A quel point Cardano est-il sécurisé ?

- Partie 2-

Traduction du blog-post de @belowsearcher "How secure is Cardano?" paru ici le 26 Janvier 2019 par @psychomb

Dans la première partie, nous avions vu que depuis la version Ouroboros Genesis, le protocole de consensus PoS de Cardano est le premier protocole PoS mathématiquement démontré comme garantissant la persistance et la vivacité dans un environnement à la fois synchrone et semi-synchrone, exactement comme Bitcoin. Par conséquent, il est plus sécurisé que d'autres protocoles PoS qui nécessitent au moins 2/3 de participants honnêtes, comme Casper (Ethereum) ou Algorand. Ouroboros est tout aussi sécurisé que Bitcoin, avec en bonus une dépense d'énergie bien inférieure et de meilleures performances.

Il reste toutefois un aspect d'Ouroboros que certains ne manqueront pas de soulever et cela est lié à sa nature de preuve d'enjeu.

Si Cardano est aussi sécurisé que Bitcoin pour ce qui est de se prémunir des attaques de type 51%, il n'en reste pas moins que Bitcoin a un avantage sur Cardano **après** (cas théorique) qu'une attaque 51% ait été exécutée. Chez Bitcoin, la minorité honnête des participants pourrait simplement ajouter de la puissance de calcul pour reprendre le contrôle du réseau, par exemple en ajoutant de nouveaux mineurs au réseau. Chez Cardano, une fois qu'un attaquant détient 51% des enjeux (ou des ADA en circulation, ce qui revient en

pratique au même), le contrôle du réseau ne peut être repris que si l'attaquant revend ses actifs ou alors en formant un nouveau registre sans lui : c'est ce que l'on appelle une 'fork'. Cependant, est-il possible que quelqu'un contrôle une telle masse d'enjeu ? Regardons donc les chiffres.

Comment ADA (la devise de Cardano) a-t-elle été distribué à l'origine ?

Dans un protocole PoS, miser un enjeu est obligatoire pour participer au mécanisme de consensus. L'existence de pièces de monnaie est donc requise pour exécuter le protocole, ce qui implique qu'une distribution des pièces était nécessaire au démarrage. En 2015, le concept des ICOs (Initial Coin Offering) devenait populaire, mais il était aussi à craindre que le fait de frapper monnaie, fusse-t-elle virtuelle, soit soumis à certaines règles. IOHK, Emurgo et la Fondation Cardano ont donc choisi de vendre 25 927 070 538 bons 'ADA' lors d'une vente privée au Japon et dans quelques autres pays asiatiques. Ces chèques étaient échangeables contre ADA après le lancement du réseau en septembre 2017.

Les puristes de Bitcoin, ceux qui pensent que seul Bitcoin a eu un lancement équitable, ont tendance à réagir négativement à l'idée de pouvoir créer et de vendre une nouvelle forme de monnaie. Au lancement de Bitcoin, Satoshi Nakamoto (le ou les inventeurs anonymes de Bitcoin) a d'abord partagé publiquement le code permettant d'exécuter un nœud de consensus Bitcoin, permettant ainsi à quiconque de participer au consensus du réseau dès son début. Bien que S. Nakamoto ait manifestement eu un avantage puisque peu de personnes connaissaient l'existence de Bitcoin à cette époque, le fait d'avoir eu un protocole ouvert très tôt à tous semble aujourd'hui une chose assez juste. De plus, il était alors loin d'être acquis que Bitcoin serait un succès. Cependant, le lancement récent de 'Grin Privacy' montre qu'un démarrage équitable dans le même esprit que Bitcoin n'est peut-être plus possible. Il se dit en effet que 100 millions de dollars de capital risque auraient été investis dans l'achat de calculateurs dédiés au minage de la pièce Grin… Le choix de la vente privée de Cardano était donc un compromis entre répartition géographique des acheteurs et certitudes réglementaires, ces dernières ayant été choisies en priorité.

