Savitribai Phule Pune University

Blockchain Technology

(Code : 410243) (Compulsory Subject)

Semester 7 - Computer Engineering

Strictly as per the New Syllabus (2019 Course) of
Savitribai Phule Pune University w.e.f. Academic Year 2022-2023

Dr. Parikshit N. Mahalle
M.E. (Computer Engineering), PhD
Professor & Head, Dept. of Artificial Intelligence & Data Science
BRACT's Vishwakarma Institute of Information Technology, Kondhawa, Pune

Riddhi R. Mirajkar
M.E. (Computer Engineering)
Assistant Professor, Dept. of Information Technology
BRACT's Vishwakarma Institute of Information Technology, Kondhawa, Pune

Dr. Darshan V. Medhane
Ph.D. (Computer Science & Engg.)
Head of Dept. of Computer Engg.,
Maratha Vidya Prasarak Samaj's
KBT College of Engg., Nashik.

Dr. Priya M. Shelke
Associate Professor, Dept. of Information Technology
BRACT's Vishwakarma Institute of Information Technology, Kondhwa, Pune

TECH-NEO PUBLICATIONS
Where Authors Inspire Innovation
A Sachin Shah Venture

P7-95

INDEX

In Sem

End Sem

❑❑❑

Chapter 1 : Mathematical Foundation for Blockchain 1-1 to 1-36

Unit 1

CHAPTER 1

Mathematical Foundation for Blockchain

University Prescribed Syllabus

Cryptography : Symmetric Key Cryptography and Asymmetric Key Cryptography, Elliptic Curve Cryptography (ECC), Cryptographic Hash Functions: SHA256, Digital Signature Algorithm (DSA), Merkel Trees.

1.1 CRYPTOGRAPHY : SYMMETRIC KEY CRYPTOGRAPHY AND ASYMMETRIC KEY CRYPTOGRAPHY

GQ. What is Cryptography? What is the basic purpose of it?

GQ. What are different security services that are offered by Cryptography?

- The study of secure communication methods, such as encryption, that only the message's originator and intended receiver can access, is known as cryptography. The word is derived from kryptos, a "hidden" word in Greek.
- The science of creating information security in the presence of adversaries is known as cryptography. It does so on the grounds that opponents have unrestricted access to resources.
- Data is encrypted or decrypted using ciphertext such that if it is intercepted by an enemy, it is useless to them without a secret key for decryption.

- Additionally, utilising methods like microdots or merging, cryptography includes the obscuring of data in pictures. These techniques were employed by the ancient Egyptians in their complex hieroglyphics, and Roman Emperor Julius Caesar is credited with discovering them.
- The main purpose of cryptography is to offer a secrecy service. It cannot be regarded as a whole solution on its own; rather, it functions as an essential component of a larger security system to handle a security issue. For instance, several distinct cryptographic primitives, including hash functions, symmetric key cryptography, digital signatures, and public key cryptography, are needed to secure a blockchain ecosystem.
- Cryptography offers non-repudiation, integrity, and authentication (including entity and data origin authentication) in addition to confidentiality as security services. Accountability is also offered, which is something that many security systems want.

☞ Confidentiality

Confidentiality is the assurance that information is only available to authorized entities.

☞ Integrity

Integrity is the assurance that information is modifiable only by authorized entities.

☞ Authentication

- Authentication provides assurance about the identity of an entity or the validity of a message.
- There are two types of authentication mechanisms, namely entity authentication and data origin authentication.

☞ Entity authentication

- Entity authentication is the assurance that an entity is currently involved and active in a communication session.
- Traditionally, users are issued a username and password that

is used to gain access to the various platforms with which they are working.

☞ Data origin authentication

- Also known as message authentication, data origin authentication is an assurance that the source of the information is indeed verified. Data origin authentication guarantees data integrity because if a source is corroborated, then the data must not have been altered.
- Various methods, such as Message Authentication Codes (MACs) and digital signatures are most commonly used.

☞ Non-repudiation

- Non-repudiation is the assurance that an entity cannot deny a previous commitment or action by providing incontrovertible evidence. It is a security service that offers definitive proof that a particular activity has occurred.
- This property is essential in debatable situations whereby an entity has denied the actions performed, for example, placement of an order on an e-commerce system.
- This service produces cryptographic evidence in electronic transactions so that in case of disputes, it can be used as a confirmation of an action.

☞ Accountability

- Accountability is the assurance which states that actions affecting security can be traced back to the responsible party.
- This is usually provided by logging and audit mechanisms in systems where a detailed audit is required due to the nature of the business, for example, in electronic trading systems.
- Detailed logs are vital to trace an entity's actions, such as when a trade is placed in an audit record with the date and timestamp and the entity's identity is generated and saved in the log file.
- This log file can optionally be encrypted and be part of the database or a standalone ASCII text log file on a system.

1.1.1 Mathematical Concepts Required

GQ. What is a finite field? Why it is crucial for cryptography?

This part will expose you to some fundamental mathematical principles because the study of cryptography is dependent on mathematics.

☞ **Set**

A set is a grouping of unique things, such as X = {1, 2, 3, 4, 5}.

☞ **Group**

- A group is a commutative set that has a single operation that joins two of its elements. The group operation is finished, and it has a specific identification element attached to it. Each component of the set also has an inverse.
- If, for instance, elements A and B are in the set, then the resultant element after performing an operation on the elements is also in the set.
- This is referred to as closure (closed). Associative implies that the ordering of the elements has no affect on the outcome of the operation.

☞ **A finite field**

- A field with a finite set of components is said to be finite.
- These structures, also known as Galois fields, are crucial for cryptography because they can be utilised to generate precise and error-free outcomes for arithmetic operations. For instance, in Elliptic Curve Cryptography (ECC), discrete logarithm problems are created using prime finite fields.

☞ **Order**

The order indicates how many elements are in a field. It is often referred to as the field's cardinality.

☞ **An abelian group**

- If an operation on a set's elements is commutative, an abelian group is created.

- The commutative law states that the outcome of an operation, for instance, A X B = B X A, is unaffected by the arrangement of the elements.

☞ Prime fields

- A field having a prime number of elements is one that is finite. Each nonzero element in the field has an inverse, and there are precise rules for addition and multiplication.
- Operations like addition and multiplication are carried out modulo p, or prime.

☞ Ring

- An abelian group becomes a ring if more than one operation can be specified over it. There are particular requirements that must be met as well.
- Closure, associative, and distributive properties are necessary for a ring.

☞ A cyclic group

A certain kind of group known as the group generator has the ability to produce cyclic groups.

☞ Modular arithmetic

- Numbers in modular arithmetic wrap around when they reach a specific fixed number, which is also known as clock arithmetic.
- All operations are carried out with relation to this fixed number, which is a positive integer known as modulus.
- The numerals from 1 to 12 are similar to a clock. The number 1 resumes when it reaches 12.
- To put it another way, this kind of mathematics deals with the leftovers from division. For instance, 50 / 11 leaves a leftover of 6, therefore 50 mod 11 is equal to 6.

The fundamental introduction to several mathematical ideas used in cryptography is now complete. You will learn about the fundamentals of cryptography in the section that follows.

1.1.2 Generic Cryptography Model

GQ. Explain general cryptography model with suitable diagram. **(4 Marks)**

A generic cryptography model is shown in the following diagram.

It has following terms :

(1) **Entity** : Either a person or system that sends, receives, or performs operations on data

(2) **Sender** : This is an entity that transmits the data

(3) **Receiver** : This is an entity that takes delivery of the data

(4) **Adversary** : This is an entity that tries to circumvent the security service

(5) **Key** : A key is data that is used to encrypt or decrypt other data

(6) **Channel** : Channel provides a medium of communication between entities

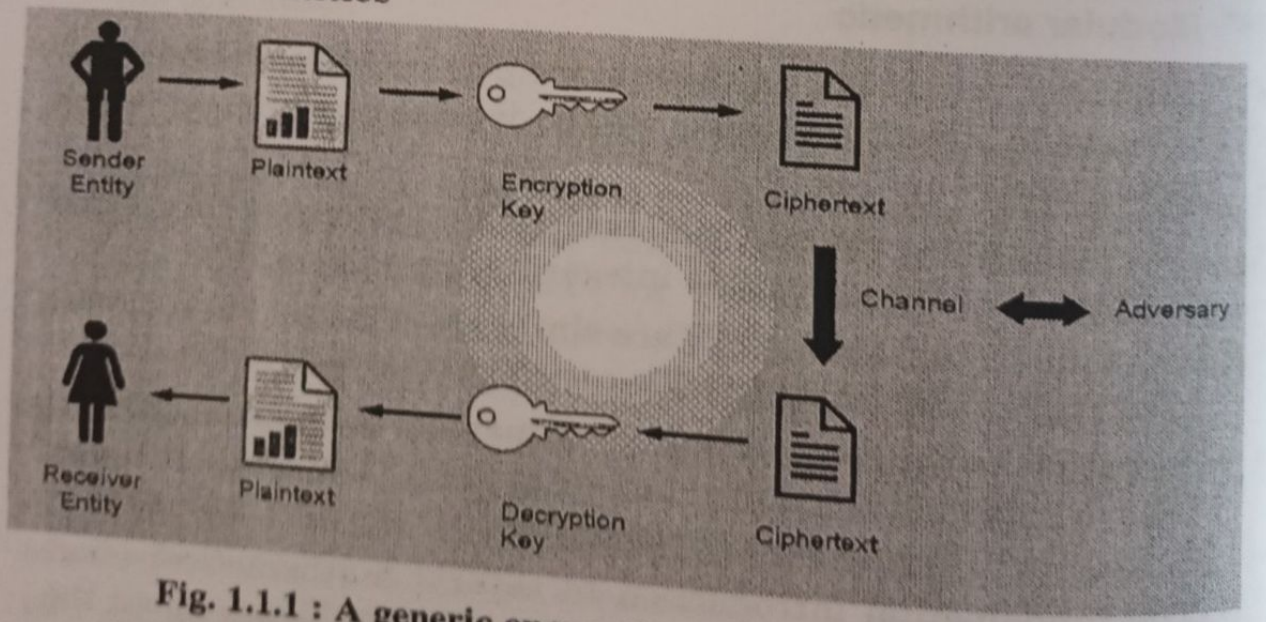


Fig. 1.1.1 : A generic encryption and decryption model

1.1.3 Cryptographic Primitives

GQ. Draw and explain the taxonomy of cryptographic primitives. **(4 Marks)**

GQ. Demonstrate symmetric key cryptography. What are pros and cons of it. **(6 Marks)**

GQ. Demonstrate asymmetric key cryptography. What are pros and cons of it. **(6 Marks)**

GQ. Compare symmetric and asymmetric key cryptography. **(4 Marks)**

GQ. Explain Stream Ciphers and block ciphers. **(4 Marks)**

- Cryptographic primitives are the basic building blocks of a security protocol or system. You will learn about cryptographic algorithms in the section that follows.
- These algorithms are crucial for creating safe protocols and systems. A security protocol is a series of actions made to use the proper security mechanisms in order to accomplish the necessary security goals.
- There are many different kinds of security protocols in use, including key management protocols, non-repudiation protocols, and authentication protocols.
- Here is an example of how the taxonomy of cryptographic primitives.

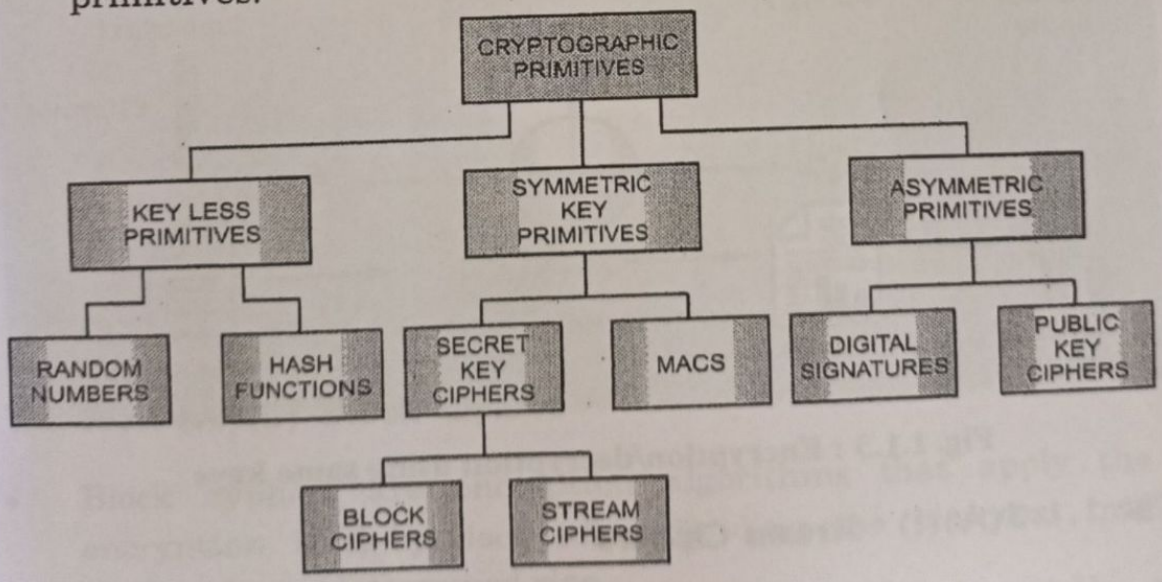


Fig. 1.1.2 : The taxonomy of cryptographic primitives

- As shown in the cryptographic primitives taxonomy diagram, cryptography is mainly divided into two categories : *symmetric cryptography* and *asymmetric cryptography*.
- These primitives are discussed further in the next section.

1.1.3(A) Symmetric Cryptography

- The term "symmetric cryptography" refers to a kind of encryption where the key used to encrypt and decrypt is the same. As a result, it is often referred to as shared key cryptography.
- The key needs to be decided upon or established before the communication parties transmit any data. Because of this, it is also known as secret key cryptography.
- Stream cyphers and block cyphers are the two categories of symmetric ciphers. Typical examples of block cyphers are Data Encryption Standard (DES) and Advanced Encryption Standard (AES), but stream ciphers like RC4 and A5 are often utilised.

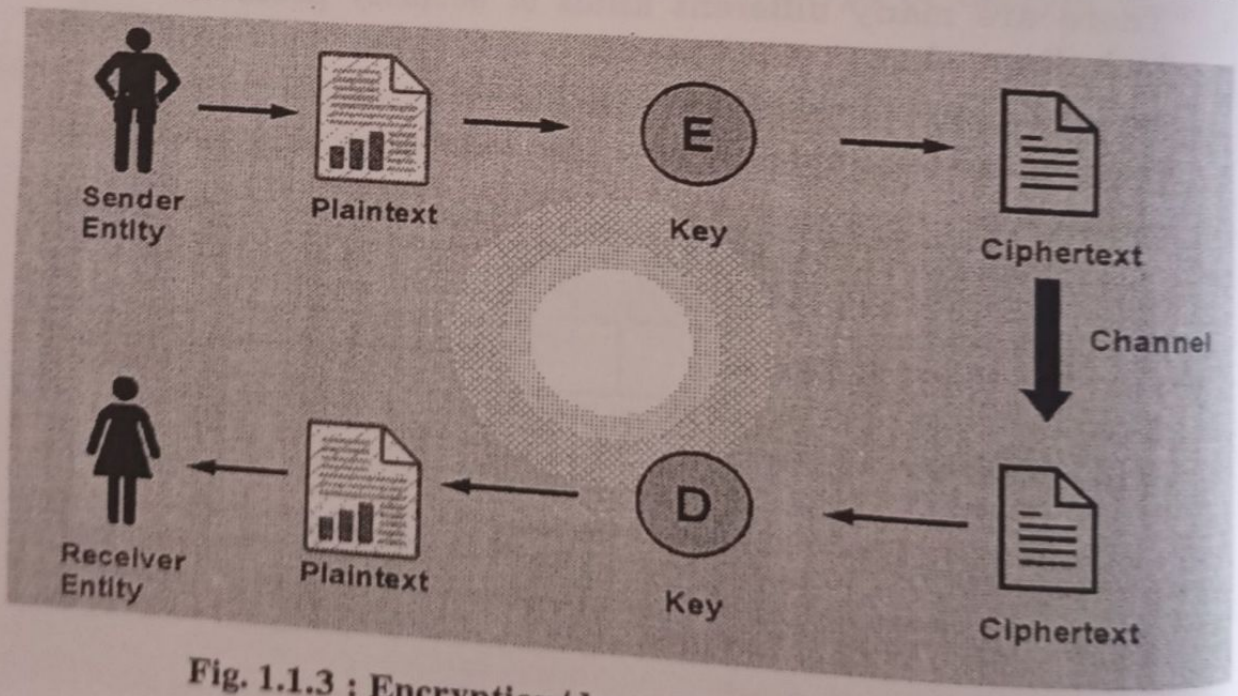


Fig. 1.1.3 : Encryption/decryption using same keys

1.1.3(A)(i) Stream Ciphers

- Using a keystream, stream ciphers encrypt plaintext by applying encryption algorithms bit-by-bit (one bit at a time) to

the data. Asynchronous and synchronous stream ciphers are the two different forms of stream ciphers.

