Virtual Assets Glossary
Key Concepts and Definitions

FINANCIAL SERVICES AUTHORITY

Bois De Rose Avenue
P.O. Box 991
Victoria
Mahé
Seychelles

Tel: +248 4380800
Fax: +248 4380888
Website: www.fsaseychelles.sc
Email: enquiries@fsaseychelles.sc

Version: 19th December, 2024

INTRODUCTION

This Glossary has been prepared by the Financial Services Authority, to assist in the understanding of terms commonly used and or association with the Virtual Asset Service Providers space.

This document is not exhaustive and must be taken in the context of the Virtual Asset Service Providers Act, 2024.

Algorithm	A process or set of computational rules that defines a sequence of operations for solving a given problem, or executing a given task.
Algorithmic Stablecoin	A subset of stablecoins whereby instead of being pegged to a stable asset (e.g. fiat currency such as $, € or £), they maintain their value through algorithmic mechanisms. This is achieved through the algorithm increasing or decreasing the supply of a virtual asset in response to changes in demand. For example, a computer or smart contract increasing or decreasing tokens in the market to maintain a stable value.
Altcoin	Any alternative cryptocurrency to Bitcoin.
Asset Tokenisation	In the context of virtual assets, tokenisation is the process of creating a digital representation of real-world assets on a blockchain. The resulting tokens represent a stake of ownership in the underlying asset which can be held, sold and traded on a blockchain (e.g. financial securities, property, artwork). These tokens may also be referred to as Asset-Backed Tokens.
Blockchain	A secure digital ledger or database of transactions relating to virtual assets which are recorded chronologically, and which are capable of being audited. It records transactions and tracks assets in a decentralised network. This means that the records are not stored in one central location but is instead spread out across a network of computers. The records are immutable as such, they cannot be erased or changed.
Coin	Virtual assets that operate on their own blockchain. They are used for transactions, investments, or fundraising mechanisms for projects. Examples of coins include Bitcoin, Litecoin, Ether.
Cold Wallet	A wallet that is not connected to the internet. The private keys and virtual assets are stored offline. For example, hardware wallets resembling USB drives or small portable devices with screens and buttons such as Ledger Nano X, Trezor Model T and KeepKey.
Consensus	The process in which participants in a decentralised network (nodes) agree on the validity of data and that the distributed ledger contains a consistent set and ordering of validated transactions. The agreement amongst nodes is required for any updates or transactions on the blockchain. Examples of consensus mechanisms include Proof of Work, Proof of Stake.
Custodial Services	A service where the Virtual Asset Service Provider (VASP) holds and manages the customers' private keys and/or virtual assets on their behalf.
Cryptocurrency	Digital or virtual currencies that use cryptography to secure transactions, investments or creating a coin to fund a project. They are decentralised and operate on blockchain technology.

Cryptography	A method of securing information against unauthorised access by using algorithms to transform the data into an unreadable format. Only authorised recipients can reverse the effects and make the information readable through the right algorithm.
Decentralised autonomous organisation (DAO)	Collectively owned, blockchain-governed organisations. There is no centralised leadership and rules are defined and enforced through smart contracts. The entities require all members to vote for changes to the rules[i]. For example, Bitcoin is a DAO.
Decentralised Finance (DeFi)	A general term for financial services and products based on distributed ledger technology (DLT). The objective of DeFi is for services to operate without centralised authorities/third parties[ii].
Decentralised or distributed application (dApp)	Software applications built out of smart contracts, often integrated with user-facing interfaces using traditional web technology[iii]**.**
Distributed Ledger Technology (DLT)	A database that is stored, shared and synchronised on a computer network. Data is updated by following rules for achieving consensus among the network participants[iv]. Blockchain is an example of distributed ledger technology.
Encryption	The process of securing data or information by converting it into code in order to prevent unauthorised access. This is achieved through mathematical modes such as cryptography.
Fiat Currency	Any legal tender designated and issued by a central authority that people are willing to accept in exchange for goods and services, such as $, € or £.[v].
Fungibility	The ability of a good or asset to be interchanged with another good or asset of the same type and value. For example, each individual unit of a specific cryptocurrency is the same as every other unit of the same cryptocurrency (e.g. one bitcoin is the same as every other bitcoin). However, non-fungible tokens (NFT) are unique and are not interchangeable.
Gas	In the context of virtual assets, gas refers to the unit of computational work or resources required in order to execute operations. This measures the amount of effort needed to perform the operations and is typically associated with the Ethereum blockchain. For example, when a transaction is initiated, the sender must specify the gas limit (how much the sender is willing to consume) and a gas price (how much the sender is willing to pay for each unit of gas). The network then uses this to determine whether the transaction will be processed.
Governance Token	Tokens that grant holders voting rights within a decentralised project, allowing them to participate in decisions on the project's future.
Hosted Wallet	A digital wallet provided by a VASP (e.g. custodian/ wallet provider or exchange). Users deposit funds into the wallet but, both the virtual asset service provider and the user have control over the private keys and virtual assets in the wallet.

