01/04/22

A Blockchain Glossary

"The beginning of wisdom is to call things by their right names" - Chinese proverb

Blockchain is classified as a General-Purpose Technology (GPT) that describes a series of decentralized distributed databases that create a tamper-proof, verifiable ledger. As with any new technology, blockchain has its own terminology. Here is a list of important terms and their meanings.
N.B. Blockchain ≠ Bitcoin

Address
A blockchain public address is a unique, 32-bit, alphanumeric string that identifies users in the blockchain. This public address can be used to reference, send, receive or record blockchain transactions. In addition, an address can be represented as a scannable QR code. An example of a blockchain address is: 5TdA55HeLopzzwe3Lg7W335tGdCc623PoQ.

Agreement Ledger
A distributed ledger used by two or more parties to negotiate and reach agreement.

Altcoin
A cryptocurrency that works similarly to bitcoin, but with modifications. For example, increasing the speed of transaction processing.

Attestation Ledger
A distributed ledger providing a durable record of agreements, commitments, or statements, providing evidence (attestation) that these agreements, commitments, or statements were made.

ASIC
An acronym for "Application Specific Integrated Circuit". ASICs are silicon chips specifically designed to do a single task. In the case of Bitcoin, they are designed to process SHA-256 hashing algorithms for "mining" new bitcoins.

Bitcoin (Two Instantiations)
Bitcoin is the first decentralized, open-source cryptocurrency that runs on a global peer-to-peer network, without the need for infomediaries or a centralized authority or issuer.

a. **Bitcoin (uppercase):** The well-known cryptocurrency, based on the Proof-of-Work blockchain.
b. **bitcoin (lowercase):** The specific collection of technologies used by Bitcoin's ledger, a particular solution. The currency is itself one of these technologies, as it provides the miners with the incentive to mine.

Block
A block is a collection of transactions. Blocks are synonymous with digital pages in a ledger, also known as a record-keeping book. These files store unalterable data related to the network.

Blockchain
A blockchain is a type of distributed ledger comprised of unchangeable, digitally recorded data in packages called blocks (rather like collating them on to a single sheet of paper). Each block is then "chained" to the next block, using a cryptographic signature. The blockchain serves as a historical record of all transactions, from the genesis block to the latest block, hence the name blockchain. Blockchains can be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions.

Block Reward
The reward given to a miner that has successfully hashed a transaction block. Block rewards can be a mixture of coins and transaction fees, depending on the policy used by the cryptocurrency and whether the coins have already been successfully mined. The current block reward for the Bitcoin network is 25 bitcoins for each block.

Bootstrapping
The process by which a cryptocurrency moves from a state where only a few nodes participate in the consensus algorithms in the network to a fully scaled peer-to-peer network with many more participating nodes. The fully scaled network must then remain secure under assumptions in the underlying consensus algorithms. During bootstrapping, the underlying assumptions may be relaxed.

Byzantine Generals Problem
The Byzantine Generals Problem is a term borrowed from the computer science literature describing a situation where involved parties must agree on a single strategy to avoid complete failure, but where some of the involved parties are corrupt and disseminating false information or are otherwise unreliable.

Central Ledger
A central ledger refers to a ledger maintained by a central agency.

Confirmation
The blockchain transaction has been verified by the network. This happens through a process known as mining, in a Proof-of-Work system (e.g., Bitcoin). Once a transaction is confirmed, it cannot be reversed or double spent. The more confirmations a transaction has, the harder it becomes to perform a double spend attack.

Consensus Process
The process whereby a group of peers responsible for maintaining a distributed ledger reach consensus on the ledger's contents.

Consensus Point
Either a point-in-time or a defined set of terms where network peers "meet and agree" on the number and volume of records that comprise the state of the ledger.

Consensus Mechanism
A process, encoded in software, by which computers in a network, called nodes, reach an agreement about a set of data. In the context of blockchains, the consensus algorithm is often used to agree on a block of transactions that should be appended to the blockchain.

Costless Verification
Recorded attributes that need to be securely verified on a blockchain and can be referred to at any point via the distributed ledger at relatively no cost.

Cryptocurrency
A mathematical form of digital currency where encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds. In this instance, operating independently from a central bank, a cryptocurrency is a scarce digital asset built on or running on top of a blockchain protocol and exchanged via that blockchain system.

