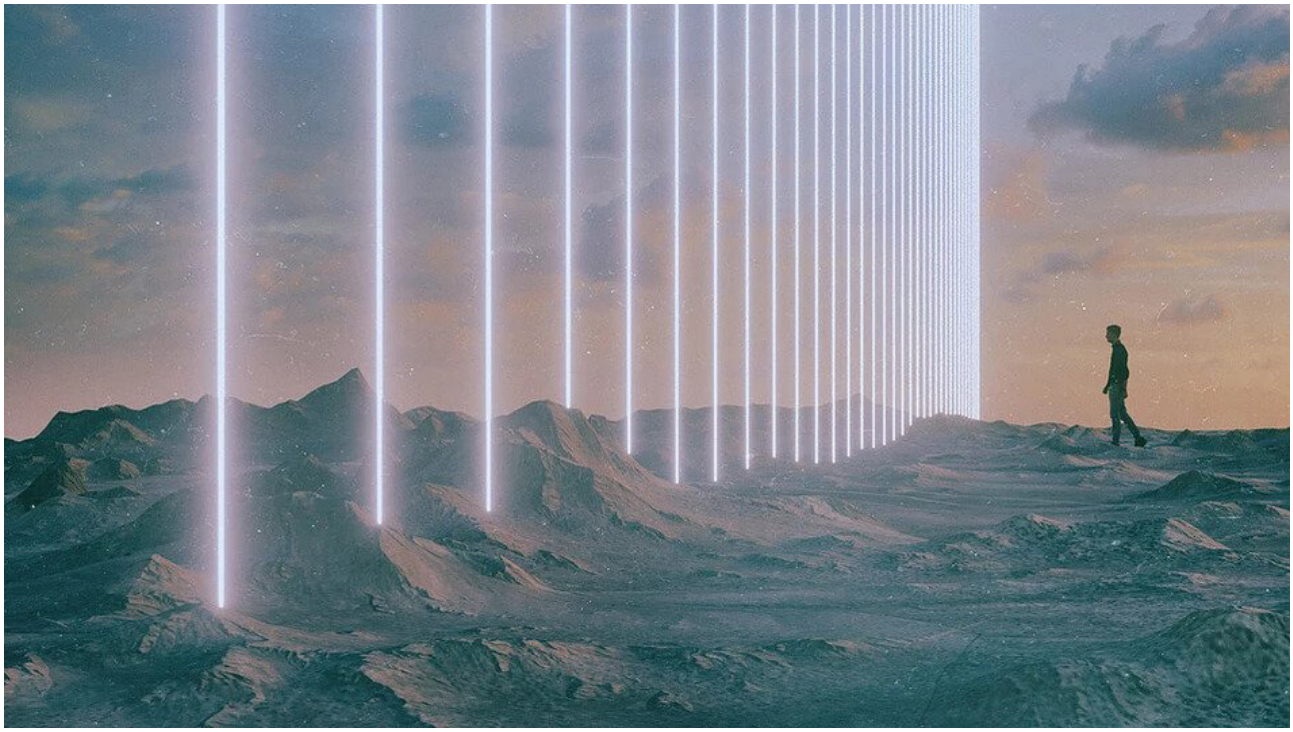

Groupes d’enjeu au sein de Cardano

Prof. Aggelos Kiayias, Directeur de recherche d’I.O.H.K., présente le principe de l’enjeu.

Dans un protocole de preuve d’enjeu (PoS), le registre est tenu à jour par les parties qui détiennent des actifs dans ce même registre. Cela permet aux chaînes de blocs (blockchains) PoS d’utiliser moins d’énergie que les blockchains basées sur la preuve de travail (PoW) ou d’autres types de protocoles. Toutefois, ce besoin impose un fardeau à ces parties prenantes. Ainsi, bon nombre d'entre elles doivent être en ligne et maintenir une connectivité au réseau suffisamment bonne pour pouvoir collecter des transactions et permettre à leurs blocs d'atteindre les autres sans retard. Il s'ensuit donc que tout registre PoS tirerait parti de nœuds de consensus fiables, détenant des actifs et se concentrant sur la maintenance.

