Introduction to Blockchain Technologies

Unit 3

Cryptocurrencies

Cryptographic Hash Functions-Cryptography Basics and Concepts-Introduction to Bitcoin-Bitcoin Network and Payments-Bitcoin clients and APIs-Alternative Coins

Cryptographic Hash Functions

1. **What**
    - A function that takes in any amount of data, converts it to a fixed-size string of characters (called a hash)
    - If even one character is changed, one gets a completely different hash
    - Similar to a digital fingerprint-unique, impossible to reverse-engineer back into the original data
    - Not only does it compress the data, also makes it tamper-proof

2. **How Cryptographic Hash Functions Work/Are Used in Blockchain**
    a. For Block Integrity
        - In blockchain, each block has a hash of the previous block embedded in it. This creates a chain of blocks that are cryptographically linked.
        - Changing one block, tampers with the whole sequence

    b. For Transaction Security
        - When one sends cryptocurrency, transaction data is hashed and then added to a block.
        - The hash guarantees that the transaction details like the amount and the recipient cannot be altered.
        - If altered, the hash changes, and the network immediately knows something has been messed with.

    c. For Proof of Work
        - In Proof of Work systems, cryptographic hash functions are what miners are solving to add new blocks to the blockchain.
        - Miners are in a race to find a has that fits certain criteria.
        - The first one to solve it gets to add the block and collect the reward.

- This concept makes blockchain secure, but that is also why PoW is a very energy hungry process. Solving these puzzles requires a lot of computational power, and that makes the system very hard to hack

3. **Importance of Cryptographic Hash Functions**
    - Are the bedrock of blockchain's security and integrity. Without it, blockchain would be no better than a regular database, vulnerable to the usual hacks and fraud.
    - Hash functions make sure that the data on a blockchain is unchangeable and trustworthy.
    - Apart from blockchain, hash functions are also used for securing passwords, verifying digital signatures, and ensuring data has not been tampered with.

Cryptography: Basics and Concepts

1. **What**
    - Science of encoding information so that only the intended recipient can decode it.
    - Also about proving identity, ensuring data integrity, and enabling secure communicatio

2. **Encryption and Decryption**

a. Encryption
    - Process of converting plaintext into ciphertext using an algorithm and a key
    - Strength of encryption depends on the complexity of the algorithm and the secrecy of the key.

Types of encryption

Symmetric Encryption

➔ Same key is used for both encryption and decryption.
➔ Fast and efficient, but has the downside of both parties needing to have the same key. One would need to find a secure way to share the key without anyone else getting their hands on it.

Asymmetric Encryption

➔ Uses both a public key (anyone can see) and a private key (only recipient holds and uses it to decrypt the data)
➔ Eliminates the need to share a secret key beforehand

b. Decryption
   Converting the ciphertext back into plaintext using a corresponding key

3. Other Concepts

a. Hashing- A process that takes input data and produces a fixed size string of characters, which is a unique representation of the data. Used for verifying data integrity, if even a single bit of the input data changes, the resulting hash will become completely different, making it easy to detect tampering.
b. Digital Signatures-Meant to serve as proof that a document was created by the intended individual and hasn't been altered since/isn't from an imposter. These signatures are created using a combination of hashing and symmetric key encryption.

c. Public Key Infrastructure (PKI)- a framwork that makes asymmetric encryption and digital signatures work on a large scale. It is a system of digital certificates, certificate authorities and other registration authorities that verify and communicate the identify of individuals/entities involved in digital communications. PKI is the foundation for SSL/TLS, which are the protocols that keep web browsing secure. PKI is also a fundamental part of blockchain technology.

Introduction to Bitcoin

1. What

- First decentralized cryptocurrency
- Not answerable to banks/government/middlemen
- Money for the people, by the people managed by a global network of computers all working together to maintain the Bitcoin blockchain
- Has a public, unchangeable ledger of every Bitcoin transaction ever made

2. Features of Bitcoin

- Bitcoin doesn't require trust
- Traditional financial systems rely on banks and institutions to keep everything running securely.
- Bitcoin replaces that with cryptographic proof and decentralized consensus.
- Peer to peer cash network that is controlled by code
- Has a limited supply- 21 million bitcoins will only ever exist- a number that is hard-coded into the system

- Every 4 years, the reward for mining new blocks is cut by half- process is called halving- this makes Bitcoin increasingly scarce over time.
- Secure, transparent and irreversible transaction- once a transaction is done, it cannot be altered or undone.
- No one has to be trusted to use Bitcoin, one only needs to trust the network and the code.

