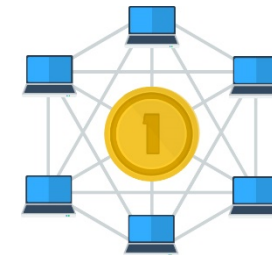


# Blockchain and cryptocurrencies – Some key terms



## Blockchain

A type of distributed ledger that is maintained by participants in a decentralised network of computers.

## Cryptography

Cryptography involves creating written or generated codes that allow information to be kept secret. Blockchain uses cryptography to convert data into a format that is unreadable for an unauthorised user, and to prevent unauthorised changes to the ledger.

## Cryptocurrency

Digital assets that are used as a medium of exchange that aim to substitute government-issued money or as a store of value (e.g. bitcoin).

## Node

A computer connected to a blockchain network that supports the network through validation and relaying of transactions on the blockchain. It also maintains a full copy of the blockchain.

## Bitcoin ‘mining’

An activity that involves processing and adding transaction records to the bitcoin’s public ledger of past transactions.

## Bitcoin ‘miners’

Miners – usually in the form of specifically programmed computers – solve transaction-related algorithms in order to validate a block of transactions. In return, they are awarded a certain number of bitcoins.

## Wallet

A wallet enables users to transact on blockchains and see balances and transactions related to the wallet.

## Public key

An alphanumeric string of characters that is the public address of the wallet. Other parties can send digital assets to a public address (similar to an email address). A user can provide the public key to a third party as part of a transaction (i.e. request for funds), but the third party cannot access or transact assets within the wallet.

## Private key

An alphanumeric string of characters that initiates a transaction. The private key is unique to each public key and cannot be reproduced if lost or stolen. Digital assets are controlled using the unique private key associated with the public addresses in which the digital assets are held. The theft, loss or destruction of a private key is generally irreversible, and those private keys would not be able to be restored.

## Signature

The mathematical operation that allows ownership of a public key to be validated. For example, a bitcoin wallet may have a public address, but only a private key can verify that a signature matches and a transaction is valid.

## Tokenisation

Creating a digital representation of an asset on a blockchain so it can be transferred between parties.

## Securities token

Digital assets that are analogous to fund interests, equities, bonds or derivatives and represent an interest in an underlying asset, business or stream of cash flows.

## Utility token

Digital assets that are the means of accessing services or transacting on blockchain or software platforms.