Dash: Une Monnaie Centrée sur la Confidentialité

Evan Duffield - evan@dash.org
Daniel Diaz - daniel@dash.org

Résumé *- Une crypto-monnaie basée sur le Bitcoin (l'oeuvre de Satoshi Nakamoto) comprenant différentes améliorations, comme par exemple un réseau incitatif à deux niveaux dénominé le réseau des Masternodes (noeud-maîtres). Autre amélioration présente, PrivateSend, qui confère une fongibilité croissante et InstantSend, qui permet la confirmation instantanée des transactions sans autorité centrale.*

1 Introduction

Le Bitcoin [1] est une crypto-monnaie qui est devenue un moyen d'échange populaire ainsi que la première monnaie numérique ayant attiré un nombre considérable d'utilisateurs [2]. Depuis ses débuts en 2009, le Bitcoin a connu une adoption rapide et grandissante de par les utilisateurs ainsi que de par les commerces [3]. Un problème majeur dans l'adoption du Bitcoin dans les points de ventes est dû au temps nécessaire pour que le réseau confirme la validité de la transaction. Des entreprises tierces ont créé des méthodes alternatives permettant aux vendeurs d'accepter des transactions avec zéro confirmation, mais ces solutions passent par des intermédiaires de confiance qui agissent en tant que médiateur de la transaction en dehors du protocole.

Le Bitcoin permet l'inscription de transactions confidentielles dans un registre comptable publique, avec une relation directe entre l'émetteur et le récepteur. Ainsi existe un registre permanent de toutes les transactions qui ont eu lieu sur le réseau depuis le début. Il est largement accepté dans les cercles académiques que le Bitcoin a un niveau de confidentialité faible. Pourtant, et malgré cette limitation, de nombreuses personnes continuent de confier leur historique financier à cette blockchain.

Dash constitue la première crypto-monnaie centrée sur la confidentialité et basée sur l'oeuvre de Satoshi Nakamoto. Dans ce livre blanc, nous proposerons une série d'améliorations au Bitcoin dans le but d'obtenir une crypto-monnnaie décentralisée et confidentielle, avec des transactions instantanées et sécurisées et un réseau de second niveau de pair à pair (P2P) incitatif qui pourra fournir différents services au réseau Dash.

2 Le réseau des Masternodes

Les noeuds entiers (full nodes) sont des serveurs fonctionnant sur un réseau P2P, permettant aux pairs de recevoir des mises à jour des événements de ce réseau. Ces nœuds requièrent un volume de trafic significatif ainsi que d'autres ressources, le tout conduisant à un coût non négligeable. Par conséquent, sur le réseau Bitcoin, on a pu observer une diminution constante du nombre de ces nœuds au fur et à mesure [7] ainsi que l'augmentation conséquente du temps de propagation des blocs jusqu'à atteindre les 40 secondes [14]. De nombreuses solutions ont été proposées comme par exemple un nouveau système de rémunération de Microsoft Research [4] ou le programme incitatif de Bitnodes [6].

Figure 1: Nombre de nœuds entiers du réseau Bitcoin durant le printemps 2014

Ces nœuds sont très importants pour la santé du réseau. Ils fournissent aux clients la capacité à synchroniser et à propager rapidement les messages à travers le réseau. Nous proposons d'ajouter un réseau de second niveau, connu sous le nom de réseau des Masternodes Dash. Ces nœuds auront une disponibilité élevée et devront fournir un certain niveau de service au réseau afin de pouvoir

faire partie du Système de Récompense des Masternodes.

2.1 Système de Récompense des Masternodes - Coûts et Paiements

La raison principale expliquant la diminution des nœuds entiers du réseau Bitcoin est l'absence d'intérêt à en faire fonctionner un. Au fur et à mesure du temps, le coût de maintenance du nœud entier augmente puisque le réseau devient de plus en plus fréquenté, générant plus de bande passante et coûtant plus d'argent à celui qui l'héberge. Avec les coûts augmentant, les opérateurs regroupent leurs services afin de faire des économies ou choisissent un client léger, ce qui n'aide pas du tout le réseau.

