

Cardano franchit une étape importante de son développement

22 Mars 2019 - Auteur : Duncan Coutts - Traduction : @psychomb

Les ingénieurs concluent la phase “Byron”, au fur et à mesure de l'avancement des travaux de “Shelley”

Pour Cardano, la sortie de Cardano 1.5 marque le début du passage de l'ère Byron à l'ère Shelley et constitue une excellente occasion de décrire le travail en cours pour Shelley et les détails de cette transition.

Il y a environ six mois, tous nos efforts de développement se sont progressivement portés sur l'écriture du code de Shelley, et le travail a progressé rapidement depuis. Pour ce qui est du code relatif à Byron, la dernière grande tâche a été réalisée lors de la sortie de Cardano 1.4, et pour Cardano 1.5, nous avons limité notre travail aux seuls changements requis pour une transition en douceur vers Shelley.

La code de Shelley n'est pas seulement une extension du code de Byron, mais une fondation entièrement nouvelle. Nous avons profité de cette occasion pour démonter et reconstruire entièrement le système, en plus d'y inclure la nouvelle fonctionnalité de preuve d'enjeu et de délégation. En conséquence, nous avons pu remédier à un certain nombre de limitations architecturales présentes dans le code de Byron, et nous engager dans l'approche semi-formelle de développement logiciel dont je parle dans mes vidéos.

En particulier, nous avons maintenant des spécifications mathématiques formelles des règles de validation de la blockchain pour Byron et Shelley, et nous présenterons ces spécifications au “IOHK Summit” en avril prochain. Lorsque le développement sera terminé, nous serons en mesure de fournir la preuve que notre code met correctement en œuvre nos spécifications. Il s'agit d'un changement majeur pour ce qui est de la qualité d'un système et ce sera une première pour notre industrie toute entière.

Une transition en douceur

Nous devons, bien sûr, gérer très délicatement la transition de Byron à Shelley. Il ne s'agit pas seulement d'un changement significatif dans les règles, mais aussi d'une migration d'un code à un

autre. Nous nous sommes efforcés de faire en sorte que le processus de transition se déroule le plus harmonieusement possible.

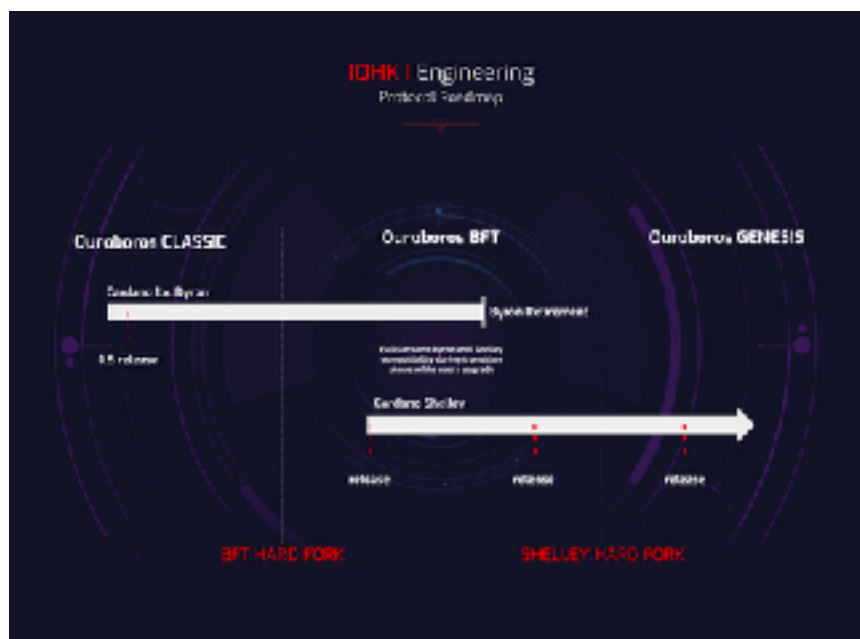
Bien que vous puissiez vous attendre à ce que la transition vers Shelly implique une seule bifurcation dure ou “hard fork” (*ndtr : pour raison pratique, nous parlerons de bifurcation*), il y aura en réalité deux bifurcations. Il convient de souligner que, même s'il s'agit de bifurcations, les perturbations associées ne seront pas aussi fortes qu'à l'accoutumé. Les changements ont été conçus pour utiliser notre système de mise à jour existant et être les plus doux possibles. Pour les utilisateurs de Daedalus, cela se fera comme n'importe quelle autre mise à jour.

