Cryptographic Principles: The Foundation of Blockchain Technology

Welcome to Unit 4 of FINTECH AND FINANCIAL ANALYTICS: BLOCKCHAIN TECHNOLOGY. Today, we will explore the core concepts of cryptography, the backbone of blockchain security and integrity.

DK **Dr. Maharajan K**

Recap: Fintech and Financial Analytics - Unit 3

Introduction to Blockchain Technology

We discussed the fundamentals of blockchain, including its core concepts, architecture, and key characteristics.

Blockchain Applications in Finance

We explored various use cases of blockchain in financial services, such as payments, trading, and asset management.

Guess the Topic: Cryptographic Principles

Security

Cryptography protects sensitive information from unauthorized access and tampering.

Identity

Cryptography is used to verify and authenticate digital identities in blockchain transactions.

Decentralization

Cryptography enables secure and transparent data storage and sharing in decentralized systems.

Importance of Cryptography in Blockchain Technology

Data Integrity

Cryptography ensures data cannot be altered without detection, maintaining the integrity of transactions.

Transaction Security

Cryptography secures transactions from unauthorized access and manipulation, protecting financial information.

User Privacy

Cryptography allows for anonymous transactions, protecting user identity and data privacy.

Fundamentals of Cryptography: Encryption, Decryption, and Hash Functions

Encryption

The process of converting plain text into an unreadable code, securing data during transmission and storage.

Decryption

The process of converting an encrypted message back into plain text, allowing authorized users to access data.

Hash Functions

Mathematical functions that generate a unique fingerprint of data, ensuring data integrity and authenticity.

Real-Life Cases: Cryptography in Payments, Identity Management, and Supply Chain

Payments

Cryptographic techniques secure online transactions, protecting financial information and preventing fraud.

Identity Management

Cryptography enables secure digital identity verification and authentication, enhancing trust and security.

Supply Chain

Blockchain and cryptography track goods and materials, enhancing transparency and reducing counterfeiting.

Cryptographic Algorithms: Symmetric, Asymmetric, and Hashing

1

Symmetric Key

Uses the same key for encryption and decryption, efficient but requires secure key sharing.

2

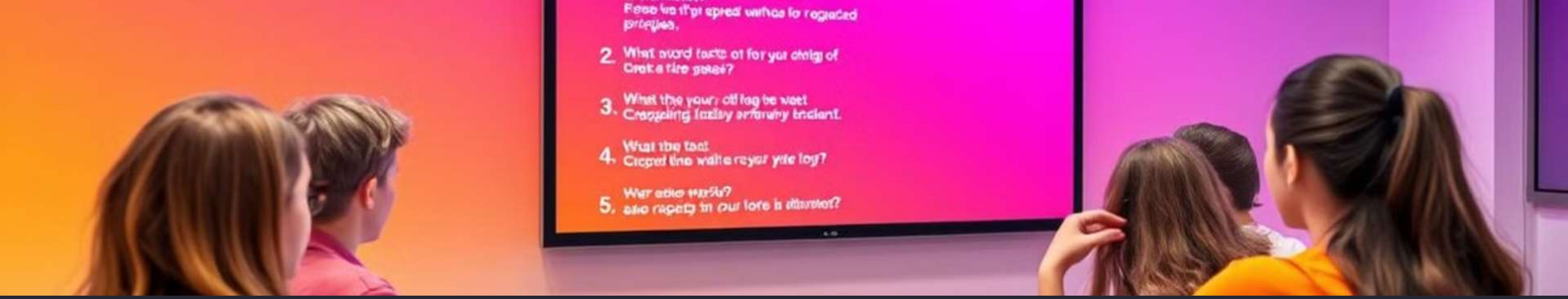
Asymmetric Key

Uses a pair of keys, one for encryption and the other for decryption, ensuring secure communication.

3

Hashing Algorithms

Generate unique fingerprints of data, ensuring data integrity and authenticity, resistant to tampering.



Student Learning Assessment: Cryptographic Principles Quiz

1

Encryption

What type of encryption uses the same key for both encryption and decryption?