Les Masternodes sont des nœuds entiers, tout comme ceux du réseaux Bitcoin, à part qu'ils doivent fournir un certain niveau de service au réseau et sont liés par une caution pour pouvoir le faire. La caution n'est jamais perdue et est sécurisée lorsque le Masternode est en fonctionnement. Cela permet aux investisseurs de fournir un service au réseau, de gagner des intérêts sur leur investissement et de réduire la volatilité de la monnaie.

Pour héberger un Masternode, le nœud doit contenir 1000 dashs. Lorsqu'ils sont actifs, les nœuds fournissent des services aux clients du réseau et sont payés en échange sous la forme de dividende. Cela permet aux utilisateurs de payer pour les services et obtenir un retour sur investissement. Les Masternodes sont tous payés depuis la même réserve d'argent : environ 45% de la récompense totale du bloc est attribuée à ce système.

Etant donné que le système de récompense des Masternodes est basé sur un pourcentage fixe et que le nombre de nœuds Masternodes dans le réseau varie, la valeur de la récompense des Masternodes variera en fonction du nombre total de Mastrnodes actifs à un moment donné. Les paiements pour une journée typique pour héberger un Masternode peuvent être calculés avec la formule suivante :

Avec:
n le nombre de Masternodes contrôlés par un hébergeur
t le nombre total de Masternodes
r la récompense actuelle du bloc (aujourd'hui environ 5 dashs)
b la moyenne du nombre de blocs dans une journée. Pour le réseau Dash cela représente en général 576.
a le paiement moyen du Masternode (45% de la récompense moyenne du bloc)

Le retour sur investissement pour héberger un Masternode peut être calculé comme suit :

Avec les mêmes variables que ci-dessus.

Le coût associé pour héberger un Masternode implique une limite rigide et une limite flexible. Avec aujourd'hui 5,3 millions de dashs en circulation, un maximum de 5300 nœuds pourraient fonctionner sur le réseau. La limite flexible dépend du prix que coûte l'acquisition d'un nœud et la liquidité limitée sur les plateformes d'échanges étant donné que Dash est aussi utilisé comme une monnaie et non pas un simple investissement.

2.2 Classement déterministe

Un algorithme déterministe spécial est utilisé pour créer un classement pseudo-aléatoire des Masternodes. En utilisant l'empreinte (hash) de la preuve de travail de chaque bloc, la sécurité de cette fonctionnalité sera assurée par le réseau de minage.

Pseudo-code permettant de sélectionner un Masternode:

```
For(mastenode in masternodes){
    current_score = masternode.CalculateScore();

    if(current_score > best_score){
         best_score = current_score;
         winning_node = masternode;
    }
}

CMasterNode::CalculateScore(){
   pow_hash = GetProofOfWorkHash(nBlockHeight); // get the hash of this block
   pow_hash_hash = Hash(pow_hash); //hash the POW hash to increase the entropy
   difference = abs(pow_hash_hash - masternode_vin);
   return difference;
}
```

Ce code d'exemple peut se développer pour fournir un classement des Masternodes sélectionnant également un “deuxième”, “troisième”, “quatrième” Masternode de la liste.

2.3 Quorums Incorruptibles

Actuellement, le réseau Dash contient environ 2400 Masternodes actifs [8]. En demandant une garantie de 1000 dashs pour héberger un Masternode actif, nous créons un système dans lequel personne ne peut contrôler le réseau entier de Masternodes. Par exemple, si quelqu'un souhaitait prendre le contrôle de 50% du réseau Masternode, il devrait acheter 2,3 millions dashs sur le marché des changes. Cela provoquerait une hausse substantielle du prix, rendant impossible l'acquisition du nombre de dashs nécessaires.

