BLOCKCHAIN AND BITCOIN FUNDAMENTALS: GLOSSARY OF KEY TERMS

By: George Levy

BlockchainInstituteofTechnology.com

Disclaimer

The information provided within this book and accompanying course “Blockchain and Bitcoin Fundamentals” is for general informational purposes only. It is not advice, and should not be treated as such. References to publicly available information, including trademarks, are without any prior consent by the owners. They are for illustrative purposes only. Trademarks belong to the respective owners, who are not affiliated with this book. While the author attempts to keep the information up-to-date and correct, there is no assurance or warranty, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the information, products or services contained in this book for any purpose. Any use of this information is at your own risk. All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system, without written permission from the author. The author bears no responsibility for any consequences resulting from the use of information provided in this book and course. Please use all information at your own risk.

51% Attack

A situation where more than 50% of the computing power on a cryptocurrency network is controlled by a single entity (a miner or a pool of miners.)

If this were to happen, this would in theory make them the authority in the network which would have complete control over all the other clients to approve and issue any transaction and stop any other transactions from being confirmed.

21 Million

The total number of bitcoins which will ever be available. This limit of 21 million bitcoins is programmed into the protocol and can never be changed. It is projected that the last bitcoin will be mined sometime in the year 2140.

Address

In Bitcoin, an address is used to receive and send transactions on the Bitcoin network. Addresses can be represented by a QR code or a string of alphanumeric characters. A Bitcoin address is mathematically related to the public key for a wallet, as it is the hashed version of that wallet's public key.

Agreement Ledger

Agreement ledgers are distributed ledgers used by two or more parties to perform negotiations and reach agreement.

Altcoin

A catch-all term for cryptocurrencies beyond Bitcoin such as Litecoin, Monero and Zcash among many others.

AML

Anti-Money-Laundering or AML is a set of laws and regulations which have been designed to stop the process of generating money through illegal activities.

ASIC

"Application Specific Integrated Circuit" (ASIC) chips are special type of computer chip designed to perform a specific task. In the context of Bitcoin, they are used by miners to process SHA-256 hashing problems in order to mine new bitcoins.

Bitcoin

The name of the Bitcoin network upon which people transact in bitcoin. Not to be confused with the actual currency which is spelled in lowercase as bitcoin.

bitcoin

A bitcoin is an asset of value that can be exchanged securely between two parties over the web, without needing a third-party like a bank, government or other organization. “bitcoin” with a lowercase b is the proper spelling for the cryptocurrency known as bitcoin. Whenever you write a certain amount of bitcoin, it should be spelled in lowercase, as in “I sent 5 bitcoins to my friend Bob.”

Bitcoin Cash

A cryptocurrency born out of the August 1st, 2017 hard fork in the Bitcoin blockchain. Bitcoin Cash increases the block size limit to 8 Megabytes (8 MBs) as well as implementing two new features: 1) Replay and wipeout protection which enables Bitcoin and Bitcoin Cash to co-exist as distinct and separate cryptocurrencies on separa blockchains, and 2) New SigHash Type - which is a new way of signing transactions. This new SigHash Type was implemented to further reduce the risk of conflicts between the Bitcoin main blockchain and the Bitcoin Cash blockchain.

Bitcoin Scripting Language

All Bitcoin transactions have scripts embedded into its input and outputs which are written in a very simple programming language called Script. This Bitcoin scripting language is purposefully not Turing Complete and does not allow loops.

Block

Transaction data is recorded on a Blockchain in files called Blocks. As new transactions are created and added to a Blockchain, they are grouped into Blocks and added chronologically to the end of the chain. Once a block is added to a Blockchain, it is added permanently, and can never be changed or removed.

Block Explorer

A Block Explorer is a type of tool that can provide information on the contents of individual blocks and transactions that are found on a Blockchain.

Block Height

The Block Height of a Block refers to how far along on a Blockchain a specific Block is found. A Block Height of 0 would imply that it is the first block on a Blockchain, also known as the Genesis Block.

Block Reward

This is the reward given to a miner who has successfully hashed a transaction block. In Bitcoin, the current reward is 12.5 BTC. Block Rewards can be a mixture of coins and transaction fees, and varies depending on the type of cryptocurrency.

Blockchain

A constantly growing ledger which keeps a permanent record of all the transactions that have taken place, in a secure, chronological and immutable way.

