Jeffrey L. Alton, CFA
Director of Research
jalton@lucylabs.io
telegram: LucyLabs999

Digital Asset Research
June 12, 2018

Stats (as of 6/12/18)

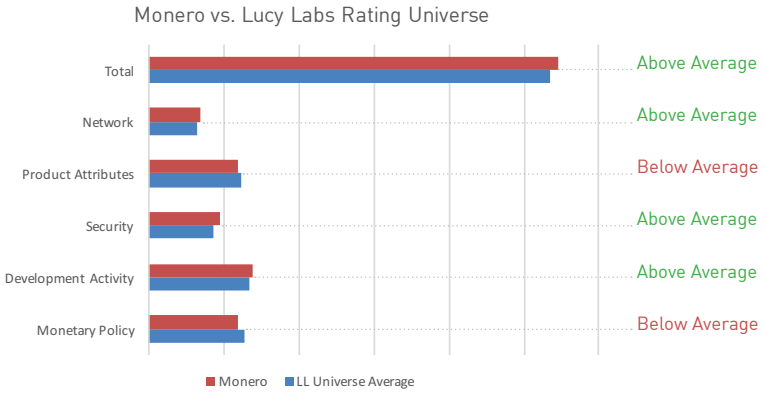
Price (USD):	$121.32
Market Cap	$1,961,773,870
Market Capitalization Rank	#12
Circulating Supply	XMR 16,169,976
2050 Supply (estimated)	XMR 22,482,673
30 day exchange volume	$1,039,962,634
Rank - 30 day exchange volume	#30
10 day price volatility annualized	99%
3 month price volatility annualized	131%
Major Exchanges	Kraken Binance Poloniex Bitfinex Bithumb

Source: Lucy Labs, Inc., Coinmarketcap.com, onchainfx.com, Coinmetrics.io

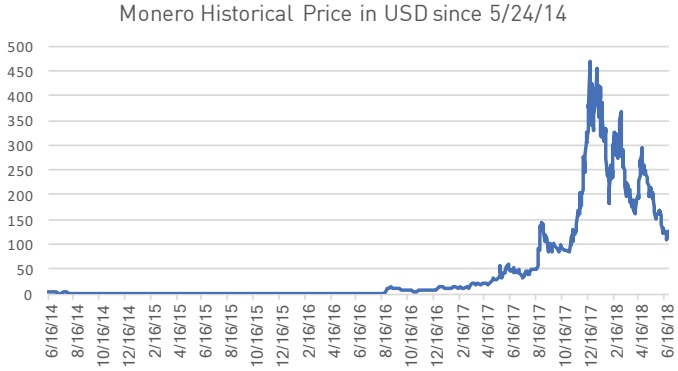
Things to know

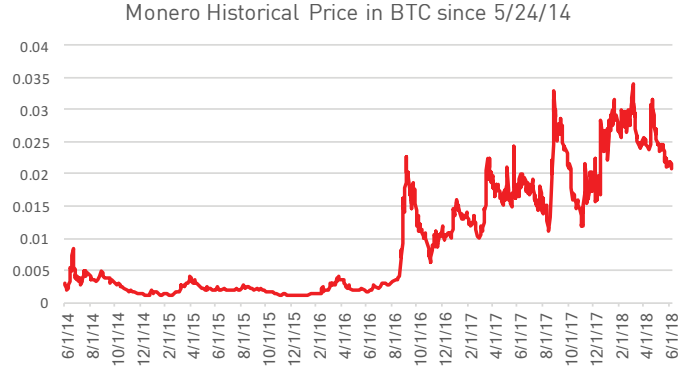
Monero (XMR)

- The privacy of the Monero blockchain provides unique ways to employ the coin and introduces a degree of fungibility not seen in more "traditional" coins such as Bitcoin and Ethereum.
- In 2019, Monero's blockchain reward will fall substantially. The decrease in supply could affect valuation positively for long investors as supply becomes more limited.
- The most recent Monero fork appears to have achieved its goal of blocking compatibility with ASICs mining machines – allowing the Monero community to maximize decentralization.



Historical Price Chart





lucylabs

Overview

Monero, which means "coin" in Esperanto, began mining in April 2014 as a fork of one of the first privacy coins. The Monero blockchain currently uses the CryptoNight V7 hash algorithm designed to obfuscate transaction information. A flaw in the original CryptoNight algorithm was patched in September 2014 and the algorithm has run free of major incidents since then.

The face of Monero is Riccardo Spagni (Fluffypony), who along with a team of developers, took control of the project that was originally called bitmonero. Mr. Spagni has been an effective leader of the development community appearing in many interviews and participating in development initiatives.

Because of its privacy attributes, Monero has been associated with criminal use and trade on various dark net sites, including Alpha Bay. However, Monero developers believe that the advantages of the privacy features outweigh the disadvantages and are committed to consistently improving Monero's privacy attributes. (Please refer to the recent Lucy Labs Privacy Coins report where we concur that privacy attributes will eventually become mainstream.) Developers are also passionate about preventing the use of ASICs machines on the Monero blockchain, which they believe would to a centralization of power among miners.

