Professional Certificate in Blockchain for Social Impact

Cryptocurrency Fundamentals

Cryptocurrency Fundamentals:

Blockchain:
A blockchain is a distributed ledger technology that enables the secure transfer of digital assets over a network of computers. It consists of a chain of blocks, each containing a list of transactions. These blocks are linked together in a chronological order, forming a chain. Each block is verified by network participants through a consensus mechanism before being added to the blockchain.

Bitcoin:
Bitcoin is the first and most well-known cryptocurrency. It was created in 2009 by an unknown person or group of people using the pseudonym Satoshi Nakamoto. Bitcoin operates on a decentralized network without a central authority, allowing users to transact directly with one another without the need for intermediaries.

Ether:
Ether is the native cryptocurrency of the Ethereum blockchain. It is used to pay for transaction fees and computational services on the network. Ether can also be traded on cryptocurrency exchanges like other digital assets.

Cryptocurrency Wallet:
A cryptocurrency wallet is a digital tool that allows users to store, send, and receive cryptocurrencies. It consists of two keys – a public key for receiving funds and a private key for authorizing transactions. There are different types of wallets, including hardware wallets, software wallets, and paper wallets.

Decentralization:
Decentralization refers to the distribution of power and control among network participants rather than a single entity. Cryptocurrencies are decentralized by design, meaning that no central authority has control over the network. This makes them resistant to censorship and manipulation.

Consensus Mechanism:
A consensus mechanism is a protocol used to achieve agreement among network participants on the validity of transactions. Popular consensus mechanisms in blockchain networks include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS).

Smart Contracts:
Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They automatically enforce the terms of the contract without the need for intermediaries. Smart contracts

are a key feature of blockchain platforms like Ethereum.

Initial Coin Offering (ICO):
An Initial Coin Offering (ICO) is a fundraising method in which a new cryptocurrency project sells a percentage of its tokens to early investors in exchange for funding. ICOs became popular in the cryptocurrency space as a way to raise capital for new projects.

Tokenization:
Tokenization is the process of converting real-world assets into digital tokens on a blockchain. These tokens represent ownership of the underlying asset and can be traded or transferred easily on the blockchain.

Decentralized Finance (DeFi):
Decentralized Finance (DeFi) refers to a movement that aims to recreate traditional financial systems using blockchain technology. DeFi applications allow users to lend, borrow, and trade assets without the need for intermediaries like banks.

Mining:
Mining is the process of validating transactions and adding new blocks to the blockchain. Miners use computational power to solve complex mathematical puzzles and compete to be the first to add a new block. In return, they are rewarded with newly minted coins and transaction fees.

Fork:
A fork occurs when a blockchain splits into two separate chains due to a change in the protocol. There are two types of forks – hard forks, which are not backward compatible, and soft forks, which are backward compatible.

Wallet Address:
A wallet address is a unique identifier used to receive cryptocurrencies. It consists of a string of alphanumeric characters and is similar to a bank account number for traditional currencies.

Private Key:
A private key is a secret code that allows users to access their cryptocurrency holdings. It should be kept secure and never shared with others to prevent unauthorized access to funds.

Public Key:
A public key is a cryptographic key that is used to receive funds in a cryptocurrency wallet. It is derived from the private key and can be shared with others to receive payments.

Altcoin:
An altcoin is any cryptocurrency other than Bitcoin. There are thousands of altcoins in existence, each with its own unique features and use cases. Examples of popular altcoins include Ethereum, Ripple, and Litecoin.

Stablecoin:

A stablecoin is a type of cryptocurrency that is pegged to a stable asset like fiat currency or a commodity. Stablecoins are designed to minimize price volatility and provide a reliable store of value.

Cryptocurrency Exchange:
A cryptocurrency exchange is a platform that allows users to buy, sell, and trade cryptocurrencies. Exchanges can be centralized or decentralized and offer a wide range of digital assets for trading.

Market Capitalization:
Market capitalization is a measure of a cryptocurrency's total value in circulation. It is calculated by multiplying the current price of a coin by the total number of coins in circulation. Market capitalization is used to rank cryptocurrencies by their relative size.