Plaidoyer pour les groupes d’enjeu

La richesse est très souvent distribuée selon une loi de puissance telle que la distribution de Pareto. Il en résulte donc qu’exécuter le protocole PoS sur des noeuds fiables ne serait une option viable que pour une minorité de riches propriétaires d’actifs, ne laissant à la plupart des utilisateurs aucune possibilité de pouvoir faire ce travail. Cela n’est pas désirable ; il serait mieux que tout le monde puisse maintenir le registre. Une approche permettant de rectifier ce problème consiste à autoriser la création de groupes d’enjeu. Plus précisément, cela fait référence à la capacité des parties prenantes à combiner leurs actifs au sein d’une entité, un groupe d’enjeu, qui peut alors exécuter le protocole PoS en utilisant la somme des actifs qui lui ont été délégués par ses membres. Un groupe aura un gestionnaire responsable de l’exécution de ce service, et donc du traitement des transactions. En même temps, ce gestionnaire ne devra pas posséder la capacité de dépenser les actifs qui lui auront été délégués, tandis que les membres représentés par ce groupe d’enjeu seront libres de changer d’avis et donc de groupe selon leurs souhaits et à l’envie. Enfin, et de manière importante, toute partie détenant des actifs doit pouvoir devenir gestionnaire de groupe si elle le souhaite.

La participation au maintien d’un registre PoS implique des coûts. Cela n’est sûrement pas aussi élevé que dans le cas d’un protocole PoW, mais cela reste significatif. Il semble donc normal que

la communauté des parties prenantes récompensent ceux qui maintiennent le registre, installent des serveurs et traitent les transactions. Cela peut être fait en combinant les contributions faites par les utilisateurs du registre (frais de transactions) et l'inflation de la monnaie en circulation (de le nouvelle monnaie est introduite et donnée en récompense à ceux qui exécutent le protocole).

Dans le cas de Bitcoin, ces deux mécanismes - groupes et récompenses - sont à l'oeuvre. D'un côté, le minage de blocs est récompensé par les frais de transactions et une récompense fixe qui diminue avec le temps en suivant une série géométrique. De l'autre côté, l'existence de groupes est facilitée en permettant de diviser le travail requis pour produire un bloc entre plusieurs participants et en utilisant une preuve de travail 'partielle' (PoW de difficulté moindre que celle indiquée par l'état actuel du registre) comme évidence de la participation au groupe.

Mettre en place un type similaire de mécanisme d'incitations est assez simple dans le cas d'un registre PoS. Cependant, il est important de d'abord se demander si un mécanisme de ce type (ou n'importe quel mécanisme) convergerait vers une configuration désirable du système. Cela nous amène à la question importante : qu'est ce qu'est la configuration désirable du système ? Si l'on s'attache à minimiser les coûts de traitement des transactions, dans un environnement sans aucun problème, alors la configuration optimale et la plus économique est la dictature. Une seule des parties maintient le registre en tant que service tandis que les autres participent au groupe créé par cette partie unique. Cela est très clairement un résultat non désirable pour la raison qu'un gestionnaire unique est aussi un point de faiblesse unique pour tout le système, ce que les registres distribués essayent exactement d'éviter. Il s'ensuit que la coexistence de plusieurs groupes, en d'autres termes la décentralisation, devrait être une caractéristique désirable du mécanisme d'incitation au maintien du registre.

