UNIT I

Chapter 1 : Role of Cryptography in Blockchain 1-1 to 1-28

Introduction : Introduction to cryptography, Use of Cryptography in Blockchain, Cryptographic algorithm, cryptographic elements, cryptocurrency and its Benefits, introduction to decentralized system Security, Integrity, and Privacy Issues of a Decentralized System.

1.1 Introduction to Cryptography 1-1

1.1.1 Introduction 1-1

1.1.2 Why do We Need Cryptography? 1-1

1.1.3 Use of Cryptography in Blockchain 1-2

1.2 Types of Cryptography 1-2

1.3 Cryptographic Hash Functions 1-3

1.3.1 Overview of Hash Function 1-3

1.3.2 Properties of Hash Function 1-4

1.3.3 Applications of Hash Functions 1-4

1.4 Cryptography Algorithms 1-5

1.4.1 Symmetric Key Cryptography 1-5

1.4.2 Asymmetric Key Cryptography 1-6

1.4.3 Difference between DES and AES 1-9

1.5 Elliptic-Curve Cryptography (ECC) 1-10

1.5.1 Pros and Cons of ECC 1-13

1.6 Comparison Symmetric Vs. Asymmetric Key Cryptography 1-13

1.7 SHA (Secure Hash Algorithm) 1-14

1.7.1 A History of SHA Hashing Algorithms 1-14

1.7.2 What is the SHA 256 Algorithm? 1-14

1.7.3 SHA 256 Terminology 1-15

1.7.4 Uses of SHA 1-15

1.7.5 Use Cases of SHA 256 1-16

1.7.6 How Does the SHA 256 Algorithm Work? 1-16

1.8 Introduction to Digital Signature Algorithms 1-17

1.8.1 Digital Signature Algorithm (DSA) 1-17

1.8.2 Pros of using Digital Signature Algorithm 1-18

1.8.3 Cons of using Digital Signature Algorithm 1-18

1.9 Merkle Tree 1-19

1.9.1 Concept and Overview 1-19

1.9.2 What is a Merkle Root? 1-19

1.9.3 Working of Merkle Trees 1-20

1.9.4 Benefits of Merkle Tree in Blockchain 1-21

1.9.5 Use-Cases of Merkle Tree in Blockchain 1-21

1.10 Currency, Cryptocurrency and its Benefits 1-21

1.10.1 Fiat Money 1-21

1.10.1(A) How Does Fiat Money Work ? 1-21

1.10.1(B) Advantages and Disadvantages of Fiat Currency 1-22
1.10.2 Evolution of Currency 1-22
1.10.3 What is Cryptocurrency ? 1-23
1.10.4 Types of Cryptocurrency 1-24
1.10.5 What is Decentralization? 1-24

UNIT II

Chapter 2 : Introduction to Blockchain Technology 2-1 to 2-38

Introduction : What is bitcoin, Mechanics of Bitcoin, bitcoin transaction, Introduction of Block chain, History of Blockchain, Block chain Technology Definition, Types of Block Chain, Peer to Peer Network, platform for decentralization, Transactional blocks, why use blockchain technology.

2.1 What is Bitcoin ? 2-1
2.2 History of Bitcoin 2-2
2.3 Bitcoin Transaction 2-3
2.3.1 Bitcoin Wallet 2-3
2.3.2 Working of Bitcoin Transaction 2-4
2.3.3 Transaction Inputs and Outputs 2-5
2.3.4 Transaction Chains 2-5
2.3.5 Making Change 2-6
2.3.6 Common Transaction Forms 2-6
2.3.7 Constructing a Transaction 2-8
2.3.8 Getting the Right Inputs 2-8
2.3.9 Creating the Outputs 2-8
2.3.10 Adding the Transaction to the Ledger 2-9
2.3.11 Bitcoin Mining 2-9
2.3.12 Mining Transactions in Blocks 2-10
2.3.13 Spending the Transaction 2-11
2.4 Mechanics of Bitcoin 2-11
2.4.1 Bitcoin Working 2-11
2.4.2 Buy Bitcoin 2-12
2.4.3 Transactions 2-12
2.4.4 Bitcoin Mining 2-12
2.4.5 So what do Miners actually do? 2-12
2.4.6 Value of Bitcoin 2-13
2.4.7 Advantages and Disadvantages of Bitcoins 2-13
2.4.7(A) Advantages of Bitcoins 2-13
2.4.7(B) Disadvantages of Bitcoin 2-14
2.4.8 Bitcoin Summary 2-14
2.5 Introduction of Block Chain 2-15
2.6 History of Blockchain 2-15
2.7 Block Chain Technology Definition 2-16
2.7.1 How does the Blockchain Work? 2-16

2.7.2 Features of Blockchain 2-17
2.8 Types of Block Chain 2-19
2.8.1 Public Blockchains 2-19
2.8.2 Private Blockchain Networks 2-21
2.8.3 Consortium Blockchain 2-22
2.8.4 Comparison of Different Types of Blockchain 2-23
2.9 Centralized Vs. Decentralized Systems 2-24
2.9.1 What does Centralization Mean? 2-24
2.9.2 Advantages of Centralization 2-25
2.9.3 Disadvantages of Centralization 2-25
2.10 What is Decentralization? 2-26
2.11 What is a Distributed System? 2-27
2.12 Distributed Ledger 2-28
2.13 Transactional Blocks 2-30
2.14 Important Properties of Blockchain 2-32
2.15 Blockchain for Industries 2-33
2.16 Blockchain Limitations 2-33
2.17 Blockchain Adoption 2-34

UNIT III

Chapter 3 : Blockchain Platforms : Ethereum 3-1 to 3-49

Blockchain Platform introduction, what is Ethereum, Ethereum feature,Components of Ethereum Ecosystem, Ethereum Programming Languages, Runtime Byte Code, Blocks and Blockchain, How Smart Contracts Work.

Introduction to Tokenization : What is token, technology behind tokenization, how blockchain tokenization can help in enterprise systems, Tokenizing Shares and Fund Raising, challenges to tokenization

3.1 Blockchain Platform Introduction 3-1
3.1.1 Ethereum 3-1
3.1.2 Hyperledger 3-2
3.1.3 R3 Corda 3-2
3.2 Key Features while Considering Blockchain Platforms 3-3
3.2.1 Benefits of Utilizing Blockchain Platform 3-4
3.2.2 Comparison of Blockchain Platforms 3-4
3.3 What is Ethereum ? 3-5
3.3.1 Compared to Bitcoin 3-6
3.3.2 The Birth of Ethereum 3-6
3.3.3 Ethereum's Four Stages of Development 3-8
3.3.4 What Is Ethereum 2.0? 3-9
3.4 Ethereum : A General-Purpose Blockchain 3-9
3.4.1 Components of Ethereum 3-10
3.4.2 Ethereum and Turing Completeness 3-11
3.4.3 Keys and Addresses 3-12
3.5 Types of Accounts 3-12

1 Role of Cryptography in Blockchain

Unit I

Syllabus

Introduction to cryptography, Use of Cryptography in Blockchain, Cryptographic algorithm, Cryptographic elements, Cryptocurrency and its benefits, Introduction to decentralized System Security, Integrity, and Privacy Issues of a Decentralized System.

1.1 Introduction to Cryptography

1.1.1 Introduction

Cryptography is the study of using mathematics to encrypt and decrypt information or data to be stored or transmitted on insecure networks. Cryptography helps you to store vital information or transmit it across public or private networks (e.g. Internet) so that it cannot be perceived by anyone except the intended recipient.

✍ ***Definition:****Cryptography is defined as storing or transferring encrypted data between sender and receiver on public or private networks such that only intended recipients can read it on receiving it.*

1.1.2 Why do We Need Cryptography?

We need cryptography to have secure communication. Following are the goals of cryptography :

- **Privacy and Confidentiality :** The message to be transmitted shall be encrypted using a secret key by the sender and similarly it shall be decrypted only by the intended recipient by his/her own secret key.
- **End-point authentication :** Authentication is a mechanism that is used whenever one wants to know exactly who is using or viewing the message. Usually login and password is used to confirm the identity and view the message.
- **Integrity of a message :** It is the mechanism to ensure that the message is not changed or modified while the message is being transmitted between sender and receiver.
- **Non-repudiation :** Sender cannot deny his intentions of transmitting a message later, once it is sent by a sender to receiver, this is known as non-repudiation. Digital signatures are the most commonly used mechanism to achieve and ensure non-repudiation.
- **Key Exchange :** It is the mechanism by which a sender and receiver can share cryptographic keys among them so that they can be used to encrypt and decrypt the message.

1.1.3 Use of Cryptography in Blockchain

Cryptography and hashing

- Cryptography is a means of protecting data against unwanted access. Cryptography is employed in the blockchain to safeguard transactions between two nodes in a blockchain network. As discussed in above sections,, there are two key ideas in a blockchain: cryptography and hashing.
- Cryptography is utilized to trustfully identify all network participants, allowing for openness of interactions while protecting all network actors' privacy. It is a useful tool for handling tokens using a programme called "wallet." Furthermore, cryptography is an essential component of the blockchain consensus system.
- Blockchain uses hashing techniques to create secured blocks in a blockchain. The Bitcoin Network primarily uses hashes in conjunction with digital signatures to secure the integrity of data transmitted over the blockchain, which employs public-key cryptography. Hashes are also employed in the context of the "Proof-of-Work" consensus technique. Bitcoin employs public-key cryptography, specifically elliptic-curve cryptography.

Encryption in blockchain

- Cryptocurrencies are a prominent real-world use of cryptography in blockchain. Cryptocurrencies employ encryption to ensure that transactions are anonymous, safe, and "trustless." Cryptographic hashing is one of the most well-known applications of cryptography. Hashing allows for immutability in the blockchain. Asymmetric-key algorithms and hash functions are the two types of cryptographic algorithms used in blockchains. Hash functions are employed to give each participant the capability of a single view of the blockchain. As a hash function, blockchains often employ the SHA-256 hashing algorithm.
- Next section gives an overview of the cryptographic algorithms used in blockchain and an overview of digital signatures. Further the use of Merkel Tree is explained which is a prominent hashing technique used in blockchain.

1.2 Types of Cryptography

As indicated in Fig. 1.2.1, types of Cryptography techniques are :

1. Symmetric Encryption
2. Asymmetric Encryption
3. Hash Functions

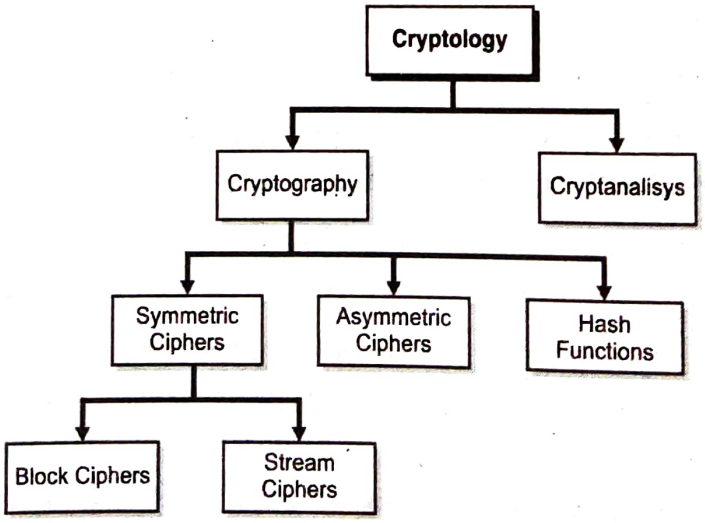


Fig. 1.2.1 : Cryptology

Cryptographic elements

- **Plaintext (Message)** : It is the message in text and human readable format which a sender wants to communicate to the receiver.
- **Sender:** Sender is a person or a device who is sending the message/plain text to the receiver.
- **Receiver:** Receiver is a person or a device who is receiving the message/plain text from the sender.
- **Encryption Key (Secret Key or Private-Public Key Mechanism):** It is the secret key, used to encrypt the message and convert it into cipher text.
- **Decryption Key (Secret Key or Private-Public Key Mechanism):** It is the secret key, used to decrypt the received cipher text and convert into the original message/plain text.
- **Encryption Algorithm:** It is the process of encryption used by sender to encrypt the message/plaintext to convert it into cipher text using encryption key.
- **Decryption Algorithm:** It is the process of decryption used by the receiver to decrypt the cipher text into message/plaintext using a decryption key.
- **Ciphertext:** It is the text which is not in readable format to the human like plaintext.

1.3 Cryptographic Hash Functions

1.3.1 Overview of Hash Function

- A cryptographic hash function is a mathematical function used in cryptography. Typical hash functions take inputs of variable lengths to return outputs of a fixed length. It is a mathematical function that transforms, or "maps" a given set of data into a bit string of fixed size which is known as the "hash value".
- A cryptographic hash function combines the message-passing capabilities of hash functions with security properties. Hash functions have variable levels of complexity and difficulty.
- Fig. 1.3.2 shows that fixed length output *(n-bit)* is generated when a hash function *h* is applied to input message *m* of arbitrary length. (Fig. 1.3.1)

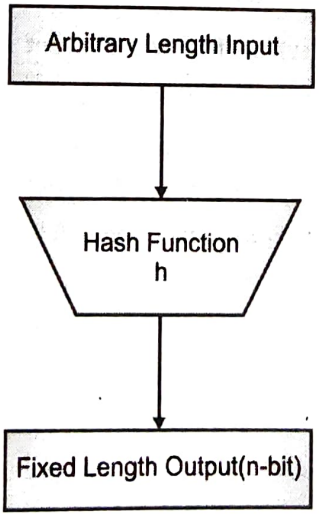


Fig. 1.3.1 : Hash function in cryptography

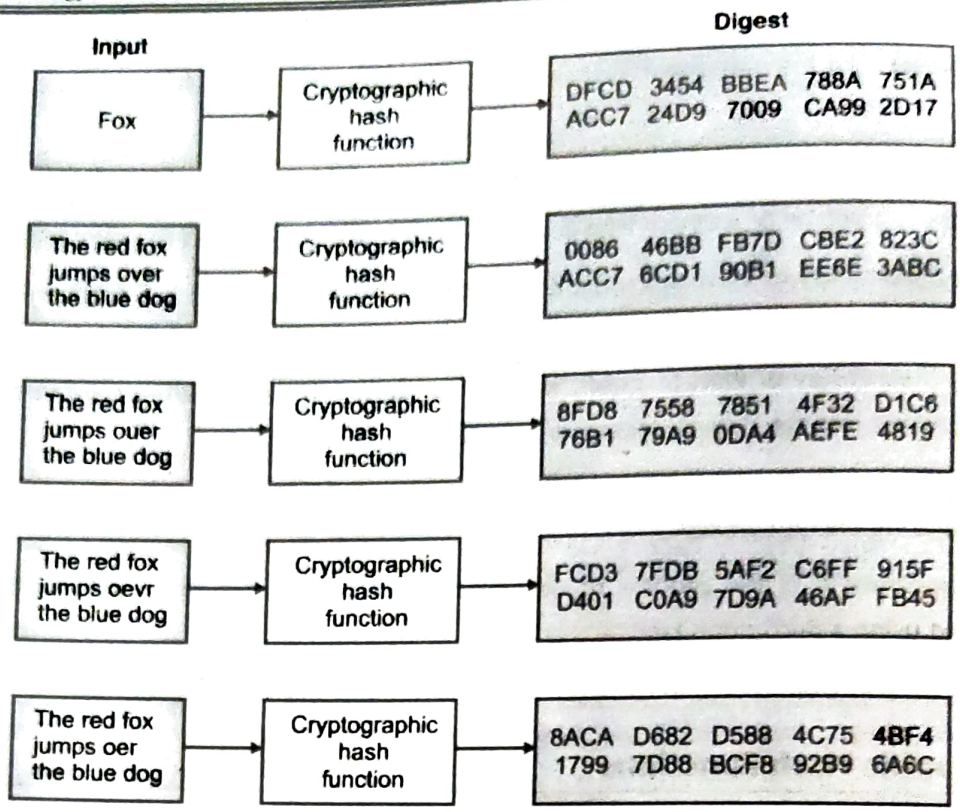


Fig. 1.3.2 : Fixed length output generated from hash function.

1.3.2 Properties of Hash Function

Security level of a cryptographic hash function is defined using following properties :

1. **Preimage resistance :** Given a hash value h, it should be difficult to get any message *m* such that *h* = *hash(m)*. Functions that lack this property are vulnerable to preimage attacks.
2. **Second pre-image resistance :** Given an input m_1, it should be difficult to find a different input m_2 such that $hash(m_1) = hash(m_2)$. This property is sometimes referred to as weak collision resistance. Functions that lack this property are vulnerable to second-preimage attacks.
3. **Collision resistance :** It should be difficult to find two different messages m_1 and m_2 such that $hash(m_1) = hash(m_2)$. Such a pair is called a cryptographic hash collision.
4. **Puzzle Friendliness :** To be referred to as puzzle friendly, a hash function must be true in the sense that there is no more effective approach for solving a computational puzzle based on the hash function than just trying random values from a set of possible solutions until one of them works. A hash function H is said to be puzzle friendly if for every possible n-bit output value y, if k is chosen from a distribution with high min-entropy, then it is infeasible to find x such that $H(k \| x) = y$, in time significantly less than 2^n.

1.3.3 Applications of Hash Functions

Hash functions are used for :

1. Verifying integrity of message
2. Proof of work in cryptocurrency

3. Password verification and security
4. File, information and data identifier
5. Signature generation and its verification

1.4 Cryptography Algorithms

Cryptographic algorithms are broadly classified under the Symmetric and Asymmetric category. Fig. 1.4.1 below shows the name and year of introduction of the algorithm.

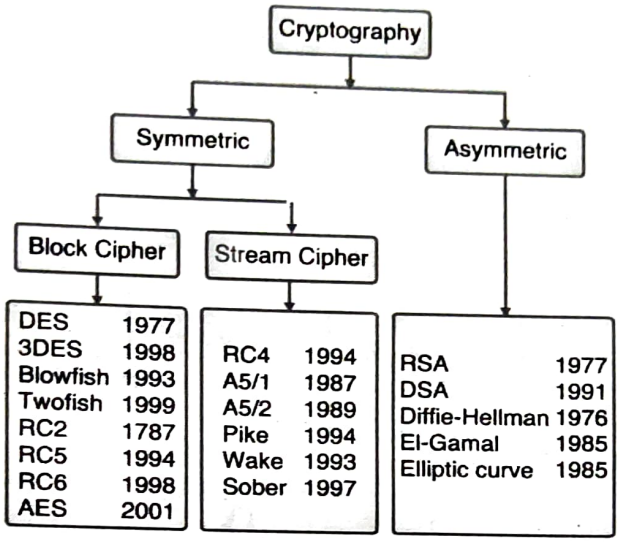


Fig. 1.4.1 : Classification of cryptography algorithms.

Let us see working of some most commonly used Symmetric and Asymmetric algorithms and understand steps in AES, SHA, ECC, ECDSA, DSA algorithm subsequently.

1.4.1 Symmetric Key Cryptography

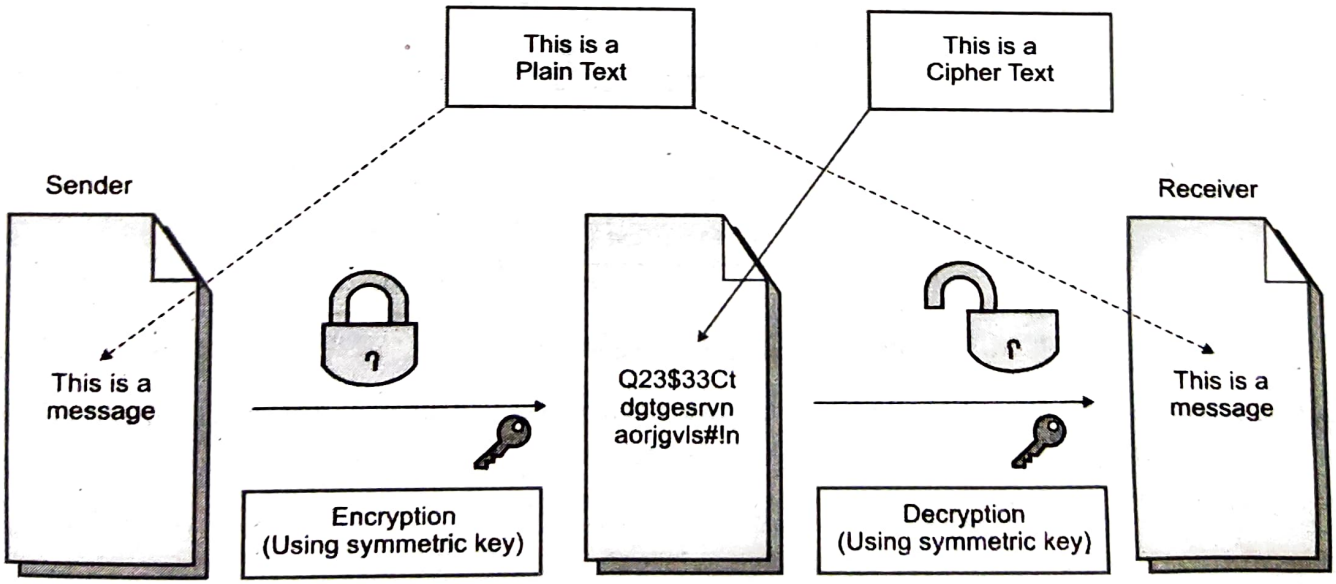


Fig. 1.4.2 : Symmetric key Encryption

- In this type of encryption, sender and receiver share the single key to encrypt and decrypt the message. Here the sender and receiver know the secret key.
- Steps and working of symmetric key encryption is as follows :
  1. Sender and receiver share the secret key through some external means.
  2. The sender encrypts the message (plain text) using his copy of the key at the sender's end. Here the plain text is encrypted to generate the cipher text.
  3. The cipher text is then sent to the receiver over the communication channel.
  4. The recipient decrypts the cipher text using his copy of the key at receiver's end.
  5. Here the cipher text is decrypted back into the original plain text.

  Similar process can be followed vice - a - versa.

