Dans la suite du blog-post de la semaine dernière rédigé par le Prof. Aggelos Kiayias, Directeur de recherche chez I.O.H.K., cet article traite d'un autre choix que nous avons fait lors de la conception du mécanisme de récompense de Cardano. Ce mécanisme est conçu pour inciter les parties prenantes à "faire ce qui est bien" et à participer au protocole de manière à en assurer le bon fonctionnement, de manière efficace et sécurisée.

Comme expliqué dans l'article sur les groupes d'enjeu au sein de Cardano, pour assurer l'équité et la décentralisation, le mécanisme de récompense suit trois principe :

- Le total des récompenses pour un groupe d'enjeu doit être proportionnel à la taille du groupe jusqu'à ce que le groupe atteigne le point de saturation.
- Les récompenses pour chaque membre au sein d'un groupe doivent être proportionnelles à la participation apportée par ces membres dans leur groupe.
- Les gestionnaires de groupes devraient obtenir une récompense plus grande pour leurs efforts.

Une modification nécessaire concerne les performances du groupe. Si un gestionnaire de groupes néglige ses "devoirs" et ne crée pas les blocs qu'il est supposé créer, les récompenses du groupe diminueront en conséquence.

Prenons l'exemple d'Alice et de Bob qui gèrent des groupes d'enjeu de tailles égales. Ils sont tous deux élus en tant que chefs de tranche 100 fois chacun. Alice crée consciencieusement les 100 blocs des 100 tranches qu'elle dirige, alors que Bob manque 20 blocs et n'en crée que 80. Dans ce cas, le groupe d'enjeu d'Alice recevra toutes les récompenses, alors que le groupe de Bob en obtiendra moins. Combien en moins exactement ? Cela est contrôlé par un paramètre.

Le défi

Cet article ne se concentre pas sur le problème du paramètre mentionné ci-dessus mais sur un autre défi potentiel et explique comment il a été décidé de surmonter ce dernier. Ce défi particulier a été mentionné à la fin de l'article sur les groupes d'enjeu au sein de Cardano : Comment empêcher une personne de créer des dizaines, voire des centaines de petits groupes d'enjeu et donc de contrôler une grande masse d'enjeu sans posséder un enjeu propre ?

Notez que pour les très gros acteurs, il est parfaitement légitime de scinder leur enjeu en plusieurs groupes de manière à obtenir une part équitable des récompenses sans tomber sous le coup des restrictions imposées par le point de saturation.

Un exemple d'attaque de type 'Sybil'

Supposons que nous souhaitions fonctionner avec 100 groupes d'enjeu. Pour atteindre ce but, nous plafonnerions les récompenses à 1% (point de saturation). Supposons en outre qu'Alice détient une participation de 3.6%. Si Alice ne partage pas sa participation, elle ne recevra que 1% du total des récompenses. Si, toutefois, Alice divise sa participation en mettant 0.9% du montant dans quatre groupes d'enjeu différents, sa récompense pour chaque groupe ne sera pas plafonnée.

Le défi se pose si un acteur petit mais sournois est autorisé à créer un grand nombre de groupes (éventuellement sous des identités factices). S'il réussit à attirer des personnes dans ces groupes (par exemple en mentant sur ses coûts et en promettant des récompenses élevées aux membres du groupe), il pourrait finir par contrôler une participation majoritaire avec très peu de participation personnelle dans le système. Comment cela pourrait-il arriver ?

Imaginons qu'il existe environ 100 groupes légitimes et honnêtes. Si nous ne nous en protégions pas, un joueur malveillant pourrait créer à peu de frais, 100, 200 ou même 500 groupes sous de faux noms, et revendiquer des coûts opérationnels faibles et une marge bénéficiaire faible. De nombreux participants honnêtes seraient alors tentés de cesser de déléguer à l'un des 100 groupes honnêtes et de déléguer leur participation à l'un de ces groupes malicieux, qui pourraient être plus nombreux que les groupes honnêtes. En conséquence, le gestionnaire de ces groupes malveillants serait choisi comme chef de tranche pour une majorité de blocs et prendrait ainsi le contrôle effectif de la blockchain. Il pourrait effectuer toutes sortes de méfaits et d'activités criminelles, telles que des doubles dépenses ! Bien sûr, il devrait payer pour le fonctionnement de centaines de groupes d'enjeu, mais ce coût est minime par rapport au coût d'acquisition d'une participation majoritaire si il avait du acheter la majorité de tous les ADA existants, ce qui représenterait des centaines de millions à des milliards de dollars (cf. A quel point Cardano est-il sécurisé ? Partie 2).