Partage des récompenses dans un registre PoS

A quoi devrait donc ressembler le partage des récompenses dans un environnement PoS ? Les récompenses devraient être données à intervalles réguliers et les coûts de maintenance du groupe devraient être prélevés par le gestionnaire du groupe avant de distribuer le reste de la récompense aux membres participant au groupe. Étant donné qu'il est possible de garder une trace de l'appartenance des utilisateurs à un groupe donné grâce au registre lui-même et l'utilisation d'une clé d'enjeu, le partage des récompenses à l'intérieur du groupe peut être codé par un contrat intelligent (smart contract) et devenir ainsi une tâche parmi les autres de maintien du registre. Tout d'abord, les gestionnaires de groupe devaient être récompensés pour leur esprit entrepreneurial. Un certificat de création de groupe posté sur le registre déclarera une marge de profit qui sera déduite des récompenses totale du groupe après avoir enlevé les coûts opérationnels, qui seront aussi déclarés sur le certificat d'enregistrement. La déclaration des coûts devrait être mise à jour régulièrement, de manière à absorber la volatilité de la monnaie native du système (cryptomonnaie) exprimée en monnaie fiduciaire, celle qui est réellement utilisée pour régler ces coûts par le gestionnaire ($, €, £, etc …). En même temps, le certificat de création du groupe, supporté par une ou plusieurs clés d'enjeu des participants, peut déclarer une certaine quantité d'actifs soutenant ce groupe et qui peuvent (i) indiquer que ce groupe représente une véritable entreprise d'un ou plusieurs propriétaires d'actifs ou (ii) servir d'actifs collatéraux, garantissant ainsi une exécution correcte du protocole.

Ces bases posées, comment s'en sortent les systèmes de type Bitcoin en ce qui concerne la décentralisation ? Chez Bitcoin, si l'on fait l'hypothèse que tout le monde suit le protocole, les récompenses des groupes sont partagées suivant la taille de chaque groupe. Par exemple, un groupe de mineur avec 20% de la puissance de calcul peut s'attendre à obtenir 20% des récompenses. Les récompenses sont en effet proportionnelles au nombre de blocs minés par le groupe et le nombre de blocs est lui même proportionnel à la puissance de calcul de ce groupe. Cela amène-t-il à une décentralisation du système ? Les évidences empiriques semblent suggérer le contraire : chez Bitcoin, les groupes de mineurs sont passés près (et parfois même passés au dessus) de la limite des 50% de la puissance de calcul, limite haute au delà de laquelle la résilience du registre distribué n'est plus assurée. Un argument simple peut valider cette observation empirique dans le cadre de notre plan de partage des récompenses : si les groupes sont récompensés proportionnellement à leur taille, et les membres dans ces groupes proportionnellement à la taille de leur apport, le plus rationnel serait alors de tout centraliser dans un seul groupe. Pour le voir, il suffit de considérer ce qui suit. Tout d'abord, il est raisonnable d'attendre que chaque participant assez riche pour créer un groupe le fera. Il en fera la promotion avec pour objectif d'attirer des membres, de telle sorte que la récompense du groupe augmente. Les autres détenteurs d'actifs qui ne sont pas gestionnaire de groupe se joindront au groupe qui maximisera leur récompense, c'est à dire le groupe avec le coût et la marge de profit les plus faibles. Pour attirer les membres, la compétition entre groupes écrasera leurs marges de profit vers des valeurs très faibles. Même avec une marge égale à zéro, tous les groupes perdront face à celui opérant avec les plus faibles coûts. N'ayant aucun levier pour retenir leurs membres, le groupe à faible coût finira par attirer tous les membres détenteurs d'actifs. Enfin, les autres gestionnaires de groupes réaliseront qu'ils auront tout à gagner à joindre ce groupe au lieu de continuer de gérer le leur, puisqu'ils percevront plus de récompenses à partir des actifs qu'ils détiennent. Finalement, le système convergera en un seul groupe dictatorial.

La figure 1 est une représentation graphique de ce phénomène. Elle provient d'une de nos nombreuses simulations que notre équipe a menées pour élaborer des systèmes efficaces de partage des récompenses. Dans cette expérience, un certain nombre de parties prenantes suivent un processus dynamique dans lequel elles essayent d'optimiser leurs gains en fonction de la configuration actuelle du système. L'expérience aboutit à un groupe unique centralisé, validant nos observations théoriques concernant les systèmes de type Bitcoin. Du point de vue de la décentralisation, il s'agit là d'une tragédie des biens communs: même si les participants accordent de la valeur à la décentralisation en tant que concept abstrait, aucun d'entre eux ne veut en supporter seul le fardeau.

