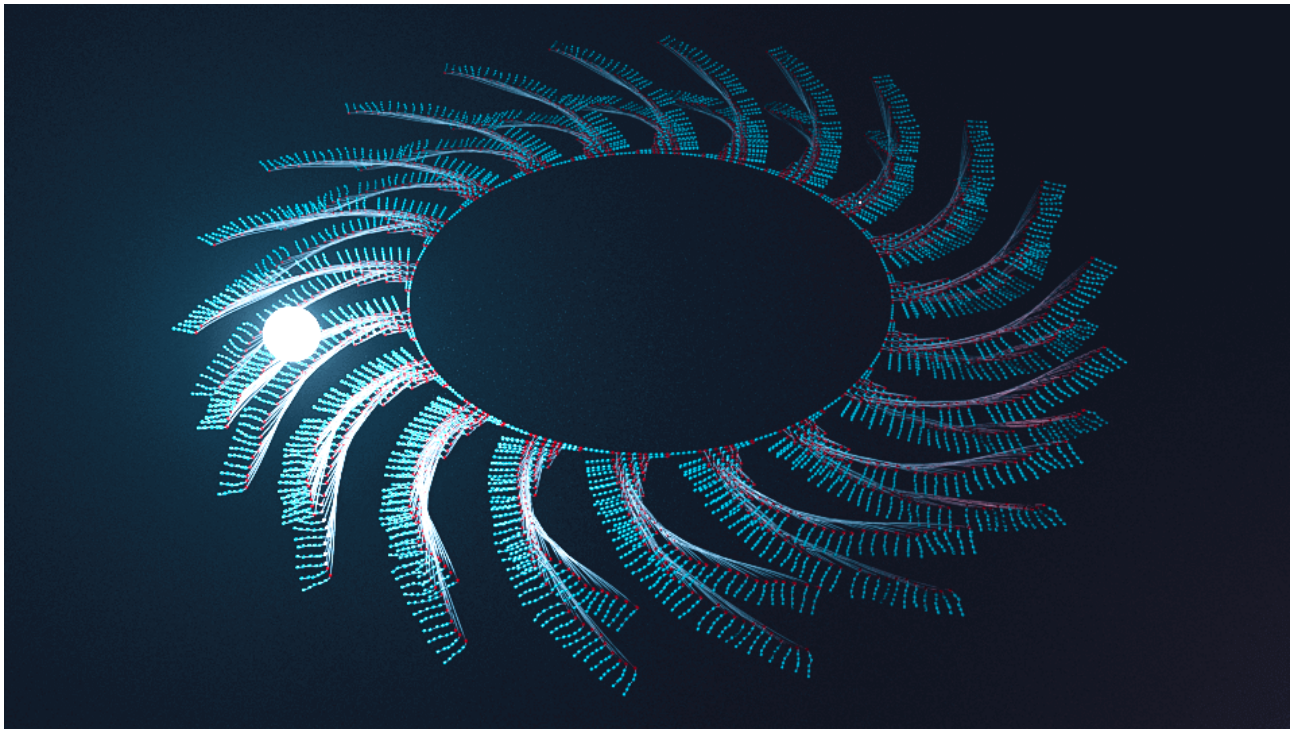

Cardano est protégé contre les attaques de type “Faux enjeux”

Auteur : Phillip Kant - Traduction : @psychomb

De part sa conception revue par les pairs, Ouroboros est exempt d'un défaut affectant de nombreuses chaînes de preuve d'enjeux.

Ada ne fait pas partie des 26 cryptomonnaies identifiées courant Janvier 2019 par des chercheurs américains comme étant vulnérables aux attaques de type “faux enjeux” [1]. La blockchain Cardano sous-jacente à Ada est basée sur la preuve d’enjeu (PoS), mais son protocole Ouroboros n'utilise aucun code issue de Bitcoin et n'est pas affecté par le problème PoSv3 [2]. Ceci n'est pas seulement une bonne chose, mais bien une conséquence de la démarche approfondie et formellement vérifiée qui a été adoptée lors du développement de Cardano.

La vulnérabilité

La vulnérabilité est très bien expliquée dans l'article original. Afin de comprendre pourquoi Cardano n'est pas concerné, nous allons résumer ici l'essentiel de la vulnérabilité décrite.

Tous les systèmes vulnérables utilisent PoSv3, une modification du code de Bitcoin qui vise à remplacer la puissance de calcul (PoW) par un enjeu, afin de déterminer qui est éligible pour créer un bloc. Dans le code de Bitcoin original, la décision de créer le bloc suivant est basée uniquement sur la puissance de calcul : celui qui parvient à trouver un nombre aléatoire approprié, et ainsi obtenir un “hachage” correct en premier, gagne. PoSv3, cependant, ajoute une variable supplémentaire pour simuler la notion d’enjeu.

Dans un système de PoS, la probabilité de créer un bloc est proportionnelle à l'enjeu qu'un utilisateur possède dans le système : plus un utilisateur possède d'enjeu, plus il est probable qu'il crée le bloc suivant. Pour imiter cette fonctionnalité, PoSv3 permet aux utilisateurs d'ajouter des informations supplémentaires à leur bloc candidat, sous la forme d'une “transaction d’enjeu”. Plus

ils ont de jetons (cryptomonnaie) disponibles pour cette transaction particulière, plus il devient facile pour eux d'obtenir un résultat correct, et donc de gagner le droit de créer le bloc suivant.

