Cryptionary: A Guide to the Terms and Concepts that Define Blockchain and Cryptocurrencies

AUG 23, 2017, 20:36 *by* CINDY23 (HTTP://NEWS.8BTC.COM/AUTHOR/CINDY23)

in BLOCKCHAIN (HTTP://NEWS.8BTC.COM/NEWS/BLOCKCHAIN) 8

0 (HTTP://NEWS.8BTC.COM/CRYPTIONARY-A-GUIDE-TO-THE-TERMS-AND-CONCEPTS-THAT-DEFINE-BLOCKCHAIN-AND-CRYPTOCURRENCIES#COMMENT)

3038

TWITTER FACEBOOK

GOOGLE REDDIT

(HTTPS://WWW.REDDIT.COI

URL=HTTP://NEWS.8BTC.C(

A-GUIDE-TO-THE-TERMS-

AND-CONCEPTS-THAT-

DEFINE-BLOCKCHAIN-

AND-

CRYPTOCURRENCIES)

Note: Author of this article is Daniel McGlynn, founder of CryptoLab.io (http://www.cryptolab.io/cryptocurrency-glossary/) that provides basic educational resources concerning cryptocurrencies and blockchain.

Altcoin: Altcoin generally refers to any cryptocurrency that is not bitcoin (https://bitcoinmagazine.com/guides/what-altcoin/). In a lot of ways this term is becoming dated as bitcoin cedes its market share of the crypto economy to other coins (see the flippening for more info on that.)

Consensus: This is a pillar of open blockchain and cryptocurrency systems like bitcoin and ethereum. Finding consensus is a sloppy decision-making process, but one that is required for a system to operate in a truly decentralized manner. Consensus is derived by node users signaling their preference for code changes and updates. If enough nodes (which can be downloaded by anyone) accept a code change, then that change will be accepted by the entire network and required before additional blocks can be added to the blockchain.

Cryptocurrency: This word generally refers to digital tokens or digital coins that are produced by a blockchain system like bitcoin and ethereum. There are other forms of digital money such as units of value produced inside video games, or even alternative money systems based on digital platforms, such as e-gold, but those systems are not cryptocurrencies. (Also, it should be noted that even if a blockchain has an associated digital token, it is not necessarily considered a cryptocurrency.) But, as the name implies, cryptocurrencies rely on encryption for security and to protect (or at least shield) a user's identity. Cryptocurrencies share some characteristics of traditional, government-backed money in that some are used a store of value, or a means of exchange. However, cryptocurrencies continue to be regulated differently across the globe. In

RECENT POSTS

(http://news.8btc.com/the-third-global-blockchain-summit-to-be-held-on-september-14-16-in-shanghai)
Blockchain
The Third Global Blockchain Summit ...
(http://news.8btc.com/the-third-global-blockchain-summit-to-be-held-on-september-14-16-in-shanghai)
(http://news.8btc.com/the-third-global-blockchain-summit-to-be-held-on-september-14-16-in-shanghai)comments 0

However, cryptocurrencies continue to be regulated differently across the globe. In some countries cryptocurrencies are considered money, in others they are regulated like commodities or securities. For more on (https://blockgeeks.com/guides/what-is-cryptocurrency/)cryptocurrencies. (https://blockgeeks.com/guides/what-is-cryptocurrency/)

dApps: A decentralized application is an autonomous, open-source entity that can be updated or modified by the consensus of a group of users. User data is encrypted on a public blockchain to prevent a single failure point. dApps also either use tokens of an existing blockchain or produce their own tokens to incentive the maintenance and operation of the application. The goal of a dApp is to remove the need for central authority such as governments or corporations. Bitcoin can be considered a Dapp. An early ethereum-powered Dapp was hacked (http://www.cryptolab.io/ethereum-investing/), causing a cascade of controversy and ultimately led to ethereum's hard fork. Github has an extensive white paper on decentralized apps. (https://github.com/DavidJohnstonCEO/DecentralizedApplications)

Digital assets: In some circles, describing cryptocurrency as a currency is considered a poor label for emerging digital assets. The label cryptocurrency can be slightly confusing (since in some instances digital tokens don't meet all of the test for money). Instead, calling cryptocurrencies digital assets (along with other parts of crypto-finance operations, such as blockchain) better capture the full capability of this emerging asset class (http://www.cryptolab.io/digital-assets/).

