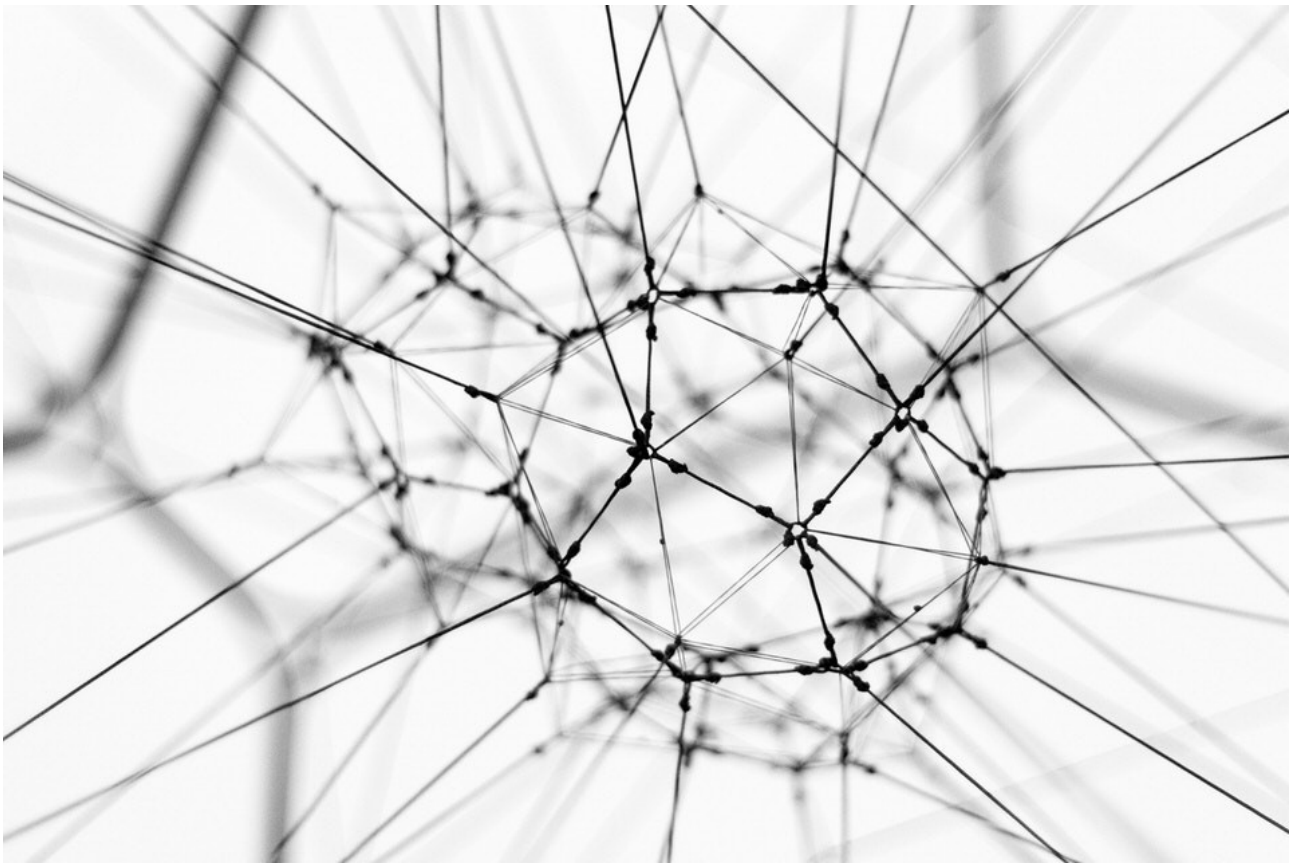


A quel point Cardano est-il décentralisé ? Une comparaison Bitcoin / Cardano

2 Mai 2019 - Auteur : @undersearcher - Traduction/adaptation : @psychomb

Charles Hoskinson, P.D.G. de l'entreprise technologique qui construit Cardano (Input Output Hong Kong, I.O.H.K.), a récemment déclaré que *"Cardano sera 100 fois plus décentralisé que Bitcoin"*. En disant cela, il fait référence au fait que Cardano utilise des incitations financières afin de diversifier le nombre de pools d'enjeu - jusqu'à 1000 - qui existeront dans le système. Hoskinson suppose aussi implicitement que les 10 plus grands mineurs de Bitcoin contrôlent plus de 50 % de la puissance de calcul total du réseau, ce qui signifie que Cardano aura cent fois plus de nœuds qui créeront des blocs sur le réseau. Cependant, s'agit-il d'une mesure juste de la décentralisation ? Et à quel point Cardano supporte-il la comparaison à Bitcoin sur d'autres aspects tel que le contrôle du réseau ?

