
eth-merkle-bridge

Release 0.1.0

Oct 28, 2019

Contents:

1	Merkle bridge design.	3
1.1	Getting started	3
1.1.1	Download	3
1.1.2	Install	3
1.2	Using the EthAergo CLI	4
1.2.1	CLI for the proposer/validator	4
1.2.2	CLI for asset transfers	7
1.3	Proposer	10
1.3.1	Starting a Proposer	10
1.3.2	Updating bridge settings	12
1.4	Validator	12
1.4.1	Starting a Validator	12
1.4.2	Updating bridge settings	13
1.5	Deploying a new bridge	14
1.6	Configuration file	17
1.7	bridge_operator	19
1.8	ethaergo_wallet	22
1.9	ethaergo_cli	26
2	Indices and tables	29
	Python Module Index	31
	Index	33

The EthAergo bridge is an efficient and decentralized way of connecting blockchains. The repository is the POC implementation of Aergo's bridge design between Aergo and Ethereum networks.

CHAPTER 1

Merkle bridge design.

In order to transfer an asset from one blockchain to another blockchain, it should be locked on its origin chain and minted on the destination chain. At all times the minted assets should be pegged to the locked assets.

The EthAergo Merkle Bridge enables decentralized custody and efficient minting of assets.

At regular intervals, a proposer publishes the state root of the bridge contract on the bridged chain. The state root is recorded only if it has been signed by 2/3 of validators. Users can then independently mint assets on the destination bridge contract by verifying a merkle proof of their locked assets with the anchored state root.

The proposers do not need to watch and validate user transfers: the benefit of the merkle bridge design comes from the fact that validators simply make sure that the state roots they sign are correct. Since onchain signature verification is only done once per root anchor, it is possible use a large number of validators for best safety and censorship resistance.

1.1 Getting started

1.1.1 Download

```
$ git clone git@github.com:aergoio/eth-merkle-bridge.git
```

1.1.2 Install

Install dependencies

```
$ cd eth-merkle-bridge
$ virtualenv -p python3 venv
$ source venv/bin/activate
$ pip install -r requirements.txt
```

Optional dev dependencies (lint, testing...)

```
$ pip install -r dev-dependencies.txt
```

Now you can start using the bridge tools to:

- create a configuration file with the cli
- deploy a new bridge
- start a proposer
- start a validator
- update bridge settings
- transfer assets through the bridge with the cli

1.2 Using the EthAergo CLI

1.2.1 CLI for the proposer/validator

Start the cli:

```
$ python3 -m ethaergo_cli.main
```

The first step is to create a config file or load an existing one

```
(venv)
Python_workspace/aergoio/eth-merkle-bridge master x
▶ python3 -m cli.main

EthAergo CLI

Welcome to the Eth Merkle Bridge Interactive CLI.
This is a tool to transfer assets across the Ethereum <=> Aergo Merke bridge and manage wallet settings (config.json)

? Do you have a config.json? (Use arrow keys)
> Yes, find it with the path
  No, create one from scratch
  Quit
```

Then the main menu appears with cli functionality:

```
? Do you have a config.json? Yes, find it with the path
? Path to config.json (path/to/config.json) test_config.json
? What would you like to do ? (Use arrow keys)
> Check pending transfer
  Check balances
  Initiate transfer (Lock/Burn)
  Finalize transfer (Mint/Unlock)
  Settings (Register Assets and Networks)
  Back
```

These are the settings available from the cli


```
(venv)
Python_workspace/aergoio/eth-merkle-bridge master x
└─ python3 -m cli.main

      _ _ _ _ _      _ _ _ _ _
     / /   / /   / /   / /
    / /   / /   / /   / /
   / /   / /   / /   / /
  / /   / /   / /   / /
 / /   / /   / /   / /
/ /   / /   / /   / /


  _ _ _ _ _      _ _ _ _ _
 / /   / /   / /   / /
/ /   / /   / /   / /
/ /   / /   / /   / /
/ /   / /   / /   / /
/ /   / /   / /   / /
/ /   / /   / /   / /

Welcome to the Eth Merkle Bridge Interactive CLI.
This is a tool to transfer assets across the Ethereum <=> Aergo Merke bridge and manage wallet settings (config.json)

? Do you have a config.json?  No, create one from scratch
Let's register 2 networks, validators(optional) and a private key for interacting with each network.
? Network name  eth-poa-local
? Network IP    localhost:8545
? Network type  ethereum
? Is this an Ethereum POA network ?  Yes
? Network name  aergo-local
? Network IP    localhost:7845
? Network type  aergo
? Would you like to register a bridge ? (needed if already deployed)  No
Register a private key for eth-poa-local
? Give your key a short descriptive name  default
? Path to json keystore  keystore/UTC--2019-05-13T09-23-35.377701000Z--fec3c905bcd3d9a5471452e53f82106844cb1e76
? Ethereum address matching private key  0xfec3c905bcd3d9a5471452e53f82106844cb1e76
Register a private key for aergo-local
? Give your key a short descriptive name  default
? Encrypted exported key string  47CLj29W96rS9SsizUz4puueuTT2GcSpkoAsvVC3USLzQ5kKTWkmz1WLKnpqr2ET7hPd73TC9
? Aergo address matching private key  AmNMFbiVsqq6vg4njsTjgy7bKPFHFYhLV4rzQyrENUS9AM1e3tw5
? Would you like to register validators ? (not needed for bridge users)  Yes
WARNING : Validators must be registered in the correct order
? Aergo Address  AmNLjcxUDmxeGZL7F8bqyaGt3zqog5HAoJmFBEZAx1RvfTKLSBsQ
? Ethereum Address  0x210467b3849a408c3a3bEE14b4627aa57F342134
? Validator ip  localhost:9841
? Add next validator ?  Yes
? Aergo Address  AmPiFGxLvETrs13QYrHUiYoFqAqqWv7TKYXG21zC8TJfJTDHc7HJ
? Ethereum Address  0x1abdc1d5568cbb639fa605e2a155480f151c0e55
? Validator ip  localhost:9842
? Add next validator ?  Yes
? Aergo Address  AmNyNPQeqXPfdHeECMnhsH1QcnZsqCtDAudjgFyG5qpasN6tyLPE
? Ethereum Address  0x429c2388cad780f8e801849cb5f1aa76389727cd
? Validator ip  localhost:9843
? Add next validator ?  No
? Path to save new config file  dummy.json
Config file stored in: /Users/pa/Python_workspace/aergoio/eth-merkle-bridge/dummy.json
? Do you have a config.json?  (Use arrow keys)
> Yes, find it with the path
No, create one from scratch
Quit
```

Registering a new bridge

```
(venv)
Python_workspace/aergoio/eth-merkle-bridge master x
▶ python3 -m cli.main
```



```
Welcome to the Eth Merkle Bridge Interactive CLI.
This is a tool to transfer assets across the Ethereum <=> Aergo Merke bridge and manage wallet settings (config.json)

? Do you have a config.json?  Yes, find it with the path
? Path to config.json (path/to/config.json)  dummy.json
? What would you like to do ?  Settings (Register Assets and Networks)
? What would you like to do ?  Register new bridge
? Departure network  aergo-local
? Destination network  eth-poa-local
Bridge between aergo-local and eth-poa-local
? Bridge contract address on aergo-local  AmgQqVWX3JADRBEVkvCM4CyWdoeXuumeYGGJJxEeoAukRC26hxmW
? Anchoring periode of eth-poa-local on aergo-local  6
? Finality of eth-poa-local  4
? Bridge contract address on eth-poa-local  0x89eD1D1C145F6bF3A7e62d2B8eB0e1Bf15Cb2374
? Anchoring periode of aergo-local on eth-poa-local  7
? Finality of aergo-local  5
? Path to Ethereum bridge abi text file  ./contracts/solidity/bridge_abi.txt
? Path to Ethereum bridge minted token abi text file  ./contracts/solidity/minted_erc20_abi.txt
? What would you like to do ?  (Use arrow keys)
> Register new asset
  Register new network
  Register new bridge
  Register new set of validators
  Update anchoring periode
  Update finality
  Back
```

Updating bridge settings

```
(venv)
Python_workspace/aergoio/eth-merkle-bridge master x
└─ python3 -m cli.main

Welcome to the Eth Merkle Bridge Interactive CLI.
This is a tool to transfer assets across the Ethereum <=> Aergo Merke bridge and manage wallet settings (config.json)

? Do you have a config.json? Yes, find it with the path
? Path to config.json (path/to/config.json) ./test_config.json
? What would you like to do ? Settings (Register Assets and Networks)
? What would you like to do ? Update anchoring periode
? Departure network aergo-local
? Destination network eth-poa-local
? New anchoring periode (nb of blocks) of aergo-local onto eth-poa-local 7
? What would you like to do ? (Use arrow keys)
> Register new asset
  Register new network
  Register new bridge
  Register new set of validators
  Update anchoring periode
  Update finality
  Back
```


