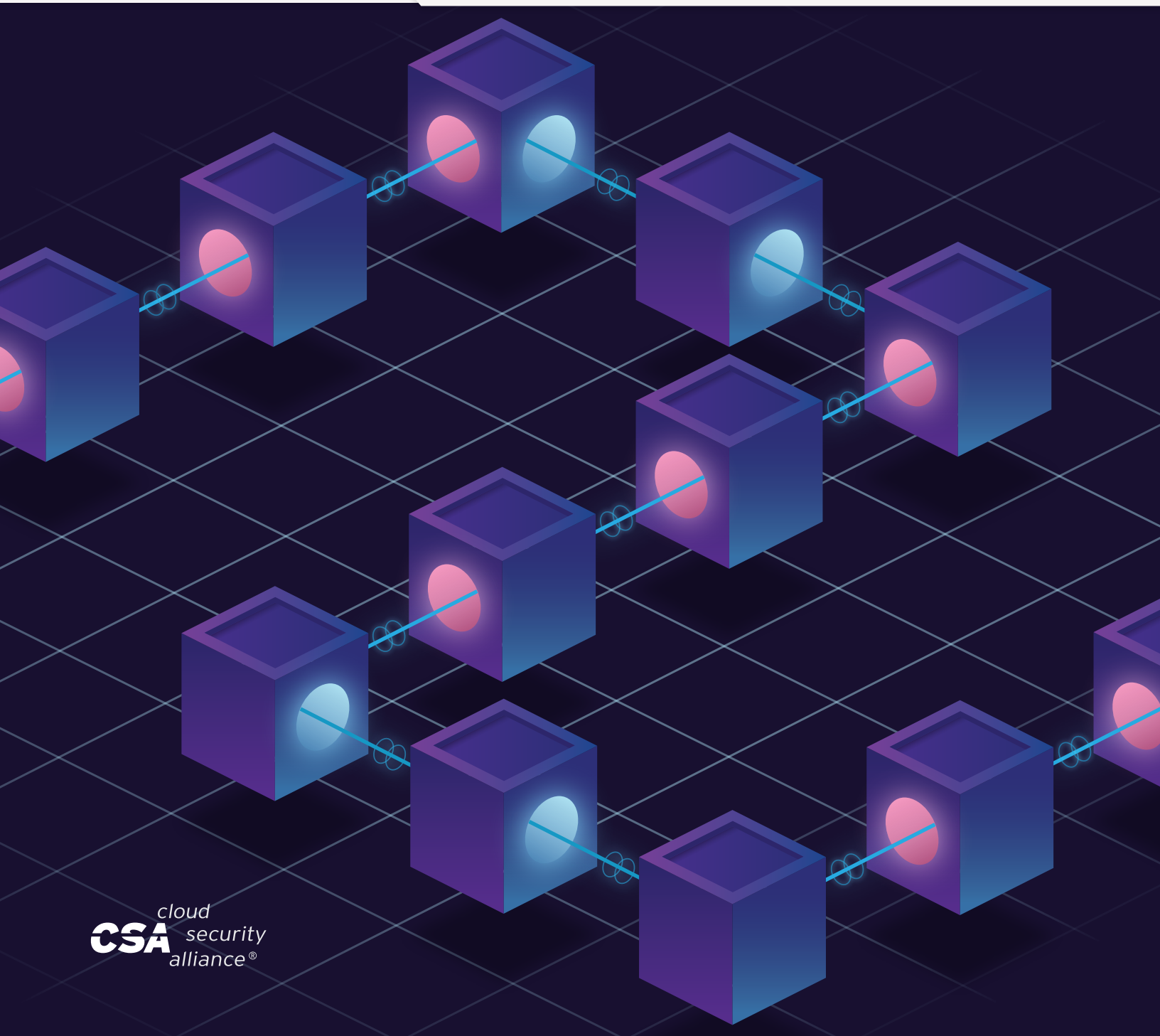
Blockchain/Distributed Ledger Working Group **Glossary**



cloud security alliance®

The permanent and official location for *Blockchain/Distributed Ledger Working Group* is https://cloudsecurityalliance.org/group/blockchain/

Acknowledgements

Cloud Security Alliance
Hillary Baron, *Research Analyst*
Stephen Lumpe, *Graphic Design*

Blockchain/Distributed Ledger Working Group
Michael Roza, *Project Lead*
Arvind Tiwari, *Co-Chair*
Sabri Khemissa, *Co-Chair*
Ashish Mehta, *Co-Chair*

The Blockchain/Distributed Ledger Working Group (BDL) was formed to research blockchain's security implications. Blockchain is a radical, evolving technology and there is little awareness or knowledge regarding security aspects or compliance implications among many technical and business communities. This glossary plus other relevant information is a collective contribution of the BDL Working Group to blockchain security awareness, and includes a compilation of common terms and other information used in the world of blockchain.

51% attack (aka Consensus HiJacking)

A theoretical situation where a single miner or group of miners controls more than half of the networks computing power and decides to use this power to their advantage. The attacker can double spend his money – meaning he can pay with the same Bitcoin twice or even more. The attacker will also be able to prevent transactions from being confirmed and prevent other miners from generating new Bitcoins.

Source: https://99bitcoins.com/bitcoin-glossary-faq/

Address

Addresses (Cryptocurrency addresses) are used to receive and send transactions on the network. An address is a string of alphanumeric characters, but can also be represented as a scannable QR code. To create the address, the wallet pushes the public key through a series of cryptographic algorithms

Source: http://www.blockchaintechnologies.com/blockchain-glossary
Source: https://blockgeeks.com/guides/blockchain-address-101/

Agreement Ledger

An agreement ledger is a distributed ledger used by two or more parties to negotiate and reach agreement.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Altcoin

A General name given to cryptocurrencies other than Bitcoin. For example, Litecoin, Feathercoin, Dash, etc. For a list of many Altcoin go to http://www.altcoins.com.

Source: https://99bitcoins.com/bitcoin-glossary-faq/

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.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Bitcoin Block Header

Contains a standard 80 bytes of information as follows:

Bytes	Name	Description
4	version	Block version information
32	hashprevblock	The hash value of the previous block
32	hashmerkleroot	Merkle tree collection - a hash of all transactions related to current block
4	time	A timestamp recording when a block was created
4	bits	The calculated difficulty target being used for a block
4	nonce	Number used to allow header variations and compute different hashes

Source: https://en.bitcoin.it/wiki/Block_hashing_algorithm

Bitcoin Currency

is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency. Cryptocurrencies are a subset of alternative currencies, or specifically of digital currencies.

Bitcoin became the first decentralized cryptocurrency in 2009. Since then, numerous cryptocurrencies have been created. These are frequently called altcoins, as a blend of bitcoin alternative. Bitcoin and its derivatives use decentralized control as opposed to centralized electronic money/centralized banking systems. The decentralized control is related to the use of bitcoin's blockchain transaction database in the role of a distributed ledger.

Source: https://en.wikipedia.org/wiki/Cryptocurrency and https://en.wikipedia.org/wiki/Bitcoin

Bitcoin Currency Units

BTC most common currency code. XBT unofficial ISO currency code

Unit	Value in BTC/XBT	@ $100 per BTC/XBT	@ $200 per BTC/XBT	@ $500 per BTC/XBT
BTC	1	$100	$200	$500
mBTC	0.001	$0.10	$0.20	$0.50
uBTC	0.000001	$0.000100	$0.000200	$0.000500
Satoshi	0.00000001	$0.000001	$0.000002	$0.000005

Source: http://bitcoinchaser.com/bitcoin-units-and-denominations

Bitcoin Payment System

is peer-to-peer with transactions taking place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in a public distributed ledger called the blockchain, which uses bitcoin as its unit of account. Since the system works without a central repository or single administrator, the U.S. Treasury categorizes bitcoin as a decentralized virtual currency. Bitcoin is often called the first cryptocurrency, although prior systems existed and it is more correctly described as the first decentralized digital currency. Bitcoin is the largest of its kind in terms of total market value.

