Cryptocurrencies in simple words

Article URL
Cryptocurrencies in simple words

Author
SecurityHome.eu

Published: 10 November 2020

Last updated on 19 November 2022.

Â

There many different cryptocurrencies and tokes. Bitcoin is the first and most famous crypto currency, but there are many other.
The goal of this article is not to give a full list of all cryptocurrencies, you can find that at coinmarketcap.com
,
We try to give an overview of the different types of cryptocurrencies and specifically how they are linked to security and privacy.
We don't want to promote any crypto coins or cryptocurrency in general. We want you to know the main differences, and what to pay attention to.
The most important you need to take away from this is to read the fine print of the specific crypto coin, before you buy any. So you understand what you buy.

Crypto currencies and tokens

A cryptocurrency is like standard currency, used for making or receiving payments. They store these transaction on their own blockchain.
A crypto token, some times called crypto assets, are normally not used for payments. They are more like a proof that you own part of an asset.
Crypto tokens are mostly on the blockchain of other cryptocurrencies, the blockchain of Ethereum is used a lot.

Centralized versus decentralized

This is an important distinction between different cryptocurrencies.
Decentralized cryptocurrencies like Bitcoin, have the ledger stored and the transactions are processed on many different places owned by many different groups.
With centralized cryptocurrencies the ledger is stored and the transactions are processed by 1 group.
Of course with centralized cryptocurrencies this 1 group has all the power.

They can refuse transaction or just completely take over you wallet.
There need to be a lot of trust here.
If central banks start with cryptocurrencies, most likely it will be centralized.

Privacy currencies

Privacy cryptocurrencies make sure that the transactions are anonymous.
For this we need to dive a little bit deeper in how the cryptocurrencies work, and we use bitcoin as base case.
The popular believe is that Bitcoin is anonymous. That is not really true. Yes, wallets can be created anonymous, and you can create as many as you want.
But, these days, crypto-exchanges are forced to do KYC (Know Your Customer). So the government can request the identity of the owner of most wallets.
And because all transactions are stored on the blockchain, they can easily follow the flow of money.
For example : When silkroad was shutdown by the FBI and the U.S. Secret Service; Some agents kept some bitcoins for themselves.
But because all bitcoin transactions are in the open. They were eventually discovered. you can read more here

.

You can yourself check the transactions of a wallet for bitcoin here : www.blockchain.com/explorer

live.blockcypher.com

Privacy cryptocurrencies try to solve this by hiding from which wallet to which wallet the transaction goes.
The transaction is still stored on the blockchain, but you can not figure out who did the transaction.
Monero (XMR) and Dash (DASH) are the most known privacy coins.

Stable coins

Stable coins are directly linked to a "real" currency like the USD, or sometimes gold.
Basically for each crypt coin there is a dollar on a bank account somewhere.
Again there is a factor of trust, you have to believe the that the money is there and that they don't just add coins when they want.
Most stable coin providers have an independent agency audit them, to prove that the money is really there.
Backed by USD : USD Coin (USDC), Binance USD (BUSD), Tether (USDT)
Backed by Euro : STASIS EURO (EURS)
Backed by Gold : Perth Mint Gold Token (PMGT), Digix Gold (DGX), Gold Coin (GLC)

Fixed supply

Bitcoin has a fixed supply. There never will be more than 21 million bitcoins.
Some still need to be mined. In October 2020 around 18.5 million bitcoins are already mined.
But the maximum supply is fixed. This is not the case for all cryptocurrencies.
Some foresee a yearly increase of few percent (inflation).
Others have a fixed supply, but all coins have already been mined and are in the hands of the creators.
And some see a fixed release of x coins in a year or month.
So you need to read the fine print of each of these cryptocurrencies.
Especially if you are looking for a store of value, you need to look into those with a fixed supply.

Mining

Most people will not be mining, But it is important to know how the new coins are made.
Like stated above some cryptocurrencies have no mining the all the coins are already available.
Some cryptocurrencies, like Bitcoin, use Proof-of-Work (PoW).
Bitcoins are "mined" using the Hashcash proof-of-work function (calculating a big number) by individual miners and the new block is verified by the decentralized nodes in the P2P bitcoin network.
When the miner "wins", is the first to calculate the correct hash, they get a certain amount of coins.