1.4.2 Asymmetric Key Cryptography

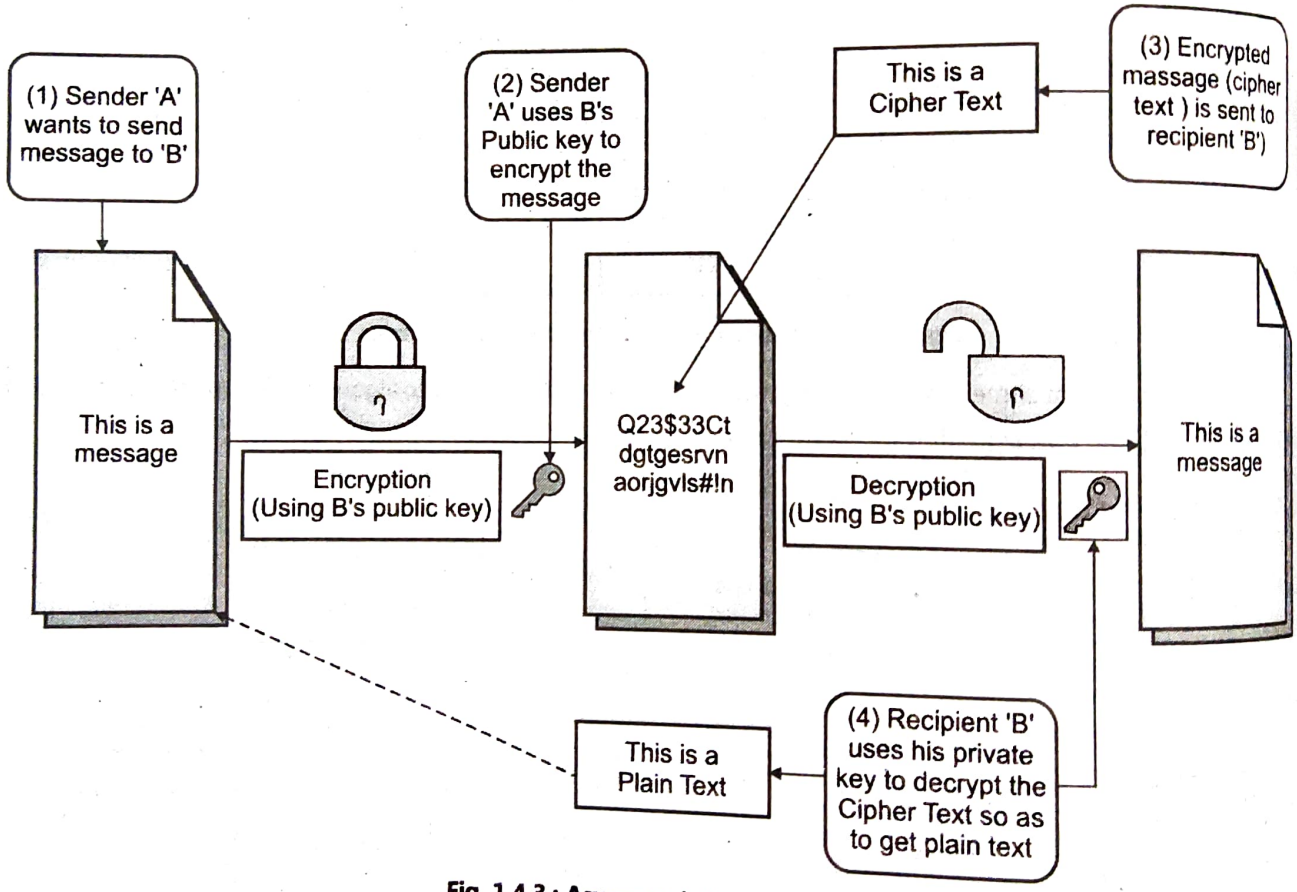


Fig. 1.4.3 : Asymmetric key Encryption

- In this type of encryption, sender and receiver use two different keys that are known as public key and private key to encrypt and decrypt the message. Here the sender and receiver do not share the secret key. As the keys are different it is said as asymmetric key cryptography.
- Steps and working of Asymmetric key encryption is as follows :

- At sender's end,
  1. Sender encrypts the message using the receiver's public key.
  2. The public key of the receiver is publicly available and known to everyone.
  3. Encryption mechanism converts the message(plain text) into a cipher text.
  4. This cipher text can be decrypted only using the receiver's private key.
  5. The cipher text is sent to the receiver over the communication channel.
- At receiver's end,
  1. Receiver decrypts the cipher text using his private key.
  2. The private key of the receiver is known only to the receiver.
  3. Using the public key, it is not possible for anyone to determine the receiver's private key.
  4. After decryption, cipher text converts back into a readable plain text format.

Advanced Encryption Standard (AES)

- AES is known as a block cipher, the standard key size can be 128/192/256 bits. The block size of encrypted data is 128 bits each. Encryption takes ten rounds for 128-bit keys, twelve rounds for 192-bit keys, and fourteen rounds for 256-bit keys.
- Each round of processing involves one single-byte replacement/substitution step, a row-wise permutation step, a column-wise mixing step, and the insertion/addition of the round key. For encryption and decryption, the order in which these four procedures are carried out differs. Except for the last round in each case, the remaining rounds are identical.

Encryption

- AES assumes each block to be a 16 byte (4 byte x 4 byte = 128) grid in a column major configuration.
- Each round comprises of 4 steps :
  - SubBytes
  - ShiftRows
  - MixColumns
  - Add Round Key
- The last round doesn't have the MixColumns round.
- The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.

SubBytes

- This step implements the substitution.
- In this step each byte is substituted by another byte. Its performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a complement of the current byte. The result of this step is a 16 byte (4 x 4) matrix like before.

- The next two steps implement the permutation.

ShiftRows

- This step is just as it sounds. Each row is shifted a particular number of times.
- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.

MixColumns

This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the posit of each byte in the column is changed as a result. This step is skipped in the last round. The fourth row is shifted thr to the left.

Add Round Keys

- Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes not considered as a grid but just as 128 bits of data.
- After all these rounds 128 bits of encrypted data is given back as output. This process is repeated until all the da to be encrypted undergoes this process.

Decryption

- The stages in the rounds can be easily undone as these stages have an opposite to it which when perform reverts the changes. Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.
- The stages of each round in decryption is as follows :
  - Add round key
  - Inverse MixColumns
  - ShiftRows
  - Inverse SubByte
- The decryption process is the encryption process done in reverse so Let us understand the steps with notab differences.

Inverse MixColumns

This step is similar to the MixColumns step in encryption, but differs in the matrix used to carry out the operation

Inverse SubBytes

Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

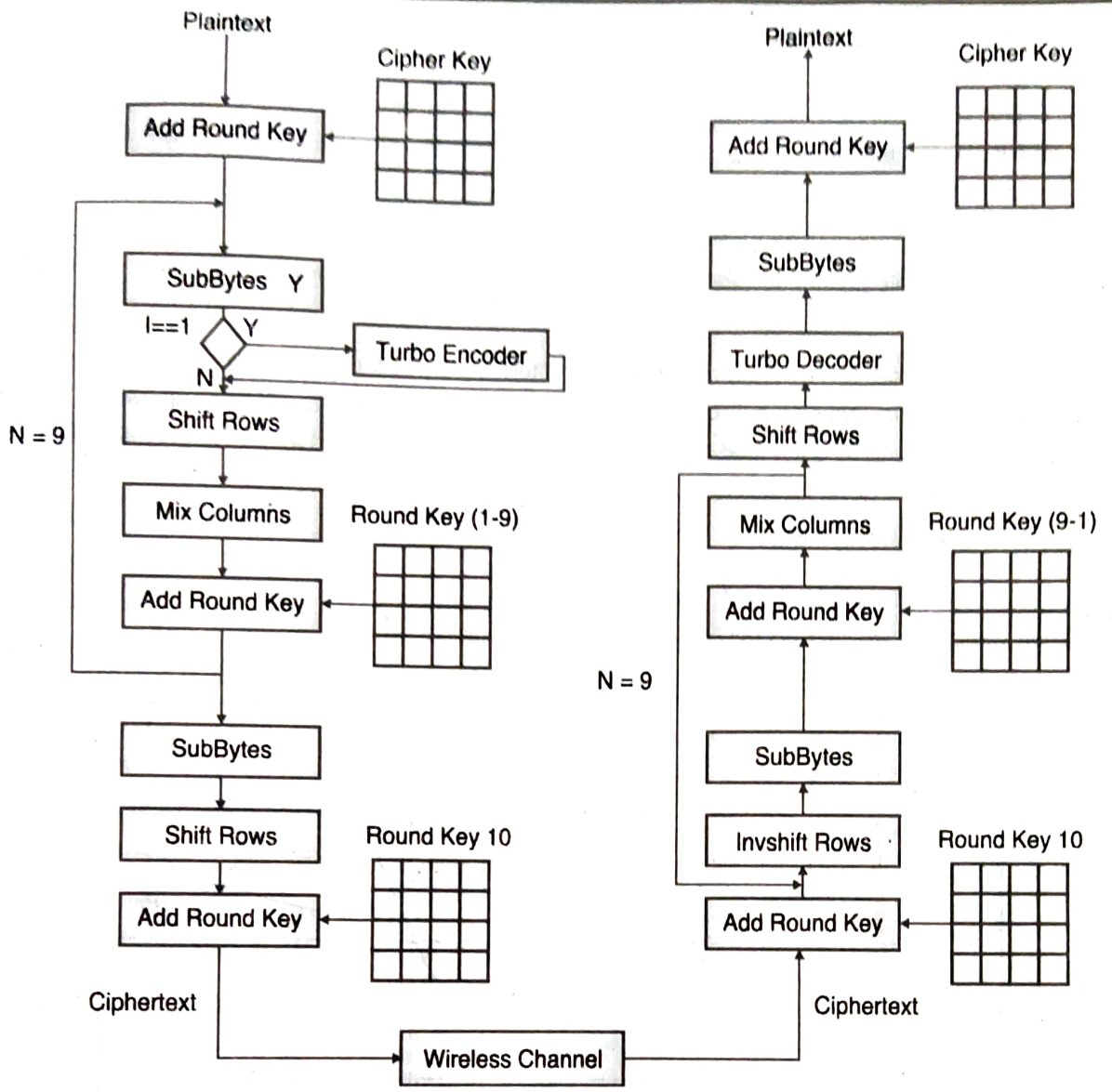


Fig. 1.4.4 : AES workflow and steps

1.4.3 Difference between DES and AES

Table 1.4.1

	DES	AES
Developed	1977	2000
Key Length	56 bits	128, 192, or 256 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block Size	64 bits	128 bits
Security	Proven inadequate	Considered secure

1.5 Elliptic-Curve Cryptography (ECC)

- Elliptic curve cryptography is used to implement public key cryptography. It was discovered by Victor Miller of IBM and Neil Koblitz of the University of Washington in 1985. ECC popularly used an acronym for Elliptic Curve Cryptography. It is based on the latest mathematics and delivers a relatively more secure foundation than the first-generation public key cryptography systems for example RSA.
- In 1985, cryptographic algorithms were proposed based on elliptic curves. An elliptic curve is the set of points that satisfy a specific mathematical equation. They are symmetrical.
- ECC is among the most commonly used implementation techniques for digital signatures in crypto currencies. Both Bitcoin and Ethereum apply the Elliptic Curve Digital Signature Algorithm (ECDSA) specifically in signing transactions. However, ECC is not used only in crypto currencies. It is a standard for encryption that will be used by most web applications going forward due to its shorter key length and efficiency.
- Elliptic curve equation is as follows :

$$y^2 = x^3 + ax + b$$

- Any non-vertical line will intersect the curve in three places or fewer.
- Fig. 1.5.1 shows the curve can be plotted on the graph and the line is intersecting at points A, B and C.

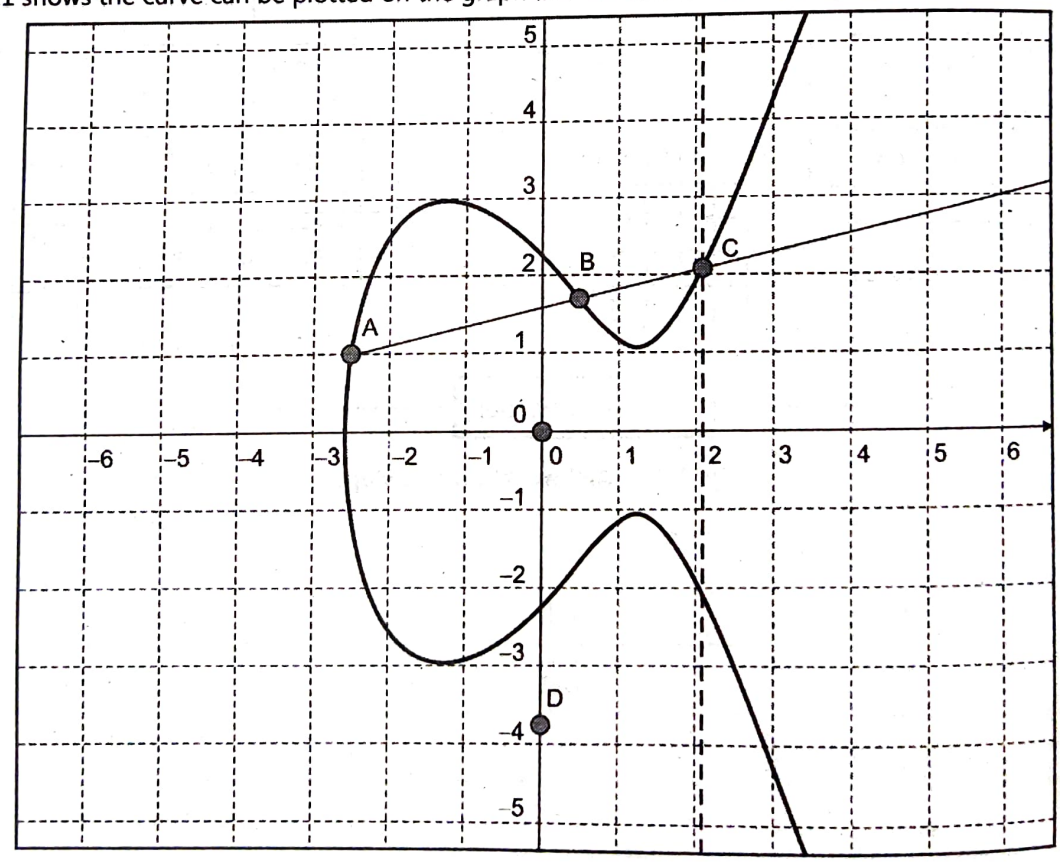


Fig. 1.5.1 : Elliptical Curve Cryptography

- ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.

- ECC is used for key agreement, digital signatures, pseudo-random generators and several integer factorization algorithms.
- Following Table 1.5.1 shows the key length (size) required to provide the equivalent level of security. For example, an elliptic curve cryptography key of 256 bit achieves the same level of security as an RSA of 3072 bit.

Table 1.5.1 : Key length (RSA and ECC)

RSA Key Length (bit)	ECC Key Length (bit)
1024	160
2048	224
3072	256
7680	384
15360	521

Real time use cases under Elliptic Curve Schemes

1. Elliptic Curve Digital Signature Algorithm (ECDSA)
2. Elliptic Curve Diffie-Hellman (ECDH)

1. Elliptic Curve Digital Signature Algorithm (ECDSA)

The Elliptic Curve Digital Signature Algorithm (ECDSA) is an elliptic-curve variation of the Digital Signature Algorithm (DSA).

ECDSA steps and algorithm

1. Chose Parameters
   - 1.1 Choose an elliptic curve $E_p(a, b)$: $y^2 = x^3 + ax + b \bmod p$, where x, y, a, b $\epsilon GF(p)$;
   - 1.2 Choose a base point G and get its multiplicative order n, which means $n \times G = 0$, where 0 is the identity element;
   - 1.3 Choose an integer $d \epsilon [1, n-1]$ as the private key, and calculate $Q = d \times G$ as the public key.
2. Sign
   - 2.1 Given a message m ✇Calculate h(m) and let z be the L_n leftmost bits s of h(m);
   - 2.2 Select $k \epsilon [1, n-1]$ ✇Calculate a curve point $(x_1, y_1) = k \times G$;
   - 2.3 Calculate $r = x_1 \bmod n$ and $s = k^{-1}(z + rd) \bmod n$;
   - 2.4 The signature is (r, s).

Note that : Q, E_p (a, b), G, n are public, d, k are kept secret.

3. Verify
   - 3.1 Receive a message m and its signature (r,s);
   - 3.2 Calculate h(m) and get z;

3.3 Calculate $u_1 = zs^{-1} \bmod n$ and $u_2 = rs^{-1} \bmod n$;

3.4 Calculate $(x_1, y_1) = u_1 \times G + u_2 \times Q$;

3.5 If $r = x_1 \bmod n$, then the signature is valid.

Correctness : $(x_1, y_1) = u_1 \times G + u_2 d \times G = (zs^{-1} + rs^{-1}d) \times G = (z + rd)\, s^{-1} \times G = k \times G$;

2. ECDH

- The Diffie-Hellman key exchange algorithm is a mechanism for two people to safely establish a shared secret (Alice and Bob). Elliptic-curve Diffie-Hellman (ECDH) allows two parties to establish the shared secret, each with an elliptic-curve public-private key pair. This shared secret can be used directly as a key or to generate another key.
- Following that, the key, or the derived key, may be used to encrypt subsequent communications with a symmetric-key cypher. It is a Diffie-Hellman protocol variation that employs elliptic-curve cryptography.
- **Working of Elliptic-curve Diffie–Hellman Key Exchange Algorithm (ECDH):** Following Fig. 1.5.2 illustrates the working of ECDH with example.

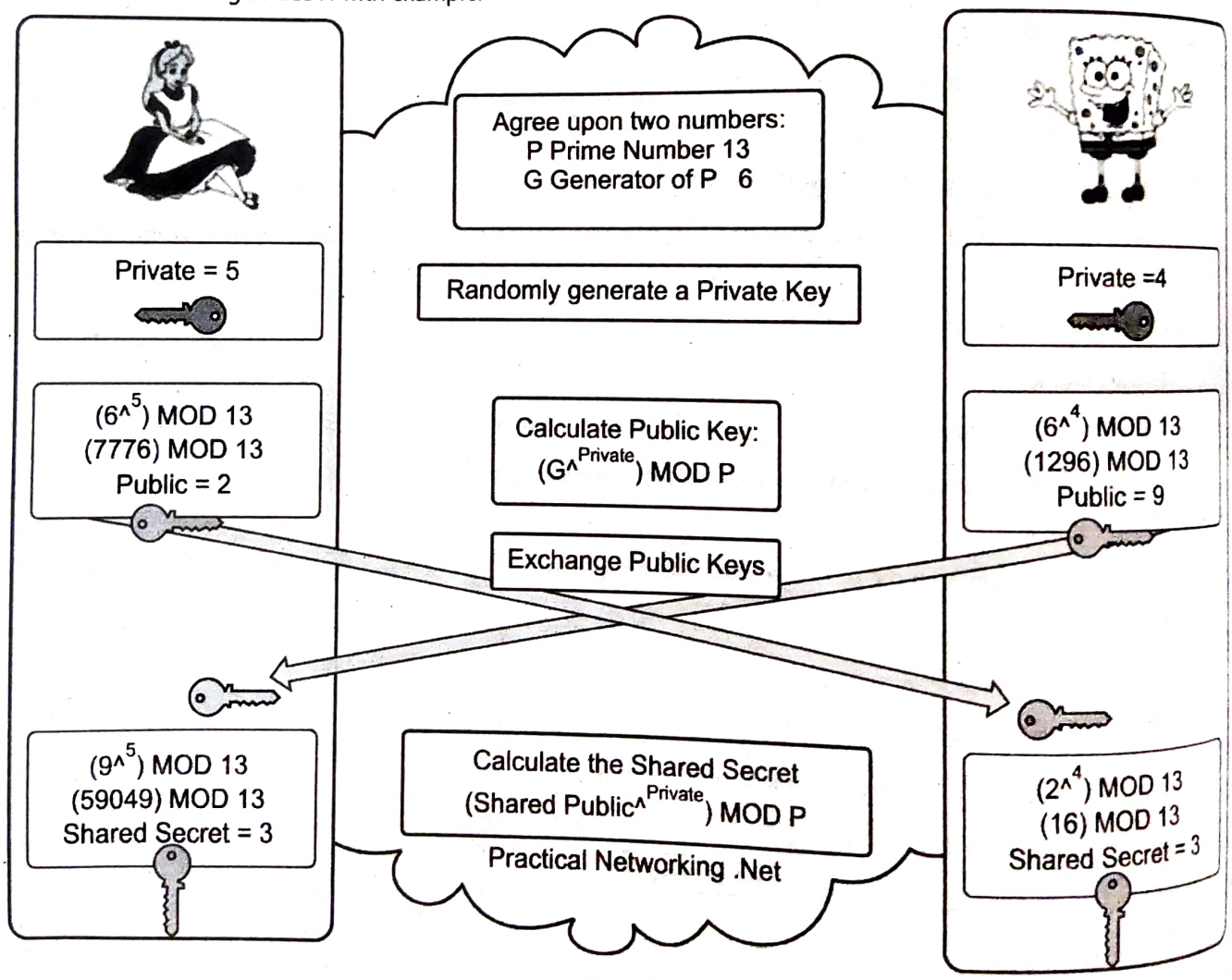


Fig. 1.5.2

1.5.1 Pros and Cons of ECC

Pros of ECC

1. **Shorter Key Length**

   Same level of security as RSA achieved at a much shorter key length

2. **Better Security**

   - Secure because of the ECDLP.
   - Higher security per key-bit than RSA.

3. **Higher Performance**

   - Shorter key-length ensures lesser power requirement – suitable in wireless sensor applications and low power devices.
   - More computation per bit but overall lesser computational expense or complexity due to lesser number of key bits.

Cons of ECC

1. **Relatively newer field**

   - Idea prevails that all the aspects of the topic may not have been explored yet – possibly unknown vulnerabilities.
   - Doesn't have widespread usage.

2. **Not perfect**

   - Attacks still exist that can solve ECC (112 bit key length has been publicly broken).
   - Well known attacks are the Pollard's Rho attack (complexity O(√n)), Pohlig's attack, Baby Step, Giant Step etc.

1.6 Comparison Symmetric Vs. Asymmetric Key Cryptography

Table 1.6.1

Parameter	Symmetric Key Cryptography	Asymmetric Key Cryptography
Key used	Single key	Public and Private key
Key exchange mechanism	Through some external means	No need to exchange keys
Knowing key	key must not be known to anyone else other than sender and receiver.	Receiver's public key can be known to everyone, but the private key should be known to only the receiver.
Algorithms used	Advanced Encryption Standard (AES) Data Encryption Standard (DES)	RSA Algorithm Diffie-Hellman Key Exchange
Advantages	They are efficient. They take less time to encrypt and decrypt the message.	Robust method. Less susceptible to third-party security breach attempts.

Parameter	Symmetric Key Cryptography	Asymmetric Key Cryptography
Disadvantages	The number of keys required is very large. In symmetric key cryptography- Each pair of users requires a unique secret key. If N people in the world want to use this technique, then there needs to be N(N-1) / 2 secret keys.	It involves high computational requirements. It is slower than symmetric key cryptography.

1.7 SHA (Secure Hash Algorithm)

1.7.1 A History of SHA Hashing Algorithms

- Secure Hash Algorithms (SHA) were designed by the National Security Agency (NSA). The U.S. government patented the algorithm, then released it under a royalty-free license so anybody could use it for free. Hashing algorithms are used as one-way functions, meaning that they are designed to be processed one way but are too cumbersome to reverse engineer.
- The SHA-0 algorithm came first in 1993. SHA-1 followed in 1995, and, although it has been cracked, SHA-1 is still in use today. The SHA-2 family, of which SHA 256 is a member, was released in 2001 and includes six hash functions :
  - SHA 224
  - SHA 256
  - SHA 384
  - SHA 512
  - SHA 512/224
  - SHA 512/256
- Each member of the family contains a set of cryptographic hash algorithms that convert data into a unique hash value. In the case of SHA 256, the hash value is 256 bits (equal to 32 bytes). The six hash functions have different numbers of rounds and use different shift amounts and additive constants.