Digital Commodity
A scarce, electronically transferrable, intangible, commodity with a set market value.

Digital Identity
An online or networked identity adopted or claimed in cyberspace by an individual, organization, or electronic device.

Difficulty
In Proof-of-Work mining, how hard it is to verify blocks in a blockchain network. In the Bitcoin network, the difficulty of mining adjusts every 2,016 blocks to maintain a block verification time of ten minutes.

Digital Signature
One of two functions involved in public-key cryptography (see definition). A digital signature is a pair of cryptographic algorithms that can be used to authenticate messages sent over public channels. The signing algorithm takes the private key and the message as input and produces an authentication tag. The verification algorithm takes the public key, the message, and the tag as input, and verifies that the message was signed by the corresponding private key.

Distributed Applications (Dapps)
Dapps are a new type of architecture being used in the blockchain. Dapps store data and source code in a decentralized manner that is distributed on the blockchain. The biggest advantage to this structure is that a Dapp ensures the blockchain application is always online and is not reliant on a single server's availability.

Distributed Ledger
Distributed ledgers are a type of database that are spread across multiple sites, countries, or institutions. Records are stored one after the other in a continuous ledger. Distributed ledger data does not have its own currency. These ledgers can be either "permissioned" or "unpermissioned" to control viewing.

Double Spend
In the Bitcoin network, double spend refers to a scenario where someone tries to send a bitcoin transaction to two different recipients at the same time. However, once a Bitcoin transaction is confirmed, it makes it nearly impossible to double spend. The more confirmations that a particular transaction has, the harder it becomes to double spend the bitcoins. Double spending occurs when a sum of money is spent more than once.

Extensive Margin
The extensive margin refers to new applications in the marketplace, that did not previously exist, enabling services that could not have been offered without this recent technology. Start-ups and incumbents using blockchain technology are experimenting with different solutions that exploit either the intensive or the extensive margin.

Fiat Currency
Fiat currency is any money declared by a government to be to be valid for meeting a financial obligation, like the US Dollar or the EURO.

Fork
A fork creates an alternate version of the blockchain, leaving two blockchains to run simultaneously on different parts of the network. Forks may be initiated by developers or members of a cryptocommunity who grow dissatisfied with functionalities offered by existing blockchain implementations. In addition, they may emerge to crowdsource funding for new technology projects or cryptocurrency offerings.

General-Purpose Technology (GPT)
A new method of producing and inventing that is important enough to have a protracted aggregate impact across multiple applications and sectors of the economy. Steam power, electricity, and TCP/IP protocols (Internet) are three important GPTs.

Genesis Block
The first block in a blockchain.

Hard Fork
A hard fork is a radical change to a network's protocol that makes previously invalid blocks and transactions valid, or vice-versa. A hard fork requires all nodes or users to upgrade to the latest version of the protocol software.

Halving
Bitcoins have a finite supply, which makes them a scarce digital commodity. The total amount of bitcoins that will ever be issued is 21 million. The number of bitcoins generated per block decreases 50% every four years. This is called “halving.” The final halving will take place in the year 2140.

Hashcash
A Proof-of-Work algorithm, which has been used as a denial-of-service counter measure in several blockchain systems.

Hashfunction
A cryptographic function that turns any input into a string of characters of a fixed length that serves as a virtually unforgeable digital fingerprint of the data, called a hash.

Hashrate
The number of hashes that can be performed by a bitcoin miner within a period (usually a second).

Hyperledger Foundation
A non-profit organization that brings together the necessary resources and infrastructure to ensure thriving and stable ecosystems around open-source software blockchain projects.

Initial Coin Offering (ICO)
An unregulated, blockchain-based fundraising mechanism in which entrepreneurs mint new crypto tokens and sell them to investors. Like the IPO mechanism, fundraising requires fiat currency backing and understanding of digital currencies and the use of digital wallets. An upside to these investments can be utility access to the associated software or product offerings.

Intensive Margin
The intensive margin is an economic term that refers to doing more of what you were doing before, but in a cheaper and more efficient way.

Ledger
An append-only record store, where records are immutable and may hold more general information than financial records.

