CRYPTO GLOSSARY

51% ATTACK

A majority attack that occurs when more than half of the computer power on a network is run by a single person or a single group of people. The entity has full control of the network and can negatively affect a cryptocurrency by halting mining, stopping or changing transactions and reusing coins.

ADDRESSES

A unique address that identifies where a cryptocurrency sits on the blockchain. It's this location at which the coin's ownership data is stored and where any changes are registered when it is traded. Addresses look different among cryptocurrencies but are usually a string of more than 30 characters.

ASSET-BACKED TOKENS

Asset-backed tokens reflect an underlying physical asset such as gold.

ASSET TOKENS

These tokens represent assets such as a debt or equity claim on the issuer, for example, a share in future company earnings or future capital flows, and may be tradable as investments.

ASIC

An "application-specific integrated circuit" — a silicon chip dedicated to a specific purpose rather than general purpose use, such as performing the hash algorithm, used to secure a proof-of-work blockchain. ASICs are more efficient at performing those specific purpose tasks than general purpose chips (it is now only viable to mine Bitcoin using an ASIC).

AIRDROP

A marketing campaign that refers to the expedited distribution of a cryptocurrency through a population of people. It can occur when the creator of a cryptocurrency provides its coin to low-ranked traders or existing community members in order to build its use and popularity. They can be given away for free or in exchange for simple tasks like sharing news of the coin with friends.

ALGORITHM

Mathematic instructions coded into and implemented by computer software to produce a desired outcome.

ALL-TIME HIGH

Highest price ever achieved by a cryptocurrency.
Abbreviated to ATH.

ALTCOIN

An altcoin is any coin that's not Bitcoin. Altcoins can be anything from the second-most popular coin, Ethereum, to any of the thousands of coins with very minimal market value. Experts say you should largely stick to the bigger, more mainstream cryptocurrencies as an investment.

ALL-TIME LOW

Lowest price ever achieved by a cryptocurrency.
Abbreviated to ATL.

ANTI-MONEY LAUNDERING

International laws and regulations designed to prevent criminals from laundering money through cryptocurrencies into real-world cash. Also referred to by initialsm AML.

APPLICATION-SPECIFIC INTEGRATED CIRCUIT

Computer hardware – similar to a graphics card or a CPU – designed to mine cryptocurrency. ASICs are built specifically to solve hashing problems efficiently.

ARBITRAGE

The act of buying from one exchange and then selling it to the another exchange if the margin between the two is profitable. Multiple exchanges trade in the same cryptocurrency at any given tie, and they can do so at different rates.

ATOMIC SWAP

A way of letting people directly and cost-effectively exchange one type of cryptocurrency for another, at current rates, without needing to buy or sell.

BAG

A large quantity of units in a certain cryptocurrency.

BEAR, BEARISH

If the price of a cryptocurrency has a negative price movement.

BEAR TRAP

This is a trick played by a group of traders aimed at manipulating the price of a cryptocurrency. The bear trap is set by this group all selling their cryptocurrency at the same time, which bluffs the market into thinking there is a drop incoming. As a result, other traders sell their assets, further driving the price down. Those who set the trap then release it, buying back their assets, which are now at a lower price. The overall price then rebounds, allowing them to make a profit.

BITCOIN

The first and most valuable cryptocurrency, launched on Jan. 3, 2009. While its value has climbed steadily since then, it has seen wild fluctuations. In the past months alone, the price of Bitcoin has fluctuated from a record high of $60,000 to below $30,000.

BITS

A sub-unit of one Bitcoin. There are 1 million bits in one Bitcoin

BIP

A "Bitcoin Improvement Proposal" — a technical design document providing information to the Bitcoin community, describing new proposed features, processes or environments affecting the Bitcoin protocol. Suggested changes to the protocol are submitted as a BIP.
The BIP author is responsible for soliciting feedback.

BITCOIN MAXIMALIST

A person or entity that believes only the Bitcoin cryptocurrency deserves to survive longterm out of all cryptocurrencies on the market.

BLOCK

Packages of data recorded on the blockchain. The block provides a lot of important information about the block, including its hash, the hash of the previous block, the nonce, timestamp, the difficulty and the block reward.

BLOCKSPACE

As block size is typically limited, there is a limit on the number of transactions that can be processed at a time. This creates a supply and demand market between miners, mining pools and users of a blockchain. The commodity of this market is often referred to as "blockspace," and is often in relation to where such blockspace is in high demand and thus at a premium cost in gas fees (e.g., as is the case with Ethereum blockspace).

