Feasibility Study - Data Availability with Validation on Cardano

Sky Protocol Team

2024-09-27

Overview

Sky Protocol is committed to constructing a tailored Data Availability Solution aligned with the requirements of Cardano. Our approach involves publishing data in a format conducive for Cardano smart contracts to seamlessly validate and integrate into Layer 1 contracts. Rooted in Cardano and underpinned by its own Cardano-based token, our network reduces reliance on external networks and minimizes trust assumptions. Our network enables multiple Cardano-based DApps to leverage the same Data Availability network, thus pooling resources and capital for network validation.

This report addresses Project Catalyst 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 for reduced size.

Merkle Proof of Data Availability

We will implement the usual Merkle membership proof approach in Plutus.

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