If the new anchoring periode reached validator consensus, it can then be automatically updated in the bridge contract by the proposer.

```
proposer.aergo: "Anchoring periode update requested: 7"  
proposer.aergo: " tAnchorUpdate success"
```

1.2.2 CLI for asset transfers

Registering a new asset in config file

```
(venv)
Python_workspace/aergoio/eth-merkle-bridge master x
▶ python3 -m cli.main
```



```
Welcome to the Eth Merkle Bridge Interactive CLI.
This is a tool to transfer assets across the Ethereum <=> Aergo Merke bridge and manage wallet settings (config.json)

? Do you have a config.json?  Yes, find it with the path
? Path to config.json (path/to/config.json)  dummy.json
? What would you like to do ?  Settings (Register Assets and Networks)
? What would you like to do ?  Register new asset
? Asset name ('aergo_erc20' and 'aergo' are used for the real Aergo)  token1
? Origin network (where the token was originally issued)  aergo-local
? Asset address  AmghHtk2gpcpMa6bj1v59qCBfNmKZTi8qDGeuMNg5meJuXGTa2Y1
? Add pegged asset on another network  Yes
? Pegged network  eth-poa-local
? Asset address  0xB7633077842e3fb1877e43C0cCa0972dB8bb6Fb0
? Add another pegged asset on another network  No
All pegged assets are registered in know networks
? What would you like to do ?  (Use arrow keys)
> Register new asset
  Register new network
  Register new bridge
  Register new set of validators
  Update anchoring periode
  Update finality
  Back
```


Check pending transfers

It is possible to check withdrawable balances of pending transfer between chains.

```
Welcome to the Eth Merkle Bridge Interactive CLI.
This is a tool to transfer assets across the Ethereum <=> Aergo Merke bridge and manage wallet settings (config.json)

? Do you have a config.json?  Yes, find it with the path
? Path to config.json (path/to/config.json)  test_config.json
? What would you like to do ?  Initiate transfer (Lock/Burn)
? Departure network  eth-poa-local
? Destination network  aergo-local
? Name of asset to transfer  aergo_erc20
? Receiver of assets on other side of bridge  AmNMFBiVs9y6vg4njsTjgy7bKPFHFYhLV4rzQyrENUS9AM1e3tw5
? Amount of assets to transfer  3.3
? Choose account to sign transaction :  default
Lock transfer summary:
Departure chain: eth-poa-local (0x89eD1D1C145F6bF3A7e62d2B8e80e1Bf15Cb2374)
Destination chain: aergo-local (AmgQqVwX3JADRBvKVCm4CyWd0eXUmeYGGJJxEeoAukRC26hxmW)
Asset name: aergo_erc20 (0xd898383A12CDE0eDF7642F7dD4D7006FdE5c433e)
Receiver at destination: AmNMFBiVs9y6vg4njsTjgy7bKPFHFYhLV4rzQyrENUS9AM1e3tw5
Amount: 3300000000000000000

? Confirm you want to execute tranfer tx  Yes, execute transfer

eth-poa-local -> aergo-local
Decrypt Ethereum keystore 'default'
Password:
👛 aergo_erc20 balance on destination before transfer : 500000000.0
⬆ Increase approval success: 0x96dd0049066aa1fcd6bb5d0f0b3ac03340db2d8ee56587e8dc1fe0ce020b1846
🔒 Lock success: 0xe68d9e9147b733aaa398799684cf4d196af4eae5f2cfc2fb0e39b28c39a0cb0b
👛 remaining aergo_erc20 balance on origin after transfer: 499999996.7
Transaction Hash : 0xe68d9e9147b733aaa398799684cf4d196af4eae5f2cfc2fb0e39b28c39a0cb0b
Block Height : 87

? What would you like to do ?  Check pending transfer
? Choose a pending transfer  ['eth-poa-local', 'aergo-local', 'aergo_erc20', 'AmNMFBiVs9y6vg4njsTjgy7bKPFHFYhLV4rzQyrENUS9AM1e3tw5', 87]
Withdrawable: 3.3 Pending: 0.0
? What would you like to do ?  Check pending transfer
? Choose a pending transfer  Custom transfer
? Departure network  eth-poa-local
? Destination network  aergo-local
? Name of asset to transfer  aergo_erc20
? Receiver of assets on other side of bridge  AmNMFBiVs9y6vg4njsTjgy7bKPFHFYhLV4rzQyrENUS9AM1e3tw5
Withdrawable: 3.3 Pending: 0.0
? What would you like to do ?  (Use arrow keys)
> Check pending transfer
  Check balances
  Initiate transfer (Lock/Burn)
  Finalize transfer (Mint/Unlock)
  Settings (Register Assets and Networks)
  Back
```

If a transfer was made with the cli, the transfer parameters are recorded but it is also possible to check the withdrawable balance of a custom transfer between any chain. ‘Withdrawable’ is the balance that can be immediatly withdrawn on the other side of the bridge. ‘Pending’ is the balance that was deposited in the bridge contract but the anchor has not happened on the other side of the bridge so it is not yet withdrawable.

Pending transfers are recorded as an array of [departure chain, destination chain, asset name, receiver, block height of lock/burn/freeze]. All pending transfer are store in `ethaergo_cli/pending_transfers.json` and deleted once finalized.

1.3 Proposer

A proposer connects to all validators and requests them to sign a new anchor with the `GetEthAnchorSignature` and `GetAergoAnchorSignature` rpc requests. To prevent downtime, anybody can become a proposer and request signatures to validators. It is the validator’s responsibility to only sign correct anchors. The bridge contracts will not update the state root if the anchoring time is not reached (`t_anchor`).

1.3.1 Starting a Proposer

```
$ python3 -m ethaergo_bridge_operator.proposer.client --help
```

(continues on next page)

(continued from previous page)

```

usage: client.py [-h] -c CONFIG_FILE_PATH -a AERGO -e ETH --eth_block_time
                ETH_BLOCK_TIME [--privkey_name PRIVKEY_NAME] [--auto_update]
                [--local_test] [--eth_gas_price ETH_GAS_PRICE]
                [--aergo_gas_price AERGO_GAS_PRICE]

Start a proposer on Ethereum and Aergo.

optional arguments:
  -h, --help            show this help message and exit
  -c CONFIG_FILE_PATH, --config_file_path CONFIG_FILE_PATH
                        Path to config.json
  -a AERGO, --aergo AERGO
                        Name of Aergo network in config file
  -e ETH, --eth ETH      Name of Ethereum network in config file
  --eth_block_time ETH_BLOCK_TIME
                        Average Ethereum block time
  --privkey_name PRIVKEY_NAME
                        Name of account in config file to sign anchors
  --auto_update          Update bridge contract when settings change in config
                        file
  --local_test          Start proposer with password for testing
  --eth_gas_price ETH_GAS_PRICE
                        Gas price (gWei) to use in transactions
  --aergo_gas_price AERGO_GAS_PRICE
                        Gas price to use in transactions

$ python3 -m ethaergo_bridge_operator.proposer.client -c './test_config.json' -a
↳ 'aergo-local' -e 'eth-poa-local' --eth_block_time 3 --privkey_name "proposer" --
↳ auto_update

proposer.eth: "Connect Aergo and Ethereum providers"
proposer.eth: "aergo-local (t_final=5 ) -> eth-poa-local : t_anchor=7"
proposer.eth: "Proposer Address: 0xc19b69591141443676a3EE56fbf1d3EA869d53D8"
proposer.eth: "Connect to EthValidators"
proposer.eth: "Validators: ['0x210467b3849a408c3a3bEE14b4627aa57F342134',
↳ '0x210467b3849a408c3a3bEE14b4627aa57F342134',
↳ '0x210467b3849a408c3a3bEE14b4627aa57F342134']"
proposer.aergo: "Connect Aergo and Ethereum providers"
proposer.aergo: "aergo-local <- eth-poa-local (t_final=4) : t_anchor=6"
proposer.aergo: "Proposer Address:
↳ AmPxVdu993eosN3UjnPDdN3wb7TNbHeiHDvn2dvZUcH8KXDK3RLU"
proposer.aergo: "Connect to AergoValidators"
proposer.aergo: "Validators: [
↳ 'AmNLjcxUDmxeGZL7F8bqyaGt3zqog5HAoJmFBEZAx1RvfTKLSBsQ',
↳ 'AmNLjcxUDmxeGZL7F8bqyaGt3zqog5HAoJmFBEZAx1RvfTKLSBsQ',
↳ 'AmNLjcxUDmxeGZL7F8bqyaGt3zqog5HAoJmFBEZAx1RvfTKLSBsQ']"
proposer.eth: "Start Eth proposer"
proposer.aergo: "Current Eth -> Aergo anchor: height: 0, root: 0xconstructor,
↳ nonce: 0"
proposer.aergo: " Gathering validator signatures for: root:
↳ 0xd97d33cb90c9e58befdba86467907ba68258b49f0f85a22781db7c4eda3033e4, height: 8262"
proposer.eth: "Current Aergo -> Eth anchor: height: 0, root:
↳ 0x0000000000000000000000000000000000000000000000000000000000000000, nonce: 0"
proposer.eth: " Gathering validator signatures for: root:
↳ 0x5d471941372b64d66361c29fca4e13c899819afe212cce87143794d80b510613, height: 8280"
proposer.eth: " Anchor success, wait until next anchor time: 7s..."
proposer.eth: " Gas used: 109287"