Distributed ledger: This is another, more descriptive, word for blockchain. Distributed ledgers use the underlying peer-to-peer network to create a verifiable and trustworthy system in which internet-connected machines, devices, and people can exchange value without the need for any kind of intermediary.

Exchange: An exchange is a place to buy and sell cryptocurrencies with traditional government issued currency (fiat currency) or to trade between different cryptocurrency systems. Most legitimate exchanges that accept fiat currency for cryptocurrency adhere to some level of Know Your Customer (KYC) laws designed to prevent money laundering and other criminal activities. These laws require customers to reveal basic identifying information before performing transactions. Most exchanges have different tiers of required disclosure, so users have to share information in relation to how much, and how frequently, they are exchanging cryptocurrency for fiat. There are also exchanges that allow users to trade between cryptocurrencies.

Fiat currency: This is traditional money. Fiat currencies are the legally recognized money created and controlled by governments, usually through central banks or some similar centralized agency. The supply of most modern fiat currencies are not tied to any commodity (like the gold standard, for example) and can be created by governments to deal with financial or economic mishaps, leading to inflationary situations and generally devaluing the strength of the currency.

51 percent attack: Open protocol blockchains are vulnerable to attacks that could

(http://news.8btc.com/mobile-wallet-bitkan-launches-bcc-otc-trading-service)

Bitcoin

Mobile Wallet Bitkan Launches Bitco...

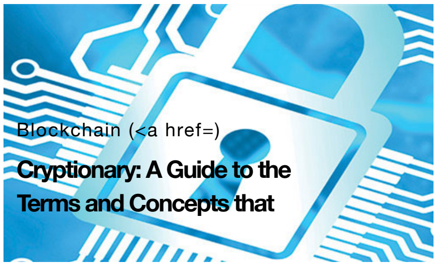
(http://news.8btc.com/mobile-wallet-bitkan-launches-bcc-otc-trading-service)

(http://news.8btc.com/mobile-wallet-bitkan-launches-bcc-otc-trading-service)comments 0

RELATED POSTS

Blockchain (<a href=)

The Third Global Blockchain Summit to be Held on



Blockchain (<a href=)

Cryptionary: A Guide to the Terms and Concepts that

Blockchain (<a href=)

8btc Interview: Binance CMO He Yi Talks About the Outlook

51 percent attack: Open protocol blockchains are vulnerable to attacks that could potentially take advantage of the need for consensus. If miners are able to control 51 percent of the nodes operating a blockchain, then they can effectively manipulate foundational rules and take control of the system by adopting their own changes in the code and overriding the need for others in the system to agree to those changes before they are put into effect.

Flippening: The flippening is when bitcoin cedes its market dominance to other cryptocurrencies. Ethereum is currently the number two cryptocurrency by market cap, but other currencies are also growing rapidly, such as Ripple and Litecoin. The crypto community is conflicted on whether the flippening is signaling a decline (or at least a serious stall) in bitcoin's growth and relevance, or whether a more diverse and competitive cryptocurrency market is a sign of maturation and increased acceptance. For more on the (http://www.cryptolab.io/whats-the-flippening/)flippening (http://www.cryptolab.io/whats-the-flippening/).

Fork: A split in the computer code that underpins blockchain systems. A blockchain might get forked for a variety of reasons, ranging from planned code updates to complete system-changing scenarios. Soft forks refer to updates or code changes that are planned and that don't change the underlying structure or functioning of the blockchain system. A hard fork is a more pronounced change that can have dramatic impacts on a blockchain and associated cryptocurrencies. Hard forks are difficult to implement, and because of the consensus required to manage decentralized blockchains like bitcoin and ethereum, can result in two distinctive blockchains. More on forks (https://coincenter.org/entry/what-are-forks-alt-coins-meta-coins-and-sidechains).