Hot Wallet	Refers to a digital wallet that is connected to the internet. For example, mobile applications, web wallets, desktop wallets.
Immutability	In the context of virtual assets, immutability refers to a feature of blockchain technology whereby data recorded and validated on the network is transmitted to other computers (nodes) in the network and cannot be altered or deleted due to each block being linked to its predecessor.
Initial Coin Offering (ICO)	A fundraising method used to raise funds for a project by issuing virtual assets and offering them in exchange for funds. When an offering is made, the issuer responsible for the project issues a set number of 'coins' or 'tokens' to the public in exchange for payment through smart contracts. Investors may gain future benefits such as future voting rights, access to the project's products or services and/or potential future profits.
Issuer	A person who is authorised to issue an initial coin offering ("ICO") or non-fungible token ("NFT"). There are no restrictions on who may cause to issue an ICO or NFT.
Layer 1	The foundational layer of blockchain architecture. It provides the underlying infrastructure for transaction validation, consensus mechanisms, as well as maintaining the blockchain network security and decentralised nature. Examples of Layer 1 blockchains are Bitcoin, Ethereum.
Layer 2 solutions	These are secondary frameworks built on top pf a pre-existing blockchain (Layer 1) as a means to increase scalability and reduce transaction costs. These solutions handle transactions off the main blockchain but ensure security and data integrity (e.g. Lightning Network for Bitcoin).
Mining	In the context of virtual assets, mining is the process that Bitcoin and several other cryptocurrencies use to generate new coins and validate transactions. The process involves miners using specialised computers to solve complex computational math problems in order to verify and validate transactions. Miners who validate a transaction correctly are awarded newly minted (created) coins, which are added in circulation on the network or earn transaction fees. Examples of mining methods are Proof of Work and Proof of Stake.
Mining Facility	A place, amenity, or equipment (software or hardware) used, as a business, for creating cryptocurrency on a blockchain through computational and cryptographic means, in order to validate transactions and add them to a public blockchain ledger, in exchange for some form of benefit (coin, transaction fees).
Minting	The process of generating new virtual assets (coins, tokens, etc.) on a blockchain. It is an alternative to mining whereby a pre-determined trusted entity is the creator of the new virtual assets. An example of a minting method is Proof of Stake.

Mixer or Tumblr Services	Mixers, also known as tumblers or coin mixers, operate tools designed to enhance user privacy by obfuscating the transaction history of digital currencies. Their primary function is to mix or shuffle virtual assets from multiple users, making it challenging to trace the origin of specific funds.
Node	In the context of virtual assets, a node is a device (e.g. computer) that participates in a blockchain network. An essential component of the network, nodes are: - interconnected and constantly exchanging latest blockchain data, - hosts and synchronises replicas of the blockchain hence, saving and storing transaction history, - undertake the validation process for block of transactions and accept or reject it.
Non-Custodial Services	Customers retain control of their private keys and assets through the use of self-managed wallets.
Non-Fungible Token (NFT)	A unique digital identifier that is recorded on a blockchain and is used to certify ownership and authenticity. Unlike cryptocurrencies and other fungible tokens which are interchangeable and identical, NFTs are distinct and cannot be traded or exchanged at the same unit of value. Their value is dependent on its individual worth and the marketplace where it exists. Examples of NFTs include artwork, domain names and music.
Peer-to-Peer Trading (P2P)	The direct exchange of virtual assets between parties without the involvement of a central authority or a third party.
Permissionless	In the context of blockchains, permissionless refers to a network that is public. There are no restrictions on who can join, view and participate in the network.
Privacy Coin	Virtual assets which aim to facilitate anonymity by using privacy enhanced techniques to hide transaction information (e.g. transaction flows, senders, recipients, transaction amounts and account balances). They are also known as Anonymity-Enhanced Cryptocurrency.
Private Key	A secret key which provides access to virtual assets and authorises withdrawals (similar to a pin associated with your account). Transactions on a blockchain network are conducted using a Private Key in conjunction with a Public Key. The Private Key is needed to decrypt (unlock) transaction/data and prove ownership of funds. Similar to an online banking password or PIN, it should never be shared with anyone.
Promoter	A person who causes the preparation or distribution of an offering document relating to the ICO or NFT but does not include a lawyer or accountant acting for or on behalf of a promoter. Under the Virtual Asset Service Providers Act, 2024, only a person licensed as a Virtual Asset Service Provider or licensed under the Securities Act, 2007 may act as a promoter. A natural person is ineligible to promote an ICO or the sale or development of NFTs in or from Seychelles.