1.7.2 What is the SHA 256 Algorithm?

- SHA-256, which stands for secure hash algorithm 256, is a cryptographic hashing algorithm (or function) that is used for message, file, and data integrity verification. It is part of the SHA-2 family of hash functions and uses a 256-bit key to take a piece of data and convert it into a new, unrecognizable data string of a fixed length. This string of random characters and numbers, called a hash value, is also 256 bits in size.
- SHA 256 is the industry standard used by the U.S. federal government and many other organizations globally.
- Let us consider the following example. Say you write the message "**Good morning**" and apply a SHA-256 hash function to it.
- It will look like this : **90a90a48e23dcc51ad4a821a301e3440ffeb5e986bd69d7bf347a2ba2da23bd3**

- Now, say you decide to do the same with a similar message, "**Good morning!**" It will result in an entirely different string of hexadecimal characters of the same length.
- The following value shows the SHA-256 hash values of two texts that differ by one character :

c9ebfb6f4b8e880908a737b8d770aa3a518fb6053b327720e8dcc79609c32858

- This example illustrates that adding an exclamation mark changes the entire resulting hash digest.
- As you can see, when just one character is added to the message, the hash value changes completely. The number of characters in the hash values remains the same, regardless of the number of characters in the original text. This helps to hide the size of the original input data because no matter how big or small the input a single word or an entire book it will result in a hash value of the same length.

1.7.3 SHA 256 Terminology

To properly understand SHA 256, we need to grasp the following terms :

1. **Rounds**

A round is a set of functions repeatedly carried out in the algorithm to scramble the data beyond recognition. There are 64 rounds in the SHA 256 algorithm.

2. **Shift Amount**

The shift amount is a fixed method used to shuffle bits. In SHA 256, the blocks are divided into eight segments that are 32 bits each. These eight pieces are then shifted in a specific way that scrambles and randomizes the data.

3. **Additive Constants**

The values added to the blocks are called additive constants. In SHA 256, there are 64 constants used to add to the blocks. These numbers are the cube roots of the first 64 prime numbers. This step uses the first 32 bits of the fractional numbers.

1.7.4 Uses of SHA

We can use SHA 256 in situations where we need the following :

1. **Protecting the Data Integrity**

SHA 256 ensures data integrity so that both parties can be sure that the communication is from the person they think it is. The recipient device creates a hash of the original message and compares it to the hash value sent by the sender. If both hash values are equal, the message has not been tampered with during transit.

2. **Verifying Digital Signatures**

- A digital signature is a way of signing digital documents, code, or software that is verifiable by the recipient or users. This way, they know whether you created or signed the document or file, or if the item in question was created or altered by someone else.
- A digital signature is created by applying a hash to the file and then using an encryption algorithm to encrypt it via private and public keys. The private key is used when the signature owner signs the document; the public key is used by the recipient to decrypt the message on their end.

- But all of that would mean nothing without verification, which is where SHA-256 comes in. Hashing ensures that the digital signature has not been altered since it was signed. The recipient's system runs the hashing algorithm on its end and uses the public key to decrypt the message. If it matches, then it knows the data is unaltered and authentic.

3. **Verifying Blockchain Transactions**

SHA-256 is also used in some popular blockchain applications, most notably the crypto currency Bitcoin. Block headers are integral to blockchains, as they help to "chain" one block of transactions to the next in a specific order. SHA-256 hash helps ensure that no previous blocks are changed without altering the new block's header.

1.7.5 Use Cases of SHA 256

SHA 256 is one of the most reliable algorithms for authentication and message integrity verification. It is used with many different authentication and encryption protocols and processes, including :

- **SSL/TLS** - Secure socket layer (SSL) and transport layer security (TLS) are encryption protocols that maintain data integrity and confidentiality while it is in transit.
- **SSH** - Secure Shell (SSH) protocol creates a secure channel between two devices for data transfer.
- **IPsec** - Internet protocol security (IPsec) is a collection of protocols designed to secure data transfer across different IP networks.
- **PGP** - Pretty good privacy (PGP) is an encryption algorithm used to sign, encrypt, and decrypt emails, files, directories, or a disk partition.
- **S/MIME** - Secure/multipurpose internet mail extensions (S/MIME) is an algorithm to secure the integrity and confidentiality of emails.
- **Blockchain** - In a blockchain, preceding hash values are used to calculate the hash value of the current block.

1.7.6 How Does the SHA 256 Algorithm Work?

SHA 256 is very complex. We will try to understand it from a broad perspective. FIPS-180 describes SHA algorithm as involving two essential stages :

- **Pre-processing** - This is where the message is padded, broken down into smaller blocks, and initialization values are set.
- **Hash computation** - This process involves a series of operations that result in a series of hash values. The 256-bit resulting hash digest we get at the very end is generated by computing these various hash values.
- SHA 256 follows the steps given below :

1. First, data is converted into binary. Binary code uses 0s and 1s to store information. For example, the letter 'A' is written as '01000001' in this basic computer language.
2. The binary data is divided into blocks of 512 bits. If the block is smaller than 512, it will be expanded to that size by adding bits of "padding". If it is larger, it will be broken into blocks of 512 bits. (If the last block is not exactly 512 bits, padding is added to the last block to make it 512 bits.)

3. The message is further divided into smaller blocks that are 32 bits each.
4. Sixty-four iterations (rounds) of compression functions are performed, wherein the hash values generated above are rotated in a specific pattern and additional data gets added.
5. New hash values are created from the output of the previous operations.
6. In the last round, one final 256-bit hash value is produced; this hash digest is the end product of SHA 256.

1.8 Introduction to Digital Signature Algorithms

DSA (Digital Signature Algorithm) incorporates the algebraic properties of discrete logarithm problems and modular exponentiations for generating an electronic signature for various applications. It was proposed in 1991 and was adopted as a Federal Information Processing Standard by NIST (National Institute of Standards and Technology) in 1994.

1.8.1 Digital Signature Algorithm (DSA)

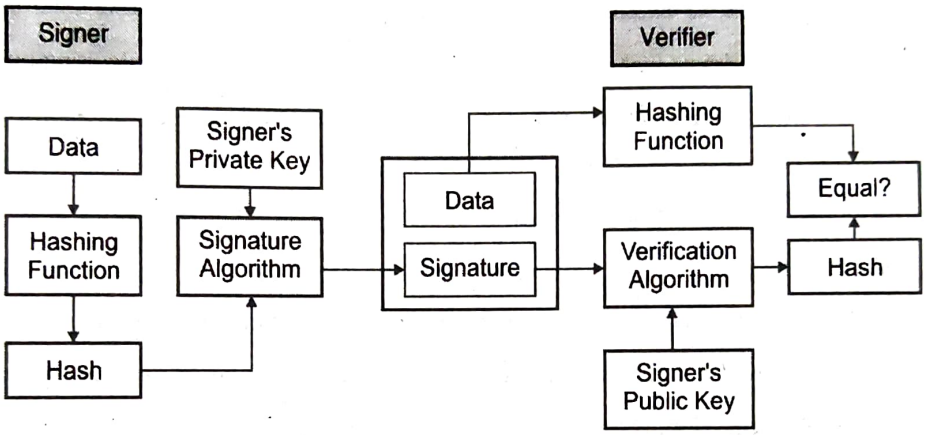


Fig. 1.8.1 : Digital Signature Algorithm

- DSA stands for Digital Signature Algorithm. It is used for digital signature and its verification. It is based on the mathematical concept of modular exponentiation and discrete logarithm. It was developed by National Institute of Standards and Technology (NIST) in 1991.
- It involves four operations :
  1. Key Generation
  2. Key Distribution
  3. Signing
  4. Signature Verification
- Steps at signer's end :
  1. Message or data is hashed using a hashing function to create a digest.
  2. Sender uses his private key to sign the generated digest in step 1 using the signature algorithm.
- Steps at Recipient's end :
  - Recipient on receiving the data and signature runs a verifier algorithm and used sender's public key.

- If the generated hash value from above step matches with the hash value which was generated from the earlier hashing then recipient is satisfied with the received data and signature. Else if matching fails, then the signature of the sender is not valid.
- The digital signature process can be divided into 2 parts :

1. Signature Generation

1. Generating a pair of public keys and providing a key by the sender of the message.
2. Generating the message digest from the message using a hash function.
3. Generating the digital signature from the message digest with the private key.
4. Sending the message, the digital signature, and the public key to the receiver.

2. Signature Verification

1. Generating the message digest from the message using the same hash function.
2. Verifying the digital signature with message digest using the public key.
3. There are 2 popular algorithms that are used to generate and verify digital signature using public keys:
4. RSA (Rivest, Shamir and Adleman) algorithm developed by Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman in 1976.
5. DSA (Digital Signature Algorithm) algorithm developed by the US government in 1991.

- The benefits DSA offers are :

1. **Non-Repudiation :** after signature verification, the sender cannot claim to have not sent the data.
2. **Integrity** : data modification during transmission prevents final verification or message decryption.
3. **Message Authentication :** right private/public keys combination help verify sender origin.

1.8.2 Pros of using Digital Signature Algorithm

1. Fast signature computation
2. Requires less storage space for the entire process
3. Freely available (Patent-free) for cost-free global use.
4. Small signature length
5. Observation in real-time
6. Non-invasive
7. DSA is accepted globally for legal compliance.
8. Time-efficient (low time consumption in comparison to processes of physical signing etc.)

1.8.3 Cons of using Digital Signature Algorithm

1. The process does not include key exchange capabilities.
2. The underlying cryptography must be new to ensure its strength.

3. The standardization of computer hardware and software vendors on RSA may cause problems due to DSA's second authentication standard.
4. The complex remainder operations require a lot of time for computation and hence signature verification.
5. It only ensures authentication, not confidentiality, as the algorithm does not encrypt the data.

1.9 Merkle Tree

1.9.1 Concept and Overview

- Merkle trees, also known as Binary hash trees, are a prevalent sort of data structure in computer science.
- In bitcoin and other cryptocurrencies, they're used to encrypt blockchain data more efficiently and securely.
- It is a mathematical data structure made up of hashes of various data blocks that summarize all the transactions in a block.
- It also enables quick and secure content verification across big datasets and verifies the consistency and content of the data.

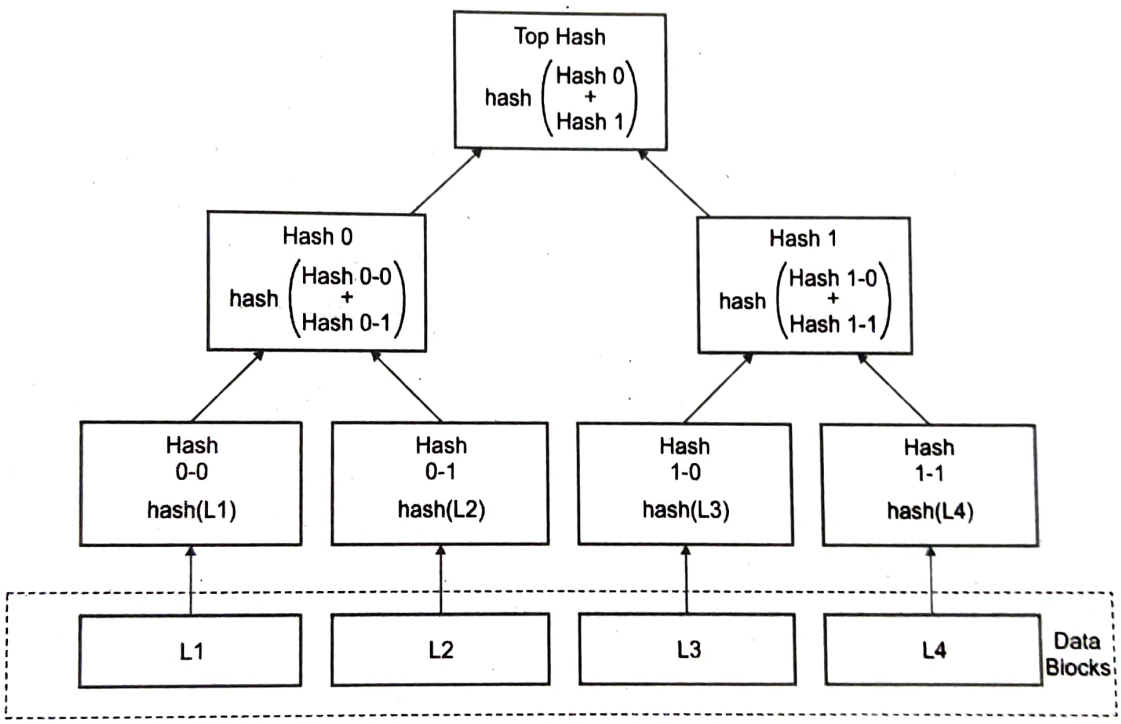


Fig. 1.9.1 : Markle Tree (Binary Hash Tree)

1.9.2 What is a Merkle Root?

- A Merkle root is a simple mathematical method for confirming the facts on a Merkle tree.
- They are used in cryptocurrency to ensure that data blocks sent through a peer-to-peer network are whole, undamaged, and unaltered.
- They play a very crucial role in the computation required to keep cryptocurrencies like bitcoin and ether running.

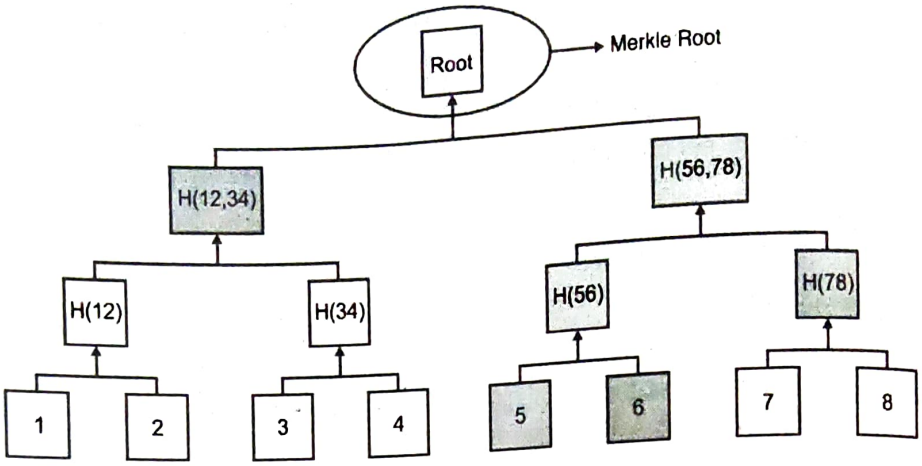


Fig. 1.9.2 : Markle Root

1.9.3 Working of Merkle Trees

- A Merkle tree totals all transactions in a block and generates a digital fingerprint of the entire set of operations, allowing the user to verify whether it includes a transaction in the block.
  - Merkle trees are made by hashing pairs of nodes repeatedly until only one hash remains; this hash is known as the Merkle Root or the Root Hash.
  - They are built from the bottom, using Transaction IDs, which are hashes of individual transactions.
  - Each non-leaf node is a hash of its previous hash, and every leaf node is a hash of transactional data.
- Now, look at a little example of a Merkle Tree in Blockchain to help you understand the concept.
- Consider the following scenario: A, B, C, and D are four transactions, all executed on the same block. Each transaction is then hashed, leaving you with :
  - Hash A
  - Hash B
  - Hash C
  - Hash D
- The hashes are paired together, resulting in :
  - Hash AB and
  - Hash CD
- And therefore, your Merkle Root is formed by combining these two hashes : Hash ABCD.

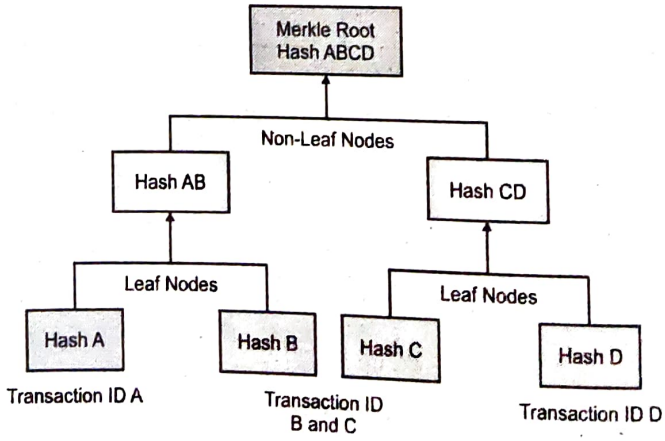


Fig. 1.9.3 : Markle Tree (Combine hashes)

1.9.4 Benefits of Merkle Tree in Blockchain

Merkle trees provide four significant advantages :

1. **Validate the data's integrity :** It can be used to validate the data's integrity effectively.
2. **Takes little disk space :** Compared to other data structures, the Merkle tree takes up very little disk space.
3. **Tiny information across networks :** Merkle trees can be broken down into small pieces of data for verification.
4. **Efficient Verification :** The data format is efficient and verifying the data's integrity takes only a few moments.

1.9.5 Use-Cases of Merkle Tree in Blockchain

1. Git, a distributed version control system, is one of the most widely used. It is used to handle projects by programmers from all around the world.
2. Interplanetary File System, a peer-to-peer distributed protocol, is another suitable implementation. It is also open source, allowing computers to join and use a centralized file system.
3. It is part of the technique that generates verifiable certificate transparency logs.
4. Amazon DynamoDB and Apache Cassandra use it during the data replication process. These No-SQL distributed databases use Merkle trees to control discrepancies.

1.10 Currency, Cryptocurrency and its Benefits

- As we all know, money represents the value of other things. The purpose of money is to facilitate exchange; it allows people to acquire what they need to live.
- Before money was invented, people traded goods for other goods by bartering. Historically, gold, shells, wheat, and salt have been used as a medium of exchange and to represent value.
- For something to be able to represent value for a long time, its users must continue to believe that a medium of exchange is indeed valuable and that this value will persist for a long time in order to continue to benefit them.
- As a result of its convenience and practicality, paper money has gained so much popularity that it has become the primary means by which goods and services are bought and sold around the world.

1.10.1 Fiat Money

- Fiat is a **money with no intrinsic value but made legal tender by a government order.** Historically, money was backed by tangible goods like silver and gold, but fiat money is dependent on the creditworthiness of the government that issues it.
- Fiat money, which was introduced as a replacement for representational money and commodity money, has a value based on supply and demand. Silver and other precious metals are used to make commodity money, whereas representational money is a claim on a redeemable commodity.

1.10.1(A) How Does Fiat Money Work ?

- Fiat currency is not backed by any physical commodity, but rather by the trust of its holders and the authority of a government declaration. Paper money serves as a medium of storage for purchasing power and an alternative to the barter system. It enables people to purchase goods and services as they require without having to trade product for product, as was the case with barter trade.

- People can make plans and create specialized economic activities with ease because of its ability to store purchasing power. A mobile phone assembly company, for example, can purchase new equipment, hire and pay employees, and expand into new markets.
- The value of fiat money is determined by how a nation's economy performs, how the government governs itself and the influence of these variables on interest rates. A country undergoing political unrest is likely to have a weaker currency and higher commodity prices, making it difficult for citizens to purchase the goods they require.
- A fiat currency performs successfully when the public has adequate faith in its potential to serve as a buying power storage medium. It must also be supported by the full credit of the government that issues a decree and prints it as legal money for financial transactions.

1.10.1(B) Advantages and Disadvantages of Fiat Currency

- The most fundamental attribute of fiat money, as opposed to commodity-based money such as gold, copper, and silver, is its value stability. Fiat money became popular in the twentieth century as governments and banks sought to shield their economies from the economic cycle's recurrent collapses.
- Because of the normal business cycle and recurrent recessions, commodity-based currencies were volatile. Central banks have the ability to issue and hold paper money as needed, providing them more influence over the money supply, interest rates, and liquidity. For example, the Federal Reserve's control over money supply and demand helped it to keep the 2008 Global Financial Crisis from wreaking havoc on the US financial system and global economy.
- Although fiat money is seen as a more stable currency capable of mitigating recessions, the global financial crisis demonstrated otherwise. Despite the fact that the Federal Reserve controls the money supply, it was unable to prevent the crisis from occurring. Critics of fiat money believe that because gold is restricted in production, it is a more stable currency than fiat money, which has an infinite supply.

1.10.2 Evolution of Currency

Fig. 1.10.1 shows timeline of the evolution of currency.

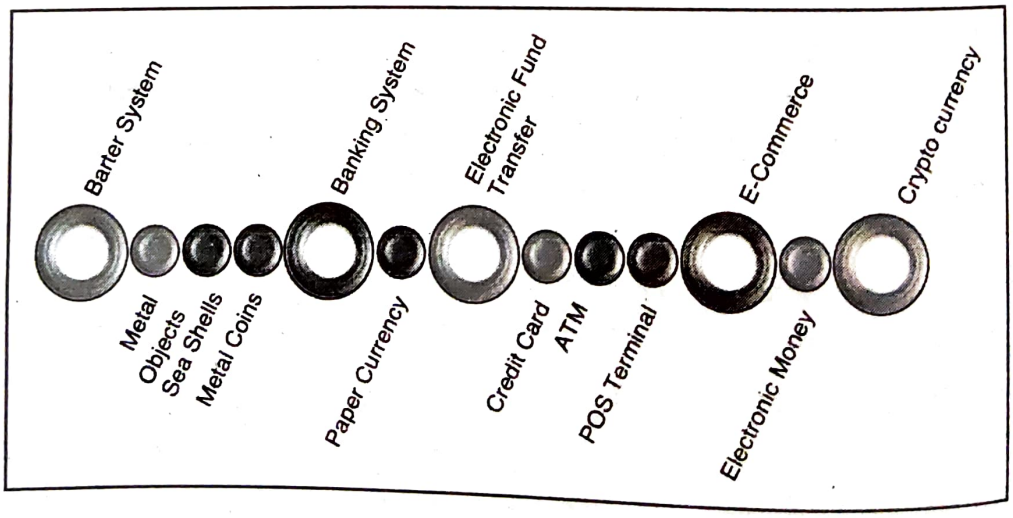


Fig. 1.10.1

1.10.3 What is Cryptocurrency ?

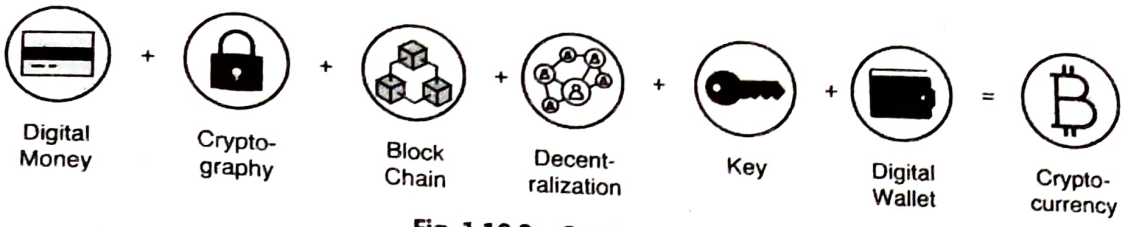


Fig. 1.10.2 : Cryptocurrency

A cryptocurrency (or "crypto") is a digital asset that can be circulated without the need for any central authority such as a government body and banks. Instead, cryptocurrencies are created using cryptographic technology to allow people to buy, sell, or trade securely.

Overview of Cryptocurrency

- Cryptocurrency is a digital or virtual currency that works on cryptographic principles. As the name suggests, they have no physical existence or are intangible. They exist only as sets of programming code. However, it offers greater security and ease of use than many existing currencies.
- Cryptocurrencies go hand in hand with blockchain technology. We have already seen how blockchain works. For cryptocurrencies, the ledger tracks cryptocurrencies generated and traded on the network. Every person on a given blockchain has a unique account ID/address.
- Cryptocurrencies are always associated with these accounts (currencies are debited and credited to this account).
- Users can manage their accounts through applications called wallets. Through the wallets, anyone can conduct transactions with anyone on the network (both sender and receiver must have an account).
- Transactions are verified by peers and added to the blockchain ledger (database). Blockchain's immutable, cryptographic ledger is therefore the backbone of cryptocurrencies.

