

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. Combining their powers together will create the most private and technologically advanced 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.

This should be on its own page.