Proof of Work (PoW):
Proof of Work (PoW) is a consensus mechanism used in blockchain networks like Bitcoin. It requires miners to solve complex mathematical puzzles to validate transactions and add new blocks to the blockchain. PoW is energy-intensive but has been proven to be secure.

Proof of Stake (PoS):
Proof of Stake (PoS) is an alternative consensus mechanism to PoW. In PoS, validators are chosen to create new blocks based on the number of coins they hold. PoS is more energy-efficient than PoW but has its own set of challenges.

Wallet Seed Phrase:
A wallet seed phrase is a list of words used to back up and restore a cryptocurrency wallet. It is essential to store the seed phrase securely as it can be used to recover access to the wallet in case of loss or theft.

Double Spending:
Double spending is a potential issue in digital currencies where the same funds are spent more than once. Blockchain technology prevents double spending by recording every transaction in a transparent and immutable ledger.

Private Blockchain:
A private blockchain is a permissioned blockchain that restricts access to certain participants. It is often used by enterprises to build internal networks for specific use cases.

Public Blockchain:
A public blockchain is a permissionless blockchain that allows anyone to participate in the network. Bitcoin and Ethereum are examples of public blockchains that are open to all users.

Cryptocurrency Regulation:
Cryptocurrency regulation refers to the legal framework governing the use and trade of cryptocurrencies in different jurisdictions. Governments around the world are working to establish clear regulations to protect

consumers and prevent illegal activities.

Token Standards:
Token standards are protocols that define the rules and functionalities of tokens on a blockchain. Examples of token standards include ERC-20 for Ethereum tokens and TRC-20 for tokens on the Tron network.

Centralized Exchange:
A centralized exchange is a cryptocurrency trading platform that is operated by a single entity. Centralized exchanges hold users' funds in custody and facilitate trades on their platform.

Decentralized Exchange:
A decentralized exchange is a platform that allows users to trade cryptocurrencies directly with one another without the need for a central authority. Decentralized exchanges operate on smart contracts and provide greater security and privacy.

Token Swap:
A token swap is the process of exchanging one cryptocurrency for another at a predetermined ratio. Token swaps are often conducted during network upgrades or rebranding events.

Fiat Currency:
Fiat currency is government-issued currency that is not backed by a physical commodity like gold or silver. Examples of fiat currencies include the US Dollar, Euro, and Japanese Yen.

Security Token:
A security token represents ownership of a real-world asset like equity, debt, or real estate. Security tokens are subject to regulations and provide investors with rights and dividends.

Non-Fungible Token (NFT):
A non-fungible token (NFT) is a unique digital asset that cannot be replicated or exchanged for another token of equal value. NFTs are used to represent ownership of digital art, collectibles, and in-game assets.

Cross-Chain Interoperability:
Cross-chain interoperability refers to the ability of different blockchain networks to communicate and transfer assets between one another. Interoperability solutions like sidechains and atomic swaps enable seamless transactions across multiple blockchains.

Scaling Solutions:
Scaling solutions are technologies designed to improve the scalability and performance of blockchain networks. Solutions like sharding, layer 2 protocols, and off-chain scaling help to increase transaction throughput and reduce fees.

Governance:
Governance in blockchain networks refers to the decision-making process for protocol upgrades, changes,

and maintenance. Governance models vary between networks and can be decentralized, community-driven, or controlled by a foundation.

Oracles:
Oracles are third-party services that provide external data to smart contracts on the blockchain. Oracles are used to connect blockchain networks with real-world events and information, enabling the execution of complex contracts.

DApps:
DApps, or decentralized applications, are software applications that run on a blockchain network. DApps are designed to be transparent, secure, and censorship-resistant, providing users with full control over their data and assets.

Privacy Coins:
Privacy coins are cryptocurrencies that focus on enhancing the privacy and anonymity of transactions. Coins like Monero and Zcash use advanced cryptographic techniques to obfuscate sender and recipient information.

Cold Storage:
Cold storage refers to storing cryptocurrencies offline in a secure hardware device or paper wallet. Cold storage is considered more secure than hot wallets connected to the internet, as it reduces the risk of hacking and theft.