Benefits of Cryptocurrency

1. Low Risk of Disruption
2. Portability
3. Better value storage
4. Limited quantity
5. Independence from other asset classes
6. Underlying or intrinsic value
7. Difficult to Fake and control

PROS and CONS of Cryptocurrency

Sr. No.	PROS	CONS
1.	No restrictions on payment	Lack of awareness / knowledge
2.	Maintenance of Anonymity	Use of complex technique
3.	Use of complex algorithm	Highly volatile in nature

Sr. No.	PROS	CONS
4.	Speed of Exchange	Not Accepted everywhere
5.	No Third party involvement	Victim of theft and scam
6	Free/very less transaction fee	No reverse of payment and recovery
7	No Inflation	Black market
8	-	Scaling issue
9	-	May not be exchanged with Fiat currency.

1.10.4 Types of Cryptocurrency

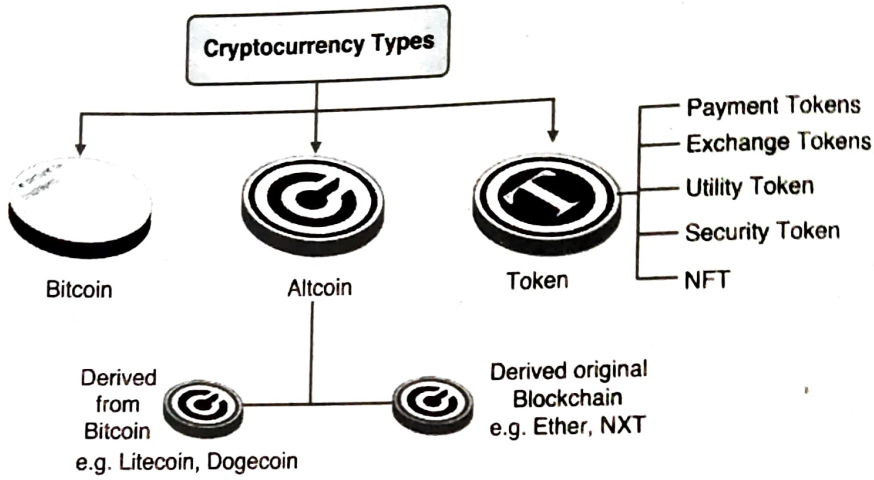


Fig. 1.10.3 : Types of Cryptocurrency

Coins are assets on their native blockchain, while tokens are assets that are foreign to the blockchain they live on. Examples of coins are Bitcoin on the Bitcoin blockchain and Ether on the Ethereum blockchain. An example of a token is Tether as a second layer token on multiple blockchains; Uniswaps "UNI" token and Chainlinks "LINK" token use the Ethereum blockchain. More detailed classification of crypto currencies can be understood by comparing coins and tokens. Chapter 5 gives an overview of tokenization and detailed description tokens in practice.

1.10.5 What is Decentralization?

- A decentralized system is a type of network in which the nodes are not dependent on a single master node; instead, control is distributed among many nodes.
- This is similar to a model in an organization where each department is in charge of its own database server, thus eliminating the power of the central server and dispersing it to the sub departments who manage their own databases.
- The fundamental idea of decentralization is to distribute authority and control to the peripheries of an organization. This configuration provides various benefits for organizations, such as enhanced efficiency, accelerated decision making, better motivation, and a reduced load on top management.

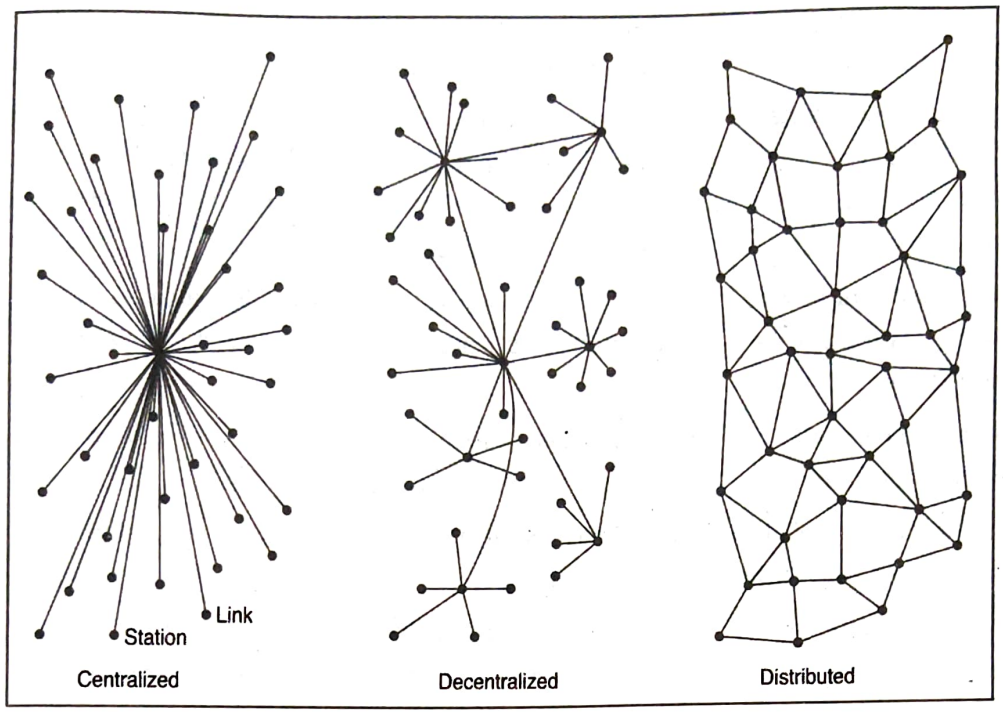


Fig. 1.10.4 : Different types of Networks/Systems

- Decentralization was initially made possible using blockchain technology. A significant innovation in the decentralized paradigm that has induced this new era of decentralization of applications is decentralized consensus.
- Bitcoin client was the first-ever blockchain, which was created in 2009. Using a consensus algorithm Bitcoin enables a user to agree on something, without the necessity for an intermediary, central, trusted third party or a service provider. A consensus mechanism governs this competition, and the most commonly used method is known as Proof of Work (PoW).
- When a person sends Bitcoin to someone else, transactions are not verified by a centralized authority. Rather, anybody can hook up their computer to the Bitcoin system to help verify a movement of funds. Every device connected to the system is known as a "node", and in total there are thousands of independent nodes all of which are helping to operate the network.
- From a semi-decentralized model to a fully decentralized one, Decentralization is applied in varying degrees depending on the circumstances and requirements.
- From a blockchain perspective Decentralization can be viewed as a mechanism that provides a way to remodel existing paradigms and applications, or to create new applications, for the sake of giving full control to the users.

Advantages of Decentralisation

- **Provides a trustless environment :** No one has to trust or know anyone else in a decentralized blockchain network. Within the network every member has a copy of the exact same data in the form of a distributed ledger. If any member's ledger is corrupted or altered in any way, majority of the members in the network will reject it.
- **Improves data reconciliation :** Many companies often exchange data with their partners. This data, is typically transformed and stored in each party's data storage place, only to resurface when it needs to be passed

downstream. Each time the data is transformed, it opens up possibility for data loss or incorrect data to enter the work stream. Every entity has access to a real-time, shared view of the data by having a decentralized data store.

- **Reduces points of weakness :** In systems Decentralization can reduce points of weakness where there may be too much dependence on specific actors. These weak points could lead to integral failures, including failure in providing promised services or inefficient service due to the depletion of resources, periodic interruptions, bottlenecks, lack of sufficient incentives for good service, or corruption.
- **Optimizes resource distribution :** Decentralization can also help optimize the distribution of resources so that the promised services are provided with consistency and better performance, as well as a reduced probability of catastrophic failure.
    - Decentralization usually has some disadvantages such as lower transaction output, but preferably, the trade offs are worth the improved stability as well as the service levels they produce.
    - Decentralization should be put in application where it makes sense. It doesn't mean that just because it's a blockchain application, it needs to be 100% decentralized.
- Information and Communication Technology (ICT) has conventionally been based on a centralized paradigm whereby a central authority, such as a system administrator controls the database or application servers.
- With Bitcoin and the emergence of blockchain technology, this model has transformed and now the technology exists, which allows anyone to start a decentralized system and operate it with no single trusted authority or no single point of failure.
- It can either be run independently or by requiring some human intervention, depending on the model and type of governance used in the decentralized application administrating on blockchain.

Difference between Centralized, Distributed and Decentralized

Table 1.10.1

	Centralized	**Decentralized**	**Distributed**
Network/hardware resources	Maintained & controlled by single entity in a centralized location.	Resources are owned & shared by network members; difficult to maintain since no one owns it.	Spread across multiple data centers & geographies; owned by network provider.
Solution components	Maintained & controlled by central entity	Each member has exact same copy of distributed ledger.	Maintained & controlled by solution provider.
Data	Maintained & controlled by central entity	Only added through group consensus.	Typically owned & managed by customer.
Control	Controlled by central entity	No one owns the data & everyone owns the data.	Typically, a shared responsibility between network provider, solution provider & customer.

	Centralized	Decentralized	Distributed
Single Point of Failure	Yes	No	No
Fault tolerance	Low	Extremely high	High
Security	Maintained & controlled by central entity	Increases as # of network members increase.	Typically, a shared responsibility between network provider, solution provider & customer.
Integrity	Maintained & controlled by central entity	Maintained & controlled by replicating data at network members	Maintained & controlled by replicating data at network provider
Privacy	Maintained & controlled by central entity	Decreases as # of network members increase.	Typically, a shared responsibility between network provider, solution provider & customer.
Performance	Maintained & controlled by central entity	Decreases as # of network members increase.	Increases as network/hardware resources scale up and out.
Example	ERP system	Blockchain	Cloud computing

- This implies that the system is still centralized in nature. The critical difference between a decentralized system and distributed system is that in a decentralized system, no central authority exists, whereas in a distributed system, there still exists a central authority that governs the entire system.

Review Questions

Q. 1 Define cryptography & its types.

Q. 2 Compare cryptographic methods- asymmetric & symmetric.

Q. 3 Steps for RSA & advantages of it.

Q. 4 Write in brief about AES & DES (pros and cons).

Q. 5 Write in brief about ECC, equation of ECC, Why ECC is preferred over RSA.

Q. 6 Compare RSA & ECC.

Q. 7 Describe SHA block diagram, Uses of SHA.

Q. 8 Explain steps in AES and characteristics of AES.

Q. 9 Explain Merkle Tree in Blockchain.

Q. 10 What are the benefits of Merkle Tree in Blockchain ?

Q. 11 What are the Use-Cases of Merkle Tree in Blockchain ?

Q. 12 Describe Working of Merkle Trees.

Q. 13 What are the Pros and Cons of DSA?

Q. 14 Explain with the diagram 'Digital Signature Algorithm (DSA)'.

Q. 15 List and explain different use cases of SHA.

Q. 16 Define cryptology, why do we need cryptography ?

Q. 17 Write steps of ECDSA.

Q. 18 Explain with example 'ECDH'.

Q. 19 Write uses of ECC and What are the pros and cons of ECC.

Q. 20 What are the Applications of Hash Functions?

Q. 21 What are the characteristics of Hash Functions?

Q. 22 explain the Difference between DES and AES

Q. 23 List and explain the cryptographic elements.

Q. 24 Explain the benefits of Cryptocurrency.

Q. 25 State the Pros and Cons of Cryptocurrency.

Q. 26 What are the types of Cryptocurrency?

Q. 27 What do you understand about Fiat currency?

Q. 28 Explain the evolution of Cryptocurrency.

Q. 29 State difference between Centralized, Distributed and Decentralized.

Q. 30 What are the design issues in decentralized system?

2 Unit II

Introduction to Blockchain Technology

Syllabus

What is bitcoin, Mechanics of Bitcoin, bitcoin transaction, Introduction of Blockchain, History of Blockchain, Blockchain Technology Definition, Types of Blockchain, Peer to Peer Network, platform for decentralization, Transactional blocks, why use blockchain technology.

2.1 What is Bitcoin ?

- Bitcoin is a collection of concepts and technologies that form the basis of the digital money ecosystem. Bitcoin is a cryptocurrency used to store and transmit value between participants of the Bitcoin network. Bitcoin users communicate with each other primarily using the Bitcoin protocol over the Internet, but other transport networks can also be used. The Bitcoin protocol stack is available as open source software, and can run on a variety of computing devices, including computer, laptops and smartphones, which makes access to the technology easy for everyone.
- Users can transfer Bitcoin over the network to do almost anything that can be done with conventional currency, including selling and buying goods, sending money to people and organizations. Bitcoin can be bought and sold at specialized currency exchanges and exchanged for other currencies. In some ways, Bitcoin is referred to as the "money of the Internet" because it is secure ,fast and borderless.
- Unlike traditional currencies, Bitcoin is completely virtual. There is no physical coin and no digital coin per se. The coin is involved in a transaction that transfers the value from sender to receiver. Bitcoin users hold digital keys that can prove their ownership of their Bitcoins on the Bitcoin network. These keys can be used to sign a transaction to unlock value and transfer it for use. Keys are often stored in a digital wallet on each user's computer or smartphone. Possession of the keys that allow to sign transactions is the only requirement for the issuance of Bitcoin, and control of it is entirely in the hands of the user.
- Bitcoin is a decentralized peer-to-peer system. Therefore, there is no "central" server or control point for managing it. Bitcoins are generated through a process called "mining". This includes finding solutions to math problems while processing bitcoin transactions. Participants in the Bitcoin network (i.e., people using devices running the full Bitcoin protocol stack) can act as miners, validating and recording transactions using the processing power of computers. Anyone can do it. On average, every 10 minutes, bitcoin miners can verify transactions in the last 10 minutes and can generate the block by solving the math puzzle and are rewarded with new bitcoins. Basically, bitcoin mining decentralizes the currency-issuance and clearing functions of a central bank and replaces the need for any central bank.

- The Bitcoin protocol incorporates algorithms that regulate mining capabilities across the network. The difficulty of the processing tasks(solving math puzzles) that miners have to perform is dynamically adjusted, so on average someone succeeds every 10 minutes, regardless of the number (and amount of processing) of competing miners. The protocol also halves the rate at which new Bitcoins are created every four years, and limits the total number of Bitcoins created to a fixed total of just under 21 million coins. As a result, the number of Bitcoins in circulation will approach 21 million by 2140. Furthermore bitcoins will not be generated.
- Behind the scenes, Bitcoin is also the name of innovation in protocols, distributed computing and peer-to-peer networks. Bitcoin currency is the first application of this invention. Bitcoin is the culmination of the decades of research in cryptography and decentralized systems and includes four of key innovations brought together in a unique and powerful combination of
  1. A decentralized peer-to-peer network (the bitcoin protocol)
  2. A public transaction ledger (the blockchain)
  3. A set of rules for independent transaction validation and currency issuance (consensus rules)
  4. A mechanism for reaching global decentralized consensus on the valid blockchain (Proof-of-Work algorithm).
- In summary Bitcoin consists of a decentralized peer-to-peer network (Bitcoin Protocol), a public transaction ledger (Blockchain), a set of rules for independent transaction authentication and currency issuance (Consensus Rules), and a mechanism for reaching global decentralized consensus.

Note :

- Blockchain is not Bitcoin; rather the technology behind Bitcoin is known as Blockchain.
- Bitcoin is the digital cryptocurrency or token on the other hand blockchain is the distributed ledger to keep track of transactions of those digital tokens.
- Blockchain can be used for a number of applications, one of them as Bitcoin.

2.2 History of Bitcoin

- Bitcoin was invented under the pseudonym Satoshi Nakamoto in a 2008 paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System".
- Nakamoto combined several previous inventions such as b-money and HashCash to make currency issuance and processing and verification of transactions completely decentralized, which is not dependent on a central authority. A key innovation was that he used a distributed computing system (algorithm "Proof-of-Work") to conduct a global "election" every ten minutes to verify the transactions. This also solves the double spending problem where one unit of currency can be spent twice. Previously, the double-spend problem was a weakness of digital currencies, which was addressed by clearing all transactions through a central clearinghouse.
- The Bitcoin Network was started in 2009 based on a reference implementation published by Nakamoto , which has been revised by many other programmers after it. The implementation of a proof-of-work (mining) algorithm that provides the security and resilience to bitcoin. Bitcoin's total market value exceeds a billion US dollar, Bitcoin can be exchanged with other FIAT currencies.
- The largest transaction ever processed by the network was $150 million, was delivered instantly and processed without fees.

- The identity of Satoshi Nakamoto who was behind the invention of Bitcoin is still unknown. However, neither Satoshi Nakamoto nor anyone else independently controls the Bitcoin system, which is based on completely transparent mathematical principles, open-source code, and consensus among participants. This invention itself, is groundbreaking and has already produced new sciences in the areas of distributed computing, econometrics and economics.

2.3 Bitcoin Transaction

2.3.1 Bitcoin Wallet

- Bitcoin is a protocol that can be accessed using a client application that speaks the protocol. The common user interface for the Bitcoin system is a "bitcoin wallet". It is as common as a web browser as the user interface for the HTTP protocol.
- As with web browsers (e.g., Chrome, Safari, Firefox, and Internet Explorer), there are many bitcoin wallet implementations and brands.
- Bitcoin wallets are one of the most actively developed bitcoin applications. Depending on the platform, Bitcoin wallets can be classified as Hot or Cold wallets :

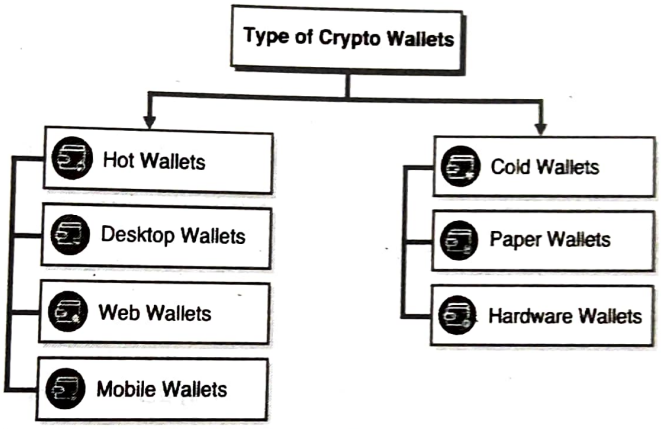


Fig.2.3.1 : Types of crypto wallets

1. **Desktop wallet**

Desktop wallets are popular because of their features, autonomy, and control. Desktop wallets are the first type of bitcoin wallet. The use of general-purpose operating systems such as Windows and Mac OS has certain security disadvantages due to their insecurity and poorly configured nature.

2. **Mobile wallet**

Mobile wallets are the most common type of Bitcoin wallet. Working with smartphone operating systems such as Apple iOS and Android, this wallet is a great option for new users. Many are designed to be simple and easy to use, but there are also full-featured mobile wallets for power users.

3. **Web wallet**

A web wallet is accessed from a web browser and the user's wallet is stored on a server owned by a third party. This is similar to his webmail in that it relies entirely on third party servers. Some of these services work with client-side code running in the user's browser, putting control of the Bitcoin key in the user's hands. However, mcst represent a compromise of controlling the user's bitcoin key in exchange for ease of use. Storing large amounts of bitcoins in third-party systems is not recommended.

4. Hardware wallet

A hardware wallet is a device that runs a secure, self-contained Bitcoin wallet on dedicated hardware. They work over USB in desktop web browsers or over Near Field Communication (NFC) in mobile devices. By handling all bitcoin-related operations on dedicated hardware, these wallets are considered highly secure and suitable for storing large amounts of bitcoin.

5. Paper wallet

- Keys used to control Bitcoin can also be printed for long-term storage. These are called paper wallets, but other materials (wood, metal, etc.) can also be used. Paper wallets offer a simple and highly secure way to store bitcoins for the long term. Offline storage is also referred to as cold storage.
- Bitcoin wallets are also categorized by their level of autonomy and how they interact with the Bitcoin network.

6. Full-node client

A full client or "full node" is a client that can store the full history of Bitcoin transactions (all transactions from any user), manage a user's wallet, and initiate transactions directly on the Bitcoin network. A full node handles all aspects of the protocol and can validate the entire blockchain and each transaction independently. A full node client consumes significant computing resources (125+ GB hard disk, 2 GB RAM, etc.) but offers full autonomy and independent transaction validation.

7. Lightweight client

A lightweight client, also known as an SPV (Simple Payment Verification) client, connects to a Bitcoin full node (described above) to access Bitcoin transaction information, but stores user wallets locally, creates transactions, and independently verifies them. A lightweight client interacts directly with the Bitcoin network without an intermediary.

8. Third-party API client

- Third-party API clients interact with Bitcoin through a third-party system of application programming interfaces (APIs) rather than connecting directly to the Bitcoin network. Wallets can be stored by the user or by a third party server, but all transactions go through the third party.
- Combining these categorizations, many bitcoin wallets fall into a few groups, with the three most common being mobile lightweight wallet, desktop full client, and web third-party wallet.

2.3.2 Working of Bitcoin Transaction

- Most electronic payment networks such as debit cards, credit cards, bank account transfers and PayPal are reversible but Bitcoin transactions are irreversible. Let us understand this in detail, consider the following example refer Fig. 2.3.2 understanding bitcoin transaction

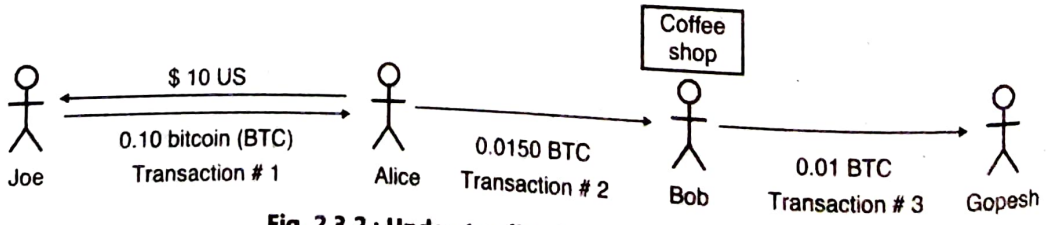


Fig. 2.3.2 : Understanding bitcoin transaction

- Alice is new to the Bitcoin ecosystem and doesn't have any bitcoins (BTC). Alice installs the Bitcoin wallet. Joe is her friend who possesses bitcoins. Alice gives $10 to Joe in cash and Joe exchanges Alice 0.10 bitcoins (Transaction #1) through the bitcoin wallet. Now Alice also possesses bitcoins. Once Alice went to Coffee shop and the shop owner Bob accepted the bitcoins for a cup of coffee (Transaction #2). After some days Bob gets some service from Gopesh and pays to Gopesh in bitcoins (Transaction #3). Let us understand all 3 transactions now.

2.3.3 Transaction Inputs and Outputs

- A transaction tells the Bitcoin network that the owner of Bitcoin value has authorized the transfer of that value to another owner. A new owner will be able to use Bitcoin in the chain of ownership by creating another transaction authorizing the transfer to another owner. This is the same as Joe transferring BTC to Alice, Alice to Bob, Bob to Gopesh and so on.
- Transactions are similar to lines in double-entry bookkeeping ledger. Each transaction can have one or more inputs which are similar to debits against a bitcoin account. On the other side of the transaction there can be one or more "outputs". The inputs and outputs (debits and credits) do not necessarily add up to the same bitcoin amount. Instead, outputs add up to slightly less than inputs, the difference between input and output is the applied transaction fee for that transaction, that transaction fee is collected by the miner who mines the block i.e. includes the transaction in the ledger. Fig. 2.3.3 shows a bitcoin transaction as a bookkeeping ledger entry.