BITCOIN CASH

A peer-to-peer electronic cash system that formed from a fork of the original Bitcoin. Where Bitcoin is widely accepted as too volatile to be useful as a currency, Bitcoin Cash is designed to be better optimized for transactions.

BLOCK EXPLORER

An online tool for exploring the blockchain of a cryptocurrency, where you can watch and follow, live, all the transactions happening on the blockchain. Block explorers can serve as blockchain analysis and provide information such as total network hash rate, coin supply, transaction growth, etc.

BLOCK HEIGHT

Refers to the number of blocks connected in the blockchain. For example, Height 0 would be the very first block, which is also called the genesis block.

BLOCK REWARD

A form of incentive for the miner who successfully calculates the hash (verification) in a block. Verification of transactions on the blockchain generates new coins in the process, and the miner is rewarded with a portion of these.

BULL/BULLISH

If the price of a cryptocurrency has a positive price movement.

BURNED

If a coin in any particular cryptocurrency has been made unspendable, it is said to be burned.

BUY WALL

When a large limit order has been placed to buy when a cryptocurrency reaches a certain value, then that is a buy wall. This can prevent a cryptocurrency from falling below that value, as demand will likely outstrip supply when the order is executed.

BLOCK

Groups of data within a blockchain. On cryptocurrency blockchains, blocks are made up of transaction records as users buy or sell coins. Each block can hold only a certain amount of information. Once it reaches that limit, a new block is formed to continue the chain.

BLOCKCHAIN

A digital form of record keeping, and the underlying technology behind cryptocurrencies. A blockchain is the result of sequential blocks that build upon one another, creating a permanent and unchangeable ledger of transactions (or other data).

CAP

Shorthand for market capitalization

CENTRAL LEDGER

When a single entity has control of all financial records, it is considered to be a central ledger. This is how banks operate.

CHAIN LINKING

Each cryptocurrency has its own blockchain – the digital ledger that stores all transaction records. Chain linking is the process that occurs if you transfer one cryptocurrency to another. This requires the transaction to be lodged in two separate blockchains, so they must link together to achieve the goal.

CHAIN TIP

The most recent block added to a growing blockchain.

CHAMELEON HASH

A cryptographic hash function that could enable authorized administrators under an agreed governance model to edit or modify a transaction block in the blockchain without compromising the integrity of the blockchain.

COLD STORAGE

The use of offline hardware devices to keep private keys used to access cryptocurrency offline in order to make it resistant to hacking, e.g., by using a USB drive (using software installed on the drive) or hardware wallet.

CORDA

An open-source permissioned DLT platform created by R3.

CRYPTOASSET

A digital asset. Includes cryptocurrencies and tokens. Depending on the particular characteristics of the cryptoasset, it may or may not be a regulated product.

CRYPTO TRADING BOTS

Automated cryptocurrency trading software that executes trade orders extremely quickly, based on a preset algorithm of buy-and-sell rules.

CIPHER

The name given to the algorithm that encrypts and decrypts information.

CIRCULATING SUPPLY

The total number of coins in a cryptocurrency that are in the publicly tradable space is considered the circulating supply. Some coins can be locked, reserved or burned, therefore unavailable to public trading.

CONFIRMED

When a transaction has been confirmed, it means it has been approved by the network and permanently appended to the blockchain.

CONSENSUS

When a transaction is made, all nodes on the network verify that it is valid on the blockchain, and if so, they have a consensus.

CONSENSUS PROCESS

Refers to those nodes that are responsible for maintaining the blockchain ledger so that a consensus can be reached when a transaction is made.

CONSORTIUM BLOCKCHAIN

A privately owned and operated, yet publicly transparent, blockchain.

CRYPTOGRAPHIC HASH FUNCTION

This process happens on a node and involves converting an input – such as a transaction – into a fixed, encrypted alphanumeric string that registers its place in the blockchain. This conversion is controlled by a hashing algorithm, which is different for each cryptocurrency.

CRYPTOGRAPHY

The process of encrypting and decrypting information.

COIN

A representative store of digital value that lives on a given blockchain or cryptocurrency network. Some blockchains have the same name for both the network and the coin, like Bitcoin. Others can have different names for each, like the Stellar blockchain, which has a native coin called Lumen.