- The keystream of a synchronised stream cipher depends exclusively on the key.
- A keystream for asynchronous stream cyphers depends on the encrypted data as well.
- Because they are just straightforward modulo-2 additions or XOR operations, encryption and decryption are the same function in stream ciphers.
- The security and unpredictability of keystreams are the essential requirements for stream ciphers. To create random numbers, a variety of methods have been devised, from hardware-implemented true random number generators to hardware-implemented pseudorandom number generators, and it is vital that all key generators be cryptographically secure.

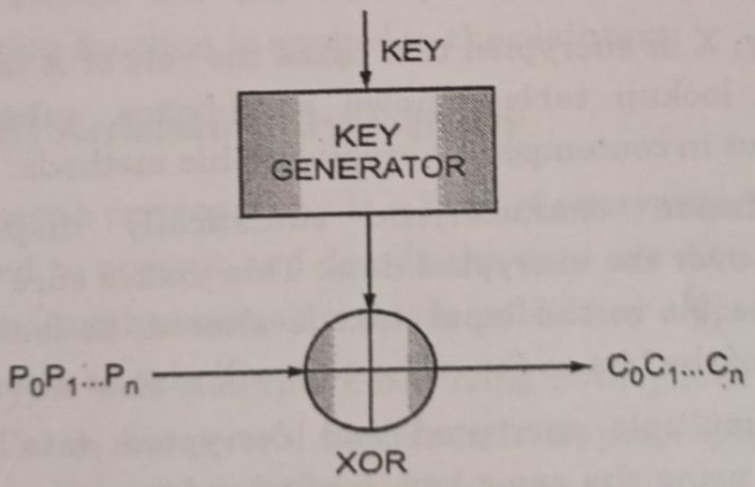


Fig. 1.1.4 : Operation of Stream ciphers

1.1.3(A)(ii) Block Ciphers

- Block cyphers are encryption algorithms that apply the encryption block-by-block after dividing the plaintext into blocks of a predetermined size.

- The design method known as a Feistel cypher is typically used to create block ciphers. A Substitution-Permutation Network, which combines substitution and permutation, has been used to create modern block cyphers like AES (Rijndael) (SPN).
- Horst Feistel created a framework called the Feistel network, on which Feistel ciphers are built.
- The foundation of this structure is the notion of combining multiple iterations of repeated operations to obtain the desirable cryptographic properties of confusion and diffusion.
- Feistel networks operate by dividing data into two blocks (left and right) and processing these blocks via keyed *round functions* in iterations to provide sufficient pseudorandom permutation.
- The relationship between the plaintext and encrypted text is complicated by confusion. Substitution is used to accomplish this.
- In reality, X in encrypted text takes the role of A in plaintext. Utilizing lookup tables known as S-boxes, substitution is carried out in contemporary cryptographic methods.
- The diffusion characteristic statistically disperses the plaintext over the encrypted data. This makes sure that, even if just one bit in the input text is altered, at least half (on average) of the bits in the ciphertext will also be altered.
- Even if multiple encrypted and decrypted data pairs are produced using the same key, confusion is necessary to make locating the encryption key highly challenging.
- In reality, this is accomplished by permutation or transposition.
- A key advantage of using a Feistel cipher is that encryption and decryption operations are almost identical and only require a reversal of the encryption process to achieve decryption. DES is a prime example of Feistel-based ciphers :

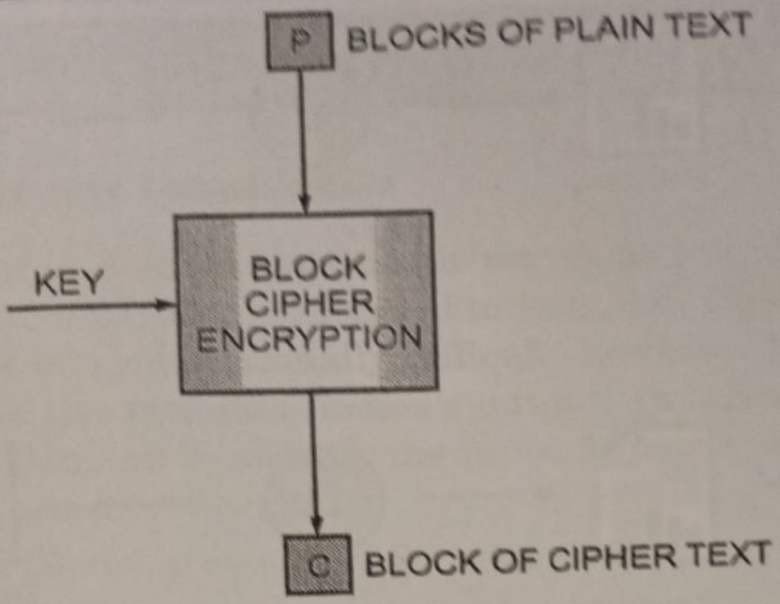


Fig. 1.1.5 : Operation of Block ciphers

- Various modes of operation for block ciphers are Electronic Code Book (ECB), Cipher Block Chaining (CBC), Output Feedback (OFB) mode, and Counter (CTR) mode.
- These modes are used to specify the way in which an encryption function is applied to the plaintext.

1.1.3(B) Asymmetric Cryptography

- Asymmetric cryptography is a kind of encryption in which the key used to encrypt and decode the data are distinct from one another. Another name for this is public key cryptography.
- It encrypts and decrypts data using both public and private keys. There are several asymmetric cryptography algorithms in use, such as RSA, DSA, and ElGammal.
- In the Fig. 1.1.6, public key cryptography is depicted in general terms :

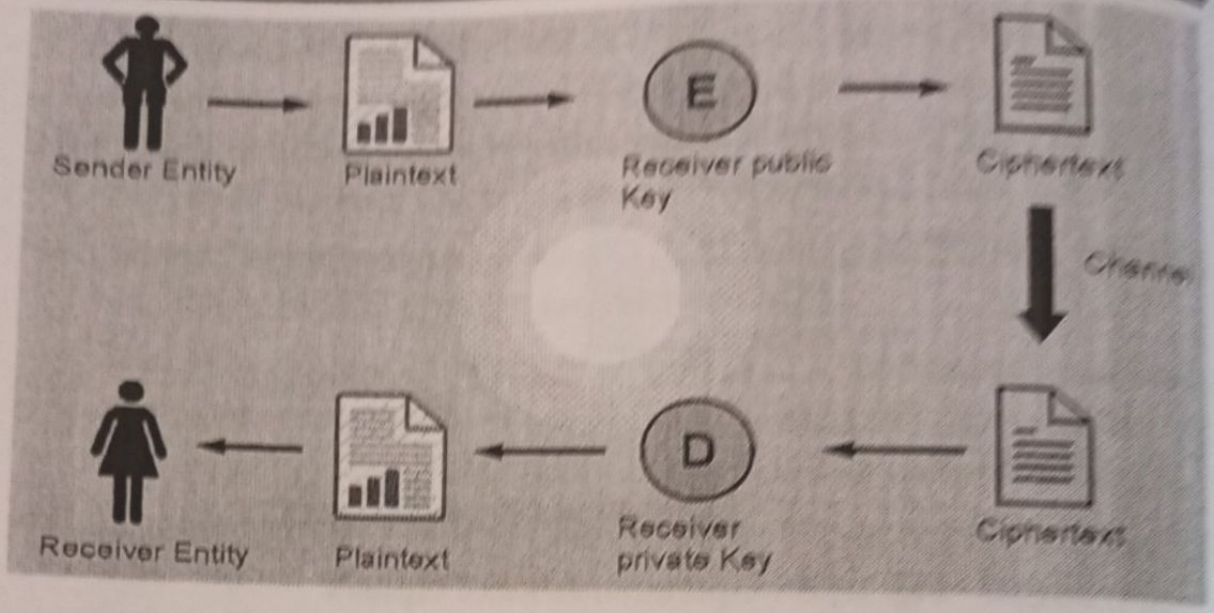


Fig. 1.1.6 : Encryption/decryption using public/private keys

- The Fig. 1.1.6 shows how a sender can encrypt plaintext using the recipient's public key and encryption function E to create ciphertext, which is subsequently sent over the network to the recipient.
- If the data is fed into function D, which produces plaintext, it may be decrypted using the receiver's private key once it reaches the recipient.
- In this approach, unlike symmetric encryption, where keys must be shared in order to accomplish encryption and decryption, the private key stays on the side of the receiver.
- Public key cryptosystems provide key setup, digital signatures, identity, identification, encryption, and decryption. Public key algorithms are slower in terms of computation than symmetric key algorithms.
- Therefore, they are not commonly used in the encryption of large files or the actual data that requires encryption. They are usually used to exchange keys for symmetric algorithm.
- Once the keys are established securely, symmetric key algorithms can be used to encrypt the data.

1.2 ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

1.2.1 Discrete Logarithm

- A problem in modular arithmetic serves as the foundation for a discrete logarithm system. Finding the exponent of the generator is computationally difficult, however it is simple to determine the modulo function's output. In other words, it is quite challenging to identify the input from the output. It only works in one direction.
- Take the following equation, for instance:

$$3^2 \bmod 10 = 9$$

- Now, it is quite difficult to identify the exponent of the generator 3 in the prior question, which is the outcome of the preceding equation finding 2 given 9.
- The Diffie-Hellman key exchange and digital signature algorithms both employ this challenging problem.

1.2.2 Elliptic curves

GQ. Write a short note on elliptic curve. **(4 Marks)**

- The collection of points that fulfil a specific mathematical equation is known as an elliptic curve. Because the curve is non-singular, it lacks cusps and self-intersections. It includes the two variables a and b as well as the infinite point. An elliptic curve's equation seems kind of like this :

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

- In this case, the numbers a and b's values are components of the field that the elliptic curve is defined on. Over real numbers, rational numbers, complex numbers, or finite fields, elliptic curves can be defined.
- An elliptic curve over prime finite fields is used in place of real numbers for cryptography reasons. The prime should also be bigger than 3. a and/or b's values can be changed to produce various curves.
- The most prominently used cryptosystems based on elliptic

curves are the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Elliptic Curve Diffie-Hellman (ECDH) key exchange.

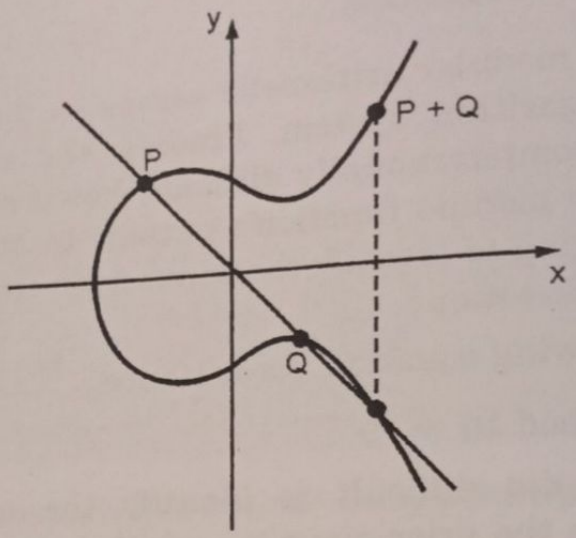


Fig. 1.2.1 : Elliptic curve

- There are other representations of elliptic curves, but technically an elliptic curve is the set points satisfying an equation in two variables with degree two in one of the variables and three in the other.
- An elliptic curve is not just a pretty picture, it also has some properties that make it a good setting for cryptography.

1.3 PUBLIC AND PRIVATE KEYS

GQ. Explore the concept of public and private keys. **(4 Marks)**

- To understand public key cryptography, the key concept that needs to be explored is the concept of public and private keys.
- As the name implies, a private key is a number that has been produced randomly and is retained secretly and privately by its users. Since this is the key used to decode communications, private keys must be kept secure and no unauthorized access should be permitted; otherwise, the entire concept of public key cryptography is put in jeopardy.
- Depending on the kind and class of algorithms being used, private keys might have different lengths.

- For instance, RSA commonly uses keys of 1024 or 2048 bits.
- A minimum key size of 2048 bits is advised rather than the outdated 1024-bit key size, which is no longer regarded as safe.
- The owner of the private key publishes and makes a public key publicly accessible.
- The message can then be encrypted with the published public key and sent to the owner of the private key by anybody who wants to send the publisher of the public key an encrypted message.
- Because the accompanying private key is securely held by the intended receiver, no one else can decrypt the communication.
- The recipient can use the private key to decrypt the communication after receiving it once it has been public key encrypted. However, there are certain issues with public keys.
- These include the veracity of the public keys and the identification of their publisher.
- In the following section, we will introduce two examples of asymmetric key cryptography: RSA and ECC. RSA is the first implementation of public key cryptography whereas ECC is used extensively in blockchain technology.

1.4 RSA

GQ. RSA is not the best cryptographic method for the near future. Why ? **(4 Marks)**

GQ. Describe the steps to generate public and private keys in RSA. **(4 Marks)**

GQ. How encryption and decryption is carried out in RSA? **(4 Marks)**

- RSA was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adelman, hence the name Rivest–Shamir-Adleman (RSA).
- This type of public key cryptography is based on the integer factorization problem, where the multiplication of two large prime numbers is easy, but it is difficult to factor it (the result of multiplication, product) back to the two original numbers.

The crux of the work involved with the RSA algorithm is during the key generation process. An RSA key pair is generated by performing the following steps :

▶ **(1) Modulus generation**

- Select **p** and **q**, which are very large prime numbers
- Multiply **p** and **q**, $n = p \cdot q$ to generate modulus **n**

▶ **(2) Generate co-prime**

- Assume a number called **e**.
- **e** should satisfy a certain condition; that is, it should be greater than 1 and less than **(p-1) (q-1)**. In other words, **e** must be a number such that no number other than **1** can divide **e** and **(p-1) (q-1)**. This is called co-prime, that is, **e** is the co-prime of **(p-1) (q-1)**.

▶ **(3) Generate the public key**

- The modulus generated in step 1 and co-prime **e** generated in step 2 is a pair together that is a public key.
- This part is the public part that can be shared with anyone; however, **p** and **q** need to be kept secret.

▶ **(4) Generate the private key**

- The private key, called **d** here, is calculated from **p, q**, and e. The private key is basically the inverse of **e *modulo*** **(p-1)** (q-1). In the equation form, it is this as follows:

$$ed = 1 \bmod (p-1)(q-1)$$

- Usually, the extended Euclidean algorithm is used to calculate **d.** This algorithm takes **p, q,** and **e** and calculates **d**.
- The key idea in this scheme is that anyone who knows **p** and q can easily calculate private key **d** by applying the extended Euclidean algorithm.
- However, someone who does not know the value of **p** and q cannot generate **d.** This also implies that **p** and **q** should be large enough for the modulus **n** to become extremely difficult (computationally impractical) to factor.

1.4.1 Encryption and Decryption using RSA

- RSA uses the following equation to produce ciphertext :

$$C = P^e \bmod n$$

- This means that plaintext P is raised to e number of times and then reduced to modulo n. Decryption in RSA is provided in the following equation:

$$P = C^d \bmod n$$

- This means that the receiver who has a public key pair (n, e) can decipher the data by raising C to the value of the private key d and reducing to modulo n.
- As the size of the numbers being factored increases, these algorithms become more effective. As the quantity (i.e., the key's bit length) grows greater, the difference in complexity between multiplying large numbers and factoring large numbers is less.
- The size of the keys must expand even more quickly as the amount of computing power available to decipher numbers rises. For portable, low-power devices with constrained processing capability, this is an unsustainable position. Factoring and multiplication are separated by an insurmountable distance.
- All of this simply indicates that RSA is not the best cryptographic method for the near future.
- In an ideal Trapdoor Function, the easy way and the hard way get harder at the same rate with respect to the size of the numbers in question.