Transaction as Double-Entry Bookkeeping

Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs :	0.55 BTC	**Total Outputs :**	0.50 BTC

Inputs	0.55 BTC
Outputs	0.50 BTC
Difference	0.05 BTC (implied transaction fee)

Fig. 2.3.3 : Transaction as double-entry bookkeeping

2.3.4 Transaction Chains

Alice's payment to Bob's coffee shop uses a previous transaction's output as its input. Alice received bitcoin from Joe in return for cash. The transactions form a chain, where the inputs from the latest transaction correspond to outputs from previous transactions. Fig. 2.3.4 shows this chain of transactions, from Joe to Alice to Bob to Gopesh.

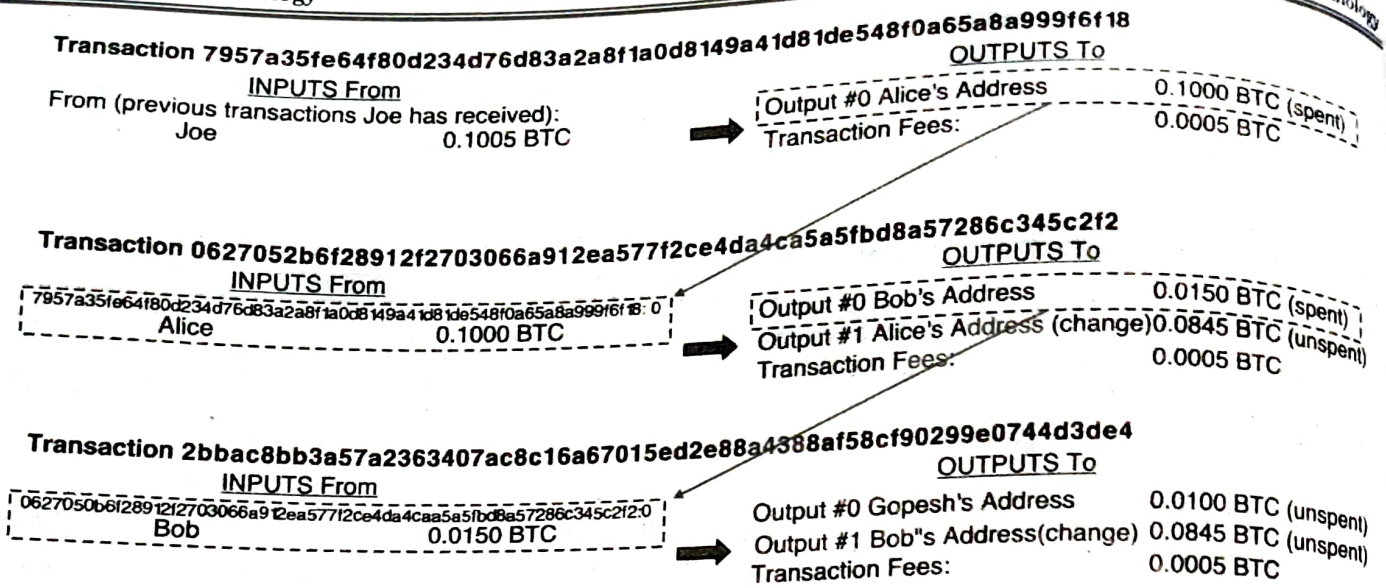


Fig. 2.3.4 : A chain of transactions, where the output of one transaction is the input of the next transaction

2.3.5 Making Change

- Many Bitcoin transactions contain outputs pointing to both the new owner's address and the current owner's new address, called the change address.
- Consider the example where you purchase an item for Rs. 30 and you pay Rs. 50 to the seller, the seller will return Rs.20 as a change.
- The same concept applies to bitcoin transaction inputs. If you buy an item for 5 bitcoins but you have 30 bitcoin inputs to use, this transaction will have one output as 5 bitcoin to the seller and one more output 15 bitcoins returned. (minus applicable transaction fees).
- A thing to note here is for privacy reasons the change address does not have to be the same address as that of the input, it is always a different address.
- Different wallets can use different strategies to select the number of input transactions for desired output transactions to get an exact match for the payment amount.
- In summary, transactions move values from transaction inputs to transaction outputs. The input is a reference to the previous transaction's output indicating where the value came from. The transaction output transfers a certain value to the new owner's Bitcoin address and may include a change output to the original owner with change address. Output from a transaction can be used as input for a new transaction, creating a chain of ownership as values move from owner to owner.

2.3.6 Common Transaction Forms

- The most common form of transaction is a simple payment from one address to another, which often includes some "change" returned to the original owner. Fig. 2.3.5 shows this type of transaction, it has one input and two outputs, out of two output one is change address.

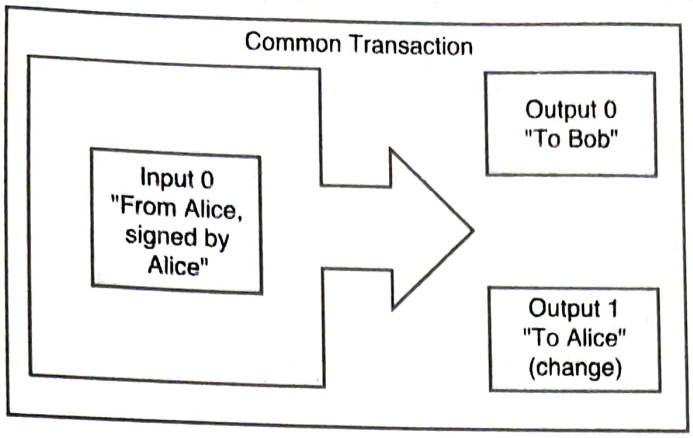


Fig. 2.3.5 : Most common transaction

- Another common form of transaction is one that have several inputs into a single output. Fig. 2.3.6 shows such a type of transaction. This represents the real-world equivalent of exchanging a pile of coins and currency notes for a single larger note.

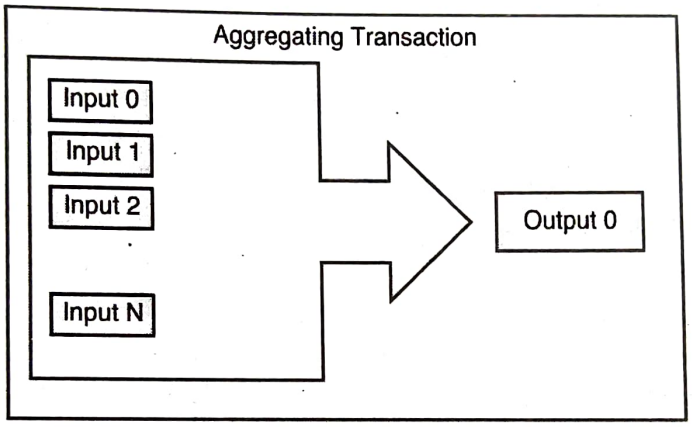


Fig. 2.3.6 : Transaction having more than one inputs

- One more transaction form that is seen often on the bitcoin ledger is a transaction that distributes one input to multiple outputs representing multiple recipients(see Fig.2.3.7). Such type of transactions are used by commercial entities to distribute funds, such as when processing payroll payments to multiple employees.

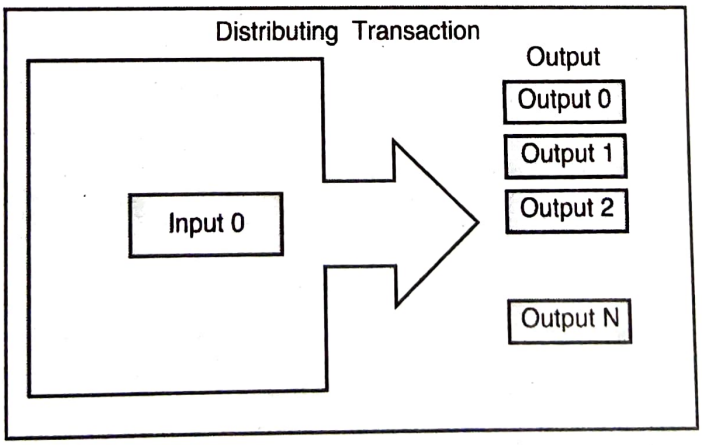


Fig. 2.3.7 : Transaction distributing funds

2.3.7 Constructing a Transaction

Bitcoin wallet application contains all the logic for selecting appropriate inputs and outputs to perform a transaction. One only needs to mention a an amount and destination, and the rest happens in the wallet application without seeing many details.

2.3.8 Getting the Right Inputs

Alice's wallet application will first have to find inputs that can pay for the amount that she wants to send it to Bob. Most wallets keep track of all the available outputs belonging to addresses in the wallet. Therefore, Alice's wallet would contain a copy of the transaction output from Joe's transaction, which was created in exchange for cash. A bitcoin wallet application that runs as a full node client actually contains a copy of each unspent output from every transaction in the blockchain. This allows a wallet to construct transaction inputs as well as quickly verify incoming transactions as having correct inputs. However, because a Full node client takes up a lot of disk space, most user wallets run "lightweight" clients that track only the user's own unspent outputs.

2.3.9 Creating the Outputs

- A transaction output is created in the form of a script that creates an encumbrance on the value and can only be redeemed by the introduction of a solution to the script. In simpler terms, Alice's transaction output will contain a script that says something like, "This output is payable to whoever can present a signature from the key corresponding to Bob's public address." Because only Bob has the wallet with the keys corresponding to that address, only Bob's wallet can present such a signature to redeem this output. Alice will therefore "encumber" the output value with a demand for a signature from Bob.
- This(Alice to Bob)transaction will also include a second output, because Alice's funds are in the form of a 0.10 BTC output is too much money for the cup of coffee which requires only 0.015 BTC. Alice will need 0.085 BTC in change. Alice's change payment is created by Alice's wallet as an output in the same transaction as the payment to Bob. Essentially, Alice's wallet breaks her funds into two payments: one to Bob and one back to herself. She can then spend the change output in a further transaction.
- Fig.2.3.8 shows the resulting transaction can be seen using a blockchain explorer web application

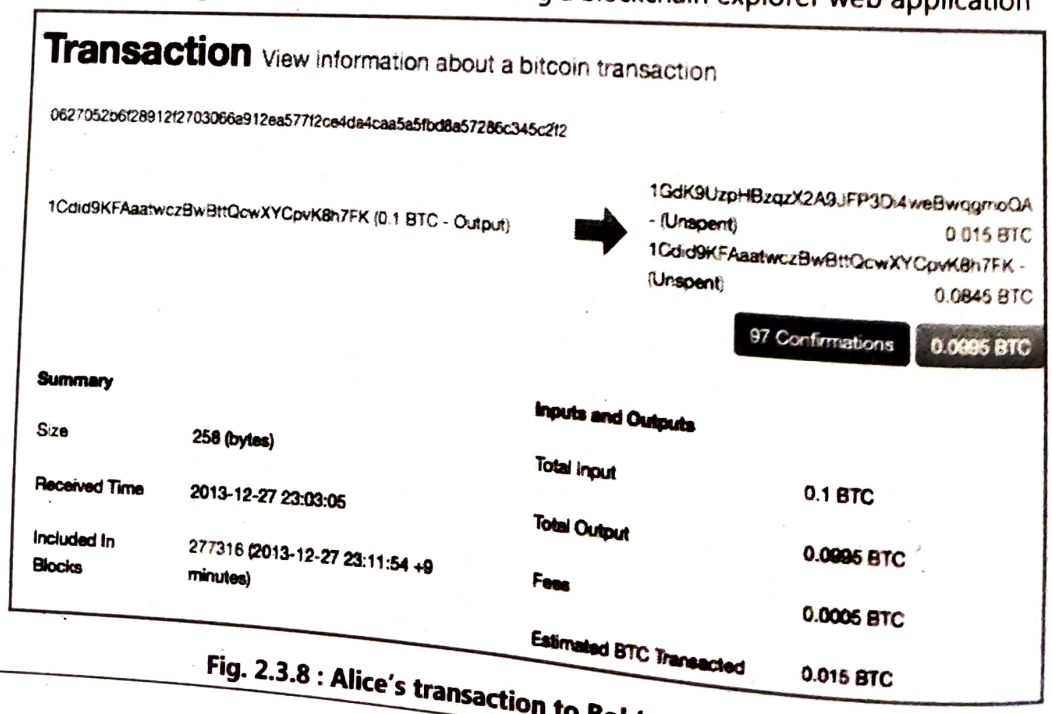


Fig. 2.3.8 : Alice's transaction to Bob's coffee shop

2.3.10 Adding the Transaction to the Ledger

- The transaction created by wallet application is of 258 bytes long and contains. All necessary information to confirm ownership of the funds and assign new owners.
- Now this transaction must be transmitted to the bitcoin network to become part of the blockchain ledger.

Transmitting the transaction

As transaction contains all the information necessary to process, it does not Matter where or how it is transmitted to the bitcoin network. The bitcoin network is a peer-to-peer network, with each bitcoin client participating by connecting to several other bitcoin clients. The purpose of the bitcoin network is to propagate blocks And transactions to all participants.

How transactions propagates

- Any system, such as a desktop application, server or wallet, that participates in the bitcoin network by "speaking" the bitcoin protocol is called a bitcoin node. Alice's wallet application can send the new transaction to any bitcoin node it is connected to over any type of connection: wired, Wi-Fi, mobile, etc. Her bitcoin wallet does not have to be connected to Bob's bitcoin wallet directly. Any bitcoin node that receives a valid transaction it has not seen before will immediately forward it to all other nodes to which it is connected, a propagation technique known as loading. Thus, the transaction rapidly propagates out across the peer-to-peer network, reaching a large percentage of the nodes within a few seconds.
- Even if Alice's wallet sends the transaction through other nodes, it will reach Bob's wallet within a few seconds. Bob's wallet will immediately identify Alice's transaction as an incoming payment because it contains outputs redeemable by Bob's keys.

2.3.11 Bitcoin Mining

- Once a transaction is propagated on the bitcoin network. It does not become part of the blockchain until it is verified and included in a block by a process called mining.
- Computation is the base of the bitcoin system's trust. Transactions are bundled into blocks, which require an large amount of computation to solve a puzzle , but only a small amount of computation to verify the solution. The mining process have two purposes in bitcoin:
  - Mining nodes validate all transactions by following all bitcoin's consensus rules. Therefore, mining provides security for bitcoin transactions by rejecting invalid or malformed transactions.
  - Mining creates new bitcoin in each block, almost like a central bank printing new money. The amount of bitcoin created per block is limited and changes in every 4 years.
- Mining uses electricity to solve a mathematical problem. A successful miner will collect a reward in the form of new bitcoin and transaction fees. However, the reward will only be collected if the miner has correctly validated all the transactions.
- The difficulty level of mathematical problem is adjusted automatically such that to mine each block i.e. to solve the puzzle on an average system will take 10 minutes by satisfying all the rules of the consensus.

2.3.12 Mining Transactions in Blocks

- New transactions are continuously flowing into the network from user wallets and other applications. All transactions are visible to the bitcoin network nodes, transactions get added to a temporary pool of unverified transactions. As miners construct a new block, they add unverified transactions from this pool to the new block and then attempt to prove the validity of that new block, with the mining algorithm (Proof-of-Work).
- Transactions are added to the new block, prioritized by the highest-fee transactions first and a few other criteria. Each miner starts the process of mining a new block of transactions as soon as he receives the previous block from the network, knowing he has lost that previous round of competition. He immediately creates a new block, fills it with transactions from the pool and the fingerprint of the previous block, and starts calculating the Proof-of-Work for the new block.
- If he finds a solution that makes that block valid, he "wins" this reward because his successful block is added to the global blockchain and the reward transaction he included becomes spendable.
- Alice's transaction was picked up by the network and included in the pool of unverified transactions. Once validated by the mining software it was included in a new block, called a candidate block generated by the miner. All the miners participating in that mining pool immediately start computing Proof-of-Work for the candidate block. By some time one of the miners gets a solution for the candidate block and that miner announces it to the network. Then other miners validate the winning block (verifies the solution obtained by the winner) and they start the race to generate the next block. Newly generated and verified block by other miners became part of the blockchain.
- For example say suppose block #277316, containing 420 transactions, including Alice's transaction. Approximately 17 minutes later, a new block, #277317, is mined by another miner.
- As this new block is built on top of block #277316 that contained Alice's transaction added even more computation to the blockchain, thereby strengthening the trust in those transactions. Each block mined on top of the one containing the transaction counts as an additional confirmation for Alice's transaction. As the blocks pile on top of each other, it becomes exponentially harder to reverse the transaction, thereby making it more and more trusted by the network.

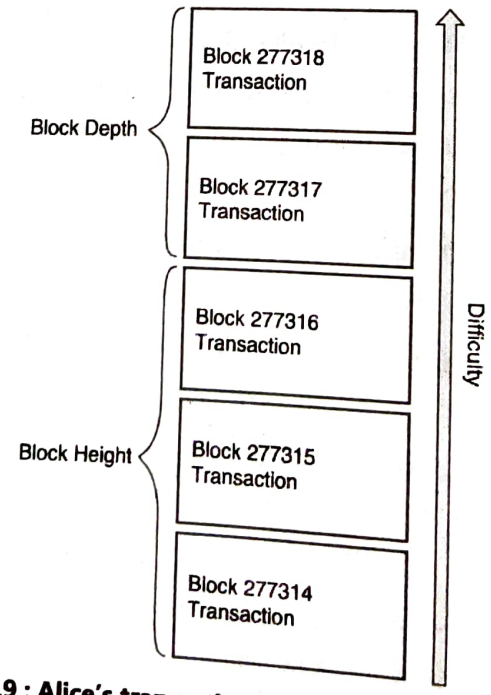


Fig. 2.3.9 : Alice's transaction included in block #277316

- In Fig. 2.3.9. we can see block #277316, which contains Alice's transaction. Below it are 277,316 blocks (including block #0), linked to each other in a chain of blocks (blockchain) all the way back to block #0, known as the genesis block.
- Over time, as the "height" in blocks increases, so does the computation difficulty for each block and the chain as a whole. The blocks mined after the one that contains Alice's transaction act as further assurance, as they pile on more computation in a longer and longer chain. By convention, any block with more than six confirmations is considered irrevocable, because it would require an immense amount of computation to invalidate and recalculate six blocks.

2.3.13 Spending the Transaction

- Now that Alice's transaction has been included in the blockchain as part of a block, it is part of the distributed ledger of bitcoin and visible to all bitcoin applications. Each bitcoin client can independently verify the transaction as valid and spendable. Full node clients can track the source of the funds from the moment the bitcoin were first generated in a block, incrementally from transaction to transaction, until they reach Bob's address. Lightweight clients can do what is called a simplified payment verification by confirming that the transaction is in the blockchain and has several blocks mined after it, thus providing assurance that the miners accepted it as valid.
- Bob can now spend the output from this and other transactions. For example, Bob can pay a contractor or supplier by transferring value from Alice's coffee cup payment to these new owners.
- Fig. 2.3.10 shows the chain of transactions from Joe to Gopesh. In this way the transactions are also traceable.

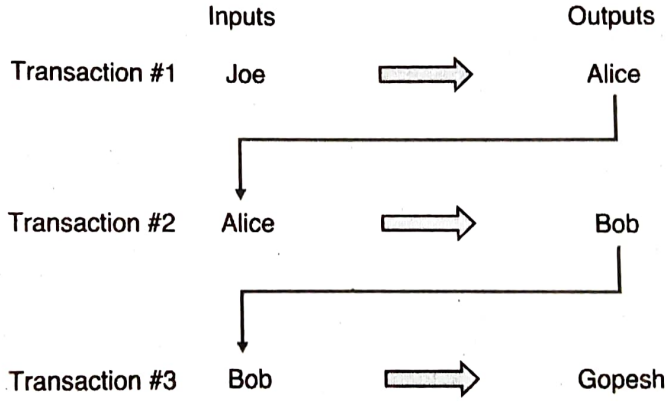


Fig. 2.3.10 : Alice's transaction as part of a transaction chain from Joe to Gopesh

2.4 Mechanics of Bitcoin

2.4.1 Bitcoin Working

It is very simple to use Bitcoin and we don't need any technical knowledge or programming skills for using Bitcoin. For using the Bitcoin Blockchain we have to create an account for it. For that, the simplest way is to create a digital wallet. BitCore, Coinbase, Exodus, etc. are a number of digital wallet service providers. While creating an account the user has to provide a 'Key' it is similar to a password. By using this key the wallet will generate a valid bitcoin Private key- Public Key pair. The public key is visible to all and it is the visible account ID of the user. While the private key the user keeps by himself, it is the access key to his account. If a person loses his private key he loses access to his account and his money.

2.4.2 Buy Bitcoin

The easiest way to own Bitcoin is to buy them from a bitcoin exchange. There are a number of online bitcoin exchanges which exchange normal currency to bitcoin. People can exchange their normal currency for bitcoin and move it to their wallet. Another way to own bitcoin is to participate in Bitcoin mining.

2.4.3 Transactions

Sending bitcoin from one account to another is called a transaction. It is usually done through wallets. The wallet app will provide an interface where we can input the account Id of the recipient and the amount we wish to transfer. Once we have made the transaction, the miners will verify the transaction and add to the blockchain ledger if it is a legitimate one. In Bitcoin, the transactions are cost-free. Usually, a transaction validation time is about 10 minutes in bitcoin, but if we give a small transaction fee we can speed up the process.

2.4.4 Bitcoin Mining

- Mining is the most interesting as well as the most important topic in bitcoin. This is the process by which new transactions are validated and added to the "blockchain'. Miners are the nodes who participate in the mining process. This demands dedicated mining hardware and thus, not all nodes are involved in mining.
- When a new bitcoin transaction happens in the network that is broadcasted on the network. The miners listen to this broadcasting and engage in transaction verification. Once the transactions are verified they are added to a block permanently.

2.4.5 So what do Miners actually do?

- Here, the mission is to find a hash value for the new block. The miner who finds the hash value first is rewarded with some bitcoins called block reward. Now it is 6.25 BTC. The reward is halved every 210,000 blocks or roughly every 4 years. Finding hash value is not a big deal. Every node can do that. Therefore, a difficulty level is associated with it to make the nodes compete with each other. The difficulty level is a measure of how difficult it is to find the hash. Difficulty level shrinks the set of hash values that a block can have. Without difficulty level, the hash can have any of the values within the super gigantic set of 2^256 possibilities (since the length of hash = 256 bits). By associating a difficult level, the target set is reduced considerably.
- The difficulty level is specified in terms of a number of zeroes, which means the miner has to find a hash value which starts with a specified number of zeroes. The nodes keep finding different hash values and check whether it satisfies the required difficulty level. Since the data of a block remains the same, the hash is always the same.
- Therefore, the only possibility to try out different hash values is by associating a nonce with the content of the block. The nonce is an arbitrary string of 32-bit length. i.e. H(block + nonce) Being a small target set, the probability of finding success is reduced.
- The miners keep changing the nonce in a brute force manner and the corresponding hash is computed each time. This is the real game and the computational power of nodes really matters here because the miners have to try out large combinations of 'Nonce'. The node which is equipped with dedicated hardware and high computational power has a greater chance to win this game and get the block reward. Those who find hash first will broadcast the block along with the nonce. By receiving this, others stop mining and validate whether the received hash satisfies the specified difficulty level. If yes, the nodes show their acceptance by adding it to the blockchain.