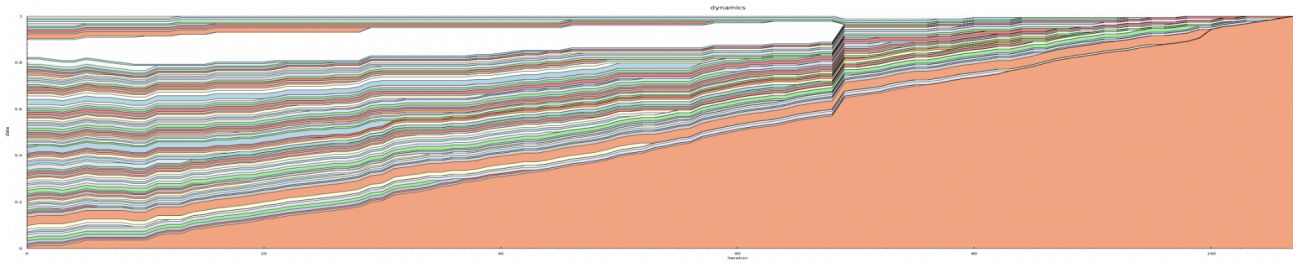

***Figure 1**. Centralisation d'un système de partage des récompenses de type Bitcoin dans une simulation avec 100 parties prenantes. Au départ, un grand nombre de groupes sont créés par les parties prenantes. À tour de rôle, les parties prenantes tentent de maximiser leur profit et changent de stratégie, aboutissant à un point de convergence où il n'existe plus qu'un seul groupe.*

Un meilleur système de partage des récompenses

Évidemment, nous devons faire mieux qu'une dictature ! Une première observation est que si nous voulons réaliser la décentralisation, la linéarité entre les récompenses et la taille devrait s'effacer après un certain niveau. En effet, si la linéarité est attrayante lorsque le groupe est petit et veut attirer les parties prenantes, elle devrait être diminuée après un certain niveau si nous voulons donner la possibilité aux groupes plus petits d'être plus compétitifs. Nous diviserons donc en deux le comportement du système de partage des récompenses en fonction de la taille du groupe : un stade de croissance, lorsque la linéarité doit être respectée, et un stade de stabilisation, lorsque le groupe est suffisamment grand. Le point de transition entre les deux états s'appellera le point de saturation et le groupe ayant dépassé ce point sera considéré comme saturé. Nous pouvons faire en sorte que les récompenses soient constantes après le point de saturation. Ainsi, si le point de saturation est égal à 1% (du total des ADA d'enjeu), deux groupes représentant une participation totale de 1% et de 1.5% des actifs recevront la même récompense.

Pour évaluer le fonctionnement d'un tel système du point de vue d'un seul membre, considérons l'exemple suivant. Supposons qu'il existe deux groupes, A et B gérés par Alice et Bob et dont les coûts opérationnels sont respectivement de 25 et 30 pièces (ici la cryptomonnaie), et chacun avec une marge bénéficiaire de 4%. Supposons de plus que le total des récompenses à distribuer soit de 1 000 pièces et que le point de saturation du mécanisme de partage des récompenses soit de 20%. À un moment donné, le groupe d'Alice détient 20% des parts, il est donc au point de saturation, alors que le groupe de Bob se situe à 19%. Un membre potentiel, Charlie, détient 1% des parts et choisit maintenant quel groupe rejoindre. Rejoindre le groupe d'Alice portera la participation totale du groupe à 21% et, comme il a dépassé le point de saturation, la récompense sera de 200 pièces (20% du total des récompenses). En déduisant les coûts opérationnels, il restera 175 pièces à distribuer entre Alice et les membres du groupe. Après avoir supprimé la marge bénéficiaire d'Alice et pris en compte la participation relative de Charlie dans le groupe, ce dernier recevra 8 pièces en récompense. Si Charlie rejoint le groupe de Bob, le total des récompenses sera de 200 pièces, ou 170 pièces après soustraction des coûts opérationnels. Cependant, étant donné que la participation de Charlie représente 5% (1/20) du groupe, il recevra 2% de pièces de plus que s'il avait rejoint le groupe d'Alice. Charlie rejoindra donc le groupe de Bob s'il veut maximiser ses récompenses.

