Optimistic OmniBridge

Introduction

Cross-chain communication is a critical aspect for projects extending main blockchain platforms. While the basic types of bridge solutions for chain interoperability have been previously described by researchers, the blockchain developer community is continuing to explore approaches more suitable and convenient for particular chains.

This document considers an innovative way for building a hybrid two-way bridge between two blockchains. Optimistic withdrawals are possible when the sister chain is based on a POS consensus and deposits are confirmed using a notary scheme with a set of bridge validators. This model assumes less stringent requirements for deposits; an optimistic light client as described in "Si-o-Se: Optimistic Cross Chain Bridges" by @barryWhiteHat may be implemented, but is beyond the scope of this outline.

Definitions

We use the following definitions and components:

1. The main chain is the Ethereum Mainnet, a chain with higher security and higher user expectations for decentralization of operations in a trustless environment.
2. The sister chain is an EVM compatible chain based on a POS consensus. An example is the xDai chain which uses POSDAO consensus. The max bound for number of validators, a POSDAO feature, is critical for this implementation.
3. The bridge contracts are EVM contracts deployed on both chains. The user will directly or indirectly interact with the contracts to deposit or withdraw funds from the bridge. POS validators will have the opportunity to challenge withdrawal requests in the contract on the main chain. Bridge validators will provide their deposit confirmations to the contracts on the sister chain.
4. Deposits are defined as user requests to transfer any ERC20 compatible token to the sister chain. Withdrawals are requests to return previously deposited ERC20 tokens back to the main chain. Since any ERC20 compatible token (and potentially tokens that follow EIP721 or EIP1155 specifications) can be deposited and then withdrawn, the bridge is called OmniBridge.
5. The bridge validators run oracles that monitor the main chain to confirm token deposits in the sister chain.
6. The POS validators run nodes with dual roles: participation in POS consensus and monitoring the main chain for withdrawal claims.

High Level Details

Deposit

The deposit operation requires the user to perform a direct or indirect (via transferFrom

) transfer of tokens to the bridge contract on Ethereum. This operation locks the tokens on the bridge. The tokens can later be unlocked with a withdrawal request.

After a deposit operation is initiated:

1. The bridge contract on the main chain emits an event.
2. The bridge validator oracles wait for chain finalization.
3. The oracles catch the event and send confirmations to the bridge contract on the sister chain.
4. As soon as enough signatures are collected by the contract on the sister chain, it sends a message to the token contract on the sister chain to mint the corresponding amount of tokens.

Withdrawal

[

withdrawals

1400×735 142 KB

](https://ethresear.ch/uploads/default/original/2X/0/0a8831f57d1c0dac0ccd68a0534385d1da277bdf.png)

The optimistic withdrawal consists of three user actions and, in the most common case, does not require any transaction

from POSDAO validators.

1. A user sends tokens to the bridge contract on the sister chain. The tokens are burnt. The contract emits an event with a unique ID. If several different tokens are sent to the contract in the same transaction, unique IDs are generated for each token. The ID is the hash of the following data: token sender

, token address

, value

, block number

, nonce

, where nonce

is the number of the burn operation for the specific token and the specific sender.

1. A user claims the tokens on the main chain side by sending the sister chain block number, the token address, and the value to the bridge contract on the main chain. Some fixed bond in ether (e.g. 1 ETH) is also sent as part of the claim request.
2. This transaction starts a timer (e.g. 24 hours) on the bridge contract and it emits the claim request ID calculated from the received information, the sender address, and expected nonce.
3. The event is caught by the POSDAO validators and they use the ID to discover whether the tokens were burnt on the sister chain.
4. If the ID is not found, the POSDAO validators can send a reject message to the bridge contract on the main chain. The reject message contains a merkle path proving the validator is a member of the current POSDAO validator set. If N of M rejections is discovered, the claim request is cleared. The bond is distributed among all of the POSDAO validators.
5. If the claim request is not rejected by the validators within 24 hours following the claim request, the user sends another request to the bridge contract on the main chain. The tokens are unlocked and the bond is returned to the user.

POSDAO validators set synchronization

POSDAO consensus assumes that the set of validators changes one time per week. The validator set change in the sister chain happens in multiple phases:

- Phase One: a new validator set is proposed, and the merkle root of the validator set is calculated.
- Phase Two: the current validators produce new blocks confirming they agree with the proposed set. In addition, each validator in the current set submits a signature to the sister chain for a message containing the block number where the proposal was raised, the block number when the proposed validator set will end, and the merkle root.
- Phase Three: As soon as 50%+1 validators from the current set produce the block, the proposal is considered finalized, and the next block is produced by a validator from the new set.

As soon as the required amount of signatures have been collected by the current validator set, anyone can submit the proof containing the new validator set to the bridge contracts on the main chain.

The bridge contracts recover addresses from the signatures provided as part of the proof and build the merkle root. The merkle root must match the previous root to apply the new validator set.

Due to nature of POSDAO consensus the following situations could occur:

1. 50% of validators fail to send their reject messages in 24 hours for a particular claim request. This could occur if they were off-line for some reason. This is a critical situation and social recovery (see below) should be used to cease bridge operations and apply a new POSDAO validator set. The new validator set will be able to complete the rejection of the claim.
2. A fraudulent claim request occurs during validator set synchronization; new validators send their reject messages prior to synchronization and are not recognized as valid rejectors. This is not a critical situation for the bridge. The new validators will re-send the reject messages as soon as the new validator set is synchronized.

Two claim timer components can preserve funds if a fraudulent claim is sent and one of the situations described above occur:

1. Every rejection sent by a POSDAO validator increases the timer to complete the claim. The increase is non-linear. For example, a single rejection will result in a transaction claim completion of 25 hours, but 9 rejections will increase the completion time to 1 week.

2. If the claim is sent to the bridge contracts after the current validator set is scheduled to expire, the claim completion time is increased to 36 hours. Once the new validator set appears in the contract, it is reduced back to 24 hours. If the new validator set does not appear, new claims start timers for greater values. For example, if the old validator set expired 24 hours ago, the new expiration timer is 48 hours, if the validator set expired 48 hours ago, the timer is 72 hours and so on.

Social recovery

A social recovery mechanism will be available for emergency use. This is a common practice of last resort, and can be used if there is a POSDAO validator set synchronization failure.

Social recovery works similar to a multisig where 5 of 9 community participants can execute a limited number of actions with the bridge contract.

Future directions

1. The suggested model provides more opportunities for implementation with chains that don't support the EVM. In these cases, Ethereum Mainnet interoperability with other chains can be achieved with less effort.

2. When a claim is completed by the user in the main chain, the bridge contract holds some amount of tokens as a bridge exit fee. The fee is then distributed among the current set of POSDAO validators. A fee exemption can be implemented for a user who participates in the validator set synchronization process.

3. The existing TokenBridge using the notary scheme could be still involved in the withdrawal process for users who wish to use 'almost' instant asset transfers from the sister chain and have no funds to provide the bond as part of the claim request described above.

Summary

Above we proposed a new approach to chain interoperability when one of the involved chains is based on a POS consensus. This new type of bridge is based on an optimistic scheme. Users are able to withdraw and claim assets completely independently while the POS chain validators act as claim challengers. Due to the nature of claim requests and the mechanism used for POS validators synchronization, the suggested bridge is a "green" solution which optimizes gas and storage requirements without compromising the security of user operations.