that need to be followed, for example if we are running a Bitcoin node application, then we have to follow by all the rules set down in the program code of the Bitcoin node application.

- The application layer comprised of smart contracts, chaincode and dApps, scripts, APIs, user interfaces and frameworks. For these applications blockchain network is the back-end system and they connect with blockchain network via APIs.
- Execution layer is the sublayer which consists of chain code, smart contracts and underlying rules.
- A transaction travels from application layer to execution layer however the transaction is validated and executed at the semantic layer.
- Applications send instructions to execution layer which ensure the deterministic nature of the Blockchain and performs the execution of transactions.

1.7 COMPONENTS OF BLOCKCHAIN

- To understand Blockchain technology applications deeply it is necessary to understand the logical components of a Blockchain ecosystem and the duties of each component.
- Fig. 1.19 shows logical components of a Blockchain.

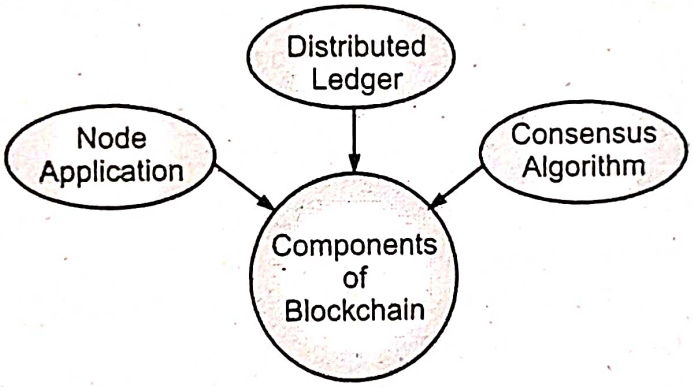


Fig. 1.19

- The main components (logical) of any Blockchain ecosystem are given below:

1. **Node Application:**

- A node application specify that every computer, connected to the internet, if its wants to participate in.
- Examples of node application are bitcoin wallet application and bankchain application.
- Node application not free from any restrictions, for example, in case of a Bankchain as a Blockchain ecosystem, only banks are allowed to participate.

2. **Distributed/Shared Ledger (Database):**

- The distributed ledger means the shared databases and contents accessible to the participants of a particular Blockchain system.
- The shared ledger lists down the rules or guidelines that need to be followed, for example if we are running a Bitcoin node application, then we have to follow by all the rules set down in the program code of the Bitcoin node application.

3. **Consensus Algorithm:**

- Consensus algorithms are one of major components of a Blockchain system and they play a vital role in the Blockchain performance and security.
- The consensus algorithm provides stability and security to the data in the Blockchain. It is represent the status of the network and how the nodes in the network arrive at an agreement regarding what transactions to accept.
- Also, what protection used the Blockchain from tampering is the fact that changing a block can be done only by making a new block from its predecessor and it also requires regenerating all successors and redoing their contents.
- It is to be noted that every block in the Blockchain contains a hash of its predecessor block, thus having a chain of blocks with enormous amount of work contained in them.
- Example, the time taken by Bitcoin to ensure a agreement of the ledger is a few minutes while that of ripple is only a few seconds.

Core Components of Blockchain Architecture:

1. **Transaction** is the smallest building block of a Blockchain system (records, information, etc.) that serves as the purpose of the Blockchain.
2. **Block** is a data structure used for keeping a set of transactions which is distributed to all nodes in the network.
3. **Chain** is a sequence of blocks in a specific order.
4. **Node** is a user or computer within the Blockchain architecture (each has an independent copy of the whole Blockchain ledger).
5. **Consensus** (or consensus protocol or consensus algorithm) is a set of rules and arrangements to carry out Blockchain operations.
6. **Miners** are the specific nodes which perform the block verification process before adding anything to the Blockchain structure.

1.8 CRYPTOGRAPHY

- Cryptography is an essential for Blockchain technology. The role of cryptography in Blockchain in terms of maintaining the trust and eliminating intermediates.
- The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.
- Cryptography is made up of two ancient greek terms, Kryptos and Graphein, the former term meaning "hidden" and latter being "to write".
- Cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible form (called ciphertext).
- Decryption is the reverse, moving from the unintelligible ciphertext back to plaintext. A cipher (or cypher) is a pair of algorithms that carry out the encryption and the reversing decryption.

- The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a "key". A key is a small amount of information that is required to induce the output of the cryptographic algorithm.
- The key is a secret (ideally known only to the communicants), usually a string of characters, which is needed to decrypt the ciphertext.
- Fig. 1.20 shows concept of cryptography.

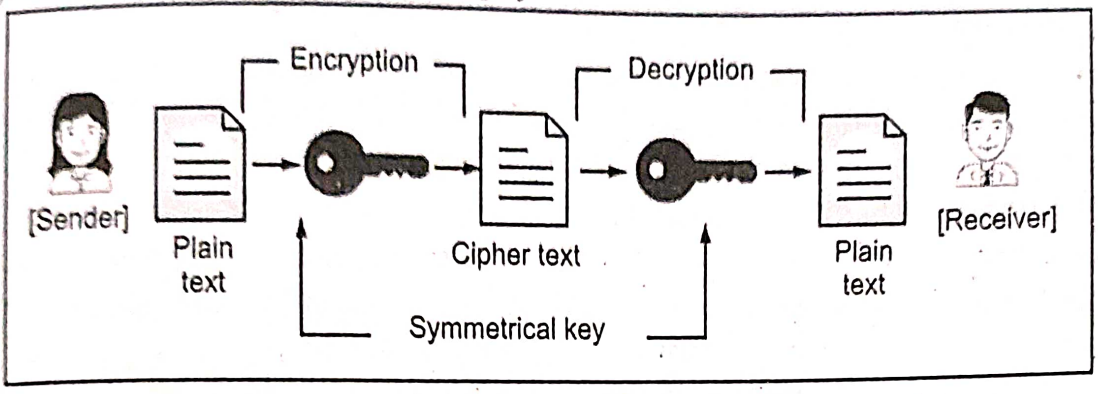


Fig. 1.20: Concept of Cryptography

Terminology in Cryptography:

1. **Plaintext** refers to the original unencrypted message that the sender wishes to send.
2. **Ciphertext** refers to the encrypted message that is received by the receiver.
3. A **key** is usually a number or a set of numbers on which the cipher operates. Encryption and decryption algorithms make use of a key to encrypt to decrypt messages, respectively.
4. The encryption and decryption algorithms are together known as **ciphers.** The ciphers need not necessarily be unique for each communicating pair; rather a single cipher can be used for communication between multiple pairs of senders and receivers.
5. **Encryption** is the process of encrypting the plaintext so that the ciphertext can be produced. Plaintext is transformed into ciphertext using the encryption algorithm.
6. **Decryption** is the reverse of the encryption process. In this process, the ciphertext is converted back to the plaintext (original) using a decryption algorithm.

- Blockchain Cryptography assumes that generated codes or making written that enable info to be unbroken secret.
- Cryptography in Blockchain converts information into a format that is unreadable for the associate user without authorization. Transmit it while entities with authorization decipher it back to a cleared or well defined format, therefore compromising the information.
- Cryptography is widely related to the disciplines of cryptanalysis and cryptology. Cryptography includes techniques equivalent to merging words with pictures, microdots and different ways in which to cover information in storage or transport.

- However, in today's computer world, cryptography is most frequently related to scrambling plaintext i.e. ordinary text, generally stated as cleartext into ciphertext ie a method known as encryption, then back once more is known as decryption.
- Modern Cryptography in Blockchain has following objectives or goals which are:
  - **Data confidentiality** assures that private or confidential information is not made available or disclosed to unauthorized users. It is sometimes referred to as privacy or secrecy.
  - **Data integrity** assures that information and programs are changed only in a specified and authorized manner. Integrity confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user.
  - **Availability** ensuring timely and reliable access to and use of information.
  - **Non-repudiation** is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party.
  - **Authentication** ensures to the receiver that the data received has been sent only by an identified and verified sender.
- To understand cryptography in Blockchain, one has to understand the types of cryptography. The two types of cryptography are symmetric-key cryptography and asymmetric key cryptography.

Symmetric Key Cryptography:

- Symmetric cryptography is a 'simple' form of cryptography which uses a single key to encrypt and decrypt data.
- This key can be almost anything, ranging from a number to a word to a random string of characters. This key is then used to encrypt the data after which the data can get sent across a network safely.
- To decrypt the data the receiver needs the key (the same one that the sender used to encrypt the data).

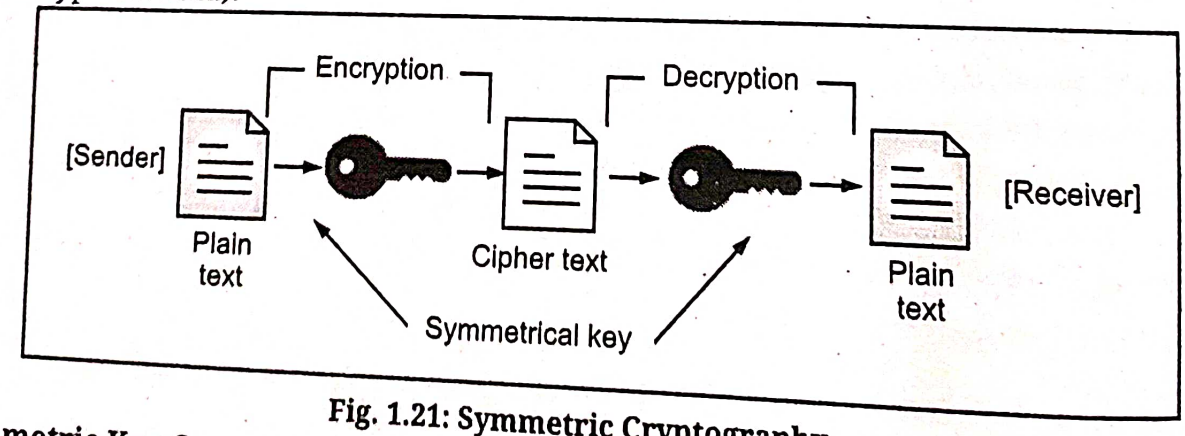


Fig. 1.21: Symmetric Cryptography

Asymmetric Key Cryptography:

- Blockchain mainly uses asymmetric cryptography, also known as public-key cryptography.
- Public key cryptography uses the keys in pair, a public and private key. Asymmetric cryptography uses these key-pairs in order to encrypt and decrypt data.

- The public key is for encryption that can be distributed commonly, but the private key is not meant to share with anyone.
- Public key cryptography is mostly used between two users or two servers in a secure way.

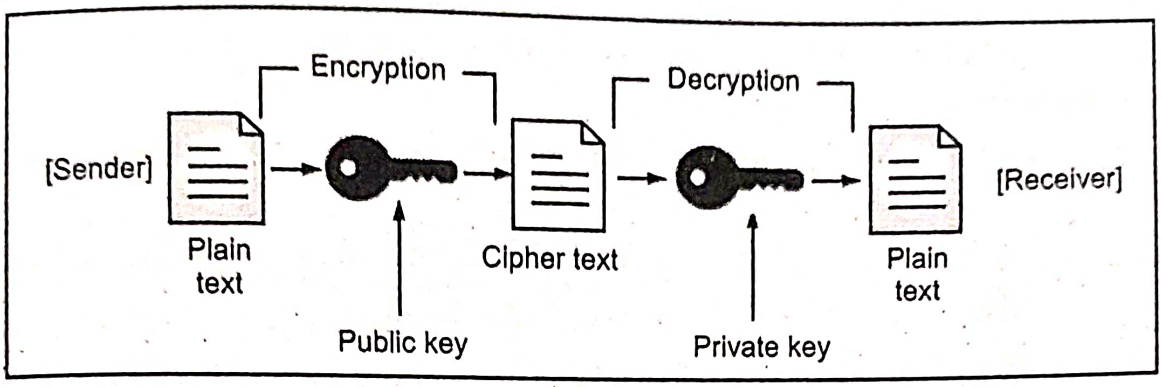


Fig. 1.22: Asymmetric Key Cryptography

1.8.1 Private and Public Keys

- Cryptography is a practice of technique to ensure security by using the cryptography keys. A key is used to encrypt or decrypt data.
- A key in cryptography is a piece of information, usually a string of numbers or letters that are stored in a file, which, when processed through a cryptographic algorithm, can encode or decode cryptographic data. Based on the used method, the key can be different sizes and varieties.
- A cryptographic key scrambles numbers and letters so they're unreadable by humans. Private keys and public key are the cryptographic keys used in Blockchain.
- Public keys, by their nature, are designed to be public and do not need to be protected. They can be freely given to anyone or even posted on the Internet. The private key must be kept confidential and never shared.
- In simple words, a private key always kept secret whereas a public key can be shared publically.

1.8.2 Hashing

- Hashing plays a very important role in cryptography. Hashing refers to the concept of taking an arbitrary amount of input data, applying some algorithm to it, and generating a fixed-size output data called the hash.
- The data is mapped to a fixed size using hashing. In a Blockchain network hash value of one transaction is the input of another transaction.
- Hashing is a cryptographic technique which simply converts a data of any size into a unique fixed size output. The input can be a text, file or image and the output is fixed size alpha-numeric string.

- Hashing in Blockchain assures the users that the data transmitted is not changed. This can be done by comparing the hash values of the input data.
- Most of the Blockchain implementation uses Secure Hash Algorithm (SHA) that generates an output of size 256-bits.
- SHA-256 hashing algorithm produces an output of 32 bytes (256-bits) usually displayed as 64 hexadecimal characters.
- Other than SHA-256, Keccak and RIPEMD-60 are some other hashing algorithms used in Blockchain network.
- Hashing techniques are used for various operations in Blockchain such as address creation, securing block data and block header etc.

Concept/Working of Hashing:

- Fig. 1.23 shows concept of hashing. Hashing is a technique to convert any function that can be used to map data of arbitrary size to data of fixed size.
- The function which is used to perform this computation is called a hash function. When a user sends a message to another user over a network, a hash of the intended message is generated and encrypted by using a hash function, and is sent along with the message.
- The result of the hash is known as a digest or hash. When the message (digest) is received, the receiver decrypts the hash as well as the message.
- Then, the receiver creates another hash from the message. If the two hashes (received and created) are identical when compared, then it can be said that a secure transmission has occurred and the message has been correctly received.
- Good hashing is achieved by following requirements:
  1. It should be easy to compute.
  2. The uniform distribution should be provided across the hash table.
  3. Collisions should be avoided.
- Hashing process ensures that the message is not altered/modified by an unauthorized user.

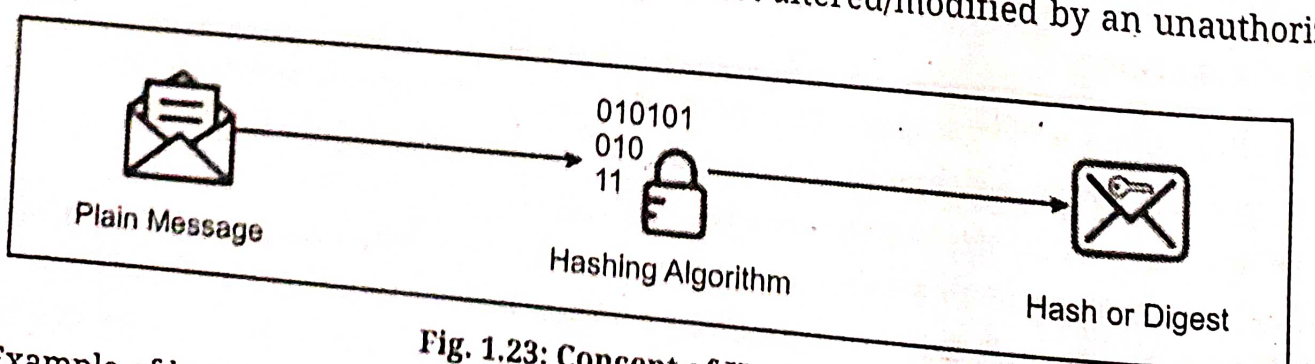
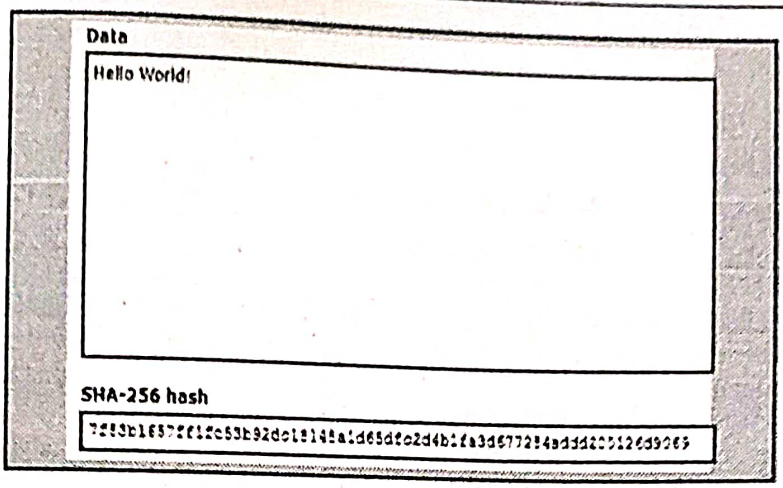


Fig. 1.23: Concept of Hashing

Example of hashing using SHA-256. Hashing means taking a string of variable size and converting it into an output of fixed length.



- Let us see an example by creating the hash function in Python programming. First, open Python IDLE then, type the following. Don't ignore the tab.

```
import hashlib
def hash(mystring):
    hash_object = hashlib.md5(mystring .enco de())
print(hash_object.hexdigest())
```

- We have now created a function, hash(), which will calculate and print out the hash value for a given string using the MD5 hashing algorithm. To run it, put a string in between the parentheses in quotation marks. For example:

```
hash("AnyString")
```

- After that, press ENTER to see the hash digest of that string. We will see that calling the hash function on the same string will always generate the same hash, but adding or changing one character will generate a completely different hash value:

```
hash("AnyString") => 7ae26e64679abd1e66cfe1e9b93a9e85
hash("AnyString!") => 6b1f6fde5ae60b2fe1bfe50677434c88
```

1.8.3 Digital Signature

- Signatures generated on the Blockchain are referred as digital. Digital signatures are an initial building block in Blockchains, they are in the first place used to verify the authenticity of transactions.
- Digital signature is a particular type of electronic signature that encrypts the signed document.
- Digital signature is a digital code which included with an electronically transmitted document, with this digital code we can verify first of all whether the content of the document is authenticated or not.
- Digital signatures are used in Blockchain where the transactions are digitally signed by senders using their private key before broadcasting the transaction to the network.
- A digital signature is generated using asymmetric cryptography, which is more secure than handwritten signatures that can be easily forged.
- A digital signature is used to prove that a message originates from a specific individual and not from someone else.

- Fig. 1.23 shows concept of digital signature. Digital signatures are incorruptible a easily verifiable thanks to their usage of asymmetric cryptography.
- Since, they use asymmetric cryptography (and a private key is only linked to a sin person) digital signatures also have the quality of non-repudiation, meaning they c be as legally binding as a normal signature.

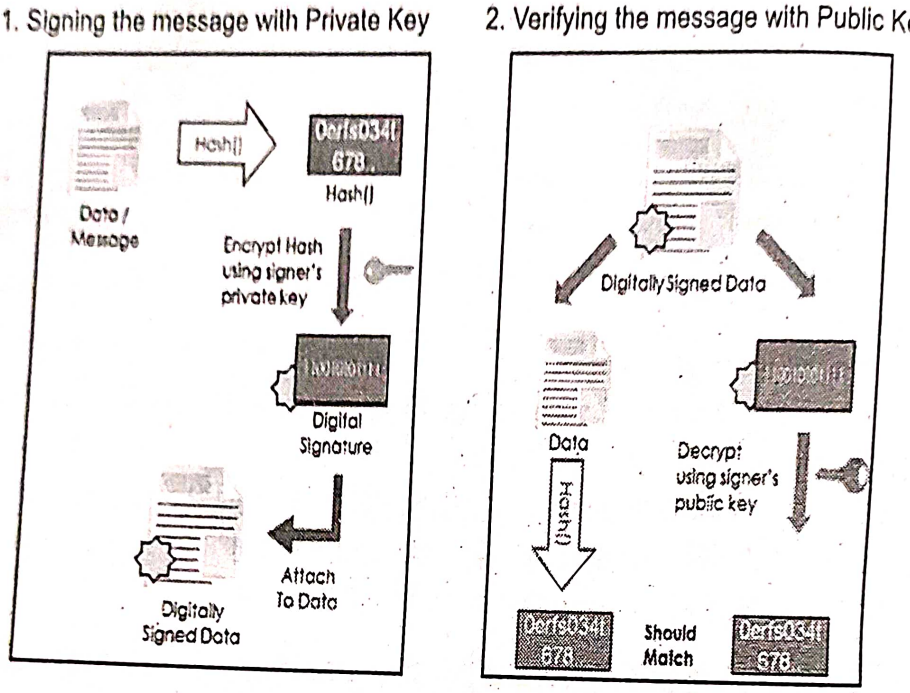


Fig. 1.24

How Digital Signatures Work?

- A digital signature presenting the authenticity of digital messages or documents. A digital signature is a cryptographic analogue of a handwritten signature to validate the authenticity integrity and non-repudiation of a message or documents transferred over a digital medium.
- A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).
- A digital signature scheme is generally used by a signer who generates a pair of private and public keys followed by publicizing his or her public key so that we can assume the verifier will have it or can obtain it at the time of verification.
- Once the public key of a signer is established, the digital signature scheme allows the signer to sign or certify the message in such a way that any other party knowing the signer's public key and the corresponding algorithm can verify that it is originated from the signer and nobody modified it in the middle.
- Fig. 1.25 shows an example of working of digital signature. In Fig. 1.25 Amar wants to send a message to Yogita using an RSA-based digital signature.

- Amar needs to go through the following steps:

Step 1: Amar generates a hash value of the message.

Step 2: Amar encrypts the hash value using his private key. The encrypted hash value can only be decrypted by his public key; hence it acts as his signature.

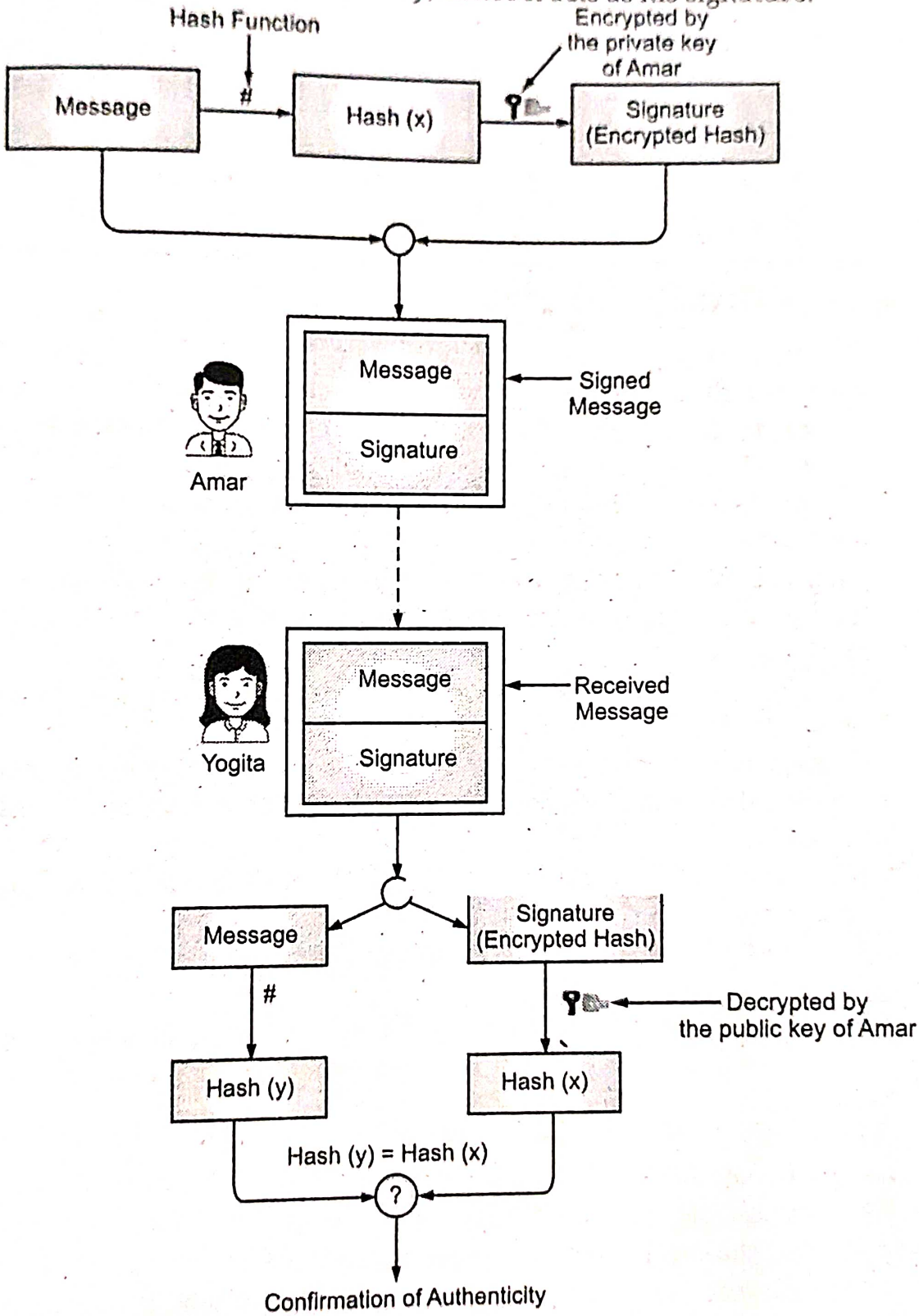


Fig. 1.25: Processing Steps in Digital Signature

Step 3: Amar attaches his signature at the bottom of the original message and sends it to Yogita using a digital communication medium.

Step 4: Having received the message, Yogita performs two tasks: first, she decryp Amar's signature using his public key to obtain the hash value, and, secon she creates a hash value for the original message sent.

Step 5: By comparing two hash values, Yogita can confirm the authenticity of t message. It is because if someone in the middle changes the message, the ne hash value will be different than that of stored in Amar's signature. Due this signature being encrypted, the man in the middle would not be able change it, or any modification attempt would result in a damaged signatur that cannot be decrypted using the public of key of Bob anymore revealin the alteration.

1.9 CONSENSUS MECHANISMS

- Consensus mechanisms (also known as consensus protocols or consensus algorithms allow distributed systems (networks of computers) to work together and stay secure.
- Consensus ensures the correct set of operations in the presence of trustless individual in a distributed environment.
- The properties of reliability and fault tolerance of a network are determined with consensus mechanisms.
- Each and every participating node agrees on a common content-updating protocol for their public ledger to maintain a consistent state, this is known as a consensus mechanism.
- Upon reaching consensus among the nodes the blocks are created and added to the existing ledger for later usage.
- Consensus mechanism are standard protocols that give a guarantee that all nodes are synchronized and checked along with the miner to confirm the transaction is included in blocks.
- The consensus protocols differ with different Blockchain networks. There are three core consensus techniques including:
  1. **Proof of Work (PoW)** which is the initial Blockchain consensus mechanism and was first used by Bitcoin.
  2. **Proof of Stake (PoS)** which solves the lag of computing power in PoW. This consensus protocol is more environmentally friendly and is a randomized process used to determine who will produce the next block.
  3. **Byzantine Fault Tolerant (BFT)** protocols that instrument a three-phase commit scheme for Blockchain enlargement.
- Blockchain being a distributed system requires its nodes to reach a consensus while running the system and keeping its data secure.
- A consensus mechanism is nothing but a fault-tolerant mechanism that is used in computer and Blockchain systems to achieve the necessary agreement on a single data value or a single state of the network through distributed processes or multi-agent systems, such as with cryptocurrencies.

- A consensus mechanism mention to any number of techniques, which used to accomplish agreement, security and trust, across a decentralized computer network.
- Consensus mechanism is helpful in record keeping, among other things.
- For instance, in the Bitcoin Blockchain, the consensus mechanism is known as Proof-of-Work (PoW), which essential the exertion of computational power in order to solve a difficult but arbitrary puzzle in order to keep all nodes in the network trustworthy.
- Proof of work (PoW) is the initial consensus protocol used for cryptocurrency that permits the Blockchain users to obtain consensus in Bitcoin.
- Proof of Work (PoW) is the original consensus algorithm in a blockchain network. The algorithm is used to confirm the transaction and creates a new block to the chain.
- In this algorithm, minors (a group of people) compete against each other to complete the transaction on the network. The process of competing against each other is called mining.
- As soon as miners successfully created a valid block, gets rewarded. The most famous application of Proof of Work (PoW) is Bitcoin.
- Another most popular consensus mechanism in blockchainsis Proof-Of-Stake (PoS). PoS protocols are a class of consensus mechanisms for blockchains that work by selecting validators in proportion to their quantity of holdings in the associated cryptocurrency.
- Unlike a proof of work (PoW) protocol, PoS systems do not incentivize extreme amounts of energy consumption. The first functioning use of PoS for cryptocurrency was Peercoin in 2012. The biggest PoS blockchain by "market cap" is Cardano.
- PoS is a type of consensus mechanism used by blockchain networks to achieve distributed consensus.

1.10 CRYPTOCURRENCY

- Cryptocurrency is a digital currency that works on the decentralized concept and uses encryption techniques to verify the transactions, maintain the historical records of the entire transactions and generate new units of currency without the necessity of a central regulatory body to oversee the process.
- It follows the peer-to-peer electronic transfer approach by using cryptography to secure its transaction, has control over new coin generation and verifies transfers made in the cryptocurrency network.
- A cryptocurrency is a digital currency and is classified as a subset of alternative currencies and virtual currencies.
- Cryptocurrency in its purest form is a peer-to-peer version of electronic cash. It allows online payments to be sent directly from one party to another without going through a financial institution.

- Cryptocurrency quite literally means "cryptographic currency" i.e., currency ba upon cryptographic technology.
- Cryptocurrencies are decentralized digital currencies that are backed up Blockchain technology.
- A cryptocurrency is a digital or virtual currency that is secured by cryptograph cryptocurrency (or "crypto") is a digital currency that can be used with an on ledger with strong cryptography to secure online transactions.
- An example of a cryptocurrency is Bitcoins. Satoshi Nakamoto published a pape the Web in 2008 for a peer-to-peer electronic cash system.
- Blockchain may be a form of technology and design for information storage whe Bitcoin may be a cryptocurrency that uses Blockchain technology. The transaction Bitcoin carry on a distributed, public ledger referred to as the Blockchain.
- Ethereum is a technology that makes use of the Blockchain development that undergirded most cryptocurrencies in the past several years.
- Ether (ETH) is the cryptocurrency of the Ethereum technology. Ether is the wor second-largest virtual currency by market capitalization as of 2021; it is second onl Bitcoin (BTC), according to market value.
- Fig. 1.26 shows how the cryptocurrencies works.