COINBASE

A popular centralized cryptocurrency exchange. Coinbase made history recently as the first cryptocurrency exchange to go public on the Nasdaq.

COLD WALLET/COLD STORAGE

A secure method of storing your cryptocurrency completely offline. Many cold wallets (also called hardware wallets) are physical devices that look similar to a USB drive. This kind of wallet can help protect your crypto from hacking and theft, though it also comes with its own risks – like losing it, along with your crypto.

CRYPTOCURRENCY

A type of currency that's digital and decentralized. Cryptocurrency can be used to buy and sell things, or as a long-term store of value.

DAO

Acronym for "decentralized autonomous organization"

DAPP

Shorthand for "decentralized application"

DECENTRALIZED APPLICATION

A computer program that utilizes a blockchain for data storage, runs autonomously, is not controlled or operated from a single entity, is open source and has its use incentivized by the reward of fees or tokens.

DECENTRALIZED EXCHANGE

A peer-to-peer exchange that allows users to buy and sell cryptocurrency and other cryptoassets without a central intermediary involved.

EIP

An acronym for "Ethereum Improvement Proposal," which is typically followed by the assignment number of the standard (e.g., "EIP-20"), and which refers to a protocols and specifications design document for the Ethereum network. EIPs are typically related to core functionality of the Ethereum network, as opposed to application layer specifications.

ERC

An acronym for "Ethereum Request for Comment," which is typically followed by the assignment number of the standard (e.g., "ERC-20"), and which refers to a standardization document containing application layer specifications that programmers use to write Ethereum-based smart contracts. Different ERC standards have emerged with different.

ERC-20

An ERC standard detailing the protocol for the issue and transfer and other aspects of fungible tokens on the Ethereum network.

ERC-721

One of the ERC standards used to build non-fungible or unique tokens on the Ethereum blockchain. While most tokens are fungible (every token is the same as every other token), ERC-721 tokens are unique.

ERC-1155

An ERC standard for the specifications of a smart contract interface that can represent any number of fungible and non-fungible token types in single transactions.

DECENTRALIZED AUTONOMOUS ORGANIZATION

Refers to organizations that are run by an application (computer program) rather than direct human input. Control of this application is granted to everyone rather than a single central entity.

DECRYPTION

Turning encrypted cipher text back into plain text.

DEFLATION

When the demand for a particular cryptocurrency decreases, bringing down the price of its economy.

DEPTH CHART

This graph plots the requests to buy (known as bids) and the requests to sell (known as asks) on a chart. Because you can put a limit order on your buy or sell transaction, the depth chart shows the crossover point at which the market is most likely to accept a transaction in a timely fashion. It also shows if there are any significant buy walls or sell walls in play.

DETERMINISTIC WALLET

This type of wallet is created by producing multiple keys from a seed. If you lose this wallet, your wallet key can be recovered from the seed. Plus, when you make transactions, instead of producing new keys each time, you use variations from the seed, which makes it more transferable

DIFFICULTY

When someone refers to difficulty in the cryptocurrency space, they are referring to the cost of mining in that moment in time. The more transactions that are trying to be confirmed at any single moment in time, divided by the total power of the nodes on the network at that time, defines the difficulty. The higher the difficulty, the greater the transaction fee – this is a fluid measurement that moves over time.

DIGITAL COMMODITY

An intangible, hard-to-get asset that is transferred electronically and has a certain value.

DIGITAL CURRENCY

Another term for digital commodity.

DIGITAL SIGNATURE

Used to confirm that a document being transmitted electronically is authentic. They generally appear as a code generated by a public key encryption.

DISTRIBUTED LEDGER

A ledger that is stored in multiple locations so that any entries can be accessed and checked by multiple parties. In cryptocurrency, this refers to the blockchain being held onmultiple nodes on the network, all of which are checked simultaneously.

DOUBLE SPEND

This occurs when someone tries to send a cryptocurrency to two different wallets or locations at the same time.

DUMP

The term used to describe selling all (or a lot) of your cryptocurrency.

DUMPING

When a lot of people dump at once, causing a sharp downward movement in a cryptocurrency's price.

DUST TRANSACTION

Sometimes people will look to slow the network by deliberately flooding it with minor transactions that are incredibly small. These minuscule amounts are referred to as a dust transaction.

DYOR

Acronym for "do your own research".