```

(continues on next page)

(continued from previous page)

```
proposer.aergo: " Anchor success, wait until next anchor time: 6s..."
```

1.3.2 Updating bridge settings

Bridge settings are updated when the config file changes and the proposer is started with `-auto_update`. The proposer will then try to gather signatures from validators to make the update on chain.

```
(venv)
Python_workspace/aergoio/eth-merkle-bridge master x
> python3 -m cli.main

EthMerkleBridge
aergoio eth

Welcome to the Eth Merkle Bridge Interactive CLI.
This is a tool to transfer assets across the Ethereum <=> Aergo Merke bridge and manage wallet settings (config.json)

? Do you have a config.json? Yes, find it with the path
? Path to config.json (path/to/config.json) ./test_config.json
? What would you like to do ? Settings (Register Assets and Networks)
? What would you like to do ? Update anchoring periode
? Departure network aergo-local
? Destination network eth-poa-local
? New anchoring periode (nb of blocks) of aergo-local onto eth-poa-local 7
? What would you like to do ? (Use arrow keys)
> Register new asset
  Register new network
  Register new bridge
  Register new set of validators
  Update anchoring periode
  Update finality
  Back
```

If the new anchoring periode reached validator consensus, it can then be automatically updated in the bridge contract by the proposer.

```
proposer.aergo: "Anchoring periode update requested: 7"
proposer.aergo: " tAnchorUpdate success"
```

1.4 Validator

A validator will sign any state root from any proposer via the `GetAnchorSignature` rpc request as long as it is valid. Therefore a validator must run a full node. Assets on the sidechain are secure as long as 2/3 of the validators validate both chains and are honest. Since signature verification only happens when anchoring (and not when transferring assets), the number of validators can be very high as the signature verification cost is necessary only once per anchor.

1.4.1 Starting a Validator

```
$ python3 -m ethaergo_bridge_operator.validator.server --help

usage: server.py [-h] -c CONFIG_FILE_PATH -a AERGO -e ETH -i VALIDATOR_INDEX
```

(continues on next page)

(continued from previous page)

```

[--privkey_name PRIVKEY_NAME] [--auto_update] [--local_test]

Start a validator on Ethereum and Aergo.

optional arguments:
-h, --help            show this help message and exit
-c CONFIG_FILE_PATH, --config_file_path CONFIG_FILE_PATH
                        Path to config.json
-a AERGO, --aergo AERGO
                        Name of Aergo network in config file
-e ETH, --eth ETH      Name of Ethereum network in config file
-i VALIDATOR_INDEX, --validator_index VALIDATOR_INDEX
                        Index of the validator in the ordered list of
                        validators
--privkey_name PRIVKEY_NAME
                        Name of account in config file to sign anchors
--auto_update          Update bridge contract when settings change in config
                        file
--local_test           Start all validators locally for convenient testing

$ python3 -m ethaergo_bridge_operator.validator.server -c './test_config.json' -a
→ 'aergo-local' -e 'eth-poa-local' --validator_index 1 --privkey_name "validator" --
→ auto_update

"Connect Aergo and Ethereum"
"Current Aergo validators : ['AmNLjcxUDmxeGZL7F8bqyaGt3zqog5HAoJmFBEZAx1RvfTKLSBsQ
→ ', 'AmNLjcxUDmxeGZL7F8bqyaGt3zqog5HAoJmFBEZAx1RvfTKLSBsQ',
→ 'AmNLjcxUDmxeGZL7F8bqyaGt3zqog5HAoJmFBEZAx1RvfTKLSBsQ']"
"Current Ethereum validators : ['0x210467b3849a408c3a3bEE14b4627aa57F342134',
→ '0x210467b3849a408c3a3bEE14b4627aa57F342134',
→ '0x210467b3849a408c3a3bEE14b4627aa57F342134']"
"aergo-local <- eth-poa-local (t_final=4) : t_anchor=6"
"aergo-local (t_final=5) -> eth-poa-local : t_anchor=7"
"WARNING: This validator will vote for settings update in config.json"
Decrypt Aergo and Ethereum accounts 'validator'
Password:
"Aergo validator Address: AmNLjcxUDmxeGZL7F8bqyaGt3zqog5HAoJmFBEZAx1RvfTKLSBsQ"
"Ethereum validator Address: 0x210467b3849a408c3a3bEE14b4627aa57F342134"
"server 1 started"
{"val_index": 1, "signed": true, "type": " anchor", "value": {"root":
→ "0xd97d33cb90c9e58befdba86467907ba68258b49f0f85a22781db7c4eda3033e4", "height":
→ 8102}, "destination": "aergo-local", "nonce": 0}
{"val_index": 1, "signed": true, "type": " anchor", "value": {"root":
→ "0x5d471941372b64d66361c29fca4e13c899819afe212cce87143794d80b510613", "height":
→ 8119}, "destination": "eth-poa-local", "nonce": 0}

```

1.4.2 Updating bridge settings

The information (validator set, anchoring periods, finality of blockchains) contained in the config file will be used by the validator to vote on changes if `--auto_update` is enabled. Be careful that the information in config file is correct as any proposer can request a signature of that information. If the proposer gathers 2/3 signatures for the same information then the bridge settings can be updated.

```
(venv)
Python_workspace/aergoio/eth-merkle-bridge master x
► python3 -m cli.main

Welcome to the Eth Merkle Bridge Interactive CLI.
This is a tool to transfer assets across the Ethereum <=> Aergo Merke bridge and manage wallet settings (config.json)

? Do you have a config.json? Yes, find it with the path
? Path to config.json (path/to/config.json) ./test_config.json
? What would you like to do ? Settings (Register Assets and Networks)
? What would you like to do ? Update anchoring periode
? Departure network aergo-local
? Destination network eth-poa-local
? New anchoring periode (nb of blocks) of aergo-local onto eth-poa-local 7
? What would you like to do ? (Use arrow keys)
> Register new asset
  Register new network
  Register new bridge
  Register new set of validators
  Update anchoring periode
  Update finality
  Back
```

