Sam Hopkins

Dr. Seamons

CS 401R

Final – Monero

# Overview:

History

Monero is an altcoin with a focus on private and censorship-resistant transaction. It was created in April 18th, 2014 with the tag XMR, and is currently the ranked 14th of all altcoins by total market cap. It claims to be a completely private, secure, and untraceable cryptocurrency. While Bitcoin and Ethereum have public block-chains, every Monero transaction is hidden. This differs from other private alt coins like Z-cash by making every transaction amount, sending address, and receiving address private, rather than being a selectively transparent cryptocurrency. There are 30 core developers, and over 500 contributors.

Key features

* Monero is completely private, which means that no one can see or trace your transactions
  + This privacy is a result of three key components of Monero: Ring Signatures, Stealth Addresses, and Confidential Transactions. A visual is included at the end of this paper to help understand what these mean and how they are put into effect.
* It is fungible, meaning it is more fluid and efficient than Bitcoin or other altcoins
* It is dynamically scalable; we will talk about what this means in the “Mining” section

Strengths

* It is ASIC resistant, due to the CryptoNight hashing algorithm, making it a desirable cryptocurrency to mine for beginners, unlike Bitcoin. More on this in the “Mining” section
* It is private and anonymous
* It has a strong development team, according to one site Monero has the “third highest code contributor count”, below only Ethereum and Bitcoin
* It is dynamically scalable
* Relatively Accessible

Weaknesses

* It is less fluid, as the complexity of Monero makes it hard to add on traditional crypto wallets
* Some hard forks produce lots of “scam coins”, and there is a Bi-annual upgrade that can pose problems long term.
* Because it is completely anonymous, it is used for lots of illegal activity, such as money laundering and black-market transactions. In some cases, there is legislation to ban the Monero currency due to criminal activity
* It is funded mainly by donations, which could pose a problem in the future for the cryptocurrency
* It has a much larger transaction size than other cryptocurrencies due to its encryption
* It is more complex than other cryptocurrencies, and can confuse less technically savvy users
* Even though it is ASIC resistant, the mining of Monero is largely dominated by three main mining pools

Mining

* Hashing Algorithm: CryptoNight

CryptoNight is a hashing algorithm that is based on the CryptoNote system. This makes Monero ASIC Resistant. Some Key features of what makes CryptoNight ASIC Resistant include:

* + CryptoNight requires 2 MB of fast memory to work, so the memory limit makes it harder and more expensive to create ASICs for Monero
  + CryptoNight is built to be CPU and GPU friendly because it can take advantage of certain instructions (AES-Ni) so some of the work done by CryptoNight is already done on modern hardware
  + There are talks of moving from a “Proof-of-work” system, which would further limit the efficiency of ASICs
* Dynamically Scalable

As mentioned before, Monero blocks are dynamically scalable. This means that although there is not block size limit like there is in Bitcoin (1MB), there is a penalty for trying to validate a large block/trying to create a malicious block with a lot of transactions. When a block is submitted, the past 100 block sizes are averaged together. This size becomes the reference, and each new block that gets submitted is reduced quadratically based on the size difference. If the new block has double the size of the median block size, there is no reward gained. If it is 80% bigger, then the reward is reduced by around 64%, and so forth. There is an incentive to not clog the system with giant block sizes, as no reward would be gained from mining.

* Each block is mined every 2 minutes, and the current reward for a block is around 1.76 XMR (April 16, 2020 2:24pm)
* There are a number of mining pools available to start mining and joining a mining pool is recommended and relatively easy. There are plenty of tutorials on how to set up the software needed to mine Monero
* There are not very many wallets that directly support Monero storage, some include MyMonero (https://mymonero.com). There is discussion of making a dedicated hardware wallet in the community

Other

Official site: <https://www.getmonero.org/>

Current Market price of Monero (XMR): 56.77 USD (as of 4:07pm, April 16, 2020)

Image that explains how Monero transactions work and keep privacy in simple terms: <https://static.blockgeeks.com/wp-content/uploads/2017/09/monerounderthehood.jpg>