Custodial Services:
Custodial services are offered by third-party providers that hold and manage cryptocurrencies on behalf of their clients. Custodial services are common for institutional investors and individuals who prefer to outsource the security of their digital assets.

Tokenomics:
Tokenomics is the study of the economics and mechanics of token-based ecosystems. It encompasses token distribution, token utility, incentives, and governance mechanisms to create sustainable and thriving networks.

Proof of Authority (PoA):
Proof of Authority (PoA) is a consensus mechanism that relies on a group of approved validators to create new blocks. PoA is often used in private blockchain networks where trust among participants is established.

Token Burn:
A token burn is the process of permanently removing a portion of tokens from circulation. Token burns are often used to reduce token supply, increase scarcity, and create value for existing token holders.

Cross-Chain Bridge:

Cross-chain bridges are protocols that enable the transfer of assets between different blockchain networks. Bridges allow users to move tokens seamlessly across multiple chains, expanding the interoperability of the blockchain ecosystem.

Hash Function:
A hash function is a cryptographic algorithm that converts input data into a fixed-size string of characters. Hash functions are used in blockchain technology to secure transactions, create digital signatures, and generate unique identifiers.

Zero-Knowledge Proof:
Zero-Knowledge Proof is a cryptographic method that allows one party to prove to another party that they know a piece of information without revealing the actual data. Zero-Knowledge Proofs are used to verify transactions and authenticate users without disclosing sensitive information.

Immutable Ledger:
A immutable ledger is a record of transactions that cannot be altered or deleted once they are added to the blockchain. The immutability of blockchain ledgers ensures transparency, security, and trust in the network.

Token Swap:
A token swap is the process of exchanging one cryptocurrency for another at a predetermined ratio. Token swaps are often conducted during network upgrades or rebranding events.

Scalability:
Scalability is the ability of a blockchain network to handle increased transaction volume and activity without compromising performance. Scalability solutions like sharding and layer 2 protocols aim to improve the efficiency of blockchain networks.

Multi-Signature Wallet:
A multi-signature wallet is a type of cryptocurrency wallet that requires multiple private keys to authorize a transaction. Multi-signature wallets are used to enhance security and prevent unauthorized access to funds.

Interoperability:
Interoperability is the ability of different blockchain networks to communicate and share data seamlessly. Interoperability solutions enable cross-chain transactions and the transfer of assets between disparate networks.

Tokenization:
Tokenization is the process of converting real-world assets into digital tokens on a blockchain. These tokens represent ownership of the underlying asset and can be traded or transferred easily on the blockchain.

Decentralized Autonomous Organization (DAO):
A Decentralized Autonomous Organization (DAO) is an organization governed by smart contracts and

decentralized decision-making. DAOs operate without central control and enable participants to vote on proposals and allocate resources autonomously.

Atomic Swap:
An atomic swap is a peer-to-peer exchange of cryptocurrencies without the need for intermediaries. Atomic swaps use smart contracts to ensure that both parties fulfill their obligations simultaneously, reducing counterparty risk.

Gas Fees:
Gas fees are transaction fees paid by users to execute operations on the Ethereum blockchain. Gas fees are calculated based on the computational work required to process the transaction and prevent network congestion.

Layer 2 Scaling:
Layer 2 scaling solutions are protocols built on top of existing blockchains to improve scalability and reduce transaction costs. Layer 2 solutions like state channels and sidechains enable faster and cheaper transactions without compromising security.

Cross-Chain Swaps:
Cross-chain swaps are transactions that allow users to exchange assets between different blockchain networks. Cross-chain swaps enable interoperability and liquidity across multiple chains, enhancing the flexibility of the blockchain ecosystem.

Sybil Attack:
A Sybil attack is a security threat in which an attacker creates multiple fake identities to gain control of a network. Sybil attacks can undermine the integrity of decentralized systems and are mitigated through identity verification and reputation systems.

Smart Contract Audit:
A smart contract audit is a process of reviewing and testing the code of a smart contract to identify vulnerabilities and security risks. Audit firms assess the integrity of smart contracts to ensure they function as intended and protect users' funds.

