Upgradeable Owners Minting Policy

Solution allows minting of tokens with multisignature approach and owners are updateable.

> Owners - public keys that need to sign transaction in order to mint tokens

Needed Cardano scripts

For implementing considered logic 3 scripts are needed:

- **Token script**

  Used for minting and burning tokens.

  In order to mint tokens, script validates:

  - Whether the token name is correct
  - Output with **NFT** is a transaction input. Check is done in order to ensure validation of **UpgradeableOwners script.**

  Script checks that transaction mints or burns just specific kind of token. Tokens can be burnt by token holder without owners' agreement.

- **NFT script** *(= thread NFT)*

  Used to create NFT

  Validates:

  - Defined utxo is consumed
  - Amount of token to mint is 1

  NFT is a token that defines a specific output, sitting at **UpgradeableOwners script**, from which information is retrieved in order to validate token management: minting, adding or removing owners, changing min threshold number.

- **UpgradeableOwners script**

  Used for:

  - Addition of owner
  - Removal of owner

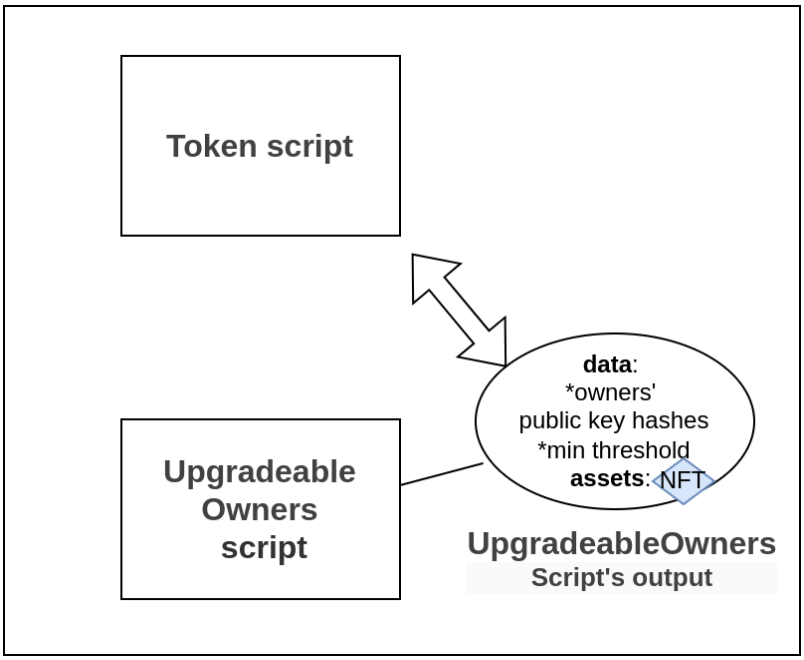
- Changing min threshold number of signatures
  > min threshold number is a number of owners that are needed to sign a transaction in order to mint token or add/remove owner

Output with **NFT** will be located at this script address. The **NFT** output will store minimum threshold number and public key hashes of owners that need to sign a transaction for minting **tokens.**

Owners' payment public key hashes can be changed through interaction that involves spending of **NFT** output.

Note: addition of owner is accompanied by off-chain transaction validation module. Each owner must have off-chain transaction validation on their side. Otherwise any owner can violate minting tokens rules and violate the protocol in general, for example, simply providing wrong pkh of the owner to add and broadcasting transaction to other owners.

Transactions will be signed by owners and submitted by payer. **UpgradeableOwners script**'s output with **NFT** and data in it will be spent in order to validate transaction logic. **UpgradeableOwners** and **Token scripts** are bound to work with single state-thread NFT. However, the same **UpgradeableOwners** can be also used to mint tokens for various asset classes produced by the **Token** script but with different policy hashes.



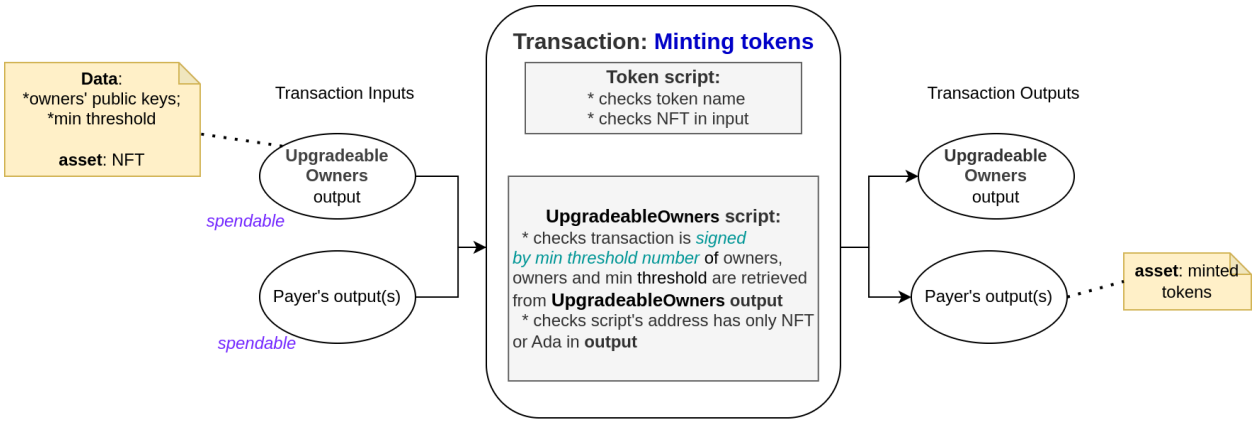
Connection between **Token script** and output with **NFT**

Preparations (semi on-chain)

In order to validate transactions by **UpgradeableOwners script,** we need firstly to mint NFT on our own and create output at script's address with NFT and initial data (owners' public key hashes, minimum threshold number).