1.5 Deploying a new bridge

Before using the bridge deployer, a config file should be created to register network node connections, bridge tempo (anchoring periode and finality of both chains), validators and the address of `aergo_erc20` on ethereum. The aergo bridge contract must record the `aergo_erc20` so that aergo can be unfrozen.

```

(venv)
Python_workspace/aergoio/eth-merkle-bridge master x
► python3 -m cli.main

      _ _ _ _ _      _ _ _ _ _      _ _ _ _ _
     / / / / /      / / / / /      / / / / /
    / / / / /      / / / / /      / / / / /
   / / / / /      / / / / /      / / / / /
  / / / / /      / / / / /      / / / / /
 / / / / /      / / / / /      / / / / /
/ / / / /      / / / / /      / / / / /


  _ _ _ _ _      _ _ _ _ _      _ _ _ _ _
 / / / / /      / / / / /      / / / / /
/ / / / /      / / / / /      / / / / /

Welcome to the Eth Merkle Bridge Interactive CLI.
This is a tool to transfer assets across the Ethereum <=> Aergo Merke bridge and manage wallet settings (config.json)

? Do you have a config.json?  No, create one from scratch
Let's register 2 networks, validators(optional) and a private key for interacting with each network.
? Network name  eth-poa-local
? Network IP    localhost:8545
? Network type  ethereum
? Is this an Ethereum POA network ?  Yes
? Network name  aergo-local
? Network IP    localhost:7845
? Network type  aergo
? Would you like to register a bridge ? (needed if already deployed)  No
Register a private key for eth-poa-local
? Give your key a short descriptive name  default
? Path to json keystore  keystore/UTC--2019-05-13T09-23-35.377701000Z--fec3c905bcd3d9a5471452e53f82106844cb1e76
? Ethereum address matching private key  0xfec3c905bcd3d9a5471452e53f82106844cb1e76
Register a private key for aergo-local
? Give your key a short descriptive name  default
? Encrypted exported key string  47CLj29W96rS9SsizUz4pueeuTT2GcSpkoAsvVC3USLzQ5kKTWKmz1WLKnqor2ET7hPd73TC9
? Aergo address matching private key  AmNMFbiVs9y6vg4njsTjgy7bKPFHFYhLV4rzQyrENUS9AM1e3tw5
? Would you like to register validators ? (not needed for bridge users)  Yes
WARNING : Validators must be registered in the correct order
? Aergo Address  AmNLjcxUDmxe6ZL7F8bqyaGt3zqog5HAoJmFBEZAx1RvfTKLSBsQ
? Ethereum Address  0x210467b3849a408c3a3bEE14b4627aa57F342134
? Validator ip  localhost:9841
? Add next validator ?  Yes
? Aergo Address  AmPiFGxLvETrs13QYrHUiYoFqAqqWv7TKYXG21zC8TJfJTDHc7HJ
? Ethereum Address  0x1abdc1d5568cbb639fa60Se2a155480f151c0e55
? Validator ip  localhost:9842
? Add next validator ?  Yes
? Aergo Address  AmNyNPEqeXPfdHeECMNhsH1QcnZsqCtDAudjgFyG5qpasN6tyLPE
? Ethereum Address  0x429c2388cad780f8e801849cb5f1aa76389727cd
? Validator ip  localhost:9843
? Add next validator ?  No
? Path to save new config file  dummy.json
Config file stored in: /Users/pa/Python_workspace/aergoio/eth-merkle-bridge/dummy.json
? Do you have a config.json?  (Use arrow keys)
> Yes, find it with the path
  No, create one from scratch
  Quit

```

```
(venv)
Python_workspace/aergoio/eth-merkle-bridge master x
▶ python3 -m cli.main
```



```
Welcome to the Eth Merkle Bridge Interactive CLI.
This is a tool to transfer assets across the Ethereum <=> Aergo Merke bridge and manage wallet settings (config.json)

? Do you have a config.json? Yes, find it with the path
? Path to config.json (path/to/config.json) dummy.json
? What would you like to do ? Settings (Register Assets and Networks)
? What would you like to do ? Register new asset
? Asset name ('aergo_erc20' and 'aergo' are used for the real Aergo) aergo_erc20
? Origin network (where the token was originally issued) eth-poa-local
? Asset address 0xae31b85bfe62747d0836b82608b4830361a3d37a
? Add pegged asset on another network Yes
? Pegged network aergo-local
? Asset address aergo
? Add another pegged asset on another network No
All pegged assets are registered in know networks
? Path to the asset's abi text file contracts/solidity/aergo_erc20_abi.txt
? What would you like to do ? (Use arrow keys)
> Register new asset
  Register new network
  Register new bridge
  Register new set of validators
  Update anchoring periode
  Update finality
  Back
```

```
$ python3 -m ethaergo_bridge_operator.bridge_deployer --help
18h17m
usage: bridge_deployer.py [-h] -c CONFIG_FILE_PATH -a AERGO -e ETH
                        [--privkey_name PRIVKEY_NAME] [--local_test]

Deploy bridge contracts between Ethereum and Aergo.

optional arguments:
  -h, --help            show this help message and exit
  -c CONFIG_FILE_PATH, --config_file_path CONFIG_FILE_PATH
                        Path to config.json
  -a AERGO, --aergo AERGO
                        Name of Aergo network in config file
  -e ETH, --eth ETH     Name of Ethereum network in config file
  --privkey_name PRIVKEY_NAME
                        Name of account in config file to sign anchors
  --local_test          Start proposer with password for testing

$ python3 -m ethaergo_bridge_operator.bridge_deployer -c './test_config.json' -a
'aergo-local' -e eth-poa-local --t_anchor_aergo 6 --t_final_aergo 4 --t_anchor_eth_
7 --t_final_eth 5 --privkey_name "proposer"
```

```
----- DEPLOY BRIDGE BETWEEN Aergo & Ethereum -----
----- Connect AERGO -----
----- Connect Web3 -----
----- Set Sender Account -----
Decrypt Aergo private key 'proposer'
```

(continues on next page)

(continued from previous page)

```

Password:
> Sender Address Aergo: AmPxVdu993eosN3UjnPDdN3wb7TNbHeiHDvn2dvZUcH8KXDK3RLU
> Sender Address Ethereum: 0xc19b69591141443676a3EE56fbf1d3EA869d53D8
aergo validators : ['AmNLjcxUDmxeGZL7F8bqyaGt3zqog5HAoJmFBEZAx1RvfTKLSBsQ',
→ 'AmNLjcxUDmxeGZL7F8bqyaGt3zqog5HAoJmFBEZAx1RvfTKLSBsQ',
→ 'AmNLjcxUDmxeGZL7F8bqyaGt3zqog5HAoJmFBEZAx1RvfTKLSBsQ']
ethereum validators : ['0x210467b3849a408c3a3bEE14b4627aa57F342134',
→ '0x210467b3849a408c3a3bEE14b4627aa57F342134',
→ '0x210467b3849a408c3a3bEE14b4627aa57F342134']
----- Deploy Aergo SC -----
> result [Cq8C52DBbfUzumGEtAZ163UQrtfuCKE2ovgawTwLk4zq] : TX_OK
----- Deploy Ethereum SC -----
> SC Address Ethereum: 0x89eD1D1C145F6bF3A7e62d2B8eB0e1Bf15Cb2374
> SC Address Aergo: AmgQqVWX3JADRBvKVCm4CyWdoeXuumeYGGJJxEeoAukRC26hxmW
----- Store bridge addresses in test_config.json -----

```

After deployment, the aer on the Aergo network should be sent (frozen) to the bridge contract so that it can be unfrozen when users sent their ERC20 from the Ethereum network.

1.6 Configuration file

The config file is used by the bridge operators, the wallet and the CLI to store information about node connections, validator connections, bridge parameters, assets and private keys.

It can be created and updated manually or with the help of the CLI.

```

{
  "networks": { // list of registered networks
    "aergo-local": { // name of the network
      "bridges": { // list of bridges between 'aergo-local' and other
→ blockchains
        "eth-poa-local": { // name of bridged network
          "addr": "AmhXrQ7KdNA4naBi2sTwHj13aBzVBohRhxy262nXsPbV2YbULXUR", //
→ address of bridge contract
          "t_anchor": 6, // anchoring periode in bridge contract
          "t_final": 4 // finality of chain anchored on bridge contract
        }
      },
      "ip": "localhost:7845", // node connection ip
      "providers": [
        "localhost:7845",
        "localhost:7845"
      ], // redundant providers for validators to query different data sources
      "tokens": { // list of tokens originating from 'aergo-local'
        "aergo": { // aer native asset
          "addr": "aergo", // 'aergo' is the reserved name and address
          "pegs": {}
        },
        "token1": { // asset name
          "addr": "AmghHtk2gpcpMa6bj1v59qCBfNmKZTi8qDGeuMNg5meJuXGTa2Y1", //
→ asset address
          "pegs": { // list of networks where this asset has a peg
            "eth-poa-local": "0xB7633077842e3fb1877e43C0cCa0972dB8bb6Fb0"
→ // address of pegged asset
          }
        }
      }
    }
  }
}

```

(continues on next page)