Token Vesting:
Token vesting is a mechanism that locks up a portion of tokens for a specified period before they are released to the holder. Token vesting is commonly used in token sales and employee incentives to align interests and prevent token dumping.

Cross-Chain Communication:
Cross-chain communication refers to the exchange of information and assets between different blockchain networks. Cross-chain communication protocols enable interoperability and data sharing across disparate chains, enhancing the connectivity of the blockchain ecosystem.

Blockchain Governance:
Blockchain governance is the process of making decisions and implementing changes to a blockchain network. Governance models define how decisions are made, conflicts are resolved, and upgrades are implemented in a decentralized manner.

Token Standardization:
Token standardization refers to the creation of common protocols and standards for issuing tokens on blockchain networks. Standardized token formats like ERC-20 and BEP-20 simplify token creation and interoperability across different platforms.

Cross-Chain Liquidity:
Cross-chain liquidity is the availability of assets for trading and exchange across multiple blockchain networks. Cross-chain liquidity solutions enable users to access a wide range of assets and markets without the need for centralized intermediaries.

Layer 1 Protocol:
A layer 1 protocol is the underlying blockchain network that defines the basic rules and functionalities of the system. Layer 1 protocols like Bitcoin and Ethereum provide the foundation for building decentralized applications and smart contracts.

Token Migration:
Token migration is the process of transferring tokens from one blockchain to another. Token migrations are often conducted during network upgrades, rebranding events, or to improve scalability and interoperability.

Cross-Chain Asset Transfer:
Cross-chain asset transfer is the movement of digital assets between different blockchain networks. Cross-chain asset transfer protocols enable users to swap tokens, assets, and data across disparate chains, enhancing the flexibility and utility of the blockchain ecosystem.

Blockchain Interoperability:
Blockchain interoperability is the ability of different blockchain networks to communicate and share data seamlessly. Interoperability solutions like cross-chain bridges and atomic swaps enable cross-chain transactions and the transfer of assets between disparate networks.

Token Locking:
Token locking is a mechanism that restricts the transfer or use of tokens for a specified period. Token locking is used to incentivize long-term holders, prevent market manipulation, and stabilize token prices.

Governance Token:
A governance token is a digital asset that grants holders the right to participate in the governance of a blockchain network. Governance tokens enable users to vote on proposals, suggest changes, and influence the development of the ecosystem.

Cross-Chain Token Swap:
Cross-chain token swap is a process that allows users to exchange tokens between different blockchain networks. Cross-chain token swaps enable interoperability and liquidity across disparate chains, providing users with more flexibility and options for asset management.

Layer 2 Solution:
An layer 2 solution is a scaling technique that processes transactions off-chain to reduce congestion on the main blockchain. Layer 2 solutions like state channels and sidechains improve transaction speed and reduce fees while maintaining security and decentralization.

Token Staking:
Token staking is the process of locking up digital assets in a wallet to support the operations of a blockchain network. Stakers are rewarded with additional tokens for securing the network and maintaining consensus.

Cross-Chain Bridge Protocol:
An cross-chain bridge protocol is a set of rules and procedures that enable the transfer of assets between different blockchain networks. Bridge protocols facilitate interoperability and liquidity across disparate chains, expanding the connectivity of the blockchain ecosystem.

Layer 1 Blockchain:
A layer 1 blockchain is the base protocol that defines the fundamental rules and functionalities of a blockchain network. Layer 1 blockchains like Bitcoin and Ethereum provide the infrastructure for building decentralized applications and smart contracts.

Token Swap Mechanism:
A token swap mechanism is a process that allows users to exchange one cryptocurrency for another at a predetermined rate. Token swap mechanisms are used during network upgrades, migrations, or rebranding events to facilitate the transition to a new token.

Cross-Chain Compatibility:
Cross-chain compatibility refers to the ability of different blockchain networks to interact and share data seamlessly. Cross-chain compatibility solutions like atomic swaps and interoperability protocols enable users to transfer assets and information across disparate chains.

Layer 2 Scaling Solution:
An layer 2 scaling solution is a technology that processes transactions off-chain to improve scalability and reduce fees on the main blockchain. Layer 2 solutions like state channels and rollups enhance transaction