3. **Origins of Bitcoin**
    - Invented by Satoshi Nakamoto, introduced in a whitepaper 'Bitcoin: A Peer to Peer Electronic Cash System'
    - Came in 2009 following the 2008 financial crisis
    - Initially a fringe idea, something that only tech geeks and libertarians were interested in.
    - Currently has a trillion dollar market cap

4. **Working of Bitcoin**
    - Runs on blockchain technology, which is a chain of blocks, each containing transaction data.
    - Each block is linked to the one before it, creating an unbreakable chain that records every transaction ever made.
    - This blockchain is maintained by a decentralized network of miners- people who use powerful computers to validate transactions and add them to the blockchain in exchange for newly minted bitcoins.
    - This process is called mining- keeps Bitcoin secure and decentralized.

5. **Why Bitcoin is Important**
    - Bitcoins offers a model where the financial system is open, decentralized and accessible to anyone with an internet connection
    - Bitcoin is a hedge against inflation and government overreach. It is a way to store value outside the traditional financial system.
    - Provides a means for financial inclusion, giving people in unbanked regions access to the global economy.
    - Has been the catalyst for thousands of other cryptocurrencies
    - Have forced governments and financial institutions to rethink their approach to digital money
    - Can be used as a store of value, a medium of exchange, or a speculative asset

Bitcoin Networks and Payment

1. **About the Bitcoin Network**
    - A decentralized network
    - Powered by thousands of nodes- computers running the Bitcoin software- that work together to validate transactions and secure the network
    - These nodes maintain the Bitcoin blockchain, and the public ledger that records every transaction ever made
    - Since the Bitcoin network is decentralized, it is nearly impossible to take down
    - To disrupt Bitcoin, every single node would have to be taken down simultaneously, which is practically impossible
    - Network is very resilient compared to traditional systems

2. **Mining and Consensus in the Bitcoin Network**

    Backbone of the Bitcoin network: Consensus mechanism called Proof of Work (PoW).

    Role of Miners: Specialized nodes compete to solve complex mathematical puzzles.
        - The first to solve the puzzle adds the next block to the blockchain.
        - Miners are rewarded with newly minted bitcoins for their efforts.

    Consensus and Security:
        - Mining ensures the network is secure and decentralized.
        - The network is trustless—no need to trust a single entity, as the decentralized network guarantees system integrity.

    Decentralization:
        - No single authority verifies transactions.
        - Miners work together to reach consensus on the state of the blockchain.

3. **Features of Payments on the Bitcoin Network**

    a. **Bitcoin Payments: Fast, Secure, and Global**
        - Traditional finance is slow, expensive, and involves intermediaries for cross-border payments.
        - Bitcoin allows for fast, global payments at a fraction of the cost.
        - With Bitcoin, you can send money to anyone in the world in minutes.

    b. **How Payments Work**
        - Sending a Bitcoin payment broadcasts a message to the network to verify that the sender has enough funds.
        - Once confirmed by the network, the transaction is added to the blockchain, and the recipient receives the funds.
        - Bitcoin payments are irreversible—no chargebacks or disputes, making finality both a strength and a challenge.

c. **Global and Borderless**
   - Bitcoin operates without traditional banking systems and borders, allowing for direct, fast, and cheap transactions.
   - It's a game-changer for unbanked or underbanked populations.
   - Anyone with a smartphone and an internet connection can participate in the global economy without needing a bank account.
   - This level of financial inclusion is unmatched by traditional financial systems.

4. **Impacts of Bitcoin on Traditional Payments**
   - Bitcoin's payment system challenges the centralized systems traditionally used for financial transactions.
   - Demonstrates that a decentralized, peer-to-peer network can be just as efficient, if not more so, than centralized systems.

   Disintermediation
   - One of Bitcoin's most disruptive features is disintermediation, the removal of intermediaries such as banks, payment processors, and card networks.
   - Traditional finance involves multiple intermediaries, each adding friction, costs, and potential failure points to transactions.
   - Bitcoin transactions are peer-to-peer, reducing costs, speeding up transactions, and lowering the risk of fraud by eliminating middlemen.

   Challenges and Opportunities
   - Bitcoin's volatility limits its effectiveness as a stable store of value for everyday transactions.
   - Transaction fees can fluctuate, sometimes spiking during periods of high network activity.
   - Scalability is another concern—Bitcoin can only process a limited number of transactions per second, which could pose a bottleneck as adoption increases.
   - However, these challenges also present opportunities. Solutions such as the Lightning Network, a second-layer protocol, are being developed to improve Bitcoin's transaction capacity, reduce fees, and enhance scalability, making the system more efficient and user-friendly as it evolves.

Bitcoin Clients and APIs

1. **Types of Bitcoin Clients**

   Full Nodes
   - Full nodes download the entire Bitcoin blockchain and independently verify every transaction.
   - They are considered the gold standard for security and privacy, as they do not rely on third parties.

- Full nodes require significant resources—storage, bandwidth, and computing power.
- Ideal for users who prioritize full control over their transactions, but the resource demands are a drawback.