(continued from previous page)

```

    },
    "type": "aergo" // type of network to differentiate between Aergo and
↳Ethereum
  },
  "eth-poa-local": {
    "bridges": {
      "aergo-local": {
        "addr": "0xbC5385259C2Dfdd99996CFb9B6C2f92767FcB32b",
        "bridge_abi": "/Users/pa/Python_workspace/aergoio/eth-merkle-
↳bridge/contracts/solidity/bridge_abi.txt", // path to bridge abi
        "minted_abi": "/Users/pa/Python_workspace/aergoio/eth-merkle-
↳bridge/contracts/solidity/minted_erc20_abi.txt", // path to minted token abi
        "t_anchor": 7,
        "t_final": 5
      }
    },
    "ip": "localhost:8545",
    "providers": [
      "http://localhost:8545",
      "http://localhost:8545"
    ], // redundant providers for validators to query different data sources
    "isPOA": true, // web3py needs middleware to connect to POA chains
    "tokens": {
      "aergo_erc20": { // reserved name of aergo erc20 issued at ico
        "abi": "contracts/solidity/aergo_erc20_abi.txt",
        "addr": "0xd898383A12CDE0eDF7642F7dD4D7006FdE5c433e",
        "pegs": {
          "aergo-local": "aergo"
        }
      },
      "ether": {
        "addr": "ether",
        "pegs": {}
      },
      "test_erc20": {
        "abi": "contracts/solidity/aergo_erc20_abi.txt",
        "addr": "0xeeEF65f288b39d1514A54852566415b973927142",
        "pegs": {
          "aergo-local":
↳"AmhiUx2hZ9phVDMZoBShEWD2sCFXPJ5BZpagNC8WfssPuZg7wzZS"
        }
      }
    },
    "type": "ethereum"
  },
  "validators": [ // list of validators, only needed for bridge operator
    {
      "addr": "AmNLjcxUDmxeGZL7F8bqyaGt3zqog5HAoJmFBEZAx1RvfTKLSBsQ", //
↳validator address in Aergo bridge contract
      "eth-addr": "0x210467b3849a408c3a3bEE14b4627aa57F342134", // validator
↳address in Ethereum bridge contract
      "ip": "localhost:9841" // ip of validator API
    },
    {
      "addr": "AmNyNPEqeXPfdHeECMNhsHlQcnZsqCtDAudjgFyG5qpasN6tyLPE",

```

(continues on next page)

(continued from previous page)

```

        "eth-addr": "0x7acb4a265bf759ec772510c2465fb7c8f4eaf54e",
        "ip": "localhost:9842"
    },
    {
        "addr": "AmPf349iHWd6kQGU45BxFzFCzEDu75Y3FqFPd4WBMteFq4mtDuZd",
        "eth-addr": "0xf1bf3497d98ead7f6a1bb9ee6dfbde9d448d7062",
        "ip": "localhost:9843"
    }
],
"wallet": { // list of Aergo wallets
    "default": { // name of wallet
        "addr": "AmNMFbiVs9y6vg4njsTjgy7bKPFHFYhLV4rzQyrENUS9AM1e3tw5", //
        ↪address matching private key
        "priv_key":
        ↪"47CLj29W96rS9SsizUz4pueeuTT2GcSpkoAsvVC3USLzQ5kKTWKmz1WLKnqor2ET7hPd73TC9" //
        ↪encrypted private key
    }
},
"wallet-eth": { // list of Ethereum wallets
    "default": { // name of wallet
        "addr": "0xfec3c905bcd3d9a5471452e53f82106844cb1e76", // address matching
        ↪private key
        "keystore": "keystore/UTC--2019-05-13T09-23-35.377701000Z--
        ↪fec3c905bcd3d9a5471452e53f82106844cb1e76" // path to json keystore
    }
}
}

```

1.7 bridge_operator

```

class ethaergo_bridge_operator.proposer.client.ProposerClient (config_file_path:
                                                                    str, aergo_net:
                                                                    str, eth_net: str,
                                                                    eth_block_time:
                                                                    int,
                                                                    aergo_gas_price:
                                                                    int,
                                                                    eth_gas_price:
                                                                    int,
                                                                    privkey_name:
                                                                    str = None,
                                                                    privkey_pwd:
                                                                    str = None,
                                                                    auto_update:
                                                                    bool = False,
                                                                    root_path: str =
                                                                    './')

```

The ProposerClient starts Aergo and Ethereum proposers

```
class ethaergo_bridge_operator.proposer.eth.client.EthProposerClient (config_file_path:
                                                                    str,
                                                                    aergo_net:
                                                                    str,
                                                                    eth_net:
                                                                    str,
                                                                    privkey_name:
                                                                    str    =
                                                                    None,
                                                                    privkey_pwd:
                                                                    str    =
                                                                    None,
                                                                    auto_update:
                                                                    bool   =
                                                                    False,
                                                                    root_path:
                                                                    str    =
                                                                    './',
                                                                    eth_gas_price:
                                                                    int    =
                                                                    None)
```

The ethereum bridge proposer periodically (every `t_anchor`) broadcasts the finalized Aergo trie state root (after lib) of the bridge contract onto the ethereum bridge contract after validation by the Validators. It first checks the last merged height and waits until `now > lib + t_anchor` is reached, then merges the current finalised block (lib). Start again after waiting `t_anchor`. `EthProposerClient` anchors an Aergo state root onto Ethereum.

Note on config_data:

- `config_data` is used to store current validators and their ip when the proposer starts. (change validators after the proposer has started)
- After starting, when users change the `config.json`, the proposer will attempt to gather signatures to reflect the changes.
- `t_anchor` value is always taken from the bridge contract
- validators are taken from the `config_data` because ip information is not stored on chain
- when a validator set update succeeds, `self.config_data` is updated
- if another proposer updates to a new set of validators and the proposer doesn't know about it, proposer must be restarted with the new current validator set to create new connections to them.

`monitor_settings ()`

Check if a modification of bridge settings is requested by seeing if the config file has been changed and try to update the bridge contract (gather 2/3 validators signatures).

`monitor_settings_and_sleep (sleeping_time)`

While sleeping, periodically check changes to the config file and update settings if necessary. If another proposer updated settings it doesn't matter, validators will just not give signatures.

`run ()` → None

Gathers signatures from validators, verifies them, and if 2/3 majority is acquired, set the new anchored root in `eth_bridge`.

`update_t_anchor (t_anchor)`

Try to update the anchoring periode registered in the bridge contract.

`update_t_final (t_final)`

Try to update the anchoring periode registered in the bridge contract.

update_validators (*new_validators*)

Try to update the validator set with the one in the config file.

wait_next_anchor (*merged_height: int*) → int

Wait until *t_anchor* has passed after merged height. Return the next finalized block after *t_anchor* to be the next anchor

```
class ethaergo_bridge_operator.proposer.aergo.client.AergoProposerClient (config_file_path:
                                                                    str,
                                                                    aergo_net:
                                                                    str,
                                                                    eth_net:
                                                                    str,
                                                                    eth_block_time:
                                                                    int,
                                                                    privkey_name:
                                                                    str
                                                                    =
                                                                    None,
                                                                    privkey_pwd:
                                                                    str
                                                                    =
                                                                    None,
                                                                    auto_update:
                                                                    bool
                                                                    =
                                                                    False,
                                                                    aergo_gas_price:
                                                                    int
                                                                    =
                                                                    None)
```

The bridge proposer periodically (every *t_anchor*) broadcasts the finalized trie state root (after lib) of the bridge contract on both sides of the bridge after validation by the Validator servers. It first checks the last merged height and waits until *now > lib + t_anchor* is reached, then merges the current finalised block (lib). Start again after waiting *t_anchor*.

Note on config_data:

- *config_data* is used to store current validators and their ip when the proposer starts. (change validators after the proposer has started)
- After starting, when users change the *config.json*, the proposer will attempt to gather signatures to reflect the changes.
- *t_anchor* value is always taken from the bridge contract
- validators are taken from the *config_data* because ip information is not stored on chain
- when a validator set update succeeds, *self.config_data* is updated
- if another proposer updates to a new set of validators and the proposer doesn't know about it, proposer must be restarted with the new current validator set to create new connections to them.

monitor_settings ()

Check if a modification of bridge settings is requested by seeing if the config file has been changed and try to update the bridge contract (gather 2/3 validators signatures).

monitor_settings_and_sleep (*sleeping_time*)

While sleeping, periodically check changes to the config file and update settings if necessary. If another proposer updated settings it doesn't matter, validators will just not give signatures.

run () → None

Gathers signatures from validators, verifies them, and if 2/3 majority is acquired, set the new anchored root in `aergo_bridge`.

update_t_anchor (*t_anchor*)

Try to update the anchoring periode registered in the bridge contract.

update_t_final (*t_final*)

Try to update the anchoring periode registered in the bridge contract.

update_unfreeze_fee (*fee*)

Try to update the anchoring periode registered in the bridge contract.

update_validators (*new_validators*)

Try to update the validator set with the one in the config file.

wait_next_anchor (*merged_height: int*) → int

Wait until `t_anchor` has passed after merged height. Return the next finalized block after `t_anchor` to be the next anchor

```
ethaergo_bridge_operator.bridge_deployer.deploy_bridge (config_path:      str,
                                                         lua_bytecode_path:  str,
                                                         sol_bytecode_path: str,
                                                         eth_net:      str, aergo_net:
                                                         str,          aergo_erc20:
                                                         str      = 'aergo_erc20',
                                                         privkey_name: str = None,
                                                         privkey_pwd: str = None)
                                                         → None
```

Deploy brige contract on Aergo and Ethereum.

exception `ethaergo_bridge_operator.proposer.exceptions.ValidatorMajorityError`

Exception raised by proposers when they fail to gather 2/3 validator signatures to make an update.

