Monero FAQ

This FAQ is meant to be search with keywords. Focus should be on short answers when possible.

Troubleshooting

how to install and mine

- official guide (not for GPU)
- superresistant's guide for Windows (also for GPU)

no payment ID, help!

"After accidentally sent some monero to an exchange without a payment id, how to get the transaction ID to claim it?"

Rename your wallet.dat something else like wallet.dat_old and then load your wallet.dat.keys file and refresh. It will list out all the tx you ever made (you may have to log the terminal output). (source)

GUI stuff

Monero is alpha. GUI is for widespread use. In its present state, Monero is not ready for the prime time a GUI wallet would bring. We are working on fixing Monero's biggest usability issues prior to release a wallet, namely the blockchain bloating.

Test GUI wallets are available on the OP, but they're experimental, use them at your own risk.

My blockchain doesn't work

The first time you mine monero on a machine, you may want to speedup the syncing process by copying the blockchain from a previous machine. The blockchain.bin file is incompatible between Windows and Linux. It is a known problem with the boost library this is using to save the files. Download a recent blockchain on the OP.

General

What is CryptoNote?

- official introduction
- Cryptonote whitepaper (updated list of footnote link)

Why CryptoNight?

So far, the best algo for ensuring that GPU (hardcore miners) do not have that much of an advantage over CPU (casual miners).

Is Monero really anonymous?

Short answer: almost

Long answer:

Not completely anonymous, but much closer to true anonymity than the competition. Ring signature is backed by almost fifteen years of study by academic cryptographers and is widely used.

Decentralized mixing based on outputs. So no risk of a VPS SPOF being snapshotted by the host (more info). Plus, being based on outputs and not on transaction, it doesn't require volume to match your own amount of coins.

Your IP can still be traced, that's why we partnered with i2P to fix this.

The OP mentions how Monero fares relative to the main competition.

What are the features of Monero?

- It uses the Cryptonote code base.
- Started *from scratch* (i.e. from genesis block).
- Emission schedule has a *flatter curve* (80% of the coins are mined within 4 years).
- Monero – XMR (*monero* = coin in the Esperanto language).
- Block target = 60 seconds.
- Penalty-free block size is increased.
  CryptoNote doesn't have hard limits: all parameters are adaptive. Max block size is adaptive also. It is recalculated the same way difficulty is. In case miner creates block bigger than `1*CURRENT_MAX_BLOCK_SIZE` the penalty is applied to block reward (i.e. block reward is decreased). In case miner creates block bigger than `2*CURRENT_MAX_BLOCK_SIZE` such block will not be accepted by network.
  For blocks below penalty-free block size this logic isn't applied. I.e. even in the blockchain with all blocks empty you can create a block of this size with full block reward. In reference code this penalty-free block size is 10Kb – this is good for 2-3 private transactions (strong privacy is given with a mixing factor of 5 or more; no privacy is given with 0). It's better to have a bit more.
- Decimal point has been moved from BCN (18.446 million max supply instead of 184.46 billion). This is purely a UI change – technically there will be $2^{64}-1$ atomic units (roughly 10^{19}).
- Monero supports multisig but the client doesn't atm (source).
- [not on OP] Why are XMR addresses some 3-5 times longer than BTC ones. (source)
  - This isn't your "true" address that coins go into. It's used (along with some random data) to automatically generate new addresses for every transaction. It needs to be this long by design because it actually consists of two parts.

This is the first layer of privacy (before ring signatures) and it makes blockchain analysis much harder.

- [not on OP] Why all addresses start with 4? (source)
    - hardcoded in XMR's configuration files

Others

I want to help with development / design / marketing...

Please PM us.

I want to integrate new currency in my sevices (pools, block explorers, exchanges etc)

Please check the API pages: https://wiki.bytecoin.org/

API is far from being complete. Please PM us for help or ask on the CryptoNote forum: https://forum.cryptonote.org