BLOCKCHAIN & INSURANCE

AN EDUCATIONAL WORKSHOP SERIES | GLOSSARY

BLOCKCHAIN

Blockchain technology allows for the recording of data—transactions, contracts, agreements—in a way that means the data is simultaneously stored, but also updated in real time—on hundreds or even thousands of computers globally. Blockchain technology makes the data almost impossible to tamper with or hack into, yet each transaction is updated instantly for every user, while still encrypting the content behind each transaction.

This means that people and computers all over world work together to create a network instead of a network being made by one single person or company. This network is enabled and protected through cryptography. We have seen this used in currency and data transfer. A blockchain is comprised of "blocks" and is constantly growing as each new record, datum, or block is added onto the chain for everyone to see.

BITCOIN

Bitcoin is a digital currency created in 2009. It follows the ideas set out in a white paper by the mysterious Satoshi Nakamoto, whose true identity has yet to be verified. Bitcoin was the first cryptocurrency to utilize blockchain technology and offers the promise of lower transaction fees than traditional online payment mechanisms and is operated by a decentralized authority, unlike government-issued currencies.

ETHEREUM

Launched in 2015, Ethereum is a decentralized software platform that enables SmartContracts and Distributed Applications (ĐApps) to be built and run without any downtime, fraud, control or interference from a third party. The cryptocurrency for Ethereum is Ether.

ALTCOIN

An altcoin is the community accepted name for any coin that isn't Bitcoin. Examples of altcoins include ZCash, Dash and Monero.

DISTRIBUTED LEDGER TECHNOLOGY (DLT)

A distributed ledger, also known as distributed ledger technology (DLT), is an agreement of shared, replicable and synchronized data, spread across multiple networks, across many CPU's. A central ledger is the opposite in that all of the data, while being synchronized and replicable, is controlled by a singular network, entity or individual.

SMART CONTRACT

A two-way smart contract is an unalterable agreement stored on the blockchain that has specific business logic tied to code akin to a real world contract. Once signed, it can never be altered. A smart contract is self-executing and can be used to define certain computational benchmarks or barriers that have to be met in turn for money or data to be deposited or even be used to verify things such as land rights.

DIGITAL WALLET

A digital wallet, similar to an online bank account, is where one can go to access their cryptocurrencies, public key and private key (see below). One can also send and receive various cryptocurrencies using their digital wallet.

PUBLIC KEY

A bitcoin address is essentially the same thing as your home address. It's the location from which you would receive, send or hold your currency. These addresses generally manifest in a long string of alphanumeric characters and will look something like:

1MhN5qfH1vgx9CLL17i3DK9D2gzrHR7dZF

PRIVATE KEY

A private key is a secret sequence of numbers and letters that allows bitcoins and other cryptocurrencies to be spent. Every Bitcoin wallet contains one or more private keys, which are saved in the wallet file. The private keys are mathematically related to all Bitcoin addresses generated for the wallet.

Because the private key is the “ticket” that allows someone to spend bitcoins, it is important that these are kept secure. Private keys can be kept on computer files, but in some cases are also short enough that they can be printed on paper. One often uses a private key to access their digital wallet.

BLOCK

Blocks are essentially pages in a ledger or record keeping book. Blocks are the files where unalterable data related to the network is encrypted and permanently stored. Each block contains, among other things, a record of some or all recent transactions, and a reference to the block that came immediately before it. It also contains an answer to a difficult-to-solve mathematical puzzle - the answer to which is unique to each block.

MINING

Mining is the term used for discovering and solving blocks along the blockchain. A reward is given for solving the algorithm and lengthening the chain, called a mining reward. The mining reward for the Bitcoin blockchain is Bitcoin.

Essentially, miners are competing to solve a complex math equation using computing power. The miner that solves the block, which consists of multiple encrypted transactions, receives the block reward.

HASH

A hash function takes an input (or ‘message’) and returns a fixed-size alphanumeric string. It is extremely easy to calculate a hash for any given data. It is extremely computationally difficult, nearly impossible to reverse the calculation to its original message. This is a key component behind blockchain’s security. An example of a hash is:

“Welcome to The Council of Insurance Agents & Brokers” calculates to:

54593b5ed02dced138734e47d30a5713ceee0314c195c148784187757a122bbb

HASHRATE

Hashrate is the speed at which a block is discovered and the rate at which the related math problem, or block, is solved. Certain tools and computing have been created to allow for higher hashrates. However, as the more blocks get added to the blockchain, the complex math problem becomes increasingly difficult and requires more computing to solve the block.

BLOCK REWARD

Block reward is the reward allotted for hashing, or solving the mathematical equation, related to a block. The reward for mining a Bitcoin block is 12.5 bitcoins per block mined, which will halve every 210,000 blocks.

BLOCK HEIGHT

Block height is the number of blocks preceding the genesis block (first block) on the chain. A genesis block will always have a height of zero because nothing precedes it. Considering that a new Bitcoin block is made every 10 minutes, you can work out certain time-related pieces of information if you have the total length of the chain.

FORK

A fork is a new set of rules that come into existence for that particular blockchain. These happen when a development team creates and inserts notably substantial changes into the system.

NODE

A node is essentially a computer connected to the Bitcoin network. A node supports the network through validation and relaying of transactions while receiving and retaining a copy of the full blockchain itself.

SIGNATURE

A signature is the mathematical operation that lets someone prove their sole ownership over their wallet, coin, data, etc. An example is how a Bitcoin wallet may have a public address, but only a private key can verify with the whole network that a signature matches and a transaction is valid. These are only known to the owner and are basically mathematically impossible to uncover.