PPCoin : Monnaie cryptographique pair-à-pair avec preuve-de-part

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

19 Août 2012

(Traduit de l'anglais par Guillaume LE VAILLANT le 28 Décembre 2013)

Résumé

Conception d'une monnaie cryptographique dérivée de Bitcoin de Satoshi Nakamoto. Une preuve-de-part remplace la preuve-de-travail pour garantir la plupart de la sécurité du réseau. Dans cette conception hybride la preuve-de-travail fournit principalement la création initiale de monnaie et n'est pas vraiment essentielle à long terme. Le niveau de sécurité du réseau ne dépend pas à long terme de la consommation énergétique fournissant ainsi une monnaie cryptographique pair-à-pair économe en énergie et plus compétitive au niveau coût. La preuve-de-part est basée sur l'âge-pièce et est générée par chaque nœud du réseau via un schéma de hachage semblable à celui de Bitcoin mais sur un espace de recherche limité. La chaîne de blocs et le règlement des transactions sont de plus protégés par un mécanisme centralisé de diffusion de points de contrôle.

Introduction

Depuis la création de Bitcoin (Nakamoto 2008), la preuve-de-travail a été le concept prédominant dans les monnaies cryptographiques pair-à-pair. Elle a été à la base de la création de monnaie et de la sécurisation du réseau dans la conception de Nakamoto.

En Octobre 2011, nous avons réalisé que le concept d'âge-pièce pouvait permettre l'émergence d'un modèle alternatif, nommé preuve-de-part, au système de preuve-de-travail de Bitcoin. Nous avons depuis formalisé un design où la preuve-de-part est utilisée pour construire le modèle de sécurité d'une monnaie cryptographique pair-à-pair et une partie de son processus de création de monnaie, tandis que la preuve-de-travail sert principalement à faciliter la création initiale de monnaie et voit son importance diminuer graduellement. Ce design tente de démontrer la viabilité de futures monnaies cryptographiques pair-à-pair ne dépendant pas de la consommation d'énergie. Nous avons nommé le projet *ppcoin***.**

Âge-pièce

Le concept d'âge-pièce était connu de Nakamoto au moins depuis 2010 et a été utilisé dans Bitcoin pour aider à définir l'ordre de priorité des transactions par exemple, cependant il n'a pas joué un rôle prépondérant dans le modèle de sécurité. L'âge-pièce est simplement définit comme la multiplication d'une quantité de monnaie par le temps de possession de celle-ci. Prenons un exemple simple à comprendre : si Bob reçoit 10 pièces d'Alice et les garde pendant 90 jours, on dit que Bob a accumulé 900 jours-pièces d'âge-pièce.

De plus, lorsque Bob dépense les 10 pièces qu'il a reçues d'Alice, on dit que l'âge-pièce que Bob a accumulé avec ces 10 pièces a été *consommé* (ou *détruit*).

Afin de faciliter le calcul de l'âge-pièce, nous avons introduit un champ d'horodatage (*timestamp*) dans chaque transaction. Les protocoles relatifs à l'horodatage des blocs et des transactions ont été renforcés afin de sécuriser le calcul de l'âge-pièce.

Preuve-de-part

Le concept de preuve-de-travail a permis de faire naître la découverte majeure de Nakamoto, cependant la nature de la preuve-de-travail implique que la monnaie cryptographique soit dépendante de la consommation d'énergie, introduisant ainsi un surcoût significatif dans le fonctionnement d'un tel réseau, ce que les utilisateurs supportent grâce à une combinaison d'inflation et de frais de transaction. Puisque la vitesse de création de monnaie du réseau Bitcoin diminue, on pourrait être forcé d'augmenter les frais de transaction afin de garantir un certain niveau de sécurité. On se demande naturellement s'il est indispensable de maintenir un haut niveau de consommation d'énergie afin d'avoir une monnaie cryptographique décentralisée.
C'est pourquoi il est important, à la fois théoriquement et techniquement, de démontrer que la sécurité des monnaies cryptographique pair-à-pair n'a pas besoin de dépendre de la consommation d'énergie.

