ElasticBridge: Trust-less Cross-Chain Bridge for Transferring Rebase Tokens

Timothy Yalugin
timauthx@gmail.com

November 28, 2021

Abstract

This paper proposes an approach for secure and robust bridging of ERC-20 compatible rebase tokens between EVM-based source chain and Substrate-based parachain deployed on Polkadot network.

1 Introduction

Emerging applications of blockchain technology indicate an ongoing trend for market diversification. Once the idea of sovereignty-preserving application-specific chains became feasible, it quickly displace a single *chain-maximalism* dogma. We are now live in a world where *multi-chain* networks like Polkadot [1] and Cosmos [2] are gathering diverse interconnected applications around their relay-chains and hub-chains respectively, creating *the Internet of Blockchains*[1].

Frameworks like Parity's Substrate[2] and Tendermint's Cosmos SDK[3] streamlined the process of building and deploying sovereign and flexible blockchains, allowing them to have different consensus mechanisms, finalities, state models, governance, etc.

1.1 Cross-chain Bridges

Effectively improved on scalability by sharding on-chain data and parallelizing transaction execution, we encountered new challenges with cross-chain interoperability. Many newborn ecosystems, all with unique features and value propositions, found themselves near of Tower of Babel[4] — unable to communicate and effectively cooperate to provide meaningful services together.

The natural reaction was the development of cross-chain bridges — protocols that allow two (or more) exogenous chains to share state by the means of inter-chain transaction passing. We have seen various implementations of these protocols ranging from trusted federations to truly trust-less decentralized Relayed SPV solutions like the IBC Protocol [3].

1.2 Rebase Tokens

Meanwhile, cryptocurrencies — the original use case of the Distributed Ledger Technology (DLT), also do not show any signs of innovation slowdown. Projects like Stellar [4] commit to building a foundation for transferring digital currency to fiat money across borders. Controversial privacy-oriented currencies like Monero [5] allow completely untraceable payments. Finally, fiat-pegged tokens like Tether [6] and multi-collateralized stablecoins like MakerDAO's Dai [7] have been one of many attempts to tackle the price-volatility — issue often synonymous with digital currencies.

Rebasing — a novel technique applied for synthetic commodities for achieving practical price stability by algorithmically adjusting circulating tokens amount, thus translating price-volatility into supply-volatility. Rebase tokens (or price-elastic tokens) demonstrated low correlation not only with stocks, fiat currencies, and precious metals, but with other cryptocurrencies, most notably with Bitcoin.

While the low correlation aspect attracts investors seeking to diversify their portfolios, the unique volatility pattern of rebase currencies makes them valuable building block[5] for DeFi as

[1] Notion proposed by Cosmos developers. https://cosmos.network
[2] The blockchain framework targeting Polkadot multi-chain network. https://substrate.io
[3] Framework of development zone-blockchains for Cosmos network. https://tendermint.com/sdk
[4] Idiom that references mythical narrative when people lose ability to speak same language.
[5] Claim from Ampleforth documentation. https://ampleforth.org/economics

well. For example, the longest-running algorithmic stablecoins based rebasing — Ampleforth [8] constructs its protocol with dependence on fast actors who benefit from short-term trades. By leveraging time windows after rebasing to make lucrative trades, these actors propagate adjustments of supply made by protocol back into the price.

1.3 Considerations taken

Notably, supply expansions and contractions — actions performed by rebase protocol to adjust total supply, affect token amount universally: all wallet balances, treasury, and accounts reserved for smart contracts. Last introduces a significant consideration for cross-chain bridges design since it generally relies on escrow account where dispatched tokens would remain locked on the source chain.

Assuming that bridge protocol will mint wrapped representation of original token on the target chain, we can draw a corresponding conclusion that *without changes to original bridging protocol wrapped token supply will eventually become out of sync with rebase-driven native token supply.* The inconsistency between amounts of native and wrapped tokens would then lead to non-deterministic behavior. Most obvious — *translation conflicts when transferring rebase tokens back to the source chain.* This would also expose both chains to novel attack vectors that would not otherwise be possible.

1.4 Proposal statement

The purpose of this paper is to firstly shed light on the implications that elastic supply of dispatchable tokens would have on cross-chain interoperability protocols applied to them. We will then go through key considerations that should be taken into account while designing a bridge for transferring such tokens. The Paper will center around the protocol proposal for the bridge connecting EVM-compatible source chain and Substrate-based parachain on the Polkadot network. However, the proposed solution should effectively work on chains of other origins as well. Finally, we will finish current paper with follow-up questions and ideas for future exploration.

2 Protocol

References

[1] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework." https://polkadot.network/PolkaDotPaper.pdf, 2016.

[2] E. B. Jae Kwon, "Cosmos: A network of distributed ledgers." https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md, 2016.

[3] C. Goes, "The interblockchain communication protocol: An overview," 2020.

[4] D. Mazi'eres, "The stellar consensus protocol: A federated model for internet-level consensus." https://www.stellar.org/papers/stellar-consensus-protocol, 2016.

[5] N. van Saberhagen, "Monero: Cryptonote v 2.0." https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf, 2013.

[6] "Tether: Fiat currencies on the bitcoin blockchain." https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf, 2016.

[7] MakerDAO, "The maker protocol: Makerdao's multi-collateral dai (mcd) system." https://makerdao.com/en/whitepaper, 2020.

[8] M. R. C. Evan Kuo, Brandon Iles, "Ampleforth: A new synthetic commodity." https://ampltools.com/Media/Ampleforth-whitepaper.pdf, 2019.