1.8 ethaergo_wallet

```
class ethaergo_wallet.wallet.EthAergoWallet (config_file_path: str, config_data: Dict[KT,
VT] = None, root_path: str = './',
eth_gas_price: int = 10, aergo_gas_price:
int = 0)
```

EthAergoWallet transfers tokens on the Eth<->Aergo Bridge

```
aergo_to_eth_sidechain (from_chain: str, to_chain: str, asset_name: str, amount:
int, aergo_receiver: str, aergo_privkey_name: str = 'default',
aergo_privkey_pwd: str = None, eth_privkey_name: str = 'default',
eth_privkey_pwd: str = None) → None
```

Transfer a native Aergo Standard Token or Aer to Ethereum

```
burn_to_aergo (from_chain: str, to_chain: str, asset_name: str, amount: int, receiver: str,
privkey_name: str = 'default', privkey_pwd: str = None) → Tuple[int, str]
```

Initiate minted Standard token transfer back to aergo origin

```
burn_to_eth (from_chain: str, to_chain: str, asset_name: str, amount: int, receiver: str,
privkey_name: str = 'default', privkey_pwd: str = None) → Tuple[int, str]
```

Initiate minted token transfer back to ethereum origin

eth_to_aergo_sidechain (*from_chain: str, to_chain: str, asset_name: str, amount: int, aergo_receiver: str, aergo_privkey_name: str = 'default', aergo_privkey_pwd: str = None, eth_privkey_name: str = 'default', eth_privkey_pwd: str = None*) → None
 Transfer a native ERC20 or ether to Aergo

freeze (*from_chain: str, to_chain: str, amount: int, receiver: str, privkey_name: str = 'default', privkey_pwd: str = None*) → Tuple[int, str]
 Initiate Aer transfer back to Ethereum AergoERC20 sidechain

get_aergo (*network_name: str, privkey_name: str = 'default', privkey_pwd: str = None, skip_state: bool = False*) → aergo.herapy.aergo.Aergo
 Return aergo provider with new account created with priv_key

get_balance_aergo (*asset_name: str, network_name: str, asset_origin_chain: str = None, account_name: str = 'default', account_addr: str = None*) → Tuple[int, str]
 Get account name balance of asset_name on network_name, and specify asset_origin_chain for a pegged asset query,

get_balance_eth (*asset_name: str, network_name: str, asset_origin_chain: str = None, account_name: str = 'default', account_addr: str = None*) → Tuple[int, str]
 Get account name balance of asset_name on network_name, and specify asset_origin_chain for a pegged asset query,

get_signer (*w3: web3.main.Web3, privkey_name: str, privkey_pwd: str = None*)
 Get the web3 signer object from the ethereum private key.

load_bridge_abi (*from_chain: str, to_chain: str*) → str
 Load Ethereum bridge contract abi from file location in config.

load_erc20_abi (*origin_chain: str, asset_name: str*) → str
 Load erc20 contract abi from file location in config.

load_keystore (*privkey_name: str*) → str
 Load encrypted private key from Ethereum json keystore.

load_minted_erc20_abi (*from_chain: str, to_chain: str*) → str
 Load Ethereum bridge contract minted token abi from file location in config.

lock_to_aergo (*from_chain: str, to_chain: str, asset_name: str, amount: int, receiver: str, privkey_name: str = 'default', privkey_pwd: str = None*) → Tuple[int, str]
 Initiate ERC20 token or Ether transfer to Aergo sidechain

lock_to_eth (*from_chain: str, to_chain: str, asset_name: str, amount: int, receiver: str, privkey_name: str = 'default', privkey_pwd: str = None*) → Tuple[int, str]
 Initiate Aergo Standard Token transfer to Ethereum sidechain

mint_to_aergo (*from_chain: str, to_chain: str, asset_name: str, receiver: str = None, lock_height: int = 0, privkey_name: str = 'default', privkey_pwd: str = None*) → str
 Finalize ERC20 token or Ether transfer to Aergo sidechain

mint_to_eth (*from_chain: str, to_chain: str, asset_name: str, receiver: str = None, lock_height: int = 0, privkey_name: str = 'default', privkey_pwd: str = None*) → Tuple[str, str]
 Finalize Aergo Standard Token transfer to Ethereum sidechain NOTE anybody can mint so sender is not necessary. The amount to mint is the difference between total deposit and already minted amount. Bridge tempo is taken from config_data

mintable_to_aergo (*from_chain: str, to_chain: str, asset_name: str, receiver: str*) → Tuple[int, int]
 Check mintable balance on Aergo.

mintable_to_eth (*from_chain: str, to_chain: str, asset_name: str, receiver: str*) → Tuple[int, int]
 Check mintable balance on Ethereum.

unfreeze (*from_chain: str, to_chain: str, receiver: str = None, lock_height: int = 0, privkey_name: str = 'default', privkey_pwd: str = None*) → *str*
Finalize ERC20Aergo transfer to Aergo Mainnet by unfreezing (aers are already minted and freezed in the bridge contract)

unfreezeable (*from_chain: str, to_chain: str, receiver: str*) → *Tuple[int, int]*
Check unfreezeable balance on Aergo.

unlock_to_aergo (*from_chain: str, to_chain: str, asset_name: str, receiver: str, burn_height: int = 0, privkey_name: str = 'default', privkey_pwd: str = None*) → *str*
Finalize Aergo Standard token transfer back to Aergo Origin

unlock_to_eth (*from_chain: str, to_chain: str, asset_name: str, receiver: str = None, burn_height: int = 0, privkey_name: str = 'default', privkey_pwd: str = None*) → *Tuple[str, str]*
Finalize ERC20 or Eth transfer back to Ethereum origin

unlockeable_to_aergo (*from_chain: str, to_chain: str, asset_name: str, receiver: str*) → *Tuple[int, int]*
Check unlockeable balance on Aergo.

unlockeable_to_eth (*from_chain: str, to_chain: str, asset_name: str, receiver: str*) → *Tuple[int, int]*
Check unlockeable balance on Ethereum.

`ethaergo_wallet.aergo_to_eth.build_burn_proof` (*aergo_from: aergo.herapy.aergo.Aergo, w3: web3.main.Web3, receiver: str, bridge_from: str, bridge_to: str, bridge_to_abi: str, burn_height: int, token_origin: str*)

Check the last anchored root includes the burn and build a burn proof for that root

`ethaergo_wallet.aergo_to_eth.build_lock_proof` (*aergo_from: aergo.herapy.aergo.Aergo, w3: web3.main.Web3, receiver: str, bridge_from: str, bridge_to: str, bridge_to_abi: str, lock_height: int, token_origin: str*)

Check the last anchored root includes the lock and build a lock proof for that root

`ethaergo_wallet.aergo_to_eth.burn` (*aergo_from: aergo.herapy.aergo.Aergo, bridge_from: str, receiver: str, value: int, token_pegged: str, gas_limit: int, gas_price: int*) → *Tuple[int, str]*

Burn a minted token on a sidechain.

`ethaergo_wallet.aergo_to_eth.freeze` (*aergo_from: aergo.herapy.aergo.Aergo, bridge_from: str, receiver: str, value: int, gas_limit: int, gas_price: int*) → *Tuple[int, str]*

Freeze aergo native

`ethaergo_wallet.aergo_to_eth.lock` (*aergo_from: aergo.herapy.aergo.Aergo, bridge_from: str, receiver: str, value: int, asset: str, gas_limit: int, gas_price: int*) → *Tuple[int, str]*

Lock can be called to lock aer or tokens. it supports delegated transfers when tx broadcaster is not the same as the token owner

`ethaergo_wallet.aergo_to_eth.mint` (*w3: web3.main.Web3, signer_acct, receiver: str, lock_proof: aergo.herapy.obj.sc_state.SCState, token_origin: str, bridge_to: str, bridge_to_abi: str, gas_limit: int, gas_price: int*) → *Tuple[str, str]*

Mint the receiver's deposit balance on aergo_to.

```
ethaergo_wallet.aergo_to_eth.unlock(w3: web3.main.Web3, signer_acct, receiver: str,
    burn_proof: aergo.herapy.obj.sc_state.SCState, token_origin: str, bridge_to: str, bridge_to_abi: str,
    gas_limit: int, gas_price: int) → Tuple[str, str]
```

Unlock the receiver's burnt balance on aergo_to.

```
ethaergo_wallet.eth_to_aergo.build_burn_proof(w3: web3.main.Web3, aergo_to:
    aergo.herapy.aergo.Aergo, receiver: str, bridge_from: str, bridge_to: str,
    burn_height: int, token_origin: str)
```