Source: https://en.wikipedia.org/wiki/Bitcoin

Bitcoin Transaction Locktime

The Bitcoin transaction lock time is the time at which a particular transaction can be added to the blockchain. This is the earliest time that miners can include the transaction in their hashing of the Merkle root to attach it in the latest block to the blockchain.There are two specific types of transaction locktime. Firstly when the locktime figure is less than 500 million it is interpreted as a block height and miners therefore have to wait until that block height has been reached before attempting to include it in a block. If it is above 500 million it is converted to a unix timestamp – a unix timestamp being the number of seconds since January 1st 1970.

Source: https://www.cryptocompare.com/coins/guides/what-is-bitcoin-transaction-locktime/

Bitcoin Tumbler/Mixer

randomly crisscrosses your bitcoins with other users' bitcoins so that you get a clean address that the blockchain cannot connect with any of the addresses from which the coins were stolen. The tumbler is only accessible through the anonymizing Tor network, making it difficult for law enforcement to trace traffic to it or discover the people behind it.

Source: http://www.theverge.com/2013/12/19/5183356/how-to-steal-bitcoin-in-three-easy-steps

Bitcoin Vanity Addres

is a customized variant of a normal Bitcoin address. The customization occurs after the first character which is always 1. For example 1BITCOINanmgjh567bh457jj5tUyJgh5. Customization can be performed a third party Vanity Address Issuer such as https://vante.me/#!/order/start. However, research the 3rd Party issuer as some have been reported to be scammers. Alternatively, software can be downloaded to a local computer so that the Vanity Address can be self issued. Note that the computational effort necessary to generate the address is significant. The BITCOIN Vanity Address

example above could take 1 week to generate.

Source: https://en.bitcoin.it/wiki/Bitcoin_Vanity_Generation_Website and https://en.bitcoin.it/wiki/Vanitygen

Block

A group of transactions. Each block has a reference to the previous block and that is how a "blockchain" is built. Mining is the process that actually builds the blockchain. Because of this there is no way for someone to tamper with the system and add their own "custom" block to the chain.

Source: https://99bitcoins.com/bitcoin-glossary-faq/

Block Explorer

Block Explorer is an open source web tool that allows you to view information about blocks, addresses, and transactions on the Bitcoin blockchain. The source code is on GitHub.

Source: https://blockexplorer.com/

Block Height

Block height refers to the number of blocks connected together in the block chain. For example, Height 0, would be the very first block, which is also called the Genesis Block.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Blockchain

Originally block chain — is a distributed database that maintains a continuously-growing list of ordered records called blocks. Each block contains a timestamp and a link to a previous block. By design blockchains are inherently resistant to modification of the data — once recorded, the data in a block cannot be altered retroactively. Blockchains are "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically.

Source: https://en.wikipedia.org/wiki/Blockchain_(database)

Blockchain 1.0

is currency - the deployment of cryptocurrencies in applications related to cash such as currency transfer, remittance, and digital payment systems.

Source: https://ieet.org/index.php/IEET2/more/swan20141110

Blockchain 2.0

is contracts - the whole slate of economic, market, and financial applications using the blockchain that are more extensive than simple cash transactions like stocks, bonds, futures, loans, mortgages, titles, smart property, and smart contracts.

Source: https://ieet.org/index.php/IEET2/more/swan20141110

Blockchain 3.0

is applications beyond currency, finance, and markets, particularly in the areas of government, health, science, literacy, culture, and art.

Source: https://ieet.org/index.php/IEET2/more/swan20141110

Blockchain Applications

A blockchain application requires three interdependent components: the user-facing application, the smart contract, and the ledger.
The top layer is the user-facing application that meets the needs of the network participants. The application lets users invoke smart contracts that trigger transactions in the business network. The smart contract encapsulates the business logic of the network: assets, ownership, and transfers. Each invocation of a smart contract creates a transaction in the network and updates the ledger. The ledger holds the current value of smart contract data (for example, vehicleOwner=Daisy), and is distributed across the network.

Source: http://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-glossary-bluemix-trs/index.html

Blockchain as a Service (BaaS)

is providing a platform to develop, test, and deploy blockchain applications.

Source: https://azure.microsoft.com/en-us/solutions/blockchain/

"Blockchain as a Service" Providers

Cloud Service Provider	Total Cloud Market Share all services Jan 2016	Blockchain as a Service (BaaS)	Blockchain (Distributed Ledger) Technology
Microsoft Azure	9%	Yes	Ethereum
IBM Bluemix	7%	Yes	Hyperledger fabric
Amazon Web Services	31%	Yes	Ethereum
Google	4%	Yes	Ripple
Rest	49%		
Total	100%		

Source: https://www.channele2e.com/2016/02/04/cloud-market-share-2016-aws-microsoft-ibm-google/

Blockchain Developer

writes chaincode (smart contracts), and client-side applications to invoke smart contracts. The Blockchain Developer could deploy chaincode directly to the network, through a REST interface. To include credentials from a Traditional Data source in chaincode, the developer could use an out-of-band connection to access the data.

Source: https://console.ng.bluemix.net/docs/services/blockchain/ibmblockchain_overview.html

Blockchain Embedded Mining

Embedded mining is a relatively new concept where mining chips are embedded into internet connected devices. In comparison to industrial grade mining hardware (e.g. servers in a data center), embedded mining chips can operate inside everyday devices such as a cell phone. Embedded mining is speculated to be a solution to previously uneconomical efforts, such as micropayments and monetizing the internet-of-things.

Source: http://www.blockchaintechnologies.com/blockchain-mining

Blockchain Hash

a hash function takes an input of any length and creates an output of fixed length. The output is called a Hash. SHA256 is a hash function that takes any length input and creates an output of 256 bits (32 bytes). A Blockchain Hash is calculated for each block in a chain with the hash for the first block used as input when calculating the hash for the next block.

Source: https://decentralize.today/if-you-understand-hash-functions-youll-understand-blockchains-9088307b745d#.lh2gflo8c

Blockchain Mining

Mining refers to the distributed computational review process performed on each "block" of data in a "block-chain". This allows for achievement of consensus in an environment where neither party knows or trusts each other.

Source: http://www.blockchaintechnologies.com/blockchain-mining

Blockchain Mining Hardware

CPU/GPU Bitcoin Mining: The least powerful category of bitcoin mining hardware is your computer itself. Theoretically, you could use your computer's CPU to mine for bitcoins, but in practice, this is so slow by today's standards that there isn't any point. You can enhance your bitcoin hash rate by adding graphics hardware to your desktop computer. Graphics cards feature graphical processing units (GPUs). These are designed for heavy mathematical lifting so they can calculate all the complex polygons needed in high-end video

games. This makes them particularly good at the SHA hashing mathematics necessary to solve transaction blocks. For example, an ATI 5970 graphics card can give you over 800 MH/sec compared with a CPU, which will generally give you less than 10 MH/sec.