Gas: This is a term that refers to the cost required to complete transactions on the ethereum network. Gas basically is a reflection of computational resources or "work" that it takes for the ethereum blockchain to verify and store a transaction. The idea behind gas is that charging a network fee will make the entire system more sustainable overall, especially once ethereum moves from proof-of-work to proof-of-stake, which is a proposed future change.

Hash: Hashing is the process of verifying blocks on the blockchain using a secure hash algorithm (in the case of bitcoin the secure hash algorithm is called SHA 256). Hashing is the process miner use to maintain the blockchain and compete for freshly minted bitcoin. The process takes a lot of computing power, and so miners are continually trying to build more sophisticated rigs, which contributes to their overall hash power.

Hash power: Cryptocurrencies are created when miners solve complex computer problems while verifying and storing data in blocks. But creating these blocks takes an ever-increasing amount of computing power. Hash power is a measure of how much computing power a miner or mining rig is using to create and maintain blocks. Miners looking to make a profit, especially by mining more established coins, are continually looking for ways to increase hash power. Some companies have created elaborate,

News (http://news.8btc.com/news) | Reviews (http://news.8btc.com/reviews)
Interview (http://news.8btc.com/interview) | Guides (http://news.8btc.com/guides)
Press Releases (http://news.8btc.com/press-releases)

and expensive, mining operations to scale hash power, but they also incur enormous energy costs.

Hodl: This is one of the words that inspired the development of the cryptionary. It's a crypto-specific word that came out of a now-famous bitcoin chat conversation. Hodl is a rushed version of "hold" is a battle cry for crypto-enthusiasts around the internet. To hodl is to resist selling during a dump, or a big loss of value in a currency. Traders trade and hodlers hold. Here's the original post that made (https://bitcointalk.org/index.php?topic=375643.0)hodl famous.

ICO: Or initial coin offering. This is how some new cryptocurrency projects come into existence. ICOs are a cross between a crowdfunding campaign and a more traditional initial public (IPO) from the stock market. The main difference is that there is a low barrier to entry for an ICO. With pretty minimal effort anyone can write a whitepaper proposing a new blockchain or a token that would serve some kind of function and piggyback on an existing blockchain. It's likely that future ICOs will be more heavily scrutinized by regulators.

Immutability: This is like a one-way travel sign. Immutability means that once a block is verified and added to the blockchain, then the contents of that block (such as transaction details) can not be edited or changed. This idea of immutability is key to the trust and functioning of a blockchain. Ethereum's developers made headlines when they decided to override the immutability of the Ethereum blockchain following the DAO attack in 2016. The blockchain was reversed in order to retrieve money from a digital heist and return it to the original investors. The decision resulted in a hardfork that created two ethereum blockchains — ethereum and ethereum classic.

Internet of things: The internet of things describes a scenario of hyper connectivity where devices, ranging from everything from household thermostats to entire energy grids, are connected to the internet. It's presumed that this hyper connectivity or real time data collection and monitoring will lead to improved quality of life and increased efficiency (in terms of energy usage, etc.). The existing internet infrastructure is currently a limiting factor of a scalable internet of things. Blockchain technology, particularly smart contracts and trusted networks, are viewed as key components to developing the internet of things.

Internet of value (also sometimes called the internet of money): The existing internet is best categorized as the internet of information. The emergence of blockchain and cryptocurrencies are making possible universal and widespread systems of value that not offer evolved systems for finance, but can also be used to store, verify, and transfer other critical activities that hold value such as votes, copyrights, and intellectual property. Like how the internet changed information and communication technologies, a new, secure way of exchanging value is likely to disrupt the current business and financial sectors and create goods and services that don't currently exist.

