Tldr:

We are proposing a new kind of roll-ups that can reverse and recover from serious failures, such as bugs in smart contracts, all without relying on multi-signatures.

Motivation:

Cryptocurrency technology embodies the principle that “code is law,” establishing a transparent and open system for financial transactions. However, this “code” is not infallible, and sometimes unforeseen bugs and challenges emerge, potentially resulting in substantial financial losses.

To operate under normal conditions with the crypto ethos, but still address this weakness, we propose the development of forkable, reversible roll-ups that allow for the reversal of problematic transactions without depending on central trusted entities. These roll-ups enable creating a system that can essentially “undo” errors and thereby protect users and their assets.

Design:

Design Idea:

Every user holding an RWA trusts the RWA issuer. This roll-up construction facilitates this existing trust to enable state reversals for hacked contracts.

Forkable Roll-up:

In simple terms, a forkable roll-up is a roll-up with the ability to fork itself: it can create a copy of itself to isolate and address issues without affecting the original chain. To do so, the original chain splits into two paths, each operating independently with their own unique identifiers (chain IDs) and continuing to record their own transactions. One fork will have a modified state - with a deployed fix for a bug - while the other fork will be the normal chain. Users can choose freely which fork to adopt: Either the one with a state update or without.

The value of each fork can then be assessed based on trading activities in the primary layer (L1), helping users to identify the more valuable option between the two.

Forkable Roll-up bridges:

There are two kinds of bridges for forkable roll-ups:

1. **Majority Chain Bridge:**

This bridge works like a normal L2 bridge and can hold any assets. After a fork, it automatically sends assets to the new fork’s bridge of the chain with the highest value.

1. **Real World Asset bridge:**

RWA will be bridged into a forkable roll-up by a bridge from L1 with an owner - ideally the RWA issuer. After a fork, the bridge will send the funds to the new child bridge of the fork that is chosen by the owner of the bridge. It is expected that the owner will send the funds to the chain with the higher marketcap, unless an attack is started against the open interest of the chain. If the owner is the RWA issuer, there is no additional trust assumption for a user.

With these definitions, we can define a reversible forkable roll-up:

Reversible forkable roll-ups:

Reversible forkable roll-ups are roll-ups that are able to recover from severe smart contract issues. They will fork each time a hack has repercussions beyond a certain threshold measured in dollars.

Then they go through two phases:

Phase 1: Containment fork:

Bots are proposing a fork that contains the hack: E.g. they set the state of the chain to the state right before the hack and freeze the vulnerable contracts - maybe by setting the bytecode of the affected contracts to zero. This will prevent the hack + restore all funds that are not yet bridged away from the chain - which can be prevented by having a delayed bridge. These forks can be triggered by bots automatically and hence are initiated quickly (only some blocks after the attack). Users can

then choose the most promising containment fork and use it for their business needs.

Phase 2: Resolution fork:

These forks will unfreeze the vulnerable contract and replace it with a fix. This for sure is much harder to organize than a containment fork and will take more time and coordination. However, it should eventually happen for each containment fork. Again users will have the choice of which fork they actually follow and RWAs issuers will likely follow the chain with the highest market value.

Analysis:

The presented roll-up builds a framework that allows to change the state in a trustless - non-multisig - manner with the following assumptions:

- Assumptions for assets in the Real World Asset bridge: Assuming the users are trusting their RWA issuer - this trust is required for any RWA - and this issuer controls the bridge, then the only additional trust in this construction taken by each user is that the RWA issuer is technically and legally able to choose the right fork for representing their RWA after a fork. In most cases this act of choosing a fork should be trivial: The market will likely decide which chain should be picked by forking and trading the forked native tokens on L1. The issuer only needs to read the onchain price and pick the fork with the higher valuation. Only in unexpected situations the market could fail and RWA issues would have to investigate the situation more deeply. But even a “wrong choice” by the issuer is not in all cases fatal as users in most situations withdraw the RWA assets to L1 from any fork.
- Assumptions for assets in the Majority Chain Bridge: For anyone holding non-forkable L1 native assets in the forkable chain that are deposited via majority-chain-bridge, there are also economic incentives securing their assets as long as the value of all the deposited L1 native tokens is less than the market cap of the native token in L2. If the L1 native assets are less valuable than the L2 native token, then the cost of manipulating the value of the L2 forks is - in a market with perfect information - higher than any potential gains from stealing L1 tokens and thereby not worth any profit-oriented attacker.