Pour les deux bifurcations, nous déploierons une mise à jour qui inclut les règles de la nouvelle ère dans un état non activé, et qui sera activé quelques semaines plus tard. C'est la clé pour éviter des perturbations majeures : aucun logiciel n'est mis à jour au moment même où intervient la bifurcation. La mise à jour du logiciel a lieu plus tôt, et une fois que tout le monde est prêt, nous pouvons activer le changement en douceur.

La seule différence entre une bifurcation et une mise à jour régulière est qu'ici, la mise à jour est obligatoire entre la sortie du logiciel et l'activation de la bifurcation. Pour les utilisateurs de Daedalus, cela se fait via le système de mise à jour standard. Les plateformes d'échanges devront quant à elles être mises à jour manuellement, mais elles ont plusieurs semaines pour le faire.

Pourquoi deux bifurcations ?

Pour des raisons techniques, la transition de Byron à Shelley est plus simple si l'on passe par une période de transition intermédiaire. Ainsi, il y a une bifurcation pour entrer dans l'ère de transition, puis une deuxième pour débiter l'ère Shelley proprement dite. L'ère Byron utilise Ouroboros Classic, et l'ère Shelley utilise Ouroboros Genesis (qui est une extension de Ouroboros Praos). Ces deux protocoles sont complexes. Pour qu'une implémentation unique d'un nœud du réseau puisse gérer une bifurcation en douceur, il est nécessaire que cette implémentation comprenne à la fois les règles d'avant et après la bifurcation. Une bifurcation directe de Byron à Shelley nécessiterait donc qu'une seule implémentation comprenne à la fois le code d'Ouroboros Classic, d'Ouroboros Genesis, et de toutes les autres règles de validation additionnelles - ce qui est très complexe à réaliser.



De plus, la version d'Ouroboros Classic de Byron présente une complexité supplémentaire qu'il faudrait reproduire dans une nouvelle implémentation pour préserver un consensus parfait. Au lieu de cela, pour la période de transition nous utilisons Ouroboros BFT, une variante simple d'Ouroboros. Cela signifie que le code de Byron n'a qu'à comprendre Ouroboros Classic et Ouroboros BFT, tandis que le code de Shelley n'a qu'à comprendre Ouroboros BFT et Ouroboros Genesis. Ni l'un ni l'autre n'a besoin de comprendre Ouroboros Classic et Ouroboros Genesis en même temps. En particulier, cela signifie que le nouveau code de Shelley n'a pas besoin de reproduire chaque détail de l'implémentation d'Ouroboros Classic propre à Byron, ce qui permet une véritable réduction de la complexité - et dans le développement logiciel, la complexité est notre ennemi.

Une ère de transition

Ceci explique donc à quoi sert réellement la version 1.5 de Cardano : c'est la version dans laquelle le code de Byron commence à comprendre Ouroboros BFT, ce qui nous permet de terminer la première bifurcation en quelques semaines. Après cette première bifurcation, nous serons dans l'ère de transition qui utilise Ouroboros BFT et nous pourrons alors commencer à déployer le nouveau code au fur et à mesure qu'il sera développé. C'est ce nouveau code qui sera utilisé pour les versions ultérieures de Shelley, mais qui utilise toujours Ouroboros BFT pour une compatibilité parfaite pendant la transition.

Au cours de cette période de transition, nous procéderons également à un test de délégation et de preuve d'enjeu. Dans un premier temps, ce réseau test ("testnet") utilisera un sous-ensemble des règles de Shelley, mais nous le mettrons à jour au fil du temps jusqu'à ce que les règles complètes de Shelley soient mises en œuvre et que tout autre problème découvert durant le "testnet" soit résolu.

Une fois que nous serons satisfaits de la mise en œuvre complète des règles de Shelley, nous déploierons alors une mise à jour du nouveau code sur le réseau principal. Quelques semaines plus tard, nous activerons la bifurcation et nous serons enfin entrés dans l'ère Shelley sur le réseau principal !

En résumé, la version Cardano 1.5 est passionnante, non pas en raison des fonctionnalités majeures ou des nombreuses petites améliorations de Daedalus, mais parce qu'elle est le jalon qui marque le début de la fin pour Cardano Byron et le début du processus de transition vers Cardano Shelley.

Oeuvre : IOHK | Agency & Dimitris Ladopoulos