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.

Revised 06/04/2024
Created for the community by Monero Outreach

getmonero.org

Core Principles

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.

PRIVACY

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.

CENSORSHIP RESISTANCE

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***.

FUNGIBILITY

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.

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, with many of them tracked in a timeline here. Nearly all improvements have provided advances to security or privacy, or they have facilitated use. Monero continues to develop with goals

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.

- **Monero Block Reward:** Monero has taken a different approach to Bitcoin regarding the block reward. Rather than limit the supply to 21 million coins, Monero uses a perpetual block reward of 0.6 XMR per 2-minute block. This allows Monero to utilize an adaptive block size, that can grow (and shrink) based on demand. This contrasts with Bitcoin's fixed block size. Note that up until 2040, there will be less XMR in circulation than BTC.

- **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. Monero Research Lab (MRL) is a group of academic researchers in fields of mathematics, physics, security, and blockchain computation who research solutions for Monero and publish academic papers with their findings.

- **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 06/04/2024)

Amount Of Active Nodes: 3,196 (Source: https://monerohash.com/nodes-distribution.html)
Network Hash Rate: 2 GH/s
Average Transactions/Day: 33,000 (30-day average)
Monero In Circulation: 18,445,551 XMR (Approximate)
Market Capitalization: $2,927,951,481 USD
Current Block Reward: 0.6 XMR
Average Block Interval: 2 Minutes

With the "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 in progress:

Full Chain Membership Proofs (FCMPs): Currently, Monero uses a technology called Ring Signatures to protect the privacy of a sender. It combines the signature of the real output with 15 decoys, to create an anonymity set size of 16. FCMPs will increase the anonymity set from 16 to every output in the blockchain. This would improve on one of the weaker aspects of Monero's privacy.

Seraphis: Seraphis is a fourth-generation privacy-focused transaction protocol abstraction for Monero, offering simpler multisig support, flexible multi-tier address schemes, and efficient key image construction for better performance and modularity, though it requires users to transition from CryptoNote-style addresses.

Cuprate: This alternative Monero node, being developed in Rust, will enhance network security and redundancy by independently validating consensus rules and significantly reducing the risk of implementation and memory safety bugs. A beneficial side effect of its creation, to date, been a small number of fixes to both the existing node implementation.

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
Satis Group Report

Monero Quick Facts - Revised 06/04/2024
Created for the community by Monero Outreach.