Address-Bound NFTs on Cardano

Minting unique tokens with a shared `PolicyId`

Lorenzo Fanton - 887857@stud.unive.it

Native Tokens

Native tokens, also called *assets*, are defined as:

- $\mathrm{AssetId} := \mathrm{PolicyId} \times \mathrm{AssetName}$
- $\mathrm{PolicyId} := (\mathbb{F}_{256})^{28}$ (hash of the minting validator script)
- $\mathrm{AssetName} := (\mathbb{F}_{256})^{32}$ (arbitrary string)

Where $\mathbb{F}_q := \{0, \ldots, q-1\}$.

Spending Validators

We call V the type of a Spending Validator:

$$V := (\mathcal{D} \times \mathcal{R} \times \mathcal{C}) \to \mathbb{B}$$

Where $\mathcal{D}$ is the type of a Datum, $\mathcal{R}$ is the type of a Redeemer and $\mathcal{C}$ is the type of a ScriptContext.

Minting Validators

We call M the type of a Minting Validator:

$$M := (\mathcal{R} \times \mathcal{C}) \to \mathbb{B}$$

NB: Minting Validators do not take Datums as inputs.

Clustering With Graph Similarities

$$newm : (\Sigma^{32} \times \mathcal{O}) \to M$$

$$addv : (M \times \Sigma^{32} \times M) \to V$$

$$addm : (M \times \Sigma^{32}) \to M$$

$$\begin{cases} (A\mathbf{x})_i = \mathbf{x}^\top A\mathbf{x} & i \in \sigma(\mathbf{x}) \\ (A\mathbf{x})_i \leq \mathbf{x}^\top A\mathbf{x} & i \notin \sigma(\mathbf{x}) \end{cases}$$

Examples

$$DS(\ , \sigma = 100, \epsilon = 0.0001, \theta = 0.3, k = 2) \mapsto$$

$$DS(\ , \sigma = 100, \epsilon = 0.001, \theta = 0.4, k = 3) \mapsto$$

$$DS(\ , \sigma = 100, \epsilon = 0.001, \theta = 0.1, k = 3) \mapsto$$

$$DS(\ , \sigma = 100, \epsilon = 0.001, \theta = 0.08, k = 1) \mapsto$$