Bien que PoSv3 réussisse à lier de cette façon les droits de création de blocs à un enjeu, il rend également la validation des blocs plus difficile. Non seulement le “hachage” du bloc lui-même doit être vérifié (comme dans Bitcoin), mais aussi la transaction d’enjeu d'un utilisateur : l'utilisateur possédait-il réellement les jetons utilisés dans sa transaction d’enjeu ? Pour vérifier ces informations, un nœud de la blockchain doit pouvoir se référer au registre. Dans le cas ou un bloc n’étend pas normalement la chaine principale mais provoque une bifurcation (ou “fork”), le noeud doit également s’en référer à l'historique du registre. Comme tout cela n'est pas mis en mémoire, et ni particulièrement bon marché à calculer, les blocs dans les systèmes PoSv3 ne sont pas validés immédiatement mais sont plutôt (au moins partiellement) stockés en mémoire ou sur disque, le temps de leur vérification.

Les vulnérabilités discutées dans l'article original peuvent être exploitées de plusieurs façons, mais impliquent en fin de compte de tromper ces mécanismes de vérification par exemple en présentant beaucoup de blocs invalides à un noeud, de sorte que le noeud manque de mémoire et plante avant de pouvoir correctement identifier que les blocs sont invalides.

Pourquoi Cardano est différent

Pour Cardano, I.O.H.K. a adopté une approche différente. Au lieu de trouver une variation minimale de Bitcoin, nous nous sommes appuyés sur des universitaires et des chercheurs de renommée mondiale pour créer un nouveau protocole et un code entièrement nouveau, à partir de zéro, avec l'exigence qu'il fournisse des garanties de sécurité équivalentes (ou meilleures) que Bitcoin, tout en reposant entièrement sur des enjeux. Le résultat est le protocole Ouroboros [3], le premier protocole PoS sécurisé et éprouvé, sur lequel est construit Cardano.

La conception de base d'Ouroboros est remarquablement simple : le temps est divisé en incréments discrets, appelés tranches, et les tranches sont regroupés en périodes plus longues, appelées époques. Au début de chaque époque, une loterie détermine qui doit créer un bloc pour chaque tranche. Au lieu d’avoir une loterie implicite, c'est à dire que celui qui obtient le bon calcul en premier est le gagnant, la loterie est explicite : un nombre aléatoire détermine un chef pour chaque tranche, et les chances de gagner pour une tranche donnée sont proportionnelles à la mise (ou l’enjeu) que l'on contrôle [4].

Dans ce protocole, valider qu'un bloc a été signé par le bon acteur est également simple : il ne faut pour cela que le calendrier des chefs de tranche pour l'époque en cours (qui ne changera pas dans le cas d'une bifurcation temporaire), et la vérification d'une signature. Ceci peut et sera fait par chaque nœud une fois qu'il aura reçu l'en-tête de bloc, contrairement aux systèmes PoSv3 qui sont vulnérables aux attaques de “faux enjeux”.

En bref : Cardano est à l'abri des attaques de “faux enjeux” parce qu'il est basé sur un système fondamentalement différent. Les cryptomonnaies PoSv3 fonctionnent sur des systèmes de preuve de travail (PoW), modifiés pour prendre en compte l'enjeu dans l'élection implicite des créateurs de

bloc. La vulnérabilité en question est le résultat de cette modification et des complexités supplémentaires que cette modification implique.

Non seulement Cardano est conçu de manière totalement différente, mais sa fondation est le résultat de multiples articles universitaires évalués par des pairs et d'une collaboration sans précédent entre chercheurs et développeurs. Les méthodes formelles et semi-formelles utilisées dans la création de la prochaine version de Cardano (“Shelley “) garantissent que sa construction au niveau du code correspond au protocole décrit dans les documents de recherche évalués par des pairs. La fiabilité et la sécurité sont intégrées dès la conception, évitant ainsi les problèmes de PoSv3 - résultats d’une modification d'un protocole existant au lieu de créer un protocole sur mesure comme Ouroboros.

Notes:

1. "Fake Stake" attacks on chain-based Proof-of-Stake cryptocurrencies" par Sanket Kanjalkar, Yunqi Li, Yuguang Chen, Joseph Kuo, et Andrew Miller du Decentralized Systems Lab de l'Université d'Illinois Urbana-Champaign.

2. Pour être plus précis, la discussion qui suit vise la sortie prochaine de Cardano Shelley. La version Byron actuellement déployée fonctionne dans un environnement fédéré, et est donc de toute façon protégée contre ce type d'attaque.

3. Il existe maintenant un certain nombre de variantes du protocole Ouroboros. Nous ne décrivons ici que la version classique d'Ouroboros, mais l'argument général vaut pour toutes ses variantes - en particulier pour Ouroboros Praos, qui sera le protocole utilisé dans la version Shelley.

4. Pour être précis, l'élection d'un chef de tranche pour une époque donnée utilise la distribution des enjeux à un moment donné avant le début de l'époque, pour éviter d’autres types d’attaques et un re-calcul du planning dans le cas d'une bifurcation temporaire à la limite de l'époque.

Oeuvre : Edan Kwan