Litecoin
A peer-to-peer cryptocurrency based on the Scrypt Proof-of-Work network. Referred to as the silver of Bitcoin's gold.

Merkle Tree
An efficient cryptographic tree in which every "leaf" node is labelled with the hash of its associated data block and every "non-leaf" branch is labelled with the hash of its associated leaves.

Miner
A miner is responsible for securing a blockchain based on Proof of Work. Miners use computing power, also known as hash power, to solve cryptographically complex mathematical problems. The result of this process is the addition of new blocks to a blockchain.

Mining
The mathematical cryptographical process by which transactions are verified and new blocks are added to the "chain". The necessity of validation warrants an incentive for the miners that use computing hardware to trigger the release of cryptocurrencies, (e.g., bitcoins).

Multi-Signature
Multi-signature (multisig) addresses allow multiple parties to require more than one key to authorize a transaction. The needed number of signatures is agreed at the creation of the address. Multi-signature addresses have a much greater resistance to theft.

Node
A participant in the blockchain network. A node may participate in the mining process, consensus algorithm, or simply store a copy of the blockchain for querying.

Nonce
An arbitrary random or pseudo-random number that may only be used once in a cryptographic communication. In this case, to verify the block to be added onto a blockchain.

Off-Ledger Currency
A currency minted off-ledger and used on-ledger. For example, using distributed ledgers to manage a national currency.

On-Ledger Currency
A currency minted on-ledger and used on-ledger. For example, the cryptocurrency bitcoin.

Oracle
A third-party service that connects smart contracts with the outside world, thereby enabling the bidirectional exchange of external information. This exchange of outside information encapsulates multiple sources so that decentralized knowledge is obtained. Information can include making payments and notifying parties. The oracle layer queries, verifies, and authenticates external data sources, usually via trusted APIs, proprietary corporate data feeds, and internet of things feeds, and relays this information via the agreed upon blockchain protocol throughout the peer-to-peer network.

Participant
An actor who can access the ledger, read records, or add records.

Peer
An actor that shares responsibility for maintaining the identity and integrity of the ledger.

Peer-to-Peer (P2P)
Peer-to-peer (P2P) refers to the decentralized interactions that happen between at least two parties in a highly interconnected network. P2P participants deal directly with each other through a single mediation point.

Permissioned Ledger
A ledger where actors must have permission to access the ledger. Permissioned ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. Currently, this consensus process is carried out by trusted actors - government departments or banks - which makes maintaining a shared record much simpler that the consensus process used by unpermissioned ledgers. Permissioned blockchains provide highly verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. As a note, a permissioned ledger is usually faster than an unpermissioned ledger.

Private Currency
A currency issued by a private individual or firm, typically secured against uninsured assets.

Private Key
A string of data that shows you have access to bitcoins in a specific wallet. Private keys can be thought of as passwords; private keys must never be revealed to anyone, as they allow the owner to spend the bitcoins from one's bitcoin wallet via a cryptographic signature.

Private-key Cryptography
Known as symmetric (or secret) key cryptography. Both participating parties share the same secret key. Before any communication, each party must exchange their shared key. Each communication requires a unique shared key.

Private-key Encryption
A form of encryption where only a single private key is required to both encrypt and decrypt information.

Proof of Stake (PoS)
A novel consensus protocol in which, instead of mining, nodes can validate and make changes to the blockchain based on their existing economic stake. An alternative to the Proof-of-Work algorithms, in which an existing stake in a cryptocurrency (the amount of that currency that one holds) is used to calculate the amount of that currency that one can mine.

Delegated Proof-of-Stake (DPoS)
An evolution of the Proof-of-Stake concept, whereby users of the network vote and elect delegates to validate the next block. Delegates are called witnesses or block producers. Using DPoS, one votes on delegates by pooling tokens into a staking pool and linking those to a particular delegate. One does not physically transfer tokens to another wallet, but instead utilizes a staking service provider to stake tokens in a staking pool.

Proof of Work (PoW)
The consensus protocol of choice for Bitcoin and many other cryptocurrencies. To add a new block, miners must find an input to a hash function so that the output of the hash function meets certain narrow criteria. Doing so requires an enormous number of random guesses as inputs to the hash function, making it a costly process that deters fraud. Mechanistically, mining capability is tied to computational power. Blocks must be hashed which is an easy computational process. However, an additional variable is added to the hashing process to make it more difficult. When a block is successfully hashed, the hashing must have taken some time and computational effort. Thus, a hashed block is considered Proof-of-Work.