Par l'ajout de ce réseau Masternode et de ses garanties, nous pouvons utiliser ce réseau de second niveau pour réaliser des tâches ultra-sensibles de manière incorruptible, où aucune entité ne peut intervenir dans le résultat. En sélectionnant N Masternodes parmi tous les Masternodes et de manière pseudo-aléatoire pour exécuter une même tâche, ces nœuds fonctionnent alors comme preuve incorruptible sans avoir besoin que le réseau tout entier fasse cette tâche.

Par exemple, par l’implémentation d'un quorum incorruptible (voir InstantSend [9]) utilisant des quorums pour approuver des transactions et verrouiller les inputs ou pour l'implémentation de la preuve de service[10].

Autre exemple possible d'utilisation des quorums incorruptibles serait d'utiliser le réseau Masternode comme une preuve décentralisée infaillible pour les marchés financiers, rendant possibles les contrats sécurisés et décentralisés. Comme exemple de contrat : si l'action d'Apple (AAPL) est au-dessus de 300 $ le 16 décembre 2016, distribuez les fonds à la clé publique A, sinon à la clé publique B.

2.4 Rôles et Preuve de Service

Les Masternodes peuvent fournir n'importe quel type de service supplémentaire au réseau. Afin de le démontrer, notre première implémentation comprend PrivateSend et InstantSend. En utilisant ce que l'on appelle la preuve de service, nous pouvons exiger de ces nœuds qu'ils soient connectés, qu'ils répondent, et cela même à la bonne hauteur de bloc.

Des acteurs néfastes pourraient opérer des Masternodes sans pour autant proposer aucune qualité de service au reste du réseau. Pour réduire la possibilité que des personnes se servent du système pour leur bénéfice unique, les nœuds doivent faire un "ping" au reste du réseau afin de prouver qu'ils sont actifs. Ce travail est réalisé par le réseau Masternode en sélectionnant 2 quorums par bloc. Le Quorum A vérifie l'état du service du Quorum B à chaque bloc. Le Quorum A comprend les nœuds

les plus proches de l'empreinte (hash) du bloc en cours, tandis que le Quorum B comprend les nœuds les plus loin de cette empreinte en question.

Le Masternode A (1) vérifie le Masternode B (position 2300)
Le Masternode A (2) vérifie le Masternode B (position 2299)
Le Masternode A (3) vérifie le Masternode B (position 2298)

Tout le travail réalisé pour prouver que les nœuds sont actifs est réalisé par le réseau Masternode lui-même. Environ 1% du réseau sera vérifié à chaque bloc. Cela signifie que le réseau en entier est vérifié environ six fois par jour. Dans le but de garder ce système incorruptible, nous sélectionnons les nœuds de manière aléatoire à travers le système de Quorum et nous exigeons un minimum de 6 "manquements" avant de désactiver un nœud.

Afin de tromper ce système, l'attaquant devra être sélectionné six fois de suite. Dans le cas contraire, les manquements seront neutralisés par le système puisque d'autres nœuds seront sélectionné par le système de Quorum.

Masternodes de l'attaquant / Total des Masternodes	Nombre de fois choisi à la suite	Probabilité de succès	Dashs nécessaires
1/2300	6	6.75e-21	1000 Dashs
10/2300	6	6.75e-15	10 000 Dashs
100/2300	6	6.75e-09	100 000 Dashs
500/2300	6	0.01055%	500 000 Dashs
1000/2300	6	0.6755%	1 000 000 Dashs

Tableau 1. Probabilité de tromper le système pour un Masternode individuel manquant à la preuve de service.

Avec:
n le nombre total de nœuds contrôlés par l'attaquant
t le nombre total de Masternodes dans le réseau
r la profondeur de la chaîne

La sélection des Masternodes est pseudo-aléatoire basée sur le système de Quorum.

2.5 Le Protocole des Masternodes

Les Masternodes se propagent au travers du réseau à travers une série d'extensions de protocole qui comprend un message d'annonce ainsi qu'un message ping du Masternode. Ces deux messages sont tout ce qu'il faut pour rendre le nœud actif sur le réseau. En plus de ces deux messages, d'autres messages sont aussi contenus pour exécuter des requêtes de preuve de service, PrivateSend et InstantSend.

