

Forum:[Hack Forums](#)

Thread: [OMNICOIN VOCABULARY - Some Omnicoin words you might hear](#)

VirusTotal - April 30, 2014, 5:21 pm

Vocabulary

Address

An Omnicoin 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 Omnicoin. An important difference, however, is that each address should only be used for a single transaction. A omnicoin address is also the public key in the pair of keys used by omnicoin holders to digitally sign transactions (see Public key).

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 Chain

The block chain is a public record of Omnicoin transactions in chronological order. The block chain is shared between all Omnicoin users. It is used to verify the permanence of Omnicoin transactions and to prevent double spending.

Block Reward

The reward earned by solving a block. In Omnicoin's case it is 66.85.

Branching Point

The block at which the block chain diverges into multiple chain branches

Checkpoint Lockin

Every once in a while, an old block hash is hardcoded into Omnicoin software. Different implementations choose different checkpoint locations. Checkpoints prevent various DOS attacks from nodes flooding unusable chains and attacks involving isolating nodes and giving them fake chains.

Client

A software program running on a desktop or laptop computer, or mobile device. It connects to the omnicoin network and forwards transactions. It may also include a omnicoin wallet (see node).

Coin age

The age of a coin, defined as the currency amount multiplied by the holding period.

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 1000 US\$, it makes sense to wait for 6 confirmations or more. Each confirmation exponentially decreases the risk of a reversed transaction.

CPU

Central Processing Unit – the ‘brain’ of a computer. In the early days, these were used to hash omnicoins transactions, but are now no longer powerful enough. They are still sometimes used to hash transactions for omnicoins.

Cryptocurrency

A form of currency based on mathematics alone. Instead of fiat currency, which is printed, cryptocurrency is produced by solving mathematical problems based on cryptography.

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 Omnicoin, 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.

Deflation

The reduction of prices in an economy over time. It happens when the supply of a good or service increases faster than the supply of money, or when the supply of money is finite, and decreases. This leads to more goods or services per unit of currency, meaning that less currency is needed to purchase them. This carries some downsides. When people expect prices to fall, it causes them to stop spending and hoard money, in the hope that their money will go further later. This can depress an economy.

Difficulty

This number determines how difficult it is to hash a new block. It is related to the maximum allowed number in a given numerical portion of a transaction block's hash. The lower the number, the more difficult it is to produce a hash value that fits it. Difficulty varies based on the amount of computing power used by miners on the omnicoin network. If large numbers of miners leave a network, the difficulty would decrease. Thus far, however, omnicoin's growing popularity has attracted more computing power to the network, meaning that the difficulty has increased.

Double Spend

If a malicious user tries to spend their omnicoins to two different recipients at the same time, this is double spending. Omnicoin 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

A central resource for exchanging different forms of money and other assets. Omnicoin exchanges are typically used to exchange the cryptocurrency for other, typically fiat, currencies.

Genesis block

The very first block in the block chain.

Gigahashes/sec

The number of hashing attempts possible in a given second, measured in billions of hashes (thousands of Megahashes).

GPU

Graphical Processing Unit. A silicon chip specifically designed for the complex mathematical calculations needed to render millions of polygons in modern computer game graphics. They are also well suited to the cryptographic calculations needed in cryptocurrency mining.

Hash

The output of a hash function.

Hash function

A computer algorithm which takes an arbitrary amount of input data and deterministically produces fixed length output, known as the data's "hash", that can be used to easily verify that data has not been altered. If you change any single bit of the original data and run the hash algorithm, the hash will completely change. Because the hash is seemingly random, it is prohibitively difficult to try to produce a specific hash by changing the data which is being hashed.

Hash Rate

The hash rate is the measuring unit of the processing power of the Omnicoin network. The Omnicoin 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.

Inflation

When the value of money drops over time, causing prices for goods to increase. The result is a drop in purchasing power. Effects include less motivation to hoard money, and more motivation to spend it quickly while the prices of goods are still low.

Input

The part of a omnicoin transaction denoting where the omnicoin payment has come from. Typically, this will be a omnicoin address, unless the transaction is a generation transaction, meaning that the omnicoin has been freshly mined (see Coinbase).

Kilohashes/sec

The number of hashing attempts possible in a given second, measured in thousands of hashes.

