Braid - Bitcoin and Ergo Double Merge-Mined Sidechain with focus on Stablecoins, Real-World Assets, Bitcoin DeFi

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 asset 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 now: somewhat L2 with EVM, or external dedicated UTXO chain (Ergo, Nervos, Cardano) as execution environment for Bitcoin UTXOs progression, with bitcoins transferred via trustless relays or trustless bridges, such as BitVM-based.
- there is big trend around stablecoins. Many private enterprises, following Tether's success, as well as nation states are starting to issue own stablecoins, there are many efforts on making stablecoin payments seamless, reduce fees to almost zero, and so on. There are even buzzy at the moment announcements of stablecoin oriented blockchains, such as Plasma.

While real-world adoption via different developments following the stated trends is highly positive, and it is still moving, slowly but surely, the world towards a financial revolution we dreamed of, the state of developments still can be significantly improved by providing better basis for trust-minimized Bitcoin DeFi as well as programmable money toolset for stablecoin and real-world assets issuers and users. For that, we propose Braid, a blockchain which is oriented towards needs of stablecoins and real-world assets issuers and users, while also allows for using Bitcoin for collateral in decentralized finance with minimal trust assumptions, and having Proof-of-Work security for every block. 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 available)
- 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 (BitVM2 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

In short, Braid is a solarpunk made to extreme: you can define precise usage rules for your token, to make it conform with any views of yours, and have any degree of control. However, other parties may do the same on the same chain. Different monetary circuits could be totally isolated. However, you can dictate in your own circuit only, others are not under your control.

For such setting, minimal trust assumptions are needed. That is why we have chosen double merged mined Bitcoin and Ergo sidechain, which is allowing to have Proof-of-Work security for every block, along with fast blocks.

The rest of the whitepaper is organized as follows. In Section 2 we provide high-level overview of Braid design. Section 3 is comparing Braid with other known players in the same field. In Section 4 we present a team which is working on Braid. In Section 5 we provide planned tokenomics. Section 6 provides some technical details for Braid design outlined in Section 2.

2 Design

Here we are going to provide high-level overview of Braid design. Technical details can be found in Section 6.

2.1 Consensus

The main motivation for Braid consensus is to have quick blocks along with most secure, simple, efficient consensus, so Proof-of-Work. Following ideas from such designs as Prism, TailStorm, Leios and sub-blocks in Ergo, we have ordering and input blocks here. Ordering blocks are committed on the Bitcoin blockchain using merge-mined sidechain standards [1]. Input blocks are committed on Ergo blockhain's input-blocks, to have blocks every few seconds. An ordering blocks is just witnessing a best input-blocks chain seen by its miner. Ordering block is also committing to UTXO set and interlinks vector [2], and, as ordering blocks are committed on the Bitcoin blockchain, that allows for Bitcoin light clients to work with cryptographically secure commitments to Bitcoin UTXO set and headers-chain.

With input blocks in Ergo coming every two seconds, Braid blocks carrying transactions will be generated every two seconds on average as well.

2.2 Programmable Money

Braid is following Ergo approach towards programmable money:

- UTXO model, simple, parallelization friendly, and powerful transactional model coming from Bitcoin
- extended context to make blockchain truly programmable. For Braid it means making both Bitcoin and Ergo blockchains accessible to contracts
- everything-is-a-contract approach, with no need for account abstractions
- natural support for intents (every contract is an intent by default)
- efficient on-chain representation
- support for real privacy-preserving ring and threshold signatures, as well as some more cryptographic applications via Sigma protocols

However, we would like to experiment with some new features as well in Braid, such as Global Transfer Policies, described below.

2.3 Global Transfer Policies

Global transfer policies (GTPs) is efficient mechanism allowing for precise control over transfers for a token, such as:

- rules can be applied to any token transfer. Possible use cases include black and white lists, for both addresses and (or) applications, mandatory payments on certain actions, and so on.
- policies can be propagated, so it is possible to demand other tokens interacting with tokens protected with a GTP to apply GPT after interaction as well. Similarly, for some parties or applications a GPT could be cleared.
- rules for updating GTPs are set separately in a transparent and manageable way. For example, GTPs can be updated by a single party, several parties via a threshold signature, via decentralized autonomous organization (DAO) voting, on schedule, and so on. Update rules can be updateable as well.