FPGA Bitcoin Mining: A Field Programmable Gate Array is an integrated circuit designed to be configured after being built. This enables a mining hardware manufacturer to buy the chips in volume, and then customize them for bitcoin mining before putting them into their own equipment. Because they are customized for mining, they offer performance improvements over CPUs and GPUs. Single-chip FPGAs have been seen operating at around 750 Megahashes/sec, although that's at the high end.
ASIC Bitcoin Miners: This is where the action's really at. Application Specific Integrated Circuits (ASICs) are specifically designed to do just one thing: mine bitcoins at mind-crushing speeds, with relatively low power consumption. Because these chips have to be designed specifically for that task and then fabricated, they are expensive and time-consuming to produce - but the speeds are stunning. At the time of writing, units are selling with speeds anywhere from 5-500 Gigahashes/sec (although actually getting some of them to them to ship has been a problem).

Source: http://www.coindesk.com/information/how-to-set-up-a-miner/

Blockchain Network

- A distributed, decentralized peer-to-peer network, with nodes that represent network participants, such as banks, government agencies, manufacturers and securities firms.
- A group of peers that validate transactions through a consensus protocol before committing them to a shared ledger.

Source: http://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-glossary-bluemix-trs/index.html

Blockchain Network Operator

manages member permissions, such as enrolling the Regulator (B) as an "auditor" and the Blockchain User (A) as a "client." An auditor could be restricted to query transactions, whereas a client could be authorized to deploy, invoke and query certain types of chaincode.

Source: https://console.ng.bluemix.net/docs/services/blockchain/ibmblockchain_overview.html

Blockchain Pruning

It is not required for most fully validating nodes to store the entire blockchain, currently around 127 GB. Reducing the amount of data to the size of the

current unspent output size, currently 1.7 GB, plus some additional for data that is needed to handle re-orgs can reduce the stress on many nodes.

Source: https://en.bitcoin.it/wiki/Scalability and https://statoshi.info/dashboard/db/unspent-transaction-output-set

Blockchain RTBF Risk

Due to the existence of multiple copies of the entire transaction database it would be difficult to prove all data had been deleted. The fact that data in the blockchain is immutable – which means that it cannot be altered or removed once it has been entered – provides transparency and accountability. However, it may also compromise privacy and data protection, especially when it comes to personal or sensitive data (which should never be stored on a blockchain). Blockchains do not guarantee anonymity and, the more personal the data is, the easier it is to identify the individual to which it pertains. This immutability may compromise the 'right to be forgotten', whereby users may, under certain circumstances, demand that their personal data be erased.

Source: https://www.enisa.europa.eu/publications/blockchain-security **and** http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA(2017)581948

Blockchain Standard Transaction Types

As of bitcoin core 0.9, transactions from the network must match a set of rules, Those transactions are called standard transactions. Only standard transactions are mined or broadcast by peers running the default Bitcoin Core software. The standard transaction types are as follows:

1. Pay to PubKey Hash (P2PKH) - standard way to send Bitcoins to a single address
2. Pay to Address - standard way of assigning newly mined Bitcoins and transaction fees to an address
3. Pay to Script Hash (P2SH) - moves the responsibility for supplying the conditions to redeem a transaction from the creator of the transaction to the payee(s)
4. Multi-Signature - used for multi-signature transactions by specifying the multi-signature script in the P2SH (#3) redeemScript, they can also be specified directly in the scriptPubKey
5. Null_Data - They allow the creator of the transaction to include some arbitrary data in the blockchain in exchange for paying a transaction fee. The output is unspendable
6. Non_Standard – None of the above

Source: http://www.quantabytes.com/articles/a-survey-of-bitcoin-transaction-types **and** https://bitcoin.org/en/developer-guide#standard-transaction

Blockchain User

submits a transaction to the Permissioned Blockchain network. The transaction can be a deploy, invoke or query, and is issued through a client-side application leveraging an SDK, or directly through a REST API.

Source: https://console.ng.bluemix.net/docs/services/blockchain/ibmblockchain_overview.html

BTC

is still the most often used code for Bitcoin and is listed on https://www.oanda.com/currency/converter/ as well as in the form of a trust on http://www.nasdaq.com/symbol/gbtc that invests in Bitcoin. XBT is the unofficial ISO 4217 International Standard for currency codes. You can find XBT traded on https://www.bloomberg.com/quote/COINXBT:SS and http://www.xe.com.

Source: http://www.coindesk.com/bitcoin-gaining-market-based-legitimacy-xbt/

Central Ledger

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

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Chaincode

Chaincode is the Hyperledger fabric's interpretation of the smart contract method/algorithm, with additional features. Embedded logic that encodes the rules for specific types of network transactions. Developers write chaincode applications and deploy them to the network. End users then invoke chaincode through a client-side application that interfaces with a network peer, or node. Chaincode runs network transactions, which if validated, are appended to the shared ledger and modify world state.

Source: https://console.ng.bluemix.net/docs/services/blockchain/ibmblockchain_overview.html

Chaincode Services

Chaincode Services provides a secure and lightweight method to sandbox chaincode execution on the validating nodes. The environment is a "locked down" and secured container, along with a set of signed base images containing secure OS and chaincode language, runtime and SDK layers for Go, Java and Node.js. Additional languages can be enabled, if required.

Source: https://console.ng.bluemix.net/docs/services/blockchain/ibmblockchain_overview.html

Chaincode Standard Transaction Types

The standard transaction types are as follows:

1. Init () - when you first deploy your chaincode. This should be used to initialize your chaincode.
2. Invoke () - when you want to call chaincode functions to do real work
3. Query () - whenever you query your chaincode's state.
4. Main () – when it's time to setup the communication between the chaincode & the peer that deployed it.

Source: https://github.com/IBM-Blockchain/learn-chaincode

Chainwashing

is the purposeful and sometimes deceptive attempt by a vendor or entrepreneur to rebrand or hype a product or service by associating the buzzword "Blockchain" with it.

Source: http://bitcoinist.com/chainwashing-r3-swanson-blockchain-hype/

Cloudwashing

is the purposeful and sometimes deceptive attempt by a vendor or entrepreneur to rebrand or hype a product or service by associating the buzzword "Cloud" with it.

Source: http://searchcloudstorage.techtarget.com/definition/cloud-washing

Confirmation

A confirmation means that 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.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Consensus Algorithms/ Protocols

A consensus algorithm, does two things: it ensures that the next block in a blockchain is the one and only version of the truth through agreement of participants, and it keeps powerful adversaries from derailing the system and successfully forking the chain. Some of the better known protocols are: Proof of Work (Pow), Proof of Stake (PoS), Proof of Activity (PoA), Proof of Burn (PoB), Proof of Elapsed Time (PoET), Proof of Capacity (PoC).

Source: http://www.coindesk.com/short-guide-blockchain-consensus-protocols/

Consensus Point	A point – either in time, or defined in terms of a set number or volume of records to be added to the ledger – where peers meet to agree the state of the ledger. **Source:** http://www.blockchaintechnologies.com/blockchain-glossary
Consortium blockchains	a consortium blockchain is a blockchain where the consensus process is controlled by a preselected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public, or restricted to the participants, and there are also hybrid routes such as the root hashes of the blocks being public together with an API that allows members of the public to make a limited number of queries and get back cryptographic proofs of some parts of the blockchain state. These blockchains may be considered "partially decentralized". **Source:** https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
Contract Accounts (Ethereum)	Contracts are written in high level language and deployed in byte code. The address of a contract is determined at the time the contract is created (it is derived from the creator address and the number of transactions sent from that address, the so-called "nonce"). **Source:** http://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html#accountsibmblockchain_overview.html
Cryptocurrency	is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency. Cryptocurrencies are a subset of alternative currencies, or specifically of digital currencies. **Source:** https://en.wikipedia.org/wiki/Cryptocurrency
Cryptographic Hashes	such as the SHA256 computational algorithm, produce a fixed-size, unique hash value, known as a digest, from variable-sized transaction input. Hashes feature a mathematical property in which a hash can be arrived at uniquely from a given input, but the input cannot be derived from its hash value. A given specific input always results in the same hash value being computed.

