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.

While real-world adoption via different developments following the trends is highly positive, and moving forward a financial revolution we dreamed of, the state of developments is [...]

To tackle with the issues stated, we propose Braid, a blockchain which is oriented towards [...]

Braid is 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
- RGB-like programmability on top of Bitcoin blockchain metadata
- 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 Competition

There are some attempts to build stablecoin and RWA focused blockchains, such as Tron and Plasma. However, usually they are just EVM chains with some features, like gasless transfers, implemented. Also, there are some attempts to build

Here we propose a comprehensive set of solutions to Bitcoin DeFi, stablecoins, RWAs, compliance granularity, precisely defined monetary circuits and so on.

Braid is offering multi-layered set of solution for both Bitcoin DeFi and stablecoins and RWA. Unmatched support for money programmability allows stablecoin and RWA issuers to define rules of usage precisely. Trustless BTC pegging along with RGB like programmability allows for different kind of DeFi tooling for Bitcoin, including issuing trustless Bitcoin-backed derivatives.

4 Team

We have team of people participated in creation of such blockchains and blockchain projects as NXT (top3 CMC back then), Chainlink (top 20), Cardano (top 10), Waves (top 20 back then), Ergo (top 100 in 2021), and so on.

5 Tokenomics and Liquidity

kushti notes : to be decided later

6 Technical Details

6.1 Consensus Layer

We have two kinds of blocks, Bitcoin-merged and Ergo-merged.

For Bitcoin-merged, header contains Bitcoin header plus digest of AVL+ tree committing to the FULL Bitcoin UTXO set (including OP_RETURN UTXOS) (at what time?), and reference to last seen Ergo-merged block. Difficulty for Bitcoin header is set to normal Bitcoin block difficulty, so only Bitcoin full block accounted for in Braid (not a mining share with lower difficulty like in). Proof of inclusion of Braid data into Bitcoin block is submitted by Bitcoin miner along with the header to Braid network.

For Ergo-merged, header contains Ergo header, reference to last-seen Bitcoin-merged block. Difficulty for Ergo header is set to input-block difficulty, so every input-block is accounted for in Braid.

6.2 Transactional Layer

Bitcoin Script was initial experiment in programmable money, which, unfortunately, got stuck too early. Ethereum started from disagreement within Bitcoin community but followed completely different paradigm of "smart" contracts, which is not quite feasible for building monetary circuits. Ergo launch in 2019 marked revival and start of new epoch in programmable power, with the same UTXO approach as in Bitcoin, but much more powerful programmability, and support for some cryptographic protocols as applications (see "ErgoScript, a Cryptocurrency Scripting Language Supporting Noninteractive Zero-Knowledge Proofs" whitepepaer).

In short, contractually-wise, Ergo is about:

* UTXO model. A transaction has potentially many inputs and outputs. We unify those entities in Ergo, so say that a transaction is creating some boxes and eliminates some boxes. A current state of the network then is a set of active boxes then. * Registers: each box is made of registers (and registers only), where a register contains a typed value. There are registers with predefined values, such as locking script, monetary value, natively supported tokens, reference to transaction where the box was created. In addition to four predefined registers, there could be up to six registers with arbitrary values.

Global Transfer Policies In Braid, we want to augment Ergo contractual capabilities with Global Transfer Policies, set of contracts and limitation for a box, which may be propagated via transactions.

A Global Transfer Policy is set in a box, which needs to have a special NFT for identification. A policy box has locking script, like every box, which is allowing to change policies as well as locking script itself. A policy box should also have following registers:

- R4 - spending policy - any computation (getting the same context avaiable to a locking script, aside of mining pubkey and votes). Should return true or false. If true, the box may be spent, otherwise, not.
- R5 - propagation policy - also computation - returns number of inputs which should have the same policy

Then we add another special register in Braid, and this register may contain multiple NFT ids. Boxes with such NFTs must be provided as read-only inputs of a transaction. An input can be spent if for all of its policies spending and propagation sub-policies satisfied.

Global Transfer Policies may have multiple use cases:

- a stablecoin issuer may use them to have black list or even white list. White list can be anonymized, by having stealth address like hiding in the white list
- there could be very flexible policies
- they can be used to build different forms of Islamic Finance systems etc

RGB++

Ergo Applications kushti notes : put a list

7 Implementation

References