

Cryptocurrency	Distribution Method	Emission Curve (if PoW)
Monero	<p>PoW; Good initial hash power distribution due to mining done by CPUs/GPUs, but it will eventually succumb to centralization due to the economies of scale ASICs bring</p> <p>A</p>	<p>Approximately 86% of pre-tail Monero will be mined within 4 years of its launch. For example, Compared to Bitcoin... that is rather steep. Since such a large percentage of the money supply will be mined in the first 4 years which will make distribution more unfair, but there is a tail emission which more closely resembles FIAT currencies.</p> <p>C</p>

**Hashrate Centralization  
(if PoW)**

**Inflationary**

**Deflationary**

Mining Monero is done with GPUs using the CryptoNight algorithm. CryptoNight is a "memory hard" algorithm, but ASICs can be developed for it as soon as it is economically feasible. If Monero gains in value, then mining will become centralized due to the economies of scale ASICs bring.

B

Yes, permanently, but very minimally after 10 years.

B

No, Monero will always be inflationary.

F

## Innovation

Monero is a fork of a cryptocurrency named Bytecoin whose release was quite shady and questionable. Monero is meant to be a more fair fork of Bytecoin's innovative technologies including ring signatures (an anonymization technique leveraging cryptography), smooth block reward reduction, and the CryptoNight PoW algorithm. Monero also quickly reviewed and implemented Confidential Transactions which improved upon their existing ring signatures to shield the amount and value sent, which increases the anonymity of transactions. Monero seems adamant about keeping up to date with the best anonymization techniques available, and it seems like they will leverage zSnares if they can be made to have a trustless setup (google Starks)

A

## Market / Niche

Fungibility / Privacy

A

## Features

Confidential Transactions  
Ring Signatures  
Smooth Block Reward  
Reduction  
A

## Road Map

- Fluffy blocks
  - GUI port to android
- Forum Funding System redesign
  - Subaddresses
  - Multi-signatures (multisig)
  - Kovri alpha release
- Additional MRL research papers
- Second-layer solutions for speed and scalability
- More efficient range proofs for RingCT to reduce transaction sizes

A

## Road Map Feasibility (Technical & Time Constraints)

Since Monero leverages RingCT and Ring Signatures, some items on the road map are made much more difficult than implementing the same features on a cryptocurrency that doesn't.

Although Monero has a solid development team, there are not many capable development teams from other cryptonote blockchains working on the same/similar either.

C

## Competiton

There is a lot of competition in the blockchain space that provides alternative means of making private transactions. zkSnarks, zkStarks, and different implementations of coin join are competitors. As it stands, Monero probably has the best anonymity with the least amount of downsides. This will likely change in the future as technological advances are researched and made. Monero will need to stay vigilant in improving its tech to stay on top of the private transaction blopckchain sector.

A

## Stakeholder Governance

Nothing on the protocol level  
F

## Developer Skills / Team

A skilled development team and researchers  
B

## Developer Updates

So far, the developers have proven to be fairly quick to research and implement new features.

B

## Hot Wallets

One: Mymonero.com

B

## Light Wallets

One: Mymonero.com

B

## Mobile Wallets

One: Mymonero.com  
(Android wallet on roadmap)

B

**Linux Wallet**

**Windows Wallet**

**Mac Wallet**

**ARM**

Four: GUI (64bit and 32bit) and CLI (64bit and 32bit)

A

Three: GUI, CLI 64bit, and CLI 32bit

A

Two: GUI and CLI

A

Two: CLI (ARM v7 and ARM v8)

A

**FreeBSD**

**DragonFlyBSD**

**Android Wallet**

**iOS Wallet**

One: CLI (64bit)  
B

One: CLI (64bit)  
B

None  
F

None  
F



**Consensus  
Algorithm**

**Network Effect**

**Reputation**

**Volume & Liquidity**

CryptoNight  
"ASIC resistant" memory  
hard algorithm, but ASICs  
will likely be made once it  
is economically feasible

B

There is quite a bit of hype  
around forums and social  
media in support of  
Monero, and a decent  
amount of cryptocurrency  
news coverage.

B

Monero does not really  
have any shady dealings in  
its past that I am aware of.

A

Top 9 crypto in volume  
with \$66,223,300 daily  
volume (as of 11/26/17).  
It is traded on many  
exchanges and therefore  
has quite a bit of liquidity.

A

**Exchange Options**

**Longterm Historical  
Performance  
(Value)**

**Shorterm Historical  
Performance  
(Value)**

**Development Funding  
(on the protocol level)**

There are numerous  
reputable exchanges with  
Monero trading pairs

A

Bullish performance since  
inception

A

Performing well in the  
current bull run

A

No budgeting/proposal  
features in the protocol

F

## Rolled Back

The blockchain has not  
been rolled back

A

## Fork

Technically a fork of Bytecoin,  
but Bytecoin has quite a shady  
start. I consider the highest  
market capitalized fork as being  
the main chain, therefore that  
is Monero. Bytecoin is the fork.

A

## Transaction Capacity

Bandwidth and memory  
requirements are the  
limiting factors since  
Monero has an adaptive  
blocksize

**Blockchain  
Bloat**

All of the cryptography  
Monero leverages leads to  
a more bloated blockchain  
than standard.

D

**Transaction  
Speeds**

3 minutes 46 seconds until  
1st confirmation, and 26  
minutes for 10  
confirmations, which is  
when the transaction is  
unlocked for spending

C

**Transaction  
Privacy**

Solid privacy with little  
downsides.

A

**Metadata  
Privacy**

Manual and separate  
Tor/I2P setup

F

## Centralization

## Fungibility

No masternodes or other  
centralizing tech other  
than standard  
centralization that can  
occur with PoW  
cryptocurrencies

B

Privacy is default, possibly  
the most fungible  
blockchain

A