Unique Attributes

Privacy

The Monero blackchain uses four main technologies to obfuscate transactions.

1. Ring Signatures
   To protect the sender's identity, Monero algorithm "mixes" the transaction with several other transactions on the blockchain to form a "ring". This ring is used to formulate a one-time key image used in the transaction. Knowing the key image is not enough for an individual scrutinizing the Monero blockchain to identify the sender's account, but the key images can be used by miners to prevent double spending.

   Monero ring signatures have been the topic of critical research reports which have shown that the system does not provide absolute privacy. Under certain circumstances, it is possible to make an educated guess as to the real transaction in a ring. Monero developers have consistently worked to lower the probability of compromising a ring signature including the mandatory use of ring signatures in each transaction, expanding the number of decoy transactions in a ring and tweaking the algorithm to select better decoy transactions. However, some observers estimate the probability of guessing the actual transaction in a ring is still relatively high in some cases.

2. Dual-Key Stealth Addresses
   To obfuscate a recipient's identity, the network creates a one-time public key for a given transaction. This public key can be viewed on the blockchain, but it is not associated with the recipient. Rather, the recipient's wallet scans the blockchain to find the public key related to the transaction and then creates a private key, not viewable on the blockchain for use in the transaction.

3. Ring Confidential Transactions
   In January 2017, the Monero development team added "Ring Confidential Transactions" (Ring CT) to the protocol to completely hide transaction amounts in rings. Newly minted Monero and Monero being used under the Ring CT system for the first time are not hidden, but once these coins have run through the Ring CT protocol, all future transactions using these coins are obfuscated by the network.

4. Kovri
   Cryptocurrencies do not store IP addresses of transaction senders or receivers on the blockchain. However, an attacker can run a node that connects to many active nodes and enables them to associate IP addresses with current transactions. The Kovri protocol, currently under development, hides both the sender's IP address and its geographical location, closing off this potential threat of deanonymization.

Dynamic Block Size and Block Rewards

Both Monero's block size and block rewards are dynamic, expanding and contracting to meet the needs of the network at any given time. The block reward algorithm is set to incentivize miners to limit block size to the median size of the last 100 blocks, above which a mining reward penalty is initiated.

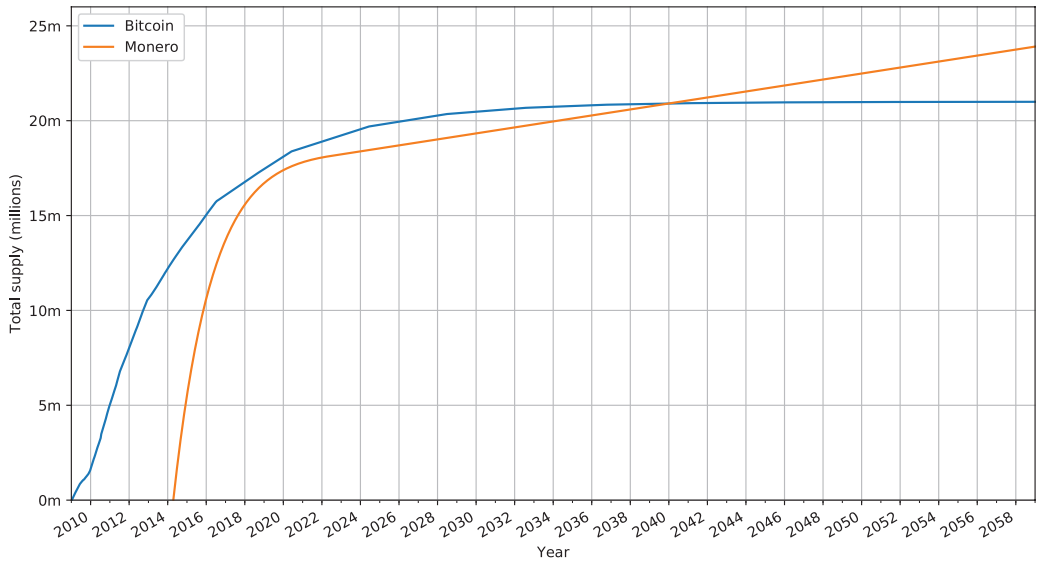
Using dynamic block size and the Lightning Memory-Mapped Data Base (LMDB), Monero is theoretically capable of processing up to 1,700 transactions per second (tps), ranking it among the highest transaction speed coins. However, because of the amount of data included in each privacy transaction (each Monero transaction is 60x-70x the size of a Bitcoin transaction), Monero confirmation speeds are severely limited by processing and network capacity. Monero developers are working on different technologies, such as Bulletproofs and Sidechains, but scaling the network is a difficult hurdle for Monero developers. That leaves Monero dependent on Moore's law and better network technology to continue to scale organically.

Monetary Policy

The Monero mining curve will enter its tail emission phase in 2022 and Monero will be mined at a constant 157,788 coins per year thereafter, resulting in an ever-decreasing inflation rate. Under this scenario, Monero will reach a total supply of 21 million coins at approximately the same time as Bitcoin in the year 2040. The tail emission is designed to act as a permanent incentive to miners to continue to process transactions efficiently.

