2018 National Seminar

Bitcoin Glossary:
2018 Annual National Seminar

Address - A Bitcoin address is similar to a physical address or an email. It is the only information you need to provide for someone to pay you with Bitcoin. An important difference, however, is that each address should only be used for a single transaction. Typically consists of between 26 and 35 alphanumeric characters.

Altcoin - A form of cryptocurrency that has the same decentralized, peer-to-peer principles as bitcoin, but which uses its own blockchain and has its own rules of operation. Altcoin is the term used to describe those digital currencies that do not have as big a market capitalization or do not have the recognition of the current incumbent cryptocurrencies such as bitcoin, litecoin and dogecoin.

ASIC - ASIC stands for application specific integrated circuit, which is a specialized silicon chip that performs just one task. In the digital currency space, these chips process SHA-256 in order to mine bitcoin and validate transactions.

ASIC Miner - An ASIC Miner is the hardware that houses the chip of the same name. You put them into your Internet connection via a modem or wireless mode. Bitcoin is independent of your desktop computer.

Bit - Bit is a common unit used to designate a sub-unit of a bitcoin - 1,000,000 bits is equal to 1 bitcoin (BTC or ฿). This unit is usually more convenient for pricing, tips, goods and services.

Bitcoin / BTC (shorthand) **-** A form of digital currency created in 2009, that is created and distributed on a peer-to-peer basis. It has no central bank - transactions are conducted directly between individuals. Bitcoin is the most popular kind of cryptocurrency.

Bitcoin Index - The live bitcoin news bitcoin index is a weighted average index that shows the value of one bitcoin versus one single unit of currency of each of the majors in the Forex space – EUR, USD, JPY, GBP and AUD.

Bitcoin Whitepaper - Written by Satoshi Nakamoto in 2008, it describes the original plan and protocol for Bitcoin.

BitPay - BitPay is a payment processing company and software that allows merchants such as eBay, Amazon and other online shopping channels to accept bitcoin as payment for its goods and services.

Block - A block is a record in the block chain that contains and confirms many waiting transactions. Roughly every 10 minutes, on average, a new block including transactions is appended to the block chain through mining.

Block Reward - This term refers to the "reward" that the Miner receives for successfully hashing a transaction block.

Blockchain - A digital file distributed to everyone participating in a crypto-currency network. The blockchain acts as a kind of general ledger, keeping track of all the transactions that happen in the network. Everyone can look at the blockchain to see what transactions have happened on the network, and the blockchain is sealed using cryptography so that no one can tamper with it.

Cold Storage – A security measure for Bitcoin that is disconnected from the internet. Could be a paper wallet [see below], USB stick or hardware wallet.

Confirmation - Confirmation means that a transaction has been processed by the network and is highly unlikely to be reversed. Transactions receive a confirmation when they are included in a block and for each subsequent block. Even a single confirmation can be considered secure for low value transactions, although for larger amounts like $1,000 US, it makes sense to wait for 6 confirmations or more. Each confirmation exponentially decreases the risk of a reversed transaction.

Cryptocurrency - The broad name for digital currencies that use blockchain technology to work on a peer-to-peer basis. Cryptocurrencies don't need a bank to carry out transactions between individuals. The nature of the blockchain means that individuals can transact between each other, even if they don't trust each other. The cryptocurrency network keeps track of all the transactions and ensures that no one tries to renege on a transaction.

Cryptography - Cryptography is the branch of mathematics that lets us create mathematical proofs that provide high levels of security. Online commerce and banking already uses cryptography. In the case of Bitcoin, cryptography is used to make it impossible for anybody to spend funds from another user's wallet or to corrupt the block chain. It can also be used to encrypt a wallet, so that it cannot be used without a password.

Dogecoin - An altcoin first started as a joke in late 2013. Dogecoin, which features a Japanese fighting dog as its mascot, gained a broad international following and quickly grew to have a multi-million dollar market capitalization.

Double Spend - If a malicious user tries to spend their bitcoins with two different recipients at the same time, this is double spending. Bitcoin mining and the block chain are there to create a consensus on the network about which of the two transactions will confirm and be considered valid.

Exchange - An exchange is exactly how it sounds, somewhere where account holders can exchange one digital currency for another or a Fiat currency for a digital currency.

Faucet - When an individual or team of individuals develop a digital currency, they may pre-mine a certain amount before release and give these pre-mined coins away. This is called a faucet.

FIAT - A Fiat currency is a traditional paperback currency that is regulated by an organization such as the central bank. Examples include the Euro, the US dollar and the Australian dollar.

Bitcoin Glossary:
2018 Annual National Seminar

2018 National Seminar

Genesis Block - The very first block in the block chain of any digital currency.