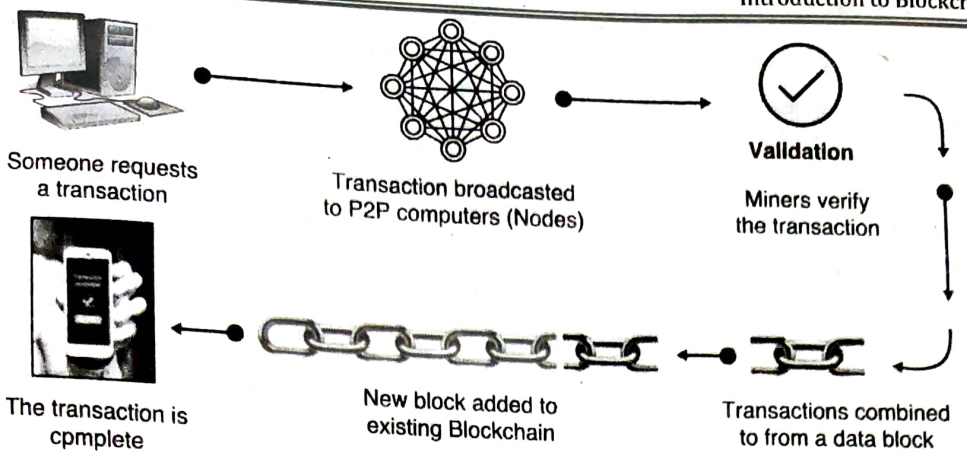


Fig. 2.4.1 : Life cycle of bitcoin transaction

2.4.6 Value of Bitcoin

- General question that may arise in anyone's mind is 'who determines the value of bitcoin. As we know there is no central bank or any other designated agency to control it; then how the value is determined, or who determines it?
- The answer lies in the basic economics, which is demand and supply. Following is the simplest model to determine the value of bitcoin.

T : Total bitcoin transaction/second

D : Duration that a BTC needed by a transaction

S : Supply of the bitcoin

P : Price of the bitcoin

We have S/D = Bitcoins available per second

T/P = Bitcoins needed per second

- According to the demand-supply rule, when the supply of bitcoin increases the demand decreases consequently the price will also decrease. And when the demand increases the supply of bitcoin will also decrease, consequently the price of the bitcoin will also increase.
- At an equilibrium state, where the supply S over D, is equal to the demand T over P. We can deduce the price P as

$$S / (D) = T / P$$

Equilibrium state :

$$P = TD / S$$

- The value of bitcoin basically depends on the demand and supply. It is evident that a single authority can't control the value of bitcoin, rather it is determined strictly based on the user transaction.

2.4.7 Advantages and Disadvantages of Bitcoins

2.4.7(A) Advantages of Bitcoins

1. **Protection From Payment Fraud :** Bitcoins are digital currencies. It uses an algorithm and cryptographic protocols. This makes them impossible to counterfeit.

2. **Reduced Possibility of Identity Theft :** Bitcoin transactions are completely anonymous. Bitcoin transactions do not require personal details or any sensitive information from either sender or receiver.
3. **Immediate Settlement :** Bitcoin does not involve a third party to facilitate the transactions. Funds are settled immediately and once initiated cannot be put on hold or can be refunded.
4. **Direct Transfer :** Transactions directly take place between users that is the sender and receiver. No third party involved there. Thus, it eliminates the fees for involving an intermediary.
5. **International Transactions :** Bitcoin is the easiest method to initiate an international transaction. It does not charge any extra fees and settle immediately to a receiver.
6. **Security :** Bitcoin has very strong security and it is impossible to counterfeit or cheat the bitcoin payment network. There will be 21 million bitcoins ever exist.
7. **Blockchain technology based :** Bitcoin transactions are tamperproof

2.4.7(B) Disadvantages of Bitcoin

1. **Scams and frauds :** Bitcoin is technically difficult and not easy to understand for a common citizen. It leads to in the name of bitcoin savings, bitcoin investment, and other bitcoin-related activities. Fake websites and apps are selling bitcoin and faking people.
2. **Black market activity :** Bitcoin is popular in the black market and criminals. Due to the complete anonymous feature, bitcoin is used in cyber hacking, drug deals, and black-market arms deals. International and national legal systems do not yet have proper laws and authority over bitcoin making it harder to stop bitcoin-related black market activities.
3. **Price volatility :** The price of Bitcoin is volatile
4. **No refund :** Once payment is initiated and complete bitcoin cannot be held and refunded. It takes place directly between users and without an intermediator. So bitcoin cannot be transferred back.
5. **Cyber hacking :** Hacking and illegal ransomware use bitcoin as a payment system to extort money from affected victims. This makes them untraceable due to bitcoins anonymous nature.

2.4.8 Bitcoin Summary

A Decentralized peer to peer electronic payment system	
BTC	Bitcoin network's main cryptocurrency
Bitcoin network	The node of computers that make the payment network
SHA256	Hash generation algorithm
Hashcash	Algorithm for bitcoin transactions
Wallet	Storing the bitcoins
Miners	Volunteers who maintain and secure the network
Blocks	Transaction data storage

2.5 Introduction of Blockchain

- Blockchain technology is a distributed, decentralized, immutable ledger that stores the record of ownership of digital assets in a business network. To put it another way, a blockchain is a distributed ledger or database that is shared among the nodes of a computer network.
- It is a mechanism enabling the secure transfer of assets without any need of intermediary. As the internet is a technology that facilitates the digital flow of information, in the same way blockchain is a technology that facilitates the digital exchange of units of value. Anything from currencies to land titles to votes can be tokenized, accumulated, and exchanged on a blockchain network.
- The majority of participants verify every transaction of the system. BitCoin is an example of the blockchain and is the most popular cryptocurrency.

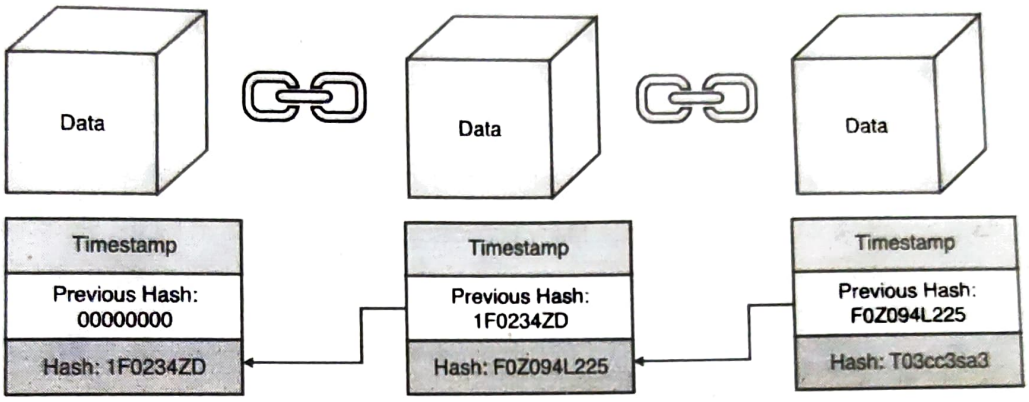


Fig. 2.5.1

- One significant difference between a typical database and a blockchain is the way the data is structured. A blockchain gathers information together in groups, known as blocks, which hold sets of information. All Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, creating a data chain known as the blockchain. All new information that follows that newly added block is compiled into a freshly formed block which will also be added to the chain once filled.

Note :

- Blockchain is not Bitcoin; rather the technology behind Bitcoin is known as Blockchain.
- Bitcoin is the digital cryptocurrency or token on the other hand blockchain is the distributed ledger to keep track of transactions of those digital tokens.
- Blockchain can be used for a number of applications, one of them as Bitcoin.

2.6 History of Blockchain

The History of Blockchain

1991 : The research scientists Stuart Haber and W. Scott Stornetta presented a computationally practical solution for time-stamping digital documents so that they could not be tampered. The concept of a cryptographically secured chain of blocks was used by them to design a system to store the time-stamped documents. To create a 'secured chain of blocks', Merkle Trees are used. It stored a series of data records, and each data record connected to the one prior to it.

1998 : The Scientist, Nick Szabo works on "Bit Gold" decentralized digital currency.

2004 : A computer scientist and cryptographic activist named Hal Finney introduced a system called Reusable Proof Of Work (RPoW) for digital cash. It was a game changing step in the history of cryptocurrencies. The RPoW system worked by obtaining a non-fungible or a non-exchangeable Hashcash based proof of work token in return. He created an RSA-signed token that further could be transferred from one person to another. This System helps others to solve the problem of Double Spending by keeping the ownership of tokens registered on a trusted server.

2008 : Satoshi Nakamoto, wrote a paper named "Bitcoin : A Peer-to-Peer Electronic Cash System". He introduced the term chain of blocks and explained the concept of distributed blockchains. Satoshi Nakamoto's actual identity is unknown. He was active in the Bitcoin developer community till 2011. A peer-to-peer network is used in it for verifying and timestamping each exchange. It could be managed autonomously without involving a central authority. Due to these improvements, blockchains are considered as the backbone of cryptocurrencies.

2009 : Nakamoto implemented first blockchain as a public ledger, for public transitions made using bitcoin.

2014 : Blockchain evolution is steady and promising and It has became a need in various fields.

Microsoft starts accepting Bitcoin as payments. Many applications are incorporated by the Blockchain technology that can be implemented in various economic sectors. Particularly in the finance sector, significant advancement in the performance of financial transactions.

2.7 Blockchain Technology Definition

Blockchain defined by IBM as: Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

2.7.1 How does the Blockchain Work?

- A blockchain is a peer-to-peer, distributed database that hosts a constantly growing number of transactions. Each transaction is referred to as a "block," and is secured through timestamped cryptography and is validated by every authorised member of the system using consensus algorithms (i.e., a set of rules). A particular transaction that is not validated by all members of the database is not added to the database. Every transaction is connected to the previous transaction in sequential order, forming a chain of transactions (or blocks). A transaction cannot be edited, or deleted thereby creating an immutable audit trial. A transaction can only be altered by adding another transaction to the chain. Transactions are fixed together in an irreversible chain known as a blockchain.
- Each additional block makes stronger the verification of the previous block and thus the entire blockchain. This makes the blockchain tamper-evident, supplying the key strength of immutability. This removes the possibility of tampering by a bad intentioned actor - and forms a ledger of transactions you and other network members can trust on.

- To exemplify this, say that person X wants to send money to person Y for paying an outstanding invoice related to the purchase of software. Person X inserts the transaction in the database, thereby creating a block. The transaction (or block) is broadcasted to every authorised member of the network. After validation of the transaction (i.e., approval of the payment) from all the members a block is added to the chain of transactions, which provides a transparent and immutable record of the transaction. The money is then transferred from person X to person Y, and the transaction is finished. The security of the blockchain forbids a hacker from acting as an authorized member of the network.

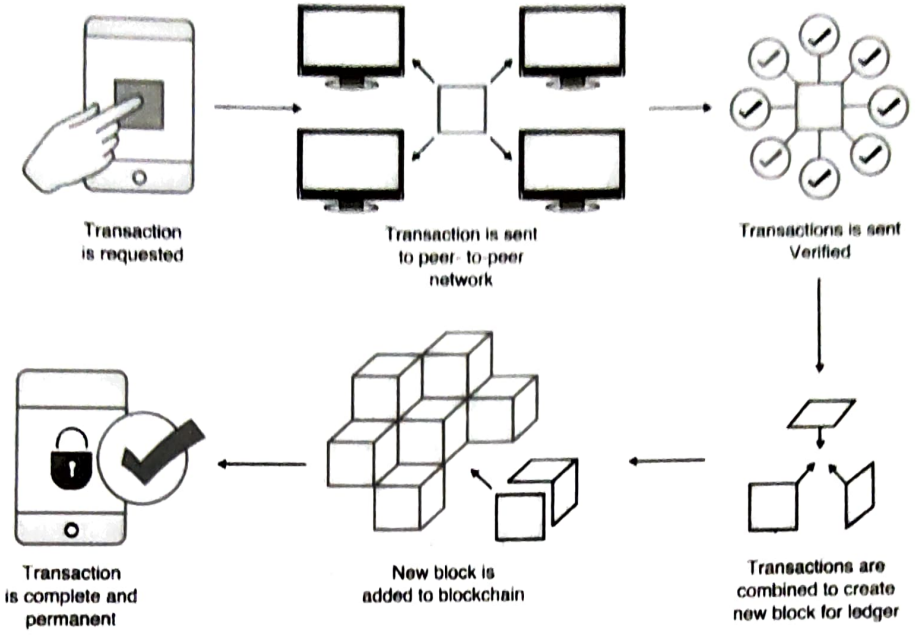


Fig. 2.7.1

- All transactions are replicated across the network of users and then accumulated in every member's computer system, enabling a distributed ledger-which can be shared across various organizations, locations, or countries.

2.7.2 Features of Blockchain

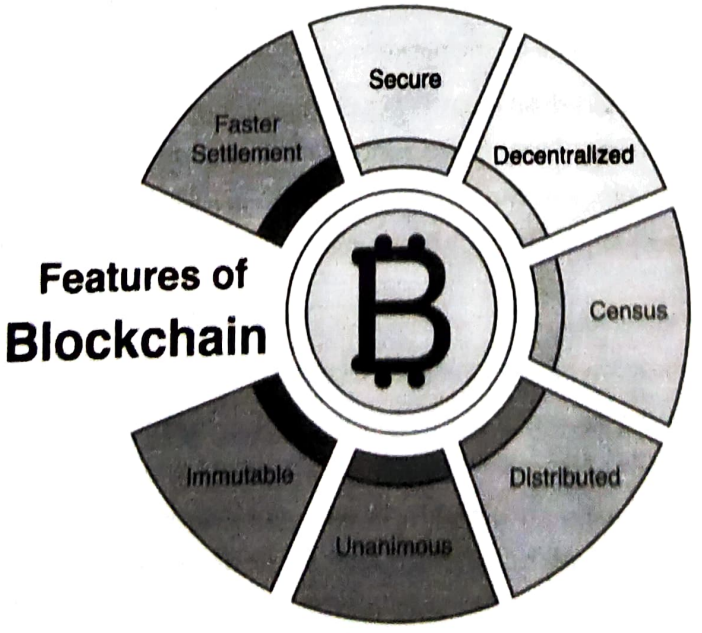


Fig. 2.7.2 : Features of Blockchain

1. Immutable

Immutability suggests that the blockchain is an unalterable and permanent network. Creation of immutable ledgers is one of the main values of Blockchain. Blockchain technology operates through a collection of nodes.

- Every node on the system has a replication of the digital ledger. In order to add a transaction validity of every node needs to be checked . It is added to the ledger, only if the majority thinks it is valid. This promotes transparency and corruption proof.
- Once the transaction blocks is added on the ledger, no one can go back and just change it. Thus, no user on the network will be able to edit, update or delete it.

2. Distributed

For complete transparency, all network participants have a copy of the ledger. A public ledger will supply complete information about all the participants on the network and transactions. Distributed ledger is one of the major features of blockchains due to many reasons like : In distributed ledger tracking the happenings in the ledger is easy as changes propagate really fast in a distributed ledger. Every node on the blockchain network should maintain the ledger and participate in the validation. The distributed ledger permits anyone with the required access to view the ledger and makes the process reliable and transparent.

3. Decentralized

Decentralized technology gives you the power to store your assets in a network without the control and oversight of a single person, entity or organization. Rather a group of nodes makes and maintains the network. In the blockchain network, each and every node has the same copy of the ledger. Decentralization property provides many advantages in the blockchain network : Because of decentralization we have User Control, No single point of failure, No intermediaries, Less Failure, and Zero Scams.

4. Secure

- All the records are individually encrypted in the blockchain. Use of encryption adds another layer of security to the complete process on the blockchain network. Since there is no central authority, it means that no one can simply add, update or delete data on the network.
- Every information on the blockchain is hashed cryptographically which signifies that every piece of data on the network has a unique identity. Every blocks contain a unique hash of their own and the hash of the previous block. As a result of this property, the blocks are cryptographically linked with each other. To modify the data means to change all the hash IDs which is nearly impossible.

5. Consensus

Every blockchain has a consensus to help the network to perform unbiased and quick decisions. Consensus is a decision-making algorithm for the group of nodes active on the network to reach an agreement quickly and for the system to function smoothly. Nodes might not trust each other although they can trust the algorithm that runs at the core of the network to make decisions. There are lot of consensus algorithms available each with its pros and cons. Every blockchain must have a consensus algorithm or else it will lose its value.

6. **Unanimous**

The records are validated by all the network participants, before they can be added to the network. If a node wants to add a block to the network then it must get majority voting otherwise the block cannot be added to the network. A node cannot just add, update, or delete information from the network. Every record is updated simultaneously and within the network the updations propagate quickly. So it is impossible to make any change without consent from the majority of nodes in the network.

7. **Faster Settlement**

- Traditional banking systems are inclined to many reasons for fallout like taking days to process a transaction after finalizing all settlements, which can be easily corrupted. On the contrary, blockchain offers a faster settlement compared to traditional banking systems. This blockchain feature makes life easier.
- Blockchain technology is improving and increasing day by day and has a really bright future in the forthcoming years. The trust, transparency, and temper proof characteristics gave rise to many applications of it like Ethereum, bitcoin, etc. It is a pillar in making the business and governmental procedures more efficient, secure, and effective.

2.8 Types of Blockchain

- In the last few years blockchain technology is used in a variety of fields as per the need, it can be divided into multiple categories based on the different attributes.
- While giving the reading access to a node there can be conflict for transparency and privacy issues on whom to grant read access and access to generate new transactions. There can be two options, grant the reading access to every node or grant a limited access to a limited group of users or nodes. With respect to this blockchain network can be distinguished as a Public blockchains or Private blockchains. Public blockchains grant read access and the right to create new transactions to all users or nodes while Private blockchains give permission to a preselected group of users or nodes.
- Fig. 2.8.1 shows the types of blockchain

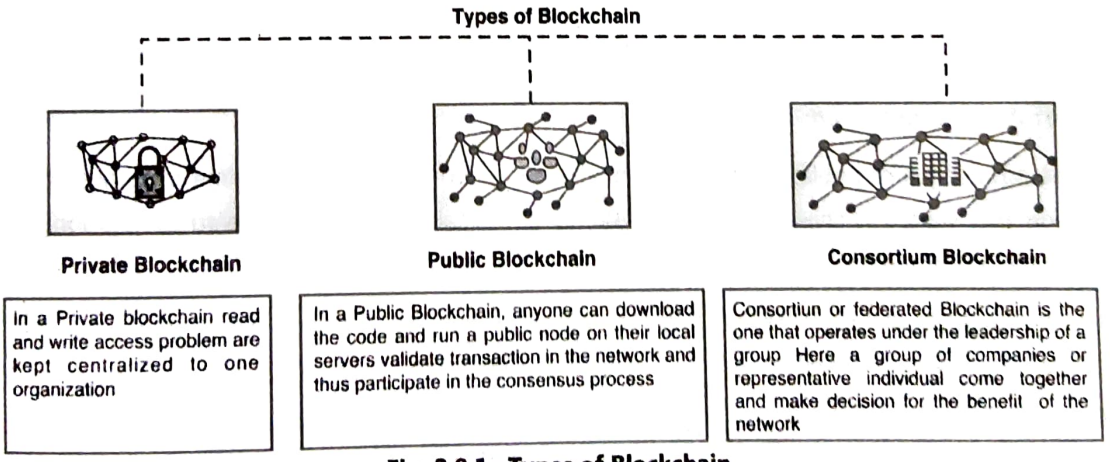
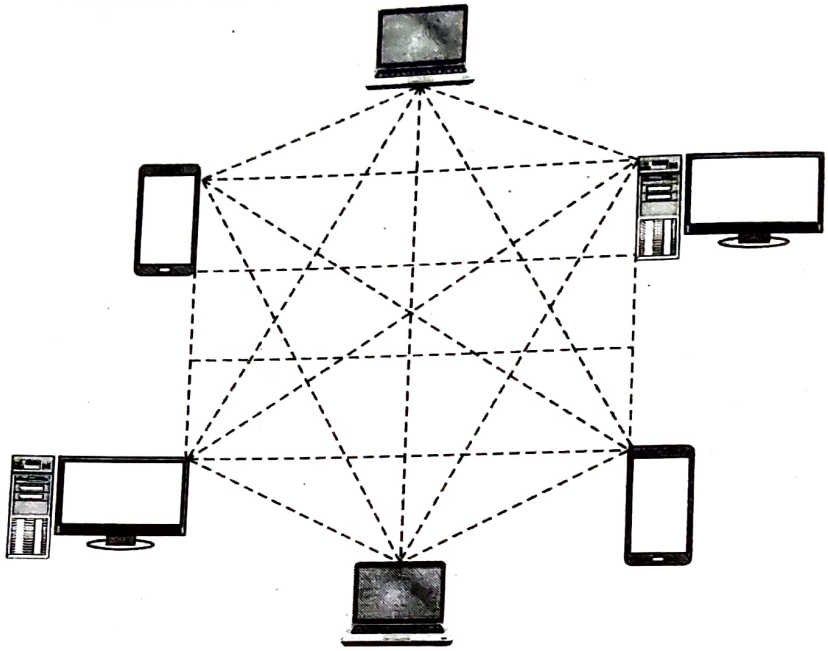


Fig. 2.8.1 : Types of Blockchain

2.8.1 Public Blockchains

- As the name suggests, public blockchains are open to the public, they are not owned by anyone. Anyone can participate as a node in the decision-making process. Users may or may not be rewarded for their participation. Bitcoin and Ethereum are both public blockchains.

- Bitcoin and other cryptocurrencies originated from public blockchains, which also played a role in popularizing Distributed Ledger Technology (DLT).
- Public blockchain is non-restrictive and anyone with internet access can sign on to a blockchain platform to become an authorized node. This user can access current and past records and conduct mining activities, the complex computations used to verify transactions and add them to the ledger. No valid record or transaction can be changed on the network, and anyone can verify the transactions, find bugs or propose changes because the source code is usually open source.
- Examples of public blockchains are Bitcoin, Ethereum, Dash, Monero, and Litecoin etc.



Public Blockchain: Permissionless
An open network system where all the devices can freely access without any kind of permission. The ledger is shared and transparent.

Fig. 2.8.2 : Public blockchain

Advantages of Public blockchain

1. One of the advantages of public blockchains is that they are completely independent of organizations, so if the organization that started it ceases to exist the public blockchain will still be able to run, as long as there are computers still connected to it.
2. Another advantage of public blockchains is the network's transparency. As long as the users follow security protocols and methods fastidiously, public blockchains are mostly secure.