BTC

The short currency abbreviation for Bitcoin. Much like USD stands for US Dollars and EUR stands for Euros.

Byzantine Generals' Problem

The Byzantine General Problem is also known as a "Coordinated Attack Problem", and it refers to the problems involved in coordinating the actions of multiple parties communicating over an unreliable link. In Bitcoin, this involves the fact that a malicious participant could attempt to add a fraudulent block of transactions to the blockchain. This problem is solved by the use of "Proof of Work" and the Blockchain keeping track of every single block of transactions previously added to the blockchain.

Central Ledger

A ledger maintained by a central agency, as opposed to a decentralized ledger.

Client

Software that runs on a computer such as a desktop or a laptop, or a mobile device. In Bitcoin, it can refer to the Bitcoin client running on a Node which connects to the Bitcoin network and processes transactions, or it could also refer to a Bitcoin wallet.

Colored Coins

A usage of Bitcoin's Scripting Language that enables the storing of small amounts of metadata on the Bitcoin blockchain. Colored coins can be used to represent and manage real world assets, and because they are running on the Bitcoin blockchain, they can leverage Bitcoin's immutability, permanence, ease of transfer and transparency among others. Colored coins serve as tokens that can be marked to represent and prove ownership of other types of assets such as real estate, precious metals, company shares and others.

Confirmation

The process of verifying transactions on the network. In the case of Bitcoin, this is done through mining and proof-of-work. Once transactions are confirmed, they cannot be reversed, and they prevent any possibility of double spending.

Consensus Point

The moment, established as a moment in time or by the set number of records to be added to the ledger, where peers meet and agree on the state of the ledger.

In Bitcoin, this is when several nodes, usually the majority of nodes on the network, all have the same blocks in their locally-validated best block chain.

Consensus Process

In Bitcoin, the consensus process is commonly referred to as “emergent consensus” and was an invention by the creator of Bitcoin Satoshi Nakamoto. Emergent consensus is a decentralized process which develops from four different processes occurring independently across the network.

These processes are:

1. Verification of transactions by every full node.
2. Aggregating those transactions into new blocks by mining nodes along with the related, demonstrated proof-of-work.
3. Verification of the new blocks by every node and assembling into a chain.
4. Selection by every node of the chain with the most computation demonstrated through proof-of-work.

CPU

Central Processing Unit (CPU) is the type of computer processor found in today’s everyday computers. In the early days of Bitcoin, it was possible to use a regular computer and its CPU to mine for bitcoin, but at this point that process would be too slow and inefficient when compared with other hardware such as FPGAs, GPUs and ASIC powered miners.

Cryptocurrency

Cryptocurrency, also written as crypto currency, is a type of digital asset designed as a medium of exchange. It uses cryptography to control the creation of additional units of the crypto currency, and to secure transactions.

Cryptographic hash function

Cryptographic hash function is a hash function which takes an input, or message, and condenses it into an irreversible fixed-size alphanumeric string, or hash.

Per the hash definition, no two different inputs or messages should produce the same hash value. As a result, the hash generated from an input be regarded as a unique digital signature as it is practically impossible to duplicate.

If an algorithm produces the same result for different strings of text, the algorithm is not "collision free" and is vulnerable to being cracked.

Cryptography

Cryptography, also known as cryptology, refers to the study and application of techniques used to transmit, protect and store information and communications in a secure and private way, in order to avoid being intercepted by third parties.

DAO / DAC

Decentralized Autonomous Organization (DAO), sometimes referred to as a Decentralized Autonomous Corporation (DAC) is an organization that is fully maintained on a blockchain, and is run through rules programmed as smart contracts on that blockchain.

In a decentralized autonomous organization, the organization runs automatically per the instructions and agreements that have been programmed into the smart contracts that establish how the organization should run.

DApp

A decentralized application (DApp) is an application that runs on a decentralized peer-to-peer network, typically making use of a Blockchain and smart contracts. Popular development platforms for DApps include Ethereum and RSK.

Dash

Dash is an open source cryptocurrency that offers instant and private transactions. Dash was rebranded from "Darkcoin" into "Dash" in 2015 as a short form of saying "digital cash"

DDoS

Distributed Denial of Service (DDoS) is a type of cyber attack where multiple systems overwhelm the bandwidth and resources of a targeted system with a Denial of Service (DOS) attack. In the process, the target machine or network resource which is being attacked is rendered unavailable to its intended users.