Au total, 25 927 070 538 ADA ont été vendus entre septembre 2015 et janvier 2017 à plus de 10 000 personnes, pour un montant de 63 millions de dollars (0,0024 USD par ADA). Selon l'audit de distribution organisé pour le compte de la Fondation Cardano, 94.45% des ADA ont été vendus à des citoyens

japonais, 2.56% à des Coréens, 2.39% à des Chinois et les 0.61% restants à des citoyens de 5 autres pays asiatiques.

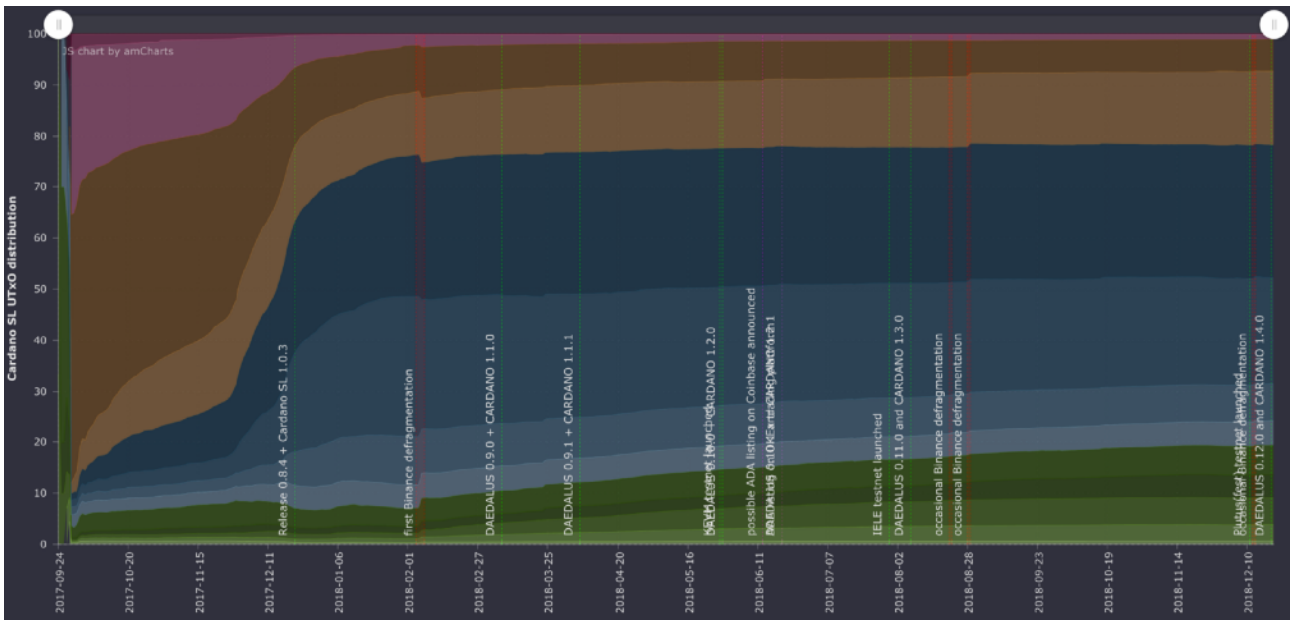
Les 5 185 414 108 ADA restants ont été répartis entre IOHK, Emurgo et la Fondation Cardano. IOHK a publiquement partagé son adresse ADA et un tiers des 2 463 071 701 ADA qu'ils ont reçus est disponible immédiatement (97,5% sont encore là), un tiers est mis à disposition le 1er juin 2018 et le dernier tiers le 1er juin 2019. Bien que la Fondation Cardano et Emurgo n'aient pas dévoilé publiquement leur adresse ADA, on pense qu'Emurgo détenait à l'origine 2 074 165 643 ADA et que la Fondation Cardano en détenait 648 176 763 ADA, la somme de ces montants totalisant exactement les 5 185 414 108 ADA à partager. Enfin, les 13 887 515 354 ADA restants sur les 45 milliards d'ADA qui existeront (offre maximale) seront utilisés comme récompense pour la fabrication des blocs par les noeuds de consensus.

Comment sont distribués les ADA aujourd'hui ?