Les Masternodes sont formés à l'origine par l'envoi de 1000 dashs à une adresse en particulier dans un portefeuille qui "activera" le nœud, le rendant ainsi capable de se propager à travers le réseau. Une deuxième clé privée est créée et est utilisée pour signer tous les futurs messages. La dernière clé permet au portefeuille d'être complètement verrouillé lorsqu'il fonctionne en mode autonome.

Une fonction Cold est possible en utilisant la deuxième clé privée sur deux machines différentes. Le client primaire "hot" signe la transaction de 1000 dashs en incluant la deuxième clé privée dans le message. Quelque temps après le client "cold" voit le message incluant sa deuxième clé privée et il active le Masternode. Cela permet au client "hot" d'être désactivé (client éteint) et empêche complètement qu'un attaquant ait accès aux 1000 dashs en entrant dans le Masternode après que ce dernier ait été activé.

Lorsqu'il démarre, un Masternode envoie un message "Annonce Masternode" au réseau et dont le contenu est le suivant :

Message: (1K DASH Input, Reachable IP Address, Signature, Signature Time, 1K Dash Public Key, Secondary Public Key, Donation Public Key, Donation Percentage)

Par la suite, toutes les 15 minutes, un ping est envoyé pour démontrer que le nœud est toujours actif.

Message: (1K DASH Input, Signature (using secondary key), Signature Time, Stop)

Après un certain temps, le réseau éliminera un nœud inactif du réseau, empêchant le nœud d'être utilisé par les clients ou de recevoir des paiements. Les nœuds peuvent aussi faire constamment un "ping" au réseau, cependant s'ils n'ont pas leurs ports d'ouverts ils seront considérés au bout d'un moment comme étant inactifs et ne seront pas payés.

2.6 Propagation de la liste des Masternodes

Les nouveaux clients rejoignant le réseau doivent connaître les Masternodes actuellement actifs afin de pouvoir utiliser leurs services. Dès qu'ils rejoignent le réseau maillé, une commande est envoyée aux pairs demandant la liste des Masternodes existants. Les clients utilisent un objet en cache pour enregistrer les Masternodes et leur statut actuel. Ainsi, lorsque les clients redémarrent, ils n'auront qu'à charger le fichier au lieu de redemander la liste complète aux Masternodes.

2.7 Paiement via le minage et l'obligation

Afin de garantir que chaque Masternode est payé son juste dû pour chaque bloc de récompense, le réseau doit s'assurer que les blocs paient le bon Masternode. Si un mineur ne respecte pas les règles, ses blocs doivent être rejetés, autrement cela revient à favoriser la tricherie.

Nous proposons une stratégie où les Masternodes forment des quorums, choisissant un Masternode gagnant et diffusant son message. Après que N messages aient été diffusés pour sélectionner le même bénéficiaire, un consensus sera formé et ce bloc en question sera sommé de payer ce Masternode.

Lorsque le minage a lieu dans le réseau, les pools (sites internet qui rassemblent les forces de mineurs individuels) utilisent l'interface API RPC pour obtenir l'information sur comment créer un bloc. Afin de payer les Masternodes, cette interface doit être étendue en ajoutant un deuxième bénéficiaire au GetBlockTemplate. Les pools propagent ensuite leurs blocs minés avec succès, comprenant un paiement qui se répartit entre eux et le Masternode.

3 PrivateSend

Afin de renforcer la protection de la vie privée des utilisateurs dans le client de référence, nous pensons qu'il est important d'avoir une implantation standard incorruptible qui fournisse un niveau important de confidentialité. D'autres clients comme Ethereum, Android et iPhone disposeront eux aussi de la même couche de confidentialité et utiliseront les extensions du protocole. Cela fournit aux utilisateurs une même expérience au moment de rendre leurs fonds confidentiels tout en utilisant un système très facile à comprendre.

PrivateSend est une version améliorée et enrichie de CoinJoin. En plus du concept central de CoinJoin, nous utilisons tout une série d'améliorations comme la décentralisation et un fort degré de confidentialité par la technique d’enchaînement et de mélange passif et anticipé des coupures.