1.5 ELLIPTIC CURVE CRYPTOGRAPHY

GQ. Write a short note on Elliptic Curve Cryptography. **(4 Marks)**

GQ. What are the advantages of ECC over other public key algorithms? **(2 Marks)**

GQ. Explain the concept of point addition in ECC. **(4 Marks)**

GQ. Explain the concept of point doubling in ECC. **(4 Marks)**

GQ. How to determine public and private key in ECC? **(4 Marks)**

- After the introduction of RSA and Diffie-Hellman, researchers explored other mathematics-based cryptographic solutions looking for other algorithms beyond factoring that would serve as good Trapdoor Functions.
- In 1985, cryptographic algorithms were proposed based on an esoteric branch of mathematics called elliptic curves.
- Elliptic Curve Cryptography (ECC) is based on the discrete logarithm problem founded upon elliptic curves over finite fields (Galois fields).
- ECC has the advantage of requiring a smaller key size while yet offering the same level of security as, say, RSA, as compared to other public key algorithms. ECDSA for digital signatures and ECDH for key exchange are two well-known ECC-derived protocols.
- ECC implements encryption, signatures, and key exchange, which are the three main asymmetric cryptosystem features.
- Although ECC may be used for encryption, it is not frequently done in reality. Instead, it's frequently utilised for key exchange and digital signatures.
- As ECC needs less space to operate, it is becoming very popular on embedded platforms and in systems where storage resources are limited. By comparison, the same level of security can be achieved with ECC only using 256-bit operands as compared to 3072-bits in RSA.
- The following table shows that ECC is able to provide the same level of cryptographic strength as an RSA based system with smaller key sizes :

Table 1.5.1

RSA key sizes (bits)	Elliptic curve key sizes (bits)
1024	160
2048	224
3072	256
7680	384
15360	521

- The ECC uses integer private keys that fall inside the field size range of the curve, which is generally 256 bits.
- The following is an example of a 256-bit ECC private key in hexadecimal format :

  0x51897b64e85c3f714bba707e867914295a1377a7463a9dae8ea6a8b914246319.
- ECC cryptography is incredibly quick since the key creation is as easy as safely producing a random integer within a given range. An ECC private key that falls inside the range is valid.
- The public keys in the ECC are what are known as EC points, which are pairs of x, y-coordinates. EC points may be reduced to only one coordinate plus one bit because of their unique characteristics (odd or even).
- Thus the **compressed public key**, corresponding to a 256-bit ECC private key, is a **257-bit** integer.
- Example of ECC public key (corresponding to the above private key, encoded in the Ethereum format, as hex with prefix 02 or 03) is :

  0x02f54ba86dc1ccb5bed0224d23f01ed87e4a443c47fc690d7797a13d41d2340e1a.
- In this format the public key actually takes 33 bytes (66 hex digits), which can be optimized to exactly 257 bits.
- Different underlying elliptic curves can be used with ECC cryptographic algorithms. Different curves offer various levels of security (cryptographic strength), performance (speed), and key length, as well as perhaps using various methods.
- In addition to having a name (named curves, for example secp256k1 or Curve25519), a field size (which defines the key length, for example 256 bits), security strength (typically the field size / 2 or less), performance (operations/sec), and many other parameters, ECC curves are widely used in cryptographic libraries and security standards.
- The length of ECC keys is closely related to the underlying curve. The default key length for the ECC private keys in the majority of programmes (including OpenSSL, OpenSSH, and Bitcoin) is 256 bits, however many alternative ECC key sizes are feasible depending on the curve: 233-bit (curve sect233k1), 192-bit (curve secp192r1), and many more.

- Elliptic-curve cryptography (ECC) provides several groups of algorithms, based on the math of the elliptic curves over finite fields :
  (1) ECC digital signature algorithms like ECDSA (for classical curves) and EdDSA (for twisted Edwards curves).
  (2) ECC encryption algorithms and hybrid encryption schemes like the ECIES integrated encryption scheme and EEECC (EC-based ElGamal).
  (3) ECC key agreement algorithms like ECDH, X25519 and FHMQV.
- All these algorithms use a curve behind (like secp256k1, curve25519 or p521) for the calculations and rely of the difficulty of the ECDLP (elliptic curve discrete logarithm problem).
- All these algorithms use public / private key pairs, where the private key is an integer and the public key is a point on the elliptic curve (EC point).

1.5.1 Mathematics Behind ECC

GQ. Explain the concept of point addition in ECC. **(4 Marks)**
GQ. Explain the concept of point doubling in ECC. **(4 Marks)**
GQ. How to determine public and private key in ECC? **(4 Marks)**

- A fundamental introduction to the underlying mathematics is required in order to understand ECC. An elliptic curve is basically a type of polynomial equation known as the Weierstrass equation, which generates a curve over a finite field.
- The field where all arithmetic operations are carried out modulo a prime p is the most often used field. Elliptic curve groups are made up of curve points over a finite field.
- An elliptic curve is defined in the following equation:

$$y^2 = x^3 + Ax + B \bmod P$$

- Here, A and B belong to a finite field Zp or Fp (prime finite field) along with a special value called the point of infinity. The point of infinity (∞) is used to provide identity operations for points on the curve.
- Furthermore, a condition also needs to be met that ensures that the equation mentioned earlier has no repeated roots. This means that the curve is non-singular.
- The condition is described in the following equation, which is a standard requirement that needs to be met. More precisely, this ensures that the curve is non-singular:

$$4a^3 = 27b^2 \neq 0 \bmod P$$

- To construct the discrete logarithm problem based on elliptic curves, a large enough cyclic group is required.
- First, the group elements are identified as a set of points that satisfy the previous equation. After this, group operations need to be defined on these points.
- Group operations on elliptic curves are point addition and point doubling. Point addition is a process where two different points are added, and point doubling means that the same point is added to itself.

(A) Point addition

- Point addition is shown in the following diagram. This is a geometric representation of point addition on elliptic curves.
- In this method, a diagonal line is drawn through the curve that intersects the curve at two points P and Q, as shown in the diagram, which yields a third point between the curve and the line.
- This point is mirrored as P+Q, which represents the result of the addition as R.
- This is shown as P+Q in the following diagram:

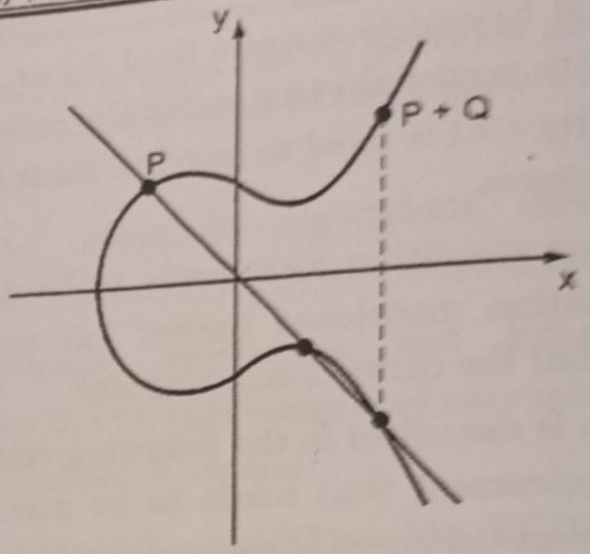


Fig. 1.5.1

- The group operation denoted by the + sign for addition yields the following equation:

$$P + Q = R$$

- In this case, two points are added to compute the coordinates of the third point on the curve:

$$P + Q = R$$

- More precisely, this means that coordinates are added, as shown in the following equation:

$$(x1, y1) + (x2, y2) = (x3, y3)$$

- The equation of point addition is as follows:

$$x3 = s2 - x1 - x2 \bmod p$$

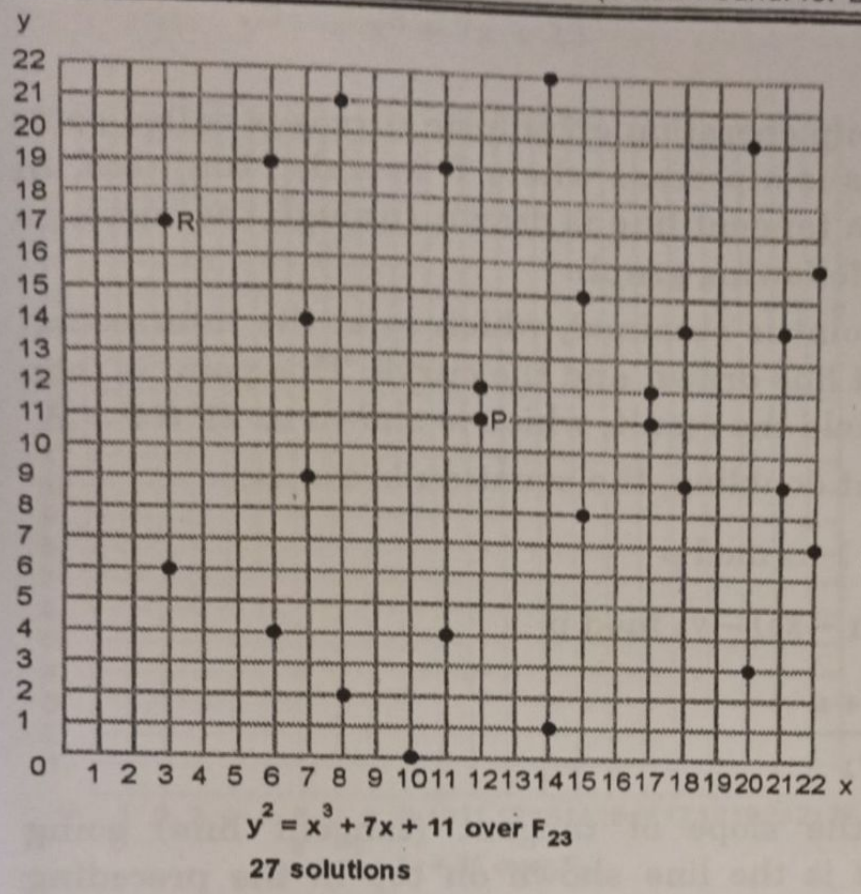
$$y3 = s\,(x1 - x3) - y1 \bmod p$$

- Here, we see the result of the preceding equation:

$$S = ((y2-y1)/(x2-x1)) \bmod p$$

S in the preceding equation depicts the line going through P and Q.

- An example of point addition is shown in the following diagram. It was produced using Certicom's online calculator. This example shows the addition and solutions for the equation over finite field F_{23}.



P (12, 11)
R (3, 17)

$l = (3x_P^2 + a) * (2y_P)^{-1} \bmod P$
$= 439 * 22^{-1} \bmod 23$
$= 2 * 22 \bmod 23$
$= 21$

$x_R = l^2 - 2x_P \bmod P$
$= 441 - 24 \bmod 23$
$= 3$

$y_R = -y_P + l * (x_P - x_R) \bmod P$
$= -11 + 21 * (12 - 3) \bmod 23$
$= 12 + 21 * 9 \bmod 23$
$= 12 + 5 \bmod 23$
$= 17$

2P = R = (3, 17).

Fig. 1.5.2 : Example of point addition

- In the preceding example, the graph on the left side shows the points that satisfy this equation:
- There are 27 solutions to the equation shown earlier over finite field *F23*. *P* and *Q* are chosen to be added to produce point *R*. Calculations are shown on the right side, which calculates the third point *R*. Note that here, *l* is used to depict the line going through *P* and *Q*.
- As an example, to show how the equation is satisfied by the points shown in the graph, a point (x, y) is picked up where $x = 3$ and $y = 6$.
- Using these values shows that the equation is indeed satisfied:

$$y^2 \bmod 23 = x^3 + 7x + 11 \bmod 23$$
$$6^2 \bmod 23 = 3^3 + 7(3) + 11 \bmod 23$$
$$36 \bmod 23 = 59 \bmod 23$$
$$13 = 13$$

(B) Point doubling

- The other group operation on elliptic curves is called point doubling. This is a process where P is added ton itself. In this method, a tangent line is drawn through the curve, as shown in the following graph.
- The second point is obtained, which is at the intersection of the tangent line drawn and the curve. This point is then mirrored to yield the result, which is shown as 2P = P + P.

- In the case of point doubling, the equation becomes:

$$X_3 = s^2 - \times 1 - x_2 \bmod p$$

$$y_3 = S(x_1 - x_3) - y_1 \bmod p$$

$$S = \frac{3x_1^2 + a}{2y_1}$$

- Here, S is the slope of tangent (tangent line) going through P. It is the line shown on top in the preceding diagram. In the preceding example, the curve is plotted over real numbers as a simple example, and no solution to the equation is shown.

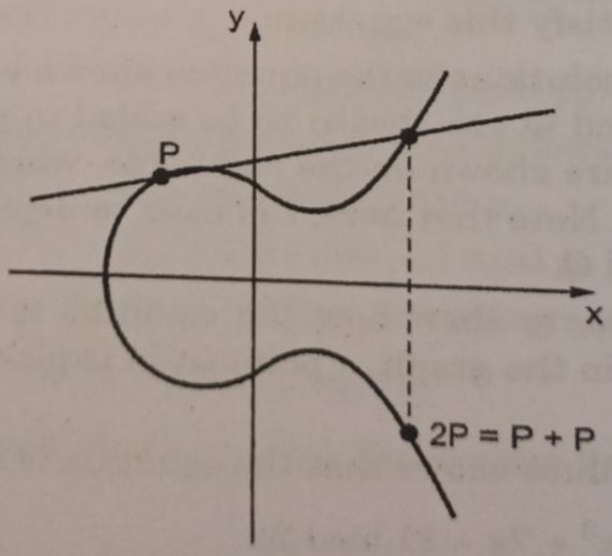


Fig. 1.5.3

- The following example shows the solutions and point doubling of elliptic curves over finite field F23. The graph on the left side shows the points that satisfy the equation:

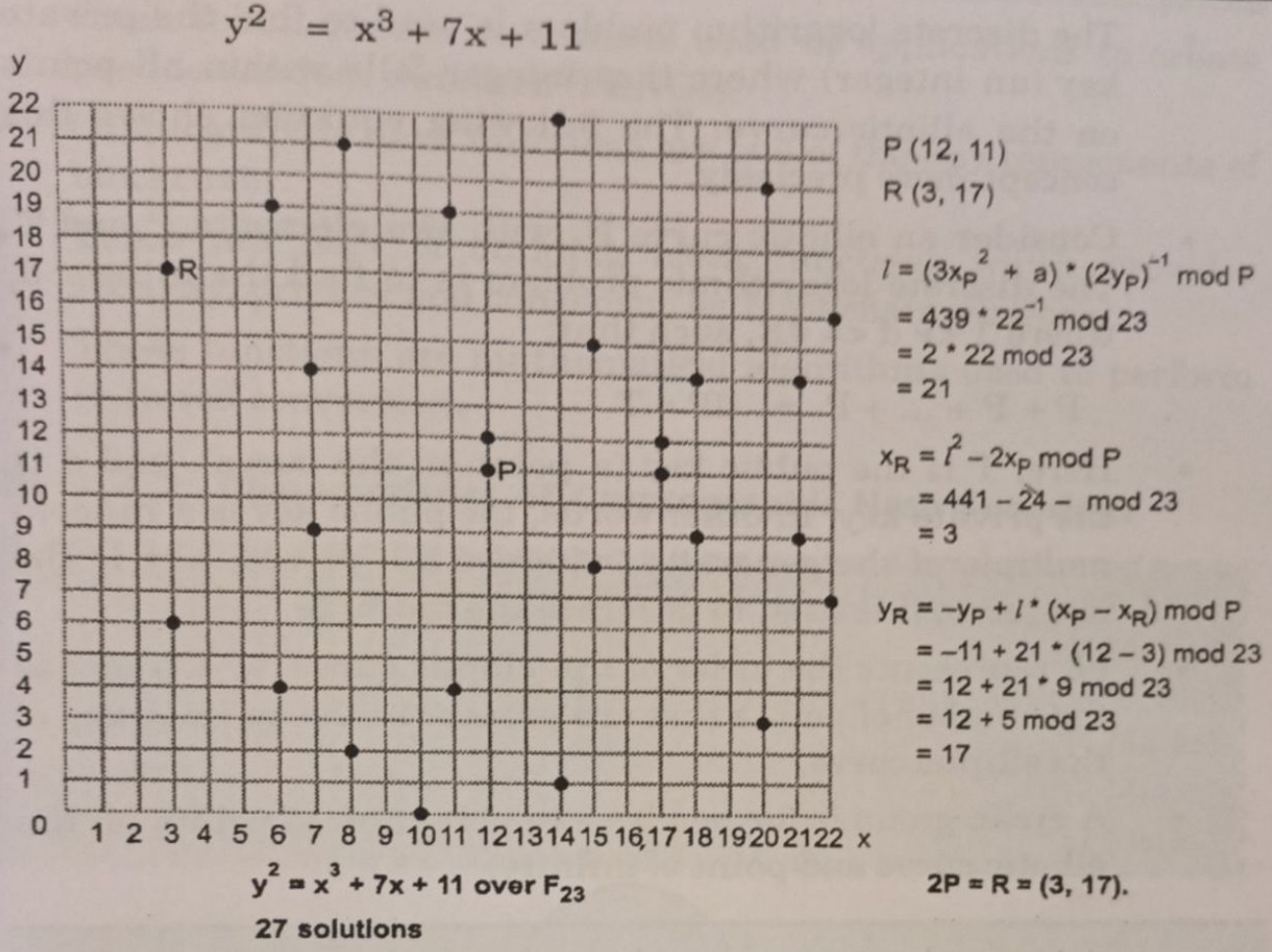


Fig. 1.5.4

- As shown on the right side in the preceding graph, the calculation that finds the *R* after *P* is added into itself (point doubling).
- There is no *Q* as shown here, and the same point *P* is used for doubling. Note that in the calculation, *l* is used to depict the tangent line going through *P*.

(C) Discrete logarithm problem in ECC

- The discrete logarithm problem in ECC is based on the idea that, under certain conditions, all points on an elliptic curve form a cyclic group.
- On an elliptic curve, the public key is a random multiple of the generator point, whereas the private key is a randomly chosen integer used to generate the multiple.
- In other words, a private key is a randomly selected integer, whereas the public key is a point on the curve.