Check the last anchored root includes the lock and build a lock proof for that root

```
ethaergo_wallet.eth_to_aergo.build_lock_proof(w3: web3.main.Web3, aergo_to:
    aergo.herapy.aergo.Aergo, receiver: str, bridge_from: str, bridge_to: str,
    lock_height: int, token_origin: str)
```

Check the last anchored root includes the lock and build a lock proof for that root

```
ethaergo_wallet.eth_to_aergo.burn(w3: web3.main.Web3, signer_acct, receiver: str, amount:
    int, bridge_from: str, bridge_from_abi: str, token_pegged: str, gas_limit: int, gas_price: int)
```

Burn a token that was minted on ethereum.

```
ethaergo_wallet.eth_to_aergo.lock(w3: web3.main.Web3, signer_acct, receiver: str, amount:
    int, bridge_from: str, bridge_from_abi: str, erc20_address: str, gas_limit: int, gas_price: int, next_nonce: int = None)
```

Lock an Ethereum ERC20 token.

```
ethaergo_wallet.eth_to_aergo.mint(aergo_to: aergo.herapy.aergo.Aergo, receiver: str,
    lock_proof: web3.datastructures.AttributeDict, token_origin: str, bridge_to: str, gas_limit: int, gas_price:
    int) → Tuple[str, str]
```

Unlock the receiver's deposit balance on aergo_to.

```
ethaergo_wallet.eth_to_aergo.unfreeze(aergo_to: aergo.herapy.aergo.Aergo, receiver:
    str, lock_proof: web3.datastructures.AttributeDict, bridge_to: str, gas_limit: int, gas_price: int) → str
```

Unlock the receiver's deposit balance on aergo_to.

```
ethaergo_wallet.eth_to_aergo.unlock(aergo_to: aergo.herapy.aergo.Aergo, receiver: str,
    burn_proof: web3.datastructures.AttributeDict, token_origin: str, bridge_to: str, gas_limit: int, gas_price:
    int) → str
```

Unlock the receiver's deposit balance on aergo_to.

```
ethaergo_wallet.eth_utils.contract_deployer.deploy_contract(bytecode: str,
    abi: str, w3: web3.main.Web3, gas_limit: int, gas_price: int,
    privkey: bytes, *args)
```

Deploy a new contract to ethereum.

```
ethaergo_wallet.eth_utils.erc20.increase_approval(spender: str, asset_addr: str,
    amount: int, w3: web3.main.Web3, erc20_abi: str, signer_acct,
    gas_limit: int, gas_price: int) → Tuple[int, str]
```

Increase approval increases the amount of tokens that spender can withdraw. For older tokens without the

increaseApproval function in the abi, approval should be set to 0 and then to amount. Newer tokens with increaseAllowance should also be supported

1.9 ethaergo_cli

class ethaergo_cli.main.EthMerkleBridgeCli (root_path: str = '/')

CLI tool for interacting with the EthAergoWallet.

First choose an existing config file or create one from scratch. Once a config file is chosen, the CLI provides an interface to the EthAergoWallet and has the following features: - edit config file settings - transfer assets between networks - check status of transfers - check balances for each asset on each network

check_balances ()

Iterate every registered wallet, network and asset and query balances.

check_withdrawable_balance ()

Check the status of cross chain transfers.

create_config ()

Create a new configuration file from scratch.

This tool registers 2 networks, bridge contracts, paths to bridge abis, a private key for each network and bridge validators

edit_settings ()

Menu for editing the config file of the currently loaded wallet

finalize_transfer ()

Finalize a token transfer between 2 chains.

finalize_transfer_arguments (prompt_last_deposit=True)

Prompt the arguments needed to finalize a transfer.

The arguments can be taken from the pending transfers or inputted manually by users.

Returns: List of transfer arguments

get_registered_assets (from_chain, to_chain)

Get the list of registered assets on each network.

get_registered_networks ()

Get the list of networks registered in the wallet config.

initiate_transfer ()

Initiate a new transfer of tokens between 2 networks.

load_config ()

Load the configuration file from path and create a wallet object.

menu ()

Menu for interacting with network.

Users can change settings, query balances, check pending transfers, execute cross chain transactions

prompt_bridge_networks ()

Prompt user to choose 2 networks between registered networks.

prompt_common_transfer_params ()

Prompt the common parameters necessary for all transfers.

Returns: List of transfer parameters : from_chain, to_chain, from_assets, to_assets, asset_name, receiver

prompt_signing_key (*wallet_name*)

Prompt user to select a private key.

Note: Keys are displayed by name and should have been registered in wallet config.

prompt_transfer_networks ()

Prompt user to choose 2 networks between registered bridged networks.

register_asset ()

Register a new asset and it's pegs on other networks in the wallet's config.

register_bridge ()

Register bridge contracts between 2 already defined networks.

register_key ()

Register new key in wallet's config.

register_network ()

Register a new network in the wallet's config.

register_new_validators ()

Register new validators in the wallet's config.

start ()

Entry point of cli : load a wallet configuration file or create a new one

store_pending_transfers ()

Record pending transfers in json file so they can be finalized later.

`ethaergo_cli.utils.format_amount` (*num: str*)

Format a float string to an integer with 18 decimals.

Example: '2.3' -> 2300000000000000000

`ethaergo_cli.utils.promptYN` (*q, y, n*)

Prompt user to proceed with a transfer or not.

`ethaergo_cli.utils.prompt_aergo_privkey` ()

Prompt user to input a new aergo private key.

Returns:

- name of the key
- address of the key
- encrypted private key

`ethaergo_cli.utils.prompt_amount` ()

Prompt a number of tokens to transfer.

`ethaergo_cli.utils.prompt_bridge_abi_paths` ()

Prompt user to input paths to text files containing abis.

`ethaergo_cli.utils.prompt_deposit_height` ()

Prompt the block number of deposit.

`ethaergo_cli.utils.prompt_eth_privkey` ()

Prompt user to input a new ethereum private key.

Returns:

- name of the key
- address of the key

- path to the json key file

`ethaergo_cli.utils.prompt_file_path(message)`

Prompt user to input a path to a file and check it exists.

`ethaergo_cli.utils.prompt_gas_price()`

Prompt aergo and eth gas price

`ethaergo_cli.utils.prompt_new_asset(networks)`

Prompt user to input a new asset by providing the following: - asset name - origin network (where it was first issued) - address on origin network - other networks where the asset exists as a peg - address of pegs

`ethaergo_cli.utils.prompt_new_bridge(net1, net2)`

Prompt user to input bridge contracts and tempo.

For each contract on each bridged network, provide: - bridge contract address - anchoring periode - finality of the anchored chain

`ethaergo_cli.utils.prompt_new_network()`

Prompt user to input a new network's information: - Name - IP/url - Network type (aergo/eth) - is POA (only needed for ethereum)

`ethaergo_cli.utils.prompt_new_validators()`

Prompt user to input validators

Note: The list of validators must have the same order as defined in the bridge contracts

Returns: List of ordered validators

`ethaergo_cli.utils.prompt_number(message, formator=<class 'int'>)`

Prompt a number.

CHAPTER 2

Indices and tables

- `genindex`
- `modindex`
- `search`

e

- ethaergo_bridge_operator.bridge_deployer,
22
- ethaergo_bridge_operator.proposer.aergo.client,
21
- ethaergo_bridge_operator.proposer.client,
19
- ethaergo_bridge_operator.proposer.eth.client,
19
- ethaergo_bridge_operator.proposer.exceptions,
22
- ethaergo_bridge_operator.validator.server,
19
- ethaergo_cli.main, 26
- ethaergo_cli.utils, 27
- ethaergo_wallet.aergo_to_eth, 24
- ethaergo_wallet.eth_to_aergo, 25
- ethaergo_wallet.eth_utils.contract_deployer,
25
- ethaergo_wallet.eth_utils.erc20, 25
- ethaergo_wallet.eth_utils.merkle_proof,
26
- ethaergo_wallet.wallet, 22
- ethaergo_wallet.wallet_config, 22

A

`aergo_to_eth_sidechain()`
(*ethaergo_wallet.wallet.EthAergoWallet*
method), 22

`AergoProposerClient` (class in
ethaergo_bridge_operator.proposer.aergo.client),
21

B

`build_burn_proof()` (in module
ethaergo_wallet.aergo_to_eth), 24

`build_burn_proof()` (in module
ethaergo_wallet.eth_to_aergo), 25

`build_lock_proof()` (in module
ethaergo_wallet.aergo_to_eth), 24

`build_lock_proof()` (in module
ethaergo_wallet.eth_to_aergo), 25

`burn()` (in module *ethaergo_wallet.aergo_to_eth*), 24

`burn()` (in module *ethaergo_wallet.eth_to_aergo*), 25

`burn_to_aergo()` (*ethaergo_wallet.wallet.EthAergoWallet*
method), 22

`burn_to_eth()` (*ethaergo_wallet.wallet.EthAergoWallet*
method), 22

C

`check_balances()` (*ethaergo_cli.main.EthMerkleBridgeCli*
method), 26

`check_withdrawable_balance()`
(*ethaergo_cli.main.EthMerkleBridgeCli*
method), 26