Le défi le plus important lorsqu'on cherche à améliorer la confidentialité et la fongibilité d'une crypto-monnaie est de le faire d'une manière qui ne rende pas opaque la blockchain dans son ensemble. Pour les crypto-monnaies basées sur Bitcoin, il est possible de savoir quels outputs sont dépensés et ceux qui ne le sont pas (appelés communément UTXO pour Unspent Transaction

Output). C'est ainsi que naît le registre comptable public dans lequel n'importe quel utilisateur peut se porter garant de l'intégrité des transactions. Le protocole Bitcoin est conçu pour fonctionner sans l'intervention d'intermédiaires de confiance. En leur absence, il est indispensable que la possibilité d'effectuer des vérifications à travers la blockchain reste facilement possible pour les utilisateurs. Notre but est d'améliorer la protection de la vie privée et la fongibilité sans pour autant perdre ces fonctionnalités primordiales qui sont nécessaires, nous en sommes convaincus, au succès d'une monnaie.

Par la présence d'un service décentralisé de mélange à l'intérieur même de la monnaie, nous pouvons alors conserver la monnaie complètement fongible. La fongibilité est une propriété de l'argent qui implique que chaque unité d'une monnaie doit être équivalente à une autre. Lorsque vous recevez de l'argent dans une devise, aucun historique de ses anciens utilisateurs ne doit être présent ou alors les utilisateurs doivent pouvoir facilement se dissocier de cet historique, ce qui permet de conserver chaque unité équivalente à une autre. Par ailleurs, il doit être possible pour tout utilisateur de se porter garant de l'intégrité financière du registre comptable public sans compromettre l'identité des autres.

Pour améliorer la fongibilité et conserver l'intégrité de la blockchain publique, nous proposons d'utiliser une stratégie incorruptible de mélange décentralisé et anticipé. Afin de permettre la conservation de la fongibilité de la monnaie, ce service est directement construit dans la monnaie, facile à utiliser et sûr pour l'utilisateur moyen.

3.1 Suivre CoinJoin à travers les Montants

Une stratégie habituelle dans les implantations existantes de CoinJoin dans Bitcoin est de tout simplement regrouper les transactions ensemble. Cela expose l'utilisateur à diverses techniques permettant de suivre l'argent de l'utilisateur à travers ces transactions groupées. 

Figure 2: Un exemple de transaction CoinJoin avec 2 utilisateurs [11][12]

Dans cette transaction, 0,05BTC ont été envoyés à travers le mixeur. Pour identifier la source de l'argent, il suffit de faire la somme des montants de droite jusqu'à ce qu'elle corresponde à un des montants de gauche.

Si on décompose la transaction :

- 0,05 + 0,0499 + 0,0001(commission) = 0,10BTC.
- 0,0499 + 0,05940182 + 0,0001(commission) = 0,10940182BTC.

La difficulté de ce procédé augmente exponentiellement au fur à mesure que d'autres utilisateurs sont ajoutés. Cependant, cet historique peut à n'importe quel moment être désanonymisé rétroactivement au bout d'un moment.

3.2 A travers le Linking et le Forward Linking

Dans d'autres implémentations de CoinJoin, un utilisateur rend confidentiel une transaction mais envoie ensuite le change de cette transaction à une plateforme d'échange ou à tout autre entité qui connait son identité. Cela interrompt la confidentialité et permet à l'entité en question de remonter les transactions de l'utilisateur. Ce type d'attaque s'appelle "Forward Linking".

Figure 3: Forward Change Linking

Dans cette exemple, Alice rend confidentiel 1,2BTC, qui vont vers 2 destinations (outputs), 1BTC et 0,2BTC. Elle dépense ensuite 0,7BTC de l'output 1BTC et reçoit le change de 0,3BTC. Ces

0,3BTC sont déplacés vers une source identifiable, prouvant qu'Alice a également dépensé 0,7 BTC dans la transaction précédente.