KYC (Know Your Customer) laws: These are anti-money laws that are in place to try and prevent bad actors from using cryptocurrency exchanges and related services as a means to launder, hide, or transfer cryptocurrencies as a means to fund criminal activities. KYC laws required exchanges and financial services to ask users for basic identifying information before allowing transactions between fiat currencies and cryptocurrencies.

Lambo: As in Lamborghini. A Lambo is an aspirational symbol used by cryptocurrency traders and enthusiasts as a symbol of success. As in "when we are driving Lambos and..." Interestingly, there are several threads, especially on Reddit, pointing out that Lambos might be great to post about, but they are actually horrible investments.

Miner: A miner is a key part of a proof-of-work system for validating and maintaining a blockchain. Miners dedicate computer power (or hash power) to solving mathematical problems, which result in creating strings of verified data that are added to the blockchain. Miners are rewarded for their work by receiving new tokens if they are the first to verify a block (which can contain hundreds of individual transactions). A new block also contains data from the preceding block, which means the system builds upon itself and prevents future fraud or tampering because it is difficult to go back and manipulate an individual block. While mining or proof-of-work is interesting from a computational perspective, it is also extremely energy intensive and requires specialized equipment to mine the major blockchain systems.

Moon kid: A subscriber to the theory that that value of cryptocurrencies will reach astronomical proportions. These people often post memes on social media during pronounced crypto pumps of some version of space shuttles launching into outer space. These memes are predictably labeled with some derivation of "to the moon."Moon kids are always optimistic during bull surges and relatively quiet during bear stretches. In a lot of ways, they are like bandwagon fans during the run-up to the World Series. Never take trading advice from a moon kid.

Multiple signature or multi-sig: This refers to a cryptocurrency address that requires more than one private key to transfer funds. The multi-sig function is commonly used in business transactions where a company does not want just one individual user to have the keys to an address. Other common applications include trustless escrow and applications where extra layers of security are needed. Coin Center has a more detailed explanation of (https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do)multisig and how it works. (https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do)

Network effect: This refers to the idea that something becomes more valuable as more people use it. User-based technology companies and services are good examples. Facebook, for example, becomes more valuable as more people use the platform. In crypto land, bitcoin has a network effect because it was the first major currency to achieve a wide user base.

Open protocol: Blockchains like bitcoin and ethereum are open protocols that allow participation by any computer user. By their nature, open protocols are decentralized, insulating them from some forms of security breaches or failures. Open protocols rely on consensus signaling to make decisions and implement changes to the code powering the blockchain.

Peer-to-peer payment: The ability for trusted peer-to-peer digital transaction is one of the driving forces that motivated the creation and early adoption of bitcoin. The idea was simple: How can users conduct business with one another over the internet and not need to rely on a trusted third party such as a bank, credit card company, or payment service. But in practice, removing a verifiable third party meant that users needed another way to trust one another before executing a transaction. Blockchain creates a verifiable ledger which can be built upon. People, groups, and companies now have a trusted system to send digital assets back and forth without the need to go through a traditional third party. The goal of blockchain-enabled systems is to make payments faster and cheaper. Another related concept is that users can send micropayments, which might be small fractions of dollar equivalents, which were too small to previously be cost effective.

Proof-of-stake: Like proof-of-work, proof-of-stake is an algorithm used to find consensus on a blockchain. Rather than using complicated (and energy intensive) computing power to verify transactions and create blocks, proof-of-stake blockchains are verified by users that own the blockchain's currency. Trust in the blockchain is collateralized by the ownership instead of incentivized like in the proof-of-work model. The logic is that miners participating in the proof-of-stake model would work to maintain the integrity of the blockchain in order to maintain the cryptocurrency's value. There is also a randomness built into the control of the proof-of-stake that is designed to prevent centralization of power.

