**What is monero**

**Security measures in Monero**

Stealth Addresses

* Supported by coins using the cryptonote algo
* Receivers privacy not the senders

In a traditional system. A user will send money from his wallet address directly to another person’s wallet address.

In a system with stealth addresses the system is the same in that the user sends to a recipient’s wallet address.

However, a random wallet is generated when a transaction is created and then money is stored in there. (not in the receiver’s wallet).

The generated wallet which contains the money, is viewable to everyone, however the only person that can access this wallet is the person who the money was sent to. The wallet is encrypted with the recipient’s public key. Only the recipient can open the wallet with their private key.

There is a one time spendable public key attached to the wallet

Technically, a Monero wallet never contains any money, it just has access to wallets which do contain money. Hpow

Ring Signatures

* Senders privacy not receivers
* Signed by multiple people

The transaction is signed by the sendee, as well as some random “decoy” signatures(picked from the blockchain)

To an outside view there is an equal probability that either of these senders sent the transaction.

Protection through obscurity.

Ring CT Confidential Transactions

Used to hide transaction amounts

The entire quantity of a transaction is sent, this verifies to the network that the money has been sent – but it does not show the amount. The network can see that the ownership of the money has changed. The receiver wallet will automatically give change of the sent amount.