Pour identifier l'émetteur de la transaction confidentielle, il suffit de partir de la transaction de la plateforme d'échange et de remonter en arrière dans la blockchain jusqu'à obtenir la transaction "Alice a envoyé 0,7BTC de manière confidentielle". La plateforme d'échange sait qu'il s'agit de l'utilisateur qui a récemment acheté quelque chose de manière confidentielle, détruisant ainsi complètement la confidentialité. Ce type d'attaque s'appelle "Through Change Linking".

Figure 4: Through Change Linking

Dans le second exemple, Alice achète 1,2 BTC sur coinbase, puis déplace cette somme de manière confidentielle dans un output de 1BTC. Elle dépense ensuite 0,7BTC et reçoit le change de 0,3BTC et le rassemble avec son change antérieur de 0,2BTC.

En regroupant le change de la transaction confidentielle (0,3BTC) et le change reçu de la transaction de CoinJoin, il est possible de faire un lien complet dans l'historique, avant et après, violant ainsi complètement la confidentialité.

3.3 Confidentialité Améliorée et Résistance au Déni de Service (DOS)

Afin de fusionner les transactions ensemble de manière à ce qu'elles ne puissent pas être démêlées par la suite, PrivateSend se sert du fait qu'une transaction peut être formée par de multiples parties et envoyée à de multiples parties. Etant donné que toutes les transactions PrivateSend sont conçues pour que les utilisateurs se paient eux-mêmes, le système est hautement protégé du vol et les transactions restent constamment sécurisées. Actuellement, pour mixer avec PrivateSend, 3 participants sont requis.

Figure 5: Trois utilisateurs envoie des fonds à travers une transaction commune. Les utilisateurs se remboursent eux-même sous la forme de nouveaux outputs qui sont rangés au hasard.

Afin d'améliorer la confidentialité du système dans son ensemble, nous proposons d’utiliser des coupures communes de 0,1 dash, 1 dash, 10 dashs et 100 dashs. A chaque mélange, tous les utilisateurs devraient envoyer les mêmes coupures en inputs et outputs. En plus des coupures, les frais de transactions devraient être retirés des transactions et prélevés ensemble dans des transactions intraçables, séparées et sporadiques.

Pour contrer les possibles attaques de déni de service, nous proposons que tous les utilisateurs qui rejoignent le pool, lui envoient une caution. Cette caution leur sera destinée et permettra de payer des frais de transaction élevés aux mineurs. Dans le cas où un utilisateur soumet une requête au pool de mélange, il doit apporter une caution au début de la transaction. Si un utilisateur refuse de coopérer, en refusant de signer par exemple, la caution sera automatiquement diffusée. Cela rendra coûteux d'exécuter une attaque en continue sur le réseau de confidentialité.

3.4 Anonymat passif des fonds et enchaînement

PrivateSend est limité à 1000 dashs par session et nécessite de multiples sessions pour rendre complètement confidentielles de grandes quantité d'argent. Pour faciliter l'expérience utilisateur et pour rendre difficile les attaques temporelles (timing attacks), PrivateSend fonctionne en mode passif. Après un intervalle déterminé, le client d'un utilisateur demandera l'autorisation de rejoindre les autres clients à travers un Masternode. Lorsqu'il rejoint le Masternode, un queue object se propage à travers le réseau détaillant les coupures que l’utilisateur cherche à rendre confidentielles,

mais aucune information ne peut être utilisée pour identifier l'utilisateur.

Chaque session PrivateSend peut être pensée comme étant un événement indépendant qui augmente la confidentialité des transactions d'un utilisateur. Cependant, comme chaque session est limitée à trois clients, un observateur a une chance sur trois de pouvoir suivre la transaction. Afin d'augmenter la qualité de la confidentialité, une technique d'enchaînement est utilisée, envoyant l'argent à travers de multiples Masternodes, les uns après le autres.

Profondeur de la Chaîne	Utilisateurs Possibles
2	9
4	81
8	6561

Tableau 2. Nombre d'utilisateurs pouvant être impliqués dans N sessions de mélange.