- The discrete logarithm problem is used to find the private key (an integer) where that integer falls within all points on the elliptic curve. The following equation shows this concept more precisely.
- Consider an elliptic curve E, with two elements P and T. The discrete logarithmic problem is to find the integer d, where 1 <= d <= #E, such that:

$$P + P + \ldots + P = dP = T$$

- Here, T is the public key (a point on the curve), and d is the private key. In other words, the public key is a random multiple of the generator, whereas the private key is the integer that is used to generate the multiple.
- #E represents the order of the elliptic curve, which means the number of points that are present in the cyclic group of the elliptic curve.
- A cyclic group is formed by a combination of points on the elliptic curve and point of infinity.

1.6 CRYPTOGRAPHIC HASH FUNCTIONS : SHA256

1.6.1 Hash Functions

GQ. State and explain hash function? **(2 Marks)**

- Hash functions are used to convert infinitely lengthy input texts into digests of a fixed length. Hash functions offer the data integrity service and are keyless. Dedicated and iterated hash function creation strategies are often used to create them.
- There are several different families of hash functions, including MD, SHA-1, SHA-2, SHA-3, RIPEMD, and Whirlpool. Digital signatures and Message Authentication Codes (MACs), like HMACs, frequently employ hash functions.
- Additionally, hash functions are frequently utilised to offer data integrity services. These may be used to create additional cryptographic primitives like MACs and digital signatures as well as one-way functions.

- Hash functions are sometimes used in applications to create pseudo-random numbers (PRNGs).
- Cryptographic hash functions are one of the key components of blockchain.
- These are part of building block functions which provides security, privacy and consensus on blockchain platform.
- These functions are mathematical algorithms used to perform required conversion.

1.6.2 Characteristics of Cryptographic Hash Functions

GQ. Enlist the features of cryptographic hash functions? Explain any two. **(4 Marks)**

GQ. Demonstrate pre image and second pre image resistance with example. **(4 Marks)**

GQ. What is collision in hash? **(2 Marks)**

GQ. Explain Avalanche effect of hash functions. **(2 Marks)**

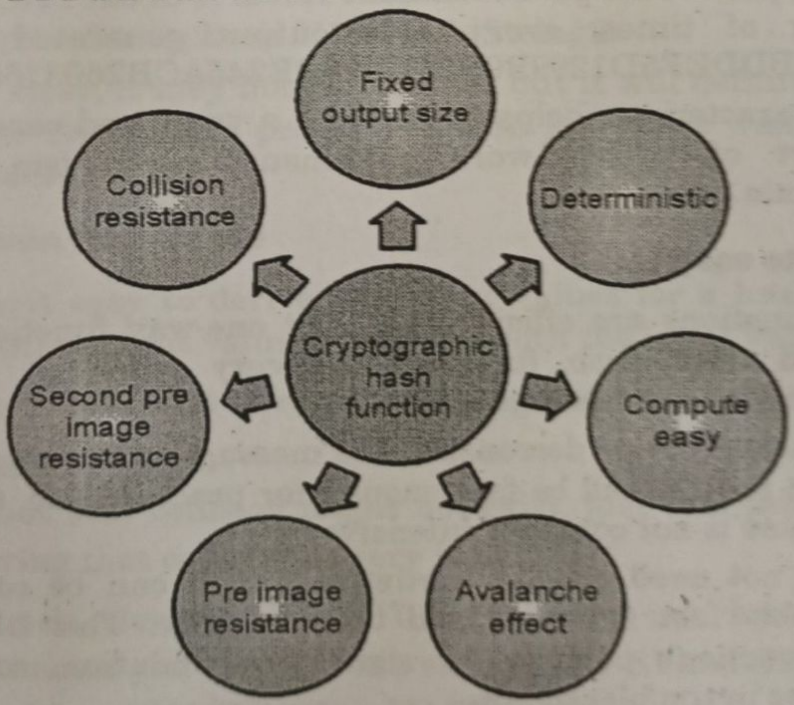


Fig. 1.6.1 : Characteristics of Cryptographic Hash Functions

Fixed output size

- Usually, if the size of input changes then size of output

changes. E.g Compression

- However, in case of cryptographic has functions, output string size remains same irrespective of input string size.

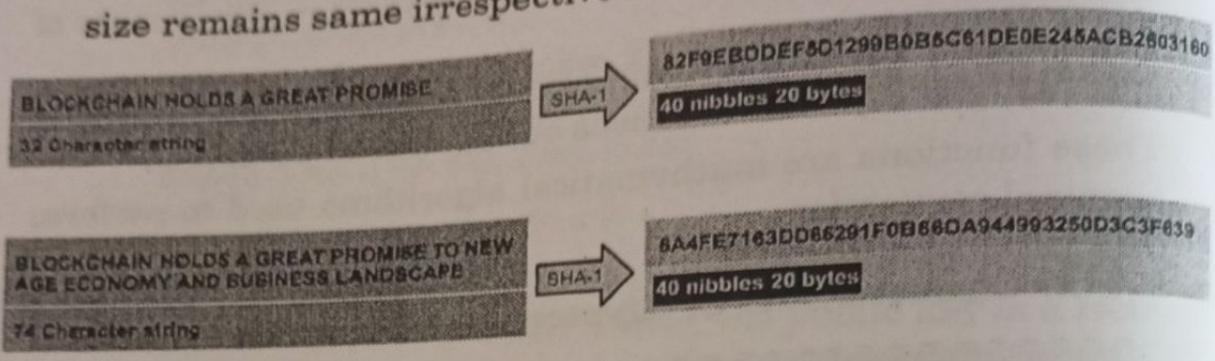


Fig. 1.6.2

☞ Deterministic

- If the input is same, the output will always be same.
- If the function is applied on the same input any number of times, the resultant answer will always be same.
- If we apply SHA-1 on "Blockchain Holds A Great Promise" any number of times, every time output generated will be "82F9EBDDEF5D1299B0B5C61DE0E245ACB2603160".
- This characteristic helps them to be a very good candidate to be part of proof-of-work consensus mechanism in the blockchain.

☞ Compute easy

- Hash functions are efficient and fast one-way functions. It is required that hash functions be very quick to compute regardless of the message size.
- The efficiency may decrease if the message is too big, but the function should still be fast enough for practical use. Creating hash value is not compute intensive.
- It does not need special hardware and it can be completed reasonably fast and not hold the end user. This has made these functions popular for signature validation, consensus scenarios in the blockchain.

☞ Pre-image resistance

- It is not computationally easy to derive input for a given output.

Say, H1 = hash(string 1)

- If H1 is given, it is not computationally easy or practical to find string1.
- It is possible but just not easy.
- The stronger the algorithm, the more computation it may require and it may have better pre-image resistance.
- Next, even if two characteristics are similar to pre image resistance, they are not the same.
- It is not easy to find source based on data, making these a kind of one way function. This is also called a one-way property.

☞ Second pre-image resistance

- It is possible to find another input that can give the same hash value as a given input.

Let's take String1 and H1 = hash (String1).

- It is not easy to find another string (String2) such that String1! = String2 and H1 = hash(String2).
- To be clear, it may not be possible, but it will definitely not be easy to do so. This property is also known as weak collision resistance.

☞ Collision Resistance

- It is not easy to derive two input values for a hash function such that output value is same for both the input values.
- If two input maps to same output, then the function is said to have collision.
- It is not that collision might not exist, just that probability of occurring that collision is very less.
- So, hash algorithm,HASH1 is said to not have collision resistance if you can find two strings, say S1 and S2, such that S1 ! = S2 and HASH1(S1) = HASH1(S2).
- It is different than second pre-image resistance as here only hash function is given while input strings can be anything.

☞ **Avalanche Effect**

A small change in input causes a large change in output.

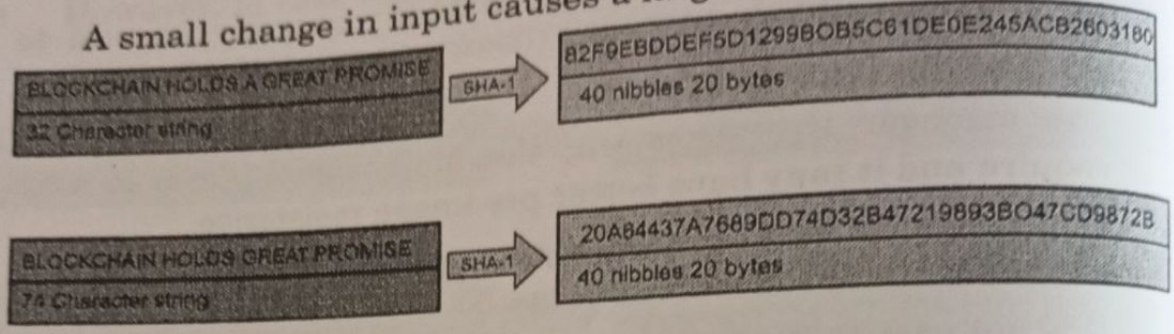


Fig. 1.6.3

1.7 SECURE HASH ALGORITHMS

The following list describes the most common **Secure Hash Algorithms** (**SHAs**) :

- **SHA-0** : This is a 160-bit function introduced by NIST in 1993.
- **SHA-1** : SHA-1 was introduced in 1995 by NIST as a replacement for SHA-0. This is also a 160-bit hash function. SHA-1 is used commonly in SSL and TLS implementations. It should be noted that SHA-1 is now considered insecure, and it is being deprecated by certificate authorities. Its usage is discouraged in any new implementations.
- **SHA-2** : This category includes four functions defined by the number of bits of the hash: SHA-224, SHA-256, SHA-384, and SHA-512.
- **SHA-3** : This is the latest family of SHA functions. SHA-3-224, SHA-3-256, SHA-3-384, and SHA-3-512 are members of this family. SHA-3 is a NIST-standardized version of Keccak. Keccak uses a new approach called **sponge construction** instead of the commonly used Merkle-Damgard transformation.
- **RIPEMD** : RIPEMD is the acronym for **RACE Integrity Primitives Evaluation Message Digest**. It is based on the design ideas used to build MD4. There are multiple versions of RIPEMD, including 128-bit, 160-bit, 256-bit, and 320-bit.
- **Whirlpool** : This is based on the W Rijndael cipher, a modified

variation of the Rijndael encryption. It makes use of the one-way function known as the Miyaguchi-Preneel compression function, which compresses two fixed-length inputs into a single fixed-length output. It does a single block length compression.

- Numerous real-world uses exist for hash functions, from straightforward file integrity checks and password storage to inclusion in cryptographic protocols and algorithms.
- They are utilised in several applications, including peer-to-peer file sharing, virus fingerprinting, distributed hash tables, bloom filters, and hash tables.
- Hash operations are essential to blockchain. In order to confirm the amount of computing work used by miners, the PoW algorithm employs SHA-256 twice. RIPEMD 160 is used to produce Bitcoin addresses.

1.8 DESIGN OF SHA-256

GQ. Explain the working of SHA-256 algorithm. **(4 Marks)**

- SHA-256 has the input message size < 264-bits. Block size is 512-bits, and it has a word size of 32-bits. The output is a 256-bit digest.
- The compression function processes a 512-bit message block and a 256-bit intermediate hash value. There are two main components of this function: the compression function and a message schedule.
- The algorithm works as follows, in eight steps :

Pre-processing

(1) If a block's length is less than the requisite 512 bits, padding of the message is used to increase it to 512 bits.

(2) Parsing the message into blocks of 512 bits, which separates the message and any padding into equal blocks.

(3) Creating the initial hash value, which is made up of the first 32 bits of the fractional portions of the square roots of the first

eight prime integers. The first hash value is composed of eight 32-bit words. These initial parameters are picked at random to start the procedure off, and they give some amount of assurance that the method has no backdoors.

☞ Hash computation

(1) Following that, each message block is analysed one at a time and it takes 64 rounds to compute the whole hash result. To ensure that no two rounds are same, each round uses slightly different constants.

(2) The message schedule has been set.

(3) Eight operational variables are initialised.

(4) A calculation is made for the intermediate hash value.

(5) After the message has been processed, the output hash is generated:

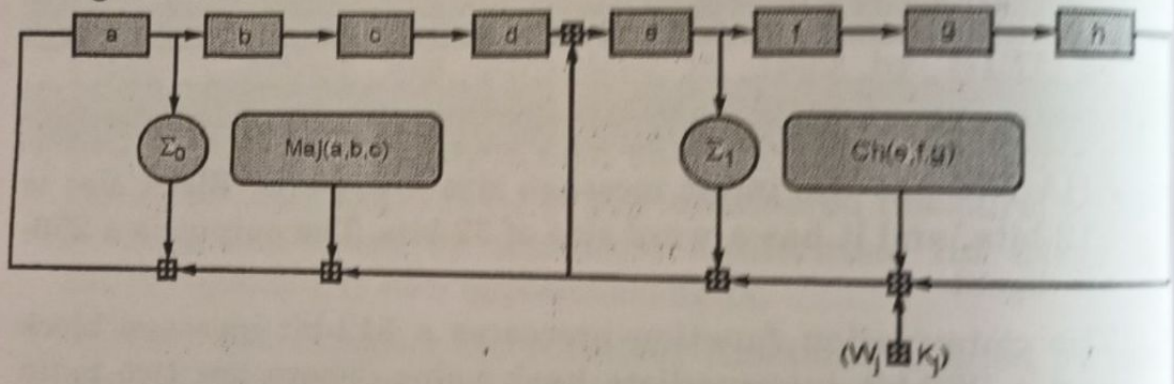


Fig. 1.8.1 : One round of SHA-256 compression function

- In the preceding diagram, a, b, c, d, e, f, g, and h are the registers. Maj and Ch are applied bitwise. Σ0 and Σ1 performs bitwise rotation. Round constants are Wj and Kj, which are added, mod 232.

⏭ 1.9 DIGITAL SIGNATURES

GQ. How the digital signing and verification is carried out with RSA digital signature algorithm? **(6 Marks)**

GQ. Explain the two approaches to using digital signatures with encryption. **(2 Marks)**

- With the use of digital signatures, it is possible to link a communication to the source of its creation. Non-repudiation and data origin authentication are provided via digital signatures.
- Blockchain technology makes use of digital signatures, with senders utilising their private key to sign transactions before publishing them to the network.
- This digital signature demonstrates that they are the legal owners of the item, like bitcoins. To confirm that the money truly belong to the node (user) that claims to be the owner, these transactions are once again validated by other nodes on the network.
- Two processes are used to calculate digital signatures. The high-level phases of an RSA digital signature method are shown in an example below.

☞ Digital signature algorithm using RSA

The RSA digital signature algorithm is as follows :

(1) **Determine the data packet's hash value :** This will ensure data integrity since the hash can be recalculated at the receiver's end and compared with the original hash to determine whether the data has been altered during transit. Although message signing technically is possible without first hashing the contents, this method is not thought to be safe.

(2) **Uses the signer's private key to tamper-proof the hash value :** The legitimacy of the signature and the signed material is guaranteed since only the signer has access to the private key.

- Important characteristics of digital signatures are authenticity, invulnerability, and nonreusability.
- Authenticity refers to the ability of a receiving party to confirm the validity of digital signatures. The unforgeability attribute makes sure that only the message's sender may use the private key signing feature. To put it another way, only the genuine sender can create a signed message.

- The concept of nonreusability states that a digital signature cannot be taken out of one communication and applied to another.
- The following diagram illustrates how a generic digital signature function works :

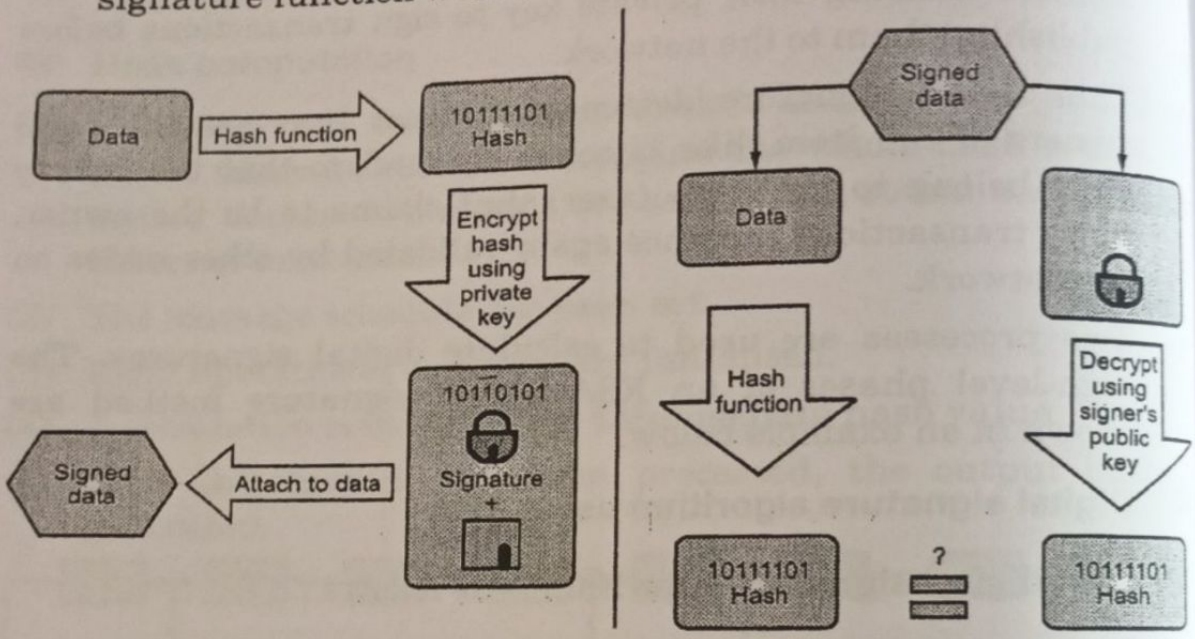


Fig. 1.9.1 : Digital signing (left) and verification process (right) (Example of RSA digital signatures)

- If a sender wants to send an authenticated message to a receiver, there are two methods that can be used: sign then encrypt and encrypt then sign.