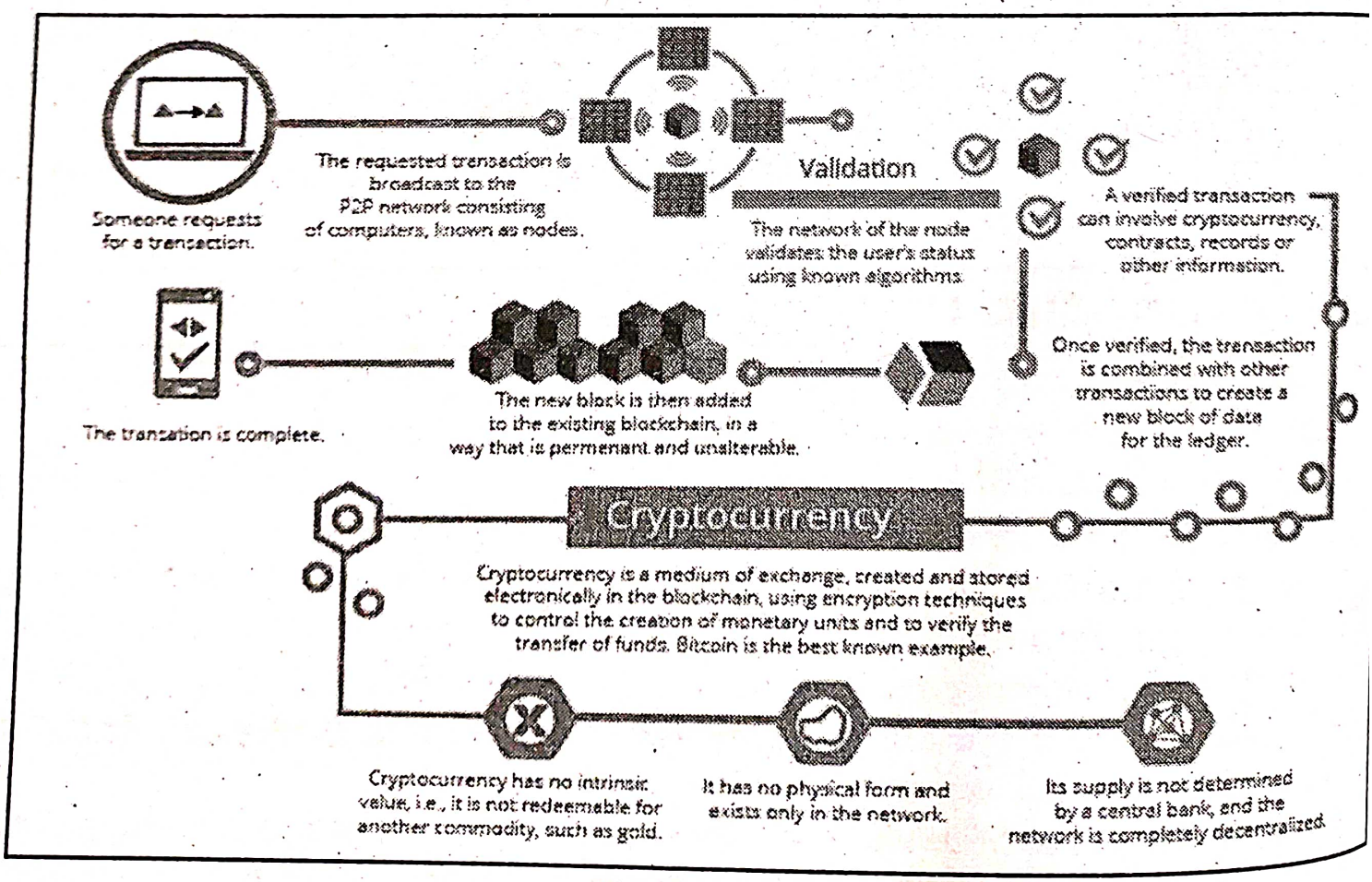
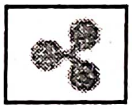


Fig. 1.26: Working of Cryptocurrency

- Popular and famous cryptocurrencies around the world given in following table:

Sr. No.	Name	Logo
1.	Ethereum	
2.	Bitcoin	
3.	NEM	
4.	Litecoin	
5.	NEO	
6.	Monero	
7.	Ripple	
8.	Dash	
9.	Vertcoin	
10.	Bytecoin	

1.10.1 Digital Currency Bitcoin

- A currency is a system of money (monetary units) in common use, especially for people in a nation/country. Under this definition, U.S. dollars (US$), euros (€), Indian rupee (₹), Japanese yen (¥), and pounds sterling (£).
- Digital currency has arisen with the popularity of computers and the Internet. Digital currency (digital money, electronic money or electronic currency) is any currency, money or money-like asset that is primarily managed, stored or exchanged on digital computer systems, especially over the Internet.
- Bitcoin is an open-source International currency and also the first cryptocurrency. The very first decentralized digital currency.

- Bitcoin is a digital money which means it does not exist in the physical form completely or even in digital form. Bitcoin is an open source international currency and also the first cryptocurrency.
- Bitcoin is the first P2P cryptocurrency that permits two participants to exchange their payments without any third-party intervention.
- Bitcoin (₿) is a decentralized digital currency, without a central bank or single administrator, that can be sent from user to user on the peer-to-peer Bitcoin network without the need for intermediaries.
- Transactions in Bitcoin are verified by network nodes through cryptography and recorded in a public distributed ledger called a Blockchain.
- The cryptocurrency was invented in 2008 by an unknown person or group of people using the name Satoshi Nakamoto. The currency began use in 2009 when its implementation was released as open-source software.
- Bitcoins are created as a reward for a process known as mining. They can be exchanged for other currencies, products, and services,[10] but the real-world value of the coins is extremely volatile.
- Bitcoin is a decentralized network and a digital currency that uses a peer-to-peer system to verify and process transactions.

1.10.2 Digital Currency Ethereum

- Ethereum was invented in 2013 by programmer Vitalik Buterin. Ethereum is a decentralized, open-source Blockchain with smart contract functionality.
- Ethereum, like Bitcoin, is a public ledger based on Blockchain technology. Ether (ETH) is the native cryptocurrency of the platform; among cryptocurrencies, it is second only to Bitcoin in market capitalization.
- Ethereum is a Blockchain platform with its own cryptocurrency, called Ether (ETH) or Ethereum, and its own programming language, known as Solidity.
- The world of cryptocurrencies and Blockchains in general, has developed and evolved extraordinarily since the launch of Bitcoin almost a decade go.
- The Ethereum network, a decentralized platform, represents an entirely new type of Blockchain that could potentially change the world and is one of the most talked about digital currencies today.
- Ethereum is an open source decentralized platform which is based on Blockchain Technology which enables developers to build DApps (Decentralized Applications) to run smart contracts.
- Ethereum is as an open software platform based on Blockchain technology that allows developers to create and deploy distributed applications. Like Bitcoin, Ethereum is a distributed public Blockchain network.

- In the Ethereum blockchain, so-called Ether (ETH), a cryptocurrency that drives the network, are earned for providing computing power ("mining").
- Ether (ETH) is the cryptocurrency generated by the Ethereum protocol as a reward to miners in a proof-of-work system for adding blocks to the blockchain. It is the only currency accepted in the payment of transaction fees, which also go to miners.
- Ethereum authorize engineers to convey and assemble decentralized applications, a decentralized application (DApps) to fill enough or specific need to its users or clients.
- For instance, Bitcoin, is a DApp that gives it's clients a shared electronic money framework that empowers online Bitcoin installments, since an application that is not centralized comprise of code that keeps on running on a blockchain arrange, which cannot control by any focal substance or individual.
- Golem and Augur are some of the most successful Ethereum based DApps.
- Ethereum can likewise utilize to construct Decentralized Autonomous Organizations (DAO/). The DAO's control by programming code, on an accumulation of know the contracts, produce on the Ethereum blockchain.

1.11 SMART CONTRACTS

- Smart contracts assist we exchange cash, property, shares, or something important in a very clear, conflict-free means whereas avoiding the services of a middleman.
- Smart contracts are translations of an agreement consisting of terms and conditions into a computational code, which is script.
- The developers write the script in a programming language like Java, C++, etc. in such a way that it lacks ambiguity and does not lead to interpretation.
- Smart contracts are self executing contracts containing the terms and conditions of an agreement among associate.
- The smart contract executes on the Ethereum Blockchains decentralized platform and its terms and conditions of the agreement are written into code.
- The agreements simplify the exchange of shares, money, any asset or property.
- Generally, there are two used programming languages for writing Ethereum smart contracts as a Solidity and Serpent.
- Solidity is a high-level programming language used for implementing smart contracts on the Ethereum Blockchain platform.
- A smart contract is a set of lines of code that is uploaded and stored to check a contract's validity and containing a set of rules under which the parties who share the smart contract agree to interact with each other.
- It is automatically executed when previously determined and defined terms and conditions are met. The smart contract is defined and executed inside a distributed Blockchain.

- In the Ethereum blockchain, so-called Ether (ETH), a cryptocurrency that drives the network, are earned for providing computing power ("mining").
- Ether (ETH) is the cryptocurrency generated by the Ethereum protocol as a reward to miners in a proof-of-work system for adding blocks to the blockchain. It is the only currency accepted in the payment of transaction fees, which also go to miners.
- Ethereum authorize engineers to convey and assemble decentralized applications, a decentralized application (DApps) to fill enough or specific need to its users or clients.
- For instance, Bitcoin, is a DApp that gives it's clients a shared electronic money framework that empowers online Bitcoin installments, since an application that is not centralized comprise of code that keeps on running on a blockchain arrange, which cannot control by any focal substance or individual.
- Golem and Augur are some of the most successful Ethereum based DApps.
- Ethereum can likewise utilize to construct Decentralized Autonomous Organizations (DAO/). The DAO's control by programming code, on an accumulation of know the contracts, produce on the Ethereum blockchain.

1.11 SMART CONTRACTS

- Smart contracts assist we exchange cash, property, shares, or something important in a very clear, conflict-free means whereas avoiding the services of a middleman.
- Smart contracts are translations of an agreement consisting of terms and conditions into a computational code, which is script.
- The developers write the script in a programming language like Java, C++, etc. in such a way that it lacks ambiguity and does not lead to interpretation.
- Smart contracts are self executing contracts containing the terms and conditions of an agreement among associate.
- The smart contract executes on the Ethereum Blockchains decentralized platform and its terms and conditions of the agreement are written into code.
- The agreements simplify the exchange of shares, money, any asset or property.
- Generally, there are two used programming languages for writing Ethereum smart contracts as a Solidity and Serpent.
- Solidity is a high-level programming language used for implementing smart contracts on the Ethereum Blockchain platform.
- A smart contract is a set of lines of code that is uploaded and stored to check a contract's validity and containing a set of rules under which the parties who share the smart contract agree to interact with each other.
- It is automatically executed when previously determined and defined terms and conditions are met. The smart contract is defined and executed inside a distributed Blockchain.

- Fig. 1.27 shows process/working of smart contracts.
- A smart contract is a computer code which is built into blockchain to facilitate, verify or negotiate a contract agreement.
- A set of conditions are made for the operation of smart contracts to which all users agrees. Whenever these conditions are satisfied, automatically the terms of the agreement are carried out.

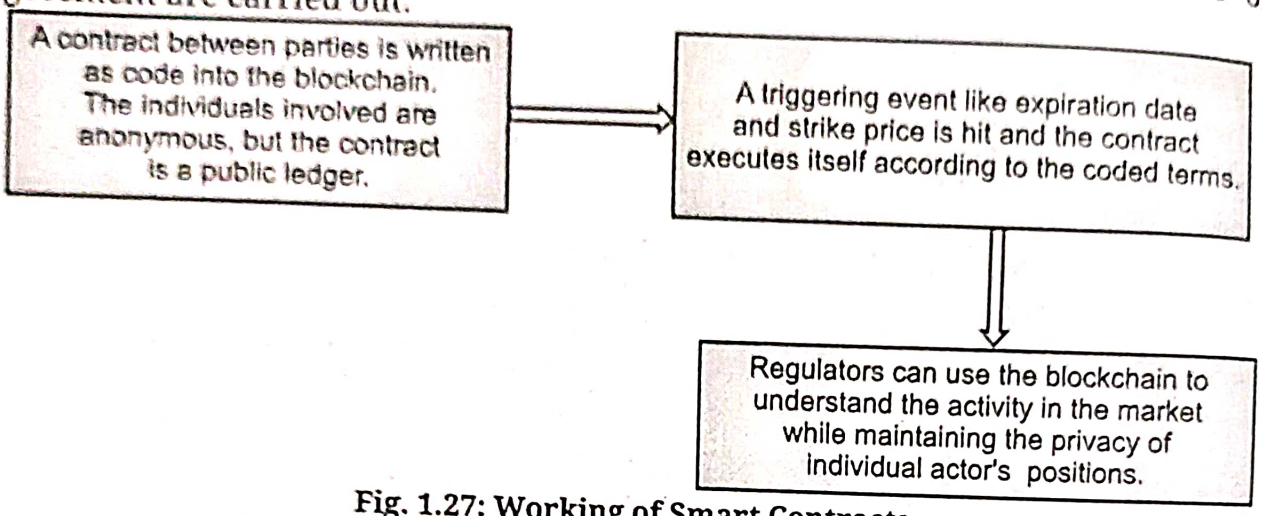


Fig. 1.27: Working of Smart Contracts

- Smart contracts are like regular contracts except the rules of the contract are enforced in real-time on a Blockchain, which eliminates the middleman and adds levels of accountability for all parties involved in a way not possible with traditional agreements.

Benefits of smart contracts with blockchain:

1. **Trust:** Smart contracts automatically execute transactions following predetermined rules, and the encrypted records of those transactions are shared across participants. Thus, nobody has to question whether information has been altered for personal benefit.
2. **Speed and Accuracy:** Smart contracts are digital and automated, so you won't have to spend time processing paperwork or reconciling and correcting the errors that are often written into documents that have been filled manually. Computer code is also more exact than the legalese that traditional contracts are written in.
3. **Savings:** The cost is minimized by removing intermediaries.
4. **Security:** Blockchain transaction records are encrypted, and that makes them very hard to hack. Protects data and transaction from fraud. It is impossible to change or update the data inside a blockchain.

Application of Smart Contracts:

1. **Insurance:** Smart contracts can identify false claims and prevent forgeries.
2. **Copy Righted Content:** Smart contracts can protect ownership rights such as music or books.
3. **Transportations:** Shipment of goods can be easily tracked using smart contracts.
4. **Employment Contract:** Smart contracts can be helpful to facilitate wage payments.

1.12 BLOCKCHAIN USE CASES

- Blockchain technology's core characteristics include decentralization, transparency, immutability, and automation.
- These elements can be applied to various industries, creating a multitude of use cases. Here are what we believe to be the most pertinent Blockchain use cases for enterprises, institutions, and governments.

1. **Blockchain in Capital Markets:** Blockchain technology has fundamentally changed the way financial institutions are exchanging value and building market infrastructure. For capital markets, Blockchain unlocks easier, cheaper, and faster access to capital. It reduces the barriers to issuance and enables peer-to-peer trading, faster and more transparent settlement and clearing, reduced costs, decreased counterparty risks, and streamlined auditing and compliance.
2. **Blockchain in Energy and Sustainability:** Blockchain technology has the potential to transform the energy sector. Energy companies, ranging from utility providers to oil and gas enterprises, are recognizing the transformative impact of blockchain technology. Oil and gas companies suffer from siloed infrastructures and a lack of transparency, efficiency, and optimization. Enterprise-grade blockchain solutions can significantly increase process efficiencies and reduce costs associated with oil and gas operations and distribution.
3. **Blockchain in Financial Services:** The financial industry is recognizing the transformative impact of Blockchain technology to generate new revenue, deliver process efficiency, improve end-user experience and reduce risk in business operations. Financial services struggle with archaic operational processes, slow payment settlements, limited transparency, and security vulnerabilities. Blockchain enhances the efficient digitization of financial instruments, which increases liquidity, lowers cost of capital, and reduces counterparty risk.
4. **Blockchain in Government and the Public Sector:** Governments and public sector organizations leverage Blockchain technology to move away from siloed and inefficient centralized systems. Current systems are inherently insecure and costly, while Blockchain networks offer more secure, agile, and cost-effective structures. A Blockchain-Based Digital Government can protect data, streamline processes, and reduce fraud, waste, and abuse while simultaneously increasing trust and accountability. On a Blockchain-based government model, individuals, businesses, and governments share resources over a distributed ledger secured using cryptography. This structure eliminates a single point of failure and inherently protects sensitive citizen and government data. Ethereum Blockchain technology allows governments to build trust, improve accountability and responsiveness, increase efficiency, reduce costs, and create high-performing government functions with more secure, agile, and cost-effective structures.

1.12 BLOCKCHAIN USE CASES

- Blockchain technology's core characteristics include decentralization, transparency, immutability, and automation.
- These elements can be applied to various industries, creating a multitude of use cases. Here are what we believe to be the most pertinent Blockchain use cases for enterprises, institutions, and governments.

1. **Blockchain in Capital Markets:** Blockchain technology has fundamentally changed the way financial institutions are exchanging value and building market infrastructure. For capital markets, Blockchain unlocks easier, cheaper, and faster access to capital. It reduces the barriers to issuance and enables peer-to-peer trading, faster and more transparent settlement and clearing, reduced costs, decreased counterparty risks, and streamlined auditing and compliance.
2. **Blockchain in Energy and Sustainability:** Blockchain technology has the potential to transform the energy sector. Energy companies, ranging from utility providers to oil and gas enterprises, are recognizing the transformative impact of blockchain technology. Oil and gas companies suffer from siloed infrastructures and a lack of transparency, efficiency, and optimization. Enterprise-grade blockchain solutions can significantly increase process efficiencies and reduce costs associated with oil and gas operations and distribution.
3. **Blockchain in Financial Services:** The financial industry is recognizing the transformative impact of Blockchain technology to generate new revenue, deliver process efficiency, improve end-user experience and reduce risk in business operations. Financial services struggle with archaic operational processes, slow payment settlements, limited transparency, and security vulnerabilities. Blockchain enhances the efficient digitization of financial instruments, which increases liquidity, lowers cost of capital, and reduces counterparty risk.
4. **Blockchain in Government and the Public Sector:** Governments and public sector organizations leverage Blockchain technology to move away from siloed and inefficient centralized systems. Current systems are inherently insecure and costly, while Blockchain networks offer more secure, agile, and cost-effective structures. A Blockchain-Based Digital Government can protect data, streamline processes, and reduce fraud, waste, and abuse while simultaneously increasing trust and accountability. On a Blockchain-based government model, individuals, businesses, and governments share resources over a distributed ledger secured using cryptography. This structure eliminates a single point of failure and inherently protects sensitive citizen and government data. Ethereum Blockchain technology allows governments to build trust, improve accountability and responsiveness, increase efficiency, reduce costs, and create high-performing government functions with more secure, agile, and cost-effective structures.

5. **Blockchain in Insurance:** Blockchain technology will bring about significant efficiency gains, cost savings, transparency, faster payouts, and fraud mitigation while allowing for data to be shared in real-time between various parties in a trusted and traceable manner. Blockchains can also enable new insurance practices to build better products and markets. Insurance companies operate in a highly competitive environment in which both retail and corporate customers expect the best value for money and a superior online experience. Blockchain technology represents an occasion for positive change and growth in the insurance industry. With Ethereum's smart contracts and decentralized applications, insurance can be conducted over Blockchain accounts, introducing more automation and tamper-proof audit trails. Notably, the low cost of smart contracts. Insurance claims are prone to fraud and claim assessments can extend long periods of time. Blockchain can securely streamline data verification, claims processing, and disbursement, reducing processing time significantly.
6. **Blockchain in Real Estate:** Real estate is the largest asset class in the world. Commercial enterprises and real estate professionals are recognizing the transformative impact of blockchain technology to optimize retail and commercial property sales, streamline payments, and increase access to real estate funds and investment opportunities.
7. **Blockchain in Media and Entertainment:** Piracy, fraud, and intellectual property theft of digital items cost the entertainment industry an estimated $71 billion annually. Blockchain technology can track the life cycle of any content, which has the potential to protect digital content, and facilitate the distribution of authentic digital collectibles.
8. **Blockchain in the Legal/Law Industry:** The legal industry has been slow to modernize. Lawyers can leverage Blockchain technology to streamline and simplify their transactional work, digitally sign and immutably store legal agreements. Using scripted text, smart contracts, and automated contract management reduces excessive time spent preparing, personalizing and maintaining standard law documents. These cost savings are passed on to the customer. Additionally, Blockchain democratizes access to the justice system by cutting down on consumer complexity and lowering hefty legal fees. Enterprise Ethereum alleviates labor-intensive manual processes while providing increased accessibility, transparency, cost savings, speed, efficiency and data integrity to the legal industry.

9. **Blockchain in Digital Identity:** The traditional identity systems of today are fragmented, insecure, and exclusive. Blockchain enables more secure management and storage of digital identities by providing unified, interoperable, and tamper-proof infrastructure with key benefits to enterprises, users, and IoT management systems. A Blockchain-based digital identity system provides a unified, interoperable, and tamper-proof infrastructure with key benefits to enterprises, users, and IoT management systems. The solution protects against theft and provides individuals greater sovereignty over their data.
10. **Blockchain in Healthcare:** Blockchain-based healthcare solutions will enable faster, more efficient, and more secure medical data management and medical supply tracking. This could significantly improve patient care, facilitate the advancement to medical discoveries, and ensure the authenticity of drugs circulating global markets. Healthcare professionals and medical providers in fields including global public health, pharmacology, medicine, and health data are recognizing the advantages of Ethereum Blockchain technology to streamline and secure medical data management, drug and medical device tracking, and more.
11. **Blockchain in Retail Fashion:** The pace of the retail fashion industry is rapidly accelerating with the ever-changing demands of consumers. Blockchain technology stands to address long-standing industry challenges by improving data management tools, enhancing supply chain operations, and reducing the risk of counterfeit and grey markets. The retail fashion industry rapidly changes with the demands of consumers. Blockchain stands to address long-standing industry challenges by improving data management tools, enhancing supply chain operations, and reducing the risk of counterfeit and grey markets. Enterprise Ethereum gives retailers, manufacturers, and end-users unprecedented transparency, traceability, and tradability in retail fashion and luxury supply chain management.
12. **Blockchain in Sports:** Major sports organizations around the world recognize the potential of Ethereum Blockchain technology to enhance fan interaction, streamline existing operations, and provide new revenue models. Ethereum enabled smart contracts can streamline existing e-sports operations, provide new revenue models, and enhance fan engagement with enhanced loyalty programs and incentives.

PRACTICE QUESTIONS

Q.I Multiple Choice Questions:

1. What is a Blockchain technology?
   (a) a centralized ledger
   (b) a type of cryptocurrency
   (c) a type of software
   (d) a distributed ledger on a P2P network

2. Which is an online decentralized and distributed ledger technology that has the ability to keep and track records in a secure, verifiable and transparent manner?
   (a) Cryptocurrency (b) Blockchain
   (c) Cryptography (d) None of the mentioned
3. Which is a collection of related data?
   (a) Database (b) Blockchain
   (c) Ledger (d) Bitcoin
4. Which is a file that contains a list of transactions in blockchain technology?
   (a) node (b) ledger
   (c) block (d) consensus
5. A Blockchain is a which type of network,
   (a) peer-to-peer (P2P) (b) client-server network
   (c) Both (a) and (b) (d) None of the mentioned
6. Blockchain ledger is,
   (a) digital (b) distributed
   (c) decentralized (d) All of the mentioned
7. Which is a decentralized digital currency can be sent from user to user on the peer-to-peer network without the need for intermediaries?
   (a) Bitcoin (b) Blockchain
   (c) Both (a) and (b) (d) None of the mentioned
8. Blockchain is a type of,
   (a) View (b) Database
   (c) Object (d) Table
9. Which is the smallest building block of a blockchain (records, information, etc.) that serves as the purpose of Blockchain?
   (a) Block (b) Chain
   (c) Transaction (d) Node
10. Example of public Blockchain includes,
   (a) Bitcoin (b) Ethereum
   (c) Litecoin (d) All of the mentioned
11. A database is implemented using,
   (a) P2P system/network (b) client-server system/network
   (c) Both (a) and (b) (d) None of the mentioned

12. Which is the process of making sure that the two entities talking with each other can establish a trust relationship among them?
    (a) Digital signature
    (b) Blockchain
    (c) Bitcoin
    (d) Digital ledger
13. Blockchain uses which cryptography,
    (a) asymmetric
    (b) symmetric
    (c) Both (a) and (b)
    (d) None of the mentioned
14. Examples for decentralized consensus mechanisms,
    (a) Proof of work (PoW)
    (b) Proof of stake (PoS)
    (c) Proof of Capacity (PoC)
    (d) All of the mentioned
15. What is a blockchain?
    (a) is a digital database consisting of records called transactions.
    (b) is a centralized digital ledger consisting of records called blocks.
    (c) is a decentralized, distributed, digital ledger consisting of records called blocks.
    (d) None of the mentioned
16. Concurrency in its purest form is a,
    (a) peer-to-peer version of electronic cash
    (b) client-server version of electronic cash
    (c) peer-to-peer version of virtual/digital cash
    (d) All of the mentioned
17. Which is a computer program which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement?
    (a) digital ledger
    (b) smart contract
    (c) Bitcoin
    (d) Blockchain
18. Which mechanism refers to any number of methodologies used to achieve agreement, trust, and security across a decentralized computer network?
    (a) smart contract
    (b) digital ledger
    (c) consensus
    (d) None of the mentioned
19. Which function that converts an input of arbitrary length into an encrypted output of a fixed length?
    (a) ledger
    (b) hash
    (c) transaction
    (d) block

20. In which Blockchain multiple companies or multiple individuals combine together to operate the node in a network.
    (a) public (b) private
    (c) hybrid (d) Consortium/Federated
21. Which is a data structure serve to encode blockchain data more efficiently and securely?
    (a) block tree (b) Merkle tree
    (c) transaction tree (d) None of the mentioned
22. Asymmetric cryptography uses which keys for encryption and decryption,
    (a) public key (b) private key
    (c) Both (a) and (b) (d) None of the mentioned
23. Digital currencies in Blockchain includes,
    (a) Bitcoin (b) ether ot ETH
    (c) Monero (d) All of the mentioned

Answers

1. (d)	2. (b)	3. (a)	4. (c)	5. (a)	6. (d)	7. (a)	8. (b)	9. (c)	10. (d)
11. (b)	12. (a)	13. (a)	14. (d)	15. (c)	16. (a)	17. (b)	18. (c)	19. (b)	20. (d)
21. (b)	22. (c)	23. (d)							

Q.II Fill in the Blanks:

1. A _____ is likely decentralized database for storing records of values and transactions.
2. Blockchain is a technology that enables distributed _____ ledger through immutable data in an encrypted and secured way.
3. A _____ contains all the information about the transactions processed on the network.
4. _____ has its own associated cryptocurrency Ether or ETH.
5. The _____ is a common consensus algorithm used by the most popular cryptocurrency networks like bitcoin and litecoin.
6. A blockchain network is in the style of a peer-to-peer network which is running a _____ blockchain framework.
7. The objectives of _____ are the reduction of need in trusted intermediators, arbitrations and enforcement costs, fraud losses, as well as the reduction of malicious and accidental exceptions.
8. A _____ is a data structure which is used for storing information.
9. A hash function takes an input string (numbers, alphabets, media files) of any length and transforms it into a _____ length.
10. _____ is a set of rules and arrangements to carry out blockchain operations.

11. The _____ Blockchain system is controlled only by users from a specific organization or authorized users who have an invitation for participation.
12. The _____ system is adistributed network in which most of the resources and services consumed by a users (clients) are managed and exhibited by a centralised servers.
13. The Merkle tree also called as _____.
14. The _____ Blockchain is a semi-decentralized network that is managed by multiple organizations.
15. _____ cryptography allows proving one's identity with a set of cryptographic keys namely, a private key known to everyone) and a public key (kept secret).
16. Cryptocurrencies like Bitcoin and Ethereum use a peer-to-peer _____ system to conduct transactions.
17. Bitcoin is based on _____Blockchain
18. Cryptocurrency is a digital _____ which can be used to exchange value between parties.
19. Ethereum is a decentralized, _____ blockchain with smart contract functionality.
20. _____ signatures are a technique used to provide message authentication and integrity over networks.

Answers

1. Blockchain	2. public	3. block	4. Ethereum
5. Power-of-Work (PoW)	6. decentralized	7. smart contracts	8. database
9. fixed	10. Consensus	11. private	12. client-server
13. hash tree	14. consortium	15. Public-key	16. decentralized
17. public	18. asset	19. open-source	20. Digital

Q.III State True or False:

1. The word 'Blockchain' is made up of two separate terms, 'block' and 'chain'. A block being referred to a collection of data, alias data records, and chain being referred to a public database of these blocks, stored as a list.
2. Digital signature provides a mathematical proof regarding identity of person that approves some particular message in blockchain.
3. A P2P network is a computer network where computers (peers/nodes) are distributed and share the network's workload to reach the end goal. Nodes perform transactions on the blockchain.
4. For a blockchain such as Ethereum, and a DLT such as Hyperledger, smart contracts, or chain-code, are the code logic that is executed on a blockchain network.
5. Consensus is responsible for validating the blocks, ordering the blocks, and ensuring that everyone agrees on it.
6. A nonce in a blockchain is a group or collection of information.

7. A blockchain distributed ledger runs on a P2P network, where transactions are validated using cryptography by consensus algorithms.
8. Hashing is the process of sending data through a hash function to produce a specific, essentially unique hash of a fixed length.
9. A blockchain network defines the consensus algorithm for it, which is essentially the rule to validate transactions on the blockchain P2P network.
10. Blockchain is a decentralized, massively replicated database (distributed ledger), where transactions are arranged in blocks, and placed in a P2P network.
11. A digital ledger provide assurance that the message was in fact sent by the sender and not even a single bit of the message has been changed.
12. The network layer in Blockchain, also known as the P2P layer, is the one that is responsible for internode communication.
13. Consensus is the rules that nodes follow to ensure that transactions are validated within the boundaries of those rules and that blocks follow those rules.
14. dApps is a distributed application that runs on top of a distributed technology like Blockchain, such as Ethereum, Bitcoin, or Hyperledger Fabric.
15. A permissioned blockchain is also known as a public blockchain because anyone can join the network.
16. Ethereum is an open source, public blockchain network.
17. Hybrid Blockachain is a combination of public Blockchain and private Blockchain.
18. Block is a data structure used for keeping a set of transactions which is distributed to all nodes in the network
19. Corda, Hyperledger Fabric, Hyperledger Sawtooth, Corda are the examples of the hybrid Blockchain.
20. A Merkle tree is a binary tree of hashes.
21. A goal of cryptography is to transform any data from its original form, called the plaintext, into an abscure form known as the ciphertext. This process is called encryption. The reverse process of recovering the plaintext from the ciphertext is called decryption.
22. The Proof of Stake (PoS) is another common consensus algorithm involves the allocation of responsibility in maintaining the public ledger to a participant node in proportion to the number of virtual currency tokens held by it.
23. Bitcoin is a client-server system based electronic cash.

Answers

1. (T)	2. (T)	3. (T)	4. (T)	5. (T)	6. (F)	7. (T)	8. (T)	9. (T)	10. (T)
11. (F)	12. (T)	13. (T)	14. (T)	15. (F)	16. (T)	17. (T)	18. (T)	19. (F)	20. (T)
21. (T)	22. (T)	23. (F)							

Q.IV Answer the following Questions:

(A) Short Answer Questions:

1. Define Blockchain.
2. What are the types of Blockchain?
3. Define block and chain.
4. Define crptocurrency.
5. What is Bitcoin?
6. What is consensus?
7. Why is Blockchain a trustworthy approach?
8. What is Ethereum?
9. Define hashing.
10. Define digital signature.
11. Define database.
12. What is nonce?
13. Define smart contracts.
14. What is cryptography?

