Block Chain Technology Cryptography and HashTechnology

Dr. Siddhartha Roy

Content

- Definition of Block Chain
- Block Chain Technology
- Cryptography
  - Symmetric Key
  - Public key
- Hashing
  - Message Digest
- Digital Signature

Definition of Block Chain

- An immutable append-only ever-growing chain of data. Data once added cannot be deleted or modified later.
- Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

Basic cryptographic techniques behind blockchain technology

- **Hash Function:** Used to connect the “blocks” in a “chain” in a tamper-proof way
- **Digital Signature:** Digitally sign the data so that no one can “deny” about their own activities. Also, others can check whether it is authentic.

Message Digest

- Message Digest is procedure that maps input data of an arbitrary length to an output of fixed length
- Takes any arbitrarily sized string as input
- Input M: The message
- •**Fixed size output** (We typically use 256 bits in Blockchain)
- Output H(M): We call this as the message digest
- •**Efficiently computable**

Characteristics of Hash Function

- **Deterministic**
- Always yields an identical hash value for identical input data
- **Collision-Free**
- If two messages are different, then their digests also differ
- **Hiding**
- Hide the original message

More Characteristics on Hash function

- Hash functions are irreversible Given an x, it is easy to find $H(x)$. However, given an $H(x)$, **one cannot find** x
- It is **difficult to find** x and y, where $x \neq y$, but $H(x)=H(y)$
- For a 256 bit hash function, the attacker needs to compute 2128 hash operations –this is significantly time-consuming
- If every hash computation takes only **1 microsecond**, it will need ~1025years

- If $H(x)=H(y)$, => $x=y$
- We need to remember just the hash value rather than the entire message – we call this as the **message digest**
- To check if two messages x and y are same, i.e., whether x=y, simply check if H(x)=$H(y)$
- This is efficient because the **size of the digest is significantly less than the size of the original messages**
- SHA256 is used in Bitcoin mining –to construct the Bitcoin blockchain

Basic concept of Cryptography

- **Symmetric Cryptography:**

- **Single Key: Symmetric cryptography, also known as secret-key or private-key cryptography, uses a single secret key for both encryption and decryption.**
- **Efficiency: It is generally faster and more computationally efficient than asymmetric cryptography because of the simplicity of the algorithms involved.**
- **Key Distribution: The main challenge is secure key distribution. If two parties want to communicate securely, they must somehow exchange the secret key without it being intercepted.**
- **Example: In symmetric encryption, a common algorithm is the Advanced Encryption Standard (AES), where the same key is used for both encryption and decryption.**

Public Key Cryptography

- Key Pair: Asymmetric cryptography, also known as public-key cryptography, uses a pair of keys: a public key and a private key.
- Encryption and Decryption: The public key is used for encryption, and the private key is used for decryption. Messages encrypted with the public key can only be decrypted by the corresponding private key and vice versa.
- Key Distribution: Asymmetric cryptography addresses the key distribution problem present in symmetric cryptography. Each participant has a public key that they can share openly, but their private key must be kept secret.

Public Key Cryptography

- •The key should be of sufficient length –increasing the length makes the key difficult to guess
- •The key should contain sufficient entropy, all the bits in the key should be equally random
- •**Encryption:** The key is used to convert a plain-text to a cypher-text; $M'=E(M,k)$
- •**Decryption:** The key is used to convert the cypher-text to the original plain text; $M=D(M',k)$

Public Key Encryption –RSA

- Invented in 1978 by Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman
- The encryption key is public and decryption key is kept secret (private key)
- Anyone can encrypt the data
- Only the intended receiver can decrypt the data

- Comparison:
- Security: Asymmetric cryptography provides a higher level of security in terms of key distribution and protecting communication channels.
- Efficiency: Symmetric cryptography is generally more efficient for bulk data encryption due to its computational simplicity.
- Key Management: Symmetric cryptography requires secure key distribution, which can be challenging, while asymmetric cryptography simplifies key management.

Digital Signature

- A **digital signature** is used to authenticate an electronically transmitted document
- **Purpose of Digital Signature**
- Only the **signing authority** can sign a document, but everyone can verify the signature
- Signature is **associated with** the particular document
- Prevent *non-repudiation* –sender will not be able to deny about the origin of the document