3.5 Considérations Liées à la Sécurité

Au fur et à mesure que les transactions sont regroupées, les Masternodes pourraient "espionner" l'argent des utilisateurs qui passent par eux. Cela n'est pas considéré comme un problème important étant donné qu'un Masternode possède une caution de 1000 dashs et le fait que les utilisateurs sélectionnent des Masternodes au hasard pour héberger leur mélange. La probabilité de suivre une transaction à travers un enchaînement peut être calculée comme suit :

Masternodes de l'attaquant / Total des Masternodes	Profondeur de la Chaîne	Probabilité de Succès	Dashs Nécessaires
10/1010	2	9.80e-05	10 000 dashs
10/1010	4	9.60e-09	10 000 dashs
10/1010	8	9.51e-11	10 000 dashs
100/1100	2	8.26e-03	100 000 dashs
100/1100	4	6.83e-05	100 000 dashs
100/1100	8	4.66e-09	100 000 dashs
1000/2000	2	25%	1 000 000 dashs
1000/2000	4	6.25%	1 000 000 dashs
1000/2000	8	0.39%	1 000 000 dashs
2000/3000	2	44.4%	2 000 000 dashs
2000/3000	4	19.75%	2 000 000 dashs
2000/3000	8	3.90%	2 000 000 dashs

Tableau 3. Probabilité de suivre une transaction PrivateSend dans le réseau quand un attaquant contrôle N noeuds.

Avec:
n le nombre total de nœuds contrôlés par l'attaquant
t le nombre total de Masternodes dans le réseau
r la profondeur de la chaîne

La sélection des Masternodes est aléatoire.

Etant donné l'existence limitée de dashs (5,3 millions au moment de la rédaction, Avril 2015) et la faible liquidité disponible sur le marché, il devient impossible d'obtenir un assez grand nombre de Masternodes pour réussir une telle attaque.

Développer le système en occultant aux Masternodes les transactions qui ont lieu en leur sein

augmenterait énormément la sécurité du système.

3.6 Aveuglement des Masternodes dans un Système de Relai

Dans la section 3.4 nous avons établi les probabilités de suivre une transaction unique à travers de multiples sessions de mélange PrivateSend. Ces probabilités peuvent être diminuées en "aveuglant" les Masternodes afin qu'ils ne puissent pas voir quels inpouts/outputs appartiennent à quels utilisateurs. A cette fin nous proposons un système simple de relai que les utilisateurs peuvent utiliser pour protéger leur identité.

Au lieu que l'utilisateur envoie ses inputs et outputs directement dans le pool, ils choisiront un Masternode au hasard dans le réseau et lui demanderont de relayer les inputs/outputs/signatures au Masternode cible. Cela veut dire que le Masternode recevra un lot de inputs/outputs et un lot de signatures. Chaque lot correspond à un des utilisateurs, mais le Masternode ne peut pas savoir lequel.

4 Transactions Instantanées avec InstantSend

En utilisant des quorums de Masternodes, les utilisateurs peuvent envoyer et recevoir des transactions instantanées irréversibles. Une fois qu'un quorum a été formé, l'input de la transaction est verrouillé afin de ne pouvoir être dépensé que dans un type spécifique de transaction. Il faut environ 4 secondes actuellement pour qu'une transaction soit verrouillée sur le réseau. Si le réseau Masternode s'est mis d'accord sur le verrouillage d'une transaction, toute transaction et ou tout bloc conflictuel ultérieur sera rejeté à moins qu'il ne corresponde exactement au numéro de la transaction verrouillée.

Cela permettra aux commerçants d'utiliser leurs téléphones au lieu des systèmes de paiement traditionnels présents dans les commerces physiques et aux utilisateurs d'effectuer physiquement et rapidement des transactions non commerciales comme ils le feraient avec des espèces. Cela est réalisé sans autorité centrale. Une explication exhaustive de cette fonction peut être lue dans le livre blanc InstantSend[9].

