

Quick Fact Sheet

What is Masari?

Masari (MSR) is a scalability-focused, untraceable, secure, and fungible cryptocurrency using the [Ring Confidential Transactions Protocol](#). It is [open source](#) and freely available to all. Masari is a truly private digital currency that aims at being simple, scalable, and secure.

Simple

Mobile wallet

Masari's [mobile wallet](#) makes everyday transactions a snap. It connects directly to the blockchain and does not collect any information from the user. It will be pushed to the Google Play Store as well as the Apple App Store.

Simple Web Wallet

The [Simple Web Wallet](#) is a first for the CryptoNote world as it is the first web wallet to connect directly to the blockchain. In doing so, the user maintains complete security and privacy as no user information can be collected. The Simple Web Wallet is also very easy to use and operates much like a Graphical User Interface wallet.

Graphical User Interface Wallet

The [GUI wallet](#) was forked from Monero and is available in many different languages. Sending Masari is as simple as clicking a few boxes.

Simple Miner

The [Simple Miner](#) was originally developed to deal with mining centralization problems as it allows for everyday users to experience mining for cryptocurrencies on whatever gadget they own. In just a few clicks, users are able to generate new Masari as well as ensure network stability.

Ledger Support

The lead developer, Thaer, has also stated the goal of [Ledger](#) integration in the near future.

Scalable

Blocktree Sharding

The Blocktree Protocol will be the crowning achievement of the MSR developers, allowing the blockchain to securely shard/partition the blockchain into parallel and synchronized chains within a blocktree. This will allow for theoretically unbound dynamic TPS scale as the blocktree can resize on demand. This is a novel idea that's being investigated in depth by the Masari Project, and a whitepaper (WP) is being worked on to prove out this protocol. Discussion about this protocol can be heard at a [Hash It Out podcast](#) with Thaer Khawaja from Masari, and such an idea has been floated before by [Howard Chu from Monero](#). Once the white paper is complete, Masari intends to execute development of it.

Courtesy of [ThaerK](#), [BazookaJeff](#), [TheDawson](#), and [LodoCrypto](#). 2018.

Uncle Mining

Uncle Mining is a cryptonote first that rewards miners for work done on abandoned blocks that were not the first to be written to the blockchain. This adds more hashpower (mining power) and 'weight' to the network, making it more secure. This subsequently allows us to significantly speed up our block emission rate for faster confirmations, while further securing the network. Code for this is [nearing completion](#) and is being staged for testnet.

Secure

Stable

Masari is especially secure against mining attacks as it necessarily needed to mitigate these adversarial attacks since its early inception. It developed a unique [Weighted-weighted Harmonic Mean \(WWHM\)](#) algorithm that paved the way for a [Linearly Weighted Moving Average \(LWMA\)](#) algorithm. In both scenarios, Masari was first to deploy such algorithms into mainnet, with LWMA being a [huge success](#) as modifications were made to securely permit asymmetric adjustments, effectively allowing the network to quickly adjust to changes in the market.

Fungible

Masari is Fungible because it is private by default. Each Masari coin is interchangeable with every other coin no matter what it was spent on. This being the case, you can never be discriminated on for what you spend your Masari on or where you spend it.

Censorship resistant

Since Masari is private and decentralized, it is free from censorship as nobody will know that you have Masari or that you are spending it. Masari is digital cash, that is, when you spend it, it is just like giving another person physical cash. This means that the transaction is only linkable if you choose for it to be.

Private

In total, Masari aims at furthering privacy while advancing its own protocol. Whatever Masari develops will be free for public scrutiny as it is open source therefore open to the public for review. In doing so, Masari will push code upstream to Monero as well as make our new privacy features available to the public. In addition, every transaction in the Masari blockchain from the genesis block to now has used the same ring size. Masari coins are fungible, meaning every coin is interchangeable and indistinguishable from one another. All transaction and address data is hidden using RingCT and Cryptonote protocol. There is no rich list, there is no public record and you are totally anonymous in every way.

Courtesy of [ThaerK](#), [BazookaJeff](#), [TheDawson](#), and [LodoCrypto](#). 2018.

Specifications

- PoW algorithm: CryptoNight-Fast
- Max supply: ~18.5 million (with tail emission)
- Block reward: Smoothly varying recurrence relation starting at around 35 MSR per block, $\text{block_reward}(\text{block_height}) = (2^{64} - 1 - \text{total_supply}(\text{block_height} - 1)) * 2^{-19} * 10^{-12}$
- Block time: 120 seconds
- Difficulty: Re-targets at every block using the LWMA adjustment algorithm
- Genesis block: Saturday, 2 September 2017 21:20:46 UTC

The Masari Difference

Masari Research Corner

Masari is focused on furthering privacy to the CryptoNote protocol. This being the case, Masari has launched the Masari Research Corner to further privacy in the cryptospace.



Active Development

Masari is actively developed by 3 core members: Thaer, Cryptochangements, and Gnock. Together they work to maintain the network by adding any necessary upgrades if any threats arise. In addition, two other core members, LodoCrypto and BazookaJeff spearhead marketing and communication efforts.

Development Milestones Already Achieved

1. CryptoNight-Fast is a new algorithm created by the Masari team
2. Weighted-Weighted Harmonic Mean difficulty adjustment algorithm making Masari ASIC resistant and more resilient against mining attacks like flash mining
3. Both algorithms have been adopted by several small Cryptonote coins. Masari is a leader, not a follower in this space.
4. The DAA has been submitted to Monero to be adopted pending review
Client-side web wallet
5. Android mobile wallet (IOS coming soon)
6. GUI and CLI desktop wallets for Windows and Mac, CLI desktop wallet for Linux

Courtesy of [ThaerK](#), [BazookaJeff](#), [TheDawson](#), and [LodoCrypto](#). 2018.

Fair Distribution

1. No ICO
2. 0.5% premine set aside for development
3. There are no masternodes or other incentives to concentrate the supply among a small number of people
4. Strong Development: Masari is developed by one full-time core member, Thaer Khawaja, and two part-timer developers, Gnock and Cryptochangements

How Will People Use Masari?

Remittances

Uses of Masari could include [remittances](#) and tipping as the Masari network is global and is not bound by a single government or entity.

Store of Wealth

Because Masari is fungible it can be used as a currency and as a store of wealth as your money is free from malevolent agents.

General Payments

Masari is just like cash. This being the case, users can just use Masari if they do not want to accept cash or have their operations solely online and simply cannot accept cash.

Where to Find out More

[GetMasari.org](https://getmasari.org)

[BitcoinTalk](#)

[r/masari](https://r.masari)

medium/@officialmasari

[Twitter @masaricurrency](#)

[Discord](#)

[Telegram](#)

[Forum](#)

Courtesy of [ThaerK](#), [BazookaJeff](#), [TheDawson](#), and [LodoCrypto](#). 2018.