Cela serait désastreux, car la sécurité d'un système PoS comme Cardano repose sur l'idée que les personnes qui ont beaucoup d'influence sur le système devraient détenir beaucoup de participation et donc avoir toutes les raisons de l'aider à fonctionner correctement.

La solution proposée

Ce type d'attaque, où l'attaquant prend de nombreuses identités, est appelé une attaque Sybil, d'après le roman Sybil de 1973, écrit par Flora Rheta Schreiber, à propos d'une femme souffrant de trouble de la personnalité multiple.

Comment pouvons-nous prévenir les attaques Sybil ?

Une idée pourrait être de rendre la création et l'enregistrement des groupes d'enjeu très coûteux. Mais pour prévenir les attaques, ces frais devraient être extrêmement élevés et empêcher les honnêtes participants de créer des groupes légitimes. Un tel obstacle serait mauvais pour la décentralisation ; nous voulons encourager les membres de notre communauté à créer leur

propre groupe et ne pas entraver leur entrée dans l'écosystème ! Des frais modestes doivent toutefois exister pour la simple raison que chaque certificat d'enregistrement doit être stocké dans la blockchain et cela consomme des ressources qui doivent être payées.

Une analyse de la théorie des jeux produite par I.O.H.K. a conduits à une solution différente, une solution qui n'empêche pas les "petits" acteurs de créer leur propre groupe en leur imposant des frais prohibitifs et un risque financier élevé.

Lors de l'enregistrement d'un groupe, le gestionnaire du groupe peut décider d'engager une partie de sa participation personnelle dans le groupe. Engager davantage augmentera légèrement les récompenses potentielles de son groupe.

Cela signifie que les groupes dont les gestionnaires ont engagés beaucoup seront plus attractifs. Ainsi, si un attaquant veut créer des dizaines de groupes, il devra scinder son enjeu personnel en plusieurs parties, rendant toutes ses groupes moins attrayants, incitant ainsi les participants à déléguer leur enjeu vers des groupes gérés par des acteurs honnêtes.

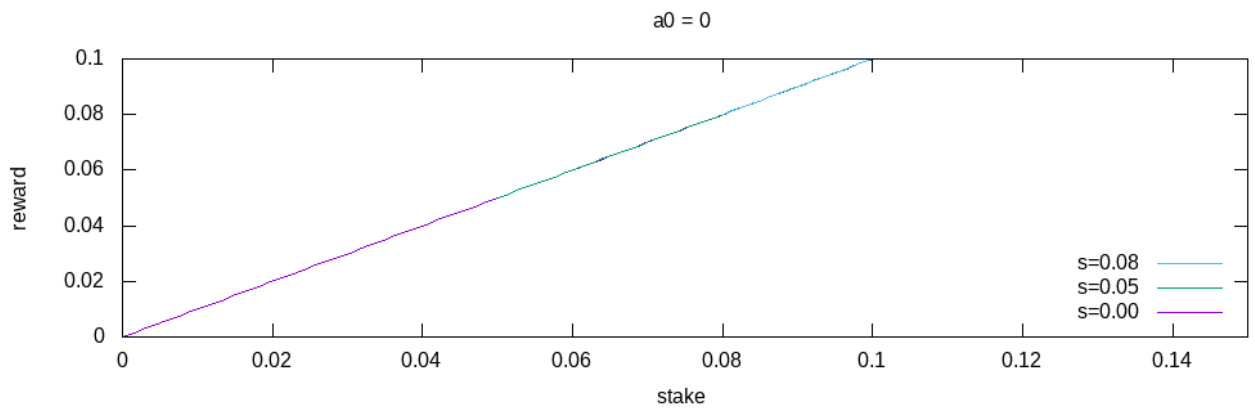
En d'autres termes, un attaquant qui crée un grand nombre de groupes devra diviser son propre enjeu de manière excessive. Ce faisant, il ne peut pas rendre attrayants touts ses groupes, car il doit diviser son enjeu en trop de fractions. Les gestionnaires de groupe honnêtes auront tendance quant à eux à regrouper tous leurs enjeux personnels dans leur groupe unique, ce qui leur donnera une bien meilleure chance d'attirer des participants.