Any modifications or alterations to transaction input — even the most minuscule change — results in a different hash value being computed, which indicates potentially compromised transaction input. Thus, the hash value can be used to detect the integrity of the transaction input.

Source: http://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-glossary-bluemix-trs/index.html

Decentralized Apps (DAPPS)

are a type of software program designed to exist on the Internet in a way that is not controlled by any single entity. For an application to be considered a Dapp it must meet the following criteria:

Application must be completely open-source - It must operate autonomously, and with no entity controlling the majority of its tokens. The application may adapt its protocol in response to proposed improvements and market feedback but all changes must be decided by consensus of its users.

Application's data and records of operation must be cryptographically stored - in a public, decentralized blockchain in order to avoid any central points of failure.

Application must use a cryptographic token - (bitcoin or a token native to its system) which is necessary for access to the application and any contribution of value from (miners /farmers) should be rewarded in the application's tokens.

Application must generate tokens - according to a standard cryptographic algorithm acting as a proof of the value nodes are contributing to the application (Bitcoin uses the Proof of Work Algorithm).

Source: https://blockchainhub.net/dapps/

Difficulty

in Proof-of-Work mining, is how hard it is to verify blocks in a blockchain network. In the Bitcoin network, the difficulty of mining adjusts verifying blocks every 2016 blocks. This is to keep block verification time at ten minutes.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Digest Access Authentication

It is a general purpose protocol for authentication that provides integrity protection through use of simple authentication and security layer (SASL). Uses include:

- Authenticated client access to a Web site
- Authenticated client access using SASL
- Authenticated client access with integrity protection to a directory service

Using LDAP

Source: https://technet.microsoft.com/en-us/library/cc778868(v=ws.10).aspx

Digital Commodity

A digital commodity is a scarce, electronically transferrable,intangible, with a market value.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Distributed Database

database in which storage devices are not all attached to a common processor. It may be stored in multiple computers, located in the same physical location; or may be dispersed over a network of interconnected computers. Unlike parallel systems, in which the processors are tightly coupled and constitute a single database system, a distributed database system consists of loosely coupled sites that share no physical components.

Source: https://en.wikipedia.org/wiki/Distributed_database

Distributed Ledger

(also called **shared ledger or register**) a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions. There is no central administrator or centralized data storage. A peer-to-peer network is required as well as consensus algorithms to ensure replication across nodes is undertaken. One distributed ledger design is through implementation of a public or private blockchain system. But all distributed ledgers do not have to necessarily employ a chain of blocks to successfully provide secure and valid achievement of distributed consensus, a Blockchain is only one type of data structure considered to be a distributed ledger.

Source: https://en.wikipedia.org/wiki/Distributed_ledger

DLT Interoperability

is the ability of the continuingly increasing number of heterogeneous DLT Systems as well as legacy non DLTs Systems to interact with each other.

Source: http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf

Double Spending

Double spend refers to a scenario, in the Bitcoin network, 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 it. The more confirmations that a particular transaction has, the harder it becomes to double spend the bitcoins.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

ECDSA Signatures

is a signature algorithm that is a variant of DSA (Digital Signature Algorithm) that like Schnorr Signatures leverages elliptic curve cryptography. Unlike Schnorr, ECDSA requires one signature for each input sent from each individual address.

Source: https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm and https://bitcoinmagazine.com/articles/the-power-of-schnorr-the-signature-algorithm-to-increase-bitcoin-s-scale-and-privacy-1460642496/

Elliptic Curve Cryptography

is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

Source: http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography

Ether

is the name of the currency used within Ethereum. It is used to pay for computation within the EVM. A list of exchanges where Ether is traded can be found at coinmarketcap.com

Source: http://ethdocs.org/en/latest/ether.html

Double Spending

Ethereum is a programmable open blockchain. Rather than give users a set of predefined operations (e.g. bitcoin transactions), Ethereum allows users to create their own operations of any complexity they wish. In this way, it serves as a platform for many different types of decentralized blockchain applications, including but not limited to cryptocurrencies. At the heart of it is the Ethereum Virtual Machine ("EVM"), which can execute code of arbitrary algorithmic complexity. In computer science terms, Ethereum is "Turing complete". Developers can create applications that run on the EVM using friendly programming languages modelled on existing languages like JavaScript and Python

Source: http://ethdocs.org/en/latest/introduction/what-is-ethereum.html

External Accounts (Ethereum)

Ethereum Virtual Machine, has concept of External Accounts which are given to the external entities (e.g. Humans). External accounts are created with public-private key pair and the account ID is derived from public key. Account ID is used in transaction messages to address owner and destination of transactions.

Source: http://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html#accounts

Fiat Currency

Legal tender that has been designated as such by government. This requires that the public has confidence and faith in the government and the money's ability to serve as a storage medium for purchasing power.

Source: http://www.dummies.com/personal-finance/investing/how-the-fiat-system-works/

Fork

a regular fork where all nodes follow the same consensus rules, so the fork is resolved once one chain has more proof of work than another. When two or more blocks have the same block height, forking the block chain. Typically occurs when two or more miners find blocks at nearly the same time. Can also happen as part of an attack.

Source: https://bitcoin.org/en/glossary/soft-fork

Genesis Block

The very first block in a blockchain.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

ECDSA Signatures

Bitcoins have a finite supply, which makes them a scarce digital commodity. The total number of bitcoins that will ever be issued is 21 million. The number of bitcoins generated per block (Block Reward) is decreased 50% every four years. This is called "halving." Currently the reward is 12.5 Bitcoins. The next haling in 2020 will drop the reward to 6.25 per block. The final halving will take place in the year 2140. The countdown to the final halving can be monitored at http://www.bitcoinblockhalf.com/

Source: http://www.blockchaintechnologies.com/blockchain-glossary

HardFork

A permanent divergence in the blockchain, commonly occurs when non-upgraded nodes can't validate blocks created by upgraded nodes that follow newer consensus rules. A hardfork is a change to the blockchain protocol that makes previously invalid blocks/transactions valid, and therefore requires all users to upgrade their clients. The most recent example of a hardfork in public blockchains is the Ethereum hardfork which happened on July 21st 2016. The hardfork changed the Ethereum protocol, therefore second blockchain emerged (Ethereum Classic, ETC) which supports the old Ethereum protocol. In order to continue existing ETC needs miners, which would validate the transactions on the blockchain.

Source: https://bitcoin.org/en/glossary/hard-fork and https://blockchainhub.net/glossary/

Digital Commodity

The number of hashes that can be performed by a bitcoin miner in a given period of time (usually a second).

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Hashrate Denominations

The denomination of hash rates follows the International System of Units (SI). kilo-, mega-, giga-, tera-, peta-, exa-

1 kH/s	1,000 (one thousand) hashes per second
1 MH/s	1,000,000 (one million) hashes per second
1 GH/s	1,000,000,000 (one billion) hashes per second
1 TH/s	1,000,000,000,000 (one trillion) hashes per second
1 PH/s	1,000,000,000,000,000 (one quadrillion) hashes per second
1 EH/s	1,000,000,000,000,000,000(one quintillion) hashes per second

Source: http://molinn.is/.crypt/btc-e/WalletBitcoinMining/bitcoin-mining-conversion.php

Hyperledger

The Hyperledger project is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration including leaders in finance, banking, Internet of Things, supply chains, manufacturing and Technology. The Linux Foundation hosts Hyperledger as a Collaborative Project under the foundation. There are currently 5 projects in progress, Blockchain Explorer, Cello, Fabric, IROHA, Sawtooth Lake.

