



MONERO

Monero is a secure, private, untraceable digital currency that is available to all. Its features make it fungible cash.

QUICK FACTS

Users can spend safely, no one can see their balances or track their activity unless the user gives them permission.



DECENTRALIZATION

As an open-source project led and funded 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.

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.

SCALABILITY

Unlike Bitcoin and other projects that often rely on hardcoded constants, Monero's dynamic block size adapts automatically to the volume of transactions, providing lower fees and faster confirmations.



Core Principles

Monero uses sophisticated cryptography through ring signatures, ring confidential transactions, and stealth addresses to obfuscate the origins, amounts, and destinations of all transactions. Users can decide exactly how much information they reveal and to whom.

PRIVACY

Due to Monero's privacy characteristics, no specific address or user wallet can be blacklisted by miners or by any economic actors. As a result, users are free from censorship and capital controls.

CENSORSHIP RESISTANCE

Monero is fungible because it is private by default. There is no visible history attached to each particular coin. It means users and businesses do not need to worry about being accused of accepting tainted money, and that one Monero will always be equal to another.

FUNGIBILITY

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](#).

Monero has made several large improvements since launch. 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

- **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 is private for every layer of a transaction: information of the sender, receiver, or the transaction itself. A user has the option to create and share a view-only wallet that reveals inputs or use view-keys to reveal specific transactions.
- **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, when 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 gives Monero a built-in, stable, and predictable inflation - considered essential for real, sound money.
- **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, academic researchers in fields of mathematics, physics, security, and blockchain computation have published [research papers](#) and have many more [goals](#) they are working toward.
- **Mining is accessible:** Anyone with a connected device or web browser can participate.

REAL-WORLD IMPLICATIONS & USES

Because Monero is secure, low-fee, and borderless, people can easily send money despite corrupt and broken governments or banks and business can be conducted without competitors snooping in critical information. This provides economic empowerment of individuals and businesses in oppressive countries, depressed economies, or highly competitive business environments.

Private financial history protects consumers and companies from price manipulation, supply chain exploitation, economic discrimination, or the like. Monero is the only cryptocurrency that has the features to serve as completely fungible, decentralized, electronic cash.

TECHNICAL FUNDAMENTALS

(As of 2/1/2019)

Amount of Active Nodes: 1,564 (Source: <https://monerohash.com/nodes-distribution.html>)
Network Hash Rate: 663.2 MH/s
Average Transactions/Hour: 149 (30-day average)
CPU Cores Securing the Network: 22,234,297
Monero in Circulation: 16,758,217 XMR (Approximate)
Market Capitalization: \$732,932,071 USD (~0.65% of total cryptocurrency market cap)
Current Block Reward: 3.22 XMR
Average Block Interval: 2 Minutes

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)

FEATURES IN DEVELOPMENT

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 and cryptocurrency in general. These are a few that are coming soon:

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 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 secure.

Hardware Wallets: The popular Ledger and Trezor hardware wallets are working on adding Monero. (Ledger is supported since CLI 0.12.2 and GUI 0.12.3) The Monero community is funding a team that is building a hardware wallet built on the Monero ethos. Both Ledger and Trezor hardware wallet options were anticipated to be operational by the end of 2018.

Kasisto: This point-of-sale solution is designed to facilitate easy sales for merchants and businesses.

ADDITIONAL RESOURCES

getmonero.org (Official Website)

monero.how

reddit.com/r/monero

Guide to Monero (post)

Monero In-Depth Technical Intro

Zero to Monero

Scams to Avoid

Monero FAQ

Connect w/ Monero Community

Mastering Monero - (coming soon)

Satis Group Report



Monero Quick Facts - Revised 2/1/2019
Created for the community by Monero Outreach.

Monero Outreach is dedicated to growing adoption and acceptance
through education and public relations. Your donations make it possible.

47oKHkoaQdBdFpTJNKaetUS6UsCGHVbJbGxPGaaHFQPqXSCLbqXYsBo6x7abwtfdXTeiBhtZLnYF5bRRAhYsUVb5Sd1aqiD