DECENTRALIZATION

The principle of distributing power away from a central point. Blockchains are traditionally decentralized because they require majority approval from all users to operate and make changes, rather than a central authority.

DECENTRALIZED APPLICATIONS (DAPPS)

Applications designed by developers and deployed on a blockchain to carry out actions without intermediaries. Decentralized finance activities are often completed using decentralized apps. Ethereum is the main network supporting activities in decentralized finance.

DIGITAL GOLD

Experts sometimes compare specific cryptocurrencies to real gold based on the way it can store and increase in value. Bitcoin is commonly referred to as digital gold.

ETHEREUM

The second largest cryptocurrency by trade volume, Ethereum is a crypto network and software platform that developers can use to create new applications, and has an associated currency called ether.

EXCHANGE

A cryptocurrency exchange is a digital marketplace where you can buy and sell cryptocurrency.

ETHER (ETH)

The native token used to operate the Ethereum platform. Ether provides the incentive for nodes to validate blocks on the Ethereum network that contain the smart contract code.

FIAT CURRENCY

Money declared by a government to be legal tender (e.g., GBP or USD).

FUD

An acronym for "fear, uncertainty and doubt," being a jargon term used in the cryptoasset industry to describe propaganda tactics and the spread of disparaging information about a crypto project or token, especially a competing one.

FORK

When a blockchain's users make changes to its rules. These changes to the protocol of a blockchain often result in two new paths — one that follows the old rules, and a new blockchain that splits off from the previous one. (Example: a fork of Bitcoin resulted in Bitcoin Cash).

GAS

A fee that developers have to pay to the Ethereum network in order to use the system. Gas is paid in ether, the native cryptocurrency of Ethereum.

GENESIS BLOCK

The first block of a cryptocurrency ever mined.

GAS LIMIT

The maximum amount of units of gas that the user is willing to spend on a transaction. The transaction must have enough gas to cover the computational resources needed to execute the code. All unused gas is refunded at the end of the transaction.

GAS PRICE

The price that a user is willing to pay for a transaction in terms of GWei.

GWEI

Each Ether is divisible into 1018 sub-units, called Wei. 1 GWei = 1 gigaWei = 1 billion Wei, or 1 billionth of an Ether.

HODL

Stands for "Hold On for Dear Life" though the term originated from a user typo on a Bitcoin forum in 2013. It refers to a passive investment strategy in which people buy and hold onto cryptocurrency — instead of trading it — in the hopes that it increases in value.

HASH

A unique string of numbers and letters that identify blocks and are tied to crypto buyers and sellers.

HOT WALLET

A software-based cryptocurrency wallet connected to the Internet. While more convenient for quickly accessing your crypto, these wallets are a bit more susceptible to hacking and cybersecurity attacks than offline wallets — just as files you store in the cloud may be more easily hacked than those locked in a safe in your home.

HARD FORK

A fork that can render previously invalid types of transactions valid, and vice versa. This type of fork requires all nodes and users to upgrade to the latest version of the protocol software. Therefore, a hard fork is a permanent change to the rules of the previous version of the blockchain, and nodes using the previous version will not recognize the new version. A hard fork may be implemented to correct security vulnerabilities, add new functionality or reverse transactions (see DAO). Bitcoin Cash is a hard fork of Bitcoin.

INITIAL COIN OFFERING (ICO)

A way that funds are raised for a new cryptocurrency project. ICOs are similar to Initial Public Offerings (IPOs) of stocks.

JUST

...under halfway now — are you still with us?

KEYS

Public key cryptography uses public and private keys to encrypt and decrypt data. In the context of cryptocurrencies and, more specifically, Bitcoin, a private key is a secret number that relates to a user's Bitcoin address. The private key enables a user to spend Bitcoins as it generates a digital signature, mathematically confirming the user has the right to issue each transaction that they send out. The Bitcoins are sent to another user's public key address and become their property, because their private key cannot be identified from their public key.

LAYER 1 BLOCKCHAIN

Describes a blockchain network that is the fundamental blockchain network in its relevant ecosystem for on-chain transactions. As a defining feature, Layer 1 networks can validate and finalize transactions without the need for another network (e.g., the Bitcoin or Ethereum networks). Developers can create Layer 2 networks atop of Layer 1 networks, often done to improve transaction efficiencies or speed. The Bitcoin Lightning Network is an example of a Layer 2 network.

LEDGER

A database that records transactions.

