Introduction

This post aims to deepen the understanding of the optimistic bridge structure idea and spark discussions about its current bottlenecks and potential solutions.

The Optimistic bridges, inspired by the design of optimistic rollups, rather than requiring Ethereum to validate every bridge transaction, the protocol inspects only those that might be fraudulent. Suspicious activity can lead to a dispute, triggering a verification process settled by Layer 1.

Mechanism

Network participants

Optimistic bridge consists of three participants - user, relayer and disputer.

- Users: wish to move tokens from one network to another through the bridge.
- Relayers: accommodate user's requests and facilitate bridge transfer on user's behalf.
- Disputers: raise alerts and initiate challenges when noticing a suspicious action by a relayer, such as running away with the tokens deposited by the user or transferring an incorrect amount.

The protocol's decentralized nature allows anyone to act as a user, relayer, or disputer.

Specific

*The token transfer and dispute processes of optimistic bridges can differ based on the involved layers.

Default

1. Relayers deposit their liquidity for facilitating transfers into a contract deployed on the destination network, along with a certain percentage of the liquidity as a bond, which will be seized when they misbehave.
2. A user sends tokens to an escrow contract on the source chain, triggering a request to the relayers.
3. If a relayer accepts this request, they directly send the tokens to the requester's address on the destination network.
4. The relayer generates a proof for transferring the tokens, derived from the transaction hash, and registers it with the escrow contract mentioned in step 2, which allows the relayer to withdraw the assets that the user deposited.

[

default

1840×840 66.3 KB

](https://ethresear.ch/uploads/default/original/2X/b/b18db19ab319f409ad7834a2138a707bc7617b36.png)

In the event of fraud

1. A disputer initiates a verification process by highlighting the relayer's alleged misconduct and depositing a predetermined amount of assets as a bond to the protocol.
2. To vindicate themselves, the accused relayer is required to submit evidence for the valid transaction within a given timeframe.
3. If the provided evidence clears the relayer — meaning the disputer's claim is unfounded — the bond deposited by the disputer will be slashed as a penalty and sent to the relayer.
4. Conversely, if the relayer fails to present valid evidence in the allotted time, the relayer's bond (referenced earlier in the token transfer process) will be slashed and divided between the disputer and the user. Additionally, the disputer can reclaim the bond they initially posted.

[

fraud

1839×840 87.7 KB

](https://ethresear.ch/uploads/default/original/2X/e/e3c78e87bdf2d8480068c4eb5d84320cc641cfcf.png)

Advantages

Enhanced Security

The optimistic bridge architecture's key advantage is enabling "fragmented liquidity," especially through the integration of the relayer role.

In optimistic bridges using a distributed relayer model, each relayer can establish their own liquidity pool, containing only assets they are willing to commit for bridge transactions. This results in a bridge infrastructure made up of several isolated liquidity pools. This design is notably different from traditional liquidity-based bridges where liquidity providers pool their assets into one centralized pool, holding the entire protocol's assets.

From a security perspective, such centralized systems are perceived as a low-hanging fruit for hackers because a single breach could provide access to the entire protocol's assets. On the other hand, the fragmented liquidity inherent in optimistic bridges reduces the attractiveness for potential attackers because the potential profit an attacker could reap is limited only to the assets a specific relayer has allocated, often making the intrusion attempt unjustifiable due to the diminished return on effort.

For the protocol, this decentralized liquidity structure serves dual purposes: it not only acts as a deterrent against malicious entities by offering minimal incentives but also confines any potential damage. Should one pool fall victim to a breach, the rest remain unscathed. Plus, the simplicity in implementing this structure makes security checks more straightforward.

The others

Besides that, there are several other advantages of an optimistic bridge.

In optimistic bridges, stakeholders are incentivized through the previously discussed bond/slash system. This enables transactions to be processed in an optimistic manner, bypassing the need for regular Layer 1 verifications unless a suspicious behavior is detected. This procedural efficiency substantially reduces gas fees for end users.

Moreover, the architectural design of optimistic bridges allows for an intentional imbalance in processing load between Layer 1 and Layer 2. As detailed in the mechanism section, it's feasible to delegate more processing responsibilities to Layer 2, minimizing interactions with Layer 1, ultimately leading to cost savings for users.

In addition, optimistic bridges significantly accelerate transaction speeds. This boost is achieved as relayers, incentivized by a portion of the user-paid protocol fee, are motivated to act swiftly, especially since transactions are processed on a first-come-first-served basis. Additionally, the direct interaction between users and relayers through their EOA minimizes the need for intermediary smart contracts, further speeding up the process.

Bottleneck

The architecture of the optimistic bridge is a relatively recent innovation that presents several challenges that need to be addressed. One of the most significant challenges is the so-called "256 problem." This issue arises from the fact that smart contracts can only query the block hashes of the most recent 256 blocks using the BLOCKHASH opcode.

More details on the bottleneck will be done in the next post to separate the discussion topics. (I will link to it when I post it.)