2.4 Dark Circuits and Dark Tokens

Among with demand for tailored compliance with precisely defined rules, there is also demand for privacy. It is often desirable to combine transparent and dark (private) circuits also. Braid would allow that by utilizing:

- dark tokens - tokens with hidden via homomorphic commitments amounts, spending would require to provide Bulletproofs++ proofs for validity of newly created outputs. This is done in Monero.
- A global transfer policy may require to use stealth addresses for receivers, as well as other means of privacy (input decoys etc).

So there is possibility to use stealth addresses, or hidden amounts, or both. A token may have requirement to be in a transparent circuit until reaching a gateway after which it can be transferred to more private one, or be swapped to a dark token, and so on.

2.5 Collateralized Algorithmic Stablecoins

Ergo already has variety of proven with time algorithmic crypto-backed stablecoins, such as SigmaUSD (Djed protocol), GluonGold (Gluon protocol), DexyGold (Dexy protocol). They can be reused on Braid, along with other financial primitives useful for stablecoin and RWA issuers, such as ChainCash [3], elastic peer-to-peer stablecoin created collectively via trust and blockchain assets, or a scheme to insure physical asset delivery using algorithmic crypto-backed counterpart [4].

2.6 New Horizons for Stablecoin and RWA Issuers

With all the tooling mentioned above, Braid, with no doubt, is two steps ahead in regards with serving needs of stablecoin and RWAs issuers, in regulatory and other enviroments of any complexity. For example, a stablecoin token maybe issued in one regulatory zone, such as United States, circulate there according to the rules of the US zone, then sent to a gateway allowing to transfer it to MiCA zone (EU) and circulate there according to global transfer policy of the zone, and so one.

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 : Make the section after getting feedback on other matters

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, thus 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 available 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 indices of outputs which should have the same policy

Then there are two ways to add GTPs to Ergo-like blockchains, one would require a hard-fork or a new chain, and another can be implemented in Ergo even:

- 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.
- We designate special context input extension variable id, for example, #120, and a box which is a subject to GTP must have script of the following form ‘blake2b256()getVar[Coll[Byte]](120)) == XXX && other_conditions‘, where XXX is hash of GTPs which should be provided in context extension, concatenated NFT ids. Older, non-GTP supporting clients will just check equality, newer clients will check that boxes with such NFT ids provided as read-only inputs, and check spending and propagations policies written there. For outputs which are subject to GTPs propagation must, again, have script corresponding to the the ‘blake2b256()getVar[Coll[Byte]](120)) == XXX && other_conditions‘ form.

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++ As commitment for Bitcoin UTXO set is available in applications, we can make contracts prescribed by commitments on the Bitcoin blockchain written into OP_RETURN attachments. This is similar to RGB and RGB++ protocols. Here we have minimal trust assumptions for such protocols.

Ergo Applications With possibility to trustlessly bring Bitcoin to Braid and back, all the application from Ergo blockchains can be freely deployed on Braid (as they are open-sourced and under permissive license mostly) without modifications.

kushti notes : add more citations throughout the text

References

1. "Merged mining specification - bitcoin wiki." `https://en.bitcoin.it/wiki/Merged_mining_specification`. Accessed: 2025-07-11.
2. A. Kiayias, A. Miller, and D. Zindros, "Non-interactive proofs of proof-of-work," in *International Conference on Financial Cryptography and Data Security*, pp. 505–522, Springer, 2020.
3. A. Chepurnoy, "Money creation with elastic supply via trust and blockchain assets in global digital peer-to-peer environment," tech. rep., Better Money Labs, 2023.
4. "Physical or digital gold: simple insurance on ergo." `https://www.ergoforum.org/t/physical-or-digital-gold-simple-insurance-on-ergo/4715`. Accessed: 2025-07-11.