Braid - Bitcoin and Ergo Double Merge-Mined Sidechain with focus on Stablecoins, RWAs, Bitcoin DeFi

kushti
kushti@protonmail.ch

No Institute Given

Abstract.

1 Introduction

While disconnected from reality financial games, such as memecoins, still present, we clearly see solid emergent trends around utilizing blockchain-based assets for the needs of the real world:

* the most known blockchain-based asset, Bitcoin, is going into different corporate and national reserves. However, there Bitcoin becomes just another assets on the sheet for traditional financial schemes. There are attempts to build decentralized financial (DeFi) tooling on Bitcoin, and it was one of the biggest trends of 2024. There are two main directions in building DeFi on Bitcoin: somewhat L2 with EVM , or dedicated UTXO chain (Ergo, Nervos, Cardano) as execution environment for Bitcoin UTXOs progression, with Bitcoin UTXO set state delivered via trustless relays or trustless bridges, such as BitVM-based.

* there is big trend around stablecoins. Many private enterprises, following Tether's success, and nation states starting to issue own stablecoins, there are many efforts on making stablecoin payments seamless, reduce fees to almost zero. There are even buzzy at the moment announcements of stablecoin oriented blockchains, such as Plasma.

We propose Braid, a blockchain which is oriented towards

We propose to build Braid, a double merged-mined sidechain of both Bitcoin and Ergo, using Sigma, Ergo's contractual layer, along with modifications perfectly suitable for stablecoins and other real world assets. This would allow to have:

- Proof-of-Work security from the biggest world's computing network (Bitcoin mining)
- Fees payable in any asset (you can even send gold-pegged tokens and pay in USD token, if there is option to swap USD for native token)
- Ready-made liqudity solutions since day one (!), such as bridges with Bitcoin, Ethereum, Binance Smartchain, Cardano
- Two-way trustless pegging with Ergo blockchain since day one

- Trustless (BitVM based, later BIP300/301 based maybe) bridge with Bitcoin
- Ready-made applications, such as AMM DEXes, orderbook DEXes, decentralized auctions, bonds, lending pools etc
- Regulatory sandboxing and compliance granularity, for example, to isolate jurisdiction-specific stablecoins, or shape real world assets usage with tailored compliance
- Compliance granularity may be combined with privacy
- Innovative algorithmic stablecoin designs, and insurance contracts, where algorithmic assets can insure non-delivery risks for tokenized real-world assets
- High performance: PoW secured blocks every few seconds

2 Design

3 Technical Details

4 Implementation

References