Le degré d'influence de cet engagement par un gestionnaire de groupe sur les récompenses peut être ajusté par un paramètre configurable. Étant un groupe de mathématiciens peu imaginatifs, les ingénieurs chez I.O.H.K. ont appelé ce paramètre "a0".

Si "a0" est égal à 0, cela signifie que les récompenses du groupe ne dépendent pas de la participation engagée par le gestionnaire de groupe. À l'inverse, choisir une valeur élevée pour "a0" constitue un avantage important pour les les gestionnaires de groupe qui engagent beaucoup de leur enjeu personnel dans leurs groupes.

C'est ici un compromis classique entre équité et égalité des chances (a0 = 0) et sécurité et protection contre les attaques Sybil de l'autre (a0 est grand).

Pour illustrer l'effet de variations de "a0", examinons les trois graphiques de la figure 1 ci-dessous.



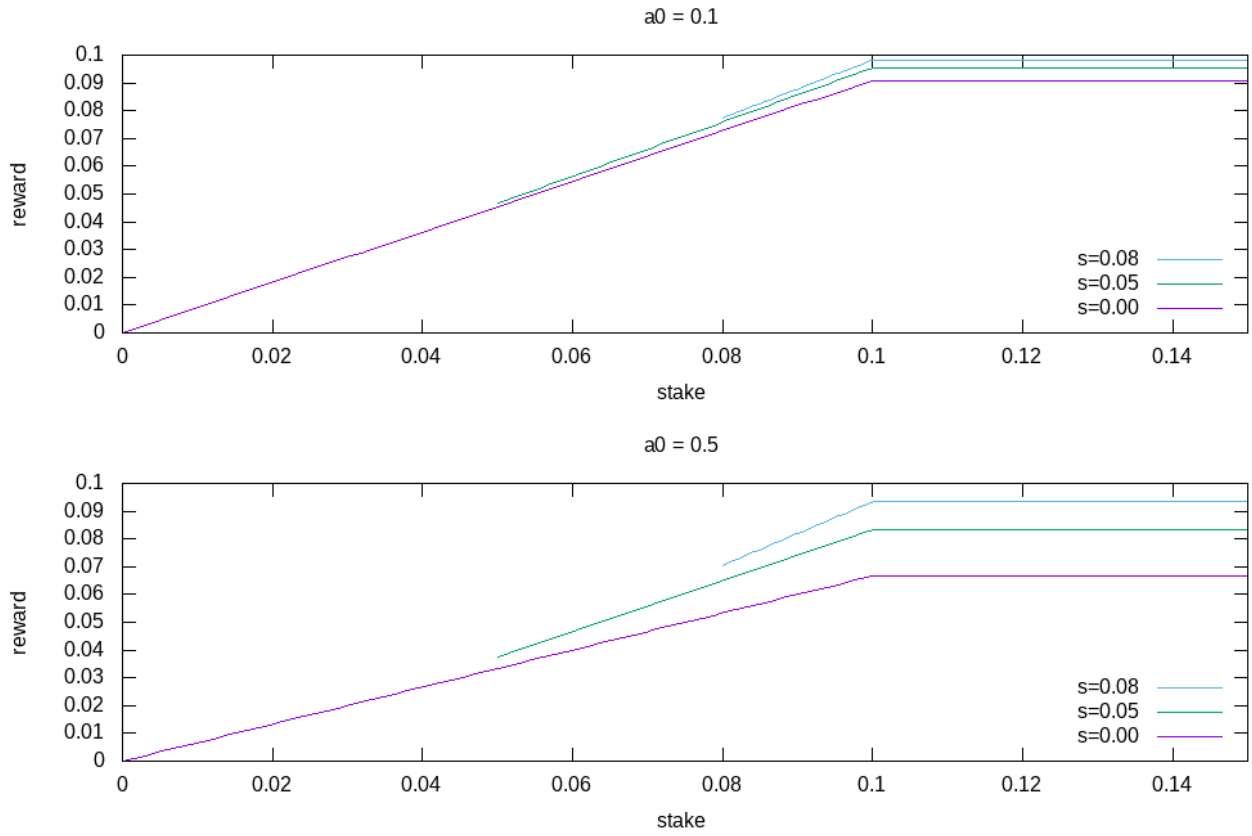


Figure 1. *Influence de l'engagement d'un enjeu propre à un gestionnaire de groupe sur les récompenses de son groupe.*

Dans les graphiques, nous visons dix groupes. Les récompenses seront plafonnées à 10% (soit 10% pour le point de saturation). La taille de l'enjeu global du groupe est indiquée sur l'axe horizontal et l'axe vertical représente les récompenses obtenues par le groupe. Chaque graphique représente trois groupes hypothétiques dans lesquels les gestionnaires ont annoncé des contributions en propre de 0%, 5% et 8%, respectivement (le montant annoncé est appelé «s» dans les graphiques).

Le premier graphique utilise a0 = 0, de sorte que la participation d'un enjeu propre par un gestionnaire de groupe n'a aucune influence sur les récompenses du groupe. Dans ce cas de figure, les trois groupes se comportent de la même manière : les récompenses continuent à augmenter à mesure que la taille en enjeu des groupes augmente, jusqu'à ce qu'ils soient plafonnés lorsque les groupes atteignent 10% de la participation (le point de saturation).