(B) Long Answer Questions:

1. What is Blockchain? Explain its importance/need. Also state its advantages and disadvantages.
2. Explain following Blockchains with examples:
   (i) Public
   (ii) Private
   (iii) Consortium
   (iv) Hybrid.
3. What is block? Explain its structure diagrammatically.
4. What is Cryptocurrency? Lists its examples.
5. What is the difference between blockchain and database?
6. Define key. Differentiate between public and private key?
7. Explain the Digital signature with its working.
8. Describe the Consensus mechanisms in detail.
9. What is digital currency Bitcoin and Ethereum?
10. Explain the Blockchain generations.
11. Write down on types of networks.
12. What is hashing? Explain in detail.
13. Write the Blockchain use cases.

14. What is the difference between client-server and peer-to-peer network.
15. Write a short note on: Evolution of Blockchain.
16. Explain the layered architecture of Blockchain.
17. Write a short note on: Smart contracts.
18. With the help of diagram describe types of Blockchain networks.

How Blockchain Works?

Objectives...

- To understand How Blockchain Works
- To learn Concepts of Hashing
- To study Mining
- To learn Consensus Protocols

2.0 INTRODUCTION

- The Blockchain is one of those new and revolutionary technologies in the 21st Century that will have a significant impact on the market and industry.
- Blockchain first came to fame in October 2008, to light when a white paper on "Bitcoin: A peer-to-peer electronic cash system" as part of a proposal for Bitcoin published by a person or Group of individuals name 'Satoshi Nakamoto'.
- Blockchain is the backbone technology of digital cryptocurrency Bitcoin. Bitcoin is a type of digital currency that we can transfer within the Bitcoin network without the help of mediators. We can store Bitcoin in a digital wallet (or e-wallet).
- A cryptocurrency wallet or crypto wallet (like BitGo) is a device or a program or a service which stores the public and/or private keys for cryptocurrency transactions.
- The blockchain is a distributed database of records of all digital event or transactions that have been executed and shared among participating parties or peoples.
- Each transaction verified by the majority of participants of the system and contains every single record of each transaction.
- Blockchain technology Records Transaction in Digital Ledger which is distributed over the Network thus making it incorruptible.

  Anything of value like Land Assets, Cars, etc. can be recorded on Blockchain as a Transaction. Blockchain technology grants us to belief the outputs of the system without trusting any user within it.
- People and institutions who do not know or trust each other, live in different countries, are subject to different authorities, and who have no legally binding agreements with each other, can now interact over the internet without the need for trusted third parties like banks, internet platforms and other types of clearing institutions.

- The Bitcoin white paper helps to resolve the problem of centralized data storage and information management.
- In the network all computers hold an identical copy of the ledger of transactions, which acts as a single point of reference.
- Storing data across a Peer-to-peer network eliminates problems emerging from the vulnerability of centralized servers while using different cryptographic methods to secure the network.
- A Blockchain network can track orders, payments, accounts, production and much more. So we can see all details of a transaction end-to-end, new efficiencies and opportunities.
- The Blockchain framework is created as the underlying transaction network behind the digital currency called Bitcoin.

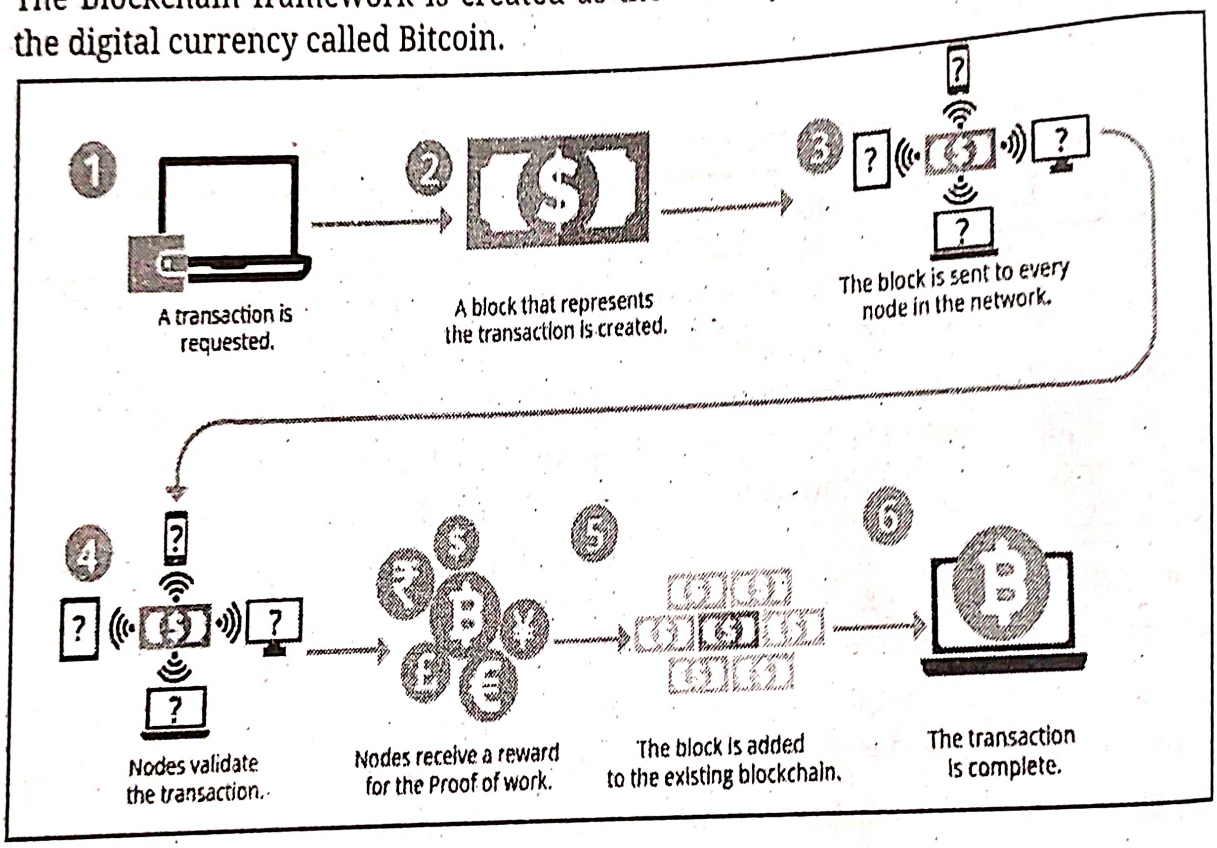


Fig. 2.1: Working of Blockchain Technology

2.1 HASHING

- Hashing is essential to Blockchain in cryptocurrency. A hash is a mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length.
- Hashing in Blockchain ensure that all blocks are well formed and tamper-free and thus the Blockchain will remain secure and virtually un-breakable.
- The following properties of cryptographic hashing makes the Blockchain data structure functionally powerful:
  1. **Collision Free:** It is impossible to find two input texts that produces the same hash value.

2. **Easy to Generate:** It is easy to generate a hash value for a particular input using hash function.
3. **Irreversible:** It is impossible to generate original text from the hash value.
4. **Commitment:** It is not feasible to modify the original text without resulting a change in hash value thus enabling data integrity.

- Blockchains uses the hashing technology extensively as identifiers for addresses, blocks and transactions.
- A hash function is a function that takes one piece of information of any size and maps it to another piece of data of a fixed size.
- Fig. 2.2 shows the process of hashing in Blockchain.

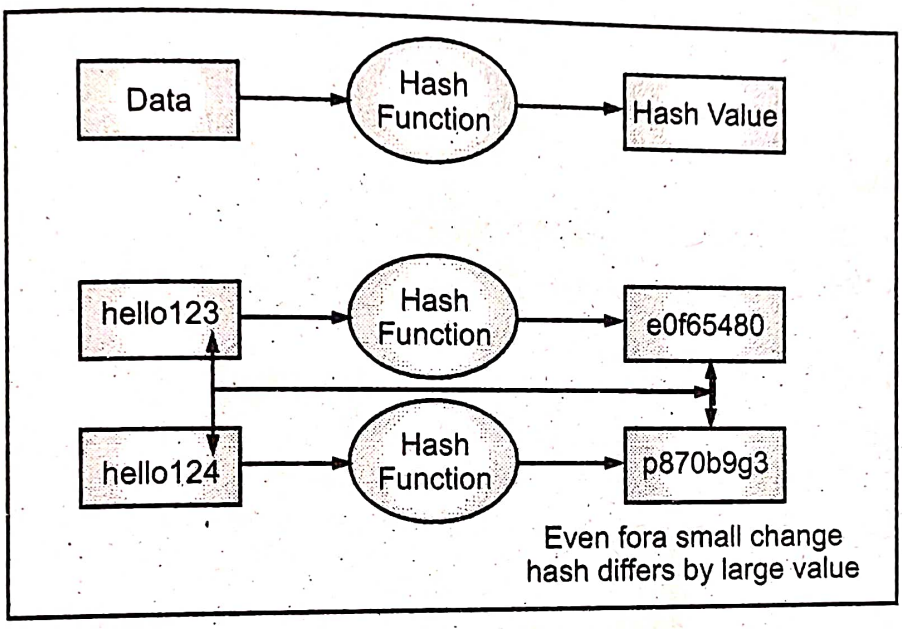


Fig. 2.2: Process of Hashing

Concept of Hash Function:

- A hash function takes any input like numbers, words, etc., and through the use of an algorithm, produces an output of a specific length.
- A hash function maps the data of any arbitrary size to data of fixed size. Bitcoin uses SHA-256 hash function that produces a hash (output) of size 256 bits (32 bytes).
- The process of applying a hash function on the data is called hashing. A cryptographic hash function has two main features:
  1. **Pre-image Resistance:** The hash function works in only one direction i.e., we cannot deduce the input from the output. Consequently, for two sets of inputs, even if the inputs only differ by the smallest detail, the outputs should be wildly different and not resemble one another.
  2. **Collision Resistance:** When a hash function produces the same or identical output for two different inputs, this is called a collision. It is imperative that collisions are avoided in order to guarantee data integrity. If two pieces of data produce the same hash, then one can be interchanged with the other, leading to a breakdown of continuity.

- A cryptographic hash function is an algorithm that takes input strings of a... (typically very large) length and maps these to short fixed length output strings.

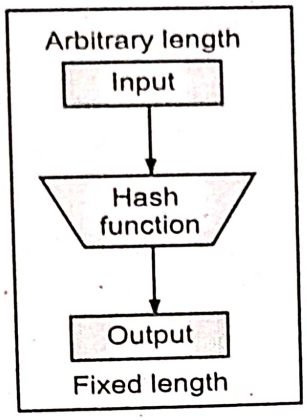


Fig. 2.3: Hashing

Concept of Hashing:

- Hashing is a cryptographic technique, which can transform any information into a hash. Hashing takes on an input (string) of any length and converts it into an output of a fixed length.
- Hashing means taking an input as a string of any length and giving output of a fixed length. The output of fixed length is called as hash.
- Blockchain uses SHA-256 hashing having a hash length of 256 bits.

Types of Cryptographic Hash Functions:

1. Secure Hashing Algorithm (SHA-2 and SHA-3).
2. RACE Integrity Primitives Evaluation Message Digest (RIPEMD).
3. Message Digest Algorithm 5 (MD5).
4. BLAKE2.

2.1.1 Understanding SHA 256 Hash

- Hash functions are mathematical functions that transform or map a given set of data into a bit string of fixed size, also known as the "hash value or hash."
- The Secure Hash Algorithm (SHA) is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST).
- Cryptographic hash function SHA-256 takes input of any size and the output is always a fixed size 256 bits (32 bytes).
- SHA-0 is the first version of the SHA algorithm. In 2004, several weaknesses were exposed in the algorithm, resulting in the creation of a new stronger version of SHA-0 called SHA-1.
- In 2005, an attack of SHA-1 reported that it would find a collision in fewer hashing operations. SHA-2 was created to overcome SHA-1's vulnerabilities and it could be implemented with a digest size of 224, 256, 384 and 512 bits.

- SHA-2 is a widely used standard in modern cryptographic applications. Bitcoin uses the SHA-256 variant as a hashing algorithm to solve Proof-of-Work (PoW) puzzles. SHA-3 is the latest family of hash functions with 224-, 256-, 384- and 512-bit variants.
- SHA-256 hash function commonly used in Blockchain technology. SHA-256 is also called as Secure Hash Algorithm 256. SHA-256 is a hashing algorithm used to convert text of any length into a fixed-size string of 256 bits or 32 bytes.
- SHA-256 is a popular hashing algorithm used in Bitcoin encryption, it was introduce when the network launched in 2009.
- After all then, SHA-256 has been adopted by a number of different Blockchain projects, including several coins created from forks of the original Bitcoin source code.
- The top three SHA-256 Blockchain projects by market capitalization are Bitcoin (BTC), Bitcoin Cash (BCH), and Bitcoin Satoshi's Vision (BSV).
- Fig. 2.4 shows process of SHA-256. Cryptographic hash functions take arbitrary blocks of data and return fixed-size bit strings.

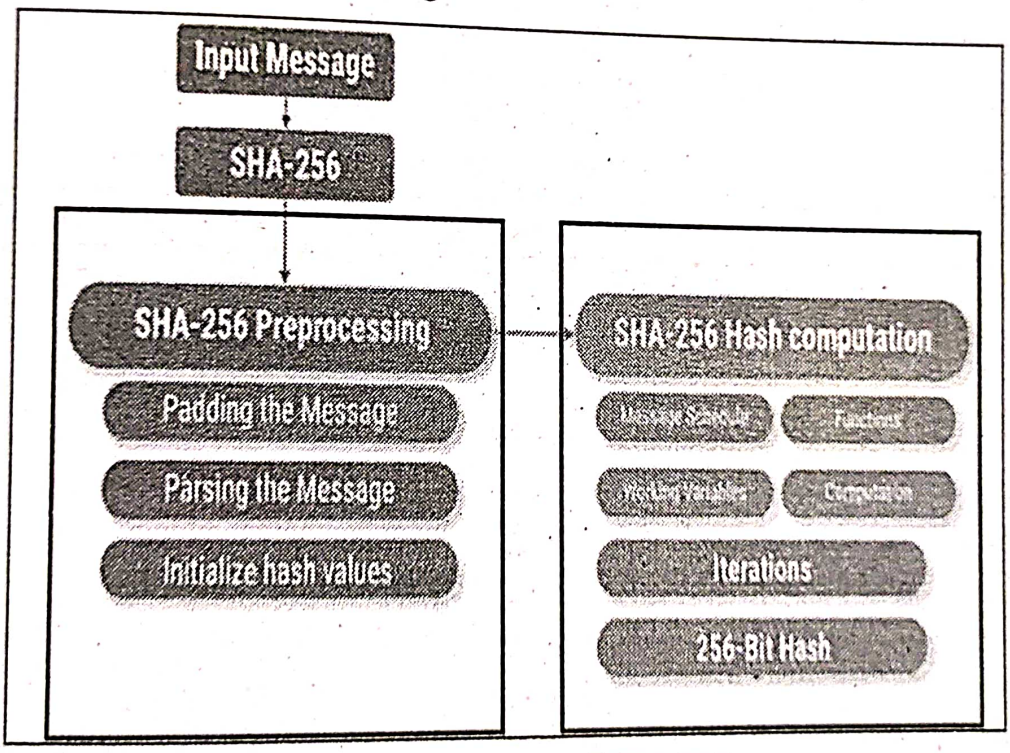


Fig. 2.4: Process of SHA-256

- We will see in Fig. 2.4 how to transform the message into the hash value, also called digest or simply hash.
- The SHA-256 starts by converting the message to a binary number and get length 1. The objective of this padding is to prepare the message before the hash computation begins. The padding ensures that the padded message is a multiple of 512 bits.
- Now we are going to parse the padded message. After the message padding, we now need to parse the message into 512-bit blocks before the hash computation can begin.
- To parse, we will take each set of 8 bits and convert the elements - i.e. each 4 set of 8 bits - into hexadecimal values.

- SHA-2 is a widely used standard in modern cryptographic applications. Bitcoin uses the SHA-256 variant as a hashing algorithm to solve Proof-of-Work (PoW) puzzles. SHA-3 is the latest family of hash functions with 224-, 256-, 384- and 512-bit variants.
- SHA-256 hash function commonly used in Blockchain technology. SHA-256 is also called as Secure Hash Algorithm 256. SHA-256 is a hashing algorithm used to convert text of any length into a fixed-size string of 256 bits or 32 bytes.
- SHA-256 is a popular hashing algorithm used in Bitcoin encryption, it was introduce when the network launched in 2009.
- After all then, SHA-256 has been adopted by a number of different Blockchain projects, including several coins created from forks of the original Bitcoin source code.
- The top three SHA-256 Blockchain projects by market capitalization are Bitcoin (BTC), Bitcoin Cash (BCH), and Bitcoin Satoshi's Vision (BSV).
- Fig. 2.4 shows process of SHA-256. Cryptographic hash functions take arbitrary blocks of data and return fixed-size bit strings.

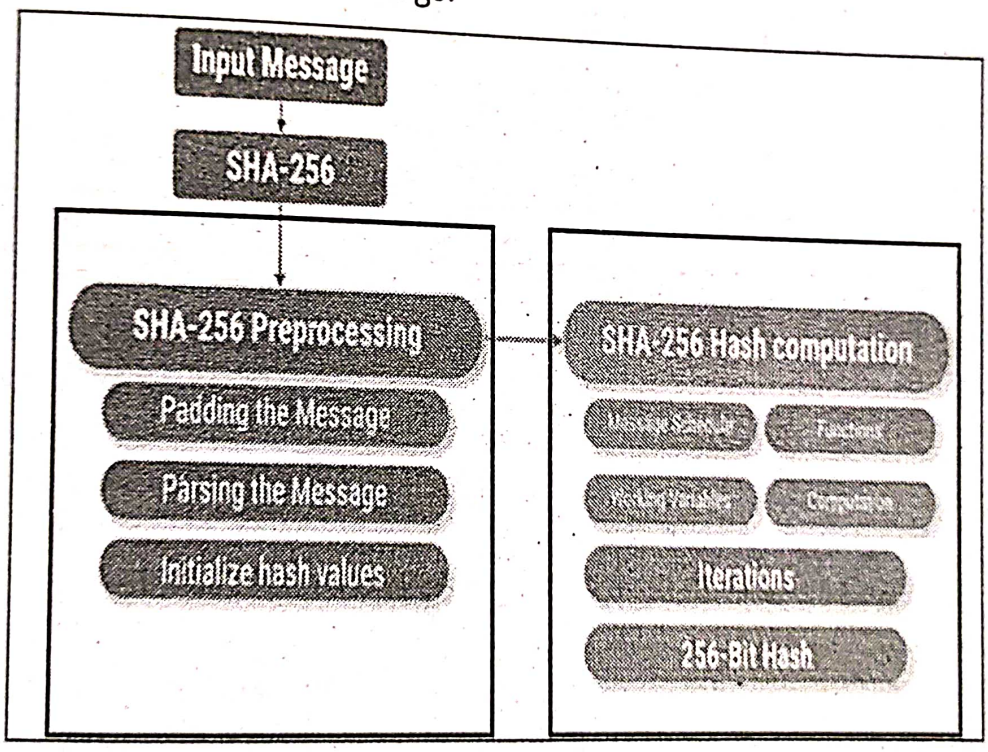


Fig. 2.4: Process of SHA-256

- We will see in Fig. 2.4 how to transform the message into the hash value, also called digest or simply hash.
- The SHA-256 starts by converting the message to a binary number and get length 1. The objective of this padding is to prepare the message before the hash computation begins. The padding ensures that the padded message is a multiple of 512 bits.
- Now we are going to parse the padded message. After the message padding, we now need to parse the message into 512-bit blocks before the hash computation can begin.
- To parse, we will take each set of 8 bits and convert the elements - i.e. each 4 set of 8 bits - into hexadecimal values.

- The hashing algorithm will then perform the necessary computations that include the iterations to create the hash. We now feed the initialize hash values that we have prepared before into the algorithms.
- For the hash function computation, the algorithm will grab the message that was divided into chunks and put it through 64 rounds of operations. The output obtained in each round is fed as an input of the next computation round.
- We can see the 64 rounds of operations that will be performed in the 512-bit message. Once that all the iterations are completed, we can complete the hashing process.
- **Examples:** We use http://blockchain.mit.edu/hash web site. If we can type any character/string in the Data: we will observe its corresponding cryptographic hash in the Hash: (See Fig. 2.5).

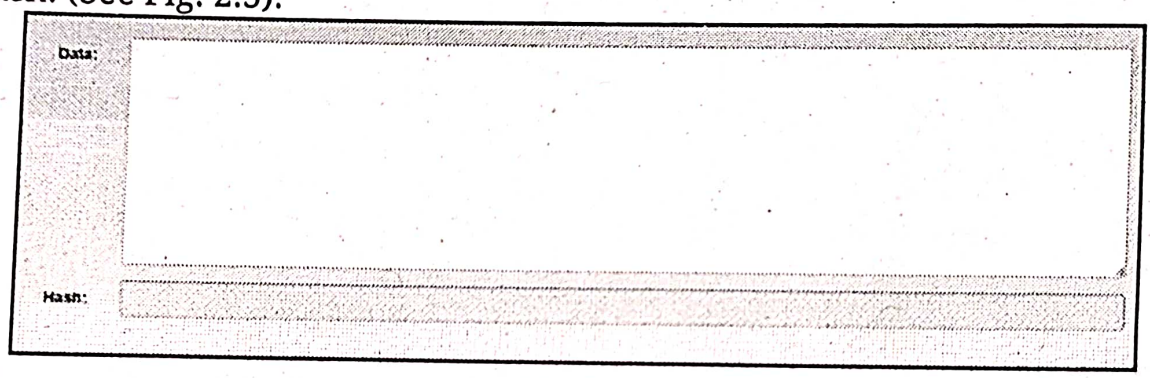
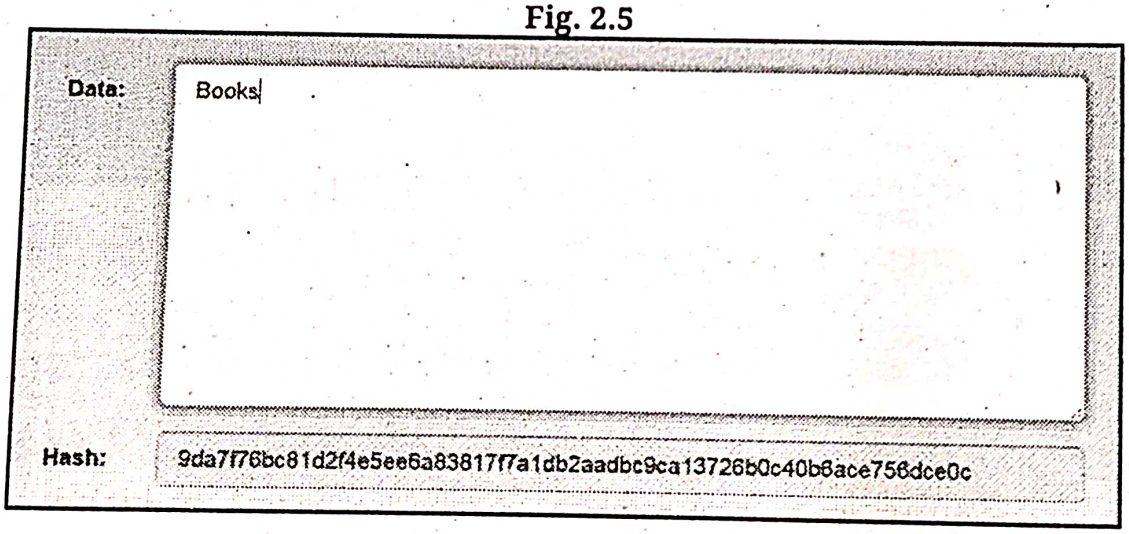
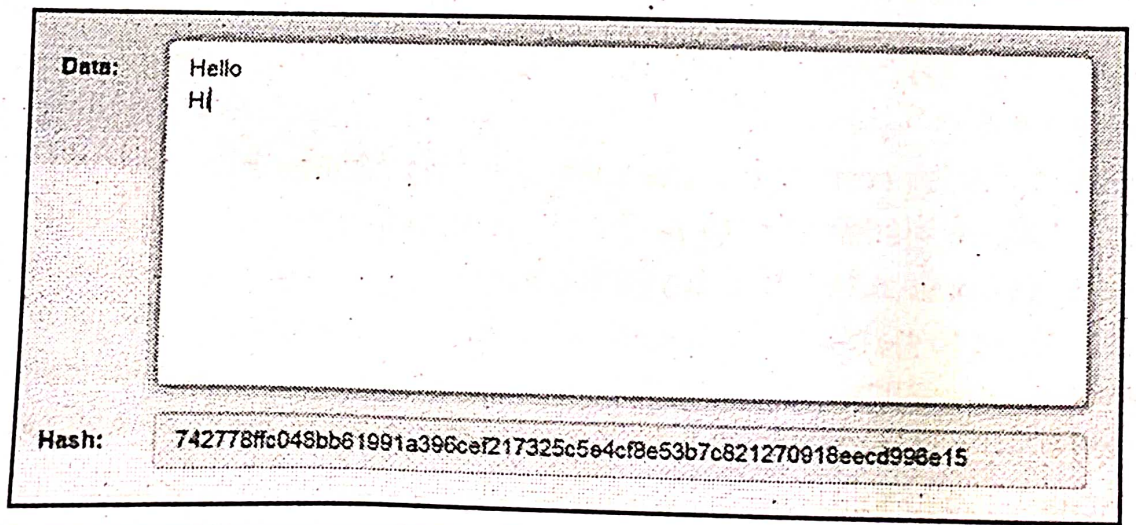
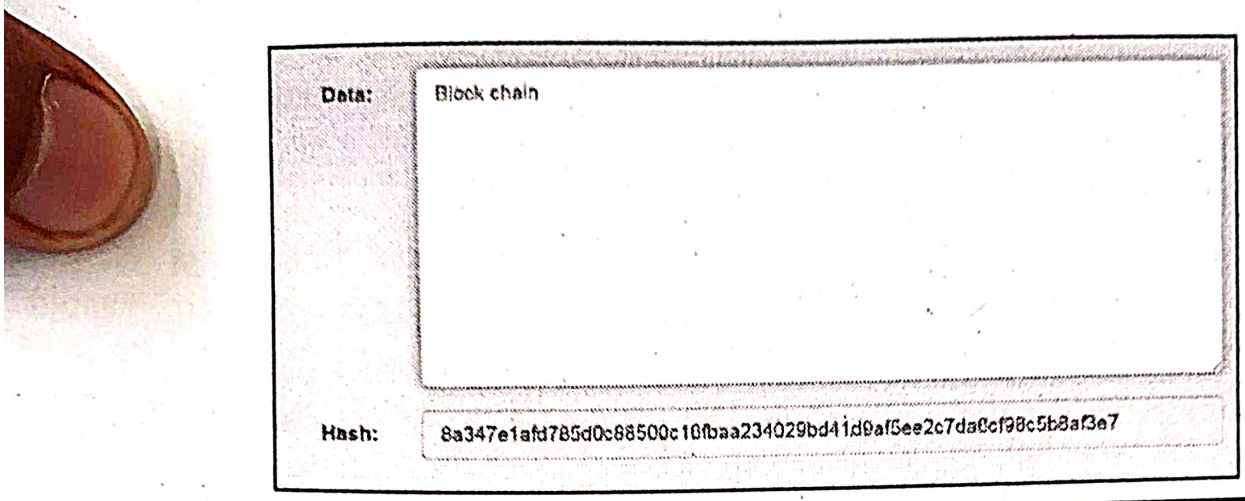


Fig. 2.5







2.2 IMMUTABLE LEDGER

- Blockchain is a decentralized, distributed and immutable ledger technology that operates over a peer-to-peer network. Immutability is defined as the ability of a Blockchain ledger to remain unchanged/unaltered/modified.
- The Blockchain is purposefully made to be practically immutable i.e., no one (in theory, atleast) can alter/modify the Blockchain's 'distributed ledger' of every single committed block.
- Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets [can be tangible (a house, a car, cash, land) or intangible (intellectual property, patents, copyrights, branding)] in a business network.
- A Blockchain is a type of digital ledger or decentralized database that is continuously updated and distributed to different participants in a network.
- Blockchain is an immutable ledger implemented in a distributed fashion without a central authority (i.e., a bank, company or government)
- The ledger or database, records the occurrence of some underlying event-whether that is a transfer of cryptocurrency (such as Bitcoin, Litecoin, and Ethereum) or a digital agreement to perform some service (such digital agreements, or smart contracts).
- The immutability property of a Blockchain means that the data which has been written once on the Blockchain cannot be changed.
- In Blockchain technology, because each block in the distributed ledger relates to the previous block constituting a chain of blocks, the blocks are permanently saved and never changed as long as the participating user continues to maintain the network.
- Blockchain technology is a form of distributed ledger technology. A Blockchain is a distributed and immutable ledger to transfer ownership, record transactions, track assets, and ensure transparency, security, trust and value exchanges in various types of transactions with digital assets.
- A distributed ledger is a digital record of transactions, shared instantaneously across a network of participants.

- It is "distributed" because the transaction record is held by each of the users of the network and each user's copy is updated with new information simultaneously.
- Immutable means cannot be changed and ledger is a fancy term for record, a record of something therefore an Immutable Ledger is a record that cannot be changed.
- Blockchain is a distributed ledger that records digital transactions in a secure, transparent, immutable and auditable manner, without necessarily using a trusted third-party intermediary to perform these transactions.
- Immutable ledger resides in the concept of the hash. If hacker tries to alter anything in the block its hash will change.
- Now the hash will no long match the previous hash in the second block. So, the hacker would have to change the next block, and the block after that, etc.
- Even if they were able to pull that off, the blockchain belong to multiple computers. The hacker would need to make all of these changes simultaneously.
- When consider the millions of nodes that make up a blockchain environment like BitCoin, it will see that would be impossible.
- Blockchain is a distributed immutable ledger that is encrypted. It is immutable for two reasons: time stamp and the encryption of preceding content.
- Blockchain can be comprehended as a shared copy of an immutable ledger, facilitating the process of recording transactions and tracking assets in a network.

2.3 DISTRIBUTED P2P NETWORK

- The Blockchain records transactions in the form of an immutable ledger. It is deployed via a distributed network of untrusting peers, each maintaining a copy of the ledger.
- Peer-to-Peer (P2P) network is a decentralized network consists of a group of devices (nodes) that collectively store and share files where each node acts as an individual peer.
- The peer-to-peer architecture of Blockchain allows all cryptocurrencies to be transferred worldwide, without the need of any middle-man or intermediaries or central server.
- With the distributed peer-to-peer network, anyone who wishes to participate in the process of verifying and validating blocks can set up a Bitcoin node.
- Blockchain is a decentralized ledger tracking of one or more digital assets on a peer-to-peer network. A peer-to-peer network is a decentralized network where all the computers are directly connected in some way and where each maintains a complete copy of the ledger and compares it to other devices to ensure the data is accurate.
- This is unlike a bank, where transactions are stored privately and are managed only by the bank.

- P2P is known as peer-to-peer network is a decentralized network communications model that consists of a group of devices or nodes that store and share data or files where each node acts as an individual peer.
- In P2P communication is done without any central administration or server, which means all nodes have equal power and perform the same tasks.
- Bitcoin creator Satoshi Nakamoto defined it as, a "peer-to-peer electronic cash system" built with the aim to create a P2P digital form of money without banks.
- The Blockchain technology leverages the power of P2P networks and also it provides a shared and trusted ledger of transactions.
- A distributed ledger technology, Blockchain records transactions as an immutable time-stamped digital block that indicates senders and receivers.
- No centralized authority manages the Blockchain networks and only the participants can validate transactions among each other.
- The technology allows people and institutions to trust the output without trusting the participants.
- This new form of distributed data storage and management acts as a digital ledger that publicly records all transactions and activities.

