PPCoin : Crypto-monnaie pair-à-pair avec preuve d'enjeu

Sunny King, Scott Nadal
(sunnyking9999@gmail.com,scott.nadal@gmail.com)

19 août 2012

Résumé

Une conception de crypto-monnaie pair-à-pair (peer-to-peer) dérivée du Bitcoin de Satoshi Nakamoto.

La preuve d'enjeu (*proof-of-stake*) remplace la preuve de travail (*proof-of-work*) pour fournir la majeure partie de la sécurité de réseau. Sous cette preuve de travail de conception hybride, le monnayage initial est principalement fourni et n'est pas essentiel à long terme. Le niveau de sécurité du réseau ne dépend pas de la consommation d'énergie à long terme, fournissant ainsi une crypto-monnaie pair-à-pair économe en énergie et à des coûts plus compétitifs. La preuve-d'intérêt est basée sur l'âge de pièce de monnaie et produite par chaque nœud via un plan de hachage similaire au Bitcoin, mais sur un espace de recherche plus limité. L'histoire de la blockchain et le règlement de transactions sont plus longtemps protégés, par un mécanisme de point de contrôle central.

Introduction

Depuis la création de Bitcoin (Nakamoto, 2008), la preuve de travail a été la conception prédominante de la crypto-monnaie pair-à-pair. Le concept de preuve de travail a été la base de monnayage et le modèle de sécurité du concept de Nakamoto.

En octobre 2011, nous avons réalisé que le concept de l'âge de la pièce (*coin age*) peut faciliter une alternative, connue sous le nom de "preuve d'enjeu" (*proof-of-stake*), à la preuve de travail (*proof-of-work*) du système Bitcoin.

Depuis, nous avons formalisé une conception où la preuve d'enjeu est utilisée pour construire le modèle de sécurité d'une crypto-monnaie pair-à-pair et une partie de son processus de monnayage, alors que la preuve de travail consiste essentiellement à faciliter la première partie du processus de monnayage et réduit progressivement son importance. Cette conception tente de démontrer la viabilité des futures crypto-monnaies pair-à-pair, **sans dépendance à l'égard de la consommation d'énergie**. Nous avons nommé le projet "**ppcoin"**.

Âge de pièce

Le concept d'âge de pièce était connu de Nakamoto au moins dès 2010 et utilisé dans le Bitcoin pour aider à prioriser les transactions par exemple, bien qu'il n'ait pas joué un rôle crucial dans le modèle de sécurité du Bitcoin. L'âge de pièce est simplement défini comme des temps de montant de la monnaie durant une période tenue. Voici un exemple simple à comprendre : si Bob a reçu 10 pièces d'Alice et les a tenues pendant 90 jours, nous disons que Bob a accumulé 900 "jours de pièce" d'âge de pièce.

De plus, quand Bob a dépensé les 10 pièces de monnaie reçues d'Alice, nous disons que l'âge de pièce que Bob a accumulé avec ces 10 pièces, avait été consommé (ou détruit).

Afin de faciliter le calcul de l'âge de la pièce, **nous avons introduit un champ d'horodatage dans chaque transaction.** Horodatage des blocs et horodatage des protocoles de transaction relatifs y sont renforcées pour assurer le calcul de l'âge de la pièce.

Preuve d'enjeu

La preuve de travail a contribué à donner naissance à la grande percée de Nakamoto, mais la nature de la preuve de travail signifie que la crypto-monnaie dépend de la consommation d'énergie, introduisant ainsi une surcharge significative des coûts dans l'exploitation de ces réseaux, qui supporte la charge par les utilisateurs via une combinaison de frais d'inflation et de transaction.
Comme le taux de minage ralentit dans le réseau Bitcoin, il pourrait éventuellement faire pression sur l'augmentation des frais de transaction pour maintenir un niveau préféré de la sécurité. On se demande naturellement si nous devons maintenir la consommation d'énergie afin d'avoir une crypto-monnaie décentralisée ? C'est donc une étape importante à la fois théorique et technologique, pour démontrer que la sécurité des crypto-devises pair-to-pair ne doit pas dépendre de la consommation d'énergie.