These two approaches to using digital signatures with encryption are as follows.

Sign then encrypt

- With this approach, the sender digitally signs the data using the private key, appends the signature to the data, and then encrypts the data and the digital signature using the receiver's public key.
- This is considered a more secure scheme as compared to the *encrypt then sign* scheme .

Encrypt then sign

- With this method, the sender encrypts the data using the receiver's public key and then digitally signs the encrypted data.

1.10 MERKEL TREES

GQ. What are Merkle trees ? Explain the structure of a Merkle tree. **(4 Marks)**

- A Merkle tree, named after its creator Ralph Merkle, is a binary tree containing hash pointers. The Merkle tree, commonly referred to as the hash tree, is a kind of data structure used for data synchronisation and verification.
- Each non-leaf node of the tree data structure is a hash of the nodes it contains as children.
- The leaf nodes are all equally deep and as far to the left as they can be.
- It employs hash functions to preserve the integrity of the data.

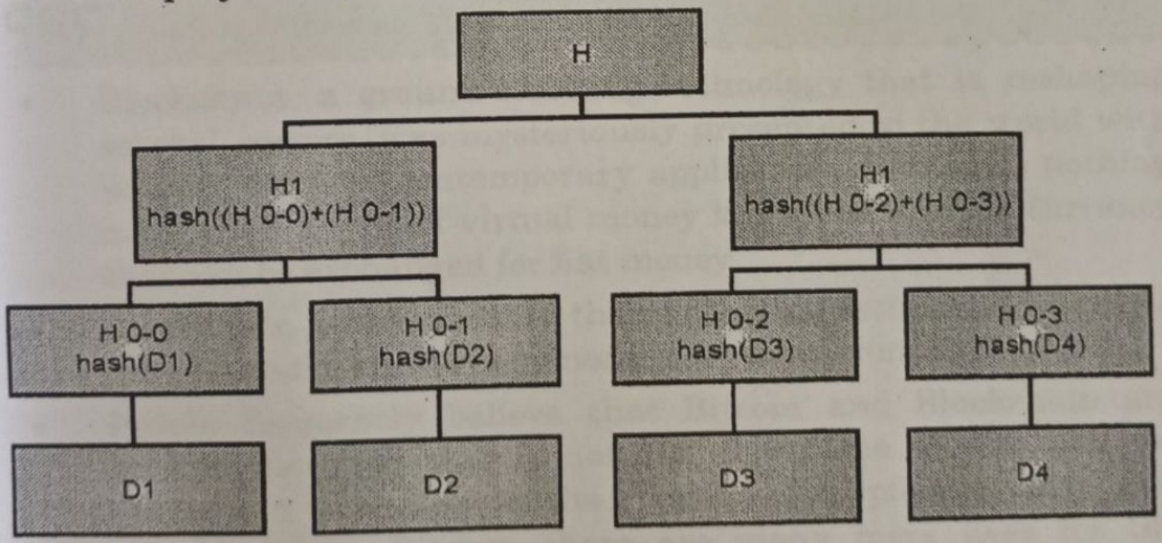


Fig. 1.10.1 : Merkel tree

- An input of data broken up into blocks labeled D1 though D4. Each of these blocks are hashed using some hash function.
- Then each pair of nodes are recursively hashed until we reach the root node, which is a hash of all nodes below it.

- The hash value at root node is called as Merkle root.
- When data is shared among parties, data is shared from regular channels and Merkle root is shared from secure channel.
- Intermediate hash values can be shared from regular or secure channels as per requirements. As data starts coming in, the verifier can verify if the data is valid by calculating hash value of the data received and comparing it with the hash value received for that segment.
- After the entire document is received, merkle root is compared with the merkle root received from the secure source. If data is manipulated in the process, then value of hash and in turn merkle root would change and this will help verifier to check authenticity of the data.
- In bitcoin and other cryptocurrencies, Merkle trees serve to encode blockchain data more efficiently and securely. They are also referred to as "binary hash trees."

Chapter Ends...

❑❑❑

Unit 2

CHAPTER 2

Feature Engineering

University Prescribed Syllabus

History, Centralized Vs. Decentralized Systems, Layers of Blockchain: Application Layer, Execution Layer, Semantic Layer, Propagation Layer, Consensus Layer, Why is Block chain important? Limitations of Centralized Systems, Blockchain Adoption So Far.

2.1 INTRODUCTION TO BLOCKCHAIN

GQ. Define Blockchain. What are important features of it?

- Blockchain, a ground-breaking technology that is reshaping several sectors, was mysteriously presented to the world with Bitcoin, its first contemporary application. Bitcoin is nothing more than a type of virtual money known as a cryptocurrency that can be exchanged for fiat money.
- Blockchain is the name of the underlying technology that has contributed to the development of cryptocurrencies.
- People frequently believe that Bitcoin and Blockchain are similar, however this is not the case. One of the uses for blockchain technology is the creation of cryptocurrencies, and in addition to Bitcoin, there are many more uses for the technology that are currently being explored.
- A data structure that stores transactional records and ensures security, transparency, and decentralisation is the simplest way to define Blockchain. It may also be viewed as a chain of records that are held in the form of blocks and are managed by many authorities.

- A distributed ledger known as a blockchain is totally accessible to everyone on the network. Once data is placed on a blockchain, it is very difficult to edit or modify it.
- On a blockchain, every transaction is protected by a digital signature that attests to its legitimacy. The information saved on the blockchain is tamper-proof and cannot be altered thanks to the use of encryption and digital signatures.
- Blockchain technology allows all the network participants to reach an agreement, commonly known as consensus. Every piece of information kept on a blockchain is digitally recorded and has a shared history that is accessible to everyone on the network.
- By doing this, any possibility of fraud or transaction repetition is avoided without the use of a third party.
- Consider the scenario where you are trying to find a way to transmit some money to a buddy who lives somewhere in order to better grasp blockchain. A bank or a payment transfer service like PayPal or Paytm are two options you can often employ.
- With this option, third parties are needed to complete the transaction, which results in a cost that is added to your money as a transfer fee.
- Additionally, in situations like these, it is impossible to guarantee the security of your money because it is very likely that a hacker may interrupt the network and take your money. The victim in both situations is the client. Blockchain is useful in this situation.
- In these situations, utilising a blockchain to transfer money instead of a bank makes the procedure considerably simpler and more secure. There is no additional cost since you process the cash directly, doing away with the need for a middleman.
- Moreover, the blockchain database is decentralised and is not limited to any single location meaning that all the information and records kept on the blockchain are public and decentralized.
- Since the information is not stored in a single place, there's no chance of corruption of the information by any hacker.

2.1.1 Features of Blockchain

The following features set the ground-breaking blockchain technology stand out :

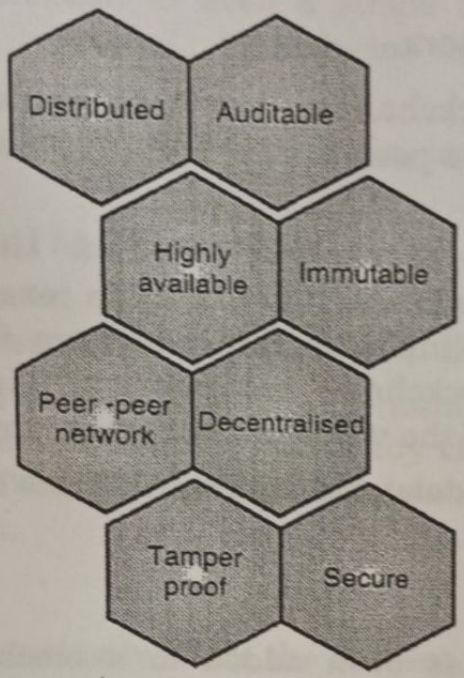


Fig. 2.1.1 : Features of Blockchain

☞ Distributed

- Collaboration is the only recurring concept in the blockchain. There must be several systems in place for collaboration to take place.
- Blockchain is a distributed system by nature since data is processed and stored by various parties. All network participants have access to the distributed ledger and its immutable record of transactions.
- With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.

☞ Decentralised

- Blockchains are decentralized in nature meaning that no single person or group holds the authority of the overall network.

- While everybody in the network has the copy of the distributed ledger with them, no one can modify it on his or her own. This unique feature of blockchain allows transparency and security while giving power to the users.

☞ Peer-to-Peer Network

- The usage of Blockchain makes it simple to engage between two parties using a peer-to-peer architecture without the need for a middleman.
- Blockchain is a peer-to-peer protocol that enables each member of the network to have an exact copy of each transaction, enabling machine consensus for approval. For instance, with blockchain, you may complete any transaction from one region of the world to another in a matter of seconds.
- Additionally, any delays or additional fees won't be subtracted from the transfer.

☞ Immutable

- Any data that has been added to a blockchain cannot be modified after it has been done so, which is known as the immutability feature of a blockchain.
- Consider sending an email as an illustration to better grasp immutability. An email that has been sent to a large group of recipients cannot be cancelled.
- You'll have to ask each receiver of your email to erase it, which is a laborious workaround. This is the operation of immutability.
- Data cannot be modified or altered once it has been processed. Because each block in a blockchain retains the hash of the one before it, if you try to modify the data of one block, you'll have to update the whole blockchain that follows it.
- Any changes to one hash will affect the remaining hashes as well. Since it takes a lot of processing power to modify all the hashes, it is quite difficult for someone to do so.
- As a result of immutability, data kept in a blockchain is immune to changes or hacker assaults.

☞ Tamper-Proof

- Because blockchains have the immutability characteristic built in, it is simpler to detect data manipulation.
- Because any alteration to even a single block can be easily discovered and corrected, blockchains are thought to be tamper-proof.
- Hashes and blocks are the two main methods for spotting tampering.
- Each block-related hash function is distinct.
- It may be compared to a block's fingerprint. Any modification to the data will result in a modification to the hash function.
- A hacker would have to modify the hashes of all the blocks following that one in order to make any changes because the hash function of one block is connected to the next, which is a challenging task.

☞ Auditable

- Blockchain does not only share the current state but the entire journey or log of how the state has been arrived. The log is available for each node to inquire.
- This makes activities happening on blockchain auditable.

☞ Highly available

Distributed and decentralized nature of blockchain network helps ensure consumers that the network always has a node available to serve the requests. This makes blockchain highly available

2.1.2 Origin of Blockchain

GQ. Explore the analogy of Rai stones with distributed ledger. **(4 Marks)**

☞ Rai/Fei Stones

- The capacity of blockchain to communicate information between untrusted parties has the potential to uplift everything from finance to politics, making it the most important advancement in knowledge storage and sharing since the creation of the internet.

- But Blockchain has a hidden past that dates back more than a thousand years.

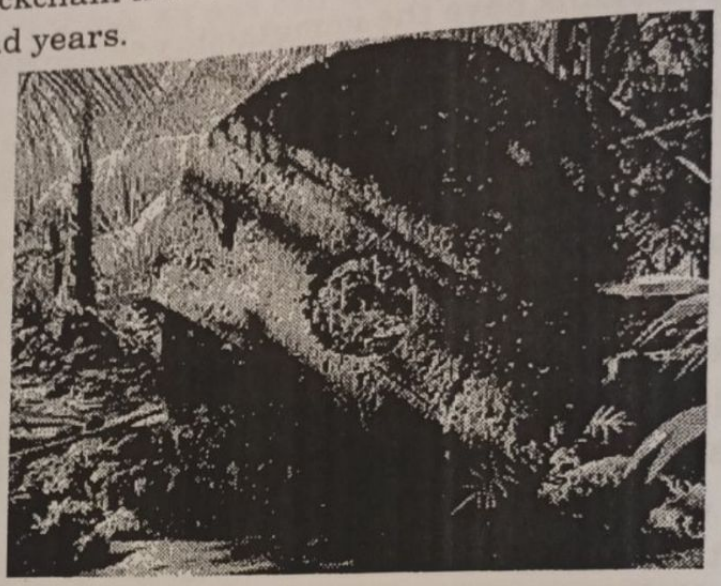


Fig. 2.1.2 : Rai Stones

- Although Bitcoin and the blockchain may appear to be complex new technical ideas, their foundation is actually far older than you may think.
- As bizarre as it may seem, there is a historical counterpart for bitcoin in a system of ancient money that dates back hundreds of years: huge stone discs known as rai, which were formerly employed as a symbolic kind of money on the Micronesian island of Yap.
- The biggest objects ever carried over the open Pacific Ocean before European contact were carved from limestone quarries in the Palau islands, around 250 miles (400 km) from Yap.
- These enormous, huge stone structures (sometimes taller than their owners) would not initially appear to have much in common with a digital value system that is encrypted, intangible, and basically invisible to human senses.
- However, that physical mismatch conceals the astounding similarity between bitcoin and rai: both currencies rely on a public, community ledger system that offers security and transaction transparency without the need for a centralised banking institution.
- In bitcoin and other cryptocurrencies, that public ledger is called the blockchain: an open record of bitcoin ownership and transactions spread across multiple computers on the internet.

- In rai – and the ancient culture of the Yapese islanders who used the giant stone coins – there was an equally dependable antecedent to the blockchain ledger.
- Although they were very precious, Rai were usually left in one spot once they had been set up because of their size, weight, and relative fragility.
- The new owner(s) of a disc may not have resided nearby if a rai were gifted or traded as a consequence. An oral ledger was kept in communities to guarantee ownership was recognised and unquestionable and to preserve security.
- Every villager kept a mental record of who owned each stone, who they got it from, and when that transaction took place.
- When a Rai/Fei stone was spent, that new transaction was shared across the village people to update everyone's mental map – just like a very ancient, early take on Blockchain.
- If someone came along and tried to wrongly claim a stone was theirs, the village could consult its mental 'decentralized ledger'.
- According to the researchers, this oral ledger – told through stories shared by the Yapese and passed down over generations – helped the community to record and communicate changes in ownership of the rai, for things like wedding gifts, political enticements, or even paying ransoms.
- If this all sounds similar, that's because it's exactly how Bitcoin transactions take place today on the Blockchain, albeit now between computers rather than people.

2.1.3 History of Blockchain Technology

GQ.	Explain The birth of blockchain along with the history of blockchains?	**(4 Marks)**
GQ.	Explain the evolution of blockchain with timeline.	**(4 Marks)**
GQ.	Explain The emergence of bitcoin.	**(2 Marks)**
GQ.	Brief about Ethereum development.	**(2 Marks)**
GQ.	What are the different phases of blockchain evolution?	**(6 Marks)**
GQ.	Discuss about major blockchain platforms evolved during phase 3 of blockchain.	**(6 Marks)**

- Given the impact that blockchain technology is having on a variety of industries, including manufacturing, education, and finance, it must rank among the most significant inventions of the twenty-first century.
- Many people are unaware that Blockchain has a history that extends back to the early 1990s.
- Numerous uses have emerged since its popularity began to rise a few years ago, all but underscoring the type of influence it is bound to have as the battle for digital economies heats up.
- We'll learn about the development of the blockchain and its history in this conversation.
- For blockchain enthusiasts and aspirants, understanding the history of blockchain is crucial.