Un concept nommé preuve-de-part a été source de discussions parmi les adeptes de Bitcoin depuis au moins 2011. En gros, une preuve-de-part est une forme de preuve de possession de monnaie. L'âge-pièce consommé par une transaction peut être considéré comme une preuve-de-part. Nous avons découvert indépendamment le concept de preuve-de-part et le concept d'âge-pièce en Octobre 2011, et nous avons ainsi réalisé que la preuve-de-part pouvait en effet remplacer la plupart des fonctions de la preuve-de-travail en repensant prudemment les modèles de création de monnaie et de sécurité de Bitcoin. Ceci est dû principalement au fait que, comme la preuve-de-travail, la preuve-de-part n'est pas facile à contrefaire. La difficulté de contrefaçon étant bien entendu une exigence critique des systèmes monétaires. D'un point de vue philosophique, l'argent est une forme de preuve-de-travail dans le passé, donc il devrait être capable de remplacer la preuve-de-travail à lui tout seul.

Génération de bloc avec preuve-de-part

Dans notre design hybride, les blocs sont séparés en deux types différents, les blocs preuve-de-travail et les blocs preuve-de-part.

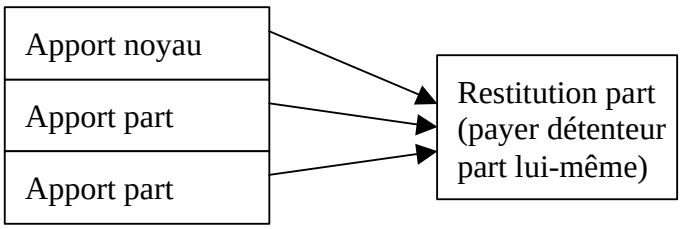

Figure : Structure de transaction preuve-de-part (coinstake)

La preuve-de-part dans le nouveau type de bloc est une transaction spéciale appelée *coinstake* (nommée d'après la transaction spéciale de Bitcoin *coinbase*). Dans la transaction coinstake le propriétaire du bloc se paye lui-même en consommant son âge-pièce, tout en gagnant le privilège de générer un bloc pour le réseau et de créer de la monnaie. Le premier apport de la transaction coinstake se nomme *noyau* et est nécessaire afin d'atteindre une certaine cible de hachage du protocole, faisant ainsi de la génération de blocs preuve-de-part un processus stochastique similaire à la génération de blocs preuve-de-travail. Cependant une différence importante est que l'opération de hachage est effectuée dans un espace de recherche limité (plus spécifiquement un hachage par contenu de portefeuille non dépensé par seconde) au lieu d'un espace de recherche non limité comme dans la preuve-de-travail, ce qui n'implique aucune consommation d'énergie significative.

La cible de hachage que le noyau doit atteindre est définie par unité d'âge-pièce (jours-pièces) consommée par le noyau (contrairement à la cible de la preuve-de-travail de Bitcoin qui est une valeur fixée appliquée à tous les nœuds). Ainsi, plus il y a d'âge-pièce consommé par le noyau, plus il sera facile d'atteindre la cible du protocole de hachage. Par exemple, si Bob a un portefeuille ayant accumulé 100 années-pièces et s'attend à générer un noyau en 2 jours, alors Alice peut s'attendre à voir son portefeuille de 200 années-pièces à générer un noyau en environ 1 jour.

Dans notre design, les cibles de hachage de la preuve-de-travail et de la preuve-de-part sont toutes les deux ajustées continuellement plutôt que par intervalle de 2 semaines comme dans Bitcoin, afin d'éviter les brusques sauts de la vitesse de génération du réseau.

Création de monnaie basée sur la preuve-de-part

Un nouveau processus de création de monnaie est introduit pour les blocs preuve-de-part en plus de la création de monnaie par preuve-de-travail de Bitcoin. Un bloc preuve-de-part crée des pièces en fonction de de l'âge-pièce consommé par la transaction coinstake. Un taux de génération d'un centime par année-pièces consommée est choisi pour donner un futur taux d'inflation faible.

Même si nous gardons la preuve-de-travail comme partie du processus de création de monnaie pour faciliter la création initiale, il est concevable que dans un système purement preuve-de-part la création de monnaie initiale puisse être effectuée complètement dans le bloc de genèse via un processus similaire à une introduction en bourse.