Source: https://www.hyperledger.org/ and https://www.hyperledger.org/community/projects

Intel® Software Guard Extensions (SGX)

is an Intel technology for application developers who are seeking to protect select code and data from disclosure or modification. Intel SGX makes such protections possible through the use of enclaves, which are protected areas of execution. Application code can be put into an enclave by special instructions and software made available to developers via the Intel® SGX Software Development Kit (SDK). The Intel SGX SDK is a collection of APIs, libraries, documentation, sample source code, and tools that allows software developers to create and debug Intel SGX.

Source: https://software.intel.com/en-us/sgxcommunity/projects

Interledger Protocol (ILP)

The Interledger Protocol provides for routing payments across different digital asset ledgers while isolating senders and receivers from the risk of intermediary failures. Secure multi-hop payments and automatic routing enables a global network of networks for different types of value that can connect any sender with any receiver.

Source: https://interledger.org/rfcs/0003-interledger-protocol/#preface

Litecoin

A peer-to-peer cryptocurrency based on the Scrypt proof-of-work network. Sometimes referred to as the silver of bitcoin's gold.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Membership Services

Membership Services manages user identities on a permissioned blockchain network through the Certificate Authority peer. Membership Services provides a distinction of roles by combining elements of Public Key Infrastructure (PKI) and decentralization (consensus). By contrast, non-permissioned networks do not provide member-specific authority or a distinction of roles.

A permissioned blockchain requires entities to register for long-term identity credentials (Enrollment Certificates), which can be distinguished according to entity type. For users, an Enrollment Certificate authorizes the Transaction Certificate Authority (TCA) to issue pseudonymous credentials; these certificates authorize transactions submitted by the user. Transaction certificates persist on the blockchain, and enable authorized auditors to associate otherwise unlinkable transactions.

Source: https://console.ng.bluemix.net/docs/services/blockchain/ibmblockchain_overview.html

Merged Mining

Merged mining is the process of allowing two different crypto currencies based on the same algorithm to be mined simultaneously. This allows low hash powered crypto currencies to increase the hashing power behind their network by bootstrapping onto more popular crypto currencies. Two of the best examples of this are scrypt mining of both litecoin and dogecoin, as well as namecoin and bitcoin with sha-256.

Source: https://www.cryptocompare.com/mining/guides/what-is-merged-mining-bitcoin-namecoin-litecoin-dogecoin/

Merkle Root

The root node of a Merkle tree, a descendant of all the hashed pairs in the tree. Block headers must include a valid Merkle root descended from all transactions in that block.

Source: https://bitcoin.org/en/glossary/merkle-root

Merkle Tree

Basic idea behind Merkle tree is to have some piece of data that is linking to another. You can do this by linking things together with a cryptographic hash. The content itself can be used to determine the hash. By using the cryptographic hashing, we can address the content, and content gets immutable because if you change anything in the data the cryptographic hash changes and the link will be different. Bitcoin uses cryptographic hashing, where every block points to the previous one, if you modify the block, the hash will change and will make the block invalid.

Source: https://blockchainhub.net/glossary/

Miner

refers to the person/entity that performs a computational review process on each “block” of data in a “blockchain” before a block is considered confirmed/approved.

Source: http://www.blockchaintechnologies.com/blockchain-mining

Mining

The process by which transactions are verified and added to a blockchain. This process of solving cryptographic problems using computing hardware also triggers the release of cryptocurrencies.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Mining Pool

where the miner pools resources with other miners to find blocks more often, with the proceeds being shared among the pool miners in rough correlation to the amount of hashing power they each contributed, allowing the miner to receive small payments with a lower variance (shorter time between payments).

Source: https://bitcoin.org/en/developer-guide#mining

Mining Solo

where the miner attempts to generate new blocks on his own, with the proceeds from the block reward and transaction fees going entirely to himself, allowing him to receive large payments with a higher variance (longer time between payments)

Source: https://bitcoin.org/en/developer-guide#mining

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. Multisignature addresses have a much greater resistance to theft.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Nakamoto Consensus

is the decentralized mechanism for emergent consensus. Emergent, because consensus is not achieved explicitly—there is no election or fixed moment when consensus occurs. Instead, consensus is an emergent artifact of the asynchronous interaction of thousands of independent nodes, all following simple rules. Decentralized consensus emerges from the interplay of four processes that occur independently on nodes across the network:

- Independent verification of each transaction, by every full node, based on a comprehensive list of criteria
- Independent aggregation of those transactions into new blocks by mining nodes, coupled with demonstrated computation through a proof-of-work algorithm
- Independent verification of the new blocks by every node and assembly into a chain
- Independent selection, by every node, of the chain with the most cumulative computation demonstrated through proof of work

Source: http://chimera.labs.oreilly.com/books/1234000001802/ch08.html

Node

Each copy of the ledger operated by a participant in the blockchain network. Entries in the ledger are synchronized to all ledgers in the network.

Source: http://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-glossary-bluemix-trs/index.html

Nonce

is an arbitrary number used only once in a cryptographic communication, in the spirit of a nonce word. They are often random or pseudo-random numbers. Many nonces also include a timestamp to ensure exact timeliness, though this requires clock synchronization between organizations. The addition of a client nonce ("cnonce") helps to improve the security in some ways as implemented in digest access authentication. To ensure that a nonce is used only once, it should be time-variant (including a suitably fine-grained timestamp in its value), or generated with enough random bits to ensure a probabilistically insignificant chance of repeating a previously generated value. Some authors define pseudo-randomness (or unpredictability) as a requirement for a nonce.

Source: https://en.wikipedia.org/wiki/Cryptographic_nonce

NXT

Nxt is an advanced open source application platform which builds on and improves the basic functionality of the first wave of pioneering cryptocurrencies. The Nxt platform includes many advanced features, including the NXT digital currency. Nxt gives its users complete freedom in many ways: for example, to use the NXT currency as a payment system, or to create advanced blockchain applications using the Nxt API and toolkit. Nxt is a powerful, open and completely decentralized application platform, leading the evolution of cryptocurrency into blockchain technology.

Source: https://nxt.org/what-is-nxt/

Off-Ledger Currency

A currency minted off-ledger and used on-ledger. An example of this would be using distributed ledgers to manage a national currency such as EUR.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

On-Ledger Currency

A currency minted on-ledger and used on-ledger. An example of this would be the cryptocurrency, Bitcoin.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Open-Transactions Project

This is a collaborative effort to develop a robust, commercial-grade, fully-featured, free-software toolkit implementing the OTX protocol as well as a full-strength financial cryptography library, API, GUI, command-line interface, and prototype notary server. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the Open-Transactions toolkit and its related documentation.

Source: http://opentransactions.org/wiki/index.php?title=Main_Page

Orphan Block

Detached or Orphaned blocks are valid blocks which are not part of the main chain. They can occur naturally when two miners produce blocks at similar times or they can be caused by an attacker (with enough hashing power) attempting to reverse transactions.

Source: https://blockchain.info/orphaned-blocks

Participant

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

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Peer

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

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Peer-to-Peer Transaction Platforms

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.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Pegged Sidechains

is the creation of another blockchain to be used to transfer Bitcoins and assets from one blockchain to another. Several advantage of Pegged Sidechains are:

1. Access to new and innovative cryptocurrency systems using the assets they already own
2. More easily interoperate with each other and with Bitcoin

3. Avoiding the liquidity shortages and market fluctuations associated with new currencies
4. Since sidechains are separate systems, technical and economic innovation is not hindered
5. Despite bidirectional transferability between Bitcoin and pegged sidechains, they are isolated:
    a. in the case of a cryptographic break (or malicious design) in a sidechain, the damage is entirely confined to the sidechain itself.

