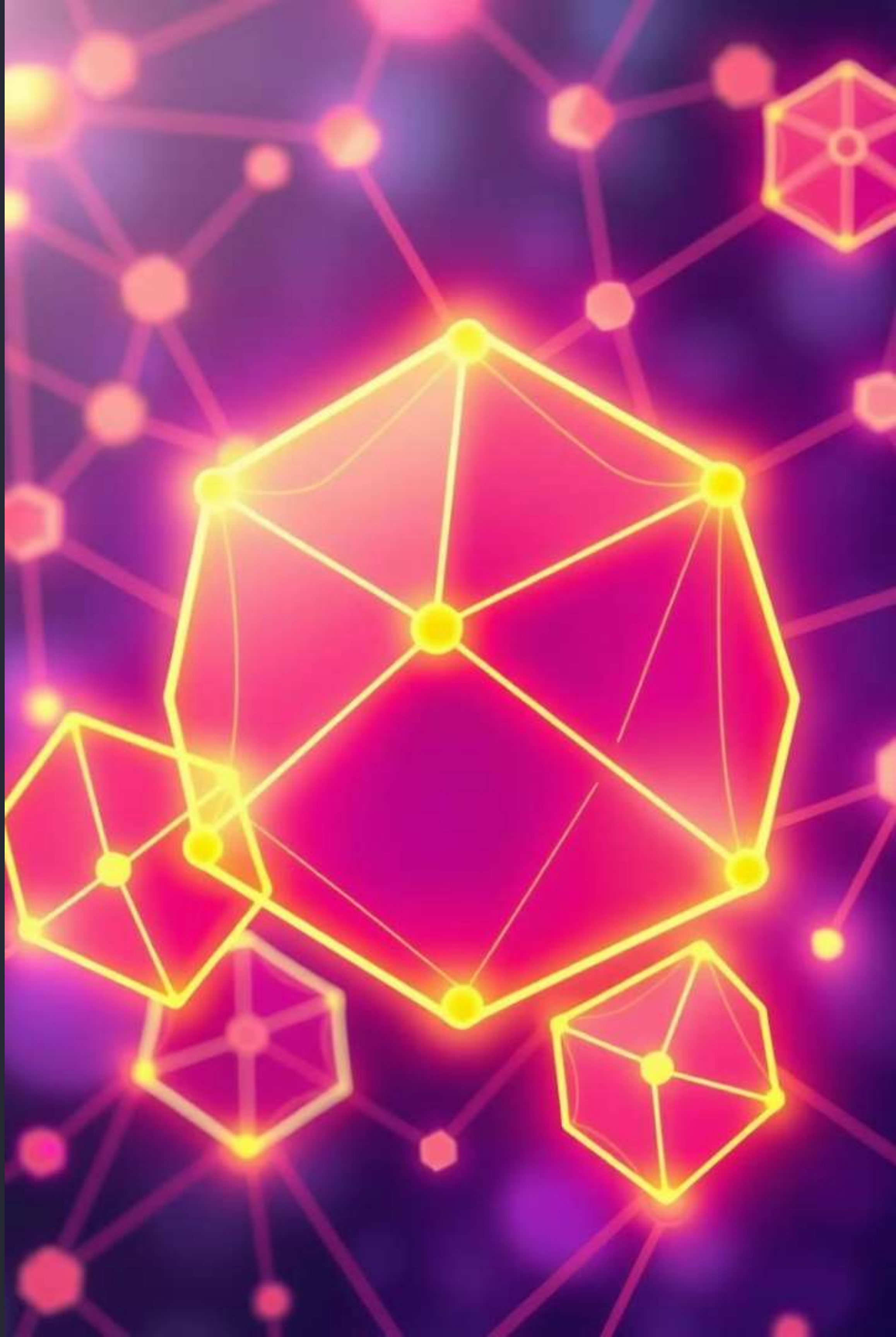
Crypto Primitives: Building Blocks of Blockchain Security

Welcome to Unit 4 of our Fintech and Financial Analytics course. Today, we'll delve into the foundational elements of blockchain security: crypto primitives. These fundamental cryptographic concepts are essential for understanding how blockchain technology works and its implications for the future of finance.

DK Dr. Maharajan K



Recap: Essential Blockchain Concepts

Decentralized Networks

Blockchains are distributed networks without a central authority, enabling trust and transparency.

Immutability

Once a block is added to the chain, it cannot be altered, guaranteeing data integrity and security.

Smart Contracts

Automated agreements executed on the blockchain, enabling trustless interactions and facilitating various financial applications.

Guess the Topic: Blockchain Applications

Digital Assets

Cryptocurrencies, NFTs, and other digital assets leverage blockchain technology for secure ownership and transfer.

Supply Chain Transparency

Blockchain tracks goods from origin to destination, improving transparency and efficiency in global trade.

Healthcare Records

Securely storing and sharing patient data on the blockchain improves data privacy and interoperability.

Identity Management

Blockchain enables decentralized identity systems, empowering individuals to control their own data and verify identities.

Fundamentals of Cryptography

Confidentiality

Ensuring only authorized parties can access sensitive information.

Integrity

Protecting data from unauthorized modification or corruption.

Authentication

Verifying the identity of parties involved in a transaction or communication.

Non-repudiation

Preventing parties from denying their involvement in a transaction or action.

Hash Functions and Digital Signatures

Hash Function

A one-way mathematical function that converts data into a unique and fixed-length hash value.

Digital Signature

Uses a hash function and private keys to create a unique signature for a document, verifying its authenticity and integrity.

Asymmetric and Symmetric Encryption

Symmetric Encryption

Uses the same key for both encryption and decryption, requiring secure key exchange.

Asymmetric Encryption

Uses separate keys for encryption and decryption, enabling secure communication without key sharing.

Real-World Case Study: Cryptocurrency Transactions

1

Transaction Initiation

User initiates a cryptocurrency transfer from a digital wallet.

2

Hashing and Signing

The transaction data is hashed and signed using the user's private key.

3

Broadcast and Validation

The transaction is broadcast to the network and validated by miners.

4

Block Addition

The validated transaction is added to a block and appended to the blockchain.

Exercises: Test Your Understanding

1

Hash Function

Describe the properties of a good hash function.

2

Digital Signature

Explain the purpose of a digital signature in blockchain security.

3

Encryption

Differentiate between symmetric and asymmetric encryption and their applications in blockchain.

Summary: Key Crypto Concepts Covered

1 Hash Functions

One-way mathematical functions ensuring data integrity and uniqueness.

2 Digital Signatures

Authenticating documents and verifying the sender's identity.

3 Encryption

Protecting sensitive information from unauthorized access.

References and Further Resources

1. Investopedia: Cryptography
2. Wikipedia: Cryptographic Hash Function
3. Coursera: Blockchain Specialization
4. "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World" by Don Tapscott and Alex Tapscott.