KubeCoin minting audit - report

2022-06-22 - MLabs

Ref: 220622-KubeCoin-Minting-Audit-V2

Table of Contents

Summary

The following document represents an MLabs audit for the correct minting of the Cardano native asset with policy ID:

`a26022096c6a8052987dabbfa94849ab7886cf0bb7840044e017d5be`

Name:

`KubeCoin` (`4b756265436f696e`).

Throughout the document, this asset is called the "*KubeCoin token V2*".

Previous Audit

MLabs previously audited the correct minting of 480 million (`480,000,000`) Cardano native asset with policy ID:

`362706e09f908e1470b90278cb50bcd834b4c2f8d489431a8965ddb8`,

name:

`KubeCoin` (`4b756265436f696e`).

Throughout the document, this asset is called the "*KubeCoin token*".

Assumptions

The trustworthiness of the claims made by this report rely on the correct implementation of the multi-signature language and the Cardano command-line interface by IOG, as well as the veracity of the data displayed by third-party tools like the API Blockfrost or alternatively the Cardanoscan blockchain explorer.

Analysis

The minting policy of a Cardano native asset specifying the conditions under which tokens can be minted or burnt can be defined using multi-signature scripts (also called simple scripts). Transfer logic and other related functionality is built into the Cardano ledger itself. Therefore, no Plutus scripts are needed to safely create new assets and interact with them.

The *KubeCoin token V2* policy ID:
`a26022096c6a8052987dabbfa94849ab7886cf0bb7840044e017d5be`
corresponds to the hash of the following script:

```
{
  "type": "all",
  "scripts":
  [
   {
      "type": "before",
      "slot": 64333187
   },
   {
      "type": "sig",
      "keyHash": "070612e1fa88ec5a6f4b30777ecc404511442591ccccca3b6238cae7"
   }
  ]
}
```

This can be checked with the Cardano command-line interface (Cardano CLI) by running the following command:

```
> cardano-cli transaction policyid --script-file <FILE>
```

where `<FILE>` is the filepath of the script.

The minting policy establishes two conditions that must be met in order to allow the minting or burning of a KubeCoin token:

- The upper bound of the transaction validity interval must be lower than slot number `64333187`
- The transaction must be signed by the key corresponding to the public key hash `070612e1fa88ec5a6f4b30777ecc404511442591ccccca3b6238cae7`.

The current slot of the Cardano blockchain can be checked by running the following command in the CLI:

```
> cardano-cli query tip --mainnet
```

At the time of writing this report, the current slot number is `7415739`, which is already past slot `64333187`. This means that no more *KubeCoin tokens V2* can be minted or burnt. Therefore, the total supply of *KubeCoin tokens V2* that will ever be in existence can be computed by aggregating the total number of minted tokens to date and subtracting the amount of tokens burnt.

Querying the blockchain, it can be checked that there is only one transaction minting *KubeCoin tokens V2* and no transactions burning them. The transaction with hash:

`f8bfda3d0c0251fedd853a7c8114490587a057189d64241d43a954e225090d32`,

included in block number:

`7407494`,

mints:

`480,000,000.000000` KubeCoin (*KubeCoin tokens V2)*

in Absolute Slot:

`64323291`

and sends them to the address:

`addr1vxlpa2jgg9tfclxymqp0v29s9mmw6de8exzn9tlm53d7lmgxstqmw`.

The public key hash of the address used to pay for the fees and minimum ADA and receive the tokens is:

`Addr1vxlpa2jgg9tfclxymqp0v29s9mmw6de8exzn9tlm53d7lmgxstqmw`

`61be1eaa4841569c7cc4d802f628b02ef6ed3727c98532affba45befed`,

different from the public key hash mentioned in the minting policy. This poses no problem at all, since the key corresponding to the public key hash

`070612e1fa88ec5a6f4b30777ecc404511442591cccca3b6238cae7`

is only needed as a witness, i.e. must sign the transaction, with no further requirements.

Found issues

1. Previous minting of a similar token

Prior to the minting of the *KubeCoin tokens V2* there were `480000000` *KubeCoin tokens*, minted named `Kubecoin` (`4b756265636f696e`) with policy ID:

`362706e09f908e1470b90278cb50bcd834b4c2f8d489431a8965ddb8`

KubeCoin tokens were covered by a previous report (linked here).
The similarity in naming of the two tokens could lead to confusion, although as can be seen in the Token Details page (link) they are clearly marked with the description:

```
InvalidCoinK (https://kubecoin.org)
Invalid coin as it doesn't meet needed requirements. A new one has been
generated to replace it.
```

While the asset *KubeCoin tokens V2 Token Details page (link)* clearly states:

```
KubeCoin (https://kubecoin.org)
The digital currency for the travel and leisure industries, universally
adoptable through multi-brand platforms
```