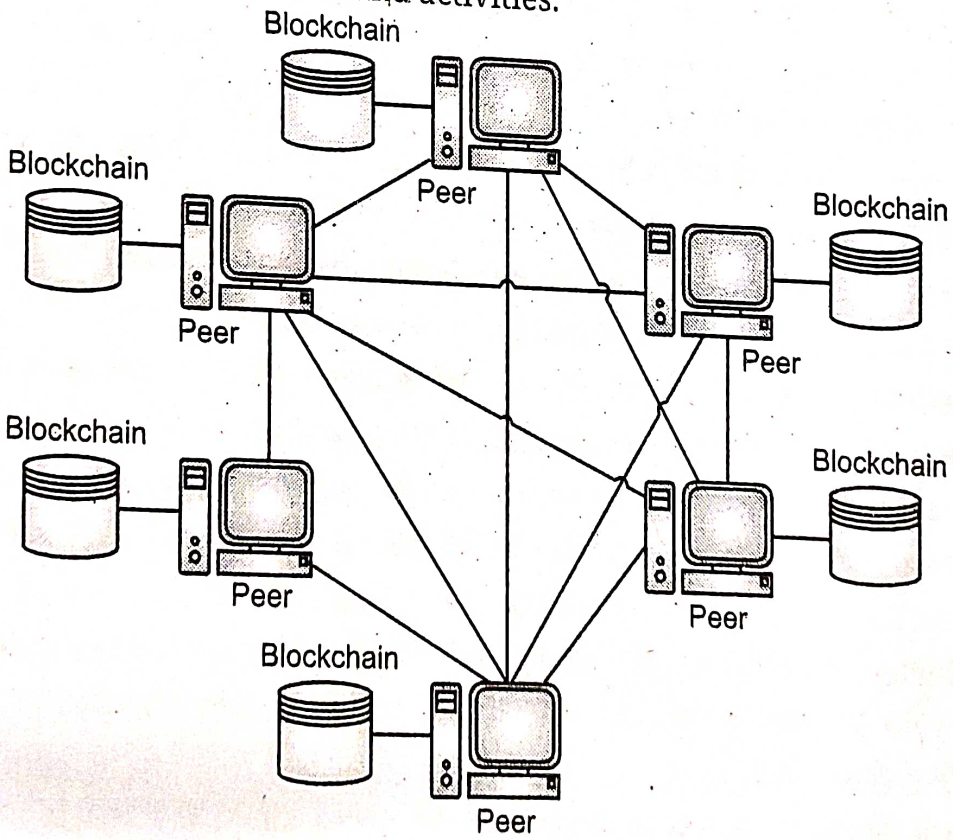


Fig. 2.6: Blockchain P2P Network

- A peer-to-peer (P2P) network is a decentralized communication model between two peers also known as nodes, which can communicate with each other without the need for a central server.

- P2P is known as peer-to-peer network is a decentralized network communications model that consists of a group of devices or nodes that store and share data or files where each node acts as an individual peer.
- In P2P communication is done without any central administration or server, which means all nodes have equal power and perform the same tasks.
- Bitcoin creator Satoshi Nakamoto defined it as, a "peer-to-peer electronic cash system" built with the aim to create a P2P digital form of money without banks.
- The Blockchain technology leverages the power of P2P networks and also it provides a shared and trusted ledger of transactions.
- A distributed ledger technology, Blockchain records transactions as an immutable time-stamped digital block that indicates senders and receivers.

No centralized authority manages the Blockchain networks and only the participants can validate transactions among each other.

The technology allows people and institutions to trust the output without trusting the participants.

This new form of distributed data storage and management acts as a digital ledger that publicly records all transactions and activities.

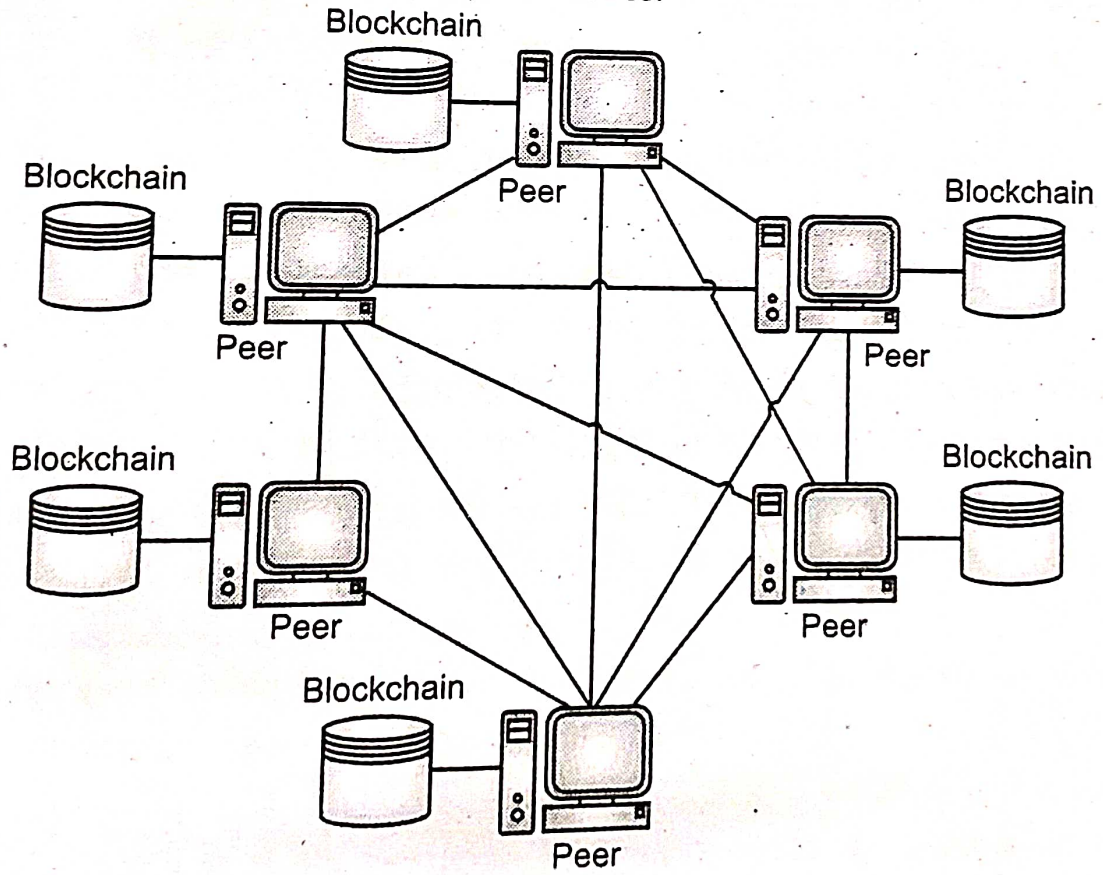


Fig. 2.6: Blockchain P2P Network

A peer-to-peer (P2P) network is a decentralized communication model between two peers also known as nodes, which can communicate with each other without the need for a central server.

Pros and Cons of P2P:

1. As Blockchain is a decentralized system of peer to peer network, available due to decentralization.
2. Because of P2P networking capability, even if one peer gets down, the other peers are still present. Thus nobody can take down the Blockchain.
3. P2P networks offer greater security compared to traditional client-server systems.
4. These networks are virtually immune to the Denial-of-Service (DoS) attacks.
5. The distributed peer-to-peer network, when paired with a majority consensus requirement, gives Blockchains a relatively high degree of resistance to malicious activity.

2.4 HOW MINING WORKS?

- Blockchain mining is a process to validate every step in the transactions while operating Bitcoins or other cryptocurrencies.
- The people involved here are known as Blockchain miners, and these miners' function in a labyrinth of computational hardware and software - their primary aim to authenticate the transfer of currency from a computer in the network to another.
- The main objective of mining is to ensure the perpetuity and security of the decentralized network.
- Mining, in the context of Blockchain technology, is the process of adding transactions to the large distributed public ledger of existing transactions.
- Blockchain mining is used to secure and verify Bitcoin transactions. Mining is the process by which new Bitcoin is added to the money supply.
- The process of new coin generation is called mining. Bitcoin mining is the process of creating new Bitcoin by solving a computational puzzle.
- Mining is serves to secure the Bitcoin system against transactions or fraudulent transactions spending the same amount of Bitcoin more than once, known as a double-spend.
- Miners provide processing power to the Bitcoin network in exchange for the opportunity to be rewarded Bitcoin. Miners confirm new transactions and record them on the global ledger.
- A new block, containing transactions that occurred since the last block, is "mined" every ten minutes, accordingly adding those transactions to the Blockchain.
- Transactions that become part of a block and added to the Blockchain are considered "confirmed," which allows the new owners of Bitcoin to spend the Bitcoin they received in those transactions.

- Miners receive two types of rewards for mining that is new coins created with each new block, and transaction fees from all the transactions included in the block.
- To earn this reward, the miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm.
- The solution to the problem, called the Proof of Work (PoW), is included in the new block and acts as proof that the miner expended significant computing effort.
- The competition to solve the PoW algorithm to earn reward and the right to record transactions on the Blockchain is the basis for Bitcoin's security model.

Working of Mining:

- Blockchain mining is a process used to validate new transactions. Mining is an essential activity in the Blockchain network.
- It is the way the peer-to-peer network verifies transactions and reaches common consensus without requiring a central authority.
- The mining process starts when miners are trying to validate new transactions and record them on the Blockchain.
- The miners are competing to solve a difficult mathematical puzzle based on a cryptographic hash algorithm.
- The solution found is called the PoW. When a block is 'solved', all the transactions contained in the candidate block are considered validated, and the new block is confirmed.
- This new block will be appended to the Blockchain. The time taken to confirm a new block is approximately 10 minutes for Bitcoin, but for other coins it is much faster.
- So, if we send or receive Bitcoins, it will take approximately 10 minutes for the transaction to be confirmed.
- Miners receive a reward when they solve the complex mathematical problem. There are two types of rewards namely, new bitcoins and transaction fees.
- Mining ensures that only legitimate transactions are verified in the Blockchain of any given cryptocurrency. Mining uses cryptographic hash function called double SHA-256.
- If we consider a block to mine first, we need to collect the new transactions into a block, and then we hash the block to form a 256-bit block hash value.
- When the hash initiates, the block has been successfully mined and is directed to the Bitcoin Blockchain network, and that has turned into the identifier for the block.
- In many cases, the hash is not successful, so we need to alter the block to some extent and try again and again.

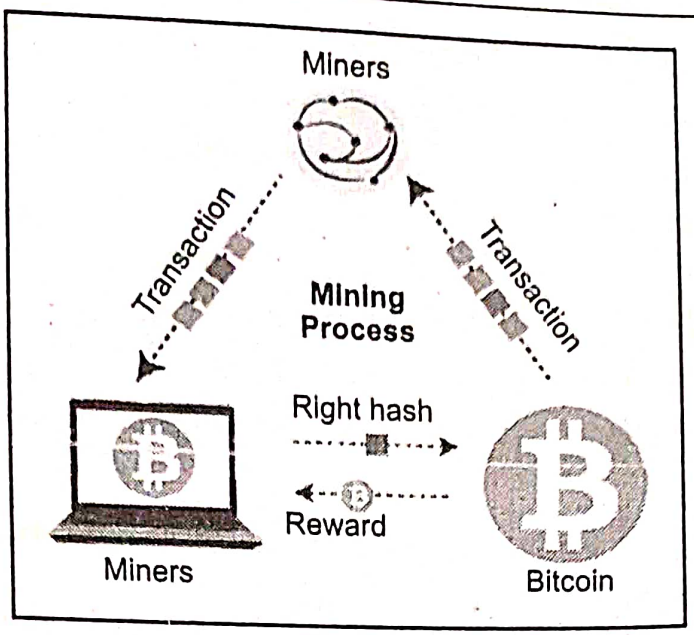


Fig. 2.7: Mining Process in Blockchain

2.4.1 Nonce

- Nonce stands for "Number used only once" i.e., Nonce refers to a number or value that can only be used once.
- Nonce is a 32-bit (4 byte) random number which can be used one time. Nonce is often used on cryptographic hash functions and authentication protocols.
- The "nonce" in a Bitcoin block is a 32-bit (4-byte) field whose value is adjusted by miners so that the hash of the block will be less than or equal to the current target of the network.
- In the Blockchain technology, a nonce refers to a pseudo-random number that is utilized as a counter during the process of mining.
- In nonce it is compared to the existing target, whether it is lower or equal to the current target.
- In the miners test and discard millions of Nonce per second until they find that Golden Nonce, which is valid.
- In order to complete the verification faster than other miners, miners compete with each other using their computer hashing power.
- Once, the Golden Nonce is found, they can complete the Block and add it to the Block Chain and there by receive the Block reward. In this rules out the possibility of any duplication, or using the same Bitcoin twice.
- Nonce will change because it is unique, whether rest of the fields are changed or not, and thus became the most important component of the Proof of Work.
- In cryptography, a nonce is a random number that can be used just once in a cryptographic communication.

It is often a random number issued in an authentication protocol to ensure that, same communication is not reused.

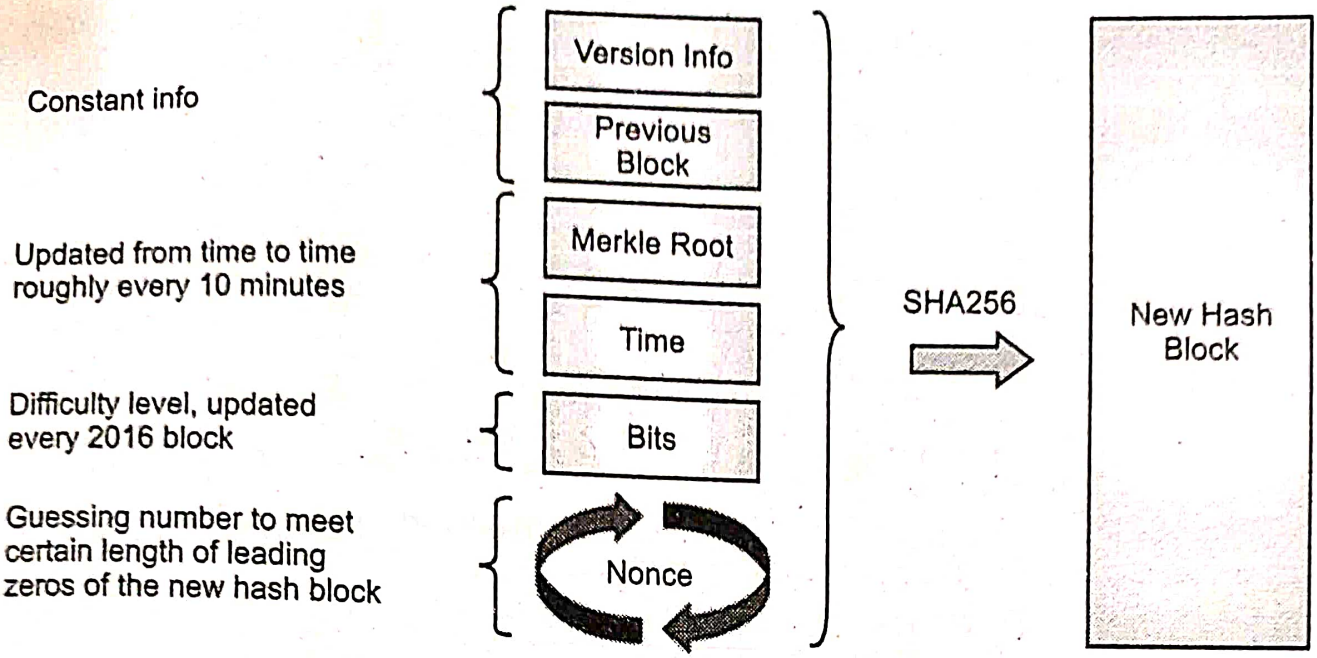


Fig. 2.8 (a): Concept of Nonce

- There will be some constant information, timestamp, hash value with difficulty, and the nonce which when passed through Hash algorithm – SHA256 will become a new block, therefore nonce plays a very important role.
- As we have already discussed, millions of nonce values are tried until the Golden Nonce is found.
- The target hash value is defined as the difficulty and the iterative calculation of the hash value requires the miner's computer resources.
- Only with the correct Nonce value, proof of work can be created and thus giving birth to a new Block in the Block chain.
- **Example:** The miner has to calculate the hash which should be below the target hash assigned to it.
- But it cannot change the Block number, Data, Previous Hash in order to guess a new hash due to the avalanche effect.
- A nonce is a 32-bit number. So there can be a maximum of approximately 4 billion possible Nonce values as 2^(32) = 4, 294, 967, 296.
- The nonce is randomly selected for each iteration. So for each iteration, a random integer between 0 and 4, 294, 967, 296 is selected.

- It is often a random number issued in an authentication protocol to ensure that, same communication is not reused.

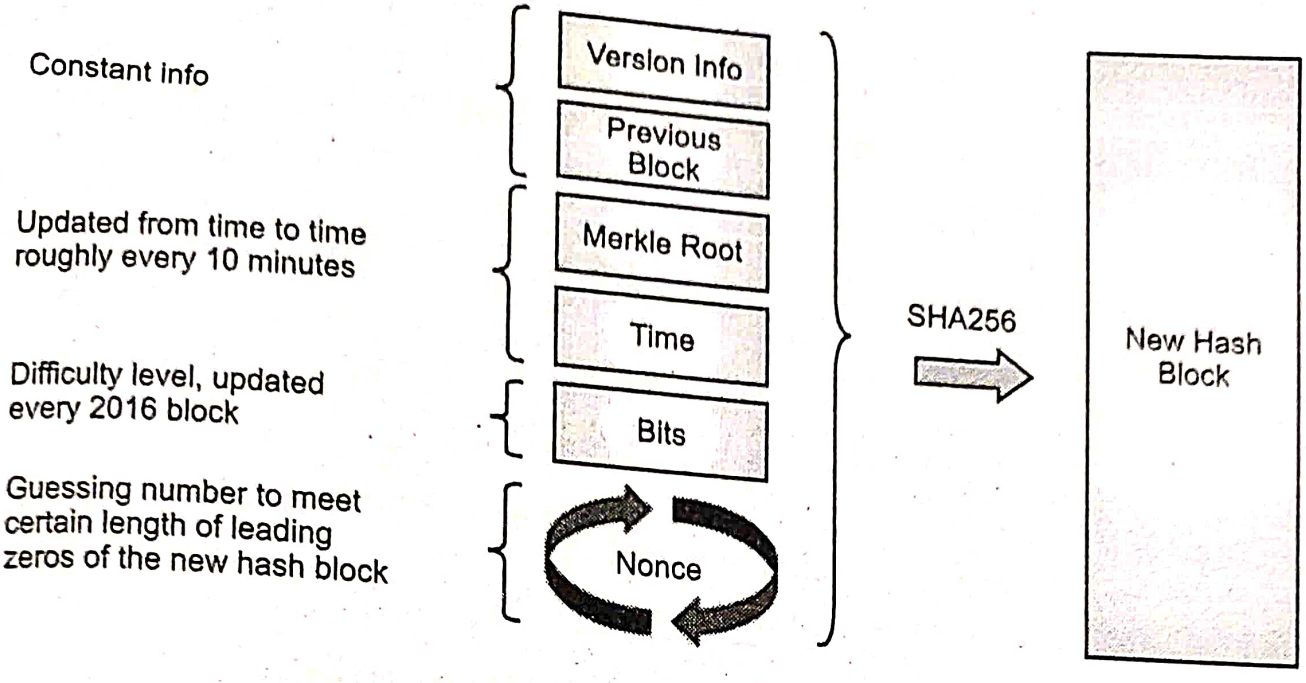


Fig. 2.8 (a): Concept of Nonce

- There will be some constant information, timestamp, hash value with difficulty, and the nonce which when passed through Hash algorithm – SHA256 will become a new block, therefore nonce plays a very important role.
- As we have already discussed, millions of nonce values are tried until the Golden Nonce is found.
- The target hash value is defined as the difficulty and the iterative calculation of the hash value requires the miner's computer resources.
- Only with the correct Nonce value, proof of work can be created and thus giving birth to a new Block in the Block chain.
- **Example:** The miner has to calculate the hash which should be below the target hash assigned to it.
- But it cannot change the Block number, Data, Previous Hash in order to guess a new hash due to the avalanche effect.
- A nonce is a 32-bit number. So there can be a maximum of approximately 4 billion possible Nonce values as 2^(32) = 4, 294, 967, 296.
- The nonce is randomly selected for each iteration. So for each iteration, a random integer between 0 and 4, 294, 967, 296 is selected.

ollowing table:

Block	8896
No. of transactions	1800
Transaction valume	$ 13849673
Timestamp	2017-11-11 01:35:55
Relayed by	ViaBTC
Difficulty	1456324543655.677
Size	1066.34 kB
Nonce	880
Block hash	000abddbcdef673bedb4 ...

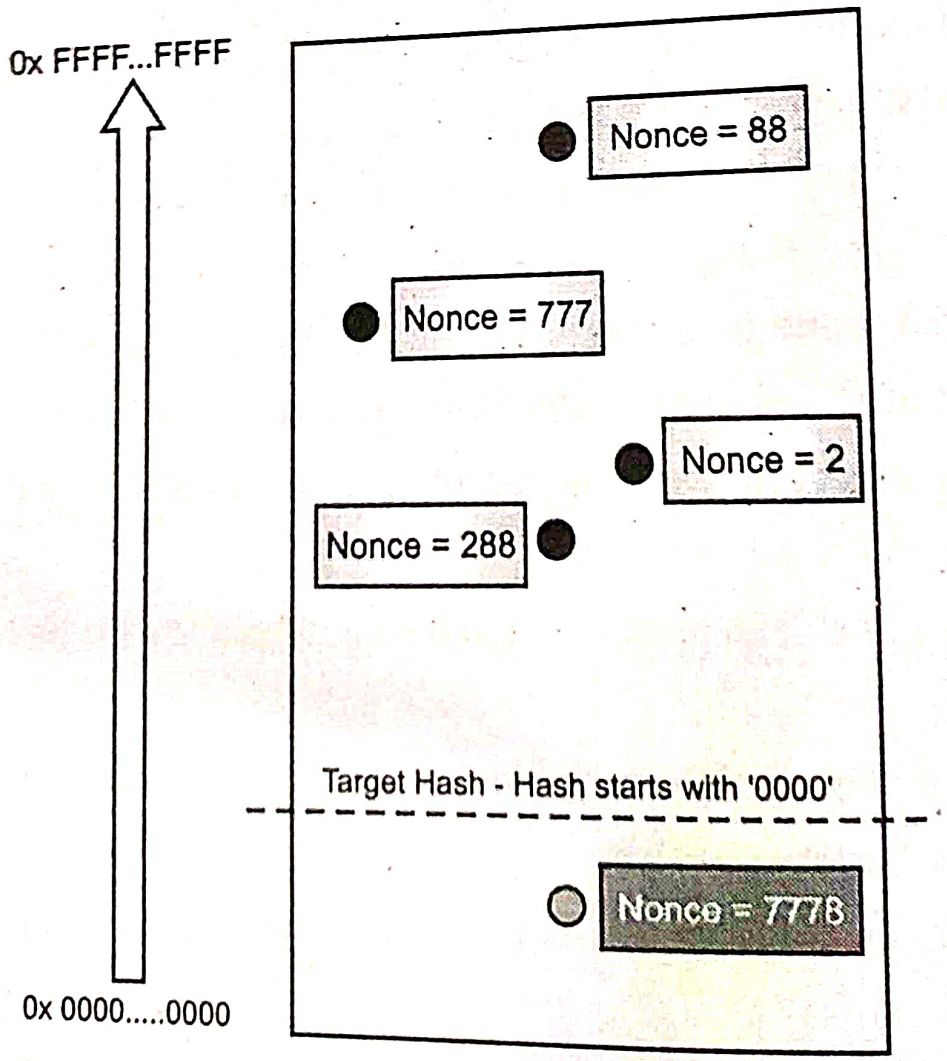


Fig. 2.8 (b): All possible Hashes

In Fig. 2.8 (b) the circles represent a hash value obtained for a particular nonce value. The Black circles imply that a hash calculated is invalid. Green circle represents a valid hash.

The Target assigned to a miner implies that a block can be mined by the miner only if the calculated hash consists of 4 leading zeros here (only as an example. Target hash can vary with multiple leading zeros). All hashes greater than that will be discarded.

We start with a nonce value of 88 which as we can see, yields a hash greater than target hash. The nonce value is changed to 777 and the hash is recalculated.

We repeat the process until we find a nonce which yields a hash whose value is less than the target hash.

According to Fig. 2.8 (b) this happens at Nonce value 7778. Now the block can be authenticated by the miner and added to the Blockchain.

2.4.2 Cryptographic Puzzle

- We knew that Blockchain is an immutable and decentralized ledger that allows transactions to take place without trusted intermediary.
- Blockchain is the sequence of blocks that stores valid transactions. Blockchain technology combined with other cryptographic techniques creates a cryptocurrency, namely Bitcoin.
- To mine Bitcoins and append transactions to the Blockchain, miners solve a cryptographic puzzle.
- In a cryptographic puzzle, miners generate the hash of a newly created block along with a cryptographic nonce. The nonce is varied until the hash value becomes smaller than or equal to the target value.
- The target value is a 256-bit number with initial few zeros (e.g., initial 40 zeros). The cryptographic hash function used in Bitcoin is Secure Hash Function-256 (SHA-256).
- Adding new blocks to the Blockchain (called mining) requires solving a moderately difficult cryptographic puzzle.
- The first miner who solves the puzzle earns some virtual currency (some fresh coins for the mined block, and a small fee for each transaction included therein).
- To construct a new block (mining), a cryptographic puzzle must be solved by the miner, and the user who solves the puzzle first will avail the reward by broadcasting the result in the network.
- The new blocks can be added to the Blockchain only once a miner has solved the puzzle by finding the correct hash for the collection of transactions that he or she selected.

- In order to gain the right to create the next block, a participant (often called a 'miner') has to be the first to solve a cryptographic puzzle. This feature prevents a malicious attack in Blockchian.
- To complete with each other, miners will create a puzzle and who solves the puzzle first is able to add the block of the transaction to the Blockchain.
- The process of solving the cryptographic puzzle is referred to as Proof-of-Work (PoW). PoW is necessary in order to build consensus among miners in the Blockchain network.
- In PoW, the miner with more computational resources has better chance to append its block to the Blockchain ledger by being the first to solve the cryptographic puzzle.
- New blocks can be added to the Blockchain only once a miner has solved the puzzle by finding the correct hash for the collection of transactions that he or she selected.
- The PoW consensus mechanisms required to compute the puzzle are miners to solve complex cryptographic puzzles so they can add a block to the Blockchain.

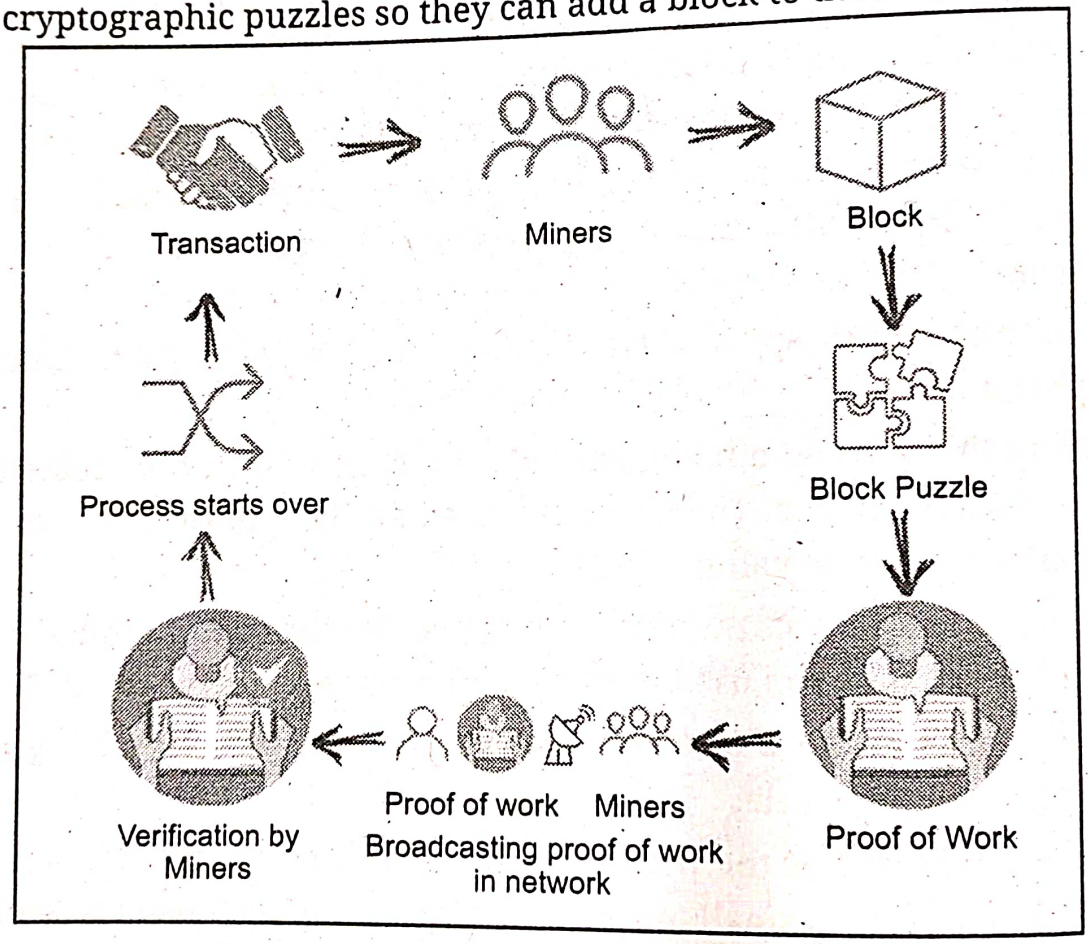


Fig. 2.9: Process of Cryptographic Puzzle

- In a PoW system, network participants have to solve so-called "cryptographic puzzles" to be allowed to add new "blocks" to the Blockchain. This puzzle-solving process is commonly referred to as "mining".
- In simple terms, these cryptographic puzzles are made up out of all information previously recorded on the block and a new set of transactions to be added to the next "block".

- Because the input of each puzzle becomes higher overtime (resulting in a more complex calculation), the PoW mechanism requires a vast amount of computing resources.
- As an example, the puzzle used by the Nakamoto consensus algorithm, is finding a value 'b' such that hash (a, b) < c holds, where hash, 'a' and 'c' are given. The value of 'a' is determined by the last accepted set of state transitions or block while 'c' is set to reflect the difficulty level of the solved puzzle. As any node trivially can check if hash (a, b) < c holds for a given 'b', the puzzle satisfies the properties of being expensive to solve and cheap to verify.

2.5 BYZANTINE FAULT TOLERANCE

- Fault tolerance refers to the ability of a system (computer, network, cloud cluster, etc.) to continue operating without interruption when one or more of its components fail thus affecting Reliability, Availability and Security.
- Byzantine fault tolerance facilitates the distributed computer network to achieve a reasonable consensus correctly even with malicious device nodes deteriorating or sending out incorrect information.
- The objective of Byzantine fault tolerance is to be able to defend against failures of system components with or without symptoms that prevent other components of the system from reaching an agreement among themselves, where such an agreement is needed for the correct operation of the system.
- Byzantine Fault Tolerance (BFT) is the ability of a distributed computer network to function as desired and correctly reach a sufficient consensus despite malicious components (nodes) of the system failing or propagating incorrect information to other peers.
- Byzantine Fault Tolerance (BFT) is one of the features of a distributed network to reach consensus or agreement on the same value even when some of the nodes in the network fail to respond or respond with incorrect data or information.
- BFT mechanism is to safeguard against the system failures by employing collective decision making (both - correct and faulty nodes) which aims to reduce to influence of the faulty nodes.
- Byzantine Fault Tolerance (BFT) in a cryptocurrency is the feature of reaching an agreement or consensus about particular blocks, even when some nodes are failing to respond or giving out malicious values to misguide the network.
- Byzantine fault tolerance is described as the capability of a distributed system to reach an agreement even in the presence of an attacker node in the network sending out misleading information.
- Practical Byzantine Fault Tolerance (PBFT) is a variant of Byzantine Fault Tolerance (BFT) over asynchronous systems.