Un concept appelé "preuve d'enjeu" a été discuté dans les milieux Bitcoin dès 2011. En gros, preuve d'enjeu signifie une forme de preuve de propriété de la monnaie. L'âge de pièce consommé par une transaction peut être considéré comme une forme de preuve d'enjeu. Nous avons découvert de façon indépendante le concept de preuve d'enjeu et le concept de l'âge de la pièce en octobre 2011, à partir duquel nous avons réalisé que la preuve d'enjeu peut en effet remplacer la plupart des fonctions de la preuve de travail avec la refonte minutieuse de monnayage de Bitcoin et le modèle de sécurité. Ceci principalement parce que, tout comme la preuve de travail, la preuve d'enjeu ne peut pas être facilement falsifiée. Bien sûr, c'est l'une des exigences essentielles des systèmes monétaires que la difficulté à contrefaire. Philosophiquement parlant, l'argent est finalement déjà une forme de « preuve de travail » dans le passé, et devrait donc être en mesure de remplacer la preuve de travail.

NB : cible = 1 opération de hachage par pièce-seconde. [ndt]

La génération bloc dans la preuve d'enjeu

Dans notre conception hybride, les blocs sont séparés en deux types différents : preuve de travail et preuve d'enjeu.

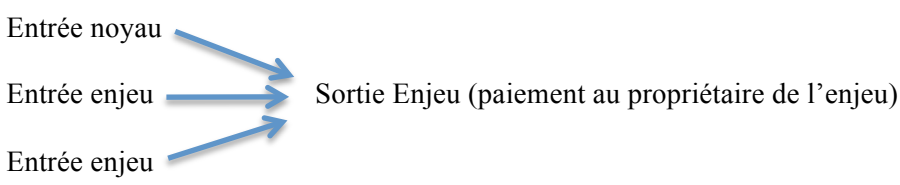

schéma : structure d'une transaction preuve d'enjeu (coinstake)

La preuve d'enjeu dans le nouveau type de blocs est une opération spéciale appelée "coinstake" (enjeu de pièce), nommé ainsi après la transaction de base spéciale Bitcoin). Dans la transaction coinstake, le propriétaire de block paie lui-même ce que consomme son âge de pièce, tout en obtenant le privilège de

générer un bloc pour le réseau et pour preuve d'enjeu de monnayage. La première entrée de *coinstake* est appelé "noyau" (*kernel* en anglais) et est nécessaire pour atteindre certains protocoles-cibles de hachage, la génération de blocs de preuves d'enjeu jalonnant ainsi un processus stochastique semblable à des blocs de preuves de travail. Néanmoins, une différence importante réside dans l'opération de hachage qui est effectuée sur un espace de recherche limité (plus précisément un hachage par seconde, par portefeuille-sortie non dépensé) au lieu d'un espace de recherche illimité comme preuve de travail, donc il n'y a pas de consommation importante d'énergie impliquée.

La cible de hachage que le noyau d'enjeu doit rencontrer est une cible par âge de pièce d'unité (pièce-jour) consommée dans le noyau (contrairement à la cible de preuve de travail du Bitcoin qui est une valeur cible fixe appliquée à chaque nœud). Ainsi, plus l'âge de la pièce est consommé dans le noyau, plus il est facile de rencontrer le protocole-cible de hachage. Par exemple, si Bob a une sortie de portefeuille qui a accumulé 100 âges de pièces (ou pièces-ans) et qu'il attend qu'il en soit généré un noyau en 2 jours, alors Alice peut attendre que ses 200 âges de pièces de sa sortie de portefeuille génèrent un noyau en 1 jour.

Dans notre conception à la fois la cible de hachage preuve de travail et la cible de hachage preuve d'enjeu sont réglées de façon continue plutôt que comme l'intervalle d'ajustement de 2 semaines du Bitcoin, et ce pour éviter un saut brusque du taux de génération de réseau.

Protocole de la chaîne principale

Le protocole, pour déterminer quelle chaîne de blocs en compétition gagne en tant que chaîne principale, a été commuté **pour utiliser l'âge de la pièce consommé. Ici, chaque transaction dans un bloc apporte son âge de pièce consommé au score du bloc. La chaîne de bloc avec le total le plus élevé d'âge de pièce consommé est choisie comme chaîne principale.**

Ceci contraste avec l'utilisation de la fonction preuve de travail dans le protocole de la chaîne principale du Bitcoin, alors que le travail total de la chaîne de bloc (on utilise aussi le terme "blockchain" en français) est utilisé pour déterminer la chaîne principale.