2

Hash Functions

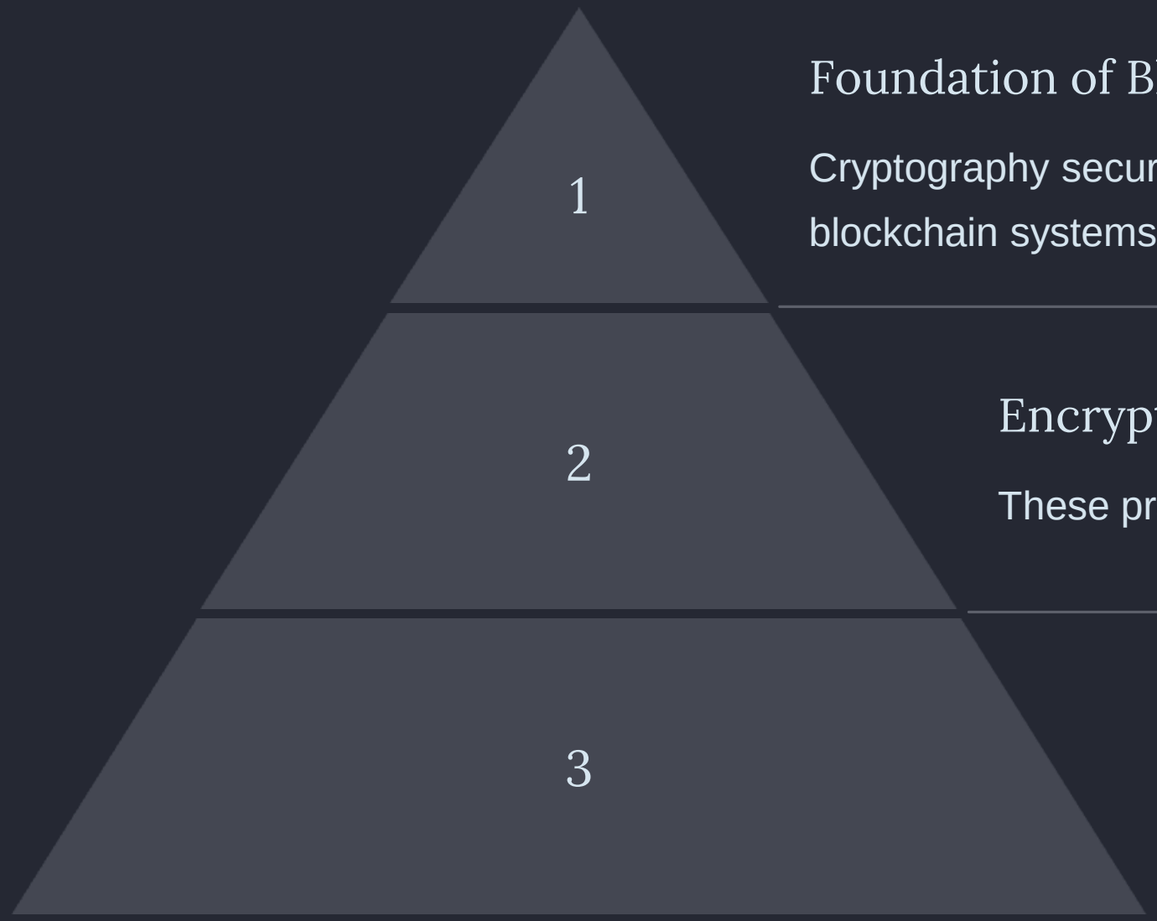
What is the primary function of a hash function in blockchain technology?

3

Asymmetric Key

What type of encryption uses a pair of keys, one for encryption and the other for decryption?

Summary: Key Takeaways on Cryptographic Principles



Foundation of Blockchain

Cryptography secures transactions, protects data, and enables trust in blockchain systems.

Encryption and Decryption

These processes ensure secure data transmission and storage.

Hash Functions

These functions guarantee data integrity and authenticity.

References: Online Resources and Recommended Textbooks

Stay tuned for the next session where we will delve into the fascinating world of consensus mechanisms!