Understanding Hashing in Blockchain

Vathna.lay@cadt.edu.kh

Step 1: Understanding Hashing (SHA-256)

- What is the purpose of hashing in cryptography?
- What do you notice about the length of the hash, regardless of the input string's length?
- How does a small change in the input affect the hash input?

Write a conclusion explaining how cryptographic hashes ensure that even small changes in data are easily detectable. Why is this important for secure communication and data integrity?

Step 2: Define the Block Class

- Why do we need to calculate a hash for each block in the blockchain?
- What role does the previous hash play in ensuring the security of the blockchain?
- What data should be included when calculating the hash for a block, and why?

Summarize the role of the block’s hash and how it contributes to the integrity and security of each block in the blockchain.

Step 3: Create the Blockchain Class

- Why do we start the blockchain with a genesis block? What is its significance?
- How does linking each block to the hash of the previous block create a chain?
- What happens to the blockchain when a new block is added?

Explain how the structure of the blockchain (with each block containing the previous block's hash) ensures that the entire chain is secure and tamper-evident.

Step 4: Display the Blockchain

- What does each block in the blockchain store? Why is it important to store both the current and previous hash?
- How does displaying the blockchain help us verify its integrity?
- What could potentially go wrong if the previous hash were incorrect?

Write a conclusion on how displaying the blockchain reveals the structure and the linked nature of each block. How does this help in detecting tampering or invalid data?

Step 5: Tamper with a Block

- What happens to the blockchain when you tamper with the data in one block?
- Why do all subsequent blocks become invalid when one block's data is changed?
- How would tampering impact real-world blockchain applications, like cryptocurrencies?

Summarize the importance of cryptographic hashes in preventing tampering. Discuss how the entire blockchain is affected when data in one block is modified, and why this makes blockchain technology secure.