Professional Certificate in Blockchain and Cryptocurrency Accounting

Smart Contracts in Blockchain

Address: A unique identifier in a blockchain that acts as a digital location for storing and sending cryptocurrencies or tokens. It is similar to an email address but is only used for blockchain transactions.

Asymmetric Encryption: A cryptographic technique that uses two keys, a public key and a private key, for secure communication. The public key is used to encrypt the message, while the private key is used to decrypt it.

Bitcoin: The first decentralized cryptocurrency, created in 2009 by an unknown person or group using the name Satoshi Nakamoto. It is based on a decentralized, peer-to-peer network and uses blockchain technology for secure transactions.

Block: A collection of transactions that are verified, validated, and added to a blockchain. Each block contains a unique code called a "hash," which connects it to the previous block, forming a chain of blocks.

Blockchain: A decentralized, digital ledger that records transactions across a network of computers. It is secure, transparent, and immutable, making it ideal for recording and verifying transactions.

Cryptocurrency: A digital or virtual currency that uses cryptography for security and operates independently of a central bank or government. Bitcoin is the most well-known cryptocurrency, but there are many others, such as Ethereum, Litecoin, and Ripple.

Decentralization: The process of distributing power, authority, or control away from a central authority or location. In blockchain technology, decentralization refers to the distribution of control and decision-making across a network of computers.

Distributed Ledger Technology (DLT): A type of database that is distributed across a network of computers, rather than being stored in a central location. DLT is used in blockchain technology to record and verify transactions.

Ethereum: A decentralized, open-source blockchain platform that enables the creation of smart contracts and decentralized applications (dApps). It was founded in 2013 by Vitalik Buterin and has since become one of the most widely used blockchain platforms.

Fork: A split in the blockchain, resulting in two separate chains. A fork can occur when there is a disagreement in the blockchain community about changes to the protocol, or when there is a bug in the code.

Immutability: The inability to change or alter data once it has been recorded in a blockchain. This feature ensures the security and integrity of the data, as it cannot be tampered with or manipulated.

Mining: The process of verifying and validating transactions on a blockchain. Miners use powerful

computers to solve complex mathematical problems, and in return, they are rewarded with cryptocurrency.

Node: A computer or device that is connected to a blockchain network. Nodes are responsible for storing a copy of the blockchain and verifying transactions.

Private Key: A secret code that is used to unlock or decrypt a message or transaction. It is a critical component of asymmetric encryption and is used to ensure the security and confidentiality of the message.

Public Key: A code that is used to encrypt a message or transaction. It is a critical component of asymmetric encryption and is used to ensure the security and integrity of the message.

Proof of Stake (PoS): A consensus algorithm used in blockchain technology that requires validators to prove they own a certain amount of cryptocurrency. Validators are then chosen to create new blocks based on the amount of cryptocurrency they hold.

Proof of Work (PoW): A consensus algorithm used in blockchain technology that requires miners to solve complex mathematical problems to create new blocks. PoW is a computationally intensive process that requires significant resources and energy.

Smart Contract: A self-executing contract that contains the terms and conditions of an agreement between parties. It is stored on a blockchain and is automatically executed when the conditions of the contract are met.

Token: A digital asset that represents a particular fungible and tradable asset or a utility. Tokens can be used for various purposes, such as to represent shares in a company, to access a particular service, or to vote on decisions.

Transaction: A digital exchange of assets between parties. Transactions are recorded on a blockchain and are verified, validated, and added to a block by miners or validators.

Transparency: The degree to which the data and transactions in a blockchain are visible and accessible to all participants in the network. Transparency is a key feature of blockchain technology, as it ensures accountability and trust.

Wallet: A digital application or device that is used to store, manage, and send cryptocurrencies or tokens. Wallets can be software-based or hardware-based and are used to secure and protect the private keys associated with the cryptocurrencies.

Zero-Knowledge Proof (ZKP): A cryptographic technique that allows one party to prove to another party that they know a value, without revealing the value itself. ZKP is used in blockchain technology to ensure privacy and security in transactions.

51% Attack: A potential attack on a blockchain network where a single entity or group controls more than 50% of the network's computing power. This would allow them to manipulate the blockchain, double-spend coins, and prevent new transactions from being confirmed.

Address Reuse: The practice of using the same address for multiple transactions. This is generally discouraged in the blockchain community, as it can compromise the privacy and security of the user's transactions.

Altcoin: A term used to describe any cryptocurrency that is not Bitcoin. Altcoins are often created to improve upon the features and functionality of Bitcoin or to provide alternative use cases.

Anonymity: The state of being unidentifiable or untraceable. While blockchain transactions are generally transparent, the use of anonymous addresses and other techniques can provide a degree of anonymity for users.

Airdrop: A marketing tactic used in the blockchain community to distribute free tokens or coins to users. Airdrops are often used to promote new projects or to incentivize community engagement.

BIP (Bitcoin Improvement Proposal): A design document used in the Bitcoin community to propose changes to the Bitcoin protocol. BIPs are used to improve the functionality, security, and scalability of the network.

Bitcoin Cash: A hard fork of the Bitcoin blockchain that occurred in 2017. Bitcoin Cash was created to increase the block size limit and improve the scalability of the network.

Block Height: The number of blocks in a blockchain, starting from the genesis block. The block height is used to identify and reference specific blocks in the blockchain.

Block Reward: The amount of cryptocurrency that is awarded to miners for successfully mining a new block. The block reward is a key incentive for miners to participate in the network and secure the blockchain.

Blockchain as a Service (BaaS): A cloud-based service that enables businesses and developers to build and deploy blockchain applications without having to manage the underlying infrastructure.

Block Explorer: A web-based tool that allows users to view and analyze the details of transactions and blocks on a blockchain.

Consensus Algorithm: A set of rules and protocols used by nodes in a blockchain network to agree on the validity of transactions and the state of the blockchain.

Custodial Wallet: A wallet that is managed by a third-party service provider, rather than the user themselves. Custodial wallets are often used by exchanges and other service providers to secure and protect user funds.

Decentralized Application (dApp): A software application that is built on a decentralized blockchain platform. dApps are designed to be transparent, secure, and resistant to censorship.

Decentralized Exchange (DEX): A cryptocurrency exchange that operates without a central authority or intermediary. DEXs are often built on decentralized blockchain platforms and allow users to trade directly with each other.

Difficulty Bomb: A feature in the Ethereum blockchain that gradually increases the difficulty of mining new blocks. The difficulty bomb is designed