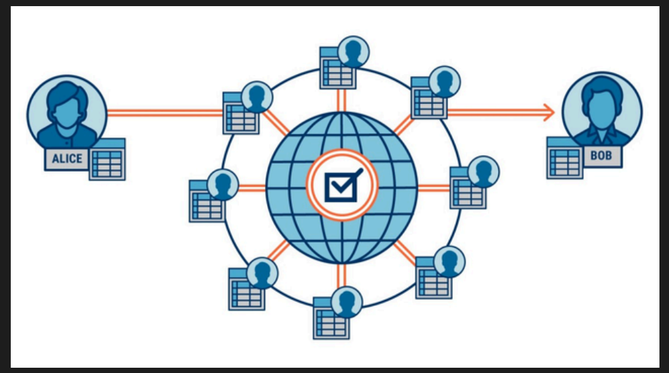
Cryptography

Vathna.lay@cadt.edu.kh

The challenge of Security



- If everything is decentralized and everyone has a copy of the data, is it secured?
- In decentralized systems like blockchain, data is shared across all participants (nodes). Without central control, how can we ensure that data is protected from tampering or fraud?

Cryptography

- Cryptography is the practice of secure communication techniques that allow only the sender and intended recipient to view the content of the message

Key Functions of Cryptography

Confidentiality

Integrity

Authentication

Non-repudiation

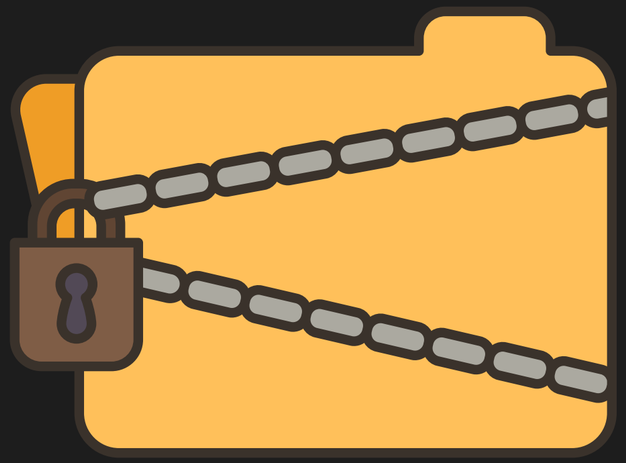
Crytography

- **Confidentiality:** Data is encrypted so that only authorized participants can read it.
- **Integrity:** Cryptographic hash functions ensure that data cannot be altered without detection.
- **Authentication:** Public and private keys verify the identity of users and validate transactions
- **Non-repudiation:** Digital signatures ensure that a transaction or message cannot be denied by the sender

Cryptography in Blockchain

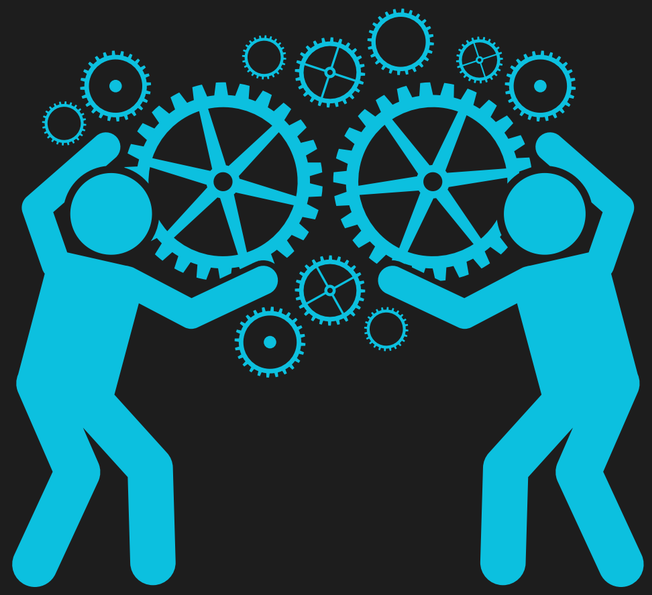
- In blockchain, cryptography ensure that
  - Data is kept secure
  - Transactions can occur between participants without the need of a trusted intermediary

Confidentiality (Keep data private)



- Only authorized participants should be able to read sensitive information
- In blockchain, confidentiality is archived using cryptographic techniques that ensure only the intended recipient can access the data

Integrity (Preventing Data Tempering)

