PIDR

Un protocole de lotterie en Bitcoin

Guillaume Stunault, Lucas Vignali

February 2018

1 Introduction

Pour notre projet de PIDR nous avions comme sujet : **Vérification des « smart contracts » sur la blockchain**. Ce sujet nous a été proposé par M. Jannik DREIER, membre du LORIA et de l'équipe PESTO, accompagné de M. Steve Kremer. Suite à l'essort des applications liées à la blockchain et principalement celle du Bitcoin, des règles de sécuritées comme les "Smart Contracts" doivent être mises en oeuvre pour la sureté de ces protocloles. Ces "Smart Contracts" permettent de définir et d'exécuter des contrats de façon automatique et sans besoin d'une tierce partie de confiance. Ainsi cela permet qu'aucun participant ayant signé le contrat ne se retrouve sans paiement car l'exécutions des contrats est automatique. Le but de ce PIDR a donc été de modéliser un système de smart contract. Pour cela nous avons utilisé un logiciel créé par l'équipe PESTO du LORIA : **Tamarin**. Sur ce logiciel nous avons modélisé un protocol de lotterie.

1.1 La Blockchain

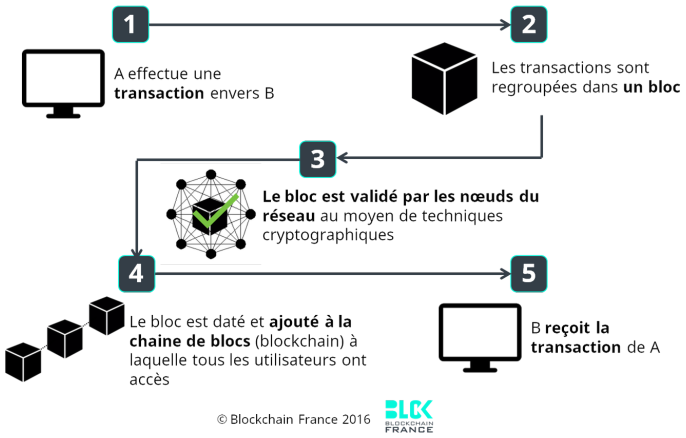
La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle.

Par extension, une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Ces échanges sont enregistrés sous forme de blocs, qui mis bout à bout forment une chaîne, d'où le terme blockchain. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne. [1]

L'intérêt de la blockchain réside dans l'aspect décentralisé de la base de données qui est stockée sur les différents serveurs des utilisateurs et fonctionne sans intermédiaire ce qui limite les frais d'infrastructure. Cette base de données que beaucoup comparent à un grand livre comptable – public et partagé – contient un historique infalsifiable des transactions qui est mis à jour en temps réel par les utilisateurs. Les utilisateurs valident chaque transaction et vérifient

la cohérence de celle-ci grâce au registre.

Pourquoi infalsifiable ?
Distribuée, et non centralisée, la base de données est aussi doublement sécurisée. D'abord par un système de cryptographie dite "asymétrique". Cela signifie simplement qu'il faut deux clés différentes (une privée, une publique) pour soumettre une transaction dans la blockchain. Ensuite, Chaque bloc est validé par les noeuds du réseau appelés les "mineurs". Les "mineurs" chargés de vérifier la validité des transactions bloc par bloc sont des particuliers, rémunérés pour mettre à disposition la puissance de calcul de leurs processeurs en résolvant des fonctions de hachage cryptographique. Dans la blockchain du Bitcoin, cette technique s'appelle le "Proof-of-Work" (preuve de travail). [2]
Ainsi pour manipuler la blockchain, il faudrait pouvoir falsifier plus de la motité des noeuds du sytème, ce qui correspond à hacker des milliers d'utilisateurs au même moment. Techniquement, il s'agit d'une prouesse impossible.



Le potentiel de la blockchain [1]

Bien que souvent associé au Bitcoin et autres cryptomonnaies, le caractère décentralisé de la blockchain, couplé avec sa sécurité et sa transparence, promet des applications bien plus larges :

- Les applications pour le transfert d'actifs (utilisation monétaire, mais pas uniquement : titres, votes, actions, obligations...)
- Les applications de la blockchain en tant que registre : elle assure ainsi une meilleure traçabilité des produits et des actifs.
- Les smart contracts : il s'agit de programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarrés.

1.2 Le Bitcoin

Le Bitcoin est une monnaie virtuelle mais aussi un sytème de paiement pair à pair. C'est la prmière monnaie électronique décentralisé. Ce type de monnaie possède différent avantages :

— Echange de particulier à particulier ce qui implique des frais inférieurs aux banques
— Utilisable dans tous les pays
— Les comptes ne peuvent pas être gelés
— Pas de conditions

Les bitcoins peuvent être générés par toute personne possédant un ordinateur et faisant tourner un logiciel appelé "mineur de bitcoin". Cette création de bitcoin requiert de de travailler sur chaque bloc de transaction. Ceci est ajusté par le réseau pour que la création des bitcoin soit prédictible et limitée. Enfin les bitcoin sont stockés dans des portes monnaies électroniques. Chaque transaction est vérifiée puis stockée sur le réseau.

1.3 Notions cryptographiques

2 Le protocole de lotterie

Nous allons analysé un protocole de smart contract qui implémente une lotterie Bitcoin. [3] 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.

3 Protocole réalisé

Nous avons simplifié le protocole au maximum pour tester ses divers propriétés de sécurité. Nous prenons désormais uniquement 2 joueurs A et B, et une seule manche de match.
La mise vaut pour le moment : 1 bitcoin
De plus, pour modéliser la blockchain, nous considérons les traces de Tamarin. En effet, la blockchain rend les transactions enregistrées consultables à chaque moment tout comme les traces de Tamarin.

— A et B génèrent chacun une clé publique et une clé secrète
— A partir de cette clé secrète, le protocole assigne un porte-monnaie avec 3 bitcoins à chaque joueur
— Chacun des 2 joueurs génère ensuite un secret pour le match, et envoie son hash signé sur le réseau.
— La blockchain retire 1 Bitcoin du porte-monnaie de A et B pour créer une mise
— La blockchain crée un contrat où A et B posent leurs mises. Lorsque les 2 mises sont posées, le match peut commencer.
— La blockchain crée un contrat où A doit révéler son secret. Elle vérifie que le hash du secret envoyé correspond au hash envoyé avant le match
— Idem pour B
— Lorsque la blockchain possède les 2 hashs, elle peut déterminer aléatoirement un gagnant entre A et B.
— La blockchain ajoute les 2 Bitcoins au porte-monnaie du gagnant.

Normalement, la blockchain est censé déterminer un gagnant avec une fonction sur la parité des secrets (processus qui est défini aléatoire et non truquable). Pour modéliser cela sur Tamarin, nous avons crée 2 règles identiques de victoire : une avec A, une avec B. Et Tamarin choisit aléatoirement une de ces 2 règles.

4 Propriétés à prouver

— Il existe une exécution normale du protocole
— A la fin, le porte-monnaie de l'un contient 4 bitcoins, et celui du perdant 2 bitcoins

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
04/04/2018	Première version compilable du protocole

Références

[1] Blockchain france.

[2] Comprendre la technologie blockchain.

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