Blockstack

# Proof of Transfer Whitepaper v1.0

Livre blanc sur la preuve de transfert v1.0

May 2020

By Blockstack PBC

# PoX : Preuve de transfert de minage avec Bitcoin

Muneeb Ali Aaron Blankstein Michael J. Freedman
Ludovic Galabru Diwaker Gupta Jude Nelson Patrick
Jesse Soslow Stanley

PBC de pile de blocs
https://blockstack.org

11 mai 2020

Abstrait

Les algorithmes de consensus pour les blockchains publiques nécessitent des ressources informatiques ou financières pour sécuriser l'état de la blockchain. Les mécanismes de minage utilisés par ces algorithmes sont largement divisés en preuve de travail, dans laquelle les nœuds consacrent des ressources informatiques, et en preuve de participation, dans laquelle les nœuds consacrent des ressources financières pour participer à l'algorithme de consensus. L'idée générale derrière la preuve de travail et la preuve de participation est de rendre pratiquement impossible à tout acteur malveillant de disposer de suffisamment de puissance de calcul ou de participation pour attaquer le réseau. Une variante de preuve de travail est la preuve de gravure dans laquelle les mineurs rivalisent en « brûlant » (en détruisant) une cryptomonnaie de preuve de travail en tant que proxy pour les ressources informatiques.

Dans cet article, nous introduisons un nouveau mécanisme de minage, appelé preuve de transfert (PoX) qui généralise le concept de preuve de brûlage. PoX utilise la crypto-monnaie de preuve de travail d'une blockchain établie pour sécuriser une nouvelle blockchain. Cependant, contrairement à la preuve de gravure plutôt que de graver la cryptomonnaie, les mineurs transfèrent la cryptomonnaie engagée à un ou plusieurs autres participants du réseau. Cela permet aux participants au réseau qui ajoutent de la valeur au nouveau réseau de crypto-monnaie de gagner une récompense dans une crypto-monnaie de base en participant activement à l'algorithme de consensus.

PoX encourage un modèle dans lequel il existe une blockchain de preuve de travail extrêmement sécurisée, par exemple Bitcoin. D'autres nouvelles blockchains peuvent être ancrées sur la blockchain sécurisée de preuve de travail au lieu d'introduire de nouvelles chaînes de preuve de travail. PoX a la propriété intéressante selon laquelle les participants peuvent gagner des paiements dans une crypto-monnaie de base distincte, potentiellement plus stable, tout en participant au nouveau réseau blockchain. Cela peut aider à résoudre un problème d'amorçage pour les nouvelles blockchains en offrant des incitations aux premiers participants. De plus, PoX présente un cas d'utilisation potentiel pour financer des fonds de développement d'écosystèmes. Nous présentons une proposition d'utilisation de PoX dans la blockchain Stacks 2.0.

Professeur d'informatique à l'Université de Princeton et conseiller technique de Blockstack PBC.

# 1 Introduction

Blockstack est un effort open source visant à développer des logiciels offrant une alternative aux applications Web traditionnelles (centralisées). Nous pensons que le prochain chapitre du Web est l'émergence d'un Internet appartenant aux utilisateurs, construit sur des blockchains publiques.

Les algorithmes de consensus pour les blockchains publiques nécessitent des ressources informatiques ou financières pour sécuriser l'état de la blockchain. Les mécanismes de minage utilisés par ces algorithmes sont largement divisés en preuve de travail (PoW), dans laquelle les nœuds consacrent des ressources de calcul, et en preuve de participation (PoS), dans laquelle les nœuds consacrent des ressources financières. L'intention derrière la preuve de travail et la preuve de participation est de rendre pratiquement impossible à un seul acteur malveillant de disposer d'une puissance de calcul ou d'une propriété suffisante.
enjeu pour attaquer le réseau.

Avec une preuve de travail, un mineur effectue un « travail » qui consomme de l'électricité et est récompensé par de la monnaie numérique. En théorie, le mineur convertit l'électricité et la puissance de calcul en monnaie numérique nouvellement créée. Bitcoin en est un exemple et est de loin la blockchain PoW la plus grande et la plus sécurisée.