Protocole de chaîne principale

Le protocole permettant de déterminer quelle chaîne de bloc en compétition gagne et devient la chaîne principale a été modifié pour utiliser l'âge-pièce consommé. L'âge-pièce consommé par chaque transaction d'un bloc contribue au score du bloc. La chaîne de blocs ayant le total d'âge-pièce consommé le plus élevé est choisie comme chaîne principale.

Ceci diffère de l'utilisation de la preuve-de-travail du protocole de chaîne principale de Bitcoin où le travail total de la chaîne de blocs est utilisé pour déterminer la chaîne principale.

Cette conception soulage certaines préoccupations concernant l'hypothèse des 51 % de Bitcoin, où le système n'est considéré comme sûr que si au moins 51 % de la puissance d'extraction du réseau est contrôlée par de bons nœuds. Tout d'abord, le coût nécessaire pour contrôler une part significative pourrait être supérieur au coût d'acquisition d'une puissance d'extraction significative, augmentant ainsi le coût d'une attaque pour une entité puissante. De plus, l'âge-pièce de l'attaquant est consommé pendant l'attaque, ce qui pourrait rendre plus difficile pour l'attaquant de continuer à empêcher des transactions d'entrer dans la chaîne de blocs principale.

Point de contrôle : protection de l'historique

Un des désavantages de l'utilisation de l'âge-pièce total consommé pour déterminer la chaîne principale est que cela diminue le coût d'une attaque sur l'intégralité de l'historique de la chaîne de blocs. Bien que Bitcoin possède une protection de l'historique relativement forte, Nakamoto a quand même introduit des points de contrôle en 2010 afin de solidifier l'historique de la chaîne de blocs, empêchant tout changement de la partie de la chaîne de blocs précédant le point de contrôle.

Une autre préoccupation est que le coût d'une attaque par double-dépense a peut-être été réduit aussi, puisque l'attaquant a juste besoin d'accumuler une certaine quantité d'âge-pièce pour forcer la réorganisation de la chaîne de blocs. Pour rendre le commerce pratique avec un tel système, nous

avons décidé d'introduire une forme additionnelle de points de contrôle qui est diffusée de manière centralisée, à intervalles plus courts (quelques fois par jour) afin de geler la chaîne de blocs et finaliser les transactions. Ce nouveau type de points de contrôle est diffusé d'une manière similaire au système d'alerte de Bitcoin.

Laurie (2011) a argumenté que Bitcoin n'avait pas complètement résolu le problème du consensus distribué puisque le mécanisme des points de contrôle n'est pas distribué. Nous avons tenté de concevoir un protocole pratique de points de contrôle distribué mais avons trouvé difficile de le sécuriser face à l'attaque par scission du réseau. Bien que le mécanisme de diffusion des points de contrôle soit une forme de centralisation, nous considérons qu'il est acceptable jusqu'à ce qu'une solution distribuée soit disponible.

Une autre raison technique entraîne l'utilisation de points de contrôle diffusés de manière centralisée. Afin de se défendre contre un type d'attaque par déni de service le noyau coinstake doit être vérifié avant qu'un bloc preuve-de-part soit accepté dans la base de données locale (arbre des blocs) de chaque nœud. À cause du modèle de données de Bitcoin (spécifiquement l'index de transaction) une date limite de création de point de contrôle est requise pour s'assurer que chaque nœud soit capable de vérifier la connexion de chaque noyau coinstake avant d'accepter un bloc dans l'arbre des blocs. À cause des considérations pratiques précédentes nous avons décidé de ne pas modifier le modèle de données des nœuds mais d'utiliser les points de contrôle centralisés à la place. Notre solution est de modifier le calcul de l'âge-pièce pour nécessiter un âge minimum, comme un mois, en dessous duquel l'âge-pièce est égal à zéro. Ensuite, le point de contrôle centralisé est utilisé pour s'assurer que tous les nœuds sont d'accord sur les transactions passées vieilles de plus d'un mois permettant ainsi la vérification de la connexion du noyau coinstake, puisqu'un noyau nécessite un âge-pièce supérieur à zéro et donc doit utiliser une sortie de transaction ayant au moins un mois.

Signatures de blocs et protocole de part dupliquée

Chaque bloc doit être signé par son propriétaire pour empêcher que la même preuve-de-part ne soit copiée et utilisée par des attaquants.