Cette conception atténue certaines des préoccupations des 51 % de la prise en charge du Bitcoin, où le système est uniquement considéré comme sûr quand les bons noeuds contrôlent au moins 51 % de la puissance minière du réseau... D'abord, le coût de la participation majoritaire importante pourrait être plus élevé que le coût d'acquisition de la puissance sur l'exploitation minière, augmentant ainsi le coût d'attaque pour de telles entités puissantes. Aussi, l'âge de pièce de l'attaquant est consommé lors de l'attaque, ce qui peut rendre plus difficile pour l'attaquant de continuer d'empêcher les transactions d'entrer dans la chaîne principale.

Point de Contrôle : Protection et Histoire

L'un des inconvénients d'utiliser la total d'âge de pièce consommé pour déterminer la chaîne principale est qu'il réduit le coût d'une attaque sur la chaîne de bloc entier de l'histoire. Même si le Bitcoin a une protection relativement forte sur l'histoire, Nakamoto a encore mis en place des points de contrôle en 2010 comme mécanisme permettant de consolider l'histoire de la chaîne de bloc (blockchain), ce qui empêche toute modification éventuelle dans la partie de la blockchain antérieure au point de contrôle.

Une autre préoccupation est que le coût d'une double attaque dépensée peut aussi avoir été réduit, comme l'attaquant peut simplement avoir besoin d'accumuler un certain montant d'âge de pièce, et forcer la réorganisation de la chaîne de bloc. Pour rendre le commerce pratique dans un tel système, nous avons décidé d'introduire une forme supplémentaire de points de contrôle qui sont diffusés de manière centrale, à des intervalles beaucoup plus courts – quelques fois par jour – pour servir à "geler" la chaîne de bloc (blockchain) et finaliser les transactions. Ce nouveau type de point de contrôle est diffusé similairement au système d'alerte du Bitcoin.

Ben Laurie (2011) a argumenté que le Bitcoin n'a pas complètement résolu le problème de consensus distribué, comme le mécanisme pour un point de contrôle n'est pas distribué. Nous avons essayé de concevoir un protocole pratique de point de contrôle distribué, mais avons trouvé difficile de le sécuriser contre les attaques de partage de réseau. Bien que le mécanisme de point de contrôle diffusé soit une forme de centralisation, nous le considérons comme acceptable avant qu'une solution distribuée soit disponible.

Une autre raison technique implique l'utilisation de point de contrôle centralisé. Afin de se défendre contre un type d'attaque par déni de service, le noyau de coinstake (enjeu de pièce) doit être vérifié avant qu'un bloc de preuve d'enjeu puisse être accepté dans la base de données locale (arbre de bloc) de chaque noeud. En raison du modèle de données de noeud du Bitcoin (indice de transaction spécifique), un délai de points de contrôle est nécessaire pour assurer la capacité de tous les noeuds à vérifier la connexion de chaque noyau coinstake avant d'accepter un bloc dans l'arbre de bloc.

Compte tenu des considérations pratiques détaillées ci-dessus, nous avons décidé de ne pas modifier le modèle de données de noeud, mais d'utiliser un point de contrôle central à la place. **Notre solution consiste à modifier le calcul de l'âge de la pièce pour exiger un âge minimum, tel que 1 mois, en dessous duquel l'âge de la pièce est calculé comme zéro.** Ensuite, le point de contrôle central est utilisé pour faire en sorte que tous les nœuds puissent convenir des transactions passées datant de plus d'un mois, permettant ainsi la vérification de la connexion du noyau *coinstake*, comme un noyau exige un âge de pièce non-nul, celui-ci devant donc utiliser une sortie de plus d'un mois.

Signatures de bloc et protocole de double-enjeu

Chaque bloc doit être signé par son propriétaire pour empêcher la même preuve d'enjeu d'être copiée et utilisée par des attaquants.

Un protocole de double-enjeu est conçu pour se défendre contre un attaquant à l'aide d'une seule preuve de participation pour générer une multitude de blocs comme une attaque par déni de service. Chaque nœud recueille la paire de toutes les transactions *coinstake* (noyau, horodatage) qu'il a vue. Si un bloc reçu contient une paire en double par rapport à un autre bloc déjà reçu, nous ignorons alors ce bloc en double-jeu jusqu'à ce qu'un bloc successeur soit reçu comme un bloc orphelin.

