PIDR

Un protocole de lotterie en Bitcoin

Guillaume Stunault, Lucas Vignali

February 2018

1 Introduction

2 Le protocole de lotterie

Nous allons analysé un protocole de smart contract qui implémente une lotterie Bitcoin. [1] Ce protocole garantit :

- chaque joueur honnête aura (en moyenne) un gain non négatif, même dans le présence d'adversaires qui jouent contre
- Si tous les joueurs sont honnetes, le protocole simule une lotterie ordinaire : 1 joueur remporte les mises des autres joueurs

Le protocole utilise un arbre de tournoi : chaque manche le gagnant remporte la mise de l'adversaire

Initialisation :

- chaque joueur génère N paires de clés, $O(N^2)$ signatures (N signatures pour N paires de clé * N transactions Win, Timeout... pour chaque joueur) et log(N) secrets qu'il hash ensuite pour tous les matchs qu'il va jouer.
- on vérifie que les hashs ne sont pas réutilisés
- ensuite il pose la mise en signant une transaction Init
- si un joueur ne pose pas la mise, les autres récupèrent leur mise
- Init est ajouté à la blockchain
- La transaction doit s'effectuer dans un temps donné, assez long pour qu'il permette la transaction. Ce temps est calculé pour permettre la géneration des clés
- Init est ensuite séparée en N mises de départ : Win(p,p) ajoutées à la blockchain

Execution :

- C'est la phase de match, soient π_k le match actuel, p_1 et p_2 les joueurs qui s'affrontent
- Au départ, on ajoute à la blockchain, les transactions Win(π_{k-1}, p_1) et Win(π_{k-1}, p_2) si ça n'a pas déjà été fait
- p_1 commence, on ajoute Turn1(π_k, p_1, p_2) à la blockchain : p_1 doit donc révéler son secret à temps en l'ajoutant, comme in-scipt dans Turn2(π_k, p_1, p_2)

— Ainsi, p_2 peut vérifier que le hash de p_1 correspond au hash envoyé au départ
— p_2 connait son propre secret et exécute la fonction aléatoire w = winner(π_k, p_1, p_2, Sk_1, Sk_2)
— p_2 ajoute finalement à la blockchain la transaction Win(w, π_k) avec pour in-script son secret Sk_2.
— Chaque joueur doit chacun son tour réveler sa clé dans un temps imparti sinon il perd.

Mise :
A tous les tours, chaque joueur mise 1 bitcoin. Pour éviter la fraude et qu'un joueur quitte la partie en plein milieu avec l'argent qu'il a récolté, chaque joueur pose au début une somme de bitcoins égale au nombre de parties possibles par un joueur. Ainsi à chaque partie gagné un bitcoin est retiré de cette somme, et si le joueur quitte la partie en plein milieu cette est reversé à chaque joueur afronté précedement ce qui fait que le joueur en question ne gagne pas d'argent. Dans le cas ou il perd une manche cette mise lui est rendu.

Date	Travail effectué
07/02/2018	Découverte du sujet
14/02/2018	Installation de Tamarin Choix du protocole : Lotterie
15/03/2018	Compréhension du sujet Rédaction du rapport Découverte Tamarin

Références

[1] Andrew Miller et Iddo Bentov : Zero-collateral lotteries in bitcoin and ethereum, 04 2017.