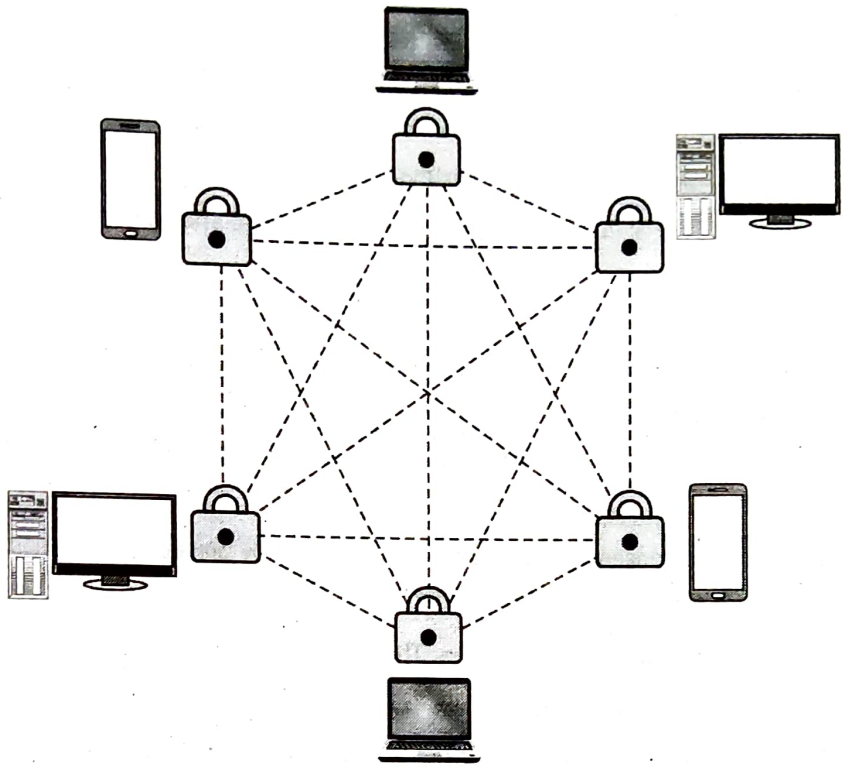
Disadvantages of Public blockchain

1. The network can be slow, and companies can't restrict access or use.
2. If hackers gain 51% or more of the computing power of a public blockchain network, they can unilaterally alter the data in the blockchain.
3. Public blockchains also don't scale well. The network slows down as more nodes join the network.

Use cases

- 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.
- This type of 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.

2.8.2 Private Blockchain Networks



Public Blockchain : Permissioned
A user has to be permitted by the blockchain authority before he/she could access the network. The user might join only if he/she gets an invitation.

Fig. 2.8.3 : Private Blockchain Network

Private blockchains operate on closed networks, and are useful for private organizations and businesses. That is, they are open only to a group of individuals or organizations who have decided to share the ledger among themselves. Companies can use private blockchains to customize their authorization preferences and accessibility, parameters to the network, other important security options, etc. A private blockchain network is managed by only one authority. They're also known as permissioned enterprise blockchains or blockchains.

Advantages of Private Blockchain

1. The controlling organization sets permission levels, security, authorizations and accessibility. For example, an organization setting up a private blockchain network can determine which nodes can view, add or change data. It can also prevent third parties from accessing certain information.

2. As users or Nodes are limited in size, private blockchains can be very fast and can process transactions much more quickly than public blockchains.

Disadvantages of Private Blockchain

1. It is more difficult to achieve full trust in the information, since centralized nodes determine what is valid.
2. As less number of nodes can also mean less security. The consensus method can be compromised If a few nodes go rogue.
3. The source code from private blockchains is often closed and proprietary.
4. Users can't independently audit or confirm closed, which can lead to less security.
5. There is no anonymity on a private blockchain.

Use cases

- 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.

2.8.3 Consortium Blockchain

- The next type of blockchain is Consortium blockchains that have both public and private components, except multiple organizations will manage a single consortium blockchain network. To set these types of blockchains can initially be more complex but they can offer better security. Consortium blockchains are optimal for collaboration with multiple organizations.
- In a consortium blockchain, the consensus procedures are controlled by preset nodes. It has a validator node that validates, initiates and receives transactions. Member nodes can initiate or receive transactions.
- A consortium blockchain consists of two types of users. They are :
  1. The users who can access the blockchain.
  2. The users who have control over the blockchain and decide who should have permission to access the blockchain.

Advantages of Consortium blockchain

1. A consortium blockchain tends to be more scalable, secure and efficient than a public blockchain network.
2. Like private and hybrid blockchain, it also offers access controls.

Disadvantages of Consortium blockchain

1. Consortium blockchain is less transparent than public blockchain.
2. It can still be compromised if a member node is breached; the blockchain's own regulations can impair the network's functionality.

Use cases

1. Payments and Banking are two uses for this type of blockchain. Different banks can band together and form a consortium, deciding which nodes will validate the transactions.
2. This type of blockchain is good for tracking food and medicine supply chains where different parties are involved.

2.8.4 Comparison of Different Types of Blockchain

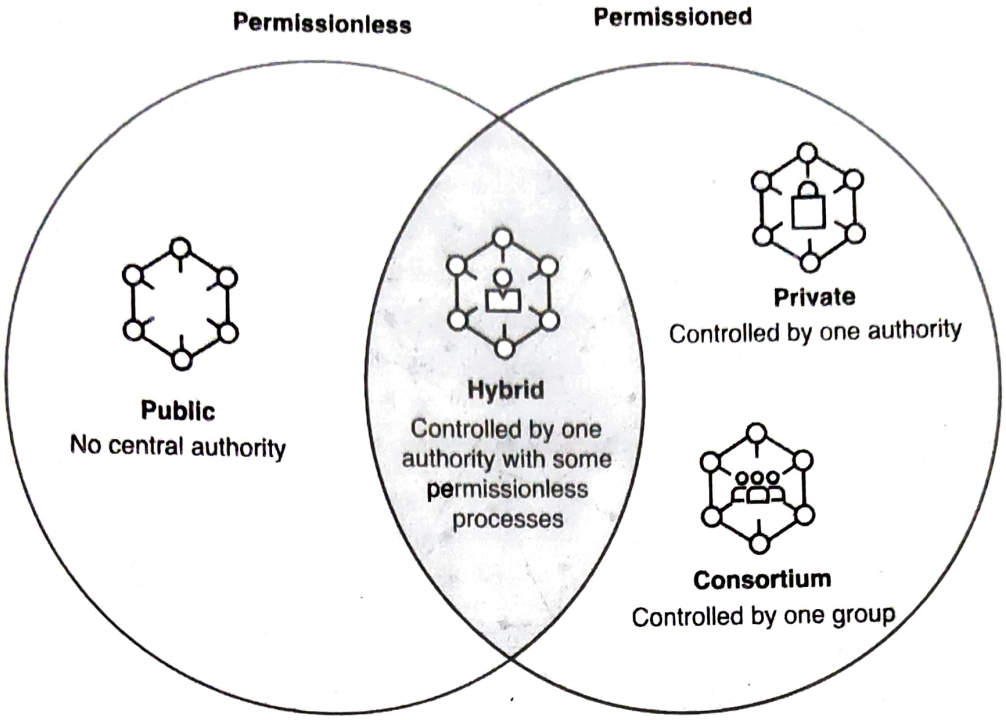


Fig. 2.8.4 : Types of blockchain

Table 2.8.1

Public Blockchain	Private Blockchain	Consortium Blockchain
Anyone can run full node	Not everyone can run full node	Selected members of the consortium can run full node
Anyone can make transactions	Not everyone can make transactions	Selected members of the consortium can make transactions
Anyone can review / audit the Blockchain	Not everyone can review / audit the Blockchain	Selected members of the consortium can review / audit the Blockchain
Example: Bitcoin, Litecoin etc.	Example: Ripple(XRP) Hyperledger	Example: R3, EWF

- Every one of these types of blockchain has potential applications that can improve trust and transparency and create a better record of transactions. Ultimately, blockchain technology is gaining enterprise support becoming more popular and rapidly.

2.9 Centralized Vs. Decentralized Systems

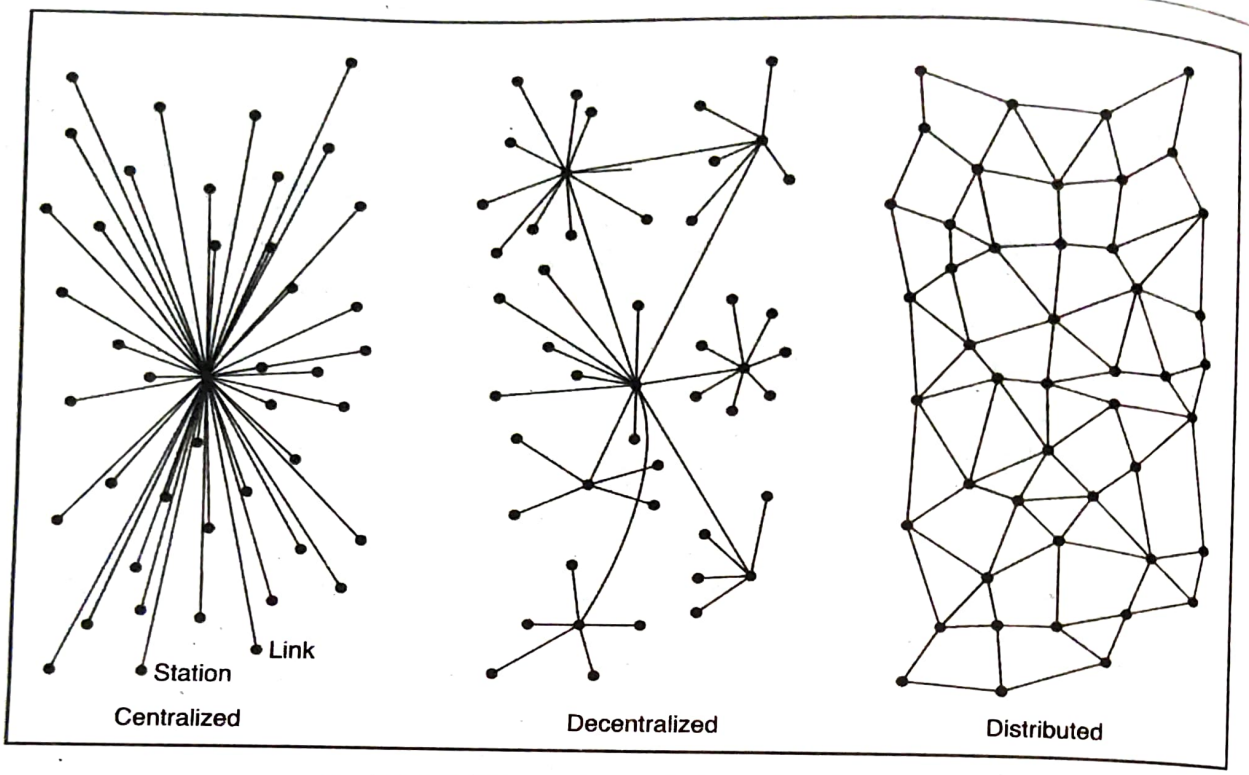


Fig. 2.9.1 : Different types of Networks / Systems

2.9.1 What does Centralization Mean?

- Centralized systems are traditional (client-server) IT systems in which a central authority is in control of the functions and data for the platform which is in use, and who is entirely in charge of all operations on the system. All users of a centralized system rely on a single source of service. A centralized authority controls the majority of online service providers like Google, Amazon, eBay, Apple's App Store, Facebook, YouTube, Twitter, and others like your bank account.
- For example, if you are using the Facebook platform, then Facebook has complete control over the various aspects of their features including the decision of who and who cannot join the platform. This means to verify a data transaction, a third-party intermediary must do this on your behalf. This means that using the Facebook platform, if you are sending a message to your friend, then the data will be verified and then transferred by the said platform.
- Another example is sending an email using any mail domain. The instant you send an email to another person, the email service provider is aware of what you sent and when you sent it. This information is accumulated privately without any identifier, but a copy of that information is with the email service provider, in any case. This means that you must trust that your data is kept private by the email provider.
- Centralized systems are traditional (client-server) IT systems in which there is a single authority that controls the system, and who is entirely in charge of all operations on the system. All users of a centralized system rely on a single source of service. The majority of online service providers like Google, Amazon, eBay, Apple's App Store, and others use this conventional model for delivering their services.

2.9.2 Advantages of Centralization

Some advantages of centralization are as follows :

- **Reduced Costs :** As centralized networks or organizations are pre-planned and setup is ready so the costs associated with it do not exceed budgets. The cost will be increased only when expansion of the network is required. So the biggest advantage of centralization is the cost associated with it.
- **Command Chain :** In the centralized organization, the chain of command is known by them. That is every person in the organization is aware of their role and whom do they need to report to. They are aware of whom they are reporting and their subordinates and actions too. This also means that delegation is effortless in the chain. Senior executives can finish the work in the best possible way by easily delegating work to their subordinates and finalizing. If work is successfully completed, it creates a trust among the workers and chain, improving the confidence necessary to make it work. One central node or a collection of nodes are responsible for transactional verification in a centralization network.
- **Quick Decision Implementation :** In centralization organizations or networks the decision implementation are quick. As centralized networks have less nodes or people, it requires fewer communication among the different levels of authorization.

Also, if a centralized network decides to implement a change, it can be finished in a matter of minutes. For example, a centralized network can put more stress on the KYC procedure and determine to add more requirements for it. As the network is centralized, they can push the new guidelines or modify the KYC procedure which can go live almost immediately after proper testing.

2.9.3 Disadvantages of Centralization

Some disadvantages of centralization are as follows :

- **Security :** For any system security is a nightmare. In the centralized system, it is a major issue since all the data is stored in one location and all operations are executed through a central server which makes it an easy victim for various types of attacks especially to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. The enormous increase of IoT devices in our environment accelerates the chances to exploit security vulnerabilities within IoT devices which are poorly secured. Therefore, both IoT devices (source of data) and centralized cloud server (data storage location) are an easy prey for various security attacks.
- **Trust :** The centralized organizations are not completely trustable or secure. The trust is an agreement that is set by the user and the service provider. Nevertheless, that's an agreement and it can break easily.
- **Privacy :** The centralized system is vulnerable to data manipulation. Collecting real-time data of different devices and storing it at one place with the authority of the centralized server can violate the data privacy. The collected data may contain sensitive information about nodes such as their passwords, financial accounts, etc. As these data are stored in one place, it can be easily violated. On the contrary, there are various examples of privacy violation by service providers. For example, information about their customers is sold by some service providers to marketing companies that can use this information to examine nodes' behaviour. Also, if a public utility company found that their smart meter data analysis might be the evidence that will result in lawsuits or high costs. They will alter or even delete these data. Hence, privacy is another issue in the centralized IoT system that needs to be tackled.

- **Single point of failure :** Due to single point where the whole network is dependent on the Centralized organization and even if Single point of failure occurs creates a problem for it. Organizations know about the disadvantage and hence have arranged measures to contain it. For mission-critical services, the fact that there is a chance for failure is a big disadvantage.
- **Scalability Limitation :** In most of the cases, a single server is used, which leads to scalability limitations. For the centralized system, it is a major issue since it based on controlling and managing all processes using a central authority. This system can scale well but only for small networks. It will be impractical, deploying a centralized system for large business organizations with many branches in different locations. Based on the management hierarchy it will be hard to transport decisions to different locations. In the IoT context, since there is a massive increase in the number of IoT devices, there are many uncertainty about the capability of the centralized architecture of the IoT to scale and function efficiently with the increasing demands.
- **Inflexibility :** There are huge workloads coming from different nodes in the network, since the centralized server carries out all processing operations and controls all nodes connected to the network. Although the centralized server schedules the workload to prevent peak-load concerns when people across an organization need to use it simultaneously, the pack schedule and delay associated with this process, restrict the flexibility of the user while doing their own work.
- **Access and Diversity :** The network can accessed by the nodes for different needs. However, centralized systems need their nodes to access the information on the network consistently using identical processes. This kind of network may not give the flexibility needed by several nodes with different needs. In addition, a single operating system is used by a centralized system for the whole network. While this can benefit some nodes, it restricts diversity within the network and can forbid some nodes from accessing the network. Since the IoT system is heterogeneous and dynamic in nature with different devices and objects, ensuring access to various heterogeneous devices should be a basic priority for the centralized IoT architecture.

2.10 What is Decentralization?

- A decentralized system is a type of network in which the nodes are not dependent on a single master node; instead, control is distributed among many nodes. This is similar to a model in an organization where each department is in charge of its own database server, thus eliminating the power of the central server and dispersing it to the sub departments who manage their own databases. The fundamental idea of decentralization is to distribute authority and control to the peripheries of an organization. This configuration provides various benefits for organizations, such as enhanced efficiency, accelerated decision making, better motivation, and a reduced load on top management.
- Decentralization was initially made possible using blockchain technology. A significant innovation in the decentralized paradigm that has induced this new era of decentralization of applications is decentralized consensus. Bitcoin client was the first-ever blockchain, which was created in 2009. Using a consensus algorithm Bitcoin enables a user to agree on something, without the necessity for an intermediary, central, trusted third party or a service provider. A consensus mechanism governs this competition, and the most commonly used method is known as Proof of Work (PoW).
- When a person sends Bitcoin to someone else, transactions are not verified by a centralized authority. Rather anybody can hook up their computer to the Bitcoin system to help verify a movement of funds. Every device

connected to the system is known as a "node", and in total there are thousands of independent nodes all of which are helping to operate the network.

- From a semi-decentralized model to a fully decentralized one, Decentralization is applied in varying degrees depending on the circumstances and requirements.
- From a blockchain perspective Decentralization can be viewed as a mechanism that provides a way to remodel existing paradigms and applications, or to create new applications, for the sake of giving full control to the users.

Advantages of Decentralisation

- **Provides a trustless environment :** No one has to trust or know anyone else in a decentralized blockchain network. Within the network every member has a copy of the exact same data in the form of a distributed ledger. If any member's ledger is corrupted or altered in any way, majority of the members in the network will reject it.
- **Improves data reconciliation :** Many companies often exchange data with their partners. This data, is typically transformed and stored in each party's data storage place, only to resurface when it needs to be passed downstream. Each time the data is transformed, it opens up possibility for data loss or incorrect data to enter the work stream. Every entity has access to a real-time, shared view of the data by having a decentralized data store.
- **Reduces points of weakness :** In systems Decentralization can reduce points of weakness where there may be too much dependence on specific actors. These weak points could lead to integral failures, including failure in providing promised services or inefficient service due to the depletion of resources, periodic interruptions, bottlenecks, lack of sufficient incentives for good service, or corruption.
- **Optimizes resource distribution :** Decentralization can also help optimize the distribution of resources so that the promised services are provided with consistency and better performance, as well as a reduced probability of catastrophic failure.
    - Decentralization usually has some disadvantages such as lower transaction output, but preferably, the trade offs are worth the improved stability as well as the service levels they produce.
    - Decentralization should be put in application where it makes sense. It doesn't mean that just because it's a blockchain application, it needs to be 100% decentralized.
    - Information and Communication Technology (ICT) has conventionally been based on a centralized paradigm whereby a central authority, such as a system administrator controls the database or application servers. With Bitcoin and the emergence of blockchain technology, this model has transformed and now the technology exists, which allows anyone to start a decentralized system and operate it with no single trusted authority or no single point of failure. It can either be run independently or by requiring some human intervention, depending on the model and type of governance used in the decentralized application administrating on blockchain.

2.11 What is a Distributed System?

- A distributed system, computation and data are spread across multiple nodes in the network. At times, this term is confused with parallel computing. While there is some intersection in the definition, the main difference between these systems is that in a parallel computing system, computation is executed by all nodes simultaneously for the sake of achieving the result; for example, parallel computing platforms are used in simulation and financial modelling, weather research and forecasting.

- On the contrary, in a distributed system, computation may not happen in parallel and data is duplicated across multiple nodes that users view as a single, coherent system. Variations of both of these models are used to achieve speed and fault tolerance. In the parallel system model, there still is a central authority which governs processing and has control over all nodes.

Difference between Centralized, Distributed and Decentralized

Table 2.11.1

	Centralized	Distributed	Decentralized
Network/hardware resources	Maintained & controlled by single entity in a centralized location.	Spread across multiple data centers & geographies; owned by network provider.	Resources are owned & shared by network members; difficult to maintain since no one owns it.
Solution components	Maintained & controlled by central entity	Maintained & controlled by solution provider.	Each member has exact same copy of distributed ledger.
Data	Maintained & controlled by central entity	Typically owned & managed by customer.	Only added through group consensus.
Control	Controlled by central entity	Typically, a shared responsibility between network provider, solution provider & customer.	No one owns the data & everyone owns the data.
Single Point of Failure	Yes	No	No
Fault tolerance	Low	High	Extremely high
Security	Maintained & controlled by central entity	Typically, a shared responsibility between network provider, solution provider & customer.	Increases as # of network members increase.
Performance	Maintained & controlled by central entity	Increases as network/hardware resources scale up and out.	Decreases as # of network members increase.
Example	ERP system	Cloud computing	Blockchain

- This implies that the system is still centralized in nature. The critical difference between a decentralized system and distributed system is that in a decentralized system, no central authority exists, whereas in a distributed system there still exists a central authority that governs the entire system.

2.12 Distributed Ledger

- The distributed ledger created using blockchain technology is unlike a traditional network, as it does not have a central authority common in a traditional network structure (see the Fig. 2.12.1). Decision-making is generally done by the central authority, who decides in all aspects. The traditional database structure therefore is controlled by the central authority.

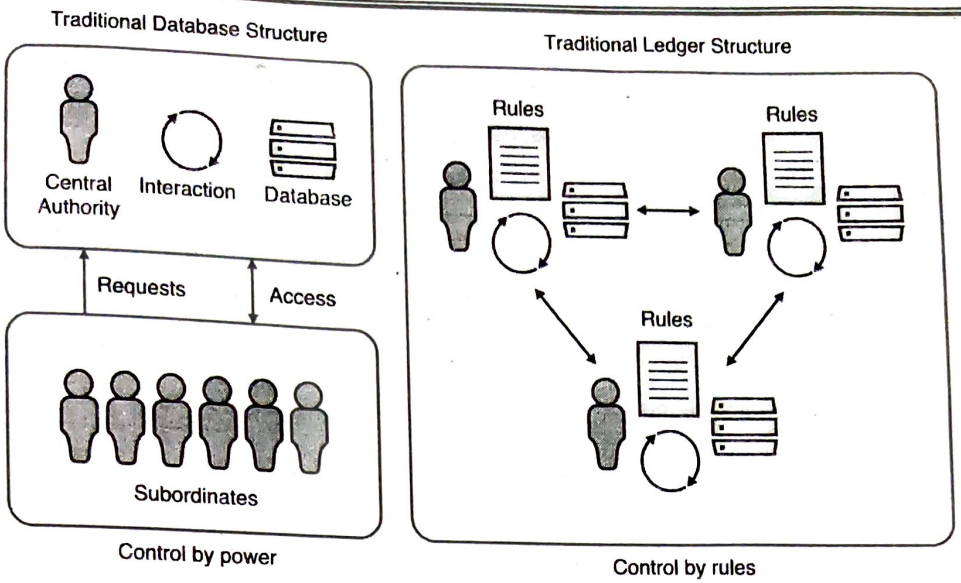


Fig. 2.12.1 : Traditional Database vs. Distributed Ledger

- Traditional network structure is effective too. Certain business functions may best be controlled by a central authority. However, such a network structure is not without its cons. Transactions cost money and take time to process; in addition they are also not validated by all parties due to limited network participation, and they are vulnerable to hacking and prone to error. Technical skills are required to process transactions in a traditional network structure.
- On the other hand, the distributed ledger is controlled by rules, and not a central authority. The database is available to all the members of the network and is installed on all the computers that use the database. To add transactions to the database, Consensus is required between members. Each transaction is encrypted through an algorithm and a "key" to convert an unencrypted input (i.e., plain text) into an encrypted output (i.e., ciphertext). Accordingly, transactions in a distributed ledger are supposed to be :
  - Processed speedily and at a lower cost
  - Validated by all participating members of a network
  - Less prone to error
  - Virtually hack-proof.
- As with any new technology, Certified public accountants will need to acquire new technical skills to review, process, and audit transactions in a blockchain, the details of which will depend upon the services provided.