LEGAL SMART CONTRACT

A type of smart contract that can be used to define and perform the obligations of a legally binding contract.

METAVERSE

Science fiction author Neal Stephenson coined the term "metaverse" in his 1992 cyberpunk novel "Snow Crash." There is no market consensus on the meaning of metaverse as broadly used today, but references to a metaverse tend to be used to describe a digital environment that provides enhanced immersive experiences.

MINTING

The process of creating new tokens in a blockchain network, typically used in reference to the creation of non-fungible tokens. In the context of NFTs, this term also incorporates the linking of digital content to non-fungible tokens on a blockchain network, as a means of creating a digital asset.

MARKET CAPITALIZATION

Cryptocurrency market capitalization refers to the total value of all the coins that have been mined. You can calculate a crypto's market cap by multiplying the current number of coins by the current value of the coins.

MINING

The process whereby new cryptocurrency coins are made available and the log of transactions between users is maintained.

MINTING

The process of creating new tokens in a blockchain network, typically used in reference to the creation of non-fungible tokens. In the context of NFTs, this term also incorporates the linking of digital content to non-fungible tokens on a blockchain network, as a means of creating a digital asset.

NODE

A computer that connects to a blockchain network.

NON-FUNGIBLE TOKENS (NFTS)

Non-fungible tokens are units of value used to represent the ownership of unique digital items like art or collectibles. NFTs are most often held on the Ethereum blockchain.

NICK SZABO

The computer scientist credited with coining the term "smart contract."

NONCE

In cryptography, an arbitrary string of numbers that can only be used once. The nonce is an important concept in proof-of-work mining, as used by Bitcoin, for example.

OFF-CHAIN

Activity that happens, or data that is stored, outside the blockchain ledger, but may be referenced from it.

ORACLE

A trusted off-chain agent for a distributed ledger system that can submit information to be used by on-chain smart contracts. For example, an oracle might link to a third-party verified source of weather data, travel timetables, stock market information, registry information, or to a physical Internet of Things device.

PAYMENT TOKENS

Digital tokens that enable the token holder to acquire goods or services from the token issuer (i.e., performs as virtual currency).

PEER-TO-PEER

Two users interacting directly without a third party or intermediary.

PRIVATE KEY

The encrypted code that allows direct access to your cryptocurrency. Like your bank account password, you should never share your private key.

PERMISSIONED

A DLT system where only pre-authorized nodes can finalize transactions into the ledger. Consortium blockchains are permissioned systems.

PERMISSIONLESS

A DLT system where all nodes can access, submit and be selected to finalize transactions into the ledger.

PHYGITAL

A term combining physical and digital (pronounced "fidge-it-al"). The concept of using technology to bridge the digital world with the physical world with the purpose of providing a unique interactive experience for the user.

POAP

An acronym for "Proof of Attendance Protocol." A POAP NFT is a type of NFT that shows that you attended a particular event or experience — a digital memento.

PRE-SALE

Tokens are offered for sale to a limited set of participants before they are made available to the general public via an ICO.

PRIVATE BLOCKCHAIN/DLT

A blockchain/DLT that is only accessible to certain participants. Only pre-authorized nodes can access and submit transactions or finalize transactions. A private blockchain/DLT is always a permissioned blockchain/DLT. Company blockchains are private systems.

PUBLIC BLOCKCHAIN/DLT

A blockchain/DLT system that permits anyone with a computer to create a node. A public blockchain can be permissioned or permissionless.

PROOF-OF-STAKE

An alternative to proof-of-work.
Mining requires a lot of computing power, which translates to high electricity usage. Proofof-stake seeks to address this by limiting what you can mine to the stake of the particular cryptocurrency that you own (for example, if you own 1% of all Ether available, then you can only mine 1% of the blocks. This also mitigates the risk that miners create competing forks because this would devalue each miner's stake).

PROOF-OF-WORK

Proof-of-work involves using computer processing power to perform repeated hash operations with different nonce values to find a resulting hash below the required difficulty. Finding such a hash allows the miner to add a block of transactions to the chain tip of a growing blockchain. Those involved in mining ("miners") are incentivized to use their computing resources to mine by receiving block rewards. Because this is difficult and consumes large amounts of electricity, it is an effective way of securing the blockchain from attempted rewriting of history (e.g., to double-spend) or breaking consensus.