Hash - A cryptographic hash is a mathematical function that takes a file and produces a relatively short code that can be used to identify that file. A hash has a couple of key properties: It is unique. Only a particular file can produce a particular hash, and two different files will never produce the same hash. It cannot be reversed. You can't work out what a file was by looking at its hash. Hashing is used to prove that a set of data has not been tampered with. It is what makes bitcoin mining possible.

Hash Rate - The hash rate is the measuring unit of the processing power of the Bitcoin network. The Bitcoin network must make intensive mathematical operations for security purposes. When the network reached a hash rate of 10 Th/s, it meant it could make 10 trillion calculations per second.

Microtransaction – The ability to pay for things in very small sums thanks to the fact that Bitcoin may be extended to 8 decimal places. Microtransactions are especially important to Bitcoin casinos by providing players the ability to deposit and gamble fractions of Bitcoins.

Mining - The act of producing units of a cryptocurrency (such as bitcoins) through some kind of effort. The effort is required so that people can't just create infinite amounts of the digital currency, which would devalue it. In bitcoin, mining requires computing power. Here is a detailed description of how mining works. Bitcoin mining is the process of making computer hardware do mathematical calculations for the Bitcoin network to confirm transactions and increase security. As a reward for their services, Bitcoin miners can collect transaction fees for the transactions they confirm, along with newly created bitcoins. Mining is a specialized and competitive market where the rewards are divided up according to how much calculation is done. Not all Bitcoin users do Bitcoin mining, and it is not an easy way to make money.

Mt. Gox – one of the first Bitcoin exchanges that began liquidating after more than 850,000 of its users' Bitcoins were lost or stolen – an amount equal to more than $450,000,000 at the time.

Output - When a bitcoin transaction takes place, the output refers to the destination address used in the transaction.

Paper Wallet - Some people prefer to store their bitcoin in the paper wallet – a form of cold storage – in order to improve security. The term simply refers to a printed sheet of paper that holds a number of public bitcoin addresses and corresponding private keys.

P2P - Peer-to-peer refers to systems that work like an organized collective by allowing each individual to interact directly with the others. In the case of Bitcoin, the network is built in such a way that each user is broadcasting the transactions of other users. And, crucially, no bank is required as a third party.

Private Key - A private key is a secret piece of data that proves your right to spend bitcoins from a specific wallet through a cryptographic signature. Your private key(s) are stored in your computer if you use a software wallet; they are stored on some remote servers if you use a web wallet. Private keys must never be revealed as they allow you to spend bitcoins for their respective Bitcoin wallet.

Proof of Work [PoW] - Proof of work simply refers to the output of any efforts to mine bitcoin. In the bitcoin block chain, the hashing of a block takes time and effort, meaning the hash block can be considered proof of work.

Public key - The public key is a string of digits and letters (your bitcoin address). When hashed with a corresponding string known as a private key it digitally signs and online communication.

Satoshi – A Bitcoin "cent", the smallest form of Bitcoins. One Bitcoin is equal to 1 million Satoshis.

Satoshi Nakamoto – the creator of Bitcoin and the author of the original Bitcoin whitepaper and code. His real identity is unknown to the world.

Silk Road – An underground website, as part of the "dark web", that was essentially a black market online. One could purchase illegal drugs, organs or hire assassins online. The site used cryptocurrencies such as Bitcoin and was shut down in 2013 by the FBI.

SHA-256 - Every digital currency must have a cryptographic function that dictates how the hash is constructed. In bitcoin, SHA-256 is this function, and is used as the basis for hash creation (*i.e.* bitcoin's proof of work).

Signature - A cryptographic signature is a mathematical mechanism that allows someone to prove ownership. In the case of Bitcoin, a Bitcoin wallet and its private key(s) are linked by some mathematical magic. When your Bitcoin software signs a transaction with the appropriate private key, the whole network can see that the signature matches the bitcoins being spent. However, there is no way for the world to guess your private key to steal your hard-earned bitcoins.

Transaction Fee - Some transactions that occur in the bitcoin block chain contain transaction fees. These transaction fees are paid to the miner that hashes the block in question.

Wallet - A Bitcoin wallet is loosely the equivalent of a physical wallet on the Bitcoin network. The wallet actually contains your private key(s) which allow you to spend the bitcoins allocated to it in the block chain. Each Bitcoin wallet can show you the total balance of all bitcoins it controls and lets you pay a specific amount to a specific person, just like a real wallet. This is different from credit cards where you are charged by the merchant.

**This glossary contains terminology and explanations of concepts relevant to various emerging technologies. The purpose of the glossary is to inform the reader of the most commonly used vocabulary terms in the cyber world. This glossary was compiled from various sources readily available on the Internet.*

To receive updates on future events and other Commission activities, visit us on Twitter @TheUSSCgov, or subscribe to e-mail updates through our website at www.ussc.gov. For guidelines questions, call our Helpline at 202.502.4545, and to request training, email us at training@ussc.gov.