Liquidity

The ability to buy and sell an asset easily, with pricing that stays roughly similar between trades. A suitably large community of buyers and sellers is important for liquidity. The result of an illiquid market is price volatility, and the inability to easily determine the value of an asset.

Low Priority

See Priority.

Megahashes/sec

The number of hashing attempts possible in a given second, measured in millions of hashes (thousands of Kilohashes).

Memory pool

Generators store transactions waiting to get into a block in their memory pool after receiving them. Received transactions are stored even if they are invalid to prevent nodes from constantly requesting transactions that they've already seen. The memory pool is cleared when Omnicoin is shut down, causing the network to gradually forget about transactions that haven't been included in a block.

Microtransaction

Paying a tiny amount for an asset or service, primarily online. Micro-transactions are difficult to perform under conventional payment systems, because of the heavy commissions involved. It is difficult to pay two cents to read an online article using your credit card, for example.

Miner

Computer software which is designed to repeatedly calculate hashes with the intention to create a

successful block and earn coins from transaction fees and new coins created with the block itself. The term references an analogy of gold miners who dig gold out of the ground and thus "discover" new gold that can be used to create new coins with a similar kind of discovery occurring with a successful hash to create new Omnicoin.

Mining

Omnicoins mining is the process of making computer hardware do mathematical calculations for the Omnicoin network to confirm transactions and increase security. As a reward for their services, Omnicoin miners can collect transaction fees for the transactions they confirm, along with newly created omnicoin. Mining is a specialized and competitive market where the rewards are divided up according to how much calculation is done. Not all Omnicoin users do Omnicoin mining, and it is not an easy way to make money.

Node

A computer connected to the omnicoin network using a client that relays transactions to others (see client). Each Omnicoin client currently running within the network is referred to as a Node of the system.

Nonce

A nonce is an otherwise meaningless number which is used to alter the outcome of a hash. Each time Omnicoin hashes a block, it increments a nonce within the block which it is trying to verify. If the numeric value of the effectively random hash is below a certain amount determined by the block generation difficulty, then the block is accepted by other clients and gets added to the chain.

OMC

OMC is the common unit of Omnicoin currency. It can be used in a similar way to USD for US dollars.

Omnicoins

Omnicoins - with capitalization, is used when describing the concept of Omnicoin, or the entire network itself.

omnicoin - without capitalization, is used to describe omnicoin as a unit of account; it is also often abbreviated OMC

Orphan block

An orphan block is a block that is not in the currently-longest block chain.

Output

The destination address for a omnicoin transaction. There can be multiple outputs for a single transaction.

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 Omnicoin, 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.

Priority

A scoring mechanism to help ensure that expensive data storage isn't consumed by lower quality and spam. Low priority transactions will not get included by a miner if the limited space is already filled by higher priority transactions. A transaction fee will affect priority.

Private Key

A private key is a secret piece of data that proves your right to spend omnicoins 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 omnicoins for their respective Omnicoin wallet.

Pool

A collection of mining clients which collectively mine a block, and then split the reward between them. Mining pools are a useful way to increase your probability of successfully mining a block as the difficulty rises.

Private key

An alphanumeric string kept secret by the user, and designed to sign a digital communication when hashed with a public key. In the case of omnicoin, this string is a private key designed to work with a public key. The public key is a omnicoin address (see Omnicoin address).

Public key

An alphanumeric string which is publicly known, and which is hashed with another, privately held string to sign a digital communication. In the case of omnicoin, the public key is a omnicoin address.

Reorganize

A block chain reorganize happens when one chain becomes longer than the one you are currently working on. All of the blocks in the old chain that are not in the new one become orphan blocks, and their generations are invalidated. Transactions that use the newly-invalid generated coins also become invalid, though this is only possible in large chain splits because generations can't be spent for 100 blocks. The number of confirmations for transactions may change after a reorg, and transactions that are not in the new chain will become "0/unconfirmed" again. If a transaction in the old chain conflicts with one in the new chain (as a result of double-spending), the old one becomes invalid.

Script

The cryptographic function used by Omnicoin, designed to be particularly friendly to CPU and GPU miners, while offering little advantage to ASIC miners.

Seed Nodes

Nodes whose IP addresses are included in the Omnicoin client for use during a new installation when the normal bootstrapping process through IRC wasn't possible.

Signature

A digital digest produced by hashing private and public keys together to prove that a omnicoin transaction came from a particular address.