Blockchain History

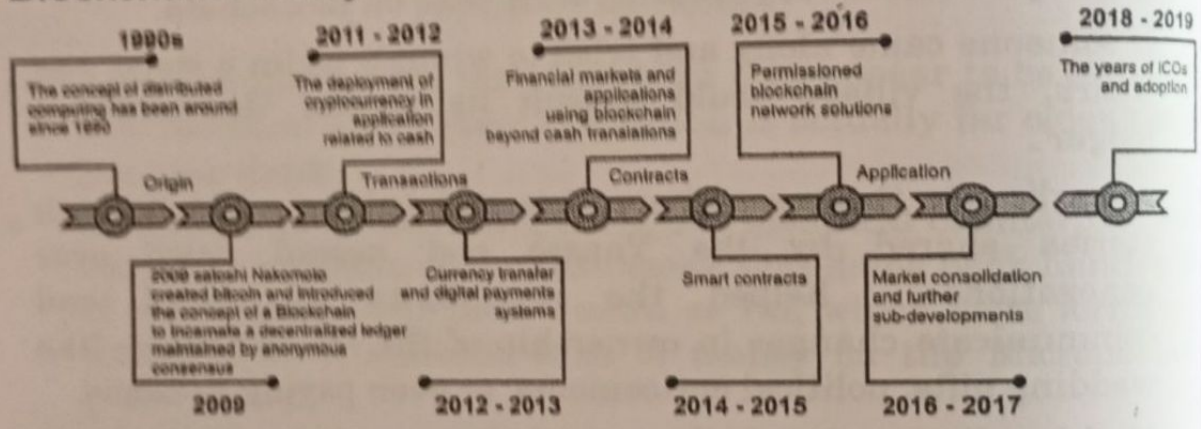


Fig. 2.1.3 : Timeline of blockchain evolution

1991–2008 : Early Years of Blockchain Technology

- Why did the blockchain develop? In 1991, Stuart Haber and W. Scott Stornetta dreamed of what many today call to as blockchain. Their initial project was creating a chain of blocks that was cryptographically secure such that document timestamps could not be altered.
- The system was modified in 1992 to include Merkle trees, which increased performance and allowed for the accumulation of more documents on a single block.
- The work of one individual or group by the name of Satoshi Nakamoto, however, is what gives Blockchain History its first real importance in 2008, as opposed to earlier years.

- Blockchain technology is credited to Satoshi Nakamoto as its creator. There isn't much information available about Nakamoto, who is said to have worked on Bitcoin, the first use of the digital ledger technology.
- In 2008, Nakamoto created the first blockchain, from which the technology developed and found use in a variety of applications outside of cryptocurrencies. In 2009, Satoshi Nakamoto published the first whitepaper on the subject.
- He explained in the whitepaper how the decentralised feature of the technology meant that nobody would ever be in control of anything and that it was thus ideally suited to enhancing digital trust.
- Since Satoshi Nakamoto left the scene and gave control of the development of Bitcoin to other core developers, the technology of digital ledgers has developed, giving rise to new applications that make up the blockchain's history. As we can see, blockchain technology was created in 1991.

Blockchain Structure

- A peer-to-peer distributed ledger that is secure and used to record transactions among multiple computers is what Blockchain is, expressed simply. The only way to change the ledger's contents is to add a new block that is connected to an existing block. It may also be thought of as an internet-based peer-to-peer network.
- Blockchain, in layman's or commercial terms, is a platform that enables individuals to conduct transactions of any kind without the need for a central or reliable mediator.
- Everyone has access to the created database's contents because it is transparently shared across network users.
- Peer-to-peer networks and a time stamping server are used to manage the database on their own. Each block in a blockchain is set up so that it refers to the information in the block before it.
- Batches of transactions that have been approved by network participants are stored in the blocks that make up a blockchain. A cryptographic hash of a previous block in the chain is included with each block.

☞ Evolution of Blockchain : Phase 1- Transactions -2008-2013: Blockchain 1.0: Bitcoin Emergence

- The majority of people think that Bitcoin and Blockchain are synonymous terms. That is untrue, as one is the fundamental technology that underlies most apps, among them cryptocurrency.
- At the height of the financial crisis in 2008, a mysterious individual, Satoshi Nakamoto sent a message to the entire world.
- This letter discussed Bitcoin, a brand-new peer-to-peer electronic payment system that did not include any middlemen.

Bitcoin P2P e-cash paper

Satoshi Nakamoto satoshi at vistomail.com
Fri Oct 31 14:10:00 EDT 2008

- Previous message: Fw: SHA-3 lounge
- **Messages sorted by: [date] [thread] [subject] [author]**

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Fig. 2.1.4 : Original email message from Satoshi Nakamoto announcing Bitcoin

- He said that the double-spending issue that had troubled earlier digital currencies or cryptocurrencies had been resolved. Nakamoto accomplished this by combining several technologies and putting them together in creative ways. These technologies and ideas include, among others, algorithms, game theory, economics, and cryptography.

- The word "blockchain" wasn't in use to characterise this new ledger technology at the time Bitcoin was introduced. Nakamoto created the first block, known as the "genesis block," from which subsequent blocks were mined and connected to create one of the longest chains of blocks holding various types of data and transactions.
- With the help of Satoshi's invention, a Bitcoin user may now deal digitally with another user without the need for a single, centralised middleman (like a bank) to approve the transaction. Previous digital transaction systems have failed to reach this achievement.
- Numerous applications have emerged since the advent of Bitcoin, a blockchain-based application, all of which aim to take use of the capabilities and guiding principles of the digital ledger technology. As a result, there is a vast number of uses for blockchain technology that have emerged over the course of history.

☞ Evolution of Blockchain : Phase 2- Contracts: 2013-2015: Blockchain 2.0 : Ethereum Development

- As one of the first contributors to the Bitcoin codebase and in a world where innovation is the norm, Vitalik Buterin is among a growing number of developers who believe that Bitcoin has not yet fully used the potential of blockchain technology.
- Because of the limits of Bitcoin, Buterin began developing what he thought would be a flexible blockchain that could serve a variety of purposes in addition to serving as a peer-to-peer network.
- A crucial turning point in the history of the blockchain came when Ethereum was introduced as a brand-new public blockchain in 2013 with more features than Bitcoin.
- By making it possible to store additional assets in addition to contracts, such as slogans, Buterin created Ethereum apart from the Bitcoin Blockchain.
- With the addition of the new functionality, Ethereum's capabilities were increased beyond those of a cryptocurrency to those of a platform for the creation of decentralised apps.
- Given its capacity to enable smart contracts that are used to carry out various functions, the Ethereum blockchain, which

was formally introduced in 2015, has developed into one of the most significant implementations of blockchain technology.

- The blockchain technology for Ethereum has also been successful in attracting a vibrant developer community, which has helped it build a real ecosystem.
- Ethereum blockchain processes the most number of daily transactions thanks to its ability to support smart contracts and decentralized applications. Its market cap has also increased significantly in the cryptocurrency space.

☞ Evolution of Blockchain : Phase 3- Applications-2018: Blockchain 3.0: the Future

- Ethereum and Bitcoin are just the beginning of the blockchain's history and evolution. Several initiatives have emerged in recent years that all make use of the potential of blockchain technology.
- In addition to developing new features utilising blockchain technologies, additional initiatives have worked to fix some of the shortcomings of Bitcoin and Ethereum.
- NEO, described as the first open-source, decentralised, and blockchain platform developed in China, is one of the latest blockchain applications.
- Even though the country has prohibited cryptocurrencies, it remains active when it comes to blockchain technology. With the support of Jack Ma, the CEO of Alibaba, NEO promotes itself as the Chinese Ethereum and aspires to challenge Baidu's influence in the nation.
- IOTA was created as a result of certain developers using blockchain technology in the race to accelerate the development of the Internet of Things.
- The cryptocurrency platform aims to offer no transaction costs and unique verification procedures, and it is designed for the Internet of Things environment. Additionally, it tackles some of the scaling problems with Blockchain 1.0 Bitcoin.
- Other second-generation blockchain systems, in addition to IOTA and NEO, are also making waves in the market. As a bid to solve some of the security and scalability challenges related

to the early blockchain applications, the MoneroZcash and Dash blockchains were launched.

- The blockchain history previously covered includes open blockchain networks, in which anybody may view a network's contents. However, as technology has advanced, many businesses have begun integrating it within to improve operational effectiveness.
- In order to get a head start on the usage of technology, large businesses are making significant investments in employing professionals.
- When it comes to investigating blockchain technology applications, businesses like Microsoft and Microsoft appear to have taken the lead, leading to what are today known as private, hybrid, and federated blockchains.

☞ 2015 : Hyperledger

- The Linux Foundation introduced the open-source blockchain Umbrella project in 2015. They continued by naming it Hyperledger, which is still being developed collaboratively as a distributed ledger.
- Under Brian Behlendorf's direction, Hyperledger aims to encourage cross-industry cooperation for the creation of blockchain technology and distributed ledgers.
- The primary goal of Hyperledger is to promote the use of blockchain technology in order to enhance the functionality and dependability of present systems that facilitate cross-border commercial transactions.

☞ 2017 : EOS.IO

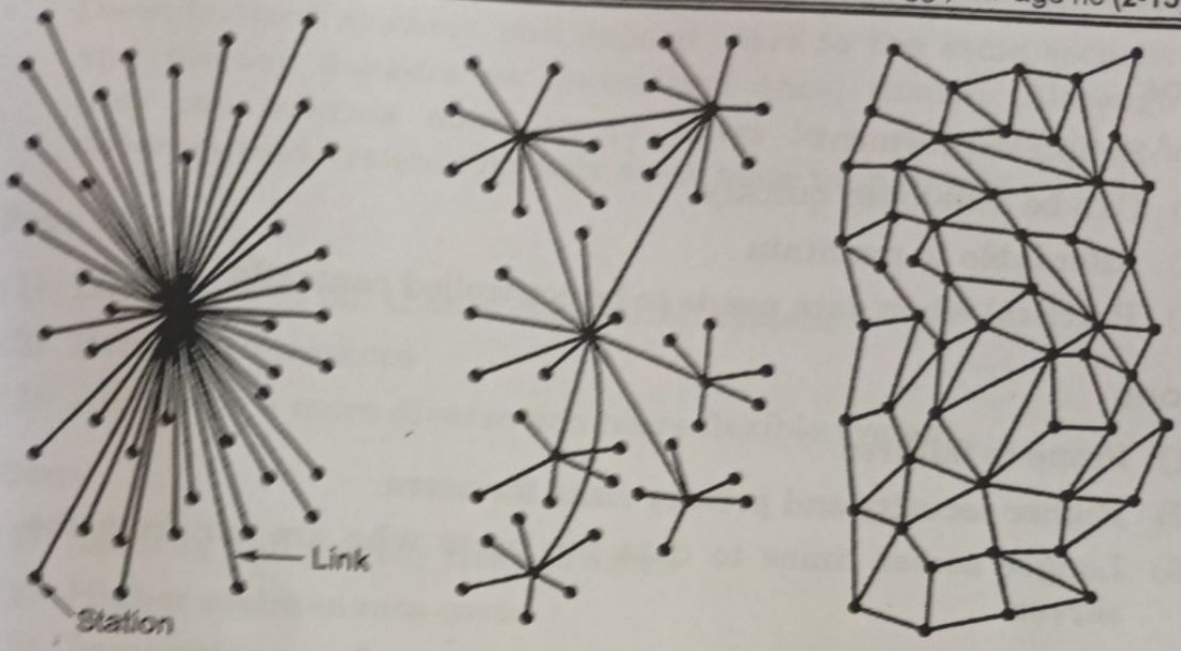
- The private firm block invented EOS. One was created in 2017 after a white paper describing a new blockchain system with EOS as the native coin was published.
- EOS, in contrast to other blockchain protocols, aims to mimic CPU and GPU functions found in real computers.

- Because of this, EOS.IO serves as both a platform for smart contracts and a decentralised operating system.
- Its primary goal is to promote the implementation of decentralised apps by means of an independent decentralised corporation.

2.2 CENTRALIZED VS. DECENTRALIZED VS. DISTRIBUTED SYSTEMS

GQ. Differentiate between centralised and decentralised system? **(4 Marks)**

- The distributed, centralised, and decentralised systems have an impact on practically everyone who uses the internet.
- It is fundamental to the growth and development of networks, financial systems, businesses, applications, web services, and other systems.
- All of these systems are capable of functioning properly, although some are by design more reliable and secure than others.
- Systems can be quite compact, connecting just a few people and devices. Or they might be enormous and cover many continents.
- In any case, they deal with the same difficulties with scalability, fault tolerance, and maintenance expenses.
- The largest network in the world is the internet itself. In fact, it is so big that it integrates all these various systems into a sizable digital ecosystem. However, most businesses and people find it impossible to use all of these technologies. They have to choose. And you may have to choose, too.



(a) Centralized (b) Decentralized (c) Distributed

Fig. 2.2.1 : Centralized Vs. Decentralized Vs. Distributed Systems

2.2.1 Centralized Systems

GQ. Explain the concept of centralised system with its pros and cons. **(4 Marks)**

- All users in a centralised system are linked to a single "server" that controls the whole network. Both user information and data that may be accessed by other users are stored by the central owner.
- User profiles, user-generated content, and other details may be included in this user information. A centralised system may be quickly constructed and is simple to set up.
- However, this technique has a significant drawback. Users are unable to access the data if the server fails since the system is no longer functional.
- The availability of the network is dependent on this owner since a centralised system needs a central owner to link all the other users and devices.
- It is simple to understand why centralised systems are no longer the first option for many firms when you consider the obvious security issues that occur when one owner keeps (and has access to) user data.

Pros

(1) Simple deployment
(2) Can be developed quickly
(3) Affordable to maintain
(4) Practical when data needs to be controlled centrally

Cons

(1) Prone to failures
(2) Higher security and privacy risks for users
(3) Longer access times to data for users who are far from the server

2.2.2 Decentralized Systems

GQ. Explain the concept of decentralised system with its pros and cons. **(4 Marks)**

- Decentralized systems don't have a single central owner, as their name suggests. As an alternative, they use a number of central owners, each of whom typically keeps a copy of the resources that users may access.
- Decentralized systems can experience crashes equally as frequently as centralised ones. It is, nevertheless, more fault-tolerant by design. This is so that users may continue to access data even if one or more central owners or servers fail.
- If at least one of the central servers is still running, resources are still available. This often implies that system administrators may fix broken servers and take care of any other issues while the system itself continues to function normally.
- In a decentralised system, server failures may degrade performance and restrict access to particular data. However, this approach provides a significant improvement over a centralised system in terms of overall system uptime.
- This approach also has the benefit of often quicker data access times. Owners can build nodes in various locations or places with a lot of user activity.

- Decentralized systems still expose users to the same security and privacy dangers as centralised ones, though. Although they can tolerate more errors, there is a cost for this. A decentralised system typically costs more to maintain.

Pros

(1) Less likely to fail than a centralized system
(2) Better performance
(3) Allows for a more diverse and more flexible system

Cons

(1) Security and privacy risks to users
(2) Higher maintenance costs
(3) Inconsistent performance when not properly optimized

2.2.3 Distributed System

GQ. Explain the concept of distributed system with its pros and cons. **(4 Marks)**

- In that it lacks a single central owner, distributed systems are comparable to decentralised ones. Further still, it does away with centralization.
- Users in a distributed system can enable user rights as required, but all users in the system have equal access to the data. The internet itself serves as the greatest example of a large, distributed system.
- Shared ownership of the data is made possible by the distributed system. Users are also given equal access to hardware and software resources, which might occasionally enhance system performance.
- A distributed system is protected from the simultaneous failure of many components, which can greatly increase uptime. The shortcomings of the previous systems led to the development of distributed systems.
- Distributed systems are the obvious choice for many businesses due to rising security, data storage, and privacy issues as well as the ongoing need to improve performance.

- The fact that distributed system technologies, most notably the blockchain, are revolutionising several sectors is therefore not surprising.

Pros

(1) Fault-tolerant
(2) Transparent and secure
(3) Promotes resource sharing
(4) Extremely scalable

Cons

(1) More difficult to deploy
(2) Higher maintenance costs

2.2.4 Centralized vs Decentralized vs Distributed Systems Comparison

GQ. Compare between centralised Vs decentralised Vs distributed system? **(4 Marks)**

- Now that you have a better understanding of every system, let's see how these systems compare with one another.
- The following head-to-head comparison focuses on key points like fault tolerance, maintenance, scalability, development, and evolution. For each of these, we are using simple ratings like low, moderate, and high.

Table 2.7.1

Parameter	Centralized	Decentralized	Distributed
Fault tolerance	Low	Moderate	High
Maintenance	Low	Moderate	High
Scalability	Low	Moderate	High
Development	High	Moderate	Moderate
Evolution	Low	High	High

2.3 BLOCKCHAIN'S MECHANISM

GQ. Describe the blockchain mechanism in brief. **(4 Marks)**

- A distributed, peer-to-peer database called a blockchain stores an ever-increasing volume of transactions.
- Using consensus algorithms (i.e., a set of rules), each transaction, known to as a "block," is encrypted, timestamped, and verified by each authorised user of the database.
- A transaction cannot be added to the database if it has not been verified by all database users. A chain of transactions is formed when each transaction is sequentially connected to the one before it (or blocks).
- A transaction cannot be altered, resulting in an unchangeable audit trial. Only by including another transaction in the chain can a transaction be changed.
- Say, for example, that company X wishes to send money to company Y in order to settle an unpaid invoice for the purchase of software (Fig. 2.3.1).
- A block is made when Company X enters the transaction into the database.
- Every network user that has permission to receive broadcasts is informed of the block (or transaction).
- A block is subsequently added to the chain of transactions, providing an immutable and transparent record of the transaction, when all the participants have validated it (i.e., approved the payment).
- The transaction is then finished when the funds are transferred from company X to company Y.
- The blockchain's security prohibits hackers from impersonating legitimate network users.
- All transactions are replicated across the network of users and then stored in each member's computer system, enabling a distributed ledger-which may be shared across numerous locations, organizations, or countries.

