Compas'2023 : Parallélisme/ Architecture/ Système
LISTIC/USMB - Annecy France, 4-7 juillet 2023

Utilisation de noeuds de confiance pour les protocoles d'échantillonage de pairs tolérants aux attaques byzantines

Augusta MUKAM *

Université de Bordeaux,
Laboratoire LABRI - 351, cours de la Libération F-33405 Talence cedex
augusta.mukam@labri.fr

Résumé
Les blockchains sont des systèmes distribués avec des contraintes propres à satisfaire. Il faut par exemple s'assurer que les nœuds du système aient un état à jour dans des délais opportun, mais aussi que l'intégrité voir de la confidentialité des données soit préservée. La prise en compte de l'existence de nœuds byzantins qui empêchent le bon déroulement des algorithmes de blockchain rend la conception de ces algorithmes plus complexe. Une des briques essentielles des blockchains est la découverte des nœuds du système. Ceci est un défi car le système étant grand et souvent ouvert, chaque nœud ne peut avoir la connaissance totale du système à un moment donné. On s'appuie donc sur les protocoles de *gossip based peer-sampling*. Dans ces protocoles, chaque nœud a connaissance d'une petite portion du système à un moment donné et la communique à ces voisins par échange de messages structurés à chaque étape du protocole. Les nœuds byzantins eux souhaitent être surreprésentés dans les vues de ces différents nœuds afin de gagner en éligibilité pour les protocoles d'autres couches de la blockchain comme celle de consensus. Nous avons l'exemple de la blockchain Bitcoin pour laquelle on a découvert une vulnérabilité aux attaques Eclipse, permettant par exemple à un attaquant de récupérer des jetons destinés à des nœuds qu'il a évincés du système.
Il existe plusieurs protocoles de peer sampling dans la littérature dont BRAHMS, qui fait parti des plus résistant aux comportements byzantins, mais donne des résultats loin d'être optimaux, avec une représentation à 80% des noeuds byzantins dans la connaissance des noeuds honnêtes lorsque les byzantins ne sont que 18% dans le système. Une des idées derrière BRAHMS est d'utiliser un échantillonnage aléatoire et uniforme des noeuds du système qui soit performant face aux attaques byzantines. L'échantillon obtenu va alimenter la vue locale du nœud, réduisant ainsi la représentation des nœuds byzantins dans sa vue. Un autre protocole RAPTEE, s'est greffé à BRAHMS en ajoutant de nouveaux acteurs dans le système, des noeuds de confiance basés sur la technologie Intel SGX, qui grâce à un mécanisme d'authentification peuvent s'échanger plus d'informations entre eux et contribuer à dépolluer les vues des noeuds corrects en partageant de l'information "moins biaisée". Ainsi, avec 1% des nœuds du système étant de confiance, RAPTEE parvient à réduire de 17% la proportion de byzantins dans les vues des nœuds honnêtes (nœuds corrects + nœuds de confiance) dans un système composé à 10% de byzantins.
Dans cette quête de réduire la résilience des noeuds honnêtes, nous travaillons sur une extension de Raptee à l'aide de la structure de donnée Count Min Sketch pour permettre aux noeuds de confiance de s'échanger plus rapidement des informations afin de dépolluer plus

*. Le texte a été relu par Joachim Bruneau-Queyreix et Laurent Réveillère.

efficacement leurs vues et d'en faire bénéficier le reste du système.

Mots-clés : Blockchain, byzantin, Gossig, peer sampling, noeud de confiance