Feasibility Study - Data Availability with Validation on Cardano

Sky Protocol Team

2024-09-27

Overview

This report addresses milestone 1 of the Sky Protocol: Data Availability for Cardano Layer 2 Solutions proposal.

Maintenance of Unique Identifiable Contract State

For the maintenance of unique identifiable contract state, we will use NFT-based oracles, similar to the example from the Plutus Pioneer Program.

Each data topic will be associated with an NFT that stores the root hash as its datum.

Off-chain code will be used to find the NFT UTXO.

Multisig for Data Availability Committee

Initially, we will use a simple M-of-N multisig based on Ed25519 signatures.

A configurable number of data operators will be required to sign hashes.

In the future we might use Schnorr signatures.

Merkle Proof of Data Availability

We will use the usual Merkle membership proof approach.

The hashes of the path segments from the root to the leaf node in question (and of required sibling nodes) is signed.