Professional Certificate in AI in Financial Crime Compliance

Blockchain Technology in Financial Crime Analysis

Address: A unique identifier in a blockchain network that represents the location from where a transaction originates or to where it is sent. It is similar to an email address, and it is used to send and receive cryptocurrencies.

Asic: Application-Specific Integrated Circuit, a piece of hardware designed to perform a specific task, such as mining cryptocurrencies. ASICs are more efficient and faster than general-purpose computers in mining, making them the preferred choice for professional miners.

Block: A collection of transactions in a blockchain network, grouped together and added to the blockchain in a sequential manner. A block contains a header and a body. The header includes the hash of the previous block, a timestamp, and the nonce. The body contains the list of transactions.

Blockchain: A distributed, decentralized, and immutable digital ledger that records transactions across a network of computers. Blockchain technology enables secure and transparent transactions without the need for intermediaries.

Consensus: The mechanism by which a blockchain network agrees on the validity and order of transactions. There are several consensus algorithms, including Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS).

Cryptocurrency: A digital or virtual currency that uses cryptography for security and operates independently of a central bank. Bitcoin, Ethereum, and Ripple are examples of cryptocurrencies.

Decentralization: The distribution of power, authority, and decision-making from a central authority to a network of computers or individuals. Decentralization is a key feature of blockchain technology, enabling secure and transparent transactions without intermediaries.

Distributed Ledger Technology (DLT): A type of database that is distributed across a network of computers, enabling secure and transparent transactions without intermediaries. Blockchain is a type of DLT that uses a sequential chain of blocks to record transactions.

Ethereum: A decentralized, open-source blockchain platform that enables the creation of smart contracts and decentralized applications (dApps). Ethereum is the second-largest cryptocurrency by market capitalization, after Bitcoin.

Fiat Currency: A currency that is issued and backed by a central government or authority, such as the US dollar or the Euro. Fiat currency is not backed by a physical commodity, such as gold or silver, but by the

government's faith and credit.

Fork: A split in a blockchain network that occurs when a group of nodes or miners disagree on the validity of a transaction or the state of the blockchain. A fork can result in the creation of two separate blockchains, one following the old rules and one following the new rules.

Hash: A fixed-size output generated by a hash function, which takes an input of any size and produces a unique output. Hash functions are used in blockchain technology to secure transactions and ensure the integrity of the blockchain.

Immutable: A characteristic of a blockchain that refers to its inability to be altered or modified once data has been added to it. Immutability ensures the integrity and transparency of the blockchain network.

Mining: The process of adding transactions to a blockchain network and validating them by solving complex mathematical problems. Miners are rewarded with cryptocurrencies for their efforts.

Nonce: A random number that is added to a hash function to change the output and find a solution to the mathematical problem in the mining process.

Private Key: A secret code that is used to unlock and access a cryptocurrency wallet. A private key is a unique and sensitive piece of information that should be kept secure and confidential.

Public Key: A code that is used to receive cryptocurrencies and is associated with a cryptocurrency wallet. A public key is a unique and open code that can be shared with others to receive payments.

Proof of Stake (PoS): A consensus algorithm that relies on the economic stake of a participant in the blockchain network, rather than computational power, to validate transactions and add them to the blockchain.

Proof of Work (PoW): A consensus algorithm that relies on computational power to validate transactions and add them to the blockchain. PoW requires miners to solve complex mathematical problems to earn the right to add the next block to the blockchain.

Smart Contract: A self-executing contract with the terms of the agreement written directly into code. Smart contracts are stored and executed on a blockchain network, enabling secure and transparent transactions without intermediaries.

Transaction: A digital exchange of value between two parties on a blockchain network. A transaction can be a transfer of cryptocurrencies, the execution of a smart contract, or any other type of digital asset.

Wallet: A digital or physical device that stores and manages cryptocurrencies. A wallet contains a public key, which is used to receive payments, and a private key, which is used to unlock and access the wallet.

Whitepaper: A detailed document that explains the technical and economic aspects of a cryptocurrency or

blockchain project. A whitepaper typically includes information on the problem that the project aims to solve, the proposed solution, the technology stack, and the roadmap for implementation.