Maintenant, voyons ce qui se passe dans le cas où Charlie est confronté à la même décision lorsque, à un stade hypothétique, le groupe d'Alice représentait déjà 20% de la participation total alors que le groupe de Bob n'était que de 3%. Dans ce cas, Bob a un très petit groupe et le total des récompenses disponibles pour ses membres est bien moindre que dans le cas précédent. En conséquence, si Charlie effectuait le même calcul pour le groupe de Bob, sa participation de 1% donnerait une participation totale de 4% pour le groupe mais, après calcul il ne recevrait que 30% des récompenses qu'il aurait obtenu s'il avait rejoint le groupe d'Alice. Dans un tel cas, la décision rationnelle est de rejoindre le groupe d'Alice, alors même que son adhésion fera en sorte que le groupe dépassera le point de saturation. Voir le tableau 1 ci-dessous pour les chiffres exacts.

Groupe	Taille du Groupe	Coût	Marge	Récompense de Charlie
Alice	20 %	25	4 %	8
Bob	19 %	30	4 %	8,16
Bob (au début)	3 %	30	4 %	2,4
Brenda	19 %	33	2 %	8,183
Ben	19 %	36	1 %	8,118

Tableau 1. *Charlie, qui détient 1% de la participation totale, envisage de rejoindre les groupes gérés par Alice, Bob, Brenda et Ben. Sa récompense est calculée en pièces. La récompense totale est de 1000 pièces et le point de saturation est fixé à 20%.*

Être prévoyant, ça compte

Ce qui précède semble être contradictoire. Pour comprendre ce que Charlie doit faire, nous devons comprendre le fait suivant. Le choix de Charlie de rejoindre le groupe d'Alice dans le deuxième scénario (celui ou Bob est à 3 %) n'est rationnel qu'à très court terme (ou myope). De fait, et comme le montre le premier scénario (Bob à 19 %), le groupe de Bob est meilleur pour Charlie à condition que le groupe de Bob atteigne le point de saturation. Ainsi, si Charlie pense que le groupe de Bob atteindra le point de saturation, le choix rationnel serait de le soutenir. D'autres parties prenantes feront de même et le groupe de Bob atteindra rapidement le point de saturation, augmentant les récompenses de tous ceux qui y ont participé, tout en soutenant en même temps l'idéal de la décentralisation : au lieu de s'agrandir constamment, le groupe d'Alice s'arrêtera au point de saturation et les autres auront la possibilité de croître à la même taille. Ce type de réflexion stratégique de la part des parties prenantes est plus avisé (non myope) et, comme nous le verrons, a la capacité d'aider à converger vers des configurations décentralisées souhaitables pour le système.

Il est inévitable que durant son évolution, le système atteigne des moments cruciaux dans lesquels il sera essentiel que les parties prenantes exercent une réflexion à long terme, comme dans le scénario ci-dessus où le groupe d'Alice atteint le point de saturation alors que les autres sont encore petits. La raison est qu'étant donné les circonstances propres à chaque gestionnaire de groupe d'enjeu, les coûts opérationnels varieront en fonction de la population des parties prenantes. Il faut donc s'attendre à ce que, à partir du point zéro où il n'existe aucun groupe d'enjeu, le groupe présentant le coût d'exploitation le plus bas sera également le premier à se développer. Cela est naturel dans la mesure ou des coûts opérationnels bas laissent une plus grande récompense à répartir entre les membres du groupe. On peut s'attendre à ce que le système atteigne des moments, comme celui du deuxième scénario ci-dessus, où le groupe le plus compétitif (celui d'Alice avec un coût opérationnel de 25 pièces) a atteint le point de saturation, tandis que le deuxième le plus concurrentiel (celui de Bob avec un coût opérationnel de 30 pièces) est encore à un faible niveau d'adhésion.

