Agora DRep Effect Specification

Tomasz Maciosowski
tomasz@mlabs.city

Gergely Szabó
gergely@mlabs.city

Abstract

DAOs that have large treasuries of ADA tokens under their control cannot use that to directly participate in Cardano-level protocol governance introduced in the Chang hard fork. They would need to delegate their stake to a dRep and rely on them as a centralized party that should reflect the values of the whole organization. Instead, we propose to create a dRep onchain validator. DAOs should be able to delegate their treasuries to dRep validators that they directly control. Using Agora proposals, organization members will be able to decide how their DAO will vote instead.

1 Overview

This document provides a specification of a set of Cardano validators that together provide Agora effect that allows DAO members to use Agora voting system to decide how they want to act on Cardano-level governance proposal together as an organization. Plutus V3 script can be registered as a Cardano DRep and we will use that to create a Plutus DRep that will allow voting on Cardano proposals only after the organization has passed a successful "internal" vote on that decision using their Agora instance. First iteration of the DRep Effect will be limited in governance actions it is allowed to do only to voting, i.e. it will not be able to create Cardano governance proposals. The implementation of this specification will be done in Plutarch and available on GitHub.

1.1 V2 / V3 Interactions Limitations

The Cardano ledger imposes limitations on what transaction can do depending on which versions of Plutus scripts are being executed in the same transaction. The limitation that is relevant for us is that transactions that execute V2 Plutus scripts cannot also contain Cardano governance voting actions (see 1).

Feature	Plutus V2	Plutus V3	Plutus V2 + V3
Plutus V1 Primitives	Yes	Yes	Yes
Governance Voting	No	Yes	No

Table 1: Part of Cardano Script Compatibility Chart

The Plutus V2 script in question is the minting policy of the Governance Authority Tokens (GAT) of already deployed Agora instances. It is important for organizations to continue using

their current Agora instances so rather then requiring them to re-deploy Agora using Plutus V3 we will provide a GAT migration mechanism - a proxy validator that will convert GATs from V2 to V3 on demand. More over the migration mechanism is separate from the voting effect thus may be used for other effects that need access to transaction features that were introduced after Plutus V2.

2 Validators

2.1 Proxy Spending Validator

Plutus V2 Agora instances can use this validator to use effects that are implemented in newer Plutus versions. To do so instead of specifying actual effect in the proposal datum the user can specify this validator instead and specify the final V3 GAT destination using datum of the Proxy Spending Validator. As a security measure the datum allows only for script destinations to make sure that GAT never reaches a public key address as it may compromise the whole Agora system. Proxy Spending Validator is parametrized by the real Agora Governance Authority Token symbol and allows for spending only if it's UTxO contains that GAT and the transaction burns it.

Note that the actual minting will be done by Proxy Minting Validator. While they are described as two separate validators actually they will be the same onchain script that acts differently depending on the purpose it is spent with. That approach avoids circular script parametrization as minting part needs to know the address of the spending part and spening part needs to know the currency symbol of the minting part, if they are implemented in the same script that then the script hash is the same and it is passed as a runtime parameter from Cardano node.

Data Types

```
data Datum = Datum
  { receiverScript :: ScriptHash
  , datumHash :: DatumHash
  }
```

Spending Conditions

- Transaction burns one GAT (symbol is known from script parameter)
- Spent UTxO contains GAT
- Transaction creates a UTxO at address of `receiverScript` with empty staking part and reference datum with hash equal to `datumHash`.

2.2 Proxy Minting Validator

2.3 Voting Effect Validator

The Voting Effect validator will utilise the above established Proxy Minting Validator, minting a Proxy Governance Authority Token (pGAT). By spending the pGAT, we essentially get the same guarantees as with GAT, but we can use Plutus V3, which introduces the functionalities to work with native Cardano governance.

In order to vote on a Cardano Governance Action using this effect the following preconditions must be met:

- The Voting Effect validator must be registered as a DRep
- staking verification key of the DAO should be delegated to the above DRep
- Governance action with well known id must be already submitted on-chain

The effect transaction will burn exactly one pGAT, and at the same time place a vote to the governance action defined in the datum.

DRep registration

Registering the Voting Effect validator is a one time action, that has to be done after deployment of the protocol. The validator script will allow DRep registration unconditionally, but DRep update will be prohibited.

Data Types

```
data Datum = Datum
  { governanceActionId :: GovernanceActionId
  , vote :: Vote
  }
```

Spending Conditions

- Transaction burns exactly 1 pGAT (symbol is known from script parameter), and doesn't mint anything
- Spent UTxO contains pGAT
- `ScriptPurpose` is either `Certifying` or `Voting`
  - if `Certifying`
    - `ScriptContext` does not contain a vote
    - `ScriptContext` contains exactly 1 transaction certificate
  - if `Voting`
    - `Voter` set to a `DRepCertificate` with the script hash of this validator
    - `ScriptContext` contains exactly 1 vote, where the `Voter` matches the one in the `ScriptPurpose`, and the `GovernanceId` and `Vote` match the ones in the Datum
    - `ScriptContext` does not contain a certificate
- `ScriptContext` does not contain proposal procedures
- `ScriptContext` does not contain treasury donations