Un protocole de part dupliquée a été conçu pour se défendre contre un attaquant qui utiliserait une preuve-de-part pour générer une multitude de blocs pour perpétrer une attaque par déni de service. Chaque nœud collecte la paire (noyau, horodatage) de toutes les transactions coinstake qu'il a vues. Si un bloc reçu contient une paire identique à celle d'un bloc reçu précédemment, il est ignoré jusqu'à ce que l'on ait reçu un bloc successeur qui soit un bloc orphelin.

Efficacité énergétique

Quand la création de monnaie par preuve-de-travail approchera zéro, il y aura de moins en moins de motivation à créer des blocs preuve-de-travail. Dans ce scénario à long terme la consommation d'énergie dans le réseau pourrait tomber très bas puisque les mineurs ne trouveront plus intéressant d'extraire des blocs preuve-de-travail. Le réseau Bitcoin fait face à un tel risque à moins que le volume ou les frais des transactions augmentent à des niveaux suffisamment hauts pour maintenir la consommation d'énergie. Avec notre design, même si la consommation d'énergie approche zéro, le réseau est toujours protégé par la preuve-de-part. On parle de monnaie cryptographique *économe en énergie à long terme* si la consommation énergétique de la preuve-de-travail est autorisée à se rapprocher de zéro.

Autres considérations

Nous avons modifié la création de monnaie par preuve-de-travail pour qu'elle ne soit pas

déterminée par la hauteur de bloc (temps) mais par la difficulté. Quand la difficulté d'extraction augmente, la création de monnaie par preuve-de-travail diminue. Une courbe relativement douce a été choisie contrairement aux fonctions escalier de Bitcoin, afin d'éviter de choquer le marché artificiellement. Plus spécifiquement, une courbe continue a été choisie telle que si la difficulté d'extraction est multipliée par 16, la quantité de monnaie crée par le bloc est divisée par 2.

Sur le long terme la courbe de production de monnaie par preuve-de-travail ne devrait pas être très différente de celle de Bitcoin en terme d'inflation, si tant est que la loi de Moore continue à se vérifier. Nous considérons qu'il est sage de suivre l'observation traditionnelle selon laquelle le marché préfère une monnaie à faible inflation plutôt qu'une monnaie à forte inflation, en dépit de critiques significatives de Bitcoin par certains économistes qui selon nous sont dues à des raison idéologiques.

Babaioff et al. (2011) a étudié l'effet des frais de transaction et a argumenté qu'ils sont une incitation à la non coopération entre les mineurs. Avec notre système cette attaque est exacerbée donc nous ne donnons plus les frais de transaction au propriétaire de bloc. À la place nous avons décidé de détruire les frais de transaction. Ceci supprime l'incitation à ne pas reconnaître les blocs des autres mineurs. Cela sert aussi de force déflationniste contrant la force inflationniste provenant de la création de monnaie de la preuve-de-part.

Nous avons aussi choisi de forcer les frais de transaction au niveau du protocole comme défense contre l'attaque par congestion de bloc.

Pendant nos recherches, nous avons aussi découvert une troisième possibilité en plus de la preuve-de-travail et de la preuve-de-part, que nous avons nommée preuve-d-excellence. Typiquement avec ce système un tournoi est organisé régulièrement pour créer des pièces en fonction des performances des participants au tournoi, imitant les prix de tournois de la vie réelle. Cependant bien que ce système ait tendance à consommer de l'énergie quand l'intelligence artificielle excelle au jeu utilisé, nous avons quand même trouvé le concept intéressant puisque d'une certaine façon il utilise une forme intelligente de consommation d'énergie.

Conclusion

Après validation de notre design par le marché, nous nous attendons à ce que la preuve-de-part devienne potentiellement plus compétitive que la preuve-de-travail dans les monnaies cryptographiques pair-à-pair à cause de l'élimination de la dépendance à la consommation d'énergie, permettant ainsi d'obtenir une inflation et des frais de transaction inférieurs à niveau de sécurité égal.

Remerciements

Merci beaucoup à Richard Smith pour l'aide avec les tests et divers travaux liés au réseau/fork. Nous voudrions remercier Satoshi Nakamoto et les développeurs de Bitcoin dont le brillant travail de pionnier a ouvert nos esprits et rendu un projet comme celui-ci possible.

Réferences

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)