Decentralization

Decentralization is the process of spreading or distributing functions and power away from a centralized location or authority.

Decentralized Application

A decentralized application (DApp) is an application that runs on a decentralized peer-to-peer network, typically making use of a Blockchain and smart contracts. Popular development platforms for

DApps include Ethereum and RSK.

Difficulty

In Bitcoin, the difficulty is measured by how difficult it is to find a hash below a given target. The difficulty level changes every 2016 blocks based on the time it took to find the previous blocks. The goal is to keep the time to process per block to 10 minutes and the difficulty level adjusts up or down as needed to achieve that schedule.

Digital Signature

Digital signature is a term used to describe the marking or signing of an electronic document through the use of a technology known as public-key cryptography.

Disintermediation

The process of reducing or eliminating intermediaries (i.e.. “middle-men”) between parties in a transaction. The fact that Bitcoin enables the exchange of value between two parties directly over the Internet without requiring the services of a bank or some other institution is an example of disintermediation.

Distributed Computing

Distributed computing is an approach to computing in which components of a software system are distributed, or shared, among multiple computers. The goals of distributed computing are to improve efficiency and performance, as well as eliminate a single point of failure by sharing the tasks across multiple systems.

Distributed Ledger

A distributed ledger, also called a shared ledger or replicated ledger, involves having a single set of data items which are replicated and shared across multiple sites. In Bitcoin, the Bitcoin blockchain serves as a distributed ledger as it contains all the transactions that have ever happened on Bitcoin, and it is replicated across all the nodes that form the Bitcoin network.

Dogecoin

A type of cryptocurrency that features a dog called “Shiba Inu” as its logo.

Double Spending

A form of attack in which a given set of currency is spent in more than one transaction. This is one of the key attacks that Bitcoin addresses through the use of Blockchain technology and distributed consensus.

ETF

Exchange Traded Fund. An ETF is a security that tracks an index, commodity, bond or other assets. It is traded like a common stock on a stock exchange, hence the name exchange traded fund.

Ether

The cryptocurrency transacted through the Ethereum platform. It is the “fuel” used as incentive to run applications on the Ethereum platform.

Ethereum

A decentralized platform that runs smart contracts.

Exahashes / Sec

Hashes per second is a unit which represents the number of double SHA-256 computations performed in one second and is used to calculate the Bitcoin network’s overall hash rate. An Exahash/Sec (EH/s) translates to 1 Quintillion Hashes per second. (1,000,000,000,000,000,000)

Faucet

In Bitcoin, a faucet is a reward system, typically a website or an app, that issues rewards in the form of bitcoin. These rewards are very small, usually in the order of one or a few satoshi (0.00000001 bitcoin.)

Fiat Currency

Fiat currency is a type of currency that is backed by a government that issues it. Currencies like the US Dollar, Euro, Yen and Yuan are all examples of fiat currency.

FinCEN

FinCEN stands for Financial crime enforcement network. It is a bureau of the US Department of Treasury that supports the detection, investigation and prosecution of financial crimes both domestic and international.

Fork

A divergence on a blockchain where the fork causes there to be two different versions of the blockchain. There are two types of forks: hard and soft.

FPGA

Field Programmable Gate Arrays (FPGA) are a type of integrated circuit that can be configured after being built. Because of this, mining hardware manufacturers can purchase multiple FPGAs, configure them for mining and include them in their hardware. They can offer performance levels above CPU and GPU powered miners, and you can use multiple chips in a single miner.

Full Node

In Bitcoin, any computer that connects to the Bitcoin network is called a node. However, a Full Node is a type of Node that fully enforces all the rules of Bitcoin and as a result can accept and validate transactions and blocks.

Genesis Block

The first block on a Blockchain. This is the first block of transactions done on a Blockchain and upon which all future transactions grow on top.

Gigahashes / Sec

Hashes per second is a unit which represents the number of double SHA-256 computations performed in one second and is used to calculate the Bitcoin network's overall hash rate. A Gigahash/Sec (GH/s) translates to 1,000,000,000 hashes per second.

GPU

Graphic Processing Unit (GPU). A type of electronic circuit which is used to perform visual display functions. The GPU typically renders images animations and video on a computer's screen.