- Because the input of each puzzle becomes higher overtime (resulting in a more complex calculation), the PoW mechanism requires a vast amount of computing resources.
- As an example, the puzzle used by the Nakamoto consensus algorithm, is finding a value 'b' such that hash (a, b) < c holds, where hash, 'a' and 'c' are given. The value of 'a' is determined by the last accepted set of state transitions or block while 'c' is set to reflect the difficulty level of the solved puzzle. As any node trivially can check if hash (a, b) < c holds for a given 'b', the puzzle satisfies the properties of being expensive to solve and cheap to verify.

2.5 BYZANTINE FAULT TOLERANCE

- Fault tolerance refers to the ability of a system (computer, network, cloud cluster, etc.) to continue operating without interruption when one or more of its components fail thus affecting Reliability, Availability and Security.
- Byzantine fault tolerance facilitates the distributed computer network to achieve a reasonable consensus correctly even with malicious device nodes deteriorating or sending out incorrect information.
- The objective of Byzantine fault tolerance is to be able to defend against failures of system components with or without symptoms that prevent other components of the system from reaching an agreement among themselves, where such an agreement is needed for the correct operation of the system.
- Byzantine Fault Tolerance (BFT) is the ability of a distributed computer network to function as desired and correctly reach a sufficient consensus despite malicious components (nodes) of the system failing or propagating incorrect information to other peers.
- Byzantine Fault Tolerance (BFT) is one of the features of a distributed network to reach consensus or agreement on the same value even when some of the nodes in the network fail to respond or respond with incorrect data or information.
- BFT mechanism is to safeguard against the system failures by employing collective decision making (both - correct and faulty nodes) which aims to reduce to influence of the faulty nodes.
- Byzantine Fault Tolerance (BFT) in a cryptocurrency is the feature of reaching an agreement or consensus about particular blocks, even when some nodes are failing to respond or giving out malicious values to misguide the network.
- Byzantine fault tolerance is described as the capability of a distributed system to reach an agreement even in the presence of an attacker node in the network sending out misleading information.
- Practical Byzantine Fault Tolerance (PBFT) is a variant of Byzantine Fault Tolerance (BFT) over asynchronous systems.

- Practical Byzantine Fault Tolerance emerged as one of the prominent optimizations of BFT in 1999 by Barbara Liskov and Miguel Castro in their academic paper with the title 'Practical Byzantine Fault Tolerance.'
- The primary objective of the practical BFT was to resolve the discrepancies evident in the original BFT consensus mechanism.
- Practical Byzantine Fault Tolerance (PBFT) was designed to optimize BFT for implementation in Blockchain network.
- The PBFT as designed to solve the Byzantine Generals problem for the asynchronous environment. It is based on assumption that less than 30% of total nodes are malicious in network.
- In other words, a minimum of 3f + 1 nodes needs to work, where f is the number of fault replicas. PBFT based Blockchain can tolerate atmost 33% of malicious nodes.
- Decentralized networks are designed such that multiple separate actors can follow a common set of rules in order to achieve a consensus on a single state for the distributed system.
- Byzantine fault tolerance is a measure of the network's ability to defend against failures that make it more difficult to achieve a consensus. Some examples of possible Byzantine failures are:
  1. Hardware components crashing or breaking.
  2. Network congestion and disconnection.
  3. Requests are processed incorrectly.
  4. Local states (the system states of one of the actors) are corrupted.
  5. Producing incorrect or inconsistent outputs.
  6. Malicious attacks from individuals or groups in the network.
  7. Respond with an incorrect result.
  8. Respond with a deliberately misleading result.
- Byzantine Fault Tolerance (BFT) is a consensus protocol that is not only able to tolerate failures in the computing systems on the network; it is also able to withstand corrupted data and malicious attacks.
- What BFT does is ensure that every node receives the same guaranteed data. This is why even faulty devices or malicious attacks are unable to breach the protocol.
- In simpler words, as long as two-thirds of the nodes are safe, consistency of consensus can be ensured.
- The credit for the development of BFT goes to Robert Shostak, Leslie Lamport and Marshall Pease, who first proposed the Byzantine General's problem.
- To understand this problem, imagine a group of Byzantine generals, leading their respective armies in preparation of an attack.

- To win the battle, the generals will need to coordinate their attack so that all attacks occur simultaneously. Now, if even one of the generals is a traitor, how will they coordinate their attack?

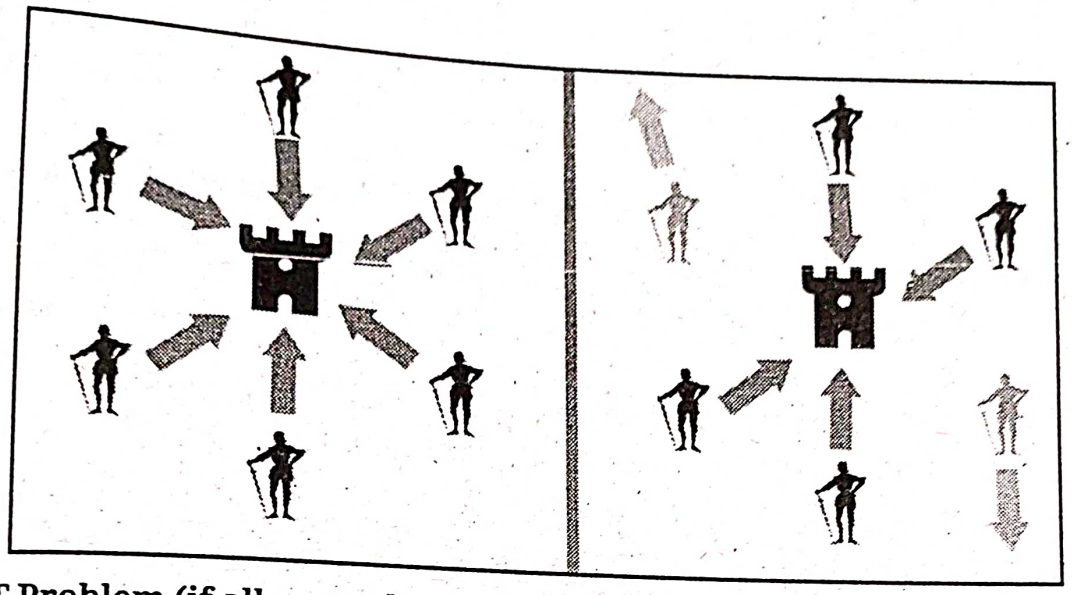


Fig. 2.10: BFT Problem (if all generals attack in coordination, the battle is won (left) and if two generals falsely declare that they intend to attack, but instead retreat, the battle is lost (right))

- This situation can be extrapolated to the Blockchain consensus mechanism. Here too, one bad actor could compromise the achievement of consensus.
- BFT takes care of this by using an algorithm through which consensus can be achieved even if only two-thirds of the nodes are in agreement.
- Using BFT, no single point of failure or uncoordinated bad actors can impact consensus.

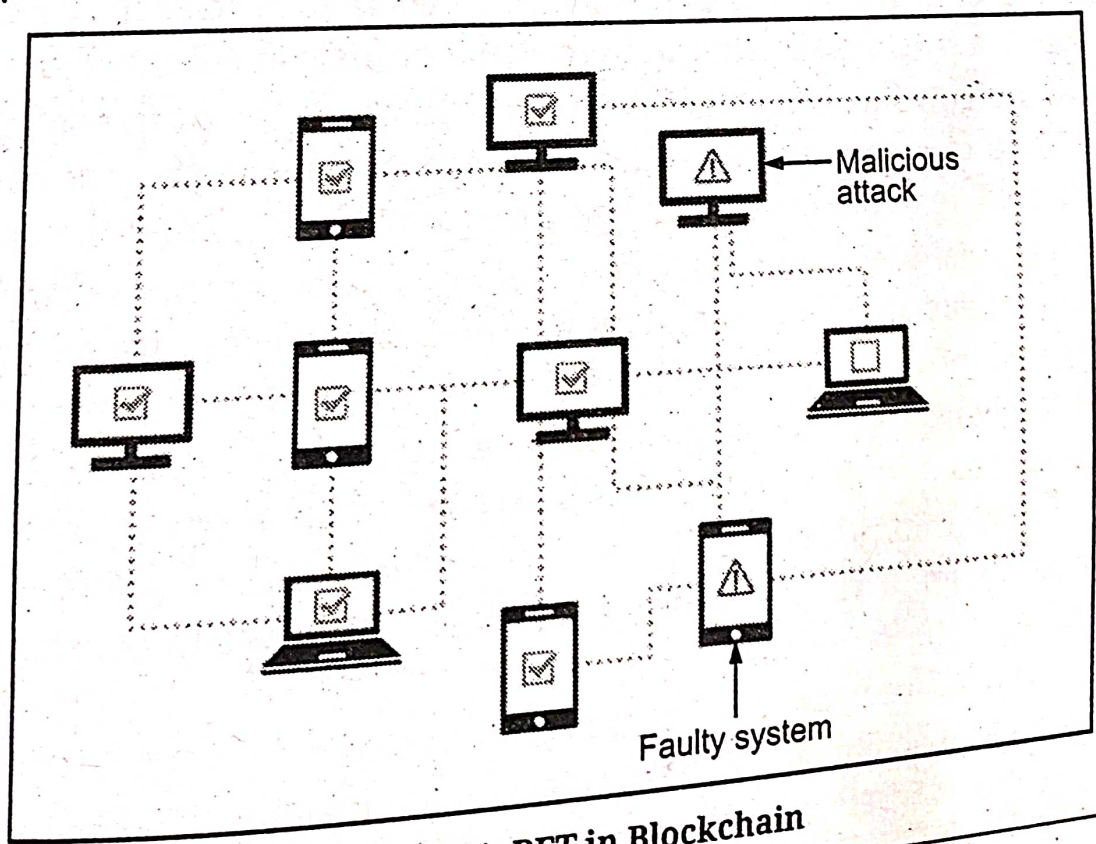


Fig. 2.11: BFT in Blockchain

2.6 CONSENSUS PROTOCOLS

- The consensus algorithm/protocol is an important component of Blockchain technology. A consensus mechanism refers to any number of methodologies used to achieve agreement, trust and security across a decentralized computer network.
- Blockchain as a distributed ledger technology has received extensive research attention.
- In addition to cryptography and P2P (peer-to-peer) technology, consensus protocols are also a fundamental part of the Blockchain technology.
- A good consensus protocol can guarantee the fault tolerance and security of the Blockchain systems.
- A consensus in a Blockchain is a set of rules to be followed to maintain a Blockchain. Consensus used in Blockchain to achieve an agreement on adding new data value in distributed servers or node in the network.
- Blockchain consensus plays a very important role in a Blockchain, basically its purpose to achieve agreement among the nodes in the distributed network.
- Consensus protocols form the backbone of Blockchain by helping all the nodes in the network verify the transactions.
- Blockchain functions work as in a decentralized manner and records large volume transactions in real-time, so there are so many issues or complexity of what is the truth is.
- The key is to get consensus one way or another, or else malicious things like double-spending attacks can occur. To handle this consensus algorithm comes in.
- A consensus algorithm is a mechanism in computer science used to establish agreement on a single data value across systems or distributed processes.
- A consensus algorithm is a protocol through which all the parties of the Blockchain network come to a common agreement (consensus) on the present data state of the ledger and be able to trust unknown peers in a distributed computing environment.
- In Blockchain networks, the consensus algorithms are an most important element because consensus algorithm maintain the integrity and security of these distributed computing systems.
- Consensus means "general agreement", general agreement needed to record information, such as balance of every address and transactions on the Blockchain.
- Consensus algorithm/protocol is open source, decentralized platform and decision-making process for a group, where individuals of the group construct and support decision for that works.
- Being a on the Blockchain called a distributed ledger network. The most commonly used consensus mechanisms for Blockchain technologies are Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS).

2.6.1 Proof of Work (PoW)

- The Proof-of-Work (PoW) is a common consensus algorithm used by the most popular cryptocurrency networks like Bitcoin and Litecoin.
- It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain.
- However, this whole mining mechanism of Bitcoin needs high energy consumption and a longer processing time.
- Proof of Work (PoW) is the process of building a cryptographic hash, and the concept was first introduced in 1993 by Cynthia Dwork and Moni Naor. It is reintroduced by Satoshi Nakamoto in the Bitcoin whitepaper in 2008.
- Proof of Work in Blockchain systems historically originates from its use in Hashcash, which was conceived by Adam Back as a system to limit email spam and denial-of-service attacks.
- The PoW system, Blockchain validators take data from a block header as an input, and continuously run it through a cryptographic hash function.
- Validators hash negligible variations of the input data by including an arbitrary random number called a nonce every time the input data is run through the cryptographic hash function.
- Proof of work i.e. PoW needs high levels of electricity of processing power to resolve that what data gets added to the next block in a Blockchain.
- Specialized computers called ASICs are required to compute complex mathematical problems needed for the PoW system.
- The PoW is a common consensus algorithm used by the cryptocurrency networks like Bitcoin and Litecoin.
- It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain.
- This whole mining mechanism of bitcoin needs high energy consumption and longer processing time.
- Fig. 2.12 shows mechanism of PoW.
- PoW is a consensus algorithm that uses a cryptographic hashing puzzle to make sure that a certain amount of work has been done before a block is created. Bitcoin's PoW uses the SHA-256 has function to create a hashing puzzle.
- Blocks in a Blockchain network are created by a special type of validator node called a miner.
- These miner nodes complete with each other to solve the hashing puzzle in order to produce a block to be appended to the ledger.
- Blockchain miners will start to solve the hashing puzzle whenever they have data (often, a set of transactions) that needs to be included in a block.

2.6.1 Proof of Work (PoW)

- The Proof-of-Work (PoW) is a common consensus algorithm used by the most popular cryptocurrency networks like Bitcoin and Litecoin.
- It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain.
- However, this whole mining mechanism of Bitcoin needs high energy consumption and a longer processing time.
- Proof of Work (PoW) is the process of building a cryptographic hash, and the concept was first introduced in 1993 by Cynthia Dwork and Moni Naor. It is reintroduced by Satoshi Nakamoto in the Bitcoin whitepaper in 2008.
- Proof of Work in Blockchain systems historically originates from its use in Hashcash, which was conceived by Adam Back as a system to limit email spam and denial-of-service attacks.
- The PoW system, Blockchain validators take data from a block header as an input, and continuously run it through a cryptographic hash function.
- Validators hash negligible variations of the input data by including an arbitrary random number called a nonce every time the input data is run through the cryptographic hash function.
- Proof of work i.e. PoW needs high levels of electricity of processing power to resolve that what data gets added to the next block in a Blockchain.
- Specialized computers called ASICs are required to compute complex mathematical problems needed for the PoW system.
- The PoW is a common consensus algorithm used by the cryptocurrency networks like Bitcoin and Litecoin.
- It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain.
- This whole mining mechanism of bitcoin needs high energy consumption and longer processing time.
- Fig. 2.12 shows mechanism of PoW.
- PoW is a consensus algorithm that uses a cryptographic hashing puzzle to make sure that a certain amount of work has been done before a block is created. Bitcoin's PoW uses the SHA-256 has function to create a hashing puzzle.
- Blocks in a Blockchain network are created by a special type of validator node called a miner.
- These miner nodes complete with each other to solve the hashing puzzle in order to produce a block to be appended to the ledger.
- Blockchain miners will start to solve the hashing puzzle whenever they have data (often, a set of transactions) that needs to be included in a block.

- Fig. 2.12 shows the basic structure of a block header used a Proof of Work (PoW)-based Blockchain application.
- A puzzle solver will create a hash value of the header, generally using the SHA-256 has function. The puzzle here is to find a has value for the header so that the hash beings with a known number of zero bits.

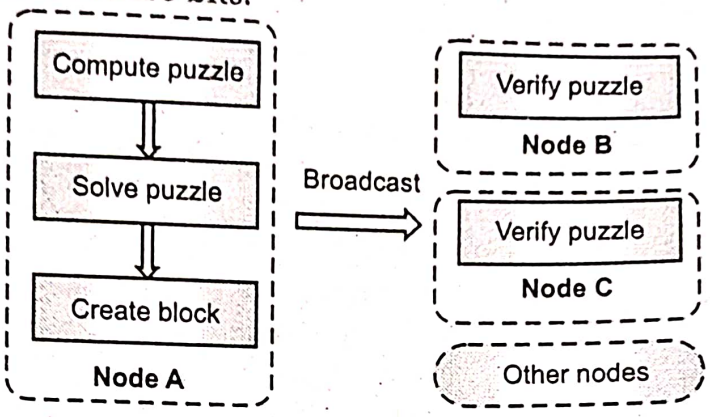


Fig. 2.12: Consensus Mechanism of PoW

- **Pros of PoW:** Highest scalability and security; serves as one of consensus smart contracts' best practices.
- **Cons of PoW:** Low performance, lot of power wasted.

2.6.2 Proof of Stake (PoS)

- Proof of Stake (PoS) protocols are the consensus mechanisms for Blockchains that work by selecting validators in proportion to their quantity of holdings in the associated cryptocurrency.
- PoS are proof of stake consensus algorithms used by cryptocurrencies to validate blocks.
- The purpose is like proof of work, but a different way to verify and validate the transactions or blocks. Once the user is selected to validate the block and accurately verify all transactions in that block.
- The PoS is another common consensus algorithm that evolved as a low-cost, low-energy consuming alternative to the PoW algorithm.
- It involves the allocation of responsibility in maintaining the public ledger to a participant node in proportion to the number of virtual currency tokens held by it.
- However, this comes with the drawback that it incentivizes cryptocoin hoarding instead of spending. PoS consensus algorithm was created in 2011 as an alternative to PoW.
- PoS and PoW have similar objectives; they have some fundamental differences and features, especially during the validation of new blocks on the blockchain network.
- The Proof of Stake (PoS) consensus algorithm differs with the PoW mining consensus with a mechanism where blocks are validated based on the stake of the network participants.

- Here, unlike running hash functions, validators stake resources primarily in the form of digital money or tokens.
- The validator of every block is then randomly selected from the stakeholders based on the amount of computational power allocated.
- Proof of Stake (PoS) system may execute the algorithm in different ways, in general, the Blockchain is secured by a pseudo-random election process that considers a nodes allocation and the allocation determining the commitment of the party to ensure the network.
- The Ethereum Blockchain, which is the world's largest Blockchain network in terms of developer activity has initiated to switch from PoW algorithm PoS in an attempt to increase the networks scalability and reduce excessive electricity wastage.
- **Pros of PoS:** High performance, scalability, smart-contract support, increased protection from malicious attack.
- **Cons of PoS:** Medium security, nothing-at-stake problem.

2.6.3 Defense against Attackers

- With the fact that cybercrime and cyber security attacks hardly seem to be out of the news these days and the threat is growing globally.
- A Blockchain system is protected with the help of ledgers and cryptographic keys, attacking and manipulating it becomes extremely difficult.
- For a blockchain system to be penetrated, the attacker must intrude into every system on the network to manipulate the data that is stored on the network.
- Blockchain technology enables decentralization through the participation of members across a distributed network.
- There is no single point of failure and a single user cannot change the record of transactions. However, Blockchain technologies differ in some critical security aspects.
- When building an enterprise Blockchain application, it's important to consider security at all layers of the technology stack, and how to manage governance and permissions for the network.
- A comprehensive security strategy for an enterprise Blockchain solution includes using traditional security controls and technology-unique controls.
- Fig. 2.13 shows different possibilities in Blockchain technology.
- A Blockchain derives its safety advantages from its nodes/peers, which are decentralized in nature, where each node has a copy of validated transactions. As a result, one of the parties cannot alter or modify the ledger.
- Blockchain safety can be described as a defense against central, external, malicious and unintended attacks to transaction data and information in one block (any type of data).
- Generally, risk identification, threat prevention, effective threat mitigation utilizing security policies, equipment and IT infrastructure are included in this defense.

- Here, unlike running hash functions, validators stake resources primarily in the form of digital money or tokens.
- The validator of every block is then randomly selected from the stakeholders based on the amount of computational power allocated.
- Proof of Stake (PoS) system may execute the algorithm in different ways, in general, the Blockchain is secured by a pseudo-random election process that considers a nodes allocation and the allocation determining the commitment of the party to ensure the network.
- The Ethereum Blockchain, which is the world's largest Blockchain network in terms of developer activity has initiated to switch from PoW algorithm PoS in an attempt to increase the networks scalability and reduce excessive electricity wastage.
- Pros of PoS: High performance, scalability, smart-contract support, increased protection from malicious attack.
- Cons of PoS: Medium security, nothing-at-stake problem.

2.6.3 Defense against Attackers

- With the fact that cybercrime and cyber security attacks hardly seem to be out of the news these days and the threat is growing globally.
- A Blockchain system is protected with the help of ledgers and cryptographic keys, attacking and manipulating it becomes extremely difficult.
- For a blockchain system to be penetrated, the attacker must intrude into every system on the network to manipulate the data that is stored on the network.
- Blockchain technology enables decentralization through the participation of members across a distributed network.
- There is no single point of failure and a single user cannot change the record of transactions. However, Blockchain technologies differ in some critical security aspects.
- When building an enterprise Blockchain application, it's important to consider security at all layers of the technology stack, and how to manage governance and permissions for the network.
- A comprehensive security strategy for an enterprise Blockchain solution includes using traditional security controls and technology-unique controls.
- Fig. 2.13 shows different possibilities in Blockchain technology.
- A Blockchain derives its safety advantages from its nodes/peers, which are decentralized in nature, where each node has a copy of validated transactions. As a result, one of the parties cannot alter or modify the ledger.
- Blockchain safety can be described as a defense against central, external, malicious and unintended attacks to transaction data and information in one block (any type of data).
- Generally, risk identification, threat prevention, effective threat mitigation utilizing security policies, equipment and IT infrastructure are included in this defense.

- Below are some important security concepts and principles in Blockchain:
  1. **Penetration Security:** It is a technique involving multiple data protection corrections. This supports the idea that data protection is more effective across multiple layers than in a single safety layer.
  2. **Maximum Prerogative:** Access to information is limited to the lowest possible level in this approach, thereby improving a high degree of trust.
  3. **Vulnerabilities Detection:** To verifies and manages vulnerabilities through identification, authentication, modification and patching.
  4. **Risk Management:** By detecting, assessing and managing threats, this approach measures danger within a system.
  5. **Patches Control:** By purchasing, reviewing and deploying updates, this technique patches the faulty part as software, program, operating system, firmware etc.
- Blockchain technology implements a number of techniques to ensure transaction information protection and block details irrespective of the block's use as well as results.
- Some use the authentication method for data security, for instance, for Bitcoin, Tschorsch and Scheuermann.

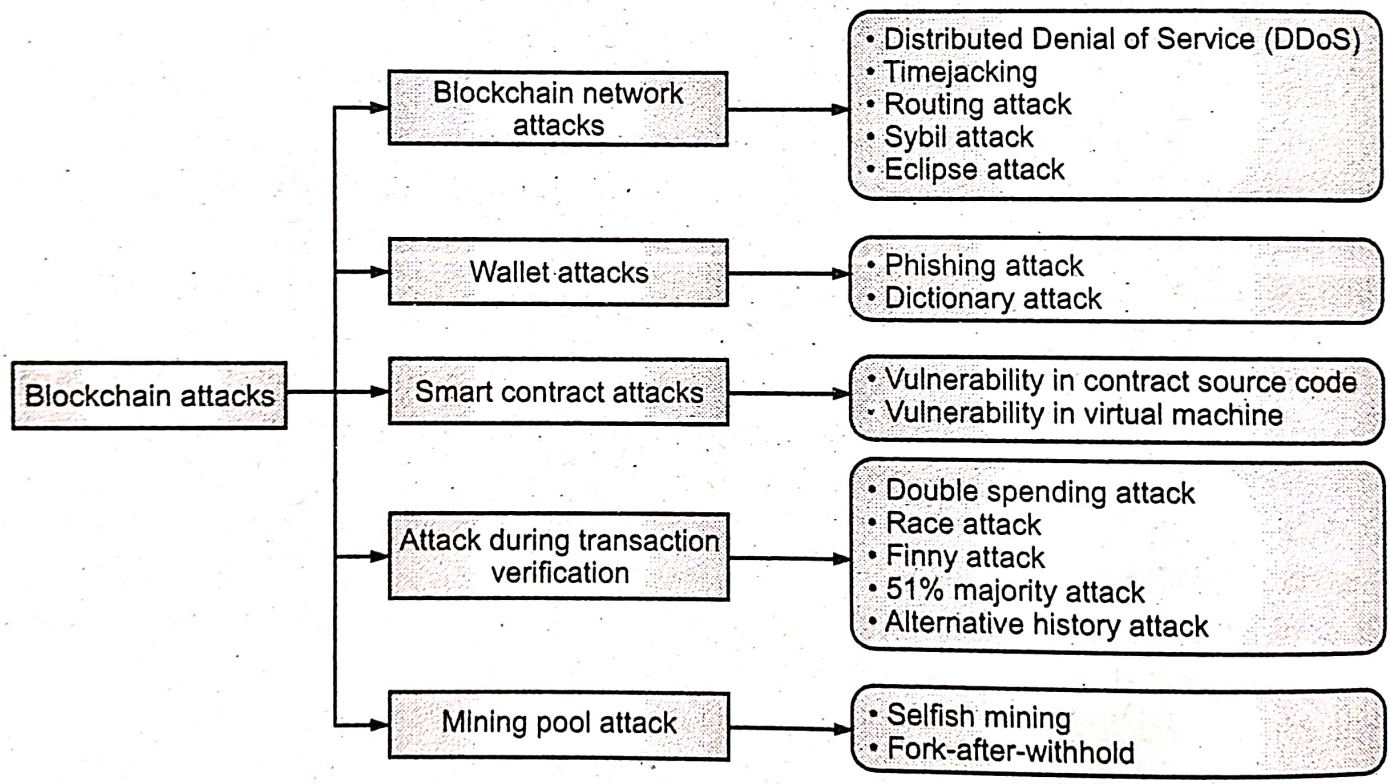


Fig. 2.13

2.6.4 Competing Chains

- Blockchain forks are an important concept in Blockchain. A fork refers to competing or coexisting side chains within the same network.
- Simply, because of the decentralized structure of the network, the occurrence of forks seems to be natural.

- Blocks are propagated through the network and arrive at different nodes at different times. This is can also be the cause of the so-called orphan blocks.
- Although the longest Blockchain becomes the distributed ledger of record which is then adopted by all computer nodes, distinct blocks will occasionally be added (near) simultaneously creating a 'fork' (two competing chains).
- One of these chains will ultimately be discarded, for example if another block is successfully added to the second chain it will become clear that the second Blockchain is longer.
- Consequently, the block on the first shorter chain will become 'orphaned'. The transactions in the orphaned block will need to be incorporated into the longer chain that has ultimately become the ledger of record, delaying the validation of these orphaned transactions.
- Normally, the nodes will try to extent the chain with the largest cumulative difficulty. We can take about a fork when there are two or more candidate blocks that are competing with one another to form the longest chain.
- If a miner discovers a "correct" block, it is immediately sent to its neighbors. Several nodes can in time discover a different solution and broadcast this through the network.
- These nodes closest to the original miners of the block will start building their chain based on this block and continue working on next blocks. If a fork comes into existence this way, the issue is normally resolved within one block.
- The reason is that one group of miners will find a next solution first, even if the computer power within the network is evenly distributed among the several competing groups.
- The next solution will be shared among the network nodes, accepted and spread through the network.
- The competing nodes will receive this next solution, accept it and stop working on the competing solution, thereby resolving the fork.
- Competing chains are two different sides of the network that hold two different chains, and attempt to extend them further.
- At some point, some miner will solve the hash puzzle, and we will propagate his next new valid block.

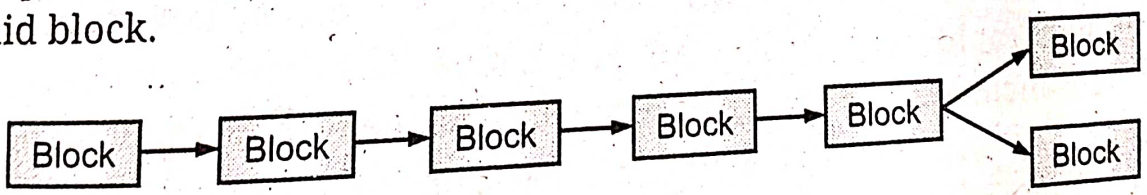


Fig. 2.14: A 'Fork' occurs when Two Blocks are formed at the Same Time

2.7 BLOCKCHAIN DEMO

- A general idea of how blocks are generated and what the relationship is between transactions and blocks.

How Blockchains accumulate Blocks?

- The steps for accumulation of blocks are explained below:
  1. A node starts a transaction by signing it with its private key.
  2. The transaction is propagated (flooded) by using much desirable Gossip protocol to peers, which validates the transaction based on pre-set criteria. Usually, more than one node is required to validate the transactions.
  3. Once, the transaction is validated, it is included in a block, which is then propagated on to the network. At this point, the transaction is considered confirmed.
  4. The newly created block now becomes part of the ledger and the next block links itself cryptographically back to this block. This link is a hash pointer. At this stage, the transaction gets itssecond confirmation and the block gets its first.
  5. Transactions are then reconfirmed every time a new block is created. Usually, six confirmations in the Bitcoin networkare required to consider the transaction final. Steps 4 and 5 can be considered non-compulsory as the transaction itself is finalized in step 3; however, block confirmation and further transaction reconfirmations, if required are then carried out in Steps 4 and 5.

Tiers of Blockchain Technology:

- It is envisaged that, due to the rapid development and progress made in Blockchain technology, many applications will evolve over time.
- Some have already been realized while some can be envisioned for the future based on the current rate of advancement in the Blockchain technology.
- First, the threelevels discussed below were originally described by Melanie Swan in her book Blockchain, Blueprint for a New Economy as tiers of Blockchain categorized on the basis of applications in each category.
- In addition tothis, Tier X or Generation X is discussed later. This is what the author thinks will become a reality when the Blockchain technology becomes advanced enough.
- **Blockchain 1.0:** This was introduced with the invention of Bitcoin and is basically used for cryptocurrencies. Also, as Bitcoin was the first implementation of cryptocurrencies it makes sense to categorize Generation 1 of Blockchain technology to only include cryptographic currencies. All alternative coins and bitcoin fall into this category. This includes core applications such as payments and applications.
- **Blockchain 2.0:** Generation 2.0 Blockchains are used by financial services and contracts are introduced in this generation. This includes various financial assets, For example derivatives, options, swaps, and bonds. Applications that are beyond currency, finance, and markets are included at this tier.
- **Blockchain 3.0:** Generation 3 Blockchains are used to implement applications beyond the financial services industry and are used in more general purpose industries such as government, health, media, the arts, and justice.

- **Generation X (Blockchain X):** This is a vision of Blockchain singularity where one day we will have a public Blockchain service available that anyone can use just like the Google search engine. It will provide services in all realms of society. This is a public open distributed ledger with general purpose rational agents (Machina Economicus) running on Blockchain, making decisions and interacting with other intelligent autonomous agents on behalf of humans and regulated by code instead of law or paper contracts.