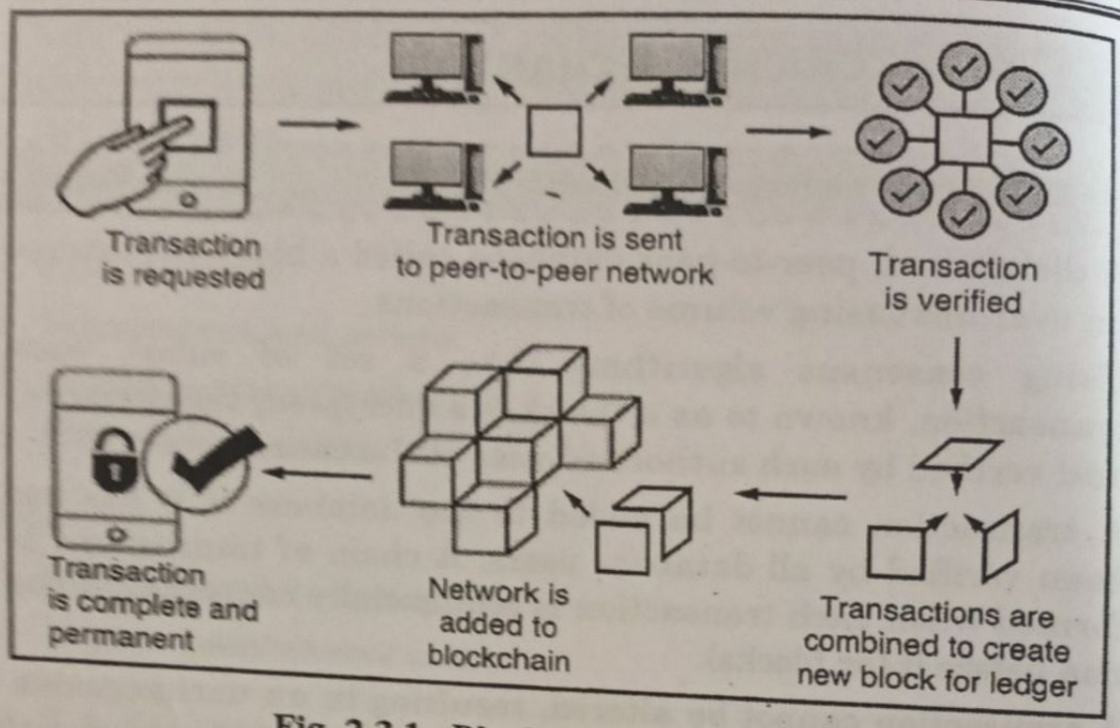


Fig. 2.3.1 : Blockchain mechanism

2.3.1 Structure of Block

GQ. Draw and explain the structure of block. **(4 Marks)**
GQ. State and explain the constituents of block header. **(4 Marks)**
GQ. Enlist the methods to identify the block uniquely? **(4 Marks)**
GQ. Write down the importance of genesis block? **(2 Marks)**

- Blocks are data structures within the blockchain database, where transaction data in a cryptocurrency blockchain are permanently recorded.
- A block records some or all of the most recent transactions not yet validated by the network. Once the data are validated, the block is closed. Then, a new block is created for new transactions to be entered into and validated.
- A block is thus a permanent store of records that, once written, cannot be altered or removed.
- A block is a container data structure that aggregates transactions for inclusion in the public ledger, the blockchain. The block is made of a header, containing metadata, followed by a long list of transactions that make up the bulk of its size.
- The block header is 80 bytes, whereas the average transaction is at least 250 bytes and the average block contains more than 500 transactions.

- A complete block, with all transactions, is therefore 1,000 times larger than the block header.

Table 2.3.1 : Structure of the Block

Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
1-9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

☞ Block Header

The block header consists of three sets of block metadata.

- First, there is a reference to a previous block hash, which connects this block to the previous block in the blockchain.
- The second set of metadata, namely the difficulty target, timestamp, and nonce, relate to the mining competition.
- The third piece of metadata is the merkle tree root, a data structure used to efficiently summarize all the transactions in the block.

Table 2.3.2 : The structure of a block header

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The proof-of-work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the proof-of-work algorithm

☞ Version

It states the version that the particular block is using, there are three types of Blockchain version.

(1) Blockchain Version 1.0 (cryptocurrency)-It used a public ledger to store the data, for example, Bitcoin.

(2) Blockchain Version 2.0 (smart Contract)- It is called smart contracts which is self-executing programs, for example, Ethereum.

(3) Blockchain Version 3.0 (DAPPS)- It is used to create a decentralized structure, for example, tor Browser.

(4) Blockchain Version 4.0 (Blockchain for Industry)- It is used to create a scalable, affordable blockchain network such that more people could use it.

☞ Previous Hash

As Blockchain is a collection of several interconnected nodes also called a block, so previous hash stores the hashed value of the previous node's address, First block in the blockchain is called the Genesis Block and has no previous block hash value.

☞ Merkle Root

A Merkle root uses mathematical formulas to check if the data is not corrupted, hacked, or manipulated. For example, Suppose one block has 10 transactions, then to identify that block we need 10 transactions to combine and form one Hash Value, so it uses the concept of the binary tree to create the hash of the block and that value is called the Merkle Root.

☞ Timestamp

Timestamp in the blockchain is used as proof that the particular block is used at what instance of a time, also this timestamp is used as a parameter to verify the authenticity of any block.

☞ Difficulty Target

It specifies the complexity and the computation power required to mine the network, if we are having a high difficulty target then it implies that we need more a computationally expensive

machine to mine it. For example, in order to increase the difficulty target algorithms such as SHA-2, SHA-3. RIPEMD, MD5,BLAKE2 is used.

☞ Nonce

It is abbreviated as 'number only used once' and it is a number which blockchain miners are finding and on average, it takes almost 10 times to find out the correct nonce. A nonce is a 32-bit number, having the maximum value as 2^(32) total possible value, so the job of the bitcoins miners is to find out the correct integer value which is a random integer between 0 and 2^(32), so it becomes computationally expensive.

Block Identifiers : Block Header Hash and Block Height

- A block's principal identifier is its cryptographic hash, or digital fingerprint, which is created by running the block header through the SHA256 algorithm twice.
- Since just the block header is utilised to compute it, the resultant 32-byte hash is more suitably known as the block header hash.
- The block hash of the very first bitcoin block ever produced, for instance, is 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.
- By simply hashing the block header, every node may independently extract the block hash, which uniquely and clearly identifies a block.
- Take note that when a block is transmitted across the network or kept on a node's persistent storage as part of the blockchain, the block hash is not really contained inside the block's data structure. Instead, as each node receives a block from the network, it computes the block's hash.
- To facilitate indexing and expedite block retrieval from storage, the block hash may be kept in a separate database table as part of the block's metadata.
- The block height, or position inside the blockchain, is a second identifier for a block.

- The first block that has ever been produced has a block height of 0 (zero), and it is the same block that was previously identified by the block hash 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.
- Thus, there are two methods to recognise a block: by using the block hash or by using the block height. Like boxes stacked on top of one another, each additional block that is placed "on top" of the original block moves it up one position in the blockchain. On January 1, 2014, there were roughly 278,000 blocks built on top of the first block that was made in January 2009.
- The block height is not an unique identifier. The block height does not always identify a single block, even though a single block will always have a unique and invariant block height.
- The same block height might be shared by two or more blocks that are competing for the same position on the blockchain. Additionally, the block height is not stored inside the block; it is not a member of the block's data structure.
- When a block is received from the bitcoin network, each node dynamically determines its position (height) on the blockchain. For quicker retrieval, the block height might alternatively be saved as metadata in a database table that is indexed.

The Genesis Block

- The genesis block, which is the first block on the blockchain, was made in 2009. Because it is the genesis block, you may start at any block in the blockchain and work your way backward in time to reach it. It is the common ancestor of all the blocks in the system.
- Because the genesis block is statically encoded inside the bitcoin client software, making it unchangeable, every node always starts with a blockchain of at least one block.
- Every node "knows" the hash and structure of the genesis block, the exact timestamp it was generated, and even the specific transaction included inside. As a result, every node has access to a safe "root" from which to construct a reliable blockchain.

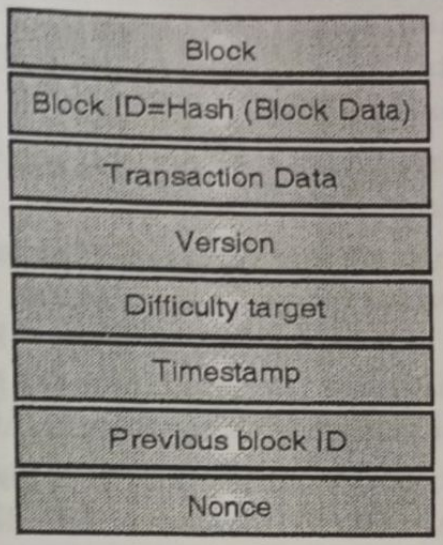


Fig. 2.3.2 : Sample block structure

2.3.2 Process of Chaining of Blocks

GQ. Elaborate the chaining process of blocks. **(4 Marks)**

GQ. If someone tries to hack Block no5 in a chain of 15 Blocks. What will happen and why? **(4 Marks)**

- Let us capture the data in fixed size sets (say 1 KB each), called as blocks. These blocks will get unique identifier based on the contents of data. These identifiers are created using hashing mechanism.

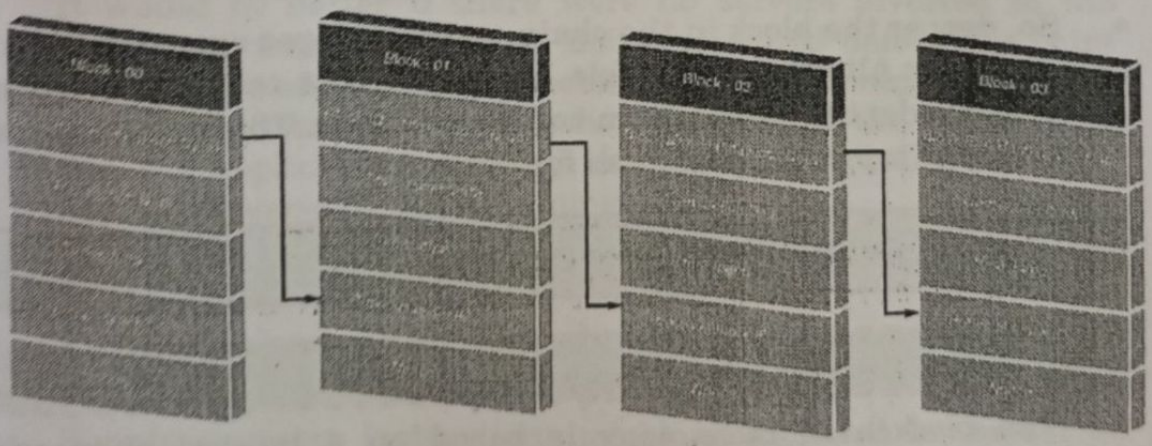


Fig. 2.3.3 : Chaining of blocks[For simplicity, few elements are not shown in block]

- Each block shall have four important sections: identifier, transaction data, timestamp and identifier of previous block along with other elements.
- Logically, the first block does not contain the pointer since this one is the first in a chain.
- The 1st block has no predecessor. Hence, it does not contain hash of the previous block. It is called as Genesis block. In the beginning, we will create first block: BLOCK-01. For this block, we will initialize "the identifier for the previous block" to zeros and the "timestamp" is set to current timestamp.
- This block does not get confirmed till it gets enough data i.e. (1 KB) that it can hold. Whenever 1 KB data is confirmed, we update "data" of BLOCK-01 to received data.
- The identifier of BLOCK-01 will be created using contents of block including "data", "timestamp" and "previous block identifier" of BLOCK-01.As BLOCK -01 is confirmed, the second block (BLOCK-02) is created with "previous block identifier: set to identifier of BLOCK-01.The process keeps repeating many times as required.
- There is potentially going to be a final block within the blockchain database that has a pointer with no value. Suppose there is chain of 10 blocks. Some malicious user try to update contents of BLOCK-07->it will impact on its identifier->it will require to change identifier of BLOCK-08->in turn ,it will need to change identifier of BLOCK 09 and 10 as well.
- So, deeper the block in the chain, more changes are required to update it.All this is possible because of the technique which creates identifiers based on contents of data.This technique is called as cryptographic hash functions.

2.4 LAYERS OF BLOCKCHAIN

GQ. Explain the layered architecture of Blockchain. **(6 Marks)**

- The blockchain technology is based on a layered approach Fig. 2.4.1. The block- chain technology is decomposed into several layers that will in turn help in better understanding of security and the design of the blockchain.

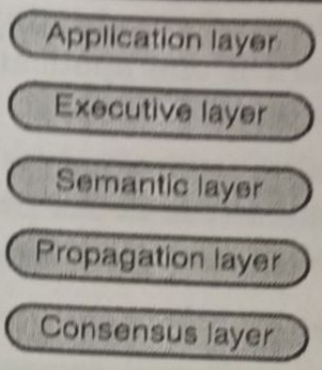


Fig. 2.4.1 : Blockchain layers

- There are few layers for the blockchain technology discussed in the following sections

(a) Application Layer

- As a shared ledger system that is tamper-proof, decentralised, and has many advantages, blockchain technology may be the foundation for a variety of applications.
- The application layer is on top of this layer suit because some apps with built-in application layers can communicate with the other levels.
- A user can programme the needed functionality and create the application for the application's user at the application layer. The programme has to be deployed on each node because the blockchain is a decentralised technology and there isn't a server involved.
- It would be better if there were no servers involved in the blockchain network because doing so would defeat the point and benefit of blockchain technology, even though there are some situations where blockchain is used in the background and the applications need to be hosted on a web server and require server-side programming.

(b) Execution Layer

- All instructions performed at the application layer are handled by this layer for all nodes connected to the blockchain network.
- Simple or many instructions might be included in the set of instructions. For instance, a smart contract is a little piece of code that must be run when payment has to be moved from one person to another.

- The code must now be performed individually on each node of the blockchain network if one application is present on all of them.
- The execution of code on a set of inputs should always result in the same output for all of the nodes present on the blockchain in order to prevent inconsistent results.

(c) Semantic Layer

- This layer is also known as the logical layer in the blockchain layer hierarchy. This layer is concerned with validating both the blocks that are created in the network and the transactions that are carried out inside the blockchain.
- A set of instructions are carried out on the execution layer and validated on the semantic layer when a transaction is initiated from a node.
- The connection of the blocks created in the network is another function of the semantic layer. With the exception of the Genesis block, each block on the blockchain contains the hash of the one before it. On this layer, this block linkage must be defined.

(d) Propagation Layer

- The peer-to-peer communications that enable nodes in a network to find one another and synchronise with another node are handled by the propagation layer.
- Every node in the network receives a broadcast when a transaction is completed. Additionally, when a node proposes a block, it is immediately broadcast throughout the whole network so that other nodes can use it and contribute to it.
- As a result, this layer defines how a block or transaction distributes throughout the network and maintains the overall stability of the system.
- But depending on the network's capacity or bandwidth, sometimes the propagation happens immediately and some other times it takes a while.

(e) Consensus Layer

- The majority of blockchain solutions start at this layer. This layer's primary goal is to ensure that all nodes must come to an agreement on a shared understanding of the shared ledger. The layer also addresses the blockchain's safety and security.
- There are a variety of consensus algorithms that may be used to create cryptocurrencies like Bitcoin and Ethereum. These algorithms employ the proof-of-work mechanism to choose a random node from among the network's nodes that can propose a new block.
- Once a new block is created, the block is propagated to all the other nodes to check if the new block is valid or not with the transactions in it and based on the consensus from all other nodes the new block gets added on to the blockchain.

2.5 ACTORS IN BLOCKCHAIN TECHNOLOGY

GQ. List and explain various actors in a blockchain technology solutions. **(4 Marks)**

(1) Blockchain Architect

- Responsible for the architecture and design of the blockchain solution.
- A blockchain architect will design how a blockchain solution is going to be built.
- He/she will identify what information needs to be stored, what are some of the transactions and business logic that need to be embedded onto a network, how the network itself should to be created, etc.

(2) Blockchain developer

- A blockchain developer will take what has been architected and he/she will develop the actual code that will run on the blockchain network.

- The developer of applications and smart contracts that interact with the blockchain and are used by blockchain users.

(3) Blockchain network operator

- A blockchain network operator manages and monitors the blockchain network.
- Each business in the network has a blockchain network operator.

(4) Traditional processing platform

- There are traditional processing platforms or other systems of record that the blockchain connects to and might send or get information.
- An existing computer system which may be used by the blockchain to augment processing. The system may also need to initiate requests into the blockchain.

(5) Traditional data sources

- Traditional data sources and databases are also part of the blockchain solution.
- An existing data system which may provide data to influence the behavior of smart contracts.

(6) Membership services

- It is an important component. It defines or provides the identity for users to come and transact on the blockchain. For example, when you open an account in the bank, the bank gives you a username and password for login to access web services.
- The membership service will provide a digital certificate that will allow an individual to transact on the network. It manages different types of certificates required to run a permissioned blockchain.