Avec la preuve de participation, les mineurs mettent en jeu leurs avoirs dans une nouvelle monnaie numérique pour participer à l'algorithme de consensus et un mauvais comportement peut être pénalisé en « réduisant » les fonds du mineur. Le PoS nécessite moins d'énergie/électricité à consommer et peut offrir aux détenteurs de crypto-monnaie qui participent au jalonnement une récompense sur leurs avoirs dans la crypto-monnaie de base. Le PoS peut être moins sécurisé que le PoW étant donné (a) le problème du canal de confiance pour les nouveaux nœuds [1], et (b) la capacité d'un attaquant à créer de nombreux « faux » historiques de la blockchain avec un coût minime [2].

La blockchain la plus sécurisée aujourd'hui est de loin le Bitcoin. Blockstack s'appuie depuis ses débuts sur Bitcoin comme mécanisme pour établir la confiance dans un réseau ouvert et sans autorisation : la blockchain Stacks 1.0, lancée en 2018, fonctionne comme une « blockchain virtuelle » au-dessus de Bitcoin [3]. Nous continuons de croire que Bitcoin peut devenir le « drapeau de la technologie » [4] et que la plupart des gens seront initiés aux crypto-monnaies via Bitcoin. L'écosystème de développeurs autour de Bitcoin continue de croître.

Cependant, l'ajout de nouvelles fonctionnalités à la blockchain Bitcoin pose un défi : le Bitcoin est sécurisé car il est stable et ne change pas. Bien qu'il possède un langage de script, ce langage est extrêmement limité. C'est intentionnel : l'ajout de complexité augmente la surface d'attaque, ce qui réduit la valeur du Bitcoin en tant que couche fondamentale.

Malgré cela, un Internet appartenant à un utilisateur nécessite un ensemble de fonctionnalités plus complexes. La chaîne de blocs qui alimente ce prochain chapitre du Web doit être conçue pour cette tâche : elle doit prendre en charge la création de nouveaux types de biens numériques, la gestion de nouveaux types d'applications décentralisées et être suffisamment flexible pour permettre aux développeurs de créer des applications. -cations que nous ne pouvons pas encore imaginer. La blockchain Stacks est une tentative de créer cette blockchain, et au cours de sa durée de vie, nous avons exploré l'espace de conception pour établir de nouvelles blockchains riches en fonctionnalités au-dessus de Bitcoin, en l'utilisant comme base de confiance.

La blockchain Stacks 1.0 fonctionne comme une « blockchain virtuelle » au-dessus de Bitcoin. Chaque transaction de la chaîne Stacks 1.0 est également une transaction Bitcoin. Toutes les données d'un

La transaction Stacks est codée dans les métadonnées d'une transaction Bitcoin. Cette conception est limité ; Les transactions Stacks doivent partager la bande passante avec les transactions Bitcoin. Piles les transactions doivent être validées séparément par des nœuds blockchain non miniers, qui le font ne pas recevoir de récompenses minières pour validation.

Dans SIP-001, nous avons proposé un mécanisme de preuve de brûlage (PoB) pour la conception du Chaîne Stacks 2.0 [5]. Avec une preuve de brûlure, les mineurs de Stacks rivalisent en détruisant une crypto-monnaie plutôt qu'en consommant de l'électricité. La preuve de gravure permet aux mineurs de participer sans matériel spécial et offre plus de transparence au réseau.
participants qu'une blockchain de preuve de travail normale. Cependant, comme une preuve de travail blockchain, la preuve de gravure est destructrice, obligeant les mineurs à détruire la valeur afin de sécuriser la blockchain.

Cependant, PoB souffre d'un problème potentiel d'amorçage. Les mineurs et les participants au réseau de la chaîne PoB sont récompensés par une nouvelle crypto-monnaie. Cependant,
dans les premiers jours de la chaîne PoB, cette crypto-monnaie n'a peut-être pas autant de valeur ou sécurité comme crypto-monnaie de base, Bitcoin. Avant que la chaîne PoB ne mûrisse et que le nouveau la crypto-monnaie gagne en valeur et en stabilité, les mineurs pourraient ne pas vouloir détruire Bitcoin afin de participer.

Preuve de transfert. Dans cet article, nous introduisons un nouveau mécanisme de minage, appelé proof-of-transfer (PoX) qui généralise le concept de proof-of-burn (PoB). PoX utilise le crypto-monnaie de preuve de travail d'une blockchain établie pour sécuriser une nouvelle blockchain. Cependant, contrairement au PoB, plutôt que de brûler la cryptomonnaie, les mineurs transfèrent la cryptomonnaie engagée à un autre participant du réseau. Cela permet au réseau
les participants, qui ajoutent de la valeur au nouveau réseau de crypto-monnaie, pour gagner des récompenses dans une cryptomonnaie de base en participant activement à l'algorithme de consensus.