Case Study:

- Car companies make leasing a vehicle look easy, but in reality, it can be quite complicated.
- A significant challenge faced by today's car leasing networks is that even though the physical supply chain is usually integrated, the supporting systems are often fragmented.
- Each party within the network maintains its own ledger, which can take days or weeks to synchronize.

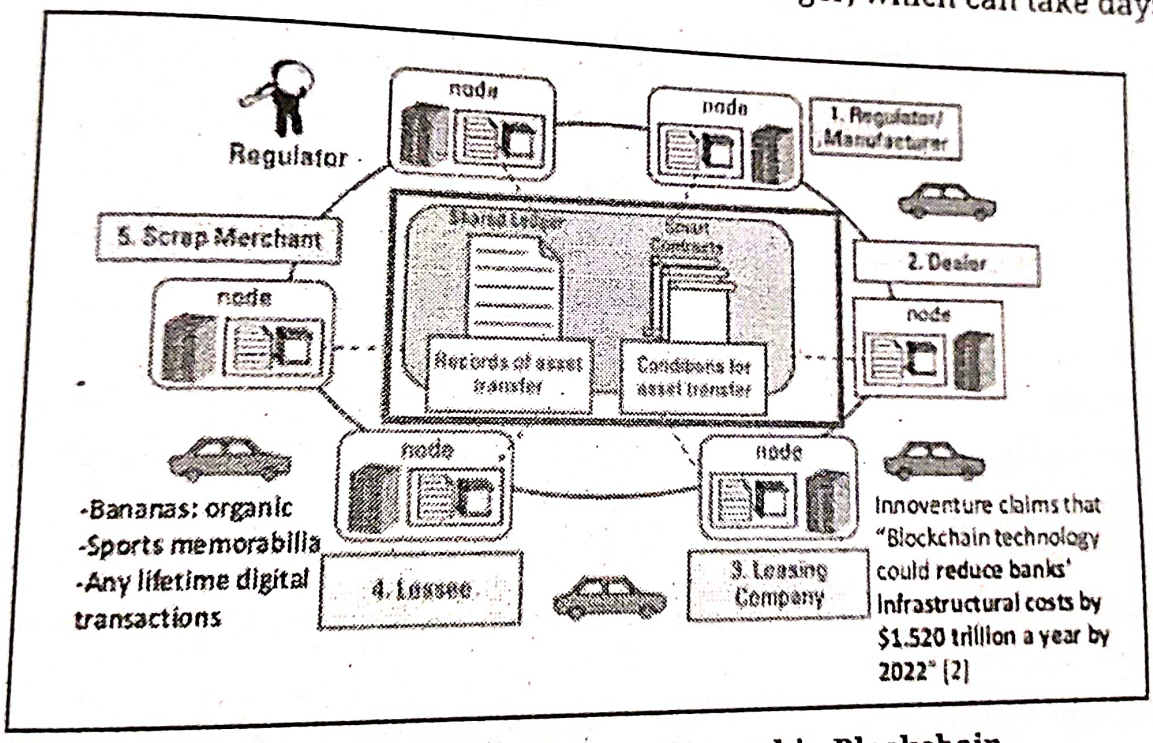


Fig. 2.15: Tracking Vehicle Ownership Blockchain

- By using a shared ledger on a Blockchain network, every partici- pant can access, monitor, and analyze the state of the vehicle irrespective of where it is within its life cycle.
- Blockchain, network participants can interact as follows:
  - The government regulator creates and populates the registration for the new vehicle on the Blockchain and transfers the ownership of the vehicle to the manufacturer.
  - The manufacturer adds the make, model, and vehicle identification number to the vehicle template within the parameters allowed by the smart contract (a digital agreement or set of rules that govern a transaction).

- **Generation X (Blockchain X):** This is a vision of Blockchain singularity where one day we will have a public Blockchain service available that anyone can use just like the Google search engine. It will provide services in all realms of society. This is a public open distributed ledger with general purpose rational agents (Machina Economicus) running on Blockchain, making decisions and interacting with other intelligent autonomous agents on behalf of humans and regulated by code instead of law or paper contracts.

Case Study:

- Car companies make leasing a vehicle look easy, but in reality, it can be quite complicated.
- A significant challenge faced by today's car leasing networks is that even though the physical supply chain is usually integrated, the supporting systems are often fragmented.
- Each party within the network maintains its own ledger, which can take days or weeks to synchronize.

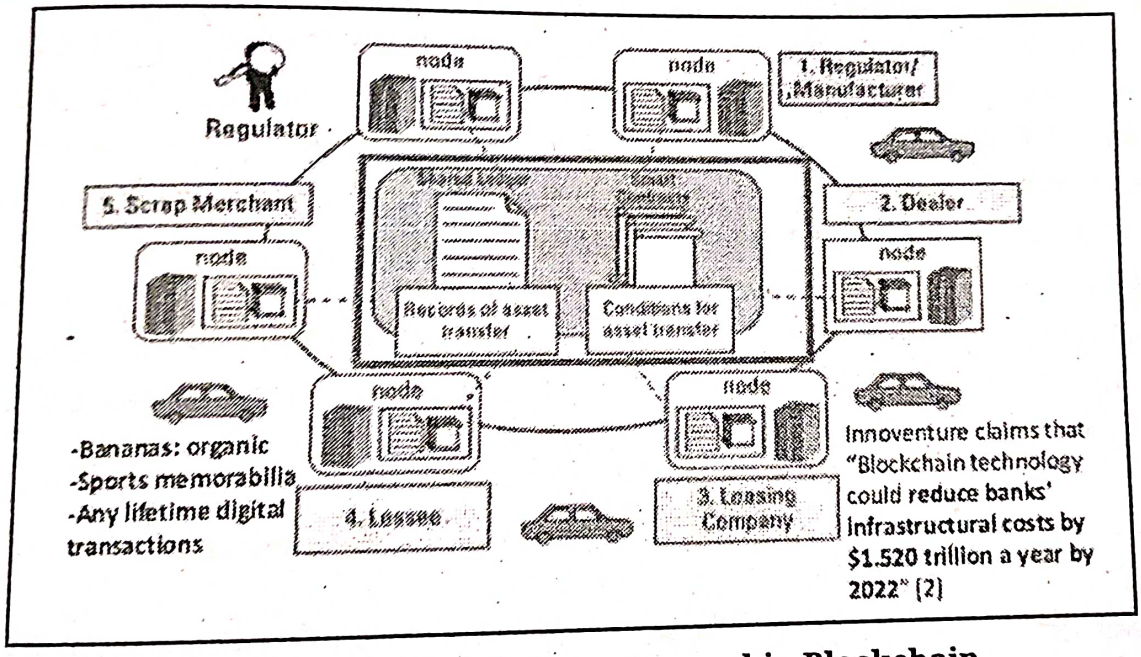


Fig. 2.15: Tracking Vehicle Ownership Blockchain

- By using a shared ledger on a Blockchain network, every partici- pant can access, monitor, and analyze the state of the vehicle irrespective of where it is within its life cycle.
- Blockchain, network participants can interact as follows:
  - The government regulator creates and populates the registration for the new vehicle on the Blockchain and transfers the ownership of the vehicle to the manufacturer.
  - The manufacturer adds the make, model, and vehicle identification number to the vehicle template within the parameters allowed by the smart contract (a digital agreement or set of rules that govern a transaction).

- The dealer can see the new stock availability, and ownership of the vehicle can be transferred from the manufacturer to the dealership after a smart contract is executed to validate the sale.
- The leasing company can see the dealer's inventory.
- Ownership of the vehicle can be transferred from the dealer to the leasing company after a smart contract is executed to validate the transfer.
- The lessee can see the cars available for lease and complete any form required to execute the lease agreement.
- The leasing process continues between various lessees and the leasing company until the leasing company is ready to retire the vehicle.
- At this point, ownership of the asset is transferred to the scrap merchant, who, according to another smart contract, has permission to dispose of the vehicle.

PRACTICE QUESTIONS

Q.I Multiple Choice Questions:

1. Which is a distributed database of records of all digital event or transactions that have been executed and shared among participating parties?
   (a) Blockchain (b) Digital ledger
   (c) Smart contracts (d) None of the mentioned
2. The process of new coin generation is called as,
   (a) chaining (b) blocking
   (c) mining (d) None of the mentioned
3. Which means taking an input as a string of any length and giving output of a fixed size length?
   (a) Forking (b) Hashing
   (c) Mining (d) None of the mentioned
4. SHA-1 produces a hash value of,
   (a) 256 bits (b) 160 bits
   (c) 180 bits (d) 128 bits
5. What is the number of round computation steps in the SHA-256 algorithm?
   (a) 80 (b) 76
   (c) 64 (d) 70
6. In SHA-512, the message is divided into blocks of size ____ bits for the hash computation.Which is the top most layer in OSI model and TCP/IP model?
   (a) 1024 (b) 512
   (c) 256 (d) 1248
7. A hash function takes an input string with,
   (a) numbers (b) alphabets
   (c) media files (d) All of the mentioned

8. The fixed-length output is called as a,
   (a) hash
   (b) data value
   (c) Bitcoin
   (d) None of the mentioned
9. Which hashing algorithm used by Bitcoin Blockchain?
   (a) SHA-128
   (b) SHA-256
   (c) SHA-512
   (d) None of the mentioned
10. A Blockchain is an _____ for recording transactions means when a transaction is inserted in block in Blockchain it become permanent and cannot be modified/changed/updated.
    (a) immutable ledger
    (b) mutable ledger
    (c) digital ledger
    (d) None of the mentioned
11. Which of the following is used to ensure consensus in Bitcoin framework?
    (a) PoS (Proof of Stake)
    (b) PoW (Proof of Work)
    (c) Proof of Concept (PoC)
    (d) None of the mentioned
12. What does a block in a blockchain consists of?
    (a) Hash, timestamp, transactions
    (b) Hash, IP of owner, transactions
    (c) Hash name, transactions, nonce
    (d) None of the mentioned
13. A blockchain system is protected with the help of ledgers and cryptographic _____, attacking and manipulating it becomes extremely difficult.
    (a) hash
    (b) ledger
    (c) keys
    (d) nonce
14. Which protocols are a class of consensus mechanisms for Blockchains that work by selecting validators in proportion to their quantity of holdings in the associated cryptocurrency?
    (a) Proof of Stake (PoS)
    (b) Proof of Work (PoW)
    (c) Proof of Capacity (PoC)
    (d) All of the mentioned
15. Which is refers to a number or value that can only be used once?
    (a) Data
    (b) Hash
    (c) Nonce
    (d) All of the mentioned
16. Which is a decentralized and distributed network communications model that consists of a group of devices or nodes that store and share data or files where each node acts as an individual peer?
    (a) client-server
    (b) peer-to-peer
    (c) Both (a) and (b)
    (d) None of the mentioned
17. Which protocols form the backbone of Blockchain by helping all the nodes in the network verify the transactions.
    (a) Hash
    (b) Network
    (c) Consensus
    (d) None of the mentioned

8. The fixed-length output is called as a,
   (a) hash
   (b) data value
   (c) Bitcoin
   (d) None of the mentioned
9. Which hashing algorithm used by Bitcoin Blockchain?
   (a) SHA-128
   (b) SHA-256
   (c) SHA-512
   (d) None of the mentioned
10. A Blockchain is an _____ for recording transactions means when a transaction is inserted in block in Blockchain it become permanent and cannot be modified/changed/updated.
    (a) immutable ledger
    (b) mutable ledger
    (c) digital ledger
    (d) None of the mentioned
11. Which of the following is used to ensure consensus in Bitcoin framework?
    (a) PoS (Proof of Stake)
    (b) PoW (Proof of Work)
    (c) Proof of Concept (PoC)
    (d) None of the mentioned
12. What does a block in a blockchain consists of?
    (a) Hash, timestamp, transactions
    (b) Hash, IP of owner, transactions
    (c) Hash name, transactions, nonce
    (d) None of the mentioned
13. A blockchain system is protected with the help of ledgers and cryptographic _____, attacking and manipulating it becomes extremely difficult.
    (a) hash
    (b) ledger
    (c) keys
    (d) nonce
14. Which protocols are a class of consensus mechanisms for Blockchains that work by selecting validators in proportion to their quantity of holdings in the associated cryptocurrency?
    (a) Proof of Stake (PoS)
    (b) Proof of Work (PoW)
    (c) Proof of Capacity (PoC)
    (d) All of the mentioned
15. Which is refers to a number or value that can only be used once?
    (a) Data
    (b) Hash
    (c) Nonce
    (d) All of the mentioned
16. Which is a decentralized and distributed network communications model that consists of a group of devices or nodes that store and share data or files where each node acts as an individual peer?
    (a) client-server
    (b) peer-to-peer
    (c) Both (a) and (b)
    (d) None of the mentioned
17. Which protocols form the backbone of Blockchain by helping all the nodes in the network verify the transactions.
    (a) Hash
    (b) Network
    (c) Consensus
    (d) None of the mentioned

18. Consensus protocols form the backbone of Blockchain by helping all the nodes in the network verify the transactions.
    (a) client-server
    (b) peer-to-peer
    (c) Both (a) and (b)
    (d) None of the mentioned
19. Consensus protocols form the backbone of Blockchain by helping all the nodes in the network verify the transactions.
    (a) client-server
    (b) peer-to-peer
    (c) Both (a) and (b)
    (d) None of the mentioned
20. Which of these facts about a ledger is not correct?
    (a) a ledger is used purely for the reporting of cash
    (b) a ledger consists of transactions, often governed by contracts
    (c) a ledger is a system of record
    (d) a ledger describes the inputs and outputs of a business

Answers

1. (a)	2. (c)	3. (b)	4. (b)	5. (c)	6. (a)	7. (d)	8. (a)	9. (b)	10. (a)
11. (b)	12. (a)	13. (c)	14. (a)	15. (c)	16. (b)	17. (c)	18. (b)	19. (b)	20. (a)

Q.II Fill in the Blanks:

1. The property of consistency is preserved in blockchain by maintaining a local copy of the _____ information.
2. The current cryptographic _____ hash algorithm used in Bitcoin.
3. Bitcoin was introduced by _____ in 2008.
4. Bitcoins are created as a reward for a process known as _____.
5. Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a _____.
6. In Bitcoin case, Blockchain is used in a _____way.
7. _____is the term for when Blockchain splits.
8. Prevents double spending is the purpose of _____.
9. _____ is a transaction and block verification protocol
10. _____ characteristic makes Blockchain tamper-proof.
11. A _____ Blockchain uses SHA-256 (Secure Hash Algorithm) hashing algorithm.
12. _____ system, Blockchain validators take data from a block header as an input, and continuously run it through a cryptographic hash function.
13. In a cryptographic _____, miners generate the hash of a newly created block along with a cryptographic nonce.
14. _____, protocol is used to allocate blocks to miners on the network.

Answers

1. global	2. SHA-256	3. Satoshi Nakamoto	4. mining
5. Blockchain	6. decentralized	7. fork	8. nonce
9. PoS	10. immutability	11. Bitcoin's	12. PoW
13. puzzle	14. Consensus		

Q.III State True or False:

1. Bitcoin is a peer-to-peer electronic cash system.
2. The Blockchain framework is created as the underlying transaction network behind the digital currency called Bitcoin.
3. The fixed-length output is called a Bitcoin token.
4. Bitcoin uses SHA-256 hash function that produces a hash (output) of size 256 bits (32 bytes).
5. Blockchain is an immutable ledger implemented in a distributed P2P network.
6. Peer-to-Peer (P2P) network is a decentralized network consists of a group of devices (nodes) that collectively store and share files where each node acts as an individual peer.
7. A consensus algorithm is a protocol through which all the parties of the Blockchain network come to a common agreement (consensus) on the present data state of the ledger and be able to trust unknown peers in a distributed computing environment.
8. The process of new coin generation is called hashing.
9. Bitcoin mining is the process of creating new bitcoin by solving a computational puzzle.
10. The term nonce stands for "number used only once".
11. The process of solving the cryptographic puzzle is referred to as Proof-of-Work (PoW).
12. Byzantine Fault Tolerance (BFT) in distributed network to reach consensus or agreement on the same value even when some of the nodes in the network fail to respond or respond with incorrect data or information.
13. Fork refers to competing or coexisting side chains within the same network.
14. BFT means taking an input as a string of any length and giving output of a fixed length.
15. PoW is the original consensus algorithm in a Blockchain network.
16. The immutability property of a Blockchain means that the data which has been written once on the Blockchain cannot be changed.

17. With PoW, adding new transaction blocks occurs with a process known as "mining".
18. Hashing means taking a string of variable size and converting it into an output of fixed length.

Answers

1. (T)	2. (T)	3. (F)	4. (T)	5. (T)	6. (T)	7. (T)	8. (F)	9. (T)	10. (T)
11. (T)	12. (T)	13. (T)	14. (F)	15. (T)	16. (T)	17. (T)	18. (T)		

Q.IV Answer the following Questions:

(A) Short Answer Questions:

1. What is Blockchin?
2. Define distributed P2P network.
3. Define ledger.
4. Define nonce.
5. What is competing chains?
6. Define PoW.
7. What is meant by consensus protocols?
8. Define mining.
9. What is cryptographic puzzle?
10. Define immutable ledger.
11. What is SHA?

(B) Long Answer Questions:

1. What is hash function? Explain its purpose and working.
2. Is Blockchain an incorruptible ledger? Describe in detail.
3. What is the nonce? Explain diagrammatically.
4. How is nonce used in mining?
5. Explain the distributed P2P network.
6. Explain Byzantine Fault Tolerance (BFT) in detail.
7. What are Proof of Work and Proof of State? Compare them.
8. Describe the term defense against attackers.
9. What is the principle on which Blockchain technology is based on?
10. With the help of example explain the competing chains.
11. Write a short note on: Cryptographic puzzle.
12. With the help od diagram describe process of SHA-256.

Smart Contracts

Objectives...

- To learn Concepts of Smart Contracts
- To study DApps and DAO
- To learn Hard and Soft Forks

3.0 INTRODUCTION

- A smart contract is a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement.
- The objectives of smart contracts are the reduction of need in trusted inter-mediators, arbitrations and enforcement costs, fraud losses, as well as the reduction of malicious and accidental exceptions.
- A smart contract is a temper-proof, digital agreement that runs on a decentralized Blockchain. Smart contracts are simply programs stored on a Blockchain that run when predetermined conditions are met.
- Smart contracts are not a new concept, but, with the advent of Blockchain, interest in this concept has revived and this is now an active area of research in the Blockchain space.
- Due to the cost saving benefits that smart contracts can bring to the financial services industry by reducing the cost of transactions and simplifying complex contracts.
- Smart contracts are a critical component of many platforms and applications being built using Blockchain or distributed ledger technology.
- Smart contract is a term used to describe computer code that automatically executes all or parts of an agreement and is stored on a Blockchain-based platform.
- Smart contracts work by "if/when...then..." statements that are written into code on a Blockchain. A network of computers executes the actions when predetermined conditions have been met and verified.
- The code can either be the sole manifestation of the agreement between the parties or might complement a traditional text-based contract and execute certain provisions, such as transferring funds from Party A to Party B.

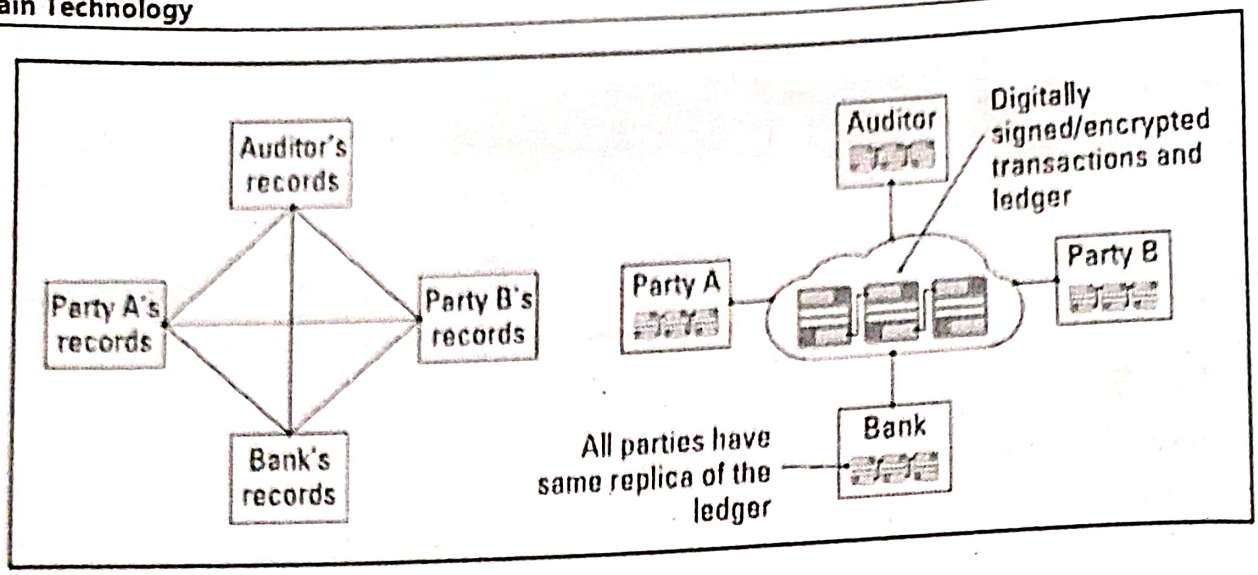


Fig. 3.1

- The code itself is replicated across multiple nodes of a blockchain and, therefore, benefits from the security, permanence and immutability that a blockchain offers.
- That replication also means that as each new block is added to the blockchain, the code is, in effect, executed.
- If the parties have indicated, by initiating a transaction, that certain parameters have been met, the code will execute the step triggered by those parameters. If no such transaction has been initiated, the code will not take any steps.
- Most smart contracts are written in one of the programming languages directly suited for such computer programs.

3.1 ETHEREUM NETWORK

- Ethereum is the hottest cryptocurrency in the Blockchain at present. Cryptocurrency is the word that's used to describe decentralized digitized currencies.
- The first cryptocurrency was created in 2008 known as Bitcoin. Ethereum is relatively new cryptocurrency and was invented in 2013.
- Ethereum is a blockchain-based open-source platform that gives developers the opportunity to build decentralized applications and deploy them.
- With the Ethereum Blockchain, rather than Bitcoin the miners will work to earn Ether or ETH. Although ETH is a type of digital currency, rather than being spent in the same way as we can make purchases with Bitcoin.
- ETH is the fuel that is needed to run the Ethereum network. Ether can be traded but is generally used by the application developers to pay for the services and the transaction fees on the Ethereum network.
- Ethereum is a technology that is home to digital money, global payments and applications.

- The community has growing a profitable digital economy, strong new ways for creators to earn online and so much more. It is open to everyone, wherever we are in the world all we need is the Internet.
- Ethereum is a Blockchain platform with its own cryptocurrency, called Ether (ETH) and Solidity is its own programming language.
- As a Blockchain network, Ethereum is a decentralized public ledger for verifying and recording transactions.
- The network's users can create, publish, monetize, and use applications on the platform, and use its Ether cryptocurrency as payment.
- Insiders call the decentralized applications on the network "DApps." Ethereum is an open-source Blockchain-based platform used to create and share business, financial services, and entertainment applications.
- Ethereum Blockchain can store much more deep data than Bitcoin Blockchain. Ethereum Blockchain allows building decentralized apps defined by smart contracts.
- Smart contract allows individuals to exchange information in trusted confident free manner without relying on third party as bank or lawyer or other way.
- So these Ethereurn smart contracts stored in special sections in Ethereum Blockchain which can be used then to build applications.
- Ethereum runs on a distributed public Blockchain network. Every node connected to the Ethereum network helps to maintain and update the Blockchain database.
- The nodes of the network run the Ethereum Virtual Machine (EVM) and execute the instructions according to the smart contracts. Ethereum nodes run the EVM to maintain consensus across the Blockchain.

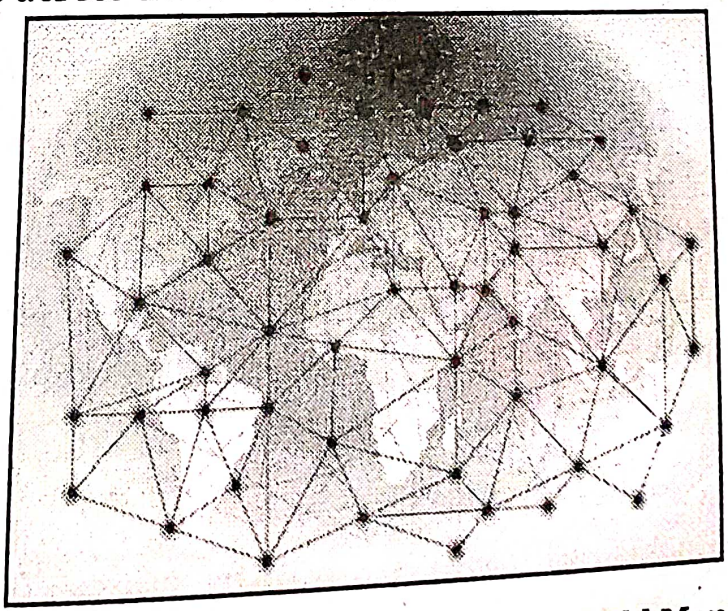


Fig. 3.2: Ethereum Network on a World Map

- Ethereum is a digital platform which allows people to build a range of decentralized applications.

- These applications can include security programs, voting systems and methods of payment. Like Bitcoin, Ethereum operates outside the mandate of central authorities such as banks and governments.
- The idea behind Ethereum was created by Vitalik Buterin. He launched the first version of the platform in 2015, with the help of several co-founders.
- Since, then it has grown rapidly in popularity and has helped prompt an increase of new rivals to Bitcoin.

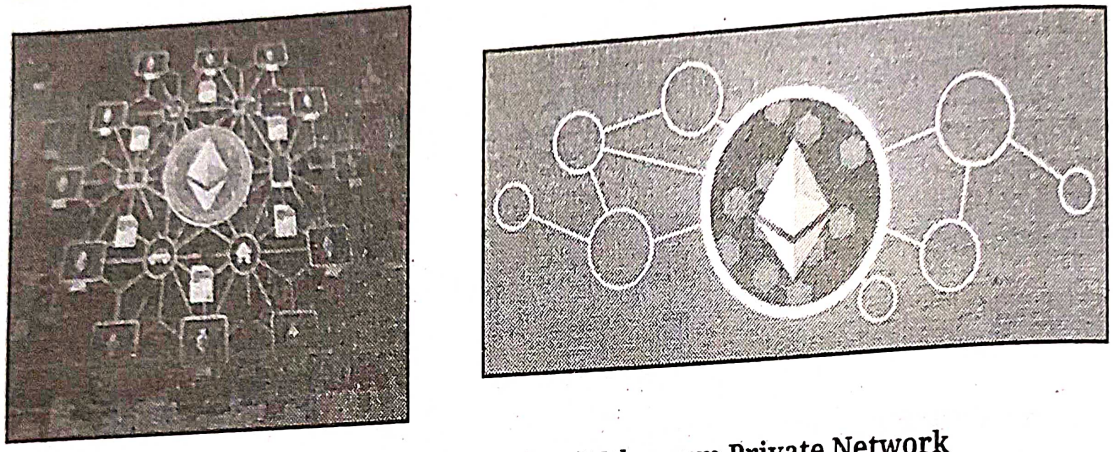


Fig. 3.3 (a): Ethereum Netwok and Ethereum Private Network

- Ethereum works as an open software platform functioning. This Blockchain is hosted on many computers around the world, making it decentralized.
- Each computer has a copy of the Blockchain, and there has to be widespread agreement before any changes can be implemented to the network.
- The Ethereum Blockchain is similar to Bitcoin's in that it is a record of the transaction history.
- However, the Ethereum network also allows developers to build and deploy decentralized applications ('dApps'). These are also stored on the Blockchain along with records of transactions.
- An Ethereum network has all the nodes connected to each other using the P2P network and each node keeps the latest copy of the Ethereum Blockchain ledger.
- A user can interact with the Ethereum network via the Ethereum client. The Ethereum client can be a desktop/laptop/mobile.
- The three types of Blockchain nodes are **mining nodes** (responsible for producing blocks; each time a mining node produces a block, it is rewarded), **full nodes** (responsible for maintaining and distributing copies of the entire Blockchain means they are responsible for the validation of blocks produced by the mining nodes) and

the **light node** (connects to a full node, downloads only the headers of previous blocks and connects to full node. By way of illustrating).

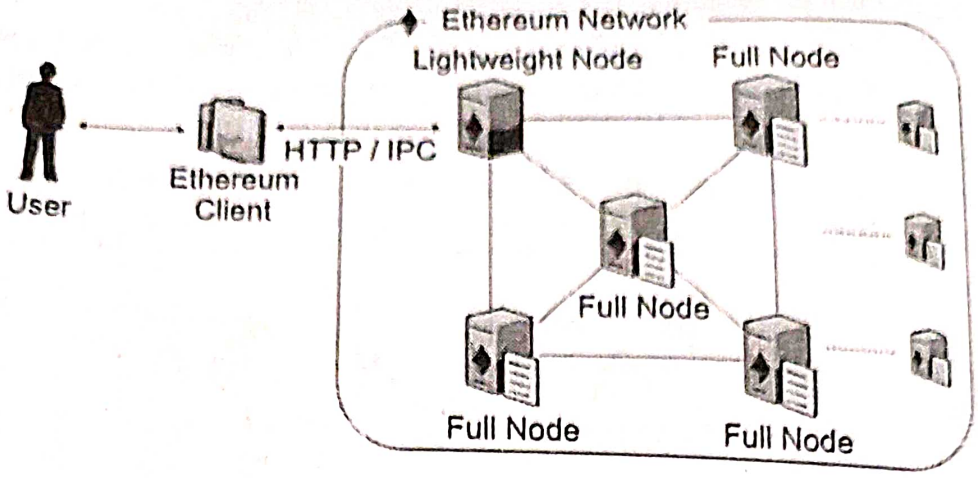


Fig. 3.3 (b)

Ethereum decentralized applications will run on the blockchain, they will all benefit from the following properties of the blockchain:

1. **Secure:** There is no single point of failure and all applications and transactions are secured with cryptography, giving them strong protection against fraud and hacking.
2. **Immutable:** Changes cannot be made to any data by a third party
3. **No Downtime:** The Blockchain cannot go down so the apps cannot go down.
4. **Tamper-proof and Corruption-free:** The frameworks the apps are built on are based on the principle of consensus and this makes censorship virtually impossible.

3.2 WHAT IS A SMART CONTRACT?

A smart contract is a self-enforcing agreement embedded in computer code managed by a Blockchain.

The code contains a set of rules under which the parties of that smart contract agree to interact with each other.

A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code.

Nick Szabo, an American computer scientist who invented a virtual currency called "Bit Gold" in 1998, defined smart contracts as computerized transaction protocols that execute terms of a contract.

The code and the agreements contained therein exist across a distributed, decentralized Blockchain network. The code controls the execution, and transactions are trackable and irreversible.

the **light node** (connects to a full node, downloads only the headers of previous blocks and connects to full node. By way of illustrating).

