Two-Way Pegged Sidechains On Ergo (ErgoHack Report)

kushti, soysor

October 14, 2023

Abstract

In this report we outline some ways to implement pegged sidechains on Ergo with smart contract powered transfers, where both main and side chains are based on UTXOs and support ErgoTree (in its current form, at the same time, sidechain may support more features). In such setting, transfer from sidechain and back can be done via on-chain contract, then security issues are reduced to sidechain consensus issue only.

1 Introduction

A sidechain [1] is a secondary blockchain connected to the main blockchain with a two-way peg. Pegged sidechains enable ERG (native cryptocurrency of the Ergo blockchain) and other Ergo blockchain assets to be transferred between multiple Ergo-like blockchains. Sidechains can be considered as playgrounds for experimental features, or scalability solution (for example, a sidechain may support shielded transactions or other privacy-preserving techniques), allowing to off-load transaction from the main chain to sidechains.

1.1 Ergo blockchain details

We provide relevant Ergo blockchain needed here.

2 Sidechain Data on the Mainnet

In this section we consider how sidechain data can be stored on the main-chain.

A sidechain progress can be represented in the simplest form as a tuple (h, T_h, U_h, C_h), where h is a sidechain height, T_h are state changes (transactions) done in h, U_h is digest of AVL+ tree built on top of UTXO set after processing the changes T_h, C_h is AVL+ tree which contains all the previous sidechain states in form of key-value pairs $h- > hash(h||T_h||U_{h-1})$.

First of all, we need to write this minimal data somewhere, to read in contracts later. Currently, we can think about two options:

- there's extension section of a block, which contains key -> value pairs, and root of a Merkle tree built upon the pairs is included into a block header (and can be read by a contract). We can include different sidechains here, or even a tree built on top of sidechains. The only issue with this approach is that Merkle trees are not supported in ErgoTree/Script yet
- we can just put sidechain data into a box identified by some NFT

2.1 Sidechain Consensus

There could be different option how sidechain can make a progress

- merged mining - PoW fields (nonce, solution) to be added to the tuple, and writted on the Ergo blockchain. Then sidechain header would be Ergo block header + extension Merkle path or path to box in UTXO set tree + sidechain tuple with PoW data. Security: subset of Ergo miners (so honest majority amongst them)
- if sidechain data is in a box, we can make the box spendable for an Ergo block miner (by using miner pubkey from context like done in emission contract). Security: subset of Ergo miners (so honest majority amongst them). There could be other options here (multisig etc)

3 Transfers

3.1 Mainchain to Sidechain

3.2 Sidechain to Mainchain

4 Security

5 Evaluation

6 Further Work

References

[1] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling blockchain innovations with pegged sidechains," *URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, vol. 72, pp. 201–224, 2014.