`create_config()` (*ethaergo_cli.main.EthMerkleBridgeCli*
method), 26

D

`deploy_bridge()` (in module
ethaergo_bridge_operator.bridge_deployer),
22

`deploy_contract()` (in module
ethaergo_wallet.eth_utils.contract_deployer),
25

E

`edit_settings()` (*ethaergo_cli.main.EthMerkleBridgeCli*
method), 26

`eth_to_aergo_sidechain()`
(*ethaergo_wallet.wallet.EthAergoWallet*
method), 22

`ethaergo_bridge_operator.bridge_deployer`
(module), 22

`ethaergo_bridge_operator.proposer.aergo.client`
(module), 21

`ethaergo_bridge_operator.proposer.client`
(module), 19

`ethaergo_bridge_operator.proposer.eth.client`
(module), 19

`ethaergo_bridge_operator.proposer.exceptions`
(module), 22

`ethaergo_bridge_operator.validator.server`
(module), 19

`ethaergo_cli.main` (module), 26

`ethaergo_cli.utils` (module), 27

`ethaergo_wallet.aergo_to_eth` (module), 24

`ethaergo_wallet.eth_to_aergo` (module), 25

`ethaergo_wallet.eth_utils.contract_deployer`
(module), 25

`ethaergo_wallet.eth_utils.erc20` (module),
25

`ethaergo_wallet.eth_utils.merkle_proof`
(module), 26

`ethaergo_wallet.wallet` (module), 22

`ethaergo_wallet.wallet_config` (module), 22

`EthAergoWallet` (class in *ethaergo_wallet.wallet*),
22

`EthMerkleBridgeCli` (class in *ethaergo_cli.main*),
26

`EthProposerClient` (class in
ethaergo_bridge_operator.proposer.eth.client),
19

F

`finalize_transfer()`
(*ethaergo_cli.main.EthMerkleBridgeCli*
method), 26

`finalize_transfer_arguments()`
(*ethaergo_cli.main.EthMerkleBridgeCli*
method), 26

`format_amount()` (in module *ethaergo_cli.utils*), 27

`freeze()` (*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

`freeze()` (in module *ethaergo_wallet.aergo_to_eth*),
24

G

`get_aergo()` (*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

`get_balance_aergo()`
(*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

`get_balance_eth()`
(*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

`get_registered_assets()`
(*ethaergo_cli.main.EthMerkleBridgeCli*
method), 26

`get_registered_networks()`
(*ethaergo_cli.main.EthMerkleBridgeCli*
method), 26

`get_signer()` (*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

I

`increase_approval()` (in module
ethaergo_wallet.eth_utils.erc20), 25

`initiate_transfer()`
(*ethaergo_cli.main.EthMerkleBridgeCli*
method), 26

L

`load_bridge_abi()`
(*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

`load_config()` (*ethaergo_cli.main.EthMerkleBridgeCli*
method), 26

`load_erc20_abi()` (*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

`load_keystore()` (*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

`load_minted_erc20_abi()`
(*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

`lock()` (in module *ethaergo_wallet.aergo_to_eth*), 24

`lock()` (in module *ethaergo_wallet.eth_to_aergo*), 25

`lock_to_aergo()` (*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

`lock_to_eth()` (*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

M

`menu()` (*ethaergo_cli.main.EthMerkleBridgeCli*
method), 26

`mint()` (in module *ethaergo_wallet.aergo_to_eth*), 24

`mint()` (in module *ethaergo_wallet.eth_to_aergo*), 25

`mint_to_aergo()` (*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

`mint_to_eth()` (*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

`mintable_to_aergo()`
(*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

`mintable_to_eth()`
(*ethaergo_wallet.wallet.EthAergoWallet*
method), 23

`monitor_settings()`
(*ethaergo_bridge_operator.proposer.aergo.client.AergoProposerC*
method), 21

`monitor_settings()`
(*ethaergo_bridge_operator.proposer.eth.client.EthProposerClient*
method), 20

`monitor_settings_and_sleep()`
(*ethaergo_bridge_operator.proposer.aergo.client.AergoProposerC*
method), 21

`monitor_settings_and_sleep()`
(*ethaergo_bridge_operator.proposer.eth.client.EthProposerClient*
method), 20

P

`prompt_aergo_privkey()` (in module
ethaergo_cli.utils), 27

`prompt_amount()` (in module *ethaergo_cli.utils*), 27

`prompt_bridge_abi_paths()` (in module
ethaergo_cli.utils), 27

`prompt_bridge_networks()`
(*ethaergo_cli.main.EthMerkleBridgeCli*
method), 26

`prompt_commun_transfer_params()`
(*ethaergo_cli.main.EthMerkleBridgeCli*
method), 26

`prompt_deposit_height()` (in module
ethaergo_cli.utils), 27

`prompt_eth_privkey()` (in module
ethaergo_cli.utils), 27

`prompt_file_path()` (in module
ethaergo_cli.utils), 28

`prompt_gas_price()` (in module
ethaergo_cli.utils), 28

prompt_new_asset()	(in module	unlock() (in module ethaergo_wallet.aergo_to_eth), ethaergo_cli.utils), 28 24
prompt_new_bridge()	(in module	unlock() (in module ethaergo_wallet.eth_to_aergo), ethaergo_cli.utils), 28 25
prompt_new_network()	(in module	unlock_to_aergo() (ethaergo_wallet.wallet.EthAergoWallet method), 24
prompt_new_validators()	(in module	unlock_to_eth() (ethaergo_wallet.wallet.EthAergoWallet ethaergo_cli.utils), 28 method), 24
prompt_number()	(in module ethaergo_cli.utils), 28	
prompt_signing_key()	(ethaergo_cli.main.EthMerkleBridgeCli method), 26	unlockeable_to_aergo() (ethaergo_wallet.wallet.EthAergoWallet method), 24
prompt_transfer_networks()	(ethaergo_cli.main.EthMerkleBridgeCli method), 27	unlockeable_to_eth() (ethaergo_wallet.wallet.EthAergoWallet method), 24
promptYN()	(in module ethaergo_cli.utils), 27	update_t_anchor() (ethaergo_bridge_operator.proposer.aergo.client.AergoProposerClient, method), 22
ProposerClient	(class in ethaergo_bridge_operator.proposer.client), 19	update_t_anchor() (ethaergo_bridge_operator.proposer.eth.client.EthProposerClient, method), 20
R		update_t_final() (ethaergo_bridge_operator.proposer.aergo.client.AergoProposerClient, method), 22
register_asset()	(ethaergo_cli.main.EthMerkleBridgeCli method), 27	update_t_final() (ethaergo_bridge_operator.proposer.eth.client.EthProposerClient, method), 20
register_bridge()	(ethaergo_cli.main.EthMerkleBridgeCli method), 27	update_unfreeze_fee() (ethaergo_bridge_operator.proposer.aergo.client.AergoProposerClient, method), 22
register_key()	(ethaergo_cli.main.EthMerkleBridgeCli method), 27	update_validators() (ethaergo_bridge_operator.proposer.aergo.client.AergoProposerClient, method), 22
register_network()	(ethaergo_cli.main.EthMerkleBridgeCli method), 27	update_validators() (ethaergo_bridge_operator.proposer.eth.client.EthProposerClient, method), 20
register_new_validators()	(ethaergo_cli.main.EthMerkleBridgeCli method), 27	V
run()	(ethaergo_bridge_operator.proposer.aergo.client.AergoProposerClient method), 22	wallet.MajorityError, 22
run()	(ethaergo_bridge_operator.proposer.eth.client.EthProposerClient method), 20	W
S		wait_next_anchor() (ethaergo_bridge_operator.proposer.aergo.client.AergoProposerClient, method), 22
start()	(ethaergo_cli.main.EthMerkleBridgeCli method), 27	wait_next_anchor() (ethaergo_bridge_operator.proposer.eth.client.EthProposerClient, method), 21
store_pending_transfers()	(ethaergo_cli.main.EthMerkleBridgeCli method), 27	U
unfreeze()	(ethaergo_wallet.wallet.EthAergoWallet method), 23	
unfreeze()	(in module ethaergo_wallet.eth_to_aergo), 25	
unfreezeable()	(ethaergo_wallet.wallet.EthAergoWallet method), 24	