Proof-of-Stake (PoS) is another way. Here the miner doesn't have to do a difficult calculation, but whether or not he can add a block to the blockchain is decided on how many coins he already has (and how long).
And for that he gets some coins. You can see it as interest on a savings account.
Of course the early adopters and the really rich guys get an unfair advantage and more control.
Most coins have a way to prevent that too much power is in the hands of a few.
Cryptocoins that use Proof-of-Stake are Neo (NEO), Tezon (XTZ), Dash (DASH), ...

Storing coins

Because the crypto coins have real value, it is important you store them safely.
Most exchanges have wallets where you can store the coins. But be aware that usually means they have access to it.
Its like an account with a bank. If times go bad, they might block or limit you from getting money from you wallet/account.

Another option is storing the coins in your PC or smartphone.
Electrum

is software that allows you to create your own wallet on you PC.
Remember, if you lose your smartphone or the hard disk of your PC crashes, you might loose all your crypto coins.
Unless you have a backup. But make sure it is a secure backup. Because hackers can also steal your coins.
It is a bit hard to explain how that stealing works; but the short version is that: if they can read your keys (files) they can steal your crypto coins.

You can also store them on a hardware wallet. It's like a USB-key that stores your crypto coins (the private keys).
This way, it is offline and so safer, but it is your responsibility to keep it safe.
You can the plug it into you PC to authorize transactions, or via Bluetooth with your cellphone.

Another way is store it on paper. Yes, it sound weird. But you can write down your private keys down on paper and keep it in a safe.
It is a long string of random characters, so don't make any mistakes.
You can also write down your backup keys, also know as seed phrase (And it is a really good idea to write them down!). It is set of up to 24 words that can give you access to your wallet in case you lost your private keys.
And make sure no one can see it, keep it safeÂ !
If they can see it or take a photo of it, they can give it in a computer and move your coins to their wallet.
So keep it in a safe where only you have access to it.

Buying cryptocurrencies

The best way to buy crypto coins on exchanges like Kraken

, Coinbase

or any other.
Most of them have to comply with KYC (Know-Your-Costumer), so they will ask a lot of personal information to prove it is you.
Once you have bought the coins, you can move it to a offline wallet.

You can also buy coins offline of Peer-to-Peer. It is a bit more complicated, but it is more private, no registration.
If you want to know more check out Bisq

Transactions Fees

For each transaction there is a fee that needs to be paid. For each cryptocurrency it can be different, but in general the fees are use to pay the miners and the ones that keep the system up.
And the price of the fees can fluctuate a lot, depending if there is a high demand at the moment or not.
Another big difference is that unlike with credit cards, where the receiver (the shop) pays the fees, with Bitcoin it is the one who sends the money pays the fees. So remember that.
You can see the average transaction of bitcoin here :
bitinfocharts.com

Crypto-Mixers or Blenders

Crypto mixers are designed to protect user privacy, by obsucuring (mixing) coins of several transactions together, so you can not (easily) follow it on the ledger.
Some well known are CoinJoin, Tornado Cash, BitCloak, ...
There are also companies that specialise in "de-mix" these transaction.
Be carefull, many countries consider the use of Crypto-Mixers suspicious, if not illegal;
and are starting to take legal steps against them.

Some words

Blockchain

: Every block, a hashed list of transactions, is added to the blockchain, in such a way that the order of the blocks is signed and fixed. So you can't change the content of an old block without breaking the entire (block)chain.

Defi coins

: DeFi stands for for "decentralized finance" it groups a variety of financial applications in cryptocurrency or blockchain geared toward disrupting financial intermediaries.

Hash-rate

: Hash-rate is the speed of which the calculating of the mining is done in hashes per second.

Mining-pool

: Because calculating a block in Proof-of-Work (PoW) needs a lot of computer power, miners work together in a mining pool.

p2p or pear-to-pear

: means it doesn't use a central server, but users (or computers) are connected directly to each others.

Seed phrase

: This is a backup "password" of 12 to 24 words, that can give you access to you wallet in case you lose your private keys (lose your password or hardware wallet).

Smart-contracts

: These are like little programs on the blockchain. They wait for certain conditions to be met before they execute (release coins). Ethereum is the best know blockchain that can use Smart-contracts. Polkadot and Uniswap can do it also.