Source: https://blockstream.com/sidechains.pdf

Permissioned Ledger

A permissioned ledger is 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. This is carried out by trusted actors which makes maintaining a shared record much simpler that the consensus process used by unpermissioned ledgers. Permissioned block chains provide highly-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. A permissioned ledger is usually faster than an unpermissioned ledger.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Private Blockchain

a fully private blockchain is a blockchain where write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent. Likely applications include database management, auditing, etc. internal to a single company, and so public readability may not be necessary in many cases at all, though in other cases public auditability is desired.

Source: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Private Key

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.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Proof of Authority (PoA)

Proof-of-Authority is a replacement for Proof-of-Work, which can be used for private chain setups. It does not depend on nodes solving arbitrarily difficult mathematical problems, but instead uses a hard-configured set of "authorities" - nodes that are explicitly allowed to create new blocks and secure the blockchain. This makes it easier to maintain a private chain and keep the block issuers accountable. A Proof of authority is a consensus mechanism in a private blockchain which essentially gives one client (or a specific number of clients) with one particular private key the right to make all of the blocks in the blockchain.

Source: https://github.com/ethcore/parity/wiki/Proof-of-Authority-Chains and https://blockchainhub.net/glossary/

Proof-of-Stake (PoS)

An alternative to the proof-of-work system, in which your existing stake in a cryptocurrency (the amount of that currency that you hold) is used to calculate the amount of that currency that you can mine.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Proof-of-Work (PoW)

A system that ties mining capability to computational power. Blocks must be hashed, which is in itself an easy computational process, but 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.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Public Blockchain

is a blockchain that anyone in the world can read, anyone in the world can send transactions to and expect to see them included if they are valid, and anyone in the world can participate in the consensus process – the process for determining what blocks get added to the chain and what the current state is. As a substitute for centralized or quasi-centralized trust, public blockchains are secured by cryptoeconomics – the combination of economic incentives and cryptographic verification using mechanisms such as proof of work or proof of stake, following a general principle that the degree to which someone can have an influence in the consensus process is proportional to the quantity of economic resources that they can bring to bear. These blockchains are generally considered to be "fully decentralized".

Source: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

QR Code

A QR code in the case of a Bitcoin transaction is the machine-readable representation of the transactors bitcoin address. The QR code is a more efficient and effective method of transferring between parties the the 27 to 34 characters that make up a bitcoin address. The QR code also has the possibility to display other information such as the amount of the transaction.

Source: https://bitcoin.stackexchange.com/questions/8111/what-are-qr-codes-and-how-do-you-use-them-as-request-payment-from-wallet **and** https://en.wikipedia.org/wiki/QR_code

Replicated Ledger

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

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Ripple

A financial solution built around an open, neutral protocol (Interledger Protocol or ILP) to power payments across different ledgers and networks globally. It offers a cryptographically secure end-to-end payment flow with transaction immutability and information redundancy. Architected to fit within a bank's existing infrastructure, Ripple is designed to comply with risk, privacy and compliance requirements. Ripple is a consortium based blockchain implementation.

Source: https://ripple.com/technology/

Schnorr Signatures

is a signature algorithm replacement for ECDSA, leveraging elliptic curve cryptography that supports "native multisig" which enables the aggregation of multiple signatures into a single one valid for the sum of the keys of their respective inputs. This algorithm has 3 significant benefits:

- Constant-size signatures irrespective of the number of participants in the multisig setup.
- Diminished size of data to be validated and transmitted translates into capacity gains.
- Entire policy of multisig is obscured and indistinguishable from a conventional single pubkey.

Source: https://bitcoincore.org/en/2017/03/23/schnorr-signature-aggregation/

Script

is a simple programming language, which is evaluated from left to right using a stack. The language is designed such that it guarantees all scripts will execute in a limited amount of time (it is not Turing-Complete).

A script is essentially a list of instructions recorded with each transaction that describe how the next person wanting to spend the Bitcoins being transferred can gain access to them. The script for a typical Bitcoin transfer to destination Bitcoin address D simply encumbers future spending of the bitcoins with two things: the spender must provide:

1. a public key that, when hashed, yields destination address D embedded in the script, and
2. a signature to show evidence of the private key corresponding to the public key just provided.

Source: https://bitcore.io/api/lib/script and https://en.bitcoin.it/wiki/Script

Scrypt

An alternative proof of work system to SHA256, designed to be particularly friendly to CPU and GPU miners, while offering little advantage to ASIC miners.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Segregated Witness (Segwit)

is where data, or more specifically data related to signatures are removed from bitcoin transactions making them smaller in size. This in turn makes the blocks smaller meaning more transactions can be included in a block. Technically, "Segregated witness (Segwit) is a soft fork that, if activated, will allow transaction-producing software to separate (segregate) transaction signatures (witnesses) from the part of the data in a transaction that is covered by the txid."

Source: https://decentralize.today/segregated-witness-explained-like-im-5-c00a8994ea7c#.k3fic6d7n

SHA 256

The SHA (Secure Hash Algorithm) is one of a number of cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file. SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one way function – it cannot be decrypted back. This makes it suitable for password validation, challenge hash authentication, anti-tamper, digital signatures. SHA-256 is one of the successor hash functions to SHA-1, and is one of the strongest hash functions available.

Source: http://www.xorbin.com/tools/sha256-hash-calculator

Sharding

In a sharding, nodes hold a subset of the state (UTXOs), and a subset of the blockchain. Instead of miners/validators redundantly doing the same work, they are going share the load but still have an only economic assurance even though they're not going to validate every transaction. For example, a sharding scheme on Ethereum might put all addresses starting with 0x00 into one shard, all addresses starting with 0x01 into another shard, etc. In a simple version of the scheme, each user maintains a light client on all shards, while validators fully download and track a few shards that they are assigned to at some particular time.

Source: https://diyhpl.us/wiki/transcripts/scalingbitcoin/sharding-the-blockchain/ **and** https://github.com/ethereum/wiki/wiki/Sharding-FAQ

Shared Ledger

The shared ledger is the single source of truth, or the entire history of validated transactions, on a blockchain network. Any discrepancies in the shared ledger across nodes are resolved through consensus. The ledger has the following attributes:

- It records all validated transactions on the network.
- It is shared across all network participants.
- It is replicated, so that each participant has their own copy.
- It is permissioned, so that participants can only view their own transactions.

Source: http://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-glossary-bluemix-trs/index.html

Signature Scheme

is a set of mathematical rules that link the private key, public key and signature together. Examples are Schnorr and ECDSA.

Source: https://bitcoinmagazine.com/articles/the-power-of-schnorr-the-signature-algorithm-to-increase-bitcoin-s-scale-and-privacy-1460642496/

Simple Payment Verification (SPV)

is a technique described in Satoshi Nakamoto's paper. SPV allows a lightweight client to verify that a transaction is included in the Bitcoin blockchain, without downloading the entire blockchain. The SPV client only needs download the block headers, which are much smaller than the full blocks. To verify that a transaction is in a block, a SPV client requests a proof of inclusion, in the form of a Merkle branch.

Source: https://bitcoin.org/bitcoin.pdf

Smart Contract

(also called **self-executing contracts**, **blockchain contracts**, or **digital contracts**) are simply computer programs that act as agreements where the terms of the agreement can be preprogrammed with the ability to self-execute and self-enforce itself. The main goal of a smart contract is to enable two anonymous parties to trade and do business with each other, usually over the internet, without the need for a middleman. The origin and history of smart contracts is much older than bitcoin and dates back to the 1990's. The term 'smart contract' was first coined in 1993 by one of bitcoin's alleged creators, Nick Szabo, and referred to self-automated computer programs that can carry out the terms of any contract.