GPU chips were used extensively by Bitcoin miners as they processed Bitcoin Proof-of-Work calculations faster than the previous CPU powered generation of hardware. GPU powered mining is almost non-existent anymore as Bitcoin mining difficulty has increased dramatically due to the release of ASIC powered Bitcoin Mining hardware.

Halving

In Bitcoin, the process of halving involves the reduction by half of the reward paid out to Bitcoin miners. This halving process takes place once every four years, and is part of Bitcoin's predictable, transparent monetary policy which clearly spells out that there will only be a maximum of 21 million bitcoin ever produced. This halving process ensures that that objective is met.

Hard Fork

A hard fork as related to a cryptocurrency blockchain such as Bitcoin, is a permanent divergence/split in the blockchain.

On August 1st, 2017, Bitcoin underwent a Hard Fork at Block 478,558 which effectively split Bitcoin into two separate Blockchains:

1) Bitcoin - The main Bitcoin blockchain which retained a 1MB Block size. This is the main Bitcoin blockchain and what has been known as Bitcoin since its launch in 2009.

and

2) Bitcoin Cash - A new cryptocurrency altogether. This Bitcoin Cash cryptocurrency runs on a separate blockchain, and has its miners running a different, new software client, which is not compatible with the main Bitcoin software. This non-compatibility is what caused the break in the blockchain as all nodes running the previous Bitcoin software would reject the new Bitcoin Cash blocks which allow for the 8MB Block size.

Hard forks typically require a change in the protocol that runs the blockchain and are not backwards-compatible. In other words, nodes running older versions of the protocol client will not accept the new blocks on the fork and will require to be upgraded if they are to participate in the new blockchain generated by the hard fork.

This is different from a Soft Fork in which no-one is forced to update their software and non-upgraded transactions will still go through as normal..

Hash

In cryptography, a hash is a type of hash function which takes an input and returns a fixed-size alphanumeric string. It is used to create a kind of "digital signature" which cannot be deciphered but will always give that result. An effective Hash function, such as SHA-256 which is the Hash function used by Bitcoin, has three qualities:

1. It is very easy to create a hash for a set of data.
2. It is extremely difficult (practically impossible) to reverse engineer and determine what was the original data that generated the hash.
3. It is extremely unlikely that different inputs may yield the same hash.

The process of generating a hash is called "Hashing".

Hash Rate / Hashrate

Hash rate is the measurement of the processing power of the Bitcoin network.

Hashing

Hashing is the act of generating a Hash. Hashing condenses an input into an irreversible fixed-length value. (See Hash)

Immutability

The quality of an object to remain unchanged. In blockchain, immutability applies to the fact that once a block has been added to a blockchain, it cannot be changed.

IPFS

InterPlanetary File System - A protocol designed to enable a permanent and decentralized method for storing and sharing files.

Key Management

In Bitcoin, Key Management involves the managing of public and private keys to access bitcoin funds. Managing keys in bitcoin involves the proper use and protection of the various keys required to access and transfer funds.

Kilohashes/Sec

Hashes per second is a unit which represents the number of double SHA-256 computations performed in one second and is used to calculate the Bitcoin network's overall hash rate. A kilohash/Sec (kH/s) translates to 1,000 hashes per second.

KYC

"Know Your Customer" or KYC refers to the process of a business verifying the identity of its clients. KYC is also used when referring to the type of bank regulation which oversees these activities.

Ledger

A ledger is a file which keeps a collection of financial accounts. In Bitcoin, the Bitcoin Blockchain acts as a ledger which keeps track of all the transactions that have taken place on the Bitcoin network.

Litecoin

A type of open source cryptocurrency created in 2011. Although it has some similarities to Bitcoin, Litecoin is a different type of cryptocurrency altogether and it processes a block of transactions every 2.5 minutes instead of every 10 minutes.

mBTC

.001 BTC. One thousandth of a Bitcoin

Megahashes/Sec

Hashes per second is a unit which represents the number of double SHA-256 computations performed in one second and is used to calculate the Bitcoin network's overall hash rate. A Megahash/Sec (MH/s) translates to 1,000,000 hashes per second.

Merkle Root

The Merkle Root in a Bitcoin transaction block is a single hash that presents a digital fingerprint of all the transactions in that block of transactions. Every block header in Bitcoin contains a Merkle Root, which summarizes the contents of the entire block.