Minting

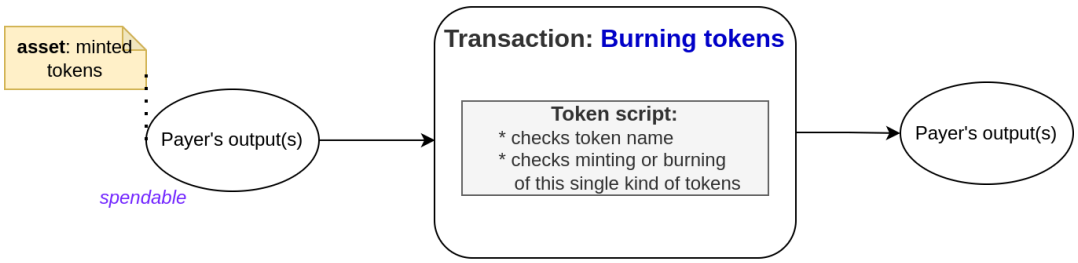
The minimum threshold number of owners must approve tokens minting. Public key hashes of owners are listed in output's data.



Demonstration of minting transaction in UTxO form

Burning

Tokens can be burnt by token holder without owners' agreement.



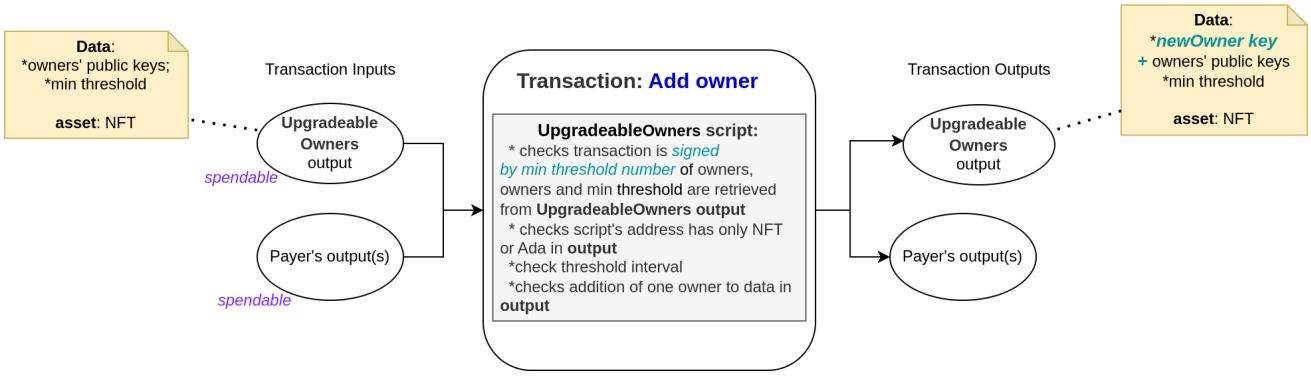
Demonstration of burning transaction in UTxO form

Addition of owner

The minimum threshold number of owners must approve addition of another owner and sign a transaction that changes data in **NFT** output.

Output with **NFT** is spent. Than new output is created at the **UpgradeableOwners script** with the same **NFT** from previous output, but with changed data: new owner key is added to array of owners' public keys.

Owners also can set new threshold number in the same transaction. Then threshold interval is checked. Minimum threshold number is 2.



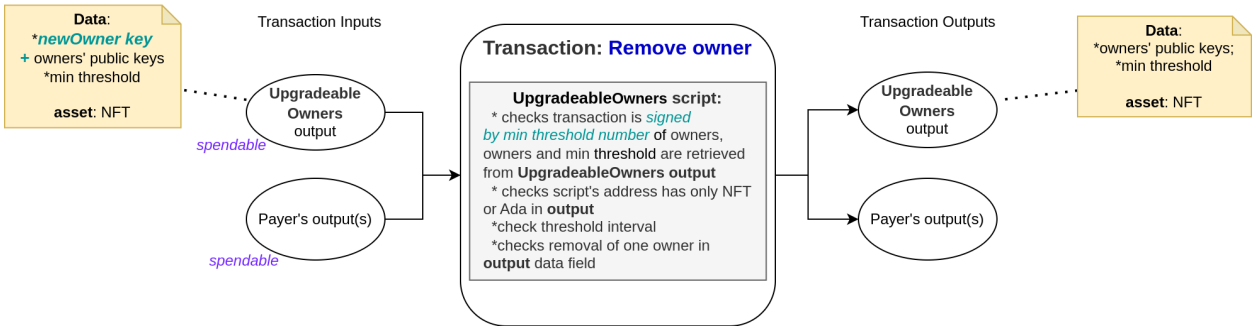
Demonstration of add owner transaction in UTxO form

Removal of owner

The minimum threshold number of owners must approve removal of another owner and sign a transaction that changes data in **NFT** output.

Output with **NFT** is spent. Than new output is created at the **UpgradeableOwners script** with the same **NFT** from previous output, but with changed data: key of excluded owner is removed from array of owners' public keys.

Owners also can set new threshold number in the same transaction. Then threshold interval is checked. Minimum threshold number is 2.



Demonstration of remove owner transaction in UTxO form

Changing min threshold number

Minimum threshold number of owners must approve changing min threshold number and sign a transaction that changes data in **NFT** output. Threshold interval is checked. New minimum threshold number must be greater than or equal to 2 and it must be less or equal to number of owners.

Output with **NFT** is spent. Than new output is created at the **UpgradeableOwners script** with the same **NFT** from previous output, but with changed minimum threshold number.