HackMD mirror: On The Trustedness of Cryptoeconomic Bridges - HackMD

The past year has seen the rise of several different bridge

designs: mechanisms to move assets from one blockchain to another. In this post we analyze one class of bridge design—cryptoeconomic bridges—and argue that they are not trust-minimized.

Background

Prerequisite Reading

- Building Scalable Decentralized Payment Systems, Adler et al.
- Nakamoto Consensus Requires Social Coordination and Subjectivity, Adler
- tBTC: A Decentralized Redeemable BTC-backed ERC-20 Token, Keep Network
- ETH-NEAR Rainbow Bridge, Zavershynskyi
- Minimal Viable Merged Consensus, Adler
- Trustless Two-Way Bridges With Side Chains By Halting, Adler et al.
- XCLAIM: Trustless, Interoperable Cryptocurrency-Backed Assets, Zamyatin et al.

Bridges

In the context of blockchains, a bridge

is a mechanism for moving assets from one blockchain to another—otherwise completely unrelated—blockchain. A two-way

bridge is a mechanism for moving an asset to and

from one blockchain and another, and is of especial interest as it would allow interactions across chains in both directions. Given that a two-way bridge can be implemented as two one-way bridges, we will reserve our analysis to the latter.

We define the primary

as the chain from which the bridged asset originates and the secondary

as the chain to which the bridged asset is sent.

Cryptoeconomic Bridges

A cryptoeconomic bridge

is a bridge where some attesting party (or parties) progresses the bridge. This party is bonded and may be penalized in case user assets are stolen from the bridge, i.e. through creating a false attestation of some event on the primary. This potentially includes the block producer set of the primary, e.g. for bridges based on on-chain light clients.

Trust Analysis of Layer-1 Blockchains

We note that in a layer-1 blockchain using Nakamoto Consensus, a re-organization or invalid block by miners will result in a temporary disruption of the chain, but no user funds can be stolen. Indeed, with social coordination (which is required for Nakamoto Consensus regardless), even re-org or censorship attempts beyond a certain depth will be ultimately unsuccessful.

Layer-1 blockchains using stake-based consensus protocols codify this mechanism of social recovery throughaccountable safety, where any attack will have at least \frac{1}{3}

of stake identifiably accountable. This accountable stake can be burned through social coordination.

Putting the above together, the cost to attack a layer-1 blockchain is therefore the cost to disrupt it, not

to cost to steal user funds (which is impossible). As a consequence, the total value of user funds on a layer-1 blockchain can far exceed the cost to attack it in a way that forces social recovery.

Trust Analysis of Cryptoeconomic Bridges

Bridges (including crypteconomic bridges) differ from layer-1 blockchains. Let us consider the most extreme case (i.e. safest)

where the bonded attesting party is the entire primary's block producer set.

If the total value of assets in the bridge exceeds the attesting party's bond (in this case, up to 2/3 of the block producer stake on the primary), the attesting party can simply make an invalid attestation and steal all assets in the bridge. Social recovery through coordination on the primary cannot recover the assets, which are now on the secondary (or could have been sold once on the secondary).

This trust profile is not trust-minimized, as even on penalizing misbehavior, users are not compensated for their loss of assets. In addition, it requires the total asset value to be strictly smaller than the bond, which is capital inefficient.

Trust-Minimized Two-Way Bridges

Trust-minimized one-way bridges can be implemented quite easily through sidechains, i.e. where the secondary fully validates the primary's consensus rules. Trust-minimized two-way bridges are more challenging.

Optimistic rollups (originally proposed by Adler) and ZK rollups (originally proposed by Whitehat) are promising avenues for building trust-minimized two-way bridges through the use of fraud proofs and validity proofs, respectively. However, both rollup techniques require the two chains to share a data availability layer (the minimum requirement for what is called shared security

). To that end, LazyLedger provides an optimally scalable general-purpose data availability layer.

Conclusion

We present an overview of cryptoeconomic bridges, and argue that they are not trust-minimized. Specifically, they have strictly stronger trust assumptions than using either

layer-1 blockchain, as the bridge enables user funds to be stolen, which is impossible for a layer-1 blockchain.