Proof of Stake	A consensus mechanism used to validate transactions on a blockchain. Validators stake their cryptocurrency (pre-pledging their existing coins by locking them on the blockchain) for the opportunity to be picked to validate a block. Validators who successfully staked their coins are randomly chosen to verify data on a blockchain. Whilst the coins are locked, validators are unable to spend their stake unless the coins are un-staked for trading. Bad actors who contravene the rules or record incorrect information risk losing their staked coins. Validators who accurately verify a transaction are rewarded with newly minted (created) coins and a transaction fee.
Proof of work	A consensus mechanism used to validate transactions on a blockchain. Miners use specialised computers to solve complex computational problems in order to verify and validate transactions. Miners who validate a transaction correctly are awarded newly minted (created) coins. The process ensures new data added to a blockchain network is accurate and prevents users from double spending. However, it entails significant computational power, hence involves high energy consumption.
Public Key	A cryptographic key that is used to receive funds using a unique code that acts like a digital address for your wallet. Transactions on a blockchain network are conducted using a Private Key in conjunction with a Public Key. The Public Key is used to encrypt transactions and similar to a bank account number, it can be freely shared with everyone.
Recovery Phrase/ Seed	A series of words which are used to gain access to funds if a wallet is lost, stolen or damaged. Similar to a "master key", it provides access to a wallet and all private keys in the associated wallet. It must be kept safe and secure because there is no way to recover funds if it is lost. It is also known as a Seed Phrase.
Security Token	Tokens which represent ownership in traditional assets (e.g. stocks, real estate).
Self-Custody Wallet	A wallet where the user controls the private keys and virtual assets through hardware (e.g. wallet devices) and/or software (e.g. mobile, desktop, browser wallets). As such, the wallet is not maintained by a virtual asset service provider, such as a wallet provider or exchange. It is also known as an unhosted wallet.
Smart Contract	A smart contract is a self-executing digital agreement built on a blockchain. They automatically enforce terms when a predefined condition is met without needing a third party (e.g. releasing payment to a seller when a buyer confirms receipt of goods).
Sharding	Sharding refers to a scaling technique that involves partitioning the blockchain's data or computational work into smaller, more manageable pieces called "shards". This is usually done to improve scalability and efficiency of a blockchain network allowing it to process more transactions and handle more users without compromising performance.

Stablecoin	A subset of cryptocurrencies that aim to maintain a stable value by pegging their price to an underlying asset (e.g. a fiat currently like US Dollar). This stability makes them useful for transactions and as a store of value.
Token	Virtual assets built on an existing blockchain network using smart contracts. They can represent ownership of an asset, provide access to services or voting rights. Examples of tokens include utility tokens, security tokens, governance tokens, and non-fungible tokens (NFT).
Transaction Hash/ TX Hash/ Transaction ID	A unique identifier assigned to a transaction on a blockchain network. It is comprised of a string of characters that serves as a reference to a specific transaction, allowing user to trace and verify that transaction on the blockchain.
Travel Rule	Derived from the FATF which requires that VASPs share certain customer information, inclusive of the sender and receivers' names and addresses for cross border transactions.
Utility Token	A type of token that is issued by projects or platforms within the blockchain ecosystem and grants the holders access to specific features, services or goods within that ecosystem. They are often used to facilitate interactions on decentralised applications (dApps).
Virtual Asset	A digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. It does not include digital representation of fiat currencies (e.g. SCR, EUR, USD), securities and other financial assets.
Virtual Asset Broking	The provision of intermediary and facilitation services for: - the exchange of virtual assets and fiat currency for and on behalf of clients - safe keeping of virtual assets on behalf of clients (e.g. storing virtual assets).
Virtual Asset Exchange	A digital marketplace that allows for: - the exchange of virtual assets with fiat currency - the transfer and conversion of virtual assets - the safekeeping and management of virtual assets (e.g. storing, depositing, and withdrawing virtual assets). It may also be referred to as a crypto exchange.
Virtual Asset Investment Provider	The management and provision of investment advice to clients (e.g. an expert guides a client on how to invest in virtual assets).
Virtual Asset Service Provider	A person that conducts one or more of the following activities as per the Virtual Asset Service Provider Act, 2024: - Virtual Asset Wallet Provider - Virtual Asset Exchange - Virtual Asset Broking - Virtual Asset Investment Provider
Virtual Asset Wallet	A software application or device used to hold, store and transfer virtual assets (e.g. cryptocurrencies and tokens). It is essential for managing and using virtual assets. Wallets provide a secure way to store your private

	keys and interact with the blockchain. They are also known as a digital wallet.
Virtual Asset Wallet Provider	The provision of custodial services. A wallet provider that provides the software application used to hold, store and transfer your virtual assets, similar to a physical purse/ wallet.
Wallet address	The shortened version of a Public Key. It is a unique string of characters that represents a wallet used to send and receive funds. Similar to an email address, it indicates the location of a wallet, or a store of value, on the blockchain.
Web 3	The next generation of the internet which emphasises decentralised web ecosystems through the use of blockchain technology whereby: - users are empowered to take ownership of their own data. - new products and services are enabled using virtual assets.
White Paper	In the context of virtual assets, a white paper is used to generate interest in a project or venture (e.g. ICO, NFT offering).

[i] https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf
[ii] https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf
[iii] https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf
[iv] https://www.imf.org/en/Publications/fintech-notes/Issues/2021/10/14/Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-1-463654
[v] https://documents1.worldbank.org/curated/ar/455961468152724527/pdf/881640BRI0Box30WLEDGENOTES0Jan02014.pdf