PoX peut aider à résoudre le problème d'amorçage des nouvelles blockchains : participants recevez des récompenses dans une crypto-monnaie de base distincte, potentiellement plus stable. Ces récompenses peuvent constituer une meilleure incitation à la participation initiale que les récompenses de la nouvelle crypto-monnaie elle-même. L'établissement de cette valeur initiale pour la nouvelle crypto-monnaie peut contribuer à accroître l'intérêt des mineurs, ce qui, à son tour, contribue à développer le nouvel écosystème de crypto-monnaie. Par offrant une incitation à la crypto-monnaie de base pour les participants aux nouvelles crypto-monnaies, PoX échappe à la spirale de la valeur dépendante qui pourrait menacer une nouvelle blockchain.

PoX peut être utilisé non seulement pour encourager la participation des détenteurs d'une nouvelle crypto-monnaie, mais il peut également être utilisé pour établir des fonds de développement. Ces développeurs les fonds peuvent être financés sur la durée de vie d'une nouvelle blockchain. Parce que les fonds seraient être dans une crypto-monnaie distincte, comme Bitcoin, ces fonds pourraient être utilisés sans affecter la valeur de la nouvelle crypto-monnaie.

## 2 Conception de preuve de transfert

Le minage PoX peut être utilisé avec un ensemble de règles consensuelles pour concevoir des blockchains PoX. Le les règles de consensus dictent la manière dont les mineurs interagissent avec une blockchain PoX et le système

| Nom | Acronyme | Mineur action pour créer une nouvelle crypto-monnaie |
|---|---|---|
| Preuve de travail | PoW | Consommer de l'électricité pour les calculs pour frapper des unités d'une nouvelle crypto-monnaie. |
| Preuve de participation | Point de vente | Consacrer une participation économique à une crypto-monnaie de base pour frapper des unités de la même crypto-monnaie. |
| Preuve de brûlure | PoB | Détruire une crypto-monnaie de base pour frapper des unités d'une nouvelle crypto-monnaie. |
| Preuve de transfert | PoX | Transférer une crypto-monnaie de base pour frapper des unités d'une nouvelle crypto-monnaie. |

Tableau 1 : Comparaison de la preuve de travail avec d'autres mécanismes.

fait des progrès, c'est-à-dire que de nouveaux blocs sont écrits dans la blockchain. Aux fins de cet article, le minage PoX utilise la blockchain Bitcoin comme crypto-monnaie de base.
Bien que n'importe quelle crypto-monnaie de preuve de travail puisse être utilisée, nous proposons d'utiliser Bitcoin car il s'agit de loin de la blockchain PoW la plus sécurisée et ses propriétés de sécurité sont actuellement supérieures à celles des autres blockchains PoW.

PoX est un mécanisme de minage qui doit être combiné à un ensemble de règles consensuelles pour un algorithme de consensus entièrement fonctionnel. Le minage PoX est une généralisation de la preuve de brûlure (PoB) proposée pour l'algorithme de consensus pour la blockchain Stacks [6, 5]. UN
Un ensemble de règles de consensus similaire peut également être utilisé avec PoX.

Comme pour PoB, dans PoX, les règles de consensus sélectionnent le mineur gagnant (c'est-à-dire le leader) d'un tour en utilisant une fonction aléatoire vérifiable (VRF). Le leader écrit le bloc suivant de la blockchain Stacks et frappe les récompenses (Stacks nouvellement créés). Cependant, dans PoX, au lieu d'envoyer du Bitcoin pour graver des adresses, les mineurs envoient le Bitcoin à un ensemble de adresses spécifiques correspondant aux autres participants du réseau.

PoX peut être utilisé pour concevoir différents types de blockchains en fonction du consensus règles et comment la crypto-monnaie de base est distribuée. Ci-dessous, nous discutons de deux cas d'utilisation :