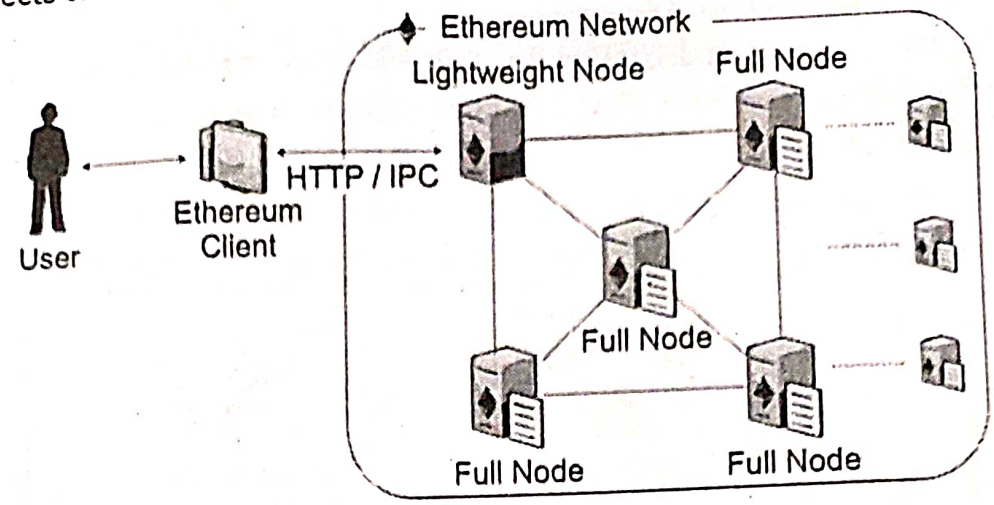


Fig. 3.3 (b)

- Ethereum decentralized applications will run on the blockchain, they will all benefit from the following properties of the blockchain:
  1. **Secure:** There is no single point of failure and all applications and transactions are secured with cryptography, giving them strong protection against fraud and hacking.
  2. **Immutable:** Changes cannot be made to any data by a third party
  3. **No Downtime:** The Blockchain cannot go down so the apps cannot go down.
  4. **Tamper-proof and Corruption-free:** The frameworks the apps are built on are based on the principle of consensus and this makes censorship virtually impossible.

3.2 WHAT IS A SMART CONTRACT?

- A smart contract is a self-enforcing agreement embedded in computer code managed by a Blockchain.
- The code contains a set of rules under which the parties of that smart contract agree to interact with each other.
- A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code.
- Nick Szabo, an American computer scientist who invented a virtual currency called "Bit Gold" in 1998, defined smart contracts as computerized transaction protocols that execute terms of a contract.
- The code and the agreements contained therein exist across a distributed, decentralized Blockchain network. The code controls the execution, and transactions are trackable and irreversible.

- A smart contract is a computer code that can facilitate the exchange of money, content, property, shares, digital assets, or anything of value among disparate and anonymous parties without a middle entity.
- When a smart contract is installed in a Blockchain system, it behaves like a self-operating computer program that automatically executes when specific terms and conditions are met.
- Because smart contracts run on the Blockchain, they run exactly as programmed without any possibility of censorship, downtime, fraud, or third-party interference.

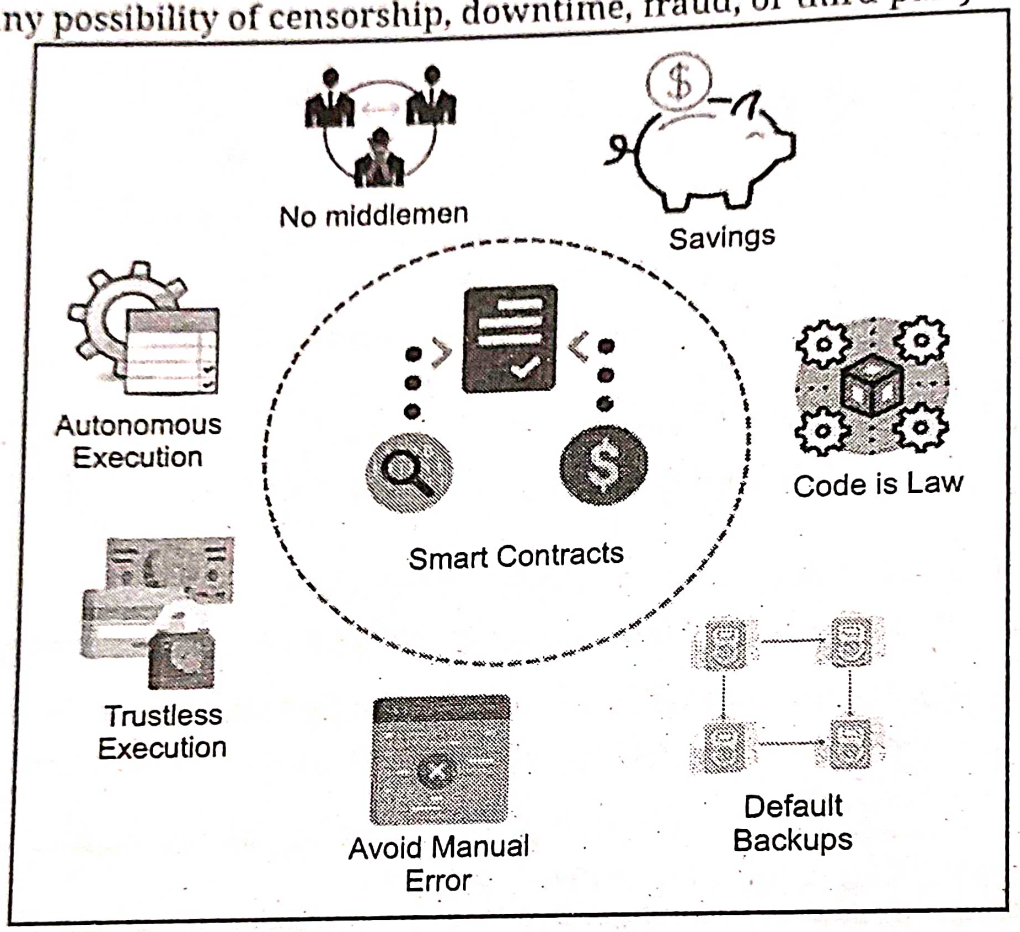


Fig. 3.4

- Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.
- While blockchain technology has come to be thought of primarily as the foundation for bitcoin, it has evolved far beyond underpinning the virtual currency.
- Smart contracts render transactions traceable, transparent, and irreversible. Smart contract is a term used to describe computer code that automatically executes all or parts of an agreement and is stored on a Blockchain-based platform.
- A key challenge in the widespread adoption of smart contracts is that parties will need to rely on a trusted, technical expert to either capture the parties' agreement in code or confirm that code written by a third party is accurate.

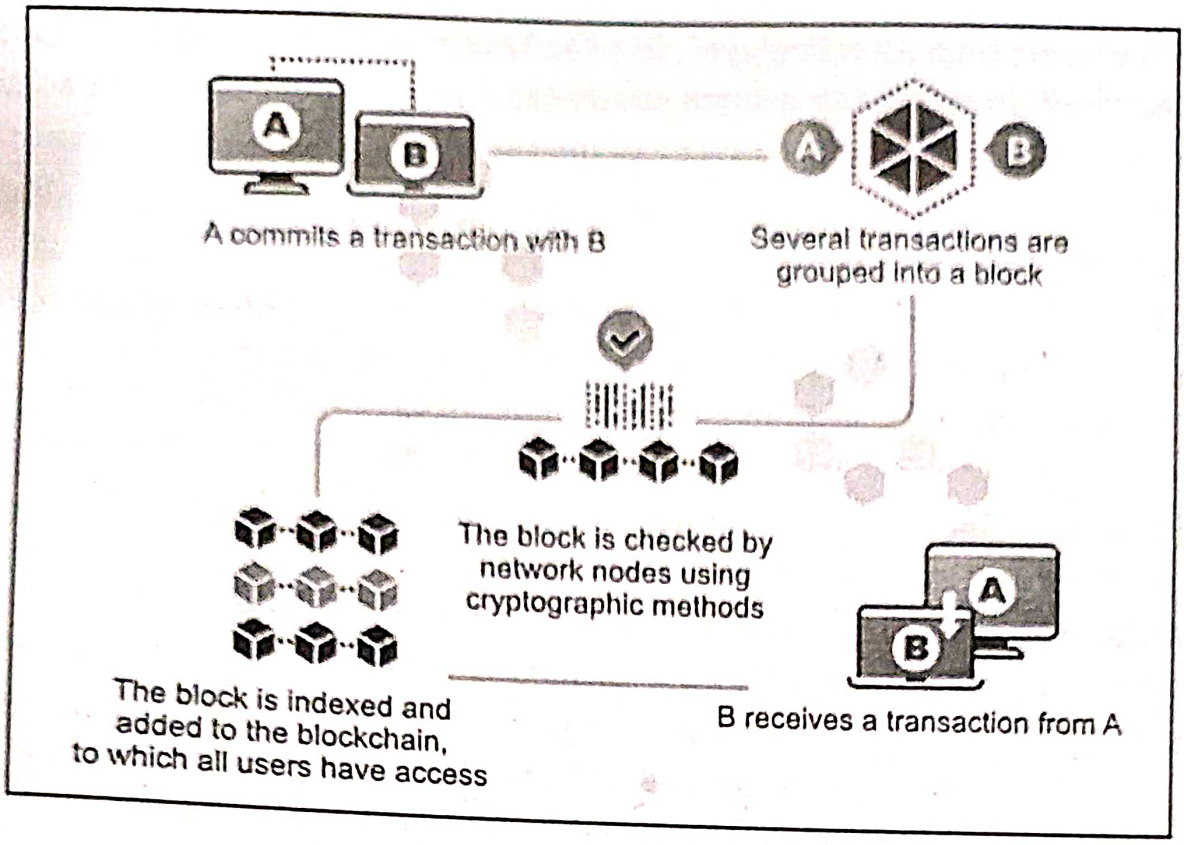


Fig. 3.5: Smart Contract

How do smart contracts work?

- A smart contract is a special kind of program that encodes business logic that runs on a special purpose virtual machine burn into a Blockchain or other type of distributed ledger.
- The process of creating a smart contract starts with business teams working with developers to describe their requirements for the wanted, behavior of the smart contract in response to various events or occurrences.
- In simple events could be conditions such as payment authorized, shipment received or a utility meter reading portal or entry.
- In many, sophisticated logic might encode more complex events such as calculating the value of a derivative financial implement and processing a trade of the derivative, or automatically releasing an insurance payment in the event of a person's death or a natural disaster.
- The originator, then work in a smart contract, writing platform to develop the logic and test it to make sure that it works as deliberate.
- After the application is developed, it is handed off to another team for a security review. This could be an internal expert or a firm that specializes in review smart contract security.
- Once the contract has been accepted, it is deployed on an existing Blockchain or other distributed ledger infrastructure.

- After the smart contract is deployed, it is configured to listen to event updates from an oracle, which is essentially a cryptographically secured streaming data source. The smart contract executes once it receives the suitable mix of events from one or more oracles.

Advantages Smart Contracts:

1. **Cost Efficiency:** Smart contracts promise to automate business processes that span organizational boundaries. This can eliminate many operational expenses and save resources, including the personnel needed to monitor the progress of a complex process that executes in response to conditions that span companies.
2. **Processing Speed:** Smart contracts can improve the processing speed of business processes that run across multiple enterprises.
3. **Autonomy:** Smart contracts are performed automatically by the network and reduce the need for a third party to manage transactions between businesses.
4. **Reliability:** Smart contracts can also take advantage of blockchain ledgers and other distributed ledger technologies to maintain a verifiable record of all activity related to execution of complex processes and that cannot be changed after the fact. It also supports automated transactions that remove the potential for human error and ensure accuracy in executing the contracts.

Example of Smart Contract:

- A smart contract may define contractual conditions under which corporate bond transfers occurs or it may encapsulate the terms and conditions of travel insurance, which may be executed automatically when, for example, a flight is delayed by more than six hours.
- Smart contracts eliminate the hassles and delays inherent in contracts by building the contract into the transaction.
- Through smart contracts, the Blockchain establishes the conditions under which a transaction or asset exchange can occur. No more faxing or emailing documents back and forth for review, revision, and signatures.

3.3 ETHEREUM VIRTUAL MACHINE, ETHER AND GAS

- Ethereum is an open-source, public Blockchain-based distributed computing platform featuring smart contract (scripting) functionality, which facilitates online contractual agreements.
- Ether is a cryptocurrency whose Blockchain is generated by the Ethereum platform. Ether can be transferred between accounts and used to compensate participant mining nodes for computations performed.

Ethereum provides a decentralized Turing-complete virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes.

The Gas, an internal transaction pricing mechanism, is used to mitigate spam and allocate resources on the network.

Ethereum Virtual Machine (EVM):

EVM stands for Ethereum Virtual Machine. The purpose of EVM is to serve as a runtime environment for smart contracts built on Ethereum.

EVM is the core engine that runs the Ethereurn Platform. It is the runtime environment that executes all the smart contracts on the Ethereum network.

The EVM can be considered a Turing complete virtual machine, which means it can perform any logical step of a computational function.

EVM is not physical but a virtual machine. Virtual machines are essentially creating a level of abstraction between the executing code and the executing machine.

- Consider it as a global supercomputer that executes all the smart contracts. The functionality of EVM is restricted to virtual machines.
- For example, it cannot make delayed calls on the internet or produce random numbers. Therefore, it is considered a simple state machine.
- Writing programs in assembly language do not make any sense, so, Ethereum required a programming language for the EVM.

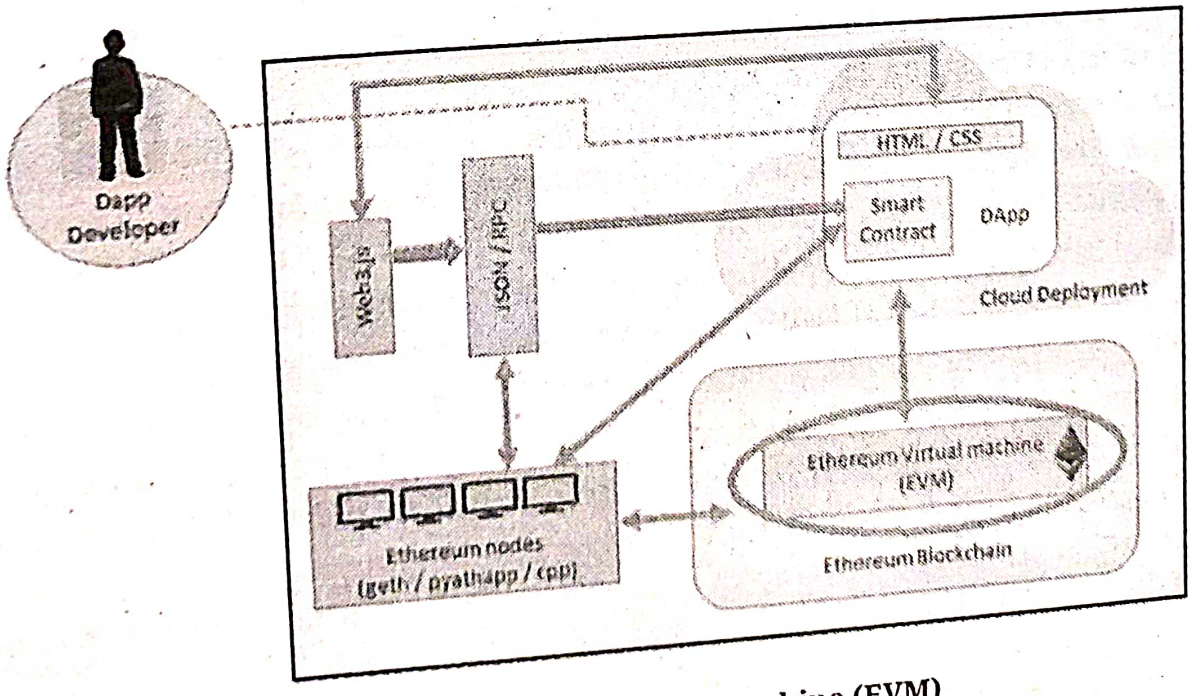


Fig. 3.6: Ethereum Virtual Machine (EVM)

- Fig. 3.7 shows architecture of Ethereum.

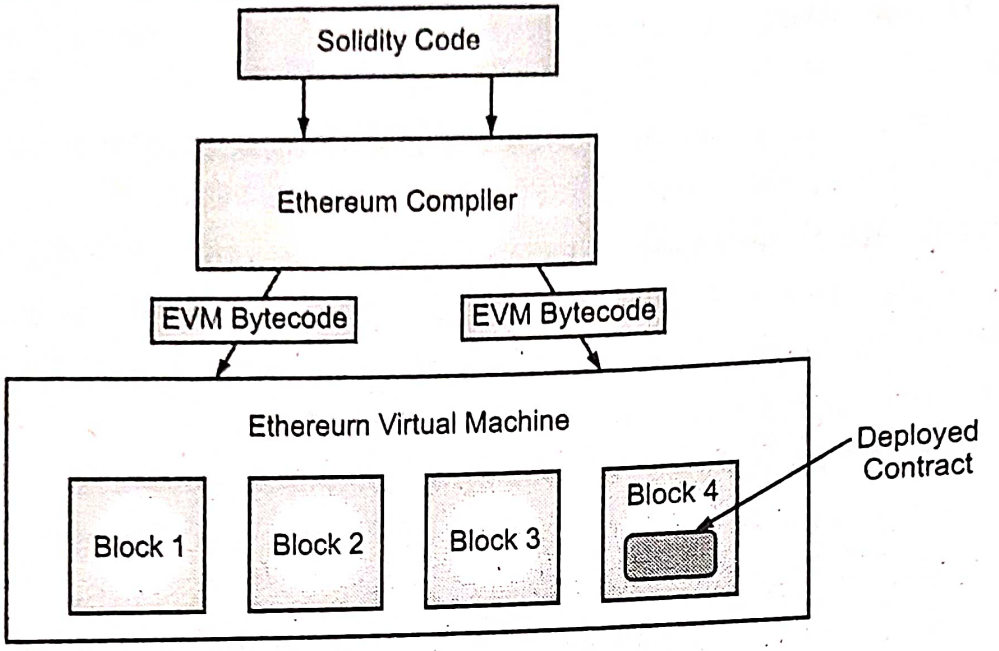


Fig. 3.7: Ethereum Architecture

- Where, Solidity is a JavaScript-like language developed specifically for creating smart contracts. It is typed statically and supports libraries, inheritance, and complex user-defined types.
- Solidity compiler converts code into EVM bytecode, which is sent to the Ethereum network as a deployment transaction.
- Ethereum Virtual Machines have been successfully implemented in various programming languages including C++, Java, JavaScript, Python, Ruby, and many others.
- The EVM is essential to the Ethereum Protocol and is instrumental to the consensus engine of the Ethereum system.
- It allows anyone to execute code in a trustless ecosystem in which the outcome of an execution can be guaranteed and is fully deterministic (i.e.) executing smart contracts.

Ether (ETH):

- Ethereum uses blockchain technology to allow network users to send and receive payments. Ether (ETH) is the currency unit of the Ethereum network.
- Ethereum brings general computations to the blockchain, it still makes use of a "coin".
- Its coin is called "Ether", and as any coin, it is a number that can be stored into account addresses and can be spent or received as part of transactions or block generation.
- Ether is used to pay for transaction fees and computational services. Users can send Ether to other users and developers can write smart contracts that receive, hold, and send Ether.
- Ether comes into existence by the validation of transactions on the Ethereum platform, through a process called mining.

- Ethereum is a decentralized computing platform that uses ETH (also called Ether) to pay transaction fees (or "gas").
- Developers can use Ethereum to run decentralized applications (dApps) and issue new crypto assets known as Ethereum tokens.

Gas:

- The key concept in Ethereum is that of gas. All transactions on the Ethereum blockchain are required to cover the cost of computation they are performing.
  The cost is coveredby something called gas or crypto fuel, which is a new concept introduced by Ethereum.
- This gas as execution fee is paid upfront by the transaction originators. The fuel is consumed with each operation. Each operation has a predefined amount of gas associated with it.
- Gas is the name for the execution fee that senders of transactions (in our case, senders of a smart contract transaction) will pay for verification.
- Each transaction specifies the amount of gas it is willing to consume for it's execution. Ifit runs out of gas before the execution is completed, any operation performed by the transaction up to that point is rolled back.
- If the transaction is successfully executed, then any remaining gas is refunded to the transaction originator.
- Gas is the name for the execution fee that senders of transactions need to pay for every operation made on an Ethereurn blockchain.
- The name gas is inspired by the view that this fee acts as cryptofuel, driving the motion of smart contracts.
- Gas is purchased for ether from the miners that execute the code. Gas and ether are decoupled deliberately since units of gas align with computation units having a natural cost, while the price of ether generally fluctuates as a result of market forces.
- The gas is used to allocate resources of the Ethereum virtual machine so that decentralized applications such as smart contracts can self execute in a secured but decentralized fashion.
- EVM, gas is a measurement unit used for assigning fees to each transaction with a smart contract. Each computation happening in the EVM needs some amount of gas.
- The more complex the computation is, the more the gas is required to run the smart contracts.

Transaction fee = Total gas used*gas price

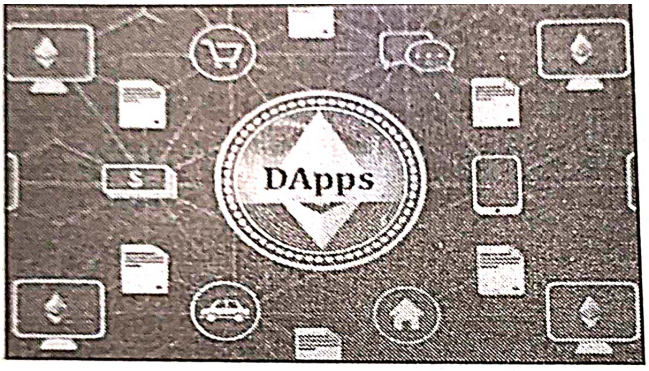


Fig. 3.8: DApps

Advantages of DApps:

1. **Zero Downtime:** Once the smart contract at the core of an app is deployed and on the blockchain, the network as a whole will always be able to serve clients looking to interact with the contract. Malicious actors therefore cannot launch denial-of-service attacks targeted towards individual dapps.
2. **Privacy:** No need to provide real-world identity to deploy or interact with a DApps.
3. **Resistance to Censorship:** No single entity on the network can block users from submitting transactions, deploying DApps, or reading data from the blockchain.
4. **Complete Data Integrity:** Data stored on the blockchain is immutable and indisputable, thanks to cryptographic primitives. Malicious actors cannot forge transactions or other data that has already been made public.
5. **Trustless Computation/Verifiable Behavior:** Smart contracts can be analyzed and are guaranteed to execute in predictable ways, without the need to trust a central authority. This is not true in traditional models; for example, when we use online banking systems, we have to trust that financial institutions will not misuse our financial data, tamper with records or get hacked.

3.4 DApps

- DApp is an abbreviation for decentralized application. A DApp has its backend code running on a decentralized peer-to-peer (P2P) network such as the Ethereum blockchain network.
- A DApp is an application built on a decentralized network that combines a smart contract and a frontend user interface. DApps can run on a P2P network or a blockchain network.
- A DApp has its backend code running on a decentralized peer-to-peer network. Contrast this with an app where the backend code is running on centralized servers.
- A DApps can have frontend code and user interfaces written in any language that can make calls to its backend.

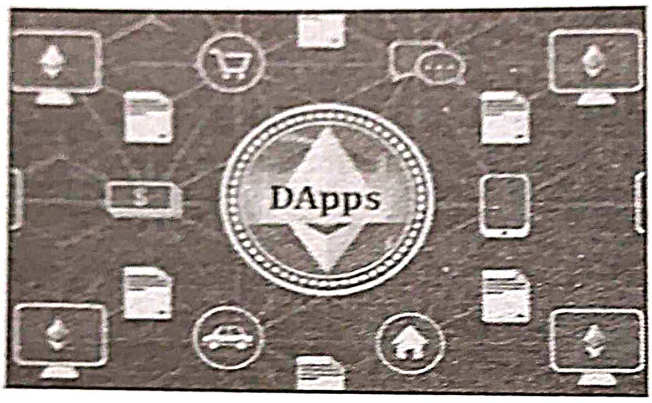


Fig. 3.8: DApps

Advantages of DApps:

1. **Zero Downtime:** Once the smart contract at the core of an app is deployed and on the blockchain, the network as a whole will always be able to serve clients looking to interact with the contract. Malicious actors therefore cannot launch denial-of-service attacks targeted towards individual dapps.
2. **Privacy:** No need to provide real-world identity to deploy or interact with a DApps.
3. **Resistance to Censorship:** No single entity on the network can block users from submitting transactions, deploying DApps, or reading data from the blockchain.
4. **Complete Data Integrity:** Data stored on the blockchain is immutable and indisputable, thanks to cryptographic primitives. Malicious actors cannot forge transactions or other data that has already been made public.
5. **Trustless Computation/Verifiable Behavior:** Smart contracts can be analyzed and are guaranteed to execute in predictable ways, without the need to trust a central authority. This is not true in traditional models; for example, when we use online banking systems, we have to trust that financial institutions will not misuse our financial data, tamper with records or get hacked.

Decentralized Applications:

- All ideas mentioned earlier come under the larger umbrella of decentralized applications.
- A decentralized application is a computer application that runs on a decentralized computing system.
- Decentralized applications are digital applications or programs that exist and run on a blockchain or P2P network of computers instead of a single computer, and are outside the purview and control of a single authority.
- All DAOs, DACs, and Dos are basically decentralized applications that run on top of a blockchain in a peer-to-peer network.
- This is the latest advancement in technology with regard to decentralization. Decentralized applications or DAPPs are software programs that can run on their own blockchain, use another already existing established blockchain or use only protocols of an existing blockchain solution. These are called Type I, Type II, and Type III DAPPs.
- The DApps should be fully open source and autonomous and no single entity should be in controlof a majority of its tokens.
- All changes to the application must be consensus, driven based on the feedback given by the community.
- Data and records of operations of the application must be cryptographically secured and stored on a public, decentralized Blockchain in order to avoid any central points of failure.
- A cryptographic token must be used by the application in order to provide access and rewards to those who contribute value to the applications, for example, miners in bitcoin.
- The tokens must be generated by the decentralized application according to a standard cryptographic algorithm. This generation of tokens acts as a proof of the value to contributors for example, miners.

Operations of DApps:

- Establishmentof consensus by a DApp can be achieved using consensus algorithms such as Proof of Work and Proof of Stake.
- So far, only PoW has been found to be incredibly resistant to 51% attacks, as is evident from bitcoin. Furthermore, a DAPP can distribute tokens (coins) via mining, fund raising, and development.
- Examples of some decentralized applications are:

KYC-Chain:

- This application provides a facility to manage Know Your Customer (KYC) data in a secure and convenient way based on smart contracts.

OpenBazaar:

- This is a decentralized peer-to-peer network that allows commercial activities directly between sellersand buyers instead of relying on a central party, as opposed to conventional providers such as eBay and Amazon.
- It should be noted that this system is not built on top of a blockchain, instead distributed hash tables are used in a peer-to-peer network in order to enable direct communication and data sharing between peers. It makes use of bitcoin as a payment network, however.

Lazooz:

- This isa decentralized equivalent of Uber. It allows peer-to-peer ride sharing and users can be incentivized by proof of movement and can earn Zooz coins.

3.5 DECENTRALIZED AUTONOMOUS ORGANIZATIONS (DAO)

- The DAO stands for Decentralized Autonomous Organization. As the name implies, it is an organization which is both autonomous and decentralized.
- A DAO is an organization which is represented by rules encoded as a computer program that is transparent, controlled by shareholders, and not influenced by the central government.
- A DAO is the most complex form of a smart contract. A smart contract is a computer program that autonomously exists on the internet, but at the same time, it needs people to perform a task that it can't do by itself.
- DAO runs through rules encoded as a computer program called Smart Contracts. A Smart Contract is an entity that lives on the internet and exists autonomously.
- It also has individuals to perform a certain task that the automation program itself cannot do.
- A DAO isalso a computer program than runs on top of a Blockchain and embedded within it are governance and business logic rules.
- DAOs are autonomous, which means that they are fully automated and contain artificially intelligent logic.
- A DAO is an entity with no central leadership. Decisions get made from the bottom-up, governed by a community organized around a specific set of rules enforced on a Blockchain.
- Ethereum Blockchain led the way with the introduction of DAOs for the first time. In DAO, the code isconsidered the governing entity rather than humans or paper contracts.
- Currently, DAOs do not have any legal status even though they may contain some intelligent code that enforces some protocols and conditions, but these rules have no value inthe current real-world legal system.

- DAOs are internet-native organizations collectively owned and managed by their members.
- They have built-in treasuries that are only accessible with the approval of their members. Decisions are made via proposals the group votes on during a specified period.
- A DAO works without hierarchical management and can have a large number of purposes.
- Freelancer networks where contracts pool their funds to pay for software contribution, welfare organizations where members approve donations and venture capital firms owned by a group are all possible with these organizations.

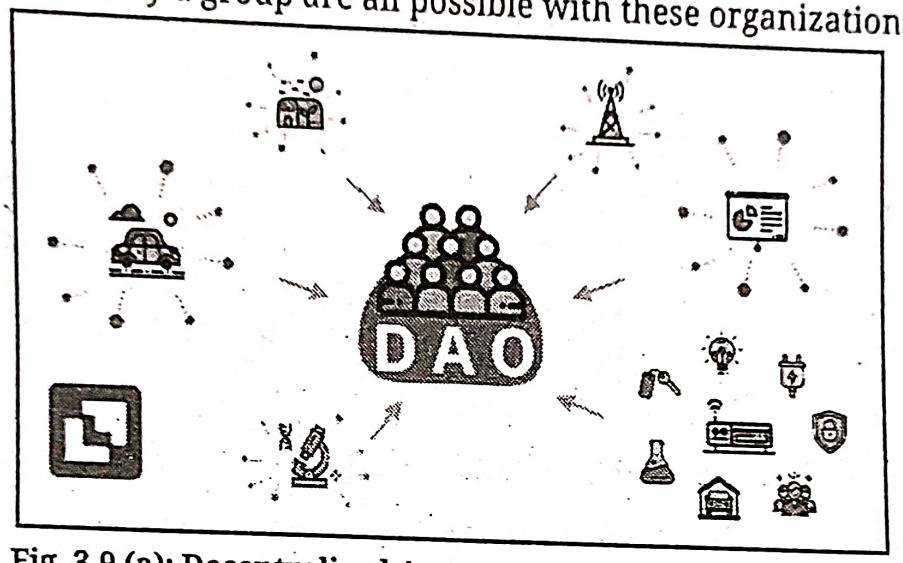


Fig. 3.9 (a): Decentralized Autonomous Organizations (DAO)

How does a Decentralized Autonomous Organizations (DAO) work?

- A DAO (Decentralized Autonomous Organizations) is an organization where decisions get made from the bottom-up, a collective of members owns the organization.
- There are various ways to participate in a DAO, usually through the ownership of a token.
- DAOs operate using smart contracts, which are essentially blocks of code that automatically execute whenever a set of criteria are encounter.
- Smart contracts are deployed on numerous Blockchains now-a-days, though Ethereum was the first to use them.
- These smart contracts establish the Decentralized Autonomous Organizations (DAO's) rules. Those with a stake in a DAO then get voting rights and may influence how the organization operates by deciding on or creating new governance proposals.
- This model prevents DAOs from being spammed with proposals. A proposal will only pass once the majority of stakeholders approve it. How that majority is determined varies from DAO to DAO and is specified in the smart contracts.
- Decentralized Autonomous Organizations are fully autonomous and transparent. As they are built on open-source Blockchains, anyone can view their code.

- Anyone can also audit their built-in resources, as the blockchain records all financial transactions.