(7) Blockchain user

- A blockchain user will perform business transactions on the blockchain. These users could belong to multiple organizations that are participating in the blockchain network.
- He/she is a business user operating in a business network. Blockchain users interact with the blockchain using an application. However, they are unaware of the blockchain.

(8) Blockchain regulator

- The regulator could be an optional actor in a blockchain solution.
- The regulator might have read only access onto the network where he/she might have some oversight into whether the transactions performed are legitimate or not. Whether the transactions are compliant with the policies set by the blockchain regulator.
- A blockchain regulator is responsible for the overall authority in a business network. In particular, they may require broad access to the contents of a ledger.

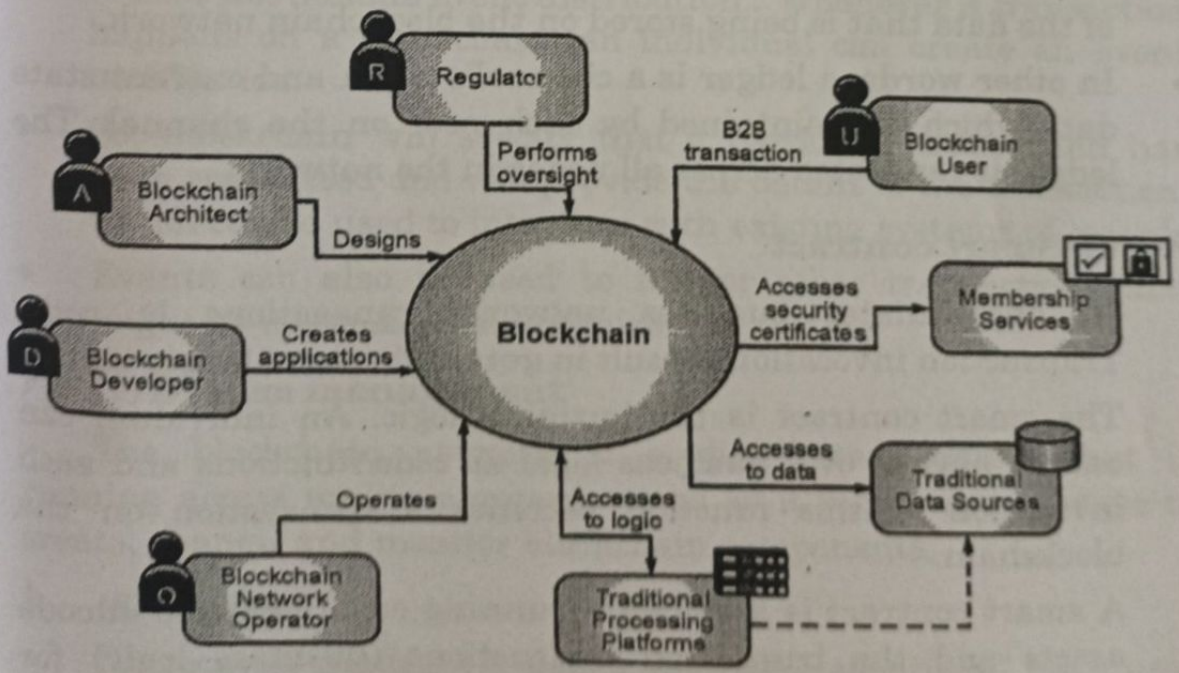


Fig. 2.5.1 : Actors in blockchain technology

2.6 IMPORTANT TERMS RELATED TO BLOCKCHAIN TECHNOLOGY

GQ. State and explain different terms related to blockchain. **(4 Marks)**

A variety of blockchain components are available in the market. Some of the major components in a blockchain solution are as follows :

(1) Ledger	(2) Smart contract
(3) Peer network	(4) Consensus network
(5) Membership	(6) Events
(7) System management	(8) Wallet
(9) System integration	

(1) Ledger

- It contains the current world state of the ledger and a blockchain of transaction invocations."
- Every node in the blockchain network will maintain a ledger of all transactions, and the transactions will maintain the state of the data that is being stored on the blockchain network.
- In other words, a ledger is a channel's chain and current state data which is maintained by each peer on the channel. The ledger is replicated across all nodes in the network.

(2) Smart contract

- "It encapsulates business network transactions in code. Transaction invocations result in gets and sets of ledger state."
- The smart contract is the business logic. An individual can encode his/her own business logic as code/functions and each invocation of this function becomes a transaction on the blockchain.
- A smart contract is a software running on a ledger to encode assets and the truncation instructions (business logic) for modifying the assets.

(3) Peer network

A broader term overarching the entire transactional flow, which serves to generate an agreement on the order and to confirm the correctness of the set of transactions constituting a block.

(4) Consensus network

- It is a collection of network data and processing peers forming a blockchain network.
- It is responsible for maintaining a consistently replicated ledger.

(5) Membership

- "It manages identity and transaction certificates as well as other aspects of permissioned access."
- A membership service provides identities for the users to transact on the blockchain.

(6) Events

- "It creates notifications of significant operations on the blockchain (e.g., a new block) as well as notifications related to smart contracts.
- It does not include event distribution." Whenever a transaction happens on a blockchain, an individual can create an event notification.
- So, blockchain will specify that a particular transaction has been committed and will provide the details of the transaction, which can be used to integrate with existing systems of record.
- Events can also be used to trigger other transactions that might be internal to an organization.

(7) System management

The blockchain network is a distributed system that is running across multiple organizations so it requires new ways to create, change, and monitor blockchain components.

(8) Wallet

- "It securely manages a user's security credentials." Each user has a digital certificate and is going to be performing transactions using the digital certificate.

- There needs to be a place where a user can securely store that private information. So, a digital certificate contains the private identity of an individual.
- He/she should not be sharing the information with anybody else, which is securely managed in a wallet.

(9) System integration

- It is responsible for integrating blockchain bi-directionally with external systems.
- It is not a part of the blockchain, but used with it.

2.7 WHY IS BLOCKCHAIN IMPORTANT ?

GQ. Elaborate the importance of blockchain w.r.t to safety. **(4 Marks)**

GQ. How decentralization is achieved through blockchain technology? **(4 Marks)**

GQ. How digital freedom can be achieved through blockchain? **(4 Marks)**

GQ. Which features makes blockchain important over traditional system? **(4 Marks)**

- By examining its fundamental characteristics, you may understand the blockchain's significance at its core.
- Blockchain stands out as the finest option because to these properties that make it tempting in a variety of situations.

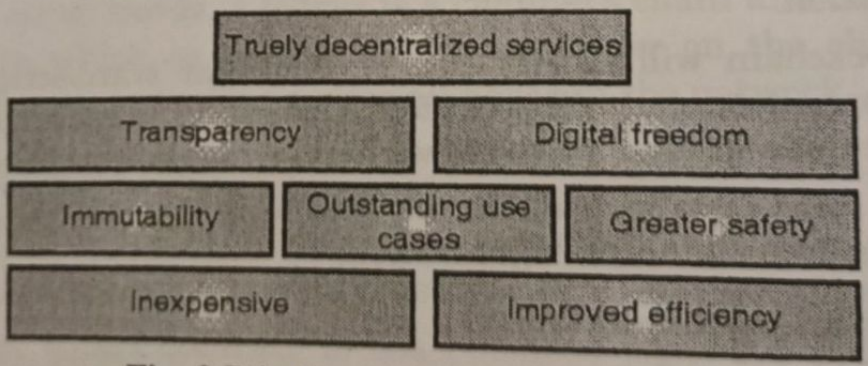


Fig. 2.7.1 : Importance of blockchain

Immutability

- Blockchain cannot be changed. This creates several chances for platforms that require immutable characteristics to improve the functionality of their system in a highly competitive industry.
- Take the supply chain as an example. Immutability enables

businesses to guarantee that the packages are not harmed while in transit.

- The package information cannot be changed in any manner since blockchain is immutable. The system will alert you to any changes.

☞ Transparency

- Transparency is another crucial factor that contributes to blockchain's significance. There are several blockchain variants.
- Due to its nature, public blockchain offers transparency. It serves many purposes in our society, including voting.
- Companies can use it to make sure that procedures are fully or partially transparent to the end user.

☞ Digital Freedom

- Freedom is one of your rights as a person. There are centralised organisations that provide connectedness in terms of the economics but also limit our independence.
- Consider your bank as an example. If considered appropriate, it has the power to halt your transactions or seize your account.
- Some banks take this action, even though the account holders haven't broken any laws. So, if you are taking blockchain into account, you will find there is no centralized authority.
- You can achieve true digital independence with blockchain. You are your own bank. You have sole authority over when and how much money you withdraw.
- You are the only owner and liable party for your assets because there is no centralised authority. It grants you the independence in the digital world that is mainly dependent on blockchain technology.

☞ Truly Decentralized Services

- Our advanced civilization is built on decentralised services. There will be decentralised services for every industry out there, whether it is asset management or energy management.

- People will have easy accessibility to products that aren't already on the market because to this. Decentralized services will be present in almost every sector.
- The music industry, for example, can benefit from truly decentralized services where both creator and consumer can participate without the need for any approval from a big centralized corporation.

☞ Outstanding Use-Cases

- Blockchain is not restricted to a single use-case. Blockchain is therefore a great technology for our society's future.
- Nearly every industry, including banking, government, education, healthcare, the oil industry, and others, may utilise it. They also have a great influence.

☞ Greater Safety

- In order to increase the security of the data kept on the network, blockchain employs cryptography. In addition to the encryption, the decentralised element of blockchain makes it more secure than previous systems.
- To safeguard the data and systems on the blockchain network, cryptography makes use of sophisticated mathematical methods.
- Additionally, every block on the network has a distinct hash, making it impossible for hackers or malevolent actors to alter or fake any data.

☞ Inexpensive

- Comparatively speaking to other technologies, blockchain is less costly. The buffer necessary to run the network effectively is removed when centralised authority is removed.
- Cost effectiveness is increased since there is no need to pay a middleman when there is no centralization. Using blockchain in the supply chain drastic decrease paperwork.
- The expense of the documentation is significant. There are other expenses, such as paying staff to handle the paperwork and keep the middlemen up to date.

☞ Improved Efficiency

- Another justification for the significance of blockchain is increased productivity. The root of the problem is improved procedures, intermediate elimination, and security.
- Additionally, transactions, particularly international ones, now take seconds to complete rather than a week.

⏭ 2.8 LIMITATIONS OF BLOCKCHAIN TECHNOLOGY

GQ. What are the limitations of blockchain technology? **(6 Marks)**
GQ. Blockchain needs high energy consumption. How? **(4 Marks)**
GQ. What are the interoperability and scalability issues of blockchain? **(4 Marks)**

- Although we are talking about the future, there are now just a few blockchain use cases that can be found and accepted, despite the fact that there are several protocols and consortiums supporting it.
- Mostly because to a lack of knowledge, resources, ability to handle the complexity that already exists, and countless other problems. What are the primary limitations limiting blockchain's potential then?

☞ Complexity of Blockchain

- The network's intricacy is what gives blockchain its charm. The greater the number of participants involved in a transaction, the more widely applicable the blockchain will be.
- Due to the fact that there were initially so few nodes running the blockchain, many PoCs were completely impractical in terms of cost-effectiveness and operationality.
- Additionally, the majority of companies and banks are now utilising blockchain in limited ways. Entities have used a mixed strategy rather than adopting a totally centralised or decentralised strategy.
- This significantly increases complexity. Even though their current applications are minor, additional businesses must deploy specialised blockchain expertise.

- Secondly, it is difficult to easily replicate a blockcha application across different activities and use-cases. Eac application requires a better comprehension of the operation requirements, and blockchain might be very different fo applications like land records and insurance contracts.

☞ Network size

- Blockchains (like other distributed systems) are "antifragile in the sense that they respond to attacks by becoming mor robust, rather than being particularly resistant to maliciou actors.
- But to do that, you need a lot of users. To fully benefit from blockchain, a network must be stable and have a grid of node that is broadly spread.

☞ Lack of speed

- The requirement to accelerate processing rates is anothe significant issue that has to be addressed. The networ typically slows down as the number of users rises, makin transactions take longer to process.
- Large transaction costs might come from this, which woul make the technology less and less appealing. Additionally, th system's encryption may slow it down even more. transaction may take several hours, or even days, to complete.
- Therefore, it works well for conducting significant transaction where timing is not a key consideration. This difficulty wit blockchain adoption might soon present a barrier.

☞ Lack of standardization

- The absence of standards is a fourth problem preventing more widespread use of blockchain technology.
- To achieve a scalable acceptance of any technology over th world, standards are necessary. For the blockchain technolog to function across all networks, they must all speak the same language in order for the transaction to be understood and completed.
- However, this is a problem with all new technology at the beginning until standards eventually improve with time and practise.

☞ Lack of interoperability

- As more companies began adopting blockchain, there is a tendency for many of them to create their own systems with unique features (governance rules, blockchain technology versions, consensus models, etc.).
- Most of these distinct blockchains do not interact with one another, and there is presently no global standard to let various networks to communicate to one another.
- Interoperability between blockchain networks refers to the capacity to share, see, and access data without the intervention of a middleman or centralised authority.
- Due to this lack of compatibility, broad adoption may be all but impossible.

☞ Unavoidable security flaw

- Bitcoin and other blockchains have one significant security flaw: if more than 50% of the computers acting as nodes to serve the network report a fraud, the lie will be accepted as the truth.
- When Satoshi Nakamoto created bitcoin, he highlighted this so-called "51 percent attack."
- Because of this, the community actively monitors bitcoin mining pools to make sure no one unintentionally gets such network dominance.

☞ Lack of privacy

- An added challenge with the blockchain is privacy.
- The transparency that results from having a record of a network's transaction history that is accessible to the public and simple to verify is one of the biggest advantages of blockchain technology, and public blockchain networks in particular.
- This is not always seen positively, though, as it also puts users' or organisations' privacy at risk. Many businesses that deal with privacy need to have clear guidelines.
- Businesses are hesitant to use some of the most well-known blockchain protocols because they want to preserve their trade secrets and other sensitive information.

☞ High Energy Consumption

- One of the most well-known and original uses of the blockchain is bitcoin. Every node that is a member of the blockchain network has to have 200 GB of storage space available for the Bitcoin Core.
- A daily 5 GB upload and 500 MB download is one of the criteria. Certainly, many nations need to modernise their infrastructure significantly before using blockchain.
- Energy use continues to be a major problem for miners in the context of the Bitcoin blockchain. According to studies conducted by the University of Cambridge, Bitcoin uses more energy than the whole country of Switzerland.
- The energy is mostly used to maintain the continuous operation of the whole network. Imagine the situation if there were many more similar networks because there is only one blockchain at now.

☞ Scalability Issues

- Another potential problem and limitation for many blockchain applications is scalability. Compare Visa, the largest centralised payment system, with Bitcoin, the largest cryptocurrency payment system.
- The maximum speed of Bitcoin is 7 transactions per second, but Visa can perform 65,000 transactions per second.
- In a centrally controlled architecture, the controlling authority determines the flow and doesn't needlessly inform other peers about a transaction. This expedites and saves time.
- Because a majority of nodes must approve the transaction in a blockchain architecture, validation might take several minutes.

☞ Politics

- There have been many possibilities for public arguments between various community sectors since blockchain protocols provide a chance to digitise governance models and because miners are effectively building another sort of incentive governance model.

- The issue or event of "forking" a blockchain, which entails altering the blockchain protocol after a majority of a blockchain's users have approved it, is where these differences, which are a significant aspect of the blockchain sector, are most visibly expressed.
- These discussions, albeit occasionally controversial and extremely technical, are instructive for anybody curious in the mix of democracy, consensus, and novel options for governance experimentation that blockchain technology is enabling.

2.9 BLOCKCHAIN ADOPTION SO FAR

GQ. Comment on various hurdle in adoption of blockchain technology by industry.

GQ. What can be the problems of blockchain technology adoption by finance sector?

GQ. What do you think, which limitations of blockchain are major hurdles in its adoption?

GQ. Are Interoperability and standardization are major roadblocks in blockchain adoption? Comment.

- Blockchain ecosystems require widespread acceptance in order to function well. The efficiency and scalability of blockchains will be constrained without widespread adoption.
- Governments and other public organisations must actively assist the adoption of blockchain and DLTs by addressing the different hurdles.
- Organizations are increasingly joining together to create collaborative blockchain working groups in order to address shared problems and create universally beneficial solutions without disclosing confidential information.
- Numerous operational apps and projects that are in great working order already exist. The evolution of the blockchain will continue, as with any technical advancement.
- There could be difficulties, but they shouldn't be viewed as roadblocks.

- Industries adapting Blockchain are :
  (1) Automotive
  (2) Banking and financial services.
  (3) Government.
  (4) Healthcare and life sciences.
  (5) Insurance.
  (6) Media and entertainment.
  (7) Retail and consumer goods.
  (8) Telecommunications.
  (9) Travel and transport
  (10) Supply chain
  (11) Oil and gas
  (12) Manufacturing

Chapter Ends...

❑❑❑