Proof-of-work: A system for verifying and maintaining a blockchain transaction. Many public blockchains and cryptocurrencies use proof-of-work. Proof-of-work takes a lot of computational power to solve a problem, but it can be easily verified, making it a useful tool to prevent things like email spam and denial-of-service attacks. In the crypto world, proof-of-work is used to incentive miners to dedicate computing power toward verifying the blockchain. This video from Khan Academy gives a more detailed explanation of proof-of-work. (https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-proof-of-work)

Permissionless: One of the key components of public blockchains or distributed ledgers is that they are permissionless, meaning anyone, anywhere, can download a network node and become part of the platform. Downloading and running a node means the user is helping to become part of the networked system. Node users can access the encrypted data on the blockchain. Hosting a node, or volunteering computer power to help create and maintain the network is different than being a miner.

Protocol investing: This is a strategy that requires investors to focus on picking, and investing in, the blockchain protocols that form the foundation of cryptocurrency systems. Bitcoin is a protocol, as is ethereum, and there are others. This idea is in contrast to trying to chase down the latest ICO and hope to hit it big. The logic implied by protocol investing is that as more apps, products, services are built, the underlying protocol becomes more valuable. Here's a more detailed post about protocol investing (http://www.cryptolab.io/building-cryptocurrency-portfolio-protocol-investing/).

SegWit: Short for segregated witness, refers to a code change on bitcoin's blockchain. SegWit incorporates a few different code fixes into the blockchain with the overarching goal of increasing the efficiency of bitcoin transactions. The bitcoin community (primarily the developers and the miners) fiercely debate SegWit activation and other bitcoin scaling ideas. SegWit and other protocol changes that will make SegWit possible were finally adopted during the summer of 2017.

Smart contract: The ability for users to interact in a trustless environment and be able to verify the information without third parties is key to ethereum's smart contract value proposition. Smart contracts can be set in advance by parties and executed algorithmically and verified on the blockchain all without the need for an intermediary. Smart contracts can be used to save time and money and are expected to become increasingly useful and popular in a world of the internet of things, where more and more devices are connected to the internet and executing increasingly complicated interactions. Here's a video explanation of how smart contracts wor (https://www.y-outube.com/watch?v=FkeLDPZ-v8g)k (https://www.youtube.com/watch?v=FkeLDPZ-v8g).

Turing complete: Named after Alan Turing, the famed code breaker and inventor of the Turing Machine, a Turing complete machine is a computer that is capable of solving any computational problem and limited only by the amount of memory available. The ethereum blockchain is referred to as Turing complete because it is designed as a virtual machine that is capable of completing sophisticated computation limited only by the need to pay "gas" to keep the network updated and the blockchain moving forward. Like other facets of the crypto world, whether or not ethereum is actually Turing complete is an ongoing debate (https://media.consensys.net/ethereum-isnt-turing-complete-and-it-doesn-t-matter-anyway-625061294d3c).

UASF: User Activated Soft Fork is a means of signaling that a cryptocurrency community wants to see a change to the rules governing how a blockchain functions (https://bitcoinmagazine.com/articles/latest-twist-block-size-debate-called-uasf/). Most recently used by bitcoin merchants, exchanges, users, and companies in July 2017, UASF signaled a general acceptance of bigger bitcoin block sizes, paving the way for the adoption of a soft fork. A UASF is an alternative means of reaching consensus on a blockchain. The other alternative is hash power decision making, which relies on miners to signal their support of blockchain changes by accepting or rejecting blocks embedded with different code changes.

Wallet: A cryptocurrency wallet is a vital piece of the cryptocurrencey system and one users need to become familiar with in order to securely store crypto coins. Cryptocurrencies are designed using public and private key encryption. The public key is a series of unique numbers and letters that is visible to other users and can be identified on the blockchain. The private key is held only by the user and is what is required to access funds and complete transactions. Meaning a user, say a merchant or a musician, could share the same public address with multiple people but still maintain control of the account because they have the private key. One often repeated piece of advice for people new to cryptocurrencies is to move their holdings off exchanges and into wallets where they can control the private keys. There are various kinds of wallets, including paper wallets which are designed for offline storage and hardware wallets which are like little vaults contained on an external memory stick. Those are both examples of cold wallets. A hot wallet is still somewhat accessible to the internet, which makes ease of transactions easier but might still be vulnerable to some security breaches. A wallet running on a mobile device or as a browser extension are examples of hot wallets. A common setup is to develop some sort of cold storage method for long term holdings and a hot wallet for shorter term transactions and trading.

