XMRGO: A Privacy Focused Platform For Contractual Money

Alyosha Fedorov
alyosha.fedorov@protonmail.com
Rev. 0

Abstract

XMRGO is the combination of Ergo and Monero. A privacy-oriented currency and smart contract platform. Taking the best of both worlds to create a new form of private smart money. The combination comes from the smart contract capabilities of Ergo and the privacy of Monero. Monero is a private and fungible currency. Ergo is the next generation smart contract platform. The goal of XMRGO is to create a completely anonymous, unlinkable, and untraceable smart contract platform.

Why Ergo and Monero?

Ergo is the top-of-the-line smart contract platform for PoW. Monero is the top-of-the-line privacy coin for PoW. Combing their powers together will create the most private and technologically advance smart contract and currency blockchain. This is no easy feat but it must be done to ensure that the future of blockchain technology will not be ruined.

Privacy-based Finance

This coin is not meant to be sold on centralized exchanges, CEX, where the know-your-customer, KYC, is dominant and well-practiced. The XER coin should only be obtainable via decentralized exchanges, peer-to-peer trading, and mining rewards. It is a coin for those to have the option out of the standard practices of cryptocurrencies, ruining privacy for maximizing profits, e.g. informing CEX to require view keys like in Monero. This is a coin for true privacy while allowing smart contracts to exist for complex financial transactions. The project will always remain open-source. It is built by developers working towards the dream of financial freedom and untraceable smart money.

XMRGO Protocol

The Xmrgo protocol is a combination of Ergo and Monero. It blends the vision of Ergo and Monero into a single entity for a singular purpose. It is designed

to be a privacy-based decentralized finance platform.

Key Features

- Smart Contracts Using Σ-protocols
- Modified Ergo + Monero Emission Rate
- RandomX Consensus Protocol
- Monero transaction security

The XMRGO Vision

Xmrgo is very private and can only be changed in the future by the community. There exist many principles that should be followed in Xmrgo. In case of intentional violation of any of these principles, the resulting protocol should not be called XMRGO.

Decentralization First

Xmrgo should be as decentralized as possible: any parties whose absence or malicious behavior may affect the security of the network should be avoided at all cost.

Created for Private People

Xmrgo is a platform for private people, and their interests should not be infringed upon in favor of big parties.

A Platform for Contractual Private Money

Xmrgo is the base layer to applications that will be built on top of it. Its main focus is to provide an efficient, secure, and easy way to implement private financial contracts.

Long-term Focus

All aspects of Xmrgo development should be focused on a long-term perspective.

Permissionless and Open

Xmrgo protocol does not restrict or limit any categories of usage.

RandomX Consensus

Xmrgo utilizes the Proof of Work (PoW) consensus protocol called RandomX.

Untraceability and Unlinkability of Transactions

All possible senders are equiprobable and it should be impossible to prove that any transaction was sent to the same person.

Implementation

At the core, XMRGO is just Ergo with a different PoW consensus protocol, emission schedule, and default privacy features. It utilizes the Σ-protocols to create Monero-style transactions for complete anonymity, untraceability, and unlinkability. The resulting blockchain should have the smart contract capabilities of Ergo with the privacy of Monero.

This is great news for building this new blockchain. The required pieces already exist. All that must be done is putting the pieces together in the correct combination such that the dream of a completely private and untraceable smart contract platform will come to fruition.

Parameters

Block Reward	1 XER + Fees per Block
Max Supply	∞
Fee	0.001 XER per kB
Block Time	2 Minutes per Block
Consensus Algorithm	RandomX
Language	ErgoScript
Block Size	Arbitrary
eUTXO Tax	4 years

Unlike Ergo, there will not be a treasury for dApp development. All fees will go directly to the miners from the first block until infinity.

XMRGO believes privacy-based decentralized finance is the future of money.