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

Masari aims at being simple enough for daily use. There are a few different wallets that allow for use on Android, Windows, and MacOS. There is also a simple miner that allows for users to easily mine Masari.

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.

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 idea has been floated before by Monero community members, and Masari intends to prove out the protocol in a whitepaper and 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

Masari is especially secure against mining attacks since it uses a unique LWMA algorithm that automatically adjusts if there is an attack on the blockchain. Furthermore, since Masari is decentralized on a global scale, transactions are confirmed on a wide consensus which allows for the blockchain to remain immutable.

Fungible

Masari is Fungible because it is private be 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 ringsize. Masari coins are fungible, meaning every coin is interchangable 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.

Stable

Masari uses a unique algorithim to help keep the network secure from mining attacks. Masari has also contributed by securely allowing asymettric bounds in difficulty adjustments

---

History of Masari

Masari was released on September 07, 2017. Masari was announced on BitcoinTalk.org with the stated goal of experimenting novel concepts to Monero's code base while also contributing back upstream to the parent project. Masari was launched with slight changes that removed Monero's legacy protocols, enforced a static mixin of 12, randomized transaction fee sources, and fluffy blocks were being enabled by default. Later, Masari impleted the Weighted Harmonic Mean WHM algorithm. Soon after, Masari ported Moneros GUI Wallet, merged the laterst changes from Monero's v0.12.0 such as subaddresses, multisig, and a PoW

change. Masari found the PoW change to be problemetatic for mining and created its own unique algorithim CryptoNight-Fast. Masari will soon add a uncle mining and blocktree sharding which should allow for a more stable network and a higher number of transactions. The lead developer, Thaer, has also stated the goal of Ledger integration in the near future.

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, block_reward(block_height) = (264 - 1 - total_supply(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 lauched 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 Distrubution

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 soley online and simply cannot accept cash.

Where to Find out More

GetMasari.org

BitcoinTalk

r/masari

medium/@officialmasari

Twitter @masaricurrency

Discord

Telegram

Forum

Courtesy of ThaerK, BazookaJeff, TheDawson, and LodoCrypto. 2018.