Énergie Efficiente

Lorsque le taux de minage de la preuve de travail se rapproche de zéro, il y a de moins en moins d'inclinations à miner des blocs par la preuve de travail. En vertu du scénario d'une consommation d'énergie à long terme dans le réseau, celle-ci peut tomber à des niveaux très bas de sort que les mineurs désintéressés arrêtent l'exploitation minière de blocs par la technique "preuve de travail".

Le réseau Bitcoin fait face à ce risque à moins que le volume de transactions/frais augmente à des niveaux suffisamment élevés pour soutenir la consommation d'énergie. **Dans le cadre de notre conception, même si la consommation d'énergie est proche de zéro, le réseau est toujours protégé par la preuve d'enjeu. Nous appelons une crypto-monnaie à efficacité énergétique long terme si la consommation d'énergie sur la preuve de travail a la permission d'approcher zéro.**

Autres considérations

Nous avons modifié le taux de minage de la preuve de travail pour qu'il ne soit pas déterminé par la hauteur du bloc (temps) mais plutôt déterminé par la difficulté. Lorsque les difficultés d'extraction augmentent, le taux de minage sur l'épreuve du travail diminue. Une courbe relativement lisse est choisie par opposition aux fonctions d'étape du Bitcoin, afin d'éviter de choquer artificiellement le marché. Plus précisément, une courbe continue est choisie de telle sorte que chaque augmentation 16 fois supérieure à la difficulté de l'extraction coupe de moitié le montant du minage du bloc.

À plus long terme, la courbe de minage de la preuve du travail ne serait pas trop différente de celle du Bitcoin en termes de comportement inflationniste, compte tenu de la poursuite de la Loi de Moore. Nous considérons donc comme judicieux de suivre l'observation traditionnelle selon laquelle le marché favorise une monnaie à faible inflation par rapport à une inflation élevée, malgré des critiques importantes envers le Bitcoin de la part de certains économistes traditionnels, mais pour des raisons idéologiques à notre avis. Babaioff et al. (2011) a étudié l'effet des frais de transaction et a soutenu que ces derniers incitent à ne pas coopérer entre les mineurs. Dans notre système, cette attaque est exacerbée, de sorte que nous ne donnons plus de frais de transaction au propriétaire du bloc. Nous avons décidé de supprimer les frais de transaction à la place. Cela supprime du coup l'incitation à ne pas reconnaître d'autres blocs de mineurs. Il sert également de levier déflationniste pour contrer l'inflation du minage par preuve de travail.

Nous choisissons également d'imposer des frais de transaction au niveau du protocole pour se défendre contre l'attaque de blocage de bloc.

Au cours de notre recherche, nous avons également découvert une **troisième possibilité** en plus de la preuve de travail et de la preuve d'enjeu, que nous avons qualifiée de **preuve d'excellence**. Dans le cadre de ce système, un tournoi se déroule périodiquement pour miner des pièces et basé sur la performance des participants au tournoi, en imitant les prix des tournois de la vie réelle. Bien que ce système ait tendance à consommer de l'énergie à l'image d'une intelligence artificielle qui excelle à ce jeu, nous avons néanmoins trouvé le concept intéressant, même dans une telle situation car il fournit une forme assez intelligence de la consommation d'énergie.

Conclusion

Lors de la validation de notre conception sur le marché, nous nous attendons à ce que les conceptions de la preuve d'enjeu deviennent une forme potentiellement plus compétitive de crypto-monnaie pair-à-pair, que les conceptions de preuve de travail, en raison de l'élimination de la dépendance à la consommation d'énergie, atteignant du coup une baisse d'inflation/baisse des frais de transaction à des niveaux de sécurité de réseau comparables.

Reconnaissance

Chaleureux remerciements à Richard Smith pour son aide durant les tests et pour son travail sur les diverses branches de réseaux.

Nous souhaitons remercier Satoshi Nakamoto et les développeurs du Bitcoin dont le brillant travail de pionniers a ouvert nos esprits et a rendu un tel projet possible.

Références

Babaioff M. et al. (2011) : *On Bitcoin and red balloons*.

Laurie B. (2011) : *Decentralised currencies are probably impossible (but let's at least make them efficient*). http://www.links.org/files/decentralised-currencies.pdf

Nakamoto S. (2008) : *Bitcoin : A peer-to-peer electronic cash system*. http://www.bitcoin.org/bitcoin.pdf

Traduction française : BioCoin.