Merkle Tree

A Merkle Tree, also known as a Hash Tree, is the structure built from the various cryptographic hashes in a blockchain. Since a hash generated from a certain input will always equal the same, and it will be different from any hash generated from a different input. A Merkle Tree is a very effective way to keep track that all the transactions that build the tree are accurate and haven't been tampered with.

Microtransaction

Microtransactions are very small transactions, usually in the magnitude of a few pennies or less.

Miner

A special type of node in a cryptocurrency network which processes and confirms transactions through what is called "mining."

Mining

Mining in the context of cryptocurrency involves processing and confirming transactions of that cryptocurrency. This process requires solving advanced math problems of increasing difficulty. For performing these tasks, miners are typically compensated for their work in the form of the cryptocurrency they are mining for. This mining process is how new units of cryptocurrency are created and added to the system.

Mining Pool

A mining pool is a mining approach where multiple miners pool their resources together to increase their overall hashing power, and then split equally the rewards they receive.

Mixing Service

Mixing, also known as Tumbling, is a process which involves a third party in order to break the connection between a Bitcoin address sending coins and the address they are being sent to.

Monero

A type of cryptocurrency created in 2014 which focuses on privacy, decentralization and scalability.

Mt. Gox

A bitcoin exchange based in Tokyo, Japan started in July, 2010 which is the subject of one of the biggest scandals in Bitcoin history. By 2013, Mt. Gox was the world's leading Bitcoin exchange, handling 70% of all bitcoin transactions. The company ended operations and suspended trading in February 2014, when they announced that 850,000 bitcoins were missing (a value of over $450 Million USD at the time) and that they were most likely stolen.

Multisignature / Multisig

In Bitcoin, Multisignature is a type of technology which requires multiple parties to digitally sign a transaction before it can be accepted and processed. This is done to add additional security to these transactions.

Node

In Bitcoin, any computer that connects to the Bitcoin network is called a node.

Nonce

In the context of cryptography, a nonce is an arbitrary number that will only be used once. A nonce is typically a random number or a pseudo-random combination that is used as part of the authentication process to ensure that previous communications could not be used as part of a malicious attack.

Orphan Block

An orphan block is a valid block that is not part of the main blockchain. These can happen naturally when two miners produce blocks simultaneously or when an attacker tries to reverse transactions. Valid transactions which wind up in an orphan block are eventually returned for processing and wind up being successfully processed in a later block.

Paper Wallet

In Bitcoin, a paper wallet is simply a document which contains the information necessary to access a certain amount of bitcoin.

Peer-to-Peer / P2P

Peer-to-Peer computing is a type of computing architecture in which peers have the same privileges and authority, and can communicate and interact directly with one another.

Permissioned Ledger

In a permissioned ledger, transactions can only be validated and processed by participants who are already recognized and have been authorized by the ledger. Permissioned ledgers are usually associated with private blockchains where an overarching entity determines who has permission to access the ledger.

Petahashes / Sec

Hashes per second is a unit which represents the number of double SHA-256 computations performed in one second and is used to calculate the Bitcoin network's overall hash rate. A Petahash/Sec (PH/s) translates to 1 Quadrillion Hashes per second. (1,000,000,000,000,000)

Pool

See Mining Pool

Private Blockchain

A blockchain managed by a centralized authority in which the participants and contents are determined and overseen by a private entity.

Private Key

A private key in the context of Bitcoin is a secret alphanumeric key which corresponds to a Bitcoin wallet, and which can authorize bitcoins to be spent from that wallet.

Proof of Stake

Proof of stake is an algorithm used by some cryptocurrency blockchain networks to achieve distributed consensus and prevent double spending. It is different from Proof of Work in that rather than basing the odds of successfully mining a new block on the amount of work performed and the computational power of a miner - it focuses instead on the amount of cryptocurrency the miner holds.

Proof of Work

Proof of work is the algorithm used by Bitcoin and several other cryptocurrencies to achieve distributed consensus and prevent double spending.

Public Blockchain

A public blockchain is a blockchain that anyone can read and transact in. Bitcoin is an example of a public blockchain as anyone can read the contents of the blockchain, and send transactions.

Public Key

A public key in the context of Bitcoin is an alphanumeric key which corresponds to a Bitcoin wallet and can be shared with others. It is mathematically related to the Bitcoin address to the corresponding wallet as a Bitcoin address is a hashed version of the public key.