What's the current state of Centralization?

- Centralization is unquestionably an effective way to manage networks or organizations. It has been effectively used by big organizations such as Facebook, Microsoft, Yahoo, and so on. In fact, our governments are also dependent on a centralized approach. The political executives coordinate the power, in the case of a centralized government. You can also apply the power in multiple cases.
- For a big corporation, centralization ensures that its data is secure. This is required so that their trade secrets are not disclosed. However, there is a modified way for manipulation of the data with the option to use decentralized networks such as blockchain.

- We can easily say that centralization is still very widespread in the current market. And, not all businesses need to adopt decentralization just for the sake of it. Different business models thrive in a centralized network and it will take some time before more and more businesses move towards decentralized models.

2.13 Transactional Blocks

- The architectural components have been generalized and then modified by numerous companies, leading to different blockchain projects like Bitcoin, Hyperledger, Ethereum, etc. Let's consider the bitcoin blockchain architecture here.
- Below are the architectural components :
  - Transaction
  - Block
  - P2P Network
  - Consensus Algorithm

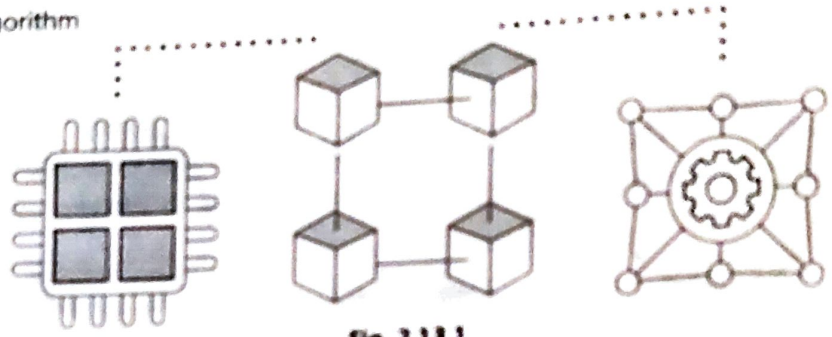


Fig. 2.13.1

1. Transaction

- The smallest building blocks of a blockchain system are Transactions. They normally comprise a recipient address, a sender address, and a value. It is identical to a standard credit card statement. The owner transfers the value by digitally signing the hash generated by adding the previous transaction and the receiver's public key.
- The transaction is then publicly declared to the network and all the nodes hold their own copy of the blockchain independently, and the current known "state" is calculated by processing each transaction in the same order as it appears in the blockchain. Transactions are packed together and delivered to each node in the block form. As new transactions are distributed throughout the network, they are independently processed and verified by each node. Every transaction is time-stamped and collected in a block.

2. Block

- Block holds the information as a block header and transactions. Blocks are data structures whose motive is to bundle sets of transactions and are copied to all nodes in the network. Miners create the blocks in the blockchain. Mining is the process of creating a valid block that will be accepted by the rest of the network.
- Nodes take pending transactions, verify if they are cryptographically precise, and bundle them into blocks to be stored on the blockchain. Block header is the metadata that assists in verifying the validity of a block. The contents of a block metadata is shown in the Fig. 2.13.2.

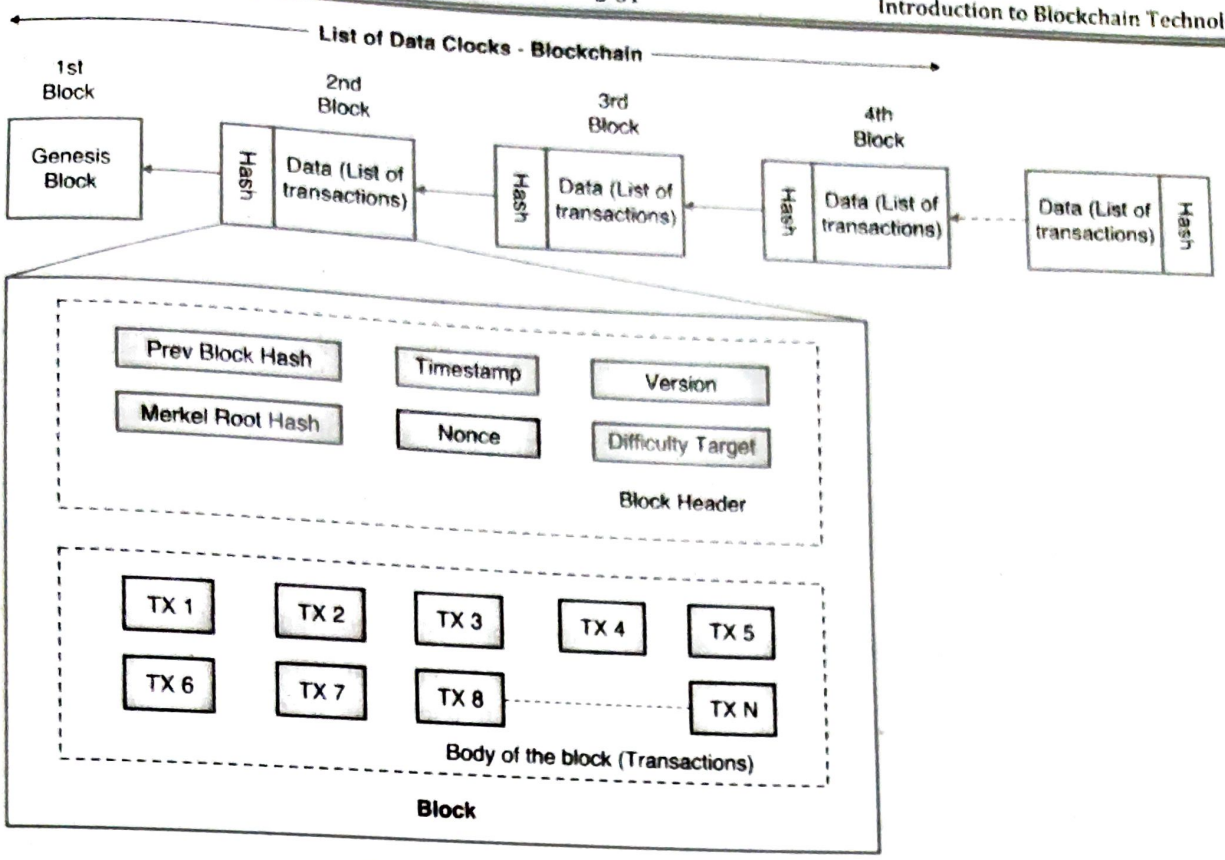


Fig. 2.13.2 : Components of Block in Blockchain

- A block stores information. Within a block there are many pieces of information, but it doesn't use a large amount of storage space. Blocks generally include these elements, but it might differ between different types
  - **Blocksize :** It sets the size limit on the block ensuring that only a specific amount of information can be written in it.
  - **Block header :** Includes information about the block.
  - **Transactions :** A list of all the transactions within a block.
- The transaction element contains the most information hence it is the largest. It is accompanied in storage size by the block header, which includes these sub-elements :
  - **Version :** The version of cryptocurrency being used.
  - **Previous block hash :** Contains an encrypted number or hash of the previous block's header.
  - **Hash Merkle root :** Hash of the transactions in the Merkle tree of the current block.
  - **Time :** A timestamp to arrange the block in the blockchain.
  - **Bits :** The rating of difficulty of the target hash, denoting the difficulty in solving the nonce..
  - **Nonce :** The encrypted number that a miner must solve in order to verify the block and close it.
- The rest of a block contains transactions. Depending on the choice of a miner, it can be any number of transactions bundled in a block .
- The First block of the chain is called the Genesis block.

3. **P2P Network**

- Blockchain is a Peer to Peer (P2P) network working on the protocol known as IP protocol. A P2P network is a flat topology with no centralized node. All nodes equally provide and can utilise services while collaborating using a consensus algorithm. Peers contribute to the storage and computing power that is required for the maintenance of the network. P2P networks are usually more secure because they do not have a single point of failure or attack as in the case of a centralized network.
- A blockchain network can be a permission-based network and a permissionless network also. A permissionless network is also called a public blockchain because anyone can join the network, while a permission-based blockchain is called a consortium blockchain. Pre-verification of the participants within the network is required in a permission-based blockchain or private blockchain and the parties are usually known to each other. In a typical blockchain architecture, every individual node in a network preserves a local copy of blockchain. The decentralization of blockchain architecture is the individual credit of the P2P network that it is built on.

4. **Consensus Algorithm**

All these copies of a single ledger are synchronized due to a consensus algorithm. The consensus mechanism makes sure that the local copy every individual party has, they are consistent with each other and is the most updated one. The copy that every individual node has are identical to each other. It could be arguably framed that the consensus algorithm forms the core of every blockchain architecture.

5. **Why use blockchain technology**

Business runs on information. The faster it's received and the more accurate it is, the better. Blockchain is ideal for delivering that information because it provides immediate, shared and completely transparent information stored on an immutable ledger that can be accessed only by permissioned network members. Blockchain technology provides one of the most secure and safe online transactions so the field of Blockchain in the IT sector is growing very fast. A blockchain network can track orders, payments, accounts, production and much more. And because members share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, as well as new efficiencies and opportunities.

2.14 Important Properties of Blockchain

Blockchain Applications are adopted because of following properties :

1. **Decentralisation**: Within a distributed network, data presented in the form of a distributed ledger. If the information is somehow corrupted, most participants can reject it, that's why it minimises possibilities of fraud.
2. **Immutability:** Once performed, a transaction is recorded with no further alterations or removal. Time and date stamps ease data tracking in the long run. Therefore, blockchain ensures reliable data audits.
3. **Cybersecurity :** Due to powerful encryption and immediate recording, the probability of attacks performed by malicious intruders falls to its lowest level. Anyways, it's a lot more complicated to hack such a network compared to systems stored on dedicated servers. Access permissions and data anonymization also guarantee high privacy protection.
4. **Cost reduction :** Organisations, an decrease in operational expenses due to eliminating facilitators, an ability to process transactions efficiently, Data can be aggregated automatically as well as reporting and auditing processes is easy.

5. **Traceability :** Tracing the origin of products and managing inventories more efficiently is of high importance for retailers. Thus, enabling a high quality of goods in real time.

By bringing disruption and business transformation, blockchain technology helps organisations minimise security-related risks and decrease operational costs.

2.15 Blockchain for Industries

- Industry leaders are using IBM Blockchain to remove friction, build trust and unlock new value. Several industries like Unilever, Walmart, Visa, etc. use blockchain technology and have gained benefits in transparency, security, and traceability.
  - Supply chain
  - Healthcare
  - Government
  - Retail
  - Media and advertising
  - Oil and gas
  - Telecommunications
  - Manufacturing
  - Insurance
  - Financial services
  - Travel and transportation
- As a database, a blockchain preserves information electronically in digital format. Blockchains are renowned for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a decentralised and secure record of transactions.
- The innovation with a blockchain is that it guarantees the security and fidelity of a record of data and builds trust without the need for a trusted third party. Virtually anything of value can be tracked and traded on a blockchain network, cutting costs and reducing risk involved. It is estimated that Blockchain technology has been adopted by more than one-third of the companies in the world and demand for blockchain developers is ever-increasing.

2.16 Blockchain Limitations

When deciding whether to implement it or not, it's important to know what challenges lie behind its introduction and the technology itself.

1. **Low Scalability**
   - The problem is that transaction speed depends largely on network congestion, which means that the more people or nodes are involved, the slower the pace is. This problem is related to scalability issues with blockchain networks. In simple words, the more people or nodes join the network, the chances of slowing down is more!
   - Here's an example: Centralized payment systems can process tens of thousands of transactions per second, while Bitcoin can only manage seven.

2. **Lack of Awareness :** People do not know the true value of blockchain and how they could implement it in different situations.

3. **Limited availability of technical talent :** According to estimates, each year, the need for high-skilled blockchain developers is more. But in blockchain technology, there are not so many developers available who have specialised expertise in blockchain technology. Hence, the lack of developers a problem of developing anything on the blockchain

4. **Implementation Challenge :** It's all about initial financial investments. For some businesses, implementation costs may turn out to be overwhelming.

5. **Immutable :** In immutable, we cannot make any modifications to any of the records. It is very helpful if you want to keep the integrity of a record and make sure that nobody ever tampers with it. But immutability also has a drawback.

6. **Private Key Issues :** In the decentralised environment, private keys owned by individuals may become a weak spot. When you are dealing with a private key, then you are also running the risk that somebody may lose access to your private key. It happens a lot in the early days when bitcoin wasn't worth that much. If stolen, it puts both sensitive data and finances in problem. If lost, then wallet access is gone forever.

7. **Problematic Integration With Legacy Systems :** If the blockchain solution is to be integrated with outdated systems already in use, possible data loss or corruption risks arise,

8. **High Energy Consumption :** Most blockchain-based solutions, like Bitcoin, use a proof-of-work consensus algorithm for validating transactions, which utilizes excessive computing power comparable to the yearly electricity consumption of a country like Denmark. With the resources needed to cool down the equipment, prices are only rising. So, if proof-of-work is your only option, you'll have to pay for it with energy costs.

2.17 Blockchain Adoption

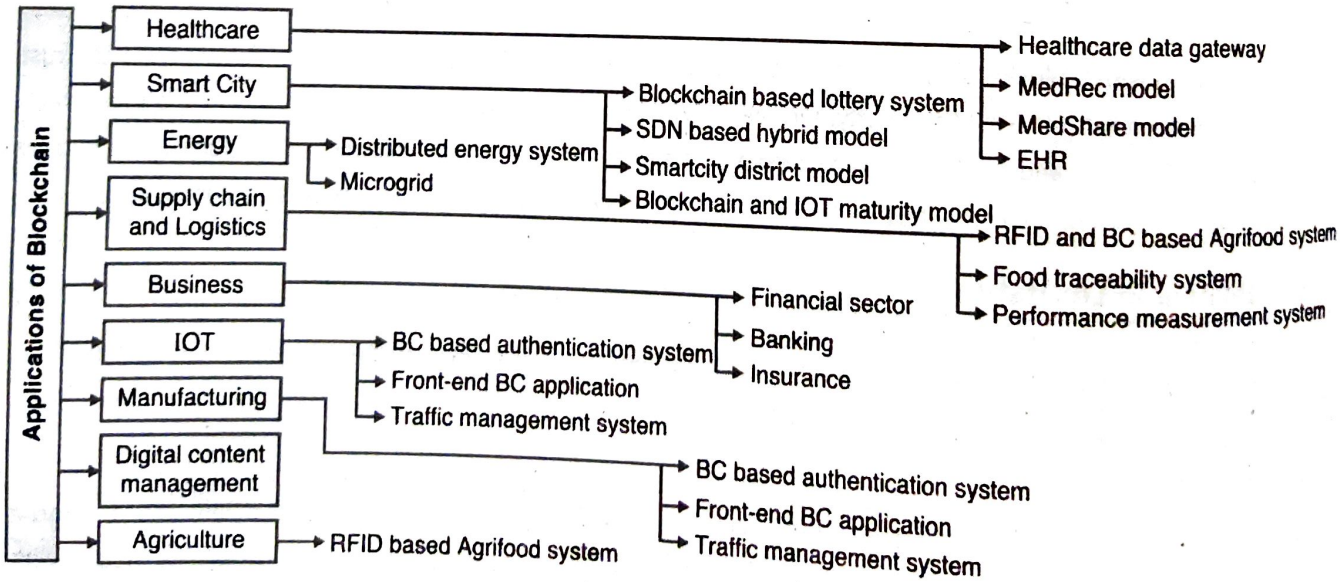


Fig. 2.17.1 : Applications of Blockchain

"Web 3.0" technology that has gained popularity. It relies on decentralized technology. Blockchains are ecosystems that demand broad adoption to work effectively.

- **Blockchain So far :** Initially, it was about Bitcoin; but afterwards many other cryptocurrencies also came into the market following the trend. While some of them found their fate, some other cryptocurrencies lagged behind. However, soon the blockchain technology found its real potential and extended to many other unpredictable domains. financial domains like Banking, Insurance, Healthcare Industry, Enterprise software development, and so on; today the blockchain is excessively changing existing technology frameworks of almost all domains. The blockchain market is expected to grow $20 billion by 2024, according to prominent statistics websites.
- **Banking and payments :** All the payment and banking systems are now moving towards blockchain. Bitcoin-like cryptocurrencies can manage the payment systems without any geopolitical restrictions. An example of bitcoin-based remittance is ABRA. JPMorgan Chase has entered the blockchain space with the JPM Coin, which is designed to facilitate real-time cross-border payments between its business clients. Other banks like Goldman Sachs and Citigroup have also experimented with blockchain. The incumbents performed an equity swap built on Axoni's Axcore blockchain in February 2020.
- **Stock market :** For years, companies have worked to ease the buying, selling, and trading of stocks, and now new blockchain-focused startups are looking to automate and secure the process more efficiently than any past solution
- **Crowdfunding :** It is a popular method of fundraising, for new projects and startups. In block-chain based crowdfunding platforms trust is built through online reputation systems and smart contracts, which eradicates the need for a central party who charges high fees for this service. Tokens of their own can be released by new projects that later can be exchanged for services, products or cash. For example, the movie BRAID became the first major feature film to be financed through a token "crowdsale" on the Ethereum blockchain through its $1.4M campaign on Weifund.
- **Crypto exchanges :** One way blockchain reduces conventional cybersecurity risk is by simply removing the need for human intermediaries — thus lessening the threat of hacking, corruption, or human error.
- **Insurance :** The global insurance market is centered on trust management. Blockchain is the new way of handling trust. Blockchain guarantees trust by mutual distrust between participants. Most blockchain applications in the insurance industry today are focused on improving operational efficiency. An example of a blockchain based insurance management system is 'Aeternity'. Insurwave, a joint project between consulting firm EY and blockchain company Guardtime, delivers a blockchain platform aimed at marine insurance.
- **Healthcare :** The use of blockchain technology could allow hospitals, payers, and other parties in the healthcare value chain to share access to their networks without compromising data security and integrity. HealthVerity is one of the platforms, combining a health data exchange with a blockchain product to manage permissions and access rights.
- **Cyber Security :** In blockchain, data is secured and verified using cryptography. This will restrict all unauthorized hacks and modifications in the system. It eliminates the middlemen from the system so that no one can make any unauthorized changes.
- **Supply chain :** The blockchain can revolutionize the supply chain by providing better accountability, transparency, and feedback mechanism along the supply chain. Using the blockchain supply chain management, any product can be tracked completely and easily. Each and every movement, along with the condition of a product, can be recorded in the blockchain with IoT sensors. Provenance and Blockverify is a blockchain based supply chain management system.

- **Online Data Storage :** Data on the centralized server like Google Drive, One drive etc. are vulnerable to the single point of failure. Blockchain permits distributed data storage in a more robust and secure way. Story is one such encrypted cloud storage facility.
- **Networking and IoT :** The blockchain technology can be applied in Networking and IoT to build a decentralized network of IoT devices. This eradicates the requirement for a central location to manage the IoT devices.
- **Government :** Applying blockchain technology in government systems will reduce red-tapism, bureaucratic hurdles, and increase transparency and efficiency of government operations. The government of Dubai has already started to implement this technology. Some governments are taking it upon themselves to realize the benefits of blockchain. For example, the Swedish Land Registry has explored the use of blockchain for land registration, potentially eliminating fraud and reducing ownership disputes. It has also tested the use of smart contracts to execute property sales.
- **Vaccine distribution & monitoring:** Governments in Malaysia and Singapore are already employing blockchain to authenticate vaccine certificates, using systems that can trace the exact vaccine batch of the vial used for an individual.
- **Multimedia and entertainment :** Now blockchain has stepped into the entertainment field where the third party interference is to a higher extent. Implementation of blockchain technology in this fields will remove the middleman from the scenario. One of the entertainment areas where blockchain has already started their implementation is Online music e.g. Ujo and Mycelia music.
- **Real estate :** It is another important area where blockchain implementation will create a drastic change. The current real estate system is facing a lot of transfer and ownership issues. Implementation of blockchain in this field can control the entire real estate systems with shared ledgers.
- **E-commerce:** Blockchain technology has the potential to transform e-commerce by lowering transaction costs and tightening transaction security. E-commerce giants such as Walmart, Amazon, and Alibaba have begun exploring blockchain technology.

Review Questions

Q. 1 Define Blockchain. What are the important features of it?

Q. 2 Explain the term distributed ledger.

Q. 3 Explain the birth of Blockchain along with the history of blockchains.

Q. 4 Write a short note on adaptation of Blockchain so far

Q. 5 What are the different phases of Blockchain evolution?

Q. 6 Differentiate between Public and Private Blockchain.

Q. 7 Compare centralized and decentralized systems.

Q. 8 Explain the concept of a centralized system with its pros and cons.

Q. 9 Explain the concept of a decentralised system with its pros and cons.

Q. 10 Explain the concept of distributed system with its pros and cons.

Q. 11 Compare between centralised versus decentralised versus distributed system.

Q. 12 Describe the Blockchain mechanism in brief.

Q. 13 Draw and explain the structure of the block.

Q. 14 State and explain the constitute of a block header.

Q. 15 Enlist the methods of identifying the block uniquely?

Q. 16 Write down the importance of genesis block?

Q. 17 List the key features of blockchain?

Q. 18 What do you mean by blocks in the blockchain technology?

Q. 19 List elements are in Every block of the Blockchain?

Q. 20 Elaborate the term change address.

Q. 21 If someone tries to hack block number 5 in a chain of 15 blocks ,what will happen and why?

Q. 22 What is bitcoin mining? Explain the functionality of miners.

Q. 23 State and explain different terms related to Blockchain.

Q. 24 Explain bitcoin and it's working. State how the value of bitcoin is decided.

Q. 25 Differentiate between different types of blockchain.

Q. 26 Give the different types of blockchain. State their advantages and disadvantages of each type.

Q. 27 Elaborate the importance of Blockchain with respect to safety.

Q. 28 How decentralization is achieved through Blockchain technology?

Q. 29 How can digital freedom be achieved through Blockchain?

Q. 30 Which features make Blockchain more important than our traditional system?

Q. 31 Why is Blockchain a trusted approach?

Q. 32 What are the limitations of Blockchain technology?

Q. 33 Blockchain needs high energy consumption, How?

Q. 34 What are the scalability issues of Blockchain?

Q. 35 Comment on various hurdles in adoption of Blockchain technology by industry.

Q. 36 Explain how Blockchain technology is adopted by the finance sector?

Q. 37 What do you think of the limitations of Blockchain or major hurdles in its adoption?

Q. 38 State importance of Blockchain.

Q. 39 Explain the consortium type of blockchain and its importance.

Q. 40 Explain the life cycle of bitcoin transaction.

Q. 41 Explain in detail how bitcoin transactions are traceable?

Q. 42 What is the candidate block?

Q. 43 Explain the different types of transactions.

Q. 44 Explain different types of blockchain nodes.

Q. 45 Give the importance of Bitcoin wallet.

Q. 46 Explain different types of Bitcoin wallet.

Q. 47 How transactions propagate?

Q. 48 Write the short note on Mining.

Q. 49 Explain the role of miner in Bitcoin.

□□□