5 Améliorations Additionnelles

5.1 Algorithme de hachage x11

x11 est un algorithme de hachage largement utilisé, qui adopte une approche différente, connue sous le nom d’enchaînement d'algorithmes. x11 comprend les 11 participants de SHA3 [13], chaque empreinte étant calculée puis soumis à l’algorithme suivant dans la chaîne. En utilisant de multiples algorithmes, la probabilité qu'un ASIC soit conçu pour cette monnaie est minimum jusqu'à un moment avancé de son cycle de vie.

Dans le cycle de vie de Bitcoin, le minage a débuté avec des passionnés qui utilisaient des processeurs (CPU) pour miner la monnaie. Puis, rapidement, des processeurs graphiques (GPU) ont été créés et ont rapidement remplacé les CPUs. Plusieurs années après, les circuits intégrés spécialisés ASICs furent créés et ont rapidement remplacé les GPUs.

Etant donné la complexité et la taille du circuit intégré pour créer un ASIC pour miner x11, nous pensons qu'il faudra beaucoup plus de temps pour en créer un que pour Bitcoin, permettant ainsi aux amateurs de participer au minage pendant plus longtemps. Nous pensons que cela est très important pour la bonne répartition et pour la bonne croissance d'une crypto-monnaie.

Un autre avantage de l'approche de hachage par enchaînement est que les CPUs haut de gamme donnent des retours moyens similaires à ceux des GPUs. Aussi, il a été rapporté que les GPUs chauffaient 30 à 50% moins (avec une consommation électrique moindre) que l'algorithme script

utilisé par la plupart des crypto-monnaies.

5.2 Réserves à Miner

Une approche différente dans la restriction de l'inflation du minage est choisie avec Dash, avec environ 7% de réduction par an. Cela s'oppose à la réduction par deux des autres crypto-monnaies. Par ailleurs, chaque bloc est directement lié au nombre de mineurs dans le réseau: plus de mineurs signifie de plus petites récompenses.

Il est prévu que la production de Dash s'étende au long de ce siècle et du prochain, diminuant progressivement jusqu'en 2150 lorsque la production cessera.

Figure 6: Système de Récompense pour le Minage

6 Conclusion

Ce livre blanc présente des concepts divers afin d'améliorer le modèle de Bitcoin, à travers une plus grande confidentialité et fongibilité pour l'utilisateur moyen, un prix moins volatile et une propagation des messages plus rapides à travers le réseau. Tout cela est réalisé à travers un système incitatif à deux niveaux au lieu d'un système à niveau unique comme dans les autres monnaies numériques comme Bitcoin. Avec la présence d'un réseau alternatif, il devient possible d'ajouter de nombreux types de services comme le mélange décentralisé de la monnaie, des transactions instantanées et des systèmes décentralisés à preuves infaillibles à travers les quorums de Masternodes.

Références

1. A peer-to-peer electronic cash system (2008)
2. http://eprints.qut.edu.au/69169/1/Boyen_accepted_draft.pdf
3. https://www.cryptocoinsnews.com/3-solutions-instant-bitcoin-confirmations/
4. http://research.microsoft.com/pubs/156072/bitcoin.pdf
5. http://www0.cs.ucl.ac.uk/staff/s.meiklejohn/files/imc13.pdf
6. https://getaddr.bitnodes.io/nodes/incentive/
7. https://medium.com/zapchain-magazine/why-don-t-people-run-bitcoin-nodes-anymore-d4da0b45aae5
8. https://dashninja.pl/
9. https://www.dash.org/wp-content/uploads/2014/09/InstantTX.pdf
10. https://github.com/dashpay/dash/blob/master/src/Masternode-pos.cpp
11. https://blockchain.info/tx/4eb3b2f9fe597d0aef6e43b58bbaa7b8fb727e645fa89f922952f3e57ee6d603
12. https://blockchain.info/tx/1694122b34c8543d01ad422ce600d59f8d8fde495ac9ddd894edc7139aed7617
13. http://en.wikipedia.org/wiki/NIST_hash_function_competition#Finalists
14. http://www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf