Monero FAQ

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

Some rules: no *argumentum ad hominem* or *ad personam*. Stick to the facts, only mention the competition (especially by name) when it is not possible to avoid it.

mining

- http://cpucoinlist.com/how-to/cpu-mine-monero-pool/
- http://monero.cc/getting-started
- https://bitcointalk.org/index.php?topic=613072.0

RTFM

https://cryptonote.org/whitepaper.pdf

(list of links: https://bitcointalk.org/index.php?topic=583449.msg7289181#msg7289181)

multisig

Monero supports multisig but the client doesn't atm (source on BTCtalk).

security

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 (source on BTCtalk). Plus, being based on outputs and not on transaction, it doesn't require volume to match your own amount of coins.

Since the weak point of Monero is IP tracing, we plan to implement TOR for IP obfuscation

Monero is immune to double-spending and 51% attack are much less of a hassle on monero.

competition

- Darkcoin (good summary by a poster; technical summary below, search for "CoinJoin-based approaches"; a note on the profitability model of masternode). x11 isn't energy efficient (fluffypony, #monero) -the power draw and heat output [of GPUs mining X11) would of course match scrypt (chmod_711, #monero), Do you happen to have a list of academics that have looked over the Darkcoin whitepaper and can vouch for the cryptographic and mathematical soundness of the architecture, and can confirm that the theories referenced in papers and publications are being applied correctly? Also, you wouldn't happen to know if these cryptographers and mathematicians have confirmed the implementation in

Darksend is correct and true to the Darkcoin whitepaper? Lastly, I can't seem to find a whitepaper on the Darkcoin website - do you have a link for me? (source)
- Zerocoin (technical summary below, search for “ZKP-based approaches”)
- Zerocash
- Fedoracoin
- Anoncoin
- Cryptonote (a.k.a.: “what doesn’t kill me makes me stronger”)
    - BCN. Original code, 80% premined
    - QCN. Parasite, original webpage (source). Present price is higher only because the coin is younger and has less coin generated. With time, the price difference will lower (source) — till next clone?
    - FCN. Merge mined coin with either BCN or XMR (user’s choice)

QCN worries

QCN mines 1/4 as many coins as XMR. So it would have to be valued at 4x as much to be par (source). If all it takes to create a valuable coin is cloning one, then there will be no valuable coins at all. (source)

transaction retrieval

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)

price manipulation/monero not a scam

“The altcoin space is mostly people who watch coinmarketcap for movement and buy during pumps initiated by 'whales'. Why would the anonymity coin subspace be different? Actual properties of coins are manifested in a long-term drift in price, not daily movements.” (source)

egalitarian

smoooth (a dev) on this

If CryptoNight achieves making GPU mining not possible or not worth it much, monero could be mined beyond the “miners oligarchy” with high-end GPU farms. Something like: "Do you want to devote some of you CPU power to help secure the network. You will be eligible to receive free coins (recommended) [check box]." Get millions of users doing that and it will drive down the value of mining to where neither botnets nor professional/industrial miners will bother, and Satoshi's original vision of a true p2p currency will be realized.

That's what cryptonote wants to accomplish with this whole "egalitarian mining" concept.

CryptoNight is sometime compared to Cuckoo Cycle, another memory-hard PoW algorithm. See this post about how Cuckoo Cycle could be optimised:

https://bitcointalk.org/index.php?topic=405483.msg6006665#msg6006665

farming

"*A large percentage of the network is cloud mining. Some of these users keep, some others dump. The price of Monero (and CPU coins in general) is partially set by the equilibrium profitability of cloud mining. It's the same situation as GPU farms or ASIC farms, except determined by the spot instance price instead of the cost of electricity.*" — (source)

wallet

There is GUI wallet bounty and the work is progressing steadily. We don' want to rush the wallet, though, we want it to right from the start. Since we prefer to underpromise and overdeliver, don't expect a GUI wallet before 4 months — Electrum is on the radar (fluffypony,#monero).

logo

Designed by designers with help from advertiser, it will be announced on Mondy June 2nd. It will be the foundation for the website.

We consulted with:

- *two independent groups of advertising executives*
- *a PR firm*
- *several groups of marketing resources*
- *UX designers*
- *graphic designers*

Some of them we consulted on a professional (paid) basis, some over business dinners, and some just by tapping into acquaintances. We are a diverse core team, geographically scattered across the globe, and we used our connections and resources to make an informed decision. These domain-level experts all had various opinions about which of the potential logos they liked, and none of their choices were the ones I personally liked. But the common thread among these domain experts, from South Africa to Germany to France to Canada and the United States, was that this logo was in their top 3. It was literally the only logo they all liked enough from the wide selection of paid-for submissions.

Now, I'm not saying the decision making process is perfect, but both casually acquainted with and paid-for experts in this field agreed on the logo. We are thus confident that it is the right choice, and that the logo is interpretive enough that it can be adapted to suite any environment.

(source)

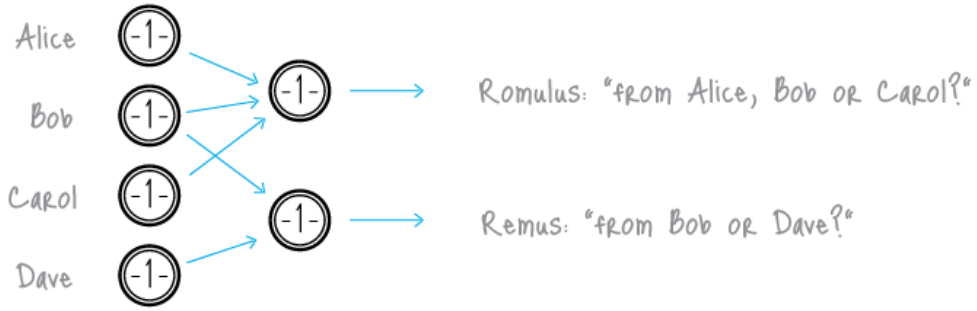
What is CryptoNote?

CryptoNote is the technology that allows creation of highly private egalitarian cryptocurrencies. You can visit their website. The level of anonymity provided by

CryptoNote isn't possible with Bitcoin code base by design. Two of the main features of CryptoNote are *ring signatures* that mask sender identities by mixing and *unlinkable transactions* accomplished by creating one-time keys for individual payments. Ring signatures are explained below and you can read the white paper for the details. The images below come from CryptoNote's website.

A normal signature looks like this. There's only one participant.

A ring signature obscures identities because it only proves that a signer belongs to a group.



This allows a high level of anonymity in cryptocurrency transactions. You can think of it as *decentralized mixing*.

What are the features of this coin?

- 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}).

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.

How does this compare to other anonymous solutions?

Ring signatures originate from the work of Rivest et al. in 2001 and the implementation in CryptoNote relies in particular on Fujisaki and Suzuki's work on traceable ring signatures. There are two other anonymity implementations currently available or in development. One is ZeroCoin/ZeroCash's use of zero-knowledge proofs. The others are based on gmaxwell'sCoinJoin idea (such as mixing services for Bitcoin or the altcoin DarkCoin).

1. Comparison with ZeroCoin and ZKP-based approaches

You can read about ZeroCoin and zero-knowledge proofs (ZKP). The ZK environment allows an anonymity set that includes everyone in the network because the validity of an output can be proven without knowing the corresponding public key until it is spent. The largest risk is that this is recent research-level cryptography that hasn't been subjected to years of cryptanalysis, so exploits may emerge down the road. Ring signatures are more mature, though CryptoNote is the first time they have been used in cryptocurrencies.

Other issues with ZKP include the RSA private key used to initiate the accumulator, which must be trusted to be destroyed by the generating party. It also obscures the entire economy, not just sender/receiver identities. If the ZK system is compromised, then an

attacker can continuously spend coins that don't exist using false proofs. This damage is hidden from everybody due to total blinding and consequently at any given time it's not possible to know if the network has already been compromised. There is a tradeoff between these inherent risks and the maximal anonymity set provided by ZKP. CryptoNote aims for a different balance through the dual layers of privacy provided by one-time keys and ring signatures.

2. Comparison with CoinJoin-based approaches

XMR is more qualitatively similar to mixing implementations like CoinJoin. The differences arise in the departure from the Bitcoin protocol, which allows XMR to use new cryptography to provide decentralized and trustless mixing of superior quality. The critical problem with mixing services is the need to trust the operators. As an example, blockchain.info's mixer gives the following disclaimer: "However if the server was compromised or under subpoena it could be force to keep logs. If this were to happen although you haven't gained any privacy you haven't lost any either."

The CoinJoin-inspired DarkCoin performs mixing with selected “masternodes” since it still uses ordinary signatures that can be mapped one-to-one. This is a marginal improvement over a more centralized mixing service since a randomly-selected node is less likely to exhibit bad faith (such as keeping logs). However, this approach still relies on the health and good behavior of the nodes, which XMR's more fundamental approach is not vulnerable to. Even under proper functioning, the quality of anonymity with this method is low compared to XMR's ring signatures.

XMR's ring signatures are also far more secure and convenient than CoinJoin because they mix outputs not transactions. This means a transaction doesn't involve waiting around for other senders to mix with. Nor is a user restricted to mixing only if others are sending the same amount. Arbitrary amounts can be sent at any time without anyone else's participation. This feature makes a timing analysis of the blockchain useless for mapping identities. The degree of anonymity is also a choice rather than decided by the protocol: do you want to be hidden as one among five or one among fifty? The size of the signature grows linearly as `O(n+1)` with the ambiguity so greater anonymity is paid for with higher fees to miners.

Overview of a transaction

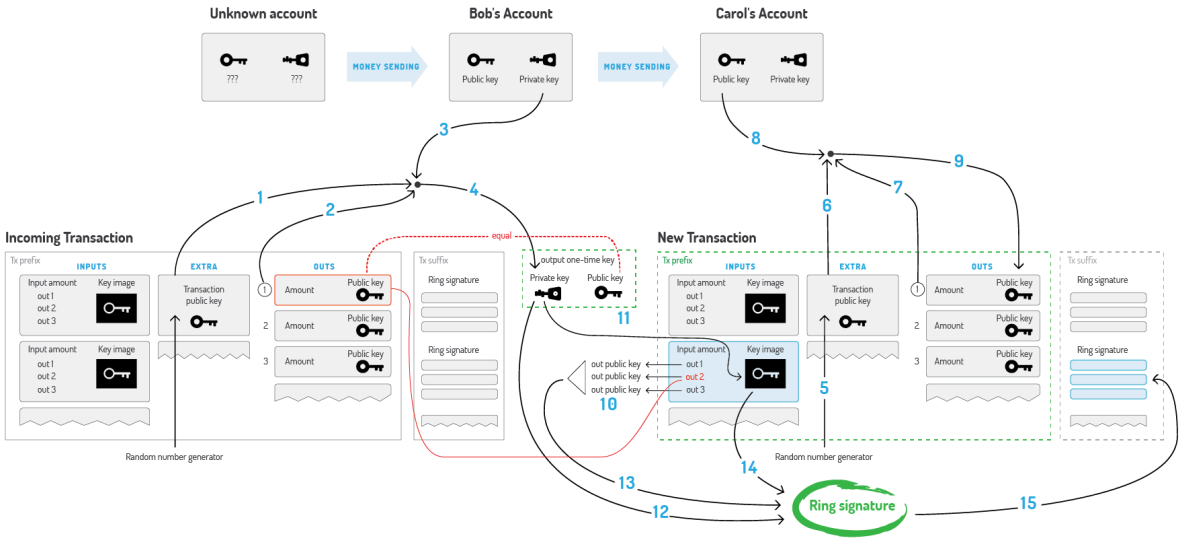
Bob decides to spend an output, which was sent to the one-time public key. He needs Extra (**1**), TxOutNumber (**2**), and his Account private key (**3**) to recover his one-time private key (**4**).

When sending a transaction to Carol, Bob generates its Extra value by random (**5**). He uses Extra (**6**), TxOutNumber (**7**) and Carol's Account public key (**8**) to get her Output public key (**9**).

In the input Bob hides the link to his output among the foreign keys (**10**). To prevent double-spending he also packs the Key image, derived from his One-time private key (**11**).

Finally, Bob signs the transaction, using his One-time private key (**12**), all the public keys

(**13**) and Key Image (**14**). He appends the resulting Ring Signature to the end of the transaction (**15**).



Others

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

Please PM me.

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 me for help or ask on the CryptoNote forum: https://forum.cryptonote.org