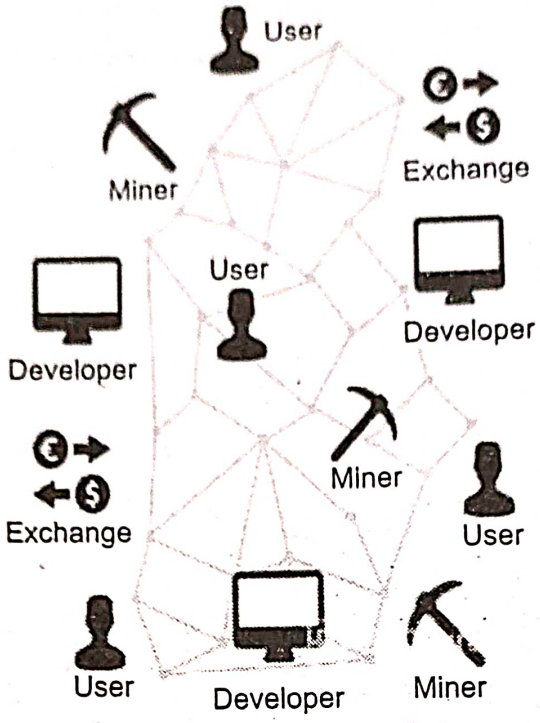


Fig. 3.9 (b): Decentralized Autonomous Organizations (DAO) Network

Examples of DAOs:

1. **A Charity:** We can accept membership and donations from anyone in the world and the group can decide how they to spend donations.
2. **A Freelancer Network:** We could create a network of contractors who pool their funds for office spaces and software subscriptions.
3. **Ventures and Grants:** We could create a venture fund that pools investment capital and votes on ventures to back. Repaid money could later be redistributed amongst DAO-members.

3.6 HARD AND SOFT FORKS

- A fork (new branch of sequence of blocks) in Blockchain is to impart change in the previous version or divergence from the existing protocol of the Blockchain.
- A fork is a change to the digital currency software which creates two different paths of the Blockchain with a shared history.
- The software which runs on the nodes of a Blockchain network is updated from time to time to add new features or to make changes in how the Blockchain functions.
- These code changes are considered adopted when a majority of nodes on the network install and start using an updated version of the Blockchain software.

- These code updates or changes to the blockchain code are referred to as forks (See Fig. 3.10).

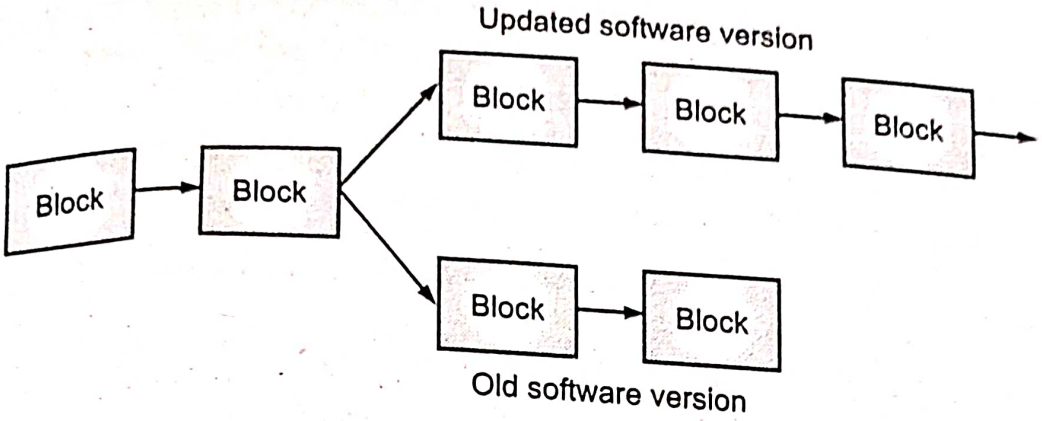


Fig. 3.10: A Fork in Blockchain

Types of Forks in Blockchain:

- Two types of forks can happen in Blockchain Soft fork and Hard fork.

1. **Hard Fork:**

- A hard fork or hardfork, as it relates to Blockchain technology, is a radical change to a network's protocol that makes previously invalid blocks and transactions valid, or vice-versa.
- A hard fork requires all nodes or users to upgrade to the latest version of the protocol software.
- Blockchain software updates which are not backwards compatible with older versions of the Blockchain software are called hard forks.
- Hard fork changes are usually significant and change fundamental aspects of how a Blockchain functions, such as the block size, hashing algorithm used, or how consensus is reached.
- Forks may be initiated by developers or members of a crypto community who grow dissatisfied with functionalities offered by existing Blockchain implementations.
- They may also emerge as a way to crowd source funding for new technology projects or cryptocurrency offerings.
- There are a number of reasons why developers may implement a hard fork, such as correcting important security risks found in older versions of the software, to add new functionality, or to reverse transaction, such as when the Ethereum Blockchain created a hard fork to reverse the hack on the Decentralized Autonomous Organization (DAO).
- After the hack, the Ethereum community almost unanimously voted in favor of a hard fork to roll back transactions that siphoned off tens of millions of dollars worth of digital currency by an anonymous hacker.

- The hard fork also helped DAO token holders get their ether (ETH) funds returned. The proposal for a hard fork did not exactly unwind the network's transaction history.
- Rather, it relocated the funds tied to the DAO to a newly created smart contract with the single purpose of letting the original owners withdraw their funds.
- DAO token holders could withdraw ETH at a rate of approximately 1 ETH to 100 DAO. The extra balance of tokens and any ether that remained as a result of the hard fork was withdrawn and distributed by the DAO curators to provide "failsafe protection" for the organization.

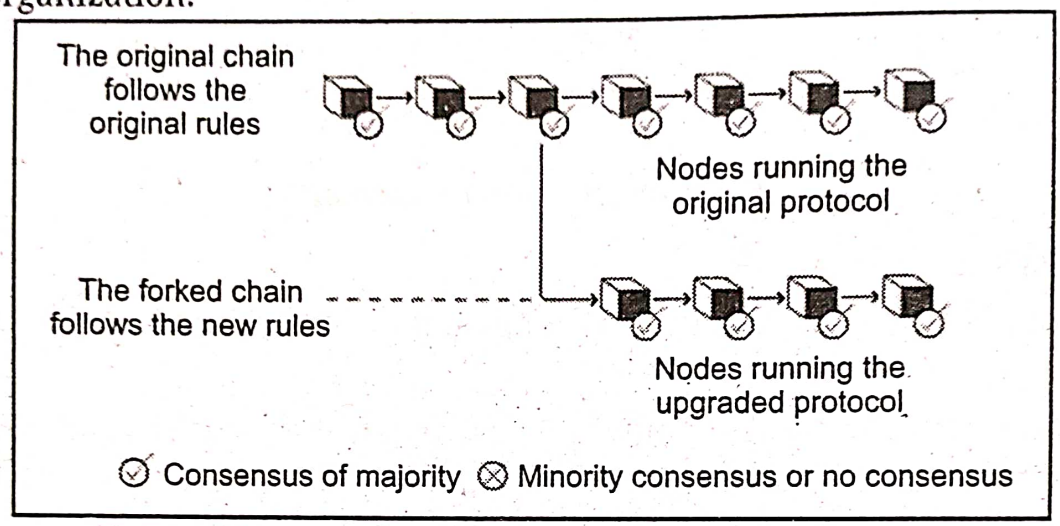


Fig. 3.11

2. Soft Fork:

- A soft fork is a change to the protocol that is backward compatible means that the new rules do not exclude the protocol rules that already existed up to the time of the soft fork. As a result, all nodes and are still capable of generating blocks and joining the Blockchain.
- Updates which are backwards compatible with prior versions of the Blockchain software are known as soft forks.
- A node running an old version of the software will still be table to submit transactions and participate in the Blockchain but may not benefit from some of the new features offered by the newer Blockchain software version. Nodes on a Blockchain usually seek to install updated software for that reason.
- Since, this all sounds very abstract, let's explain the situation again with an example. The protocol's already existing rules dictate that a block must reach 5MB, and then it is attached to the Blockchain.
- However, now the protocol is updated, and the blocks are supposed to be only 3MB until they are pinned to the Blockchain. Since the older nodes can append blocks with a storage capacity of 5MB, they are now also able to append blocks with 3MB to the Blockchain. Thus, both old and new nodes can append blocks to the Blockchain.

- However, if old nodes try to append a block with 5MB to the blockchain, the new nodes will be rejected because this block does not comply with the new rules of the protocol. Over time, the old nodes now also only follow the rules of the new protocol.

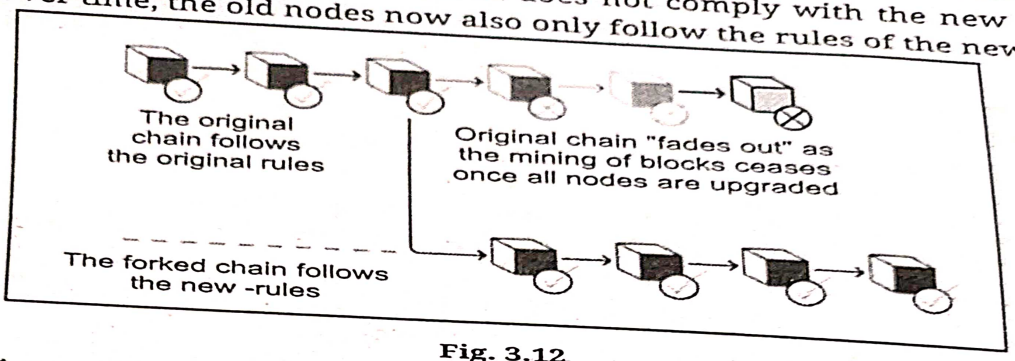


Fig. 3.12

Difference between Hard Forks and Soft Forks:

- A soft fork is a backward-compatible change in the blockchain software where the rules become stricter, and less is permitted than in the situation before. A hard fork is a non-backward compatible change in the blockchain software that introduces a new rule to the network.
- Hard forks are not the only way to upgrade the software behind a cryptocurrency. Soft forks are, by contrast, seen as a safer alternative that is backward compatible, which means that nodes that do not upgrade to newer versions will still see the chain as valid.
- A soft fork can be used to add new features and functions that do not change the rules a blockchain must follow. Soft forks are often used to implement new features at a programming level.

3.7 INITIAL COIN OFFERINGS

- An Initial Coin Offering (ICO) or initial currency offering is a type of funding using cryptocurrencies.
- It is often a form of crowd-funding, (funding a project or venture by raising small amounts of money from a large number of people, typically via the Internet).
- In an ICO, a quantity of cryptocurrency is sold in the form of "tokens" ("coins") to speculators or investors, in exchange for legal tender or other (generally established and more stable) cryptocurrencies such as Bitcoin or Ether.
- The tokens are promoted as future functional units of currency if or when the ICO's funding goal is met and the project successfully launches.

- An ICO can be a source of capital for startup companies. ICOs can allow startups to avoid regulations that prevent them from seeking investment directly from the public, and intermediaries such as venture capitalists, banks, and stock exchanges, which may demand greater scrutiny and some percentage of future profits or joint ownership.
- ICO is a crowd-funding method in the world of cryptocurrencies. In an ICO, there is an exchange of ICO tokens or ICO coins.
- An initial coin offering (ICO) is a type of capital raising activity in the cryptocurrency and blockchain domain.
- The ICO can be viewed as an initial public offering (IPO) that uses cryptocurrencies. Though, it is not the most specific comparison, as there are some major differences between the two fundraising activities.
- Startups primarily use an Initial Coin Offering (ICO) is to raise capital.

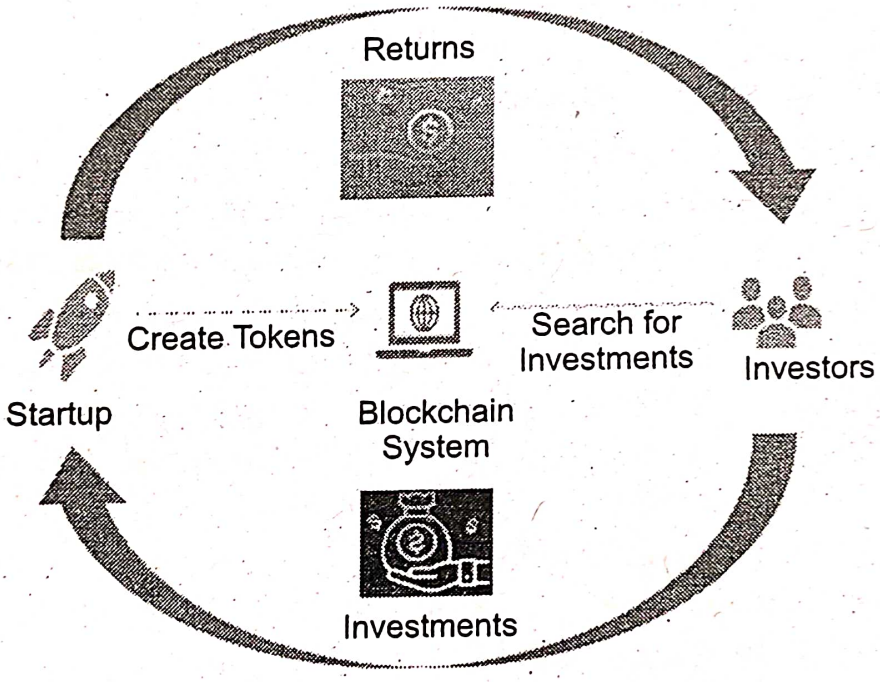


Fig. 3.13: Working of ICO

- An initial coin offering is a sophisticated process that requires a deep knowledge of technology, finance, and the law.
- The main idea of ICOs is leveraging the decentralized systems of Blockchain technology in capital-raising activities that will align the interests of various stakeholders.
- The steps in an ICO are listed below:

1. **Identification of Investment Targets:**

- Every ICO starts with the company's intention to raise capital.
- The company identifies the targets for its fundraising campaign and creates the relevant materials about the company or project for potential investors.

next step in the initial coin offering is the creation of tokens. Essentially, the tokens are representations of an asset or utility in the Blockchain.

- The tokens are fungible and tradeable. They should not be confused with crypto-currencies because the tokens are just modifications of existing cryptocurrencies.
- Unlike stocks, the tokens generally do not provide an equity stake in a company. Instead, most of the tokens deliver their owners some stake in a product or service created by the company.
- The tokens are created using specified Blockchain platforms. The process of the creation of tokens is relatively simple because a company is not required to write the code from scratch as in the creation of new cryptocurrency.
- Instead, existing Blockchain platforms that run existing cryptocurrencies such as Ethereum allow the creation of the tokens with minor modifications of the code.

3. **Promotion Campaign:**

- At the same time, a company usually runs a promotion campaign to attract potential investors. Note that the campaigns are commonly executed online to achieve the widest investor reach.
- However, currently, several large online platforms such as Facebook and Google ban the advertising of ICOs.

4. **Initial Offering:**

- After the creation of the tokens, they are offered to the investors. The offering may be structured in several rounds.
- The company can then use the proceeds from the ICO to launch a new product or service while the investors can expect to use the acquired tokens to benefit from this product/service or wait for the appreciation of the tokens' value.

ICO Regulations:

- The initial coin offering is a completely new phenomenon in the world of finance and technology.
- The introduction of ICO's made a significant impact on capital-raising processes in recent years. However, regulatory authorities around the world were not prepared for the introduction of the new fundraising model in finance.
- Approaches to the regulation of initial coin offerings vary among different countries. For example, the governments of China and South Korea prohibit ICOs.
- Many European countries, as well as the United States and Canada, are working on the development of specific regulations to govern the conduct of ICOs.
- At the same time, there are already published guidelines governing ICOs in a number of countries, including Australia, New Zealand, Hong Kong, and the United Arab Emirates (UAE).

offering is the creation of tokens. Essentially, the
- The tokens are fungible and tradeable. They should not be confused with crypto-currencies because the tokens are just modifications of existing cryptocurrencies.
- Unlike stocks, the tokens generally do not provide an equity stake in a company. Instead, most of the tokens deliver their owners some stake in a product or service created by the company.
- The tokens are created using specified Blockchain platforms. The process of the creation of tokens is relatively simple because a company is not required to write the code from scratch as in the creation of new cryptocurrency.
- Instead, existing Blockchain platforms that run existing cryptocurrencies such as Ethereum allow the creation of the tokens with minor modifications of the code.

3. **Promotion Campaign:**
- At the same time, a company usually runs a promotion campaign to attract potential investors. Note that the campaigns are commonly executed online to achieve the widest investor reach.
- However, currently, several large online platforms such as Facebook and Google ban the advertising of ICOs.

4. **Initial Offering:**
- After the creation of the tokens, they are offered to the investors. The offering may be structured in several rounds.
- The company can then use the proceeds from the ICO to launch a new product or service while the investors can expect to use the acquired tokens to benefit from this product/service or wait for the appreciation of the tokens' value.

ICO Regulations:
- The initial coin offering is a completely new phenomenon in the world of finance and technology.
- The introduction of ICO's made a significant impact on capital-raising processes in recent years. However, regulatory authorities around the world were not prepared for the introduction of the new fundraising model in finance.
- Approaches to the regulation of initial coin offerings vary among different countries. For example, the governments of China and South Korea prohibit ICOs.
- Many European countries, as well as the United States and Canada, are working on the development of specific regulations to govern the conduct of ICOs.
- At the same time, there are already published guidelines governing ICOs in a number of countries, including Australia, New Zealand, Hong Kong, and the United Arab Emirates (UAE).

- The main advantage of ICOs is that they remove intermediaries from the capital-raising process and create direct connections between the company and investors. In addition, the interests of both parties are aligned.

3.8 DEMO OF SMART CONTRACTS

- Blockchain is a new technology that introduces decentralized, replicated, autonomous and secure databases.
- Blockchain is mostly known for its use with Bitcoin, but it has more applications beyond that, such as smart contracts.
- Smart contract is a transaction embedded to Blockchain that contains executable code and its own internal storage, offering immutable execution and record keeping.
- Smart contracts enable the creation of more complex decentralized applications (DApps) and even decentralized autonomous organizations (DAOs) on Blockchain.
- Smart contract is a transaction embedded in Blockchain that contains enhanced logic - a contract that is executable, has its own data storage and can access other resources to evaluate its current state and perform actions - a contract made of code.
- Smart contracts are self-executing contracts containing the terms and conditions of an agreement among peers in P2P network. The terms and conditions of the agreement are written into code.
- The smart contract executes on the Ethereum Blockchain's decentralized platform. The agreements facilitate the exchange of money, shares, property, or any asset.
- A smart contract defines the rules between different organizations in executable code. Applications invoke a smart contract to generate transactions that are recorded on the ledger.
- A number of reasons why smart contracts are so helpful:
  - Significantly reduces processing times for agreeing orders, making payments and ensuring everyone is working to agreed standards.
  - Provides traceability of raw materials, parts and finished products to all the supply chain organizations that handled them.
  - Allows for consensus that all the activities recorded and reported on in a smart contract have been carried out.
  - Integrates with other technology and organizations, for example, goods received notifications for payments release or integrating with IoT tracking devices and updating contracts when locations are reached.
  - Increases efficiency due to less rework and duplication of effort.
  - Enhances trust that goods will be delivered and payment will be made once criteria are met.
- Fig. 3.14 shows demo of smart contract.

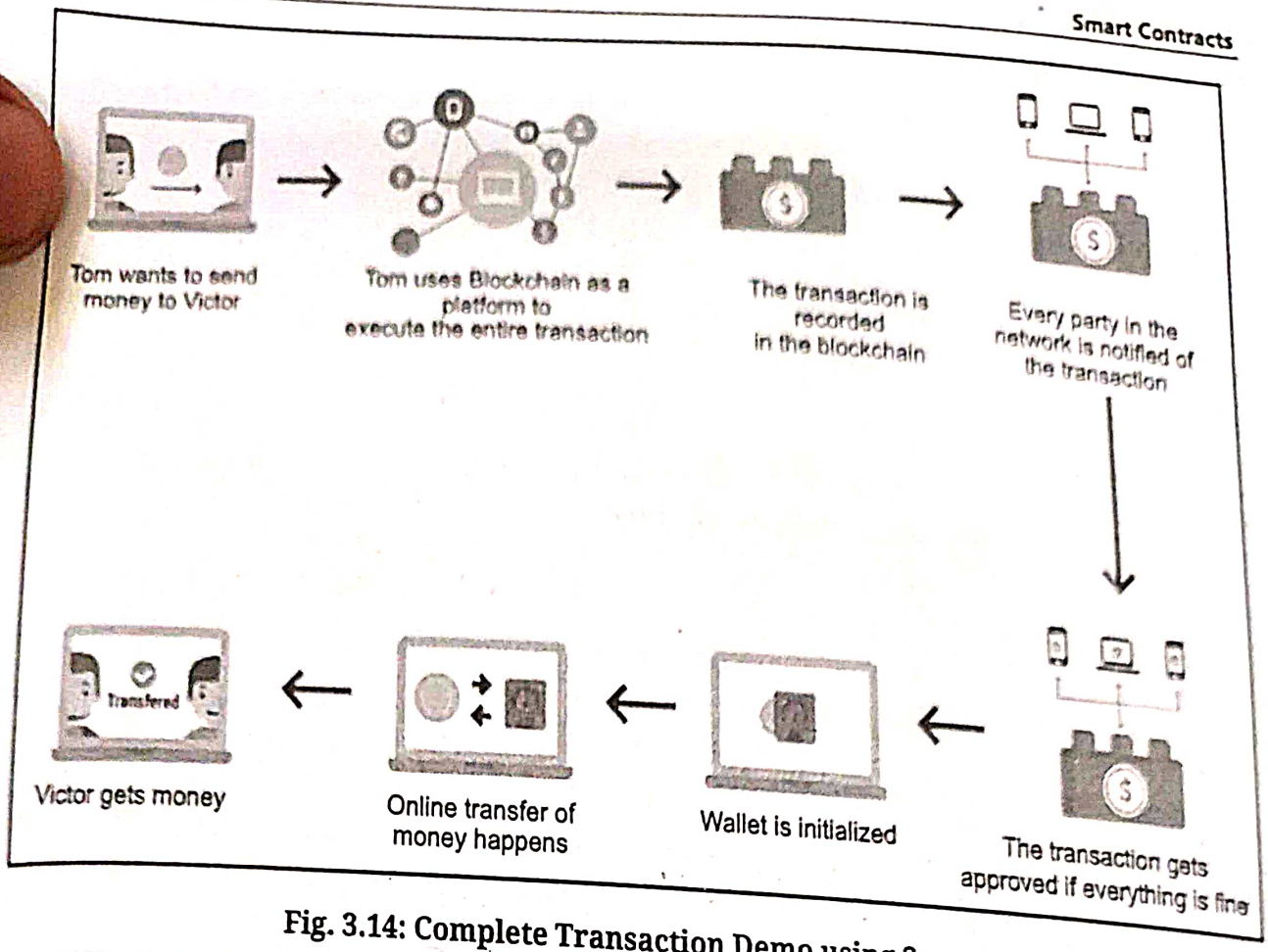


Fig. 3.14: Complete Transaction Demo using Smart Contract

PRACTICE QUESTIONS

Q.I Multiple Choice Questions:

1. Which is a self-executing contract with the terms of the agreement between two parties being directly written into lines of code and the code and the agreements contained therein exist across a distributed, decentralized Blockchain network?
   (a) smart contracts (b) digital ledger
   (c) digital nonce (d) None of the mentioned
2. Which is a distributed public blockchain P2P network that focuses on running programming code of any decentralized application?
   (a) Ethereum (b) Bitcoin
   (c) Both (a) and (b) (d) None of the mentioned
3. Ethereum network uses a decentralized digital currency known as,
   (a) Bitcoin (b) Ether or ETH
   (c) Lightcoin (d) All of the mentioned
4. Smart contracts are also known as,
   (a) self-executing contracts (b) Blockchain contracts
   (c) digital contracts (d) All of the mentioned

5. Ethereum is,
   (a) closed-source networks (b) open source Blockchain networks
   (c) Worldwide private networks (d) None of the mentioned
6. In which programming language is Ethereum written?
   (a) Python (b) Java
   (c) Solidity (d) All of the mentioned
7. What does machines belonging to distributed system join to Ethereum network and validate transactions called as,
   (a) blocking (b) mining
   (c) chaining (d) hashing
8. Which is a clever mechanism that Ethereum uses as the network's internal pricing fee for running a transaction or contract?
   (a) Gas (b) Ether or ETH
   (c) EVM (d) All of the mentioned
9. Which is a virtual state machine that functions as a runtime environment for smart contracts in Ethereum?
   (a) Gas (b) Ethereum Virtual Machine (EVM)
   (c) Ether or ETH (d) All of the mentioned
10. Which is the process through which new transactions get consolidated into blocks of the blockchain.
    (a) mining (b) hashing
    (c) chaining (d) blocking
11. Which is Decentralized Autonomous Organizations (DAO) is a company/ organization governed in a decentralized manner through Blockchain-based smart contracts?
    (a) Centralized Autonomous Organizations (CAO)
    (b) Decentralized Automatic Organizations (DAO)
    (c) Decentralized Autonomous Company (DAC)
    (d) None of the mentioned
12. Which can make use of smart contracts on the Ethereum network to achieve decentralization?
    (a) Bitcoin (b) dApps
    (c) Lightcoin (d) Monero
13. Which can use a platform like Ethereum that allows decentralized apps (dApps) to be built on its platform with the help of smart contracts?
    (a) Initial Coin Offering (ICO) (b) Bitcoin
    (c) Blockinchain (d) None of the mentioned

Answers

1. (a)	2. (c)	3. (b)	4. (d)	5. (b)	6. (c)	7. (b)	8. (a)	9. (b)	10. (a)
11. (b)	12. (b)	13. (a)							

Q.II Fill in the Blanks:

1. A _____ is a self-executing contract with the code and the agreements across a distributed, decentralized Blockchain network.
2. _____ provides a platform for building decentralized applications (dApps) to implement business logic and applications.
3. Ethereum implements an execution environment on the Blockchain called the _____ and every node participating in the network runs the EVM as part of the block verification protocol.
4. _____ is Ethereum's cryptocurrency.
5. EVM is designed to operate as a _____ environment for compiling and deploying Ethereum-based smart contracts.
6. The _____ are organizations that run autonomously and could make decentralized decisions through the use of Blockchain technology.
7. Decentralized applications, or _____, are essentially Blockchain-based smart contract-powered versions of apps popularized by the Ethereum network.
8. To perform any transaction within the Ethereum network, a user has to make a payment-shell out ethers-to get a transaction done, and the intermediary monetary value is called _____.
9. A Dapp consists of a backing code that runs on a distributed _____ network.
10. Blockchain _____ are essentially a split in the Blockchain network.
11. With a _____ fork, the rules of the Blockchain protocol are updated or changed so that the old blockchain and the resulting Blockchain are incompatible.
12. Ethereum is a _____ Blockchain platform created by Vitalik Buterin which, along with tracking cryptocurrencies, is additionally intended to execute program codes of different decentralized applications (DApps).
13. A _____ fork is backwards-compatible in which the upgraded Blockchain is responsible for validating transactions.
14. _____is the name of the language used within Ethereum to implement smart contracts.

Answers

1. smart contract	2. Ethereum	3. EVM	4. Ether (or ETH)
5. runtime	6. DAOs	7. DApps	8. gas
9. peer-to-peer	10. forks	11. hard	12. public
13. soft	14. Solidity		

Q.III State True or False:

1. A smart contract is actually a tiny computer program that's stored and runs on a Blockchain platform.

2. A smart contract is simply a program that runs on the Ethereum Blockchain. It is a collection of code (its functions) and data (its state) that resides at a specific address on the Bitcoin Blockchain.
3. The Ethereum network runs the EVM and executes identical instructions as all of the other nodes in order to achieve and maintain consensus about the state of the system.
4. Smart contracts run on the Blockchain Platform, which will process all the transactions in a contract; hence, middle men are not required for executing the transactions.
5. Ethereum is an open-ended, decentralized, Blockchain-based, public software platform that facilitates peer-to-peer contracts, known as Smart Contracts, as well as Decentralized Applications, known as DApps.
6. EVM (Ethereum Virtual Machine) is the Ethereum smart contracts runtime execution environment in which every node in the network runs EVM and all the nodes execute all the transactions that point to smart contracts using EVM.
7. Bitcoin is the cryptocurrency that the Ethereum Blockchain supports.
8. A fork is said to have happened when there is a conflict among the nodes regarding the validity of a Blockchain, that is, more than one Blockchain happens to be in the network, and every Blockchain is validated for some miners.
9. The Ethereum network is a peer-to-peer network where nodes participate in order to maintain the Blockchain and contribute to the consensus mechanism.
10. Ethereum is an implementation of Blockchain technology that can run smart contracts.
11. Gas refers to the fee or pricing value, required to successfully conduct a transaction or execute a contract on the Ethereum Blockchain platform.
12. On the Ethereum network, ether is a unit that measures the computational power and fee required to run a smart contract or a transaction.
13. A Decentralized Autonomous Organization (DAO) is also a computer program than runs on top of a Blockchain and embedded within it are governance and business logic rules.
14. Initial Coin Offerings (ICOs) are a popular fundraising method used primarily by startups wishing to offer products and services, usually related to the crypto-currency and Blockchain space.
15. A DAO is an organization where users on the Blockchain network are owners themselves and are responsible for the rules, regulations made for the transactions.
16. The Ethereum Blockchain running on the client-server Ethereum network.
17. The DAO was a decentralized autonomous organization that exists as a set of contracts that resides on the Ethereum Blockchain.

18. A fork is defined variously as, "what happens when a Blockchain diverges into two potential paths forward."
19. A hard fork is a new software update implemented by a Blockchain on nodes that is incompatible with the existing Blockchain and causing a permanent split into two separate chains that run in parallel.
20. A soft fork refers to the changes applied to a Blockchain for modifying or adding any functionality without causing any fundamental structural change.
21. Examples of hard forks includes Bitcoin Cash (BCH) Ethereum Classic (ETC) while an example of a Bitcoin soft fork is Segregated Witness (Segwit).
22. A ICO was instantiated on the Ethereum Blockchain, and the code of the DAO is open-source.
23. Initial Coin Offerings (ICOs) are a popular fundraising method used primarily by startups wishing to offer products and services, usually related to the crypto-currency like Bitcoin or Ether and Blockchain space.
24. An Ethereum dApp development involves direct interaction of the dApp with the decentralized Ethereum Blockchain consisting of peer-to-peer nodes, all working together to reach a consensus required to confirm transactions.
25. Ethereum is a Blockchain platform with its own cryptocurrency, called Ether and its own programming language, Solidity.

Answers

1. (T)	2. (F)	3. (T)	4. (T)	5. (T)	6. (T)	7. (F)	8. (T)	9. (T)	10. (T)
11. (T)	12. (T)	13. (F)	14. (T)	15. (T)	16. (F)	17. (T)	18. (T)	19. (T)	20. (T)
21. (T)	22. (F)	23. (T)	24. (T)	25. (T)					

Q.IV Answer the following Questions:

(A) Short Answer Questions:

1. What is Ethereum?
2. Define Ethereum network.
3. Define smart contract.
4. What is EVM?
5. Define DAO.
6. What is Ether?
7. What is fork?
8. What is Gas?
9. Define ICO.
10. What is DApps?

(B) Long Answer Questions:

1. What is the Ethereum Network? Explain with diagram.
2. What is Smart Contracts (SC)? Describe its working.
3. What is DAO? Explain in detail.
4. What is gas? Why it is important in Ethereum?
5. Describe is DApps in detail.
6. What is the fork? What are some of the types of forking? Explain with diagram.
7. Differentiate between hard copy and soft copy.
8. Why does it cost money to invoke a method on a smart contract?
9. With the help of diagram describe EVM.