Pump and Dump

The fraudulent practice of encouraging investors to buy certain asset as a way to increase the price artificially, and then selling one's own share at the inflated price. Pump and Dump is usually referred to what are commonly known as "scamcoins."

QR Code

A two dimensional barcode which can be used to store and retrieve information. In Bitcoin, QR codes are regularly used to represent and share Bitcoin addresses. This enables an easy way to share a Bitcoin address with others.

Race Attack

A type of attach to the Bitcoin network where multiple conflicting transactions are sent to the network in rapid succession with the objective of causing a double spend.

Replicated Ledger

A replicated ledger, also called a shared ledger or distributed ledger, involves having a single set of data items which are replicated and shared across multiple sites. In Bitcoin, the Bitcoin blockchain serves as a distributed ledger as it contains all the transactions that have ever happened on Bitcoin, and it is replicated across all the nodes that form the Bitcoin network.

Ripple

Ripple is an open source technology for interbank transactions which uses distributed ledgers. By using Ripple, users can make payments between each other by using cryptographically signed transactions. These transactions can be in fiat currency or in Ripple's own internal currency XRP.

RSK / Rootstock

RSK, also known as Rootstock, is a smart contracts platform which leverages the Bitcoin network.

Satoshi

0.00000001 BTC. The smallest unit of Bitcoin possible.

Satoshi Nakamoto

Satoshi Nakamoto is the author of the white paper “Bitcoin: A Peer to Peer Electronic Cash System”. As of today, no one knows who Satoshi Nakamoto is or even if he is one person or a group of people.

Scamcoin

A catch-all term for cryptocurrencies that are designed to “get rich quick” and eventually disappear taking away all the funds invested in them.

Scrypt

Scrypt is an algorithm system used by Litecoin and other cryptocurrency miners to authenticate blocks of transaction data.

Segregated Witness (SegWit)

Segregated Witness, also known as SegWit for short, is a change that was implemented in Bitcoin on August 1st to address several perceived deficiencies in Bitcoin, including a 1 MB limit Block size.

This 1 MB Block size limit has been a severe limitation to the scalability of Bitcoin, and had been a point of dissent in the Bitcoin community as there have been multiple proposed solutions with different approaches, including the Hard Fork that eventually led to the development of Bitcoin Cash.

SegWit was successfully activated on Bitcoin on August 24th with a soft fork at block #481824, and is now live on Bitcoin. Because SegWit has been activated as a soft fork, no-one is forced to update their software and non-SegWit transactions will still go through as normal.

The key element of Segregated Witness is a change in the way that transactions are processed, primarily on how digital signatures are used. In SegWit, the Signature Data is removed from the actual Bitcoin transaction and moved to a different part of the block. This signature data is what is known as the “”Witness”” and what SegWit does is effectively “”segregate”” what witness data by moving it to a different part of the block. This effectively frees up space within the block which can be repurposed to fit in more transactions per block. This increase in Block size is one of the primary reasons for the implementation of SegWit.

Another stated benefit of SegWit is that it can address and solve Transaction Malleability a vulnerability in Bitcoin, in which an attacker, given the right conditions, could be able to change the unique ID of a Bitcoin transaction before it is confirmed on the bitcoin network.

This transaction malleability vulnerability can potentially make it possible for a malicious entity to make it seem as if a transaction had never taken place.

SHA-256

A type of Secure Hash Algorithm (SHA), published by the National Institute of Standards and Technology (NIST) and used by Bitcoin and other cryptocurrency miners to authenticate blocks of transaction data. SHA-256 generates a fixed size 256-bit (32-byte) hash that is almost unique. A SHA-

256 Hash is a one way function which cannot be decrypted back.

Sidechain

In Bitcoin, a sidechain is a Blockchain where bitcoins can be moved back and forth from the main chain, to be used for specific needs.

Silk Road

An online marketplace launched in 2011 which was used for illegal activities such as selling drugs. Part of a hidden area of the Internet commonly known as the Darknet, Silk Road was shut down by the FBI in 2013. It is famous in the history of Bitcoin as many transactions on the site were done using Bitcoin.

Smart Contracts

Smart Contracts, also known as Smart Code or Smart Property, are computer protocols that can act as a contract. A Smart Contract can handle autonomously the enforcement and fulfillment of a contract without needing a third party to oversee that the contract is executed.

Soft Fork

A soft fork is a change to the software protocol where only previously valid blocks and transactions are made invalid. Since old nodes will recognize the new blocks as valid, a soft fork is backwards compatible.