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

Super Nodes

A participant in a p2p network which connects to as many other nodes as possible.

Stale

When a omnicoin block is successfully hashed, any others attempting to hash it may as well stop, because it is now 'stale'. They would simply be repeating work that someone else has already done, for no reward. The term is also used in mining pools to describe a share of a hashing job that has

already been completed.

Terahashes/sec

The number of hashing attempts possible in a given second, measured in trillions of hashes (thousands of Gigahashes).

Transaction block

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

Transaction Fee

A voluntary fee which can be added to a transaction which is used as an incentive to add the omnicoin transaction to a block. The fee determines the likelihood of inclusion in any given block, where a high fee included with a transaction has a priority over transactions with a lower fee included or no fee at all.

Vanity address

A omnicoin address with a desirable pattern, such as a name.

Volatility

The measurement of price movements over time for a traded financial asset (including omnicoin).

Wallet

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

Credits: <http://bitcoin.it>
<http://www.coindesk.com>

patb8man - April 30, 2014, 5:22 pm

Thank you I appreciate your contribution. This is very good information to know

Crypto Broker - April 30, 2014, 5:23 pm

A very nice post. This will be helpful for all the people in the crypto-section.

Cubs - April 30, 2014, 5:38 pm

This is a great post, especially for when users search, they will find this.

webdev77 - April 30, 2014, 5:41 pm

Excellent little list of vocab for crypto coins in general.

parity - April 30, 2014, 5:50 pm

This is a great post that will probably help a lot of users, however it should be noted that pretty much all this apply to most cryptocurrencies.

Meechy Darko - April 30, 2014, 5:53 pm

Nice. This'll help out a lot of new users.

I think this should be stickied.

VirusTotal - April 30, 2014, 6:14 pm

Thank you all guys! Tell me if there is something to add/edit/delete! :)

B?wseR - April 30, 2014, 6:15 pm

Nice man I think this will help a lot of people out.

VirusTotal - April 30, 2014, 7:10 pm

(Apr 30, 2014 06:15 PM)B?wseR Wrote: [\[CITE\]](#) Nice man I think this will help a lot of people out. Thanks a lot dude. I'll create another OMC thread asap. Stay updated! ;)

.Matt - April 30, 2014, 11:39 pm

One thing, It says that Omnicoin is refereed to as OMC and XBT? I thought Omnicoin was only OMC and XBT was bitcoin?

'Snorlax - May 1, 2014, 1:35 am

Some "Omnicoin words"? lol.

Nice giving out credit too. You totally wrote this yourself.

<https://en.bitcoin.it/wiki/Vocabulary>

Crake - May 1, 2014, 1:37 am

These are generic as fuck (I'd put them in the forum above this one) but helpful nonetheless. Thanks for the valid contribution to HF's pool of knowledge.

VirusTotal - May 1, 2014, 1:49 am

(May 1, 2014 01:35 AM)Snorlax Wrote: [\[CITE\]](#) Some "Omnicoin words"? lol.

Nice giving out credit too. You totally wrote this yourself.

<https://en.bitcoin.it/wiki/Vocabulary>

Credits for what? This is a list of words. I put all of them in a thread.

'Snorlax - May 1, 2014, 1:50 am

(May 1, 2014 01:49 AM)VirusTotal Wrote: [\[CITE\]](#) Credits for what? This is a list of words. I put all of them in a thread.

You took some from the vocabulary list on <http://bitcoin.it/>

Giving them credits for making your dirty work is the only correct thing to do.

And here are some more: <http://www.coindesk.com/information/bitcoin-glossary/>

If you were to hand this in at school, they would flag it for 100% plagiarism.

VirusTotal - May 1, 2014, 1:56 am

(May 1, 2014 01:50 AM)Snorlax Wrote: [\[CITE\]](#) You took some from the vocabulary list on <http://bitcoin.it/>

Giving them credits for making your dirty work is the only correct thing to do.

Ok i'll add "credits" to my "dirty work" where i spent time

Chilluminati - May 1, 2014, 1:57 am

Great thread lot of information, thanks for share.

-Chilluminati

'Snorlax - May 1, 2014, 1:57 am

(May 1, 2014 01:56 AM)VirusTotal Wrote: [\[CITE\]](#) Ok i'll add "credits" to my "dirty work" where i spent time

Spending time copying and pasting other people's work and claiming them as yours is not "spending time". That's cheating and everyone knows that.