Source: http://www.blockchaintechnologies.com/blockchain-smart-contracts#smart-contract-explained

SoftFork

A SoftFork is a change to the bitcoin protocol wherein only previously valid blocks/transactions are made invalid. Since old nodes will recognize the new blocks as valid, a SoftFork is backward-compatible.

Source: https://bitcoin.org/en/glossary/soft-fork

Solidity

Solidity is a contract-oriented, high-level language whose syntax is similar to that of JavaScript and it is designed to target the Ethereum Virtual Machine (EVM). Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features.

Source: http://solidity.readthedocs.io

SPV (Simplified Payment Verification)

Simplified Payment Verification. A Bitcoin protocol feature that is usually implemented in wallets. It allows the creation of "lightweight" wallet clients - wallets that don't need to download the whole blockchain in order to operate. This makes it possible to install SPV wallets on mobile phones and other space limited devices.

Source: https://bitcoin.org/en/glossary/simplified-payment-verification

Swarm

Swarm is a distributed storage platform and content distribution service, a native base layer service of the Ethereum web 3 stack. The primary objective of Swarm is to provide a decentralized and redundant store of Ethereum's public record, in particular to store and distribute Dapp code and data as well as block chain data.

Source: http://swarm-gateways.net/bzz:/theswarm.eth/

Tainted % Bitcoin

The taint percent for a bitcoin is the amount of correlation between two addresses. In other words, how likely the two addresses are related.

Source: https://blockchain.info/taint/1dice6GV5Rz2iaifPvX7RMjfhaNPC8SXH

Timestamp Blockchain

Cryptocurrencies can serve as decentralized trusted timestamping services if hash values of digital data are embedded into the transactions recorded in the block chain of the crypto currency. When a user submits a file or plain text through the browser, a client-side Javascript hashes the data. Alternatively, the data can be hashed offline, e.g., using an open source tool. In either case, only the hash, not the data is transmitted to the server. Then a bitcoin transaction, using the smallest amount possible, is created that includes the document hash. By processing the transaction, the hash and the timestamp of the transaction are permanently embedded in the distributed Bitcoin block chain. The timestamp of confirmed transactions and the data they encode can be verified by inspecting the Bitcoin block chain, e.g. using websites like blockchain.info.

Source: https://www.gipp.com/wp-content/papercite-data/pdf/gipp15a.pdf and https://app.originstamp.org/home

Timestamp Trusted

Initially, the original data is hashed. Hashing authenticates the exact data content, because the hash function ensures that changing a single bit in the data would generate a different hash value. The hash is then transmitted to a TSA, which joins the hash with a plain text timestamp. The resulting string, i.e. the hash combined with the timestamp, is hashed once more and digitally signed using the TSA's private key. The resulting ciphertext represents the trusted timestamp, which, together with the plain text timestamp, is returned to the requester. The validity of the trusted timestamp can be verified by decoding the ciphertext using the public key of the TSA. To verify that some data is identical to the data authenticated by the TSA, the process of creating the trusted timestamp has to be replicated and the results have to be compared to the decoded trusted timestamp. The need for a central TSA is a weakness of established timestamping approaches, since the integrity of the timestamping process is inevitably bound to the integrity of the TSA (Adams et al., 2001).

Source: https://www.gipp.com/wp-content/papercite-data/pdf/gipp15a.pdf

Tokenless Ledger

A tokenless ledger refers to a distributed ledger that doesn't require a native currency to operate.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Tokens Asset-Backed

Asset backed tokens are claims on an underlying asset.

Source: https://bitsonblocks.net/2015/09/28/a-gentle-introduction-to-digital-tokens/#more-130

Tokens Intrinsic

(also known as 'native or 'built-in' tokens) are made-up resources that have some utility. Bitcoin for example. Even though they are traded there is no claim to an asset.

Source: https://bitsonblocks.net/2015/09/28/a-gentle-introduction-to-digital-tokens/#more-130

Traditional Data Source

a data system that already exists which may impact the behavior of smart contracts.

Source: https://www.docdroid.net/zNAiO8Z/exploring-hyperledger-applications.pdf.html

Transaction

A request by a transactor to execute a function on the blockchain network. The transaction types are deployed, invoked, and queried, which are implemented through the chaincode functions set forth in the fabric's API contract.

Source: https://console.ng.bluemix.net/docs/services/blockchain/ibmblockchain_overview.html

Transaction Block

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

Source: http://www.blockchaintechnologies.com/blockchain-glossary

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.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Transactions Confirmed (CTXNs)

A transaction that has been added to the blockchain and is irreversible.

Source: https://blockchain.info/wallet/bitcoin-faq

Transactions Unconfirmed (UTXNs)

It means that the transaction has not yet been included in the blockchain, and is still reversible. A transaction typically takes around 10 minutes to be confirmed. When that happens, it is said that one confirmation has occurred for the transaction. With each subsequent block that is found, the number of confirmations is increased by one. To protect against double spending, a transaction should not be considered as confirmed until a certain number of confirmations is seen.

Source: https://blockchain.info/wallet/bitcoin-faq

Transactor

A network participant connected to the blockchain network through a node, who submits transactions from a client using an SDK or API.

Source: https://console.ng.bluemix.net/docs/services/blockchain/ibmblockchain_overview.html

Trusted Stamping Authority (TSA)

a trusted third party that issues timestamps. These timestamps prove when data existed (e.g. contracts, medical records, and prevents backdating by the data's owners. Blockchain does not need TSAs because transactions are included in blocks which are generated every 10 minutes (on average) and you get a block's timestamp for all its transactions.

Source: https://blog.signatura.co/using-the-blockchain-as-a-digital-signature-scheme-f584278ae826

Turing Completeness

A machine is Turing complete if it can perform any calculation that any other programmable computer is capable of. All modern computers are Turing-complete in this sense. The Ethereum Virtual Machine (EVM) which runs on the Ethereum blockchain is Turing complete. Thus, it can process any "computable function". It is, in short, able to do what you could do with any conventional computer and programming language.

Source: https://blockchainhub.net/glossary/

Unpermissioned (Permissionless) Ledgers

Unpermissioned ledgers such as Bitcoin have no single owner — indeed, 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, which means 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 dynamically in real-time.

Source: http://www.blockchaintechnologies.com/blockchain-glossary

Unspent Transaction Output (UTXO)

Bitcoin phrase for output or the amount that is sent through a standard transaction to a Bitcoin address with a set of rules to unlock the output amount.

Source: https://www.cryptocoinsnews.com/bitcoin-transaction-really-works/

User Agent

user agent fields embedded in the each node's software contain information related to the version and codebase the nodes are using. These fields are exchanged between 2 nodes anytime contact is made. By reading and summarizing these fields for all nodes a conclusion can be reached regarding the health of the network. For Example: Node 1: /Satoshi:5.64/bitcoin-qt:0.4/ Node 2: /Satoshi:5.12/Spesmilo:0.8/. Both nodes use the same protocol version of Bitcoin software but they use different versions of the codebase.

Source: http://libbitcoin.dyne.org/doc/network.html **and** https://github.com/bitcoin/bips/blob/master/bip-0014.mediawiki

User-facing-application

The top layer is the user-facing application that meets the needs of the network participants. The application lets users invoke smart contracts that trigger transactions in the business network.

Source: http://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-glossary-bluemix-trs/index.html

Validating Peer

A network node that runs the consensus protocol for the network to validate transactions and maintain the ledger. Validated transactions are appended to the ledger, in blocks. If a transaction fails consensus, it is purged from the block and therefore, not written to the ledger. A validating peer (VP) has authority to deploy, invoke and query chaincode.