Récompenses de participation. PoX peut être utilisé pour récompenser les détenteurs d'une nouvelle crypto-monnaie pour avoir ajouté de la valeur au réseau. Le mécanisme Stacking, proposé dans SIP-007 [7], est un système qui récompense les détenteurs de Stacks (STX) qui participent et ajoutent de la valeur.
au réseau Stacks. Les détenteurs de STX qui contrôlent un certain nombre seuil de STX pouvoir émettre un message signé qui verrouille leurs jetons STX pendant un certain temps, spécifie une adresse Bitcoin pour recevoir des fonds et des signaux (votes) sur une version/fork de la chaîne Stacks comme celle actuelle. Ces informations seraient utiles aux mineurs (honnêtes) sur le réseau. Les mineurs du protocole exploiteraient selon des cycles de récompense et, pour chaque cycle, enverraient leurs engagements Bitcoin aux détenteurs de jetons STX qui ont émis ces messages signés avant le début du cycle de récompense. Les mineurs qui sont également détenteurs de STX peuvent obtenir un avantage sur les autres mineurs, ce qui pourrait potentiellement conduire à une consolidation des mineurs. Dans la section 4.1, nous discutons des solutions possibles à cette consolidation potentielle.

Fonds de développement. PoX peut être utilisé pour financer un fonds de développement dans un écosystème blockchain. Le fonds de développement contrôlerait un portefeuille Bitcoin (vraisemblablement un portefeuille multi-signature) et fournirait l'adresse du portefeuille au protocole PoX en tant que constante du protocole. Les mineurs enverraient du Bitcoin engagé à cette adresse plutôt qu'à l'adresse graver l'adresse. Le protocole pourrait imposer certaines contraintes sur le Bitcoin du fonds de développement en utilisant des scripts Bitcoin pour, par exemple, bloquer les fonds pour un certain nombre de blocs, etc. Quoi qu'il en soit, ce système de récompense nécessite que le réseau accepte que le développeur finance devrait être un participant de confiance dans le système.

# 3 Proposition minière PoX pour Stacks 2.0

Cette section présente une proposition d'utilisation du minage PoX avec des récompenses de participation pour la blockchain Stacks 2.0. Pour plus de détails, nous renvoyons le lecteur à SIP-007 [7].

Bien que l'utilisation de PoX pour récompenser un fonds de développeur soit plus simple, la mise en œuvre de récompenses de participation nécessite des mécanismes de validation et d'exploration de données supplémentaires. En plus des opérations normales d'exploitation minière PoB (voir SIP-001 [5]), l'exigence distribuer des récompenses aux participants signifie que le protocole doit déterminer l'ensemble des adresses auxquelles les mineurs peuvent valablement transférer des fonds. L'exploitation minière PoB n'a pas besoin pour effectuer ces étapes, car l'adresse est toujours la même, c'est-à-dire l'adresse de gravure. Cependant, avec les récompenses de participation, les participants au réseau doivent être en mesure de valider les adresses Bitcoin des destinataires.

Dans SIP-007, la progression dans l'empilement se fait au fil des cycles de récompense. Dans chaque récompense cycle, un ensemble d'adresses Bitcoin est itéré, de telle sorte que chaque adresse Bitcoin dans le un ensemble d'adresses de récompense contient exactement un bloc Bitcoin dans lequel les mineurs transféreront fonds à l'adresse de récompense.

Les mineurs participant à la blockchain Stacks rivalisent pour diriger les blocs en transférant Bitcoin en anneau. Les leaders de blocs Stacks particuliers sont choisis par tri, pondérés par la quantité de Bitcoin envoyée (pour plus de détails, voir SIP-001 [5]). Avant un cycle de récompense commence, le réseau Stacks doit parvenir à un consensus sur les adresses qui sont des destinataires valides. Parvenir à un consensus sur ce point n'est pas trivial : la blockchain Stacks elle-même a de nombreux propriétés indépendantes de la blockchain Bitcoin et peuvent subir des forks, des données de bloc manquantes, etc., ce qui rend difficile l'obtention d'un consensus. Comme un extrême Par exemple, considérons un mineur qui bifurque la chaîne Stacks avec un bloc qui prétend détenir une grande fraction (par exemple, 100 %) de tous les avoirs de Stacks, et procède à l'émission d'engagements en bloc qui se rémunèrent tous les frais. Comment les autres nœuds du réseau peuvent-ils détecter que les transferts d'engagement de ce mineur sont invalides ?

L'algorithme de consensus résout ce problème avec un cycle en deux phases. Avant chaque récompense Dans ce cycle, les nœuds Stacks s'engagent dans une phase de préparation, au cours de laquelle deux éléments sont décidés :

1. Un bloc d'ancrage - le bloc d'ancrage est un bloc de chaîne Stacks. Pour la durée du cycle de récompense, l'extraction de toutes les fourches descendantes du bloc d'ancrage nécessite transférer des fonds miniers aux adresses de récompense appropriées.

