Vérification du contrat multisig en Coq

Raphaël Cauderlier

11 mars 2019

Le contrat multisig d'Arthur

stockage :

- un compteur incrémenté à chaque appel
- un seuil: le nombre de signature à avoir pour effectuer une action
- une liste de clés

paramètres :

- un compteur (doit être égal à celui qui est stocké)
- une action parmi :
  - transfert,
  - changement de délégué, ou
  - changement des clés et du seuil
- une liste de signatures optionnelles
  - Pour chaque clé stockée, on peut fournir une signature de (compteur, action, adresse(self)).

Rejeu

Le compteur et l'adresse de self sont là pour éviter les attaques par rejeu.
Attention, je n'ai pas prouvé que ce contrat est résistant au rejeu.

Spécification

J'ai prouvé en Coq une propriété de la forme :

$\forall$ params, storage, operations, storage',
eval (`multisig`, params, storage) = **Success** (operations, storage')
$\Leftrightarrow$ R (params, storage, operations, storage')

La relation R est la spécification du contrat `multisig`, elle caractérise les executions réussies du contrat.

Futur

- Autres contrats
- Mécanisation des preuves
- Gas
- Compilation
- Annotations
- Extraction
- Chaînes d'execution