Dans le deuxième graphique, nous voyons l'effet de a0 = 0.1. Les trois groupes restent similaires, en particulier pour les petites tailles d'enjeu, mais ils sont plafonnés à des valeurs légèrement différentes. Les groupes dont la participation propre est plus importante bénéficient de récompenses légèrement plus importantes lorsqu'ils grandissent (gèrent plus d'enjeu).

Enfin, le troisième graphique montre l'effet de a0 = 0.5. Il ressemble au deuxième graphique, mais les différences entre les trois groupes sont plus prononcées. Reste encore à choisir une «bonne» valeur pour a0. Ce choix dépendra d'autres valeurs telles que les coûts opérationnels attendus, les bénéfices totaux et, surtout, le niveau de sécurité souhaité.

Il est souhaitable d'avoir un a0 aussi petit que possible, tout en garantissant un haut niveau de sécurité contre les attaques "Sybil".

Quoi qu'il en soit, il est important de garder à l'esprit que l'introduction de a0 n'empêche pas les "petites" parties prenantes de gérer des groupes performants, car une personne qui a une bonne idée peut toujours s'adresser à la communauté, convaincre les autres et les inviter à travailler ensemble, en engageant avec eux un enjeu de groupe plus important par exemple. En fin de compte, gérer un groupe d'enjeu solide et fiable et travailler en étroite collaboration avec la communauté sera plus important que de simplement posséder beaucoup d'ADA.

Egalement, il sera aussi possible de remplacer la dépendance des récompenses à l'enjeu du gestionnaire du groupe par un système de réputation. Cela permettrait aux personnes ayant un faible enjeu propre de rendre leurs groupes d'enjeu plus attractifs, en les exploitant de manière fiable et efficace sur une longue période. Ceci ne sera pas mis en oeuvre dès la première itération du protocole décentralisé, mais cela est clairement sur la table pour les futures versions de Cardano.

Vous pouvez également lire le rapport technique d'I.O.H.K. intitulé "Spécification de conception pour la délégation et les incitations dans Cardano" pour une description plus détaillée du système.

Lars Brünjes

Création artistique : Mike Beeple

Traduction : @psychomb