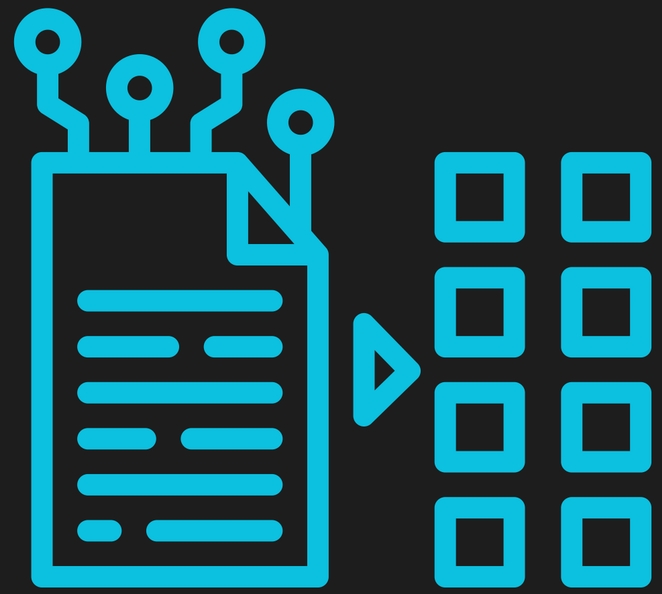


- Data must remain unchanged from the time it was sent to when it’s received.
- Cryptographic hashing ensure that any changes to data are detectable safeguarding the integrity of information on the blockchain

Authentication (Verify Data Origins)

- Ensuring that the data or transaction is from the expected sender
- Authentication methods use cryptographic techniques to verify that data was sent by the rightful participant, without the possibility of impersonation

Cryptographic Hash Functions



- A Cryptographic hash function converts input data into a fixed-length string of characters, called a hash.
- Hashing ensure that any attempt to change the data in the blockchain is immediately detectable because even a tiny change in the input drastically alters the output hash.

Secureing Decentralized Systems

- Cryptography is critical for ensuring that data in decentralized systems is both secure and trustworthy, despite the lack of a central authority.
- By using cryptographic techniques, blockchain enables participants to engage in secure transactions and share data without compromising trust.

MCQ

What is the main purpose of cryptography in blockchain technology?

A) To slow down the processing of transactions

B) To ensure the security and integrity of data in a decentralized system

C) To centralize the control of blockchain data

D) To create new blocks automatically without validation

MCQ

Which of the following is NOT a core principle of cryptography?

A) Confidentiality

B) Integrity

C) Availability

D) Authentication

MCQ

How does cryptography ensure data integrity in blockchain?

A) By using hash functions to detect any changes in the data

B) By encrypting data so only authorized users can view it

C) By allowing only one central entity to control the data

D) By distributing data across all nodes in the network

MCQ

What does confidentiality in cryptography refer to?

A) The ability to make data accessible to everyone

B) The process of verifying the identity of the sender

C) The ability to ensure that data is only accessible to authorized participants

D) The method of sharing encryption keys with all network participants

MCQ

Which cryptographic technique is primarily used to verify the integrity of data in blockchain?

A) Symmetric encryption

B) Cryptographic hash functions

C) Digital signatures

D) Public and private keys

MCQ

Why is cryptography essential for a decentralized system like blockchain?

A) It allows central authorities to access and manage data.

B) It secures data and transactions, even in a system without a central authority.

C) It limits the number of participants in the network.

D) It enables the use of passwords for transaction validation.

MCQ

What happens when even a small change is made to the data that has been hashed?

A) The hash remains the same.

B) The original data is automatically restored.

C) A completely different hash value is generated.

D) The blockchain automatically adds another block.

MCQ

In cryptography, authentication refers to?

A) Encrypting data so that only authorized people can read it.

B) Ensuring that the data has not been altered since it was sent.

C) Verifying that the data or transaction originates from a legitimate source.

D) Sharing data among all users in a network.

MCQ

Which of the following best describes the role of cryptographic hash functions in blockchain?

A) To encrypt data before it is shared across the network.

B) To produce a fixed-length string that represents the data, making it easy to detect any changes.

C) To generate a private key for every transaction.

D) To allow participants to modify the transaction history.

MCQ

What makes blockchain tamper-proof?

A) The ability of participants to easily edit blocks

B) The use of cryptography, including hashing and encryption, which makes it nearly impossible to alter data once added

C) The central control of the blockchain

D) The reliance on government regulation

Conclusion

After a natural disaster, a platform is set up to collect donations from around the world. A central authority manages all the funds and decides how and when to distribute them to affected areas.

Question: Would a centralized or decentralized system be better for managing disaster relief funds to ensure transparency and fairness? Why?