Weak hand: A weak hand is the opposite of a hodler and not quite a trader. Weak hands bail during dumps and generally make a mess of crypto situations by not understand the true potential or upside to the technology. Don't be a weak hand.

Whale: A whale is a person or entity holding a big position in cryptocurrency. Whales can influence price (usually creating drops) when they sell. As cryptocurrencies mature, or as their market caps (the amount of money in the system) get bigger, it's possible that whales will have less of an influence on price fluctuations.

(0)
(http://news.8btc.cc
login.php)

8btc Interview: Binance CMO He Yi T…
(http://news.8btc.com/8btc-interview-binance-cmo-he-yi-talks-about-the-outlook-and-strategy-for-2017)

Founder of 8btc Chang Jia Talks Ab…
(http://news.8btc.com/founder-of-8btc-chang-jia-talks-about-the-bitcoin-ecosystem-and-the-bytom-project)

ttp://new

Cindy23 (http://news.8btc.com/author/cindy23)

I have been living two lives. In one life, I am a news editor of 8btc. I translate news, interview bitcoiners and miners. In the other life, I am an AI bot programmed to ....Forget it! Who is gonna buy this BS! I'm just me, Cindy, nobody else.

PLEASE SIGN IN FIRST

Username or email address

Password

SIGN IN

CONTACT

Xihu District, Hangzhou, Zhejiang, PRC 310012

(+86)0571-86093123

miner@8btc.com (Bussiness)
cindy@8btc.com (Submission)

gzreddragon (Red Li)

1Lt8Gs3mDe1SU8952WPsfXUUqfbwRvnbL9

QUICK LINKS

/r/btc (https://www.reddit.com/r/btc)
BitcoinMagazine (https://bitcoinmagazine.com/)
Coindesk (http://www.coindesk.com/)
Cointelegraph (http://cointelegraph.com/)
NewsBTC (http://www.newsbtc.com/)
The Blockchain News (http://www.the-blockchain.com/)
8BTCBook (http://book.8btc.com/)
8BTCForum (http://8btc.com)
8BTCNews（Chinese) (http://www.8btc.com)
BiZhongChou (https://bizhongchou.com/)
Blockmeta (https://blockmeta.com/)
Bytom (https://bytom.io/)

TAGS

8BTC (http://news.8btc.com/tag/8btc)
PBOC (http://news.8btc.com/tag/pboc)
Alibaba (http://news.8btc.com/tag/alibaba)
Qtum (http://news.8btc.com/tag/qtum)
ETH (http://news.8btc.com/tag/eth)
Blockchain (http://news.8btc.com/tag/blockchair
ICO (http://news.8btc.com/tag/ico)
BTCC (http://news.8btc.com/tag/btcc)
Bitcoin (http://news.8btc.com/tag/bitcoin)
HuoBi (http://news.8btc.com/tag/huobi)
OKCoin (http://news.8btc.com/tag/okcoin)
ETC (http://news.8btc.com/tag/etc)
LocalBitcoins (http://news.8btc.com/tag/localbitc
Ethereum (http://news.8btc.com/tag/ethereum)
Mining (http://news.8btc.com/tag/mining)
Bitmain (http://news.8btc.com/tag/bitmain)
F2Pool (http://news.8btc.com/tag/f2pool)
SegWit (http://news.8btc.com/tag/segwit)
Bytom (http://news.8btc.com/tag/bytom)
Litecoin (http://news.8btc.com/tag/litecoin)

NEWSLETTER

Get in touch with us right now.

Enter your email

Hangzhou Shichuo Information Technology Co, Ltd. 2016 | 8btc.com

(https://twitter.com/btcinch