Quick-Fact Sheet (For Journalists & Investors)   *5/15/2018*

What is Monero?

Monero is private digital currency that is available to all. It allows users to spend safely, knowing others cannot see their balances or track their activity. With Monero, individuals can be their own bank. Some principles of Monero include:

Decentralization. As an open-source project led by a decentralized team of developers and community members, it cannot be censored. Most contributors are volunteers and the community is spread all over the globe.	**Scalability.** Monero's dynamic block size limit that changes based on transaction volume, provides lower fees and faster transactions. Higher transaction volume leads to larger block size limit, whereas, low transaction volume leads to a smaller block size limit.
Security. As a decentralized cryptocurrency, Monero is secured by a large network of users throughout the world. Transactions are confirmed by distributed consensus and then immutably recorded on the blockchain.	**Un-censorable.** Transactions on the Monero blockchain do not reveal a particular user or real-world identity. As a result, users are free from censorship or capital controls.
Privacy. Monero uses sophisticated cryptography through ring signatures, ring confidential transactions, and stealth addresses to obfuscate the origins, amounts, and destinations of all transactions.	**Fungibility.** Monero is fungible because it is private by default. This means that one Monero will always be equal to another. Units of Monero cannot be discriminated by vendors or exchanges due to the origin or history of your coins.

Basic Coin Info

Approximate # of Monero in circulation: **16,030,365 XMR**

Coin emission info:

- Current Block reward: **4.65 XMR**
- Reward rate will steadily decrease until the end of May 2022, when there are 18.132 million XMR in circulation, at which point a 0.6 XMR block reward will remain indefinitely
- With "tail emission" of 0.6 XMR/block, by 2040 there will be an equal amount of Monero as Bitcoin (roughly 21 million) (See "Differentiating Facts" below to learn why this is important)

Market cap: **$3,446,681,803**

Monero Market cap % of total: **0.85%**

Basic Network Info

Amount of Active Nodes: **2,022** *(Source: https://monerohash.com/nodes-distribution.html)*
Network hash rate: **433.2 MH/s**
30-day-average transactions/hour: **255**
CPU cores securing the network: **14,440,024**

History of Monero

Monero was launched in April 2014. It was a fair, pre-announced launch of the CryptoNote reference code. There was no pre-mine or "insta"-mine, and no portion of the block reward goes to development. See the original Bitcointalk thread here. Shortly after the founder proposed some controversial changes the community disagreed with. A fallout ensued, and the Monero Core Team forked the project with the community following this new Core Team. This Core Team has provided oversight since.

Monero has made several large improvements since launch. The blockchain was migrated to a different database structure to provide greater efficiency and flexibility, minimum ring signature sizes were set so that all transactions were private by mandate, and RingCT was implemented to hide the transaction amounts. Nearly all improvements have provided advances to security or privacy, or they have facilitated use. Monero continues to develop with goals of privacy and security first, ease of use and efficiency second.

What does 'Monero' mean?

The word Monero is from the Esperanto language. The creators chose to use Esperanto because it is a 'decentralized' language and represents the breaking of barriers between people, on a global scale.

In Esperanto, Monero is a word composed of three elements freely put together, one syllabus each: mon + er + o. Each has a meaning.
mon- : money
-er- : the smallest part
-o : a thing (grammatically speaking : a noun)

Which means 'monero' can be analyzed as meaning: "a noun that describes the smallest part of money". Or, **a coin**.

Key Differentiating Factors

What differentiates Monero from other currencies like Bitcoin or fiat?

- **Monero uses the CryptoNote codebase.** This is fundamentally different from codebases used by bitcoin or ethereum and the many other cryptocurrencies that are derived from each. It is known for its considerable privacy improvements.
- **Privacy is mandatory; transparency is opt-in.** Monero's state-of-the-art cryptography obfuscates every layer of a transaction; information of the sender, receiver, or the transaction itself. That said, if a user prefers transparency, they may opt-in by creating and sharing a view-only wallet that reveals inputs.
- **Routine network upgrades.** The community of Monero developers regularly perform network upgrades (hard-forks) to ensure that all users can take advantage of the best available security, privacy, and features. This allows the Monero network to remain more nimble and secure by adapting to any opportunities or threats that arise. What's with all the hard forks I'm reading about?
- **Monero block reward trajectory**. Rewards will gradually drop until tail emission commences at the end of May 2022. At this point, rewards will be fixed at 0.6 XMR per block. Tail emission will provide for continued and indefinite mining incentive. Additionally, and perhaps more importantly, tail emission will provide Monero with a built-in, stable, and predictable inflation. If any cryptocurrency were to replace fiat, this would be an essential component.
- **Monero Research Lab.** Monero is not only committed to making a fungible currency, but also to continuing research into the realm of financial privacy as it involves cryptocurrencies in general. To that end, Monero has five published white papers and have many more research goals they are working toward.

Features Coming Soon

Although Monero is already available and being used across the globe, the community of developers have exciting goals to continue enhancing the privacy, security, and usability features of Monero. These are a few that are coming soon:

Bulletproofs. This development will slow the blockchain growth rate and allow for speedier transaction verification. Ultimately, this will make for a more efficient blockchain, lower fees, and better user experience.

Kovri. This is a major privacy upgrade, adding a fourth layer of privacy to Monero transactions. Kovri uses garlic-encryption (think of Tor on steroids) to mask the IP addresses of senders and receivers using the Monero network. Every layer of a Monero transaction, from the sender, receiver, transaction amount, and (with Kovri) the backbone of the transaction itself, will all be private and secured with state-of-the-art encryption.

Hardware Wallets. The popular Ledger hardware wallet is in the final stages of adding Monero. Additionally, the Monero community is funding the work of a team that is building a hardware wallet built on the Monero ethos. Both of these hardware wallet options are anticipated to be operational by the end of 2018 at the very latest.

Long Term Design Goals

The core community of developers have many long-term goals to continually refine and enhance Monero features. A comprehensive list can be found here, but a list of the more noteworthy goals are below:

- Improvements for wallet functionality and business/merchant use
- **Tippero** for ultra-lightweight side-chain micro transactions
- **MoneroID** for private/optionally public online identity management
- **MoneroTrust** to create a web of trust for interaction between multiple entities
- **MoneroChat** to store and forward encrypted messages, as well as payment requests
- **MoneroAssets** for cross-chain trading and assets markets on sidechains
- **MoneroTrade** for decentralized ecommerce with products and services

Additional Resources

getmonero.org (Official Website)
monero.how
reddit.com/r/monero
Guide to Monero (post)
Monero In-Depth Technical Intro

Scams to Avoid
Monero FAQ
Monero SWOT Analysis
Connect w/ Monero Community