PUBLIC KEY

A cryptographic key used to encrypt messages. A user can "sign" data with their private key and anyone who knows the user's public key can verify that the signature is valid. However, encrypted messages can be deciphered only by using the paired private key, which cannot be calculated from knowing the public key. A Bitcoin wallet address is a hashed version of the user's public key.

QUANTUM COMPUTING

Quantum computing is seen as a possible threat to the security of blockchain systems because quantum computers are expected to be able to make decrypting information encrypted using certain mathematical principles (such as prime factorization) far easier. These principles underpin many of the encryption methods (such as the SHA-256 hash) used in not only the blockchain industry, but also in securing information transmitted over the internet.

REGULATORY SANDBOX

A controlled space set up by regulators, such as the UK's Financial Conduct Authority, to allow authorized and unauthorized firms to test innovative products services, business models and delivery mechanisms in the real market with real consumers.

SATOSHI NAKOMOTO

The pseudonymous creator of Bitcoin. No one knows the true identity of Nakomoto — or if it's more than one person.

SMART CONTRACT

An algorithmic program that enacts the terms of a contract automatically based on its code. One of the main value propositions of the Ethereum network is its ability to execute smart contracts.

STABLECOIN OR DIGITAL FIAT

A stablecoin pegs its value to some other non-digital currency or commodity. A digital fiat represents a fiat, or government-backed currency on the blockchain. (Example: Tether, which is pegged to the U.S. dollar)

SHA-256 HASH

A "Secure Hash Algorithm 2" function that produces 256-bit long output values. The cryptographic hash algorithm used in proof-of-work mining to secure Bitcoin and many other blockchain-based cryptocurrencies (notably not Ethereum, Monero, or Ripple).

SIDE CHAIN

A blockchain that is connected to a parent (primary) blockchain and allows a user to use the cryptoassets securely within that blockchain, but also transfer cryptoassets to and from the parent blockchain.

SOFT FORK

Unlike a hard fork, in a soft fork, the fork is a software upgrade that is backwardscompatible, i.e., existing nodes will recognize the new code and still be able to function on the network, but cannot take advantage of the new features on offer. Because of this reduced functionality, soft forks incentivize those who have not upgraded to upgrade.

TIMESTAMP

Each block contains a timestamp of when it was created. This provides an indication of when a transaction was added to the chain.

TOKEN

A unit of value on a blockchain that usually has some other value proposition besides just a transfer of value (like a coin).

UTILITY TOKENS

A token that provides users with digital access to an application, product or service (think membership card).

VITALIK BUTERIN

Programmer who invented Ethereum in 2015.

VERIFICATION

Transaction verification is a mathematical process of checking that a transaction submitted to a node is a permitted unique transfer of unspent value (see Double-spending) and that the correct private key has been used to sign the transaction. Block verification checks additional parameters involved in the consensus process, for example, that the block has been correctly mined and has an appropriate timestamp.

WEB3

An envisaged version of the internet that is decentralized and based on peer-to-peer technologies, such as public blockchains, and decentralized participants, such as DAOs, and that incorporates digital assets and currencies in a token-based economy.

WALLET

A place to store your cryptocurrency holdings. Many exchanges offer digital wallets. Wallets may be hot (online, software-based) or cold (offline, usually on a device).

WHALE

A term used to describe extremely wealthy investors or traders who have enough funds to manipulate the market.

WHITELIST

Prior to an ICO, interested parties can sign up/register their involvement and intent to purchase or even purchase under pre-sale conditions. The list of these parties is referred to as the whitelist.

WHITE PAPER

A detailed explanation of a cryptocurrency, designed to offer satisfactory technical information, explain the purpose of the coin and set out a roadmap for how it plans to succeed. It's designed to convince investors that it's a good choice ahead of an ICO.

XRP

XRP is the native cryptocurrency of the Ripple platform. Unlike Bitcoin, XRP is pre-mined, i.e., it was all introduced at its inception.

YIKES

With this much jargon, you can see why blockchain causes so much head-scratching.

ZERO KNOWLEDGE PROOF

A cryptographic method by which one party can prove (the prover) to another party (the verifier) that they know secret information, without revealing the secret information (for example, by way of analogy, in the case of identity, being able to prove that you are over 21 without revealing your actual age or date of birth).

ZERO CONFIRMATION TRANSACTION

Alternative phrasing for an unconfirmed transaction.

www.cyber-gear.io