Plagiarism to the top.

<http://www.coindesk.com/information/bitcoin-glossary/>
<https://en.bitcoin.it/wiki/Vocabulary>

There are your sources for most of them.

VirusTotal - May 1, 2014, 2:03 am

(May 1, 2014 01:57 AM)Snorlax Wrote: [\[CITE\]](#) Spending time copying and pasting other people's work and claiming them as yours is not "spending time". That's cheating and everyone knows that.

Plagiarism to the top.

<http://www.coindesk.com/information/bitcoin-glossary/>
<https://en.bitcoin.it/wiki/Vocabulary>

There are your sources for most of them.

Dude you are so kiddy. Srsly. You could have pmed me instead of flaming here in the thread. I added credits btw. Hope you are happy.

'Snorlax - May 1, 2014, 2:05 am

(May 1, 2014 02:03 AM)VirusTotal Wrote: [\[CITE\]](#) Dude you are so kiddy. Srsly. You could have pmed me instead of flaming here in the thread. I added credits btw. Hope you are happy.
I felt it would be more appropriate to write it here in public ?

You're welcome, kid.

Fatboy Slim - May 1, 2014, 2:06 am

This is so insanely complete. If you wrote all of this yourself, I congratulate you.

Ombra - May 1, 2014, 6:27 am

Very nice thread, all newbyes 'll enjoy this ?

VirusTotal - May 1, 2014, 7:34 am

(May 1, 2014 05:09 AM)Aceman Wrote: [\[CITE\]](#) OP Pmed me asking me to remove my thread, not entirely sure why since mine covers more than copy and paste...
I sent you a message dude. Feel free to read it

ada? - May 1, 2014, 8:07 am

"OMNICOIN VOCABULARY - Some Omnicoin words you might hear" should be
CRYPTOCURRENCY VOCABULARY - Some Cryptocurrency words you might hear

VirusTotal - May 1, 2014, 9:59 am

(May 1, 2014 08:07 AM)EYDAM Wrote: [\[CITE\]](#) "OMNICOIN VOCABULARY - Some Omnicoin words you might hear" should be CRYPTOCURRENCY VOCABULARY - Some Cryptocurrency words you might hear
Yeah maybe :)

A lot of vocabularies are general to cryptocurrency and not OMC only... :D

Cletus Kasady - May 1, 2014, 10:31 am

Very Nice list, it helped me understand a few things and I am sure it will help many others.

'Snorlax - May 1, 2014, 10:43 am

(May 1, 2014 10:23 AM)Aceman Wrote: [\[CITE\]](#) OP just gave me a neutral rep because I won't delete my thread and called me low quality. I'd say it's pretty low quality to copy and paste something and not give anyone credit until you get caught for the snake that you are ?.

Yeah he gave me a neutral too LOL. I guess that's what you get for being the good guy ?

VirusTotal - May 1, 2014, 10:45 am

(May 1, 2014 10:43 AM)Snorlax Wrote: [\[CITE\]](#) Yeah he gave me a neutral too LOL. I guess that's what you get for being the good guy ?

This guy -rep me (he's a Aceman's friend) for "Copies text then makes a thread. Then he claims it's his work and won't add credit until he has been caught. LOW QUALITY MEMBER to the max.

Thread: <https://hackforums.net/showthread.php?tid=4202528>" and +rep aceman "HQ and shouldn't listen to people who copies stuff and claims it as his."

Pffft.

Karnan - May 1, 2014, 11:26 am

very useful tutorial
thanks for sharing :)

VirusTotal - May 1, 2014, 12:14 pm

(May 1, 2014 11:26 AM)nanthakumar29 Wrote: [\[CITE\]](#) very useful tutorial
thanks for sharing :)

Thanks! Tell me if there is something to add/edit/delete! :)

GamerBoy1499 - May 21, 2014, 2:00 am

Awesome....thanks a lot.....i can really see the hardwork

VirusTotal - May 21, 2014, 8:25 am

(May 21, 2014 02:00 AM)Argo-Hacker Wrote: [\[CITE\]](#) Awesome....thanks a lot.....i can really see the hardwork

Thanks dude ? Tell me if there is something to add/delete ;)

Pessotto - June 4, 2014, 12:03 pm

Thanks for the list op :D

Very useful!!!