On pourrait être tenté d'envisager une réflexion à long terme basé sur un système de partage des récompenses de type Bitcoin et penser qu'il peut lui aussi aider à converger vers la décentralisation. Malheureusement, ce n'est pas le cas. Dans un système similaire à Bitcoin - contrairement à notre système de partage des récompenses avec point de saturation - il ne sert à rien de développer les groupes d'Alice et de Bob avec l'idée que le groupe de Bob deviendra plus

attrayant aux yeux de Charlie. En effet, sans point de saturation, le plus grand groupe d'Alice offrira toujours plus de récompenses à Charlie : cela tient au fait que les coûts opérationnels d'Alice sont moins importants et qu'ils laissent donc plus de récompenses à toutes les parties prenantes. Cela laissera le groupe de Bob sans aucun membre et, comme indiqué ci-dessus, le choix rationnel pour Bob sera de dissoudre son groupe et de rejoindre Alice, faisant d'Alice le dictateur du système.

Pour en revenir à notre programme de partage des récompenses, nous avons établi qu'une stratégie non-myope favorise la décentralisation ; toutefois, il reste un point important. À un moment crucial, lorsque Charlie - acteur non-myope - décide rationnellement de renoncer à rejoindre le groupe saturé d'Alice, il peut choisir parmi un certain nombre d'autres groupes. Par exemple, avec le groupe de Bob qui a des coûts opérationnels de 30 et une marge bénéficiaire de 4%, le groupe de Brenda avec un coût opérationnel de 33 et une marge bénéficiaire de 2%, et le groupe de Ben avec un coût opérationnel de 36 et une marge bénéficiaire 1%. Le choix rationnel serait d'aller chez celui qui atteindra le point de saturation ; Y a-t-il un moyen de prédire lequel sera le meilleur choix ? Dans notre document d'analyse complet, nous fournissons un mécanisme explicite qui classe les groupes en fonction de leur désirabilité en utilisant les informations concernant chaque groupe d'enjeu et consignées dans le registre. Cela peut aider les parties prenantes à faire le meilleur choix à tout moment. Dans notre exemple, c'est le groupe de Brenda que Charlie devrait rejoindre s'il veut maximiser ses récompenses (voir tableau 1). Pour aider les utilisateurs de Cardano, ce mécanisme de tri des groupes sera intégré à Daedalus (et à d'autres portefeuilles compatibles avec Cardano) et offrira aussi une représentation visuelle des meilleurs choix à faire pour les parties prenantes, en utilisant les informations relatives aux inscriptions dans les groupes contenues dans le registre.

Évaluation expérimentale

Comment se comporte notre système de récompense pour ce qui est de la décentralisation ? Dans notre analyse complète, nous prouvons qu'il existe une classe de configurations de systèmes décentralisés qui sont des "équilibres de Nash non-myopes". Une stratégie d'équilibre signifie ici que les parties prenantes disposent d'un moyen spécifique de créer des groupes, d'en définir les marges de profit et/ou de déléguer leurs actifs à d'autres groupes, de sorte qu'aucune partie prenante ayant une vision à long terme n'ait intérêt à suivre une stratégie différente. De plus, nous démontrons expérimentalement que le jeu entre acteurs ayant une pensée non-myope converge rapidement vers cet équilibre, comme le montre la figure 2.