Lightweight Clients
- Lightweight clients do not download the entire blockchain but instead focus on essential parts, making them faster and less resource-intensive.
- They rely on full nodes for verification, which involves placing some trust in the network.
- The main benefit is convenience, especially for mobile device users, as they offer a good balance between functionality and resource efficiency.

Mobile and Web Wallets
- Mobile and web wallets are user-friendly applications that make Bitcoin accessible to the masses.
- These wallets are easy to use but often rely on third-party services for network interaction.
- While they offer less security compared to full or lightweight clients, they are preferred for quick, everyday transactions due to their simplicity and convenience.

2. **APIs for Developers**
   - APIs (Application Programming Interfaces) are tools that allow developers to create new services on top of the Bitcoin network.
   - They are essential in expanding Bitcoin from niche technology to a global financial system.

   Wallet APIs
   - Wallet APIs enable developers to create and manage Bitcoin wallets programmatically.
   - Functions include generating addresses, sending/receiving transactions, and checking balances.
   - Businesses can easily integrate Bitcoin into their operations, from small shops to large e-commerce platforms, with minimal complexity.

   Blockchain APIs
   - Blockchain APIs provide direct access to the entire Bitcoin blockchain.
   - These APIs allow developers to query transaction histories, track specific transactions, and build custom analytics tools.
   - They are critical for services requiring detailed insights into Bitcoin activity, such as block explorers and crypto exchanges.

   Payment Gateway APIs
   - Payment gateway APIs handle Bitcoin commerce by managing processes like converting Bitcoin to local currencies and processing payments.

- They simplify Bitcoin transactions, making it as easy to accept Bitcoin as traditional credit card payments.

Exchange APIs

- Exchange APIs offer access to market data, allowing users to buy and sell orders.
- They enable complex trading strategies and are vital for building trading bots or portfolio management tools.
- Exchange APIs serve as the backbone for traders by streamlining interactions with market data.

3. **Importance of Bitcoin Clients and APIs**
    - Without bitcoin clients, the average person would not be able to use Bitcoin
    - Without the APIS, the developers would not be able to build the tools and services that make Bitcoin useful.

Alternative Coins

1. **What**

    - Altcoins refer to any cryptocurrency that is not Bitcoin.
    - Bitcoin is likened to the first revolutionary product (e.g., the iPhone), which spurred the creation of numerous alternatives.
    - Altcoins emerged due to Bitcoin's success, with some aiming to improve on Bitcoin’s model, while others pursue entirely different goals.
    - Altcoins vary significantly, ranging from well-known ones like Ethereum and Litecoin to lesser-known niche coins.
    - Each altcoin offers distinct features, use cases, and communities.

2. **Why do Altcoins exist?**
    - Altcoins focus on innovation and competition.
    - Bitcoin was the first cryptocurrency but has limitations (e.g., it's slow, energy-intensive, and less flexible).
    - Altcoins aim to address these issues or cater to niche markets.
    -

    Improving on Bitcoin

    - Some altcoins improve on Bitcoin's flaws.
    - **Litecoin**: Faster, more efficient, shorter block times, and different hashing algorithm.
    - **Bitcoin Cash**: Created to handle more transactions by increasing block size.

    New Use Cases

    - Other altcoins serve different purposes rather than competing with Bitcoin.

- **Ethereum**: A platform for decentralized applications (dApps) using smart contracts. Focuses on computing, not just currency.
- **Ripple (XRP)**: Aimed at fast, low-cost international money transfers, used by banks rather than the general public.

3. **Altcoin Landscape**
   The altcoin space is diverse, dynamic, and chaotic, with thousands of coins, including legitimate innovations and scams.

   Ethereum and Smart Contracts
   - Ethereum is the leading altcoin, introducing smart contracts (self-executing contracts with predefined terms).
   - It has enabled decentralized finance (DeFi) and non-fungible tokens (NFTs), creating an entire ecosystem of blockchain innovation.

   Stablecoins
   - Stablecoins are pegged to stable assets (e.g., USD), providing less volatility than typical cryptocurrencies.
   - Useful for everyday transactions and as protection against market volatility.
   - **Tether (USDT)** is the most well-known stablecoin, but there are others.

   DeFi Tokens
   - Decentralized Finance (DeFi) is a major trend built mostly on altcoins.
   - DeFi platforms like Uniswap (UNI) and Aave (AAVE) use tokens for decentralized exchanges and financial services without relying on traditional banks.
   - DeFi tokens are increasingly popular as alternatives for financial interactions.

4. **Risks and Rewards of Altcoin**
   Altcoin Investment
   - High risk, high reward.
   - More volatile and less regulated than Bitcoin.
   - Susceptible to scams and rapid price changes.

   Opportunities
   - Altcoins offer early entry into game-changing technologies.
   - Innovation in consensus, privacy, and new use cases.
   - A space for experimentation.