The Monero block reward path is steeply downward sloping and the annual block reward to all miners will be lower than Bitcoin's from 2019 through 2027. So, while Monero had a double-digit inflation rate in 2017, new annual supply is set to fall rapidly. Traders may want to position themselves ahead of Monero's rapidly decreasing blockchain reward path.

Total coin supply of Bitcoin vs. Monero



Source: Lucy Labs, Inc.

Development Activity

Monero developers maintain a vibrant community with seven active core developers listed on the website. Riccardo Spagni reported that over 80 developers contributed to the recent Monero hard fork in April. The hard fork included over 40 improvements to the Monero protocol including increased ring size from 5 to 7 and a modified PoW block to prevent DoS attacks from ASICs. The hard fork also initiated Bulletproofs on testnet. Bulletproofs are designed to reduce Monero transaction size by 80% to increase the scalability of the network.

Monero developers are also heading up the "Tari" project which is being built on the Monero blockchain. Tari is conceived as a sidechain which will enable the issuance and transfer of digital assets, such as concert tickets. Users will be able to set the privacy desired for transactions using a toggle feature. The project is designed as a private alternative to Ethereum. Tari mining will be merged with Monero, meaning Monero miners will receive Tari tokens. The Tari project is venture-backed.

lucylabs

Security

Monero is the only cryptocurrency to use the Cryptonight V7 hashing algorithm and has a relatively high hashrate relative to other altcoins. That combination limits the ability of malevolent actors to rent mining capacity and launch a 51% attack on the network. Hashing power is also spread more evenly among mining pools compared to other coins.

The Monero network is comprised of over 2,300 nodes spread over 75 countries as of early May according to Monerohash.com. A higher, decentralized node count indicates a higher chance for the coin to survive natural disasters relative to other coins.

Network and Community

Monero has an active development community and Riccardo Spagni is effective in keeping Monero in the crypto spotlight both through public appearances and participating in a development team that is looking to constantly innovate. Monero enthusiasts are active on social media, particularly on reddit, where daily posts rival those of all the major coins.

Monero developers did not reserve any coins for themselves and therefore there is no current coin overhang. Transaction volumes run at about the average as other privacy coins Zcash and Dash, but about 1/50th of Bitcoin.

Conclusion

The Monero development community's passion for the coin, its stable operating history and privacy attributes place it among those coins with the potential for longevity in the crypto world. The coin's Achilles heel is the difficulty in scaling transactions given computing and network limitations. As Monero developers continue to chip away at the scaling problem, the case for Monero as digital cash will become stronger. However, Monero shows little inclination toward adopting a regulatory-friendly position, and therefore is likely to remain operating outside the legacy financial system.

* Officers and/or employees of Lucy Labs, Inc. currently have a position in Monero.

Tip jar

If you liked this report and want to support continuing research in cryptocurrencies, send a tip to Monero address

`47ajkLad4eac57EgatMRTnUEoak2cYKbUWQasSRVoZ7AFKLqANatA8S99jAEKTEhmAi9ir7nVxf463ovYA7bB3KZKoU6RWi`

Disclaimer

Lucy Labs, Inc. is a crypto-currency merchant bank, publishing information about markets, industries, sectors and investments in which it believes subscribers may be interested. The information in this article is not intended to be personalized recommendations to buy, hold or sell investments. Lucy Labs, Inc. is not permitted to offer personalized trading or investment advice to subscribers. The information, statements, views and opinions included in this publication are based on sources (both internal and external sources) considered to be reliable, but no representation or warranty, express or implied, is made as to their accuracy, completeness or correctness. Such information, statements, views and opinions are expressed as of the date of publication, are subject to change without further notice and do not constitute a solicitation for the purchase or sale of any investment referenced in the publication. Readers should do their own research before trading in any investments referenced herein. Investing in crypto-currencies is highly speculative and may carry a high degree of risk. Readers may sustain significant losses in these securities.

Advisors to Lucy Labs, Inc. serve as investment advisers to clients, including limited partnerships and other pooled investment vehicles. The affiliates may give advice and take action with respect to their clients that differs from the information, statements, views and opinions included in this publication. Nothing herein or in the subscription agreement shall limit or restrict the right of affiliates of Lucy Labs, Inc. to perform investment management or advisory services for any other persons or entities. Furthermore, nothing herein or in any subsequent agreement between Lucy Labs, Inc. and the readers shall limit or restrict advisors to or affiliates of Lucy Labs, Inc. from buying, selling or trading securities or crypto-currencies for their own accounts or for the accounts of their clients. Advisors to or affiliates of Lucy Labs, Inc. may at any time have, acquire, increase, decrease or dispose of the securities or crypto-currencies referenced in this publication.

Lucy Labs, Inc. shall have no obligation to recommend securities or crypto currency investments in this publication as result of its affiliates' investment activities for their own accounts or for the accounts of their clients.

If you have received this communication in error, please notify us immediately by electronic mail or telephone. This disclaimer applies to all versions of publications for Lucy Labs, Inc.