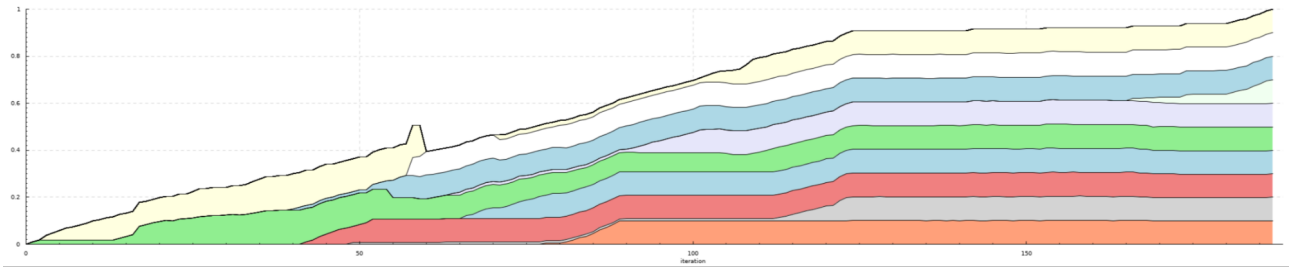

Figure 2. *Décentralisation observée avec notre système de partage des récompenses dans une simulation avec 100 parties prenantes et un point de saturation fixé à 10%. Les groupes sont progressivement créés par les parties prenantes. À tour de rôle, les parties prenantes tentent de maximiser leurs récompense de façon non-myope, ce qui aboutit à un point de convergence comportant 10 groupes, avec chacun une part égale de la participation totale. À la fin, aucun participant rationnel ne souhaite changer l'état du système.*

Une caractéristique de notre approche est que le nombre de groupes n'est qu'une partie de la description du système de partage des récompenses et n'est donc nullement imposé par le système aux parties prenantes. Cela signifie que les parties prenantes sont libres d'expérimenter avec la création de groupe et la délégation de participation sans se conformer à aucune architecture prédéterminée. Cela est en contraste avec les autres approches adoptées par d'autres systèmes PoS, tel que EOS, dans lequel le nombre de groupes est un paramètre fixe du système de consensus (plus précisément, 21 groupes). Dans le même temps, notre approche permet à l'ensemble des parties prenantes d'exprimer leur volonté, en rejoignant et en quittant librement des groupes, en recevant des récompenses garanties pour leur participation tout en témoignant de l'impact positif de leurs actions sur la gestion du registre distribué, et ce quelque soit la somme de leurs actifs en jeu. Cela est aussi en contraste avec d'autres approches dans les systèmes PoS, tel que Ethereum 2.0, dans lequel la maintenance du registre est effectuée par des validateurs enregistrés sur la base d'un dépôt de garantie et sans processus de vérification par l'ensemble des parties prenantes.

Quel est alors le choix judicieux du nombre de groupes à atteindre dans le système de récompense de Cardano? Étant donné que la décentralisation est notre objectif principal, il est judicieux de définir ce paramètre au plus haut possible. Nos expériences de réseaux ont montré que le système peut toujours fonctionner efficacement avec 1 000 groupes en même temps. En choisissant un seuil de saturation pour notre système de partage des récompenses basé sur ce nombre, il sera rentable de disposer d'un groupe d'enjeu, même si la participation totale qui y est déléguée ne représente que 0,1% de la circulation totale d'Ada.

Prévoir - Les attaques 'Sybil'

Étant donné que la décentralisation peut être réalisée par un grand nombre de groupes indépendants, il est également important de voir si certaines configurations du système décentralisées sont plus préférables que d'autres. Comme décrit jusqu'ici dans notre article, notre système de partage des récompenses dirigera les parties prenantes rationnelles vers la promotion des groupes d'enjeu qui auront les coûts le plus faible. Même si cela maximise les récompenses et minimise les coûts, il ne s'agit pas forcément du résultat le plus souhaitable. La raison en est qu'au point d'équilibre, on peut voir un ensemble de parties prenantes promues en tant que gestionnaires de groupes d'enjeu et qui possèdent collectivement très peu d'enjeu. Ce déséquilibre, dans lequel un faible montant d'enjeu représente l'ensemble de l'enjeu du système, peut être préjudiciable à bien des égards : les gestionnaires de groupes d'enjeu peuvent être enclins à la corruption, ou peut-être pire encore, un acteur important peut enregistrer de nombreux groupes d'enjeu dans l'espoir de contrôler l'ensemble de l'écosystème, réalisant ainsi une attaque de type 'Sybil' qui nuirait à la décentralisation. Pour cette raison, le schéma de partage des récompenses présenté dans notre document d'analyse complet est modifié de manière à tenir compte de l'enjeu adossé au groupe (un fond de garantie), de sorte que ce type de comportement soit atténué. Nous approfondirons cet aspect du partage des récompenses de Cardano dans un prochain article de blog.

Création artistique, Mike Beeple

Traduction : Malick Mbengue ; @psychomb