Qu'est ce que la décentralisation ?

Lorsque l'on cherche une définition, il est tentant de commencer par une simple recherche sur le Web. Par exemple, c'est ainsi que la décentralisation est définie sur Wikipedia :

*"La décentralisation est le processus par lequel les activités d'une organisation, en particulier celles qui concernent la planification et la prise de décision, sont réparties ou déléguées en dehors d'un lieu ou d'un groupe central faisant autorité." - **Wikipédia***

Bien qu'utile, il s'agit d'une définition assez large, qui mériterait d'être précisée un peu - en particulier pour ce qui est des cryptomonnaies. Il existe de nombreuses définitions différentes de ce concept, illustrant dès lors que ce concept n'est pas toujours facile à quantifier. L'exercice est

donc difficile si l'on souhaite tracer une ligne claire entre ce qui est décentralisé et ce qui ne l'est pas. Une description que je trouve particulièrement utile est celle du fondateur d'Ethereum, Vitalik Buterin. Buterin divise ce concept en trois aspects :

- *Décentralisation architecturale* - le nombre de nœuds de consensus dont le système est composé ; c'est ce à quoi Hoskinson a fait référence plus tôt.

- *Décentralisation politique* - combien d'entités contrôlent les logiciels sur lesquels ces nœuds fonctionnent ; ce que l'on appelle aussi souvent la "gouvernance".

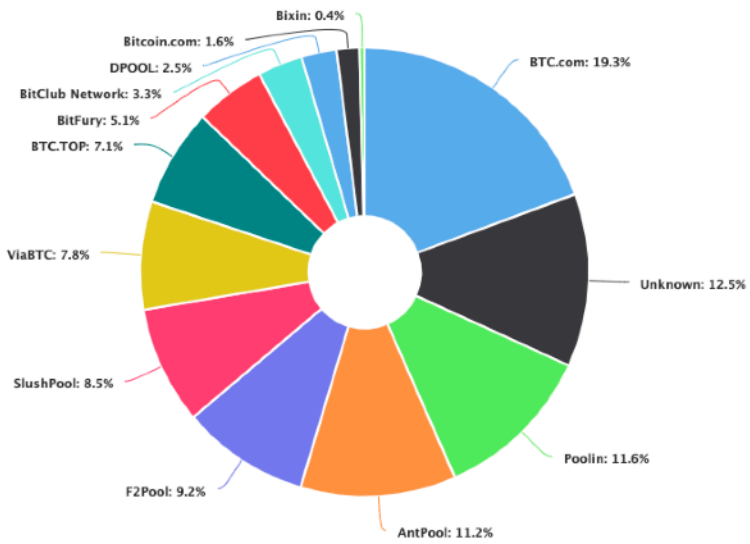
- *Décentralisation logique* - si vous coupez le système en deux, les deux moitiés continueront-elles à fonctionner pleinement comme des unités indépendantes ? Comme Buterin le décrit dans son article, les blockchains sont logiquement décentralisées de par leur conception ; il existe un état accepté de tous et le système se comporte comme un seul ordinateur.

Puisque Buterin a déjà donné ici la réponse à la question de la "décentralisation logique", abordons plutôt le reste dans cette liste.

L'architecture de Bitcoin est-elle décentralisée ?

Au moment d'écrire ces lignes, le réseau Bitcoin se compose d'une puissance de calcul de 56 029 PH/s, ce qui représente des plusieurs milliers de fois celui du second réseau (Ethereum ; 138 TH/s). À l'heure actuelle, il en coûterait 520 000 $ de l'heure pour effectuer une attaque 51 % sur Bitcoin. Bien que coûteux, si que les avantages (par ex. doubler les dépenses) l'emportent sur les coûts, cela pourrait bien en valoir la peine. Mais cela ne serait bénéfique pour l'attaquant que si il est capable de doubler les dépenses d'une transaction de plus d'un demi-million de dollars.

Comme Hoskinson l'a laissé entendre plus haut, à l'heure actuelle, seule une poignée de mineurs contrôlent la majorité de la puissance de calcul du réseau Bitcoin. Pour être plus précis, à la date de parution de cet article, les 4 plus grands mineurs contrôlent 51,3% de la puissance de calcul (voir figure ci-dessous). Si ces opérateurs se réunissaient, ils pourraient en théorie réussir une attaque 51% sur le réseau.



En réalité, il en faut plus pour effectuer une telle attaque. Comme décrit dans un article de “Stop And Decrypt”, des nœuds complets non mineurs valident aussi la blockchain (par ex. les nœuds Casa ou NODL) et jouent donc un rôle dans le consensus global. Il existe aujourd’hui 9 444 noeuds de validation sur le réseau Bitcoin. Ces nœuds forment un maillage complexe qui empêche les transactions invalides d'être incorporées dans la blockchain Bitcoin. Toute attaque 51% réussie dans Bitcoin signifierait donc que ce réseau de noeuds de validation annexe est lui aussi “trompé”, par exemple par l'attaquant contrôlant lui-même des milliers de ces noeuds - ce qui serait en pratique extrêmement lourd.

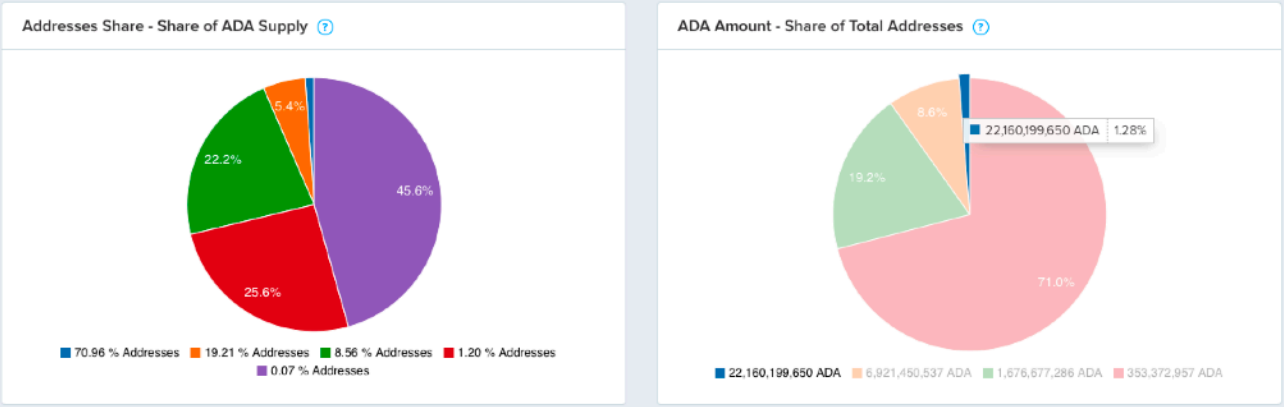
Jusqu'à présent, le réseau Bitcoin a été fonctionnel 99,98% du temps depuis plus de 10 ans sans qu'une attaque 51% réussie connue ne soit exécutée. Au fur et à mesure que le prix et l'adoption de Bitcoin augmentent, ce dernier attire de plus en plus de mineurs et de personnes exploitant des nœuds complets, ce qui rend le réseau de plus en plus sécurisé. A ce stade, Bitcoin est donc sans doute la cryptomonnaie la plus décentralisée d’un point de vue architectural.

L'architecture de Cardano est-elle décentralisée ?

Actuellement, Cardano est un système fédéré dans lequel I.O.H.K., Emurgo et la Fondation Cardano contrôlent l'écosystème dans son ensemble - y compris les 7 groupes d’enjeu en fonction. Quand Hoskinson a déclaré que “*Cardano sera cent fois plus décentralisé que Bitcoin”*, il faisait donc référence au nombre de groupes d’enjeu attendus pour gérer Cardano après la prochaine mise à jour intitulée “Shelley” - la phase de la feuille de route qui comprendra la décentralisation de l'architecture du réseau. La base du code de cette phase comprendra une structure incitative dans laquelle les groupes d’enjeu seront incités financièrement à ne pas dépasser une certaine taille, ce qui encouragera la création de groupes d’enjeu jusqu'à 1000 groupes. Si vous voulez en savoir plus sur le fonctionnement de ce système, je vous encourage à lire mon article précédent “***A quel point Cardano est-il sécurisé ?*** Partie 1 / Partie 2”.

Si la décentralisation du réseau est définie comme le nombre de nœuds créant des blocs sur le réseau, la déclaration d'Hoskinson serait même une sous-estimation, car elle serait en fait (1000/4=) 250 fois plus décentralisée. Toutefois, puisqu'une seule entité peut en réalité gérer de nombreux groupes d’enjeu (par ex. Hoskinson a déclaré que I.O.H.K. en gérera environ 80), la distribution réelle de la cryptomonnaie parmi les participants est le facteur le plus déterminant pour mesurer la décentralisation de Cardano.

Comme les adresses de la blockchain sont anonymes et qu'une personne ou entité peut contrôler plusieurs adresses, il est impossible de prouver qu'une seule entité ne contrôle pas plusieurs d'adresses. Néanmoins, un audit des transactions UTxO au sein des adresses de Cardano est actuellement la meilleure mesure dont nous disposons pour révéler la distribution de cryptomonnaie. La figure ci-dessous montre la répartition des ADA entre toutes les adresses actuelles de Cardano.



Source: Adascan.net (2 Mai 2019)

Comme le montre la figure, les 1,28 % des adresses Cardano les plus importantes détiennent 71,2 % de l'offre totale d'ADA (31,1 milliards). Notons que cela comprend un certain nombre d'adresses extrêmement riches comme celles de plateformes d'échanges, I.O.H.K., Emurgo et la Fondation Cardano. Cela est décrit plus clairement dans "liste des riches" ci-dessous, décrivant les 10 principales adresses détentrices d'ADA.

Rank	Address	Balance (ADA)	Share	Transactions	Last Activity
#1	Binance_4	3,851,793,745.591150	12.380300%	181	2019-04-12 08:09:31
#2	IOHK_2	2,414,658,192.000000	7.761109%	25	2018-12-28 14:21:51
#3	Ae2tdPwUPEZ4HkWASSoJi...XuT8so28CM5FXbQgGJodY	714,056,913.754498	2.295097%	1	2019-04-29 13:01:11
#4	CardanoFoundation_2	648,176,761.600000	2.083347%	8	2018-06-27 16:23:51
#5	DdzFFzCqrhsnSx4tTAmbP...o8EzQaZdqRfh8qdRJ6RHK	522,854,304.131068	1.680540%	1	2019-04-26 09:48:11
#6	DdzFFzCqrhswYBdxQvKFK...nP7yFC3bLTHDh2SWhHPZ4	515,694,887.134896	1.657528%	4591	2019-05-02 15:21:31
#7	DdzFFzCqrht8FaAf9FYJ4...SyQ2WmEZSZyT8cEwfZ3Mi	414,626,935.883804	1.332679%	1	2019-04-30 04:34:31
#8	DdzFFzCqrht3S2wCyTzWg...UJCJCNyI79d2XDjAV5fjy	249,788,425.700000	0.802861%	116	2019-04-12 17:26:51
#9	DdzFFzCqrht9fr6x1891n...w8Mvjpzb3CR8j5GM7L2va	200,000,000.000000	0.642833%	2	2018-05-05 10:54:31
#10	DdzFFzCqrhseMuShaXzLD...rf3H6LjpvK3dFsf8yZ6qo	189,041,127.603200	0.607609%	130	2018-12-15 21:36:51

Source: Adascan.net (2 Mai 2019)

Selon la façon dont vous interprétez les définitions de Buterin (voir début de cet article), cela pourrait être considéré à la fois comme une "décentralisation architecturale" et une "décentralisation politique". Quoi qu'il en soit, on pourrait soutenir que la distribution actuelle des pièces de Cardano a besoin d'être améliorée, particulièrement si l'on veut dire que Cardano est décentralisé de façon optimale après la sortie de Shelley. Qu'en est-il de la décentralisation politique ?

Bitcoin est-il politiquement décentralisé ?

Jameson Lopp a déjà très bien décrit qui contrôle Bitcoin - ce qui était littéralement le titre de son article. Je vais essayer de le résumer en termes simples.

Bitcoin est un logiciel libre, ce qui signifie que n'importe qui peut auditer le code et proposer des améliorations (“Bitcoin Improvement Proposals” ou “BIP”). Que ce code soit réellement implémenté dans le logiciel Bitcoin ou non dépend d'un processus social. Un certain consensus est nécessaire pour convaincre les développeurs principaux de l'implémenter dans le logiciel.

Si aucun consensus social ne peut être trouvé, n'importe qui peut toujours choisir de copier la base de code de Bitcoin, d’y intégrer des changements et de créer sa propre version du logiciel,. Cette bifurcation peut être compatible avec les règles du réseau original (bifurcation douce) ou non (bifurcation dure). Les mineurs décident ensuite de la version du logiciel qu'ils choisissent d'exécuter. Dans le cas d'une bifurcation dure, cela signifie essentiellement qu'ils votent quelle version de la chaîne sera “l'état réel", assurant ainsi la décentralisation logique qui a été mentionnée précédemment.

Bifurquer la base du code de Bitcoin afin de changer réellement “la vraie version” de Bitcoin n'a donc de sens que si vous êtes sûr qu'il existe un consensus social autour des mineurs et que votre version du logiciel sera prise en charge. C'est pourquoi Bitcoin est en partie une innovation sociale, plutôt qu'une innovation purement technologique. L'œuvre phare de Hasu, “Unpacking Bitcoin's social contract”, le décrit également.

En raison de la nécessité d'un consensus social sous l'égide des promoteurs et/ou des mineurs pour mettre en œuvre tout changement significatif du système, on peut donc soutenir que Bitcoin est politiquement décentralisé. Toutefois, il convient de noter que pour participer de manière significative à ce mécanisme de gouvernance, il faut soit des compétences techniques, soit posséder une grande puissance de calcul.

De plus, en raison de la complexité de ce processus social, le rythme réel des innovations techniques sur la couche de base de Bitcoin est très lent. Pour beaucoup de gens, c'est l'une des caractéristiques les plus importantes de Bitcoin : l’immutabilité (ou immuabilité) d'un point de vue social. Ces personnes souhaitent que la couche de base de Bitcoin reste simple et sûre, et espèrent voir une éventuelle ossification du protocole, ce qui signifie que la couche de base restera inchangée, tandis que les innovations se produiront sur différentes couches du système (par exemple, le réseau “Lightning”).

Pour d'autres, ce manque d'adaptabilité a été une raison d'aller de l'avant et de lancer de nouveaux projets, visant à développer des couches d'infrastructures basées sur une perspective différente. Cardano est l'un de ces projets.

Cardano est-il politiquement décentralisé ?

Comme mentionné précédemment, Cardano fonctionne actuellement sous le contrôle de la fédération I.O.H.K. / Emurgo / Fondation Cardano. I.O.H.K. fait de la recherche fondamentale et développe la technologie elle-même, Emurgo s'efforce d'attirer les entreprises dans l'écosystème et la Fondation Cardano vise, entre autres, à renforcer la communauté. Bien que plus décentralisé qu'un groupe unique contrôlant tout, ce mode de fonctionnement n'est aujourd'hui manifestement pas “politiquement décentralisé”. Cependant, I.O.H.K. a des plans très ambitieux pour Cardano lorsqu'il s'agit de “résoudre” sa décentralisation politique.

L'un des aspects clés de Cardano est qu'il aura sa propre trésorerie (ou Trésor), combinée à un système de gouvernance sur la blockchain qui permettra aux parties prenantes de décider quels développements seront financés par cette trésorerie, ainsi que les propositions d'amélioration qui seront mises en œuvre dans le système. Ce mécanisme de gouvernance sera fondé sur une démocratie liquide (décrite plus en détail dans la dernière partie de cet article).

Comme pour Bitcoin, la base du code de Cardano sera libre et n'importe qui peut soumettre des propositions d'amélioration au système. Le consensus social décidera quelles propositions seront effectivement mises en œuvre. Contrairement à Bitcoin, le pouvoir de décision dans ce cas est directement entre les mains des personnes qui détiennent la cryptomonnaie du système. En raison de l'instabilité de la démocratie, les gens peuvent choisir soit de voter directement eux-mêmes, soit de déléguer leur vote à quelqu'un qui, à leur avis, est mieux informé sur le sujet. Cela signifie que pour participer de manière significative au mécanisme de gouvernance de Cardano, il faut soit avoir les connaissances techniques nécessaires pour élaborer une proposition d'amélioration, soit détenir beaucoup de pièces.

Les deux mécanismes de gouvernance (Bitcoin et Cardano) sont donc tous les deux fondés sur des processus sociaux, la différence la plus frappante étant le rôle des mineurs dans un cas et des parties prenantes (possesseurs de cryptomonnaie) de l’autre.

Avantages et les inconvénients de la gouvernance sur la blockchain

Le système de gouvernance envisagé par Cardano, où les parties prenantes peuvent voter sur les propositions d'amélioration qui seront mises en œuvre et sur ce à quoi les fonds du Trésor seront dépensés, présente plusieurs avantages :

- Le système est autofinancé, ce qui signifie qu'une incitation monétaire à créer des propositions d'amélioration avec une forte probabilité de trouver un consensus social est intégrée.

- Les incitations des parties prenantes sont alignées sur l'intérêt à long terme du système lui-même, car l'acceptation de propositions qui nuisent à la valeur du système nuira également à la valeur nette des parties prenantes.

- En abaissant le seuil d'entrée - comparé à l'acquisition d'équipement spécialisé pour mineurs (ASIC) dans le cas de Bitcoin et de la plupart des systèmes PoW -, n'importe qui peut participer aux décisions de gouvernance,

- L'utilisation de la gouvernance sur la blockchain, la recherche d'un consensus social et la mise en œuvre des résultats seront probablement plus efficaces, ce qui entraînera une innovation plus rapide et un risque moindre de bifurcations et donc de fractionnement de la communauté.

Tout cela peut sembler attrayant, mais le vote sur la blockchain basé sur les enjeux présente aussi des inconvénients. Il en existe deux qui sont particulièrement importants ici.

Premièrement, si les parties prenantes sont incitées à prendre des décisions qui sont dans l'intérêt à long terme du système, elles n'ont pas nécessairement les connaissances nécessaires pour prendre les meilleures décisions qui soient, ce qui signifie qu'elles pourraient être persuadées de prendre des décisions illicites ou dommageables. On pourrait appeler cela une "attaque sociale". Même si une telle attaque est possible dans n'importe quel système qui dépend d'un consensus social et que les décisions peuvent probablement être inversées lors d'un vote futur, le faire dans un système où le résultat du vote sur la blockchain est automatiquement appliqué a des conséquences plus directes que dans un système comme Bitcoin. Aujourd'hui, très peu de détails sur le fonctionnement du système de vote sur la blockchain de Cardano sont disponibles (la mise en œuvre est prévue pour la fin de 2020), de sorte que le temps dira dans quelle mesure cette préoccupation est fondée.

Le deuxième inconvénient peut en fait être déduit à partir de la conception fondamentale des systèmes de PoS en général. Comme décrit dans **"A quel point Cardano est-il sécurisé ?** Partie 1 / Partie 2", une fois qu'un attaquant (ou un groupe d'attaquants) est capable de collecter >50% de toutes les enjeux du système (ce qui serait très coûteux et prendrait probablement beaucoup de temps), il n'y a essentiellement aucun moyen pour la minorité honnête de reprendre le contrôle du système - du moins de manière non-violente. Après tout, enlever les jetons de monnaie de l'attaquant en bifurquant le système signifierait que l'immutabilité du système est terminée. Dans les systèmes PoW comme Bitcoin, il n'est pas non plus possible de supprimer la puissance de calcul de l'attaquant, mais contrairement aux systèmes PoS, où l'enjeu est nécessaire, la minorité honnête pourrait ici ajouter de la puissance de calcul afin de récupérer la majorité.

La distribution d'ADA est-elle un problème pour Cardano ?

I.O.H.K., Emurgo et la Fondation Cardano ont vendu des bons d'achat entre septembre 2015 et janvier 2017. En raison des incertitudes réglementaires, cela a été fait dans une zone géographique très spécifique. Au total, 20 % (~5,19 milliards ADA) de l'approvisionnement total (~31,12 milliards ADA) ont été distribués à la I.O.H.K., à Emurgo et à la Fondation Cardano. Selon l'audit de la distribution, 94,45 % du reste de l'ADA a été vendu à des citoyens japonais, 2,56 % à des Coréens, 2,39 % à des Chinois et 0,61 % à des citoyens de cinq autres pays asiatiques.

Outre la question de savoir si cette distribution géographique étroite et la distribution globale actuelle des ADA posent un problème pour la décentralisation de Cardano (sans réponse ici), il est

également intéressant de se demander si cette méthode de distribution elle-même ne pourrait pas se révéler être une limitation quant à l'acceptabilité sociale de l'ADA comme forme de monnaie.

La raison en est que certaines personnes - en particulier les puristes de Bitcoin et du PoW - semblent croire que le simple fait de créer des pièces de monnaie et de les vendre au public ne peut donner lieu à une forme de monnaie qui possède une valeur fondamentale. Cette croyance découle du principe de “coûts infalsifiables” qui a été introduit par Nick Szabo dans son article de 2002 intitulé “Shelling Out : Les origines de l’argent". Dans son article, Szabo décrit que pour qu'une forme de monnaie ait de la valeur, elle doit être difficile à créer et cette difficulté doit pouvoir être vérifiée par toute partie. Pour certains, c'est donc la consommation réelle d'énergie requise par le calcul qui garantit que les bitcoins ont une valeur.

Si vous supposez que c'est vrai, vous pouvez soutenir que les bons ADA qui ont été initialement vendus ne possédaient pas cette propriété, mais qu'ils tiraient leur valeur par anticipation du futur écosystème de Cardano. La question de savoir s'il est “juste et bien” que ces entités puissent créer ces bons, en conserver 20 % et vendre le reste pour 63 millions de dollars afin de financer essentiellement le développement de Cardano est également subjective (cette question restera sans réponse ici).

Cependant, si l'on se base sur la quarantaine d'articles scientifiques (dont 20 ont été examinés par des pairs et sont pour la plupart en libre accès) qui ont été produits jusqu'à présent et qui ajoutent de la valeur à tout l'espace et à la création d'une nouvelle cryptomonnaie développée de manière très rigoureuse, on pourrait soutenir à l’inverse que beaucoup d'efforts vérifiables ont été faits. De plus, une fois que le lancement de Shelley sera terminé et que les nouvelles pièces ne pourront être frappées qu'après avoir participé équitablement au protocole, il n’est pas certain que les préoccupations concernant l'impossibilité de falsifier les coûts seront toujours valables. Personnellement, je n'ignore donc pas la possibilité que l'ADA puisse devenir une forme d'argent socialement acceptée basée sur ce principe - ce qui, après tout, n'est que de la théorie.

Conclusions

Par rapport aux systèmes PoW comme Bitcoin, les systèmes PoS comme Cardano présentent des avantages tels qu'une consommation d'énergie et des exigences matérielles réduites, mais aussi des inconvénients comme le fait de ne pas pouvoir reprendre le contrôle après une attaque réussie à 51% sans bifurcation dure.

Les systèmes de PoS comme Cardano dépendront toujours d'un ensemble différent d'avantages et de compromis par rapport aux systèmes de PoW comme Bitcoin. Dire “Cardano est mieux que Bitcoin” ou l’inverse est donc absurde ; ce sont des bêtes fondamentalement différentes avec des propriétés génétiques différentes.

Par exemple, il est tout à fait possible que les propriétés de la couche de base de Bitcoin et les réseau déjà construits garantissent sa fonction de réserve universelle de valeur et d'unité de compte, tandis que les solutions de seconde couche seront en fait les technologies qui capturent la majorité de l'utilisation quotidienne. De ce point de vue, il est fort possible que le réseau “Lightning” devienne un véritable concurrent de Cardano, et non la couche de base de Bitcoin.

L’espace des cryptomonnaies est très jeune pour savoir dès aujourd’hui quelles technologies deviendront les couches d'infrastructure que nous continuerons à utiliser au cours des prochaines décennies et au-delà. Le temps nous dira quelles couches d'infrastructure seront utilisées, à quelles fins et dans quelle mesure les systèmesPoW et PoS coexisteront et se compléteront.