Source: https://console.ng.bluemix.net/docs/services/blockchain/ibmblockchain_overview.html

Virgin Bitcoin

All bitcoins start out as virgins, and stay that way until the second they are moved to another address. When new bitcoins are mined, they are noted on the blockchain in the first transaction in a block. This is called the coinbase transaction, (nothing to do with the popular bitcoin wallet coinbase). These bitcoins are always created by a miner, and they include a single coinbase (or coinbase field) as the sole input for coinbase transactions. The purpose of the coinbase is to allow the miner who solved the block to claim the block reward, which is currently 12.5 bitcoins.

Source: https://ihb.io/2015-07-30/news/virgin-bitcoins-8248

Wallet DDOS

A DDOS attack can be made by using wallets, of which there are an estimated 12.8 million wallet users, pushing spam transactions to a targeted network. Denial of service results from increased processing due to the nodes verifying the validity of the transactions.

Source: https://www.enisa.europa.eu/publications/blockchain-security **and** https://blockchain.info/charts/my-wallet-n-users

Wallet Hardware

A bitcoin wallet that uses a physical piece of hardware in order to operate and keep it more secure. Examples of hardware wallets are TREZOR, LedgerWallet and Keepkey. A hardware wallet is usually more secure since it's considered to be a form of cold storage.

Source: https://99bitcoins.com/bitcoin-glossary-faq/

Wallet Hot

Any Bitcoin wallet that is connected to the Internet. Hot wallets are considered far less secure than cold storage since they can be hacked easier due to their connectivity.

Source: https://99bitcoins.com/bitcoin-glossary-faq/

Weak Key Risk

is the risk that the Key generation method used is faulty allowing the attacker to duplicate the key gaining access to the objective (wallet,etc.). For example a poor random number generator (RNG) can create the same 'random' number on more than one occasion. When the transaction is hashed, this number is multiplied by the same generator point (ie: same random number) as the public key. Since one unknown has been removed from the equation, the private key can be revealed by effectively reversing the hash through additional mathematical operations.

Source: https://www.enisa.europa.eu/publications/blockchain-security **and** http://www.coindesk.com/open-source-tool-identifies-weak-bitcoin-wallet-signatures/

Wei

"Sathosi" is the smallest unit of coin in Bitcoin blockchain system, likewise "Wei" is the smallest unit in Ethereum coin, which is equal to 0.000000000000000001 ether (1 Ether = 1000000000000000000 Wei). There are other units as well wei, Kwei, Mwei, szabo, finney, Kether, Mether, Gether and Tether.

Source: http://ether.fund/tool/converter

World State

Key-value database used by chaincodes to store their state when executed by a transaction.

Source: https://console.ng.bluemix.net/docs/services/blockchain/ibmblockchain_overview.html

XBT

is the unofficial ISO 4217 currency code. ISO 4217 is the International Standard for currency codes. You can find XBT traded on https://www.bloomberg.com/quote/COINXBT:SS and http://www.xe.com. BTC is still the most often used code for Bitcoin and is listed on https://www.oanda.com/currency/converter/ as well as in the form of a trust on http://www.nasdaq.com/symbol/gbtc that invests in Bitcoin.

Source: http://www.coindesk.com/bitcoin-gaining-market-based-legitimacy-xbt/

Zero Confirmation Transaction

are transactions that are not yet included in a block. They reside in the miners memory pool. Once included in a block and written to the block chain the transaction has one confirmation.

Source: https://www.cryptocoinsnews.com/zero-confirmation-transactions-safe/

Zero-Knowledge Proofs

In cryptography, a zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true.

Source: https://en.wikipedia.org/wiki/Zero-knowledge_proof

ZkSNARK (Zero-knowledge Succinct Non-interactive ARguments of Knowledge)

are the cryptographic tools underlying Zcash (open, permissionless cryptocurrency protecting privacy of transactions using zero-knowledge cryptography). They are proofs that you have performed a computation over some inputs without revealing all of the inputs. Zcash uses these proofs to verify transactions while protecting users' privacy.

Source: https://z.cash/blog/zksnarks-in-ethereum.html and https://z.cash/

Further Reading

Website	Description
http://blockchainstudies.org/	Theoretical/phil./social effects of blockchain
http://blockgeeks.com/	Bitcoin/Blockchain articles, guides, VC Access
https://bitsonblocks.net/	Bitcoin/Blockchain plain English explanations
http://bitcoinist.com/	Bitcoin demand, security, privacy, investment
http://www.blockchaintechnologies.com/	Blockchain focused technical explanations
http://www.the-blockchain.com/	Blockchain news, technology, mergers, VC
https://en.bitcoin.it/	Bitcoin Wiki
https://blockchainhub.net/	Blockchain Hubs: Links to Local Think Groups
https://github.com/	Developers Platform including Blockchain
http://www.righto.com/	Blog about motherboards, software, blockchain
http://ethdocs.org/	Everything Ethereum Documentation
https://www.elliptic.co/	Identify Illicit Activity on the Bitcoin Blockchain
https://99bitcoins.com/	Bitcoin Currency Related: Buy, Sell, Mining
https://www.paxos.com/	Post-Trade Settlement Blockchain
https://www.ibm.com/developerworks/cloud/library/	IBM Developer Technical Library
http://www.coindesk.com/	Bitcoin news and trading Info
https://blockchainhub.net/	Network of Groups with common interests
https://www.torproject.org/	Software/Open preventing network traffic analysis
https://blog.ethereum.org/	Ethereum blog
https://blockexplorer.com/	View info: blocks, addresses, and transactions
http://bitcoinchaser.com/	Bitcoin news, basics, gambling, apps
https://decentralize.today/	Bitcoin, Blockchain news and articles
https://bitcoin.org/en/	Bitcoin currency and payment network
https://dev.iota.org/	IOTA developer hub
https://www.gipp.com/projects/	Projects run by a Univer. of Konstanz professor
https://software.intel.com/en-us/sgx	Trusted execution environment
http://chimera.labs.oreilly.com/	Writing, collaborating, learning platform
https://nxt.org/	Blockchain platform to create applications
https://interledger.org/	Interconnection platform and technologies
https://console.ng.bluemix.net/	Cloud Infrastructure Apps and Services
https://www.hyperledger.org/	Platform for Blockchain frameworks
http://www.bitcoinblockhalf.com/	Bitcoin Stats and Halving Monitoring
http://www.litecoinblockhalf.com/	Litecoin Stats and Halving Monitoring

The above table lists websites that provide in depth technical, financial and operational information concerning all aspects of Blockchain/Distributed Ledger technology.

Examples of Public Blockchain Companies

Website	Description	Ticker	Market	Country
https://www.coinsilium.com/	Blockchain Investment company	COIN	NEX	UK
http://bitcoincapitalcorp.com/	Acquisition of startups and funding companies	BITCF	OTC PINK	USA
http://www.btcs.com/index.php	Bitcoin mining: building digital payment platform	BTCS	OTCQB	USA
http://btl.co	Blockchain solutions finance, gaming, energy	BTL	TSX	CAD
https://digitalx.com/about/	Blockchain enhanced payment solutions	DCC	ASX	AUS
http://globalarenaholding.com/	Acquires blockchain companies and patents	GAHC	OTC PINK	USA
http://www.grayscale.co	Invests in Bitcoins	GBTC	OTCQX	USA

Source: http://investingnews.com/daily/tech-investing/fintech-investing/7-blockchain-technology-stocks/

The above table lists 7 Blockchain/Distributed Ledger Technology companies that have made it to the public markets via an IPO or other means (restructuring). These are just a handful of examples at the time of the publication of this document.