2. L' ensemble de récompenses - l'ensemble de récompenses est l'ensemble des adresses Bitcoin qui recevront fonds dans le cycle de récompense. Cet ensemble est déterminé à l'aide de l'état de la chaîne Stacks du bloc d'ancrage.

Pendant le cycle de récompense, les mineurs s'affrontent pour devenir le leader du prochain bloc Stacks en diffusant les engagements de bloc sur la chaîne Bitcoin. Ces engagements de bloc envoient des fonds Bitcoin soit à une adresse de gravure, soit à une annonce de récompense PoX.
robe.

La validité des adresses est déterminée selon deux règles différentes :

1. Si un mineur construit à partir d'une pointe de chaîne qui n'est pas un descendant du bloc d'ancrage, tous les fonds d'engagement du mineur doivent être envoyés à l'adresse de gravure (c'est-à-dire que les fonds sont brûlés).
2. Si un mineur construit à partir d'un descendant du bloc d'ancrage, le mineur doit envoyer des fonds d'engagement à 5 adresses de l'ensemble de récompenses, choisies comme suit :
   - Utilisez la fonction aléatoire vérifiable (également utilisée par tri) pour choisir 5 adresses dans l'ensemble de récompenses. Ces 5 adresses sont les adresses de récompense pour ce bloc.
   - Une fois que les adresses ont été choisies pour un bloc, ces adresses sont supprimées de l'ensemble de récompenses, afin que les futurs blocs du cycle de récompense ne répètent pas les adresses.

Notez que la fonction aléatoire vérifiable (VRF) utilisée pour la sélection des adresses garantit que les mêmes adresses sont choisies par chaque mineur sélectionnant les adresses de récompense. Si un mineur soumet un engagement de gravure qui n'envoie pas de fonds à une adresse valide, ces engagements sont ignorés par le reste du réseau (car n'importe quel nœud Stacks peut en déduire que les adresses de transfert ne sont pas valides).

Pour réduire la complexité de l'algorithme de consensus, les cycles de récompense Stacks sont de longueur fixe : si moins d'adresses participent à l'ensemble de récompenses qu'il n'y a d'emplacements dans le cycle, alors pour les blocs restants, tous les mineurs doivent envoyer des fonds pour graver des adresses.

Pour plus de détails sur la phase de préparation, comment le bloc d'ancrage serait choisi et comment la blockchain Stacks pourrait récupérer des données de bloc d'ancrage manquantes, voir SIP-007 [7].

## 3.1 Ajustements du seuil de récompense basé sur la participation

Chaque cycle de récompense peut transférer les fonds des mineurs vers jusqu'à 5 000 adresses Bitcoin. Pour garantir que ce nombre d'adresses est suffisant pour couvrir le pool de participants (avec une participation de 100 % de STX liquide), le seuil de participation doit être de 0,02 % (1/5000e) de l'offre liquide de STX. Cependant, si la participation est inférieure à 100 %, le pool de récompenses pourrait admettre de plus petits détenteurs de STX. Le protocole précise 2 niveaux de fonctionnement :

- 25% - Si moins de 0,25 · ST X LIQUID SUP P LY STX participe à une récompense cycle, les portefeuilles des participants contrôlant x STX peuvent inclure le plancher (x/(0,00005 · ST X LIQUID SUP P LY ))

adresses dans l'ensemble de récompenses. C'est-à-dire que le seuil minimum de participation est de 1/20 000ème de l'approvisionnement en liquide.

- 25%-100% - Si entre 0,25·ST X LIQUID SUP P_ LY et 1,0·ST_X LIQUID SUP P LY STX participent à un cycle de récompense, le seuil de récompense est réduit afin de maximiser le nombre d'emplacements remplis. Autrement dit, le seuil minimum T de participation sera d'environ 1/5 000ème du STX participant (ajusté par incréments de 10 000 STX). Les portefeuilles des participants contrôlant « x » STX peuvent inclure des adresses d'étage (x/T) dans l'ensemble de récompenses.

Dans le cas où un participant signale et verrouille suffisamment de STX pour soumettre plusieurs adresses de récompense, mais ne soumet qu'une seule adresse de récompense, cette adresse de récompense sera incluse plusieurs fois dans l'ensemble de récompenses.

## 3.2 Soumission des adresses de récompense

Les participants à la récompense doivent diffuser des messages signés à trois fins :

1. Indiquer au réseau combien de STX doivent être verrouillés, et pour combien