BLOCKCHAIN INSTITUTE

4649 N BROADWAY CHICAGO, IL 60640
INFO@THEBLOCKCHAININSTITUTE.ORG
THEBLOCKCHAININSTITUTE.ORG

WHAT ARE BLOCKCHAINS AND CRYPTOCURRENCIES?

WHAT ARE THE DIFFERENCES BETWEEN THE TWO?

What is a blockchain?

Blockchains are essentially public databases that everyone can access and read, but the data can only be updated by the data owners. Instead of the data residing on a single centralized server, data is copied across thousands and thousands of computers worldwide. Blockchains are distributed ledgers that are secured by cryptography. Data is grouped into blocks that are made permanent after set time interval. The consecutive string of every block ever executed makes up a blockchain.

What is cryptocurrency?

Cryptocurrency, such as bitcoin, is a digital store of monetary value of which the primary use is for buying and selling goods, services, or property. Cryptography is what secures cryptocurrencies against counterfeit. Cryptocurrencies can be referred to as tokens or coins, are not issued or controlled by any centralized authority.

What's the difference?

Blockchains serve as the base technology that allows **cryptocurrencies** to exist. Blockchains and cryptocurrency go hand in hand, and crypto is often a necessity if trying to transact on a blockchain. But without the blockchain, we would not have a means for these transactions to be recorded and transferred.

BLOCKCHAIN JARGON

BITCOIN

A type of digital currency, where encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

- Capital 'B' in Bitcoin: referencing the Bitcoin network
- Lowercase 'b' in bitcoin: referencing the token/ cryptocurrency bitcoin

INITIAL COIN OFFERING (ICO)

An Initial Coin Offering is somewhat similar to an IPO in the non-crypto world. Startups issue their own token in exchange for ether or bitcoin. This is essentially crowdfunding in exchange for a token.

Examples: Golem (GNT), Status (SNT) & Augur (REP)

MINING

The process of trying to 'solve' the next block. Through mining, the users secure the network and verify computation and transactions. Currently, systems including Bitcoin's blockchain, miners are incentivized to validate transactions based of off Proof-of-Work (PoW) protocol, fees, and protocol subsidies. PoW typically requires huge amounts of computer processing power. Proof-of-Stake

(PoS) is the upcoming, virtualized system of incentivization for validating transactions. Both of these systems provide economic guarantees and a form of consensus by bet. But, Proof-of-Stake relies more heavily on the betting concept. (See our Intermediate Glossary for more specific definitions of PoW and PoS.)

NODES

A computer that possesses a copy of the blockchain and is working to maintain it. Child nodes point to parent nodes. So, nodes further "up the tree" are hashes of their respective children. Most hash trees implementations are binary, with each node under two child nodes. Though, more than two child nodes can be used under each node.

PRIVATE KEYS

A private key is a string of data that shows you have access to bitcoins in a specific wallet. Private keys can be thought of as a password; private keys must never be revealed to anyone but you, as they allow you to spend the bitcoins from your bitcoin wallet through a cryptographic signature.

PUBLIC KEY

A cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient (the private key).

SMART CONTRACTS

Also known as a smart property, they are computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that make a contractual clause unnecessary. Smart contracts often mirror the logic of contractual clauses, and are being implemented in certain protocol blockchains.

WALLET

Basically, it's the Bitcoin or cryptocurrency equivalent of a bank account. It allows you to receive cryptocurrency, store them, and then send them to others. There are two main types of wallets: software and hardware.

- A software wallet is one that you install on your own computer or mobile device. Software wallets are storage for cryptocurrency that exists purely as software files on a device. Software wallets can be generated for free from a variety of sources. Read more about different software wallets, and explore some options, here.
- A hardware wallet stores private keys on a secure hardware device. Hardware wallets are often regarded as the most secure way to hold cryptocurrency, partly due to being 'cold storage' devices and having additional security features.