Public-key Cryptography
Known as asymmetric cryptography this system uses a pair of keys consisting of a public key and a private key. A public key may be circulated between many users, whereas a private key is known to the owner exclusively. There are two functions accomplished by public-key cryptography, public-key encryption (privacy) and digital signatures (authentication). Features of an asymmetric cryptography system are:

1. Each user has two keys: a *public* key and a *private* key.
2. Both keys are mathematically related (both keys together are called the *key pair*).
3. The public key is made available to anyone. The private key is kept secret.
4. Both keys are required to perform an operation. For example, data encrypted with the private key is unencrypted with the *public* key. Data encrypted with the public key is unencrypted with the *private* key.
5. Encrypting data with the private key creates a digital *signature.* This ensures the message has come from the stated sender (because only the sender had access to the private key to be able to create the signature).
6. A digital envelope is signing a message with a recipient's public key. A digital *envelope*, which serves as a means of access control by ensuring that only the intended recipient can open the message (because only the receiver will have the private key necessary to unlock the envelope; this is also known as *receiver authentication*).
7. If the private key is ever discovered, a new key pair must be generated.

Public-key Encryption
One of two functions involved in public-key cryptography (see definition). Public-key encryption is a pair of cryptographic algorithms that can be used to privately send messages over public channels. The encryption algorithm takes the public key and a message as input and produces a scrambled/encrypted ciphertext. The decryption algorithm takes the private key and the ciphertext as input and outputs the message in clear text.

Relational Contract
A contract theory that posits all contracts are comprised of two parts: 1) An explicit description of all transaction details, and 2) An implicit description of the trust relationship between the contracting parties.

Ripple
A payment network built on distributed ledgers that can be used to transfer any currency. The network consists of payment nodes and gateways operated by authorities. Payments are made using a series of IOUs, and the network is based on trust relationships.

Replicated Ledger
A ledger with one master (authoritative) copy of the data, and many slave (non-authoritative) copies.

Satoshi
The smallest unit of bitcoin that can currently be sent: 0.00000001 bitcoin (BTC), that is, a hundredth of a millionth bitcoin (BTC).

Satoshi Nakamoto
The pseudonym used by the unknown person or persons who designed the Bitcoin protocol.

Scrypt
An alternative Proof-of-Work system to SHA-256, designed to be “friendly” to CPU and GPU miners, while offering little advantage to ASIC miners.

SHA256 Hash
The cryptographic function used as the basis for Bitcoin’s Proof-of-Work system.

Smart Contract
A computer protocol used to digitally facilitate a contract in terms of its verification, negotiation, or performance. A smart contract allows transactions to be carried out and tracked without the use of intermediaries. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system.

Soft Fork
A change to the software protocol where only previously valid transaction blocks are made invalid. Because old nodes will recognize the new blocks as valid, a soft fork is backwards-compatible. This kind of fork requires only a majority of the miners upgrading to enforce the new rules, as opposed to a hard fork that requires all nodes to upgrade and agree on the new protocol version.

The Last Mile Problem
A phrase used to describe the interface between online records and the entities or users they represent in the offline world.

Tokenless Ledger
A distributed ledger that doesn't require a native currency to operate.

Transaction
A transaction is a string that represents a transfer of money from a user with public address X to another user in the system with public key Y.

Transaction Block
A collection of transactions on the Bitcoin network, gathered into a block that can then be hashed and added to the blockchain.

Transaction Fee
A small fee imposed on some transactions sent across the Bitcoin network. The transaction fee is awarded to the miner that successfully hashes the block containing the relevant transaction.

Unpermissioned Ledger
Unpermissioned ledgers such as Bitcoin have no single owner, in fact, they cannot be owned. The purpose of an unpermissioned ledger is to allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies. This creates censorship resistance, meaning that no actor can prevent a transaction from being added to the ledger. Participants maintain the integrity of the ledger by reaching a consensus about its state.

Wallet (Digital Wallet)
Software that manages a user's private keys. It usually contains a software client that allows access to view and create transactions on a specific blockchain that the wallet is designed for.