As an example, Segregated Witness (SegWit) was activated in the Bitcoin network as a soft fork at block #481824. Since it’s a soft fork, no-one was forced to update their software, and non-SegWit transactions will still go through the network as normal.compatible.

Solidity

Solidity is a high-level contract language, similar to JavaScript, which is used to develop smart contracts. Solidity is used to compile code for the Ethereum Virtual Machine and it is also compatible with RSK.

SPV

Simplified Payment Verification. In Bitcoin, it is a method used to verify transactions that have been included in a block without having to download the entire block.

Stale shares

Stale shares are shares that are sent after a block of transactions has already been solved. In other words, stale shares have been sent in late and are no longer valid.

Sybil Attack

A Sybil Attack is a malicious attack on a network that involves creating very large number of pseudonymous identities in order to gain a large influence on that network. The attack is named after the main character in the book “Sybil” who suffers from multiple personalities. This is one of the security vulnerabilities specific to peer-to-peer decentralized networks.

Taint

In Bitcoin, “taint” refers to the level of association of a bitcoin between an address and earlier addresses which have had transactions of that bitcoin. In other words, given that the Bitcoin blockchain keeps a permanent record of every single transaction ever done, it is possible to know the source and trajectory of a bitcoin throughout its history. The taint of that bitcoin can be measured as it relates to the different addresses it comes in contact with.

Terahashes / Sec

Hashes per second is a unit which represents the number of double SHA-256 computations performed in one second and is used to calculate the Bitcoin network’s overall hash rate. A Terahash/Sec (TH/s) translates to 1 Trillion Hashes per second. (1,000,000,000,000)

Testnet

An alternative blockchain for bitcoin that is used exclusively for testing purposes.

Token

A token, or digital token, can represent any type of tradable good or asset. As such, it is possible to assign an asset to a token and exchange the ownership of that token securely over the Internet without the need of a third party.

TOR

A type of free software that is used to hide the location and browsing habits of the person using it. The name TOR is short for the original name of the software “The Onion Router”

Transaction Block

Transaction data is recorded on a Blockchain in files called Blocks. As new transactions are created and added to a Blockchain, they are grouped into Blocks and added chronologically to the end of the chain. Once a block is added to a Blockchain, it is added permanently, and can never be changed or removed.

Transaction Fee

In Bitcoin, transaction fees are fees processed and received by the bitcoin miner who successfully generates a new transaction block on the Bitcoin blockchain.

Trustless

In the context of Bitcoin, Trustless means that the ability to trust in the Bitcoin network does not depend on the intentions of any particular party. Instead, Bitcoin can be trusted because it relies on the network itself, not on a particular party which could be malicious.

Tumbler

A Tumbler, also known as a Mixer, is a service which involves a third party in order to break the connection between a Bitcoin address sending coins and the address they are being sent to.

Turing Complete

A Turing Complete language is language that can encode any computation that can be conceivably carried out, including infinite loops. The Ethereum Virtual Machine and RSK are both Turing Complete.

uBTC

.000001 BTC / One microbitcoin

Vanity Address

In Bitcoin, a Vanity Address is a custom address that can be assigned to your Bitcoin address. Much like getting vanity plates for a car, a Vanity Bitcoin address provides a customized option where people can send you Bitcoin.

Virgin bitcoin

A bitcoin is said to be virgin at the moment when it is mined. In other words, it has not exchanged hands and has not been tainted.

Wallet

In cryptocurrency, a wallet is a secure digital application used to store, send and receive digital currencies such as Bitcoin, Litecoin and others.

XBT

The ISO 4217 unofficial currency code for Bitcoin, sometimes used instead of BTC.

Zcash

A decentralized cryptocurrency that offers a high degree of privacy by requiring a key to view the sender, recipient and value of transactions.

Zero-confirmation transaction

A zero-confirmation transaction is a transaction that has not been confirmed by any nodes on the network. Zero confirmation transactions do not yet reside on a block and instead are waiting in the memory pool of miners. As such, until a block is mined which includes that transaction, it is said to have zero confirmations.

ABOUT
George Levy

George Levy is an instructor on blockchain and cryptocurrency at Blockchain Institute of Technology (BIT), a leading professional training and certification organization specialized on blockchain technology.

BlockchainInstituteofTechnology.com