Dans un système PoS, posséder des pièces équivaut à posséder un pouvoir. La vente initiale d'ADA s'étant faite sur une région géographique limitée, il est légitime de se demander si une distribution initiale sur un plus grand nombre de personnes n'aurait pas mieux aidé la décentralisation du réseau et donc sa sécurité.

La manière dont cela est réalisable (et réalisé) est simple ; les détenteurs de pièces doivent les vendre à des personnes qui n'en possèdent pas encore. Dans le cas de Cardano, la vente de bons 'ADA' a eu lieu au début d'un marché haussier, entre septembre 2015 et janvier 2017. Lorsque le réseau de Cardano a été lancé en septembre 2017, les acheteurs des bons ont reçu leur ADA tandis que la valeur de l'ADA s'était déjà grandement appréciée. En conséquence, lorsque les pièces ont été négociables sur les marchés, les investisseurs initiaux des bons 'ADA' ont ont vendu (certaines de) leurs pièces.

Le graphique ci-dessous est tiré d'une page Web créée par un membre du Forum Cardano, Markus (@Werkof), et donne une représentation de la distribution des pièces. Les couleurs représentent différentes catégories d'adresses contenant un certain nombre de pièces. Les couches supérieures représentent les adresses contenant de grandes quantités d'ADA. Par exemple : (i) violet = ADA 10M-100M, (ii) rose = ADA 1M-10M, (iii) brun foncé = ADA 100k-1M, (iv) brun clair = 10k-100k ADA, (v) bleu foncé = 1k- 10k ADA etc …



En décembre 2017, alors que Bitcoin atteignait un nouveau sommet et que les autres cryptomonnaies devenaient très populaires, le graphique ci-dessus montre un passage important des adresses les plus riches aux adresses plus petites. Tout au long du marché baissier de 2018, une légère diminution des deux couches supérieures peut être observée, bien que la tendance générale puisse être décrite comme une consolidation, car il n'y a pas de changements significatifs (pertinents) dans la distribution. Une hypothèse de principe peut donc être formulée selon laquelle des cycles de marché répétés pourraient améliorer encore la distribution des ADA, puisque les cycles haussiers incitent les détenteurs de pièces à vendre (certaines) leurs avoirs et que de nouvelles personnes peuvent être attirées par un ‘hype’ grandissant.

Dans un système UTxO (comptabilité particulière), une chose importante à comprendre est qu’un portefeuille peut gérer plusieurs adresses et qu’une seule personne peut gérer plusieurs portefeuilles. Cela donne à penser que le nombre d'adresses non vides surestime très certainement le nombre de personnes qui possèdent réellement des ADA. Le fait que les adresses de plateformes d’échanges contiennent également des pièces pour le compte de plusieurs personnes ne simplifie pas la tâche visant à analyser en détail la distribution des ADA. Bien que cela ne prouve pas nécessairement quoi que ce soit, il peut être utile d’analyser la quantité d’ADA détenue par les adresses les mieux fournies afin de mieux en appréhender la répartition globale. AdaScan et Clio.1 sont de très bonnes ressources à ce sujet, notamment à travers la 'Rich List’.

Au 21 Janvier 2019, bien qu'une seule de ses adresses soit répertoriée, il est clair que Binance est le plus gros détenteur d'ADA (voir ci-dessus). Les adresses ADA de I.O.H.K. et de la Fondation Cardano sont également visibles dans le top 5. Sur la base du nombre de transactions, il est probable que les adresses n°4 et n°7 de la 'rich list' soient également des plateformes d'échanges. Ce jour-là, ces 10 plus grands détenteurs d'ADA détenaient 30% de l'offre courante en ADA de Cardano. En poussant un peu l'analyse, il apparait que 1.34 % des adresses les plus fournies détiennent environ 72 % de l'offre courante en ADA. Ce chiffre est sans doute à revoir à la baisse étant donné que beaucoup d'adresse ne contiennent que du 'dust' (résidus de transactions UTxO).

Tirer des conclusions sur la probabilité d'une attaque 51% de Cardano sur la base de ces chiffres serait au mieux hasardeux et arbitraire. Cependant, il faudra observer de près la distribution des pièces et le nombre d'adresses actives au cours du temps, de manière à s'assurer qu'assez de personnes utilisent l'écosystème, renforçant alors l'idée qu'il est peu probable qu'une seule personne ou un groupe de personnes soit en mesure de contrôler 51% des actifs.

A ce propos, acquérir 51% des ADA : comment cela peut-il fonctionner?

À la date de rédaction de cet article, les mises d'enjeu ne sont pas encore possibles sur Cardano. Par conséquent, on ne sait pas quelle quantité de l'approvisionnement en ADA aujourd'hui en circulation sera dévolu à cette fonction une fois que cela sera possible. Toutefois, si une seule personne ou entité possédait 51% des ADA en circulation aujourd'hui (possédait ~12.5 milliards d'ADA), le contrôle du réseau serait garanti. Un ADA vaut ~0,04 USD au 21/01/2019, ce qui signifie que la capitalisation boursière actuelle de Cardano est de 1 114 118 098 $. Au prix actuel, un attaquant devrait donc posséder au moins 557 059 050 $ d'ADA pour être sûr qu'une attaque 51% puisse être exécutée sur Cardano. Sur la base du prix le plus élevé jamais observé pour ADA, ce montant serait de 17 milliards de dollars.

Si cela montre que l'attaquant mettrait littéralement beaucoup d'argent dans l'attaque du réseau, une telle acquisition pourrait être encore plus coûteuse en réalité. En effet, une telle pression d'achat entraînerait très probablement une forte augmentation du prix de l'ADA. Outre le prix lui-même, acquérir autant d'ADA serait difficile car pour le faire, le marché devrait extrêmement liquide.

En raison des possibilités limitées d'acheter actuellement de l'ADA (nombre de plateformes ou ADA est disponible), le volume global proposé par les échanges serait un point limitant pour l'attaquant.

Dans l'hypothèse la plus favorable pour l'attaquant, acquérir 50% de tous les ADA via des échanges, sur la base d'un volume d'échange similaire à ces jours derniers, prendrait plus de 34 jours. Cela voudrait aussi dire que personne d'autre n'achète des ADA, seulement l'attaquant…

Selon CoinMarketCap, les marchés ADA/USDT et ADA/BTC de Binance sont les deux marchés ADA les plus liquides et représentent 35% de l'ensemble des transactions ADA. Cependant, à la date de rédaction de cet article, 16.12 millions d'ADA seulement sont disponibles au total sur ces deux marchés. Dans l'hypothèse prudente selon laquelle cette quantité d'ADA serait disponible chaque jour, il faudrait plus de 1608 jours pour commercialiser 50% de l'offre en circulation. Cependant, en achetant quotidiennement tous les ADA disponibles sur le marché, le prix grimperait en flèche, attirant probablement de nouveaux vendeurs et peut-être aussi de nouveaux acheteurs. Quoi qu'il en soit, ces exemples (bien que simplistes) illustrent le fait qu'acquérir une majorité des ADA demanderait beaucoup de temps et beaucoup d'argent.

Conclusions

Il a été prouvé mathématiquement que le mécanisme de consensus de Cardano était sûr, en supposant que la majorité (> 50%) de ses participants soient honnêtes. Le fait que le mécanisme de consensus (Ouroboros) s'appuie sur cette hypothèse signifie que par définition, il ne résiste pas aux attaques de type 51%. Cela peut paraître problématique et peu rassurant, mais cela n'est pas différent de toute autre cryptomonnaie sur le marché. Comme l'a souligné le fondateur de Litecoin, Charlie Lee, après l'attaque de 51% sur Ethereum Classic :

"Par définition, une cryptomonnaie décentralisée est susceptible de subir une attaque de type 51%, que cela soit par la puissance de calcul, par les enjeux et/ou par toute autre ressource que l'on peut acquérir librement. Si une crypto ne peut pas être attaquée à 51%, elle n'est alors qu'un système soumis à une autorité et un projet centralisé." - Charlie Lee

Une attaque réussie à 51% sur Cardano aurait des implications majeures pour le système. Contrairement aux monnaies PoW, où le contrôle peut être repris

en ajoutant plus de puissance de calcul au réseau, dans un système PoS, le pouvoir d'un attaquant ne peut lui être retiré que si celui-ci vend ses pièces ou si la blockchain se fracture et produit une 'fork'.

D'un autre coté, puisqu'une attaque réussie contre Cardano à 51% obligerait l'attaquant à détenir la majorité (> 50%) de toutes les pièces d'enjeu, une telle attaque signifierait aussi que l'attaquant met littéralement "en jeu" une énorme somme d'argent. Un comportement malveillant pourrait potentiellement déprécier la valeur des pièces que l'attaquant utilise comme mise. Au prix actuel, est-ce que quelqu'un investirait des centaines de millions de dollars dans une cryptomonnaie pour ensuite attaquer le système, risquant ainsi de déprécier la valeur de l'investissement lui-même ?

Bien que cela soit une hypothèse non nulle, il semble peu probable qu'une attaque 51% se produise avec Cardano. Si une seule entité se donnait la peine d'acquérir 51% des ADA en circulation, il est sans doute plus probable que le pouvoir ainsi acquis serve à influencer les futures prises de décision se faisant par le biais du système de gouvernance (système de vote basé sur les enjeux) que Cardano a prévu de mettre en place. Le ou les attaquants pourraient ainsi faire passer automatiquement leurs propres propositions de financement qu'ils auront soumises eux-mêmes auprès de la trésorerie décentralisée de Cardano. Il n'en reste donc pas moins très important de répartir l'offre d'ADA entre de nombreuses personnes via la dynamique de marché, quelle que soit la manière dont le risque d'une attaque de 51% est évalué.

En fin de compte, il appartient au marché de décider de la manière dont les avantages et les inconvénients de Cardano pèsent par rapport à ceux d'autres cryptomonnaies comme Bitcoin. En substance, ce n'est pas la technologie elle-même qui détermine la valeur du produit, mais les phénomènes sociaux qui l'entourent. Par exemple, il est possible que le marché valorise fortement dans Bitcoin le concept de domination par la majorité honnête et le fait que la puissance de calcul puisse toujours être reconquise après une attaque de type 51% réussie. Dans ce scénario, le marché considérerait (et considère aujourd'hui) le bitcoin comme une valeur de réserve supérieure à toutes les autres, et notamment à Cardano.

Néanmoins, cela laisserait toujours à Cardano la possibilité d'être utilisé comme un moyen plus efficace et moins coûteux d'interagir entre les différents systèmes cryptos et d'offrir des contrats intelligents sécurisés. Dans ce scénario volontairement très contrasté, cela signifie que Cardano fonctionnerait

fondamentalement comme une chaîne latérale de Bitcoin. Cependant, plus le système de Cardano sera utilisé de manière intensive, plus il y aura des frais de transaction convertis en récompenses pour les propriétaires d'enjeu dans sa blockchain. Cela encouragera la participation à l'enjeu et réduira la pression de vente. Si la demande de pièces reste constante (posséder ADA est nécessaire pour payer les frais de transaction), le prix augmentera mécaniquement, rendant une attaque 51% plus chère et donc moins probable. Cela améliore la sécurité du système, ce qui en fait une meilleure valeur de réserve et donc plus compétitive en tant que devise, créant ainsi une boucle de rétroaction positive.

Il faudra du temps pour faire confiance au jeune système Cardano - en particulier par rapport au Bitcoin qui résiste déjà depuis plus de 10 ans et sans aucun problème connu. La base académique rigoureuse de Cardano est sans doute la meilleure possible, mais elle doit encore prouver qu'elle est résistante aux attaques du monde réel et qu'elle subira l'épreuve du temps sans fléchir, de manière à gagner la confiance des investisseurs. Pour justifier un prix de l'ADA croissant - point important dans la proposition de sécurité de Cardano -, il est essentiel que le système soit réellement utilisé. Ce n'est donc pas un hasard si c'est exactement ce sur quoi se concentrent I.O.H.K., Emurgo et la Fondation Cardano.

Nous remercions chaleureusement Ruslan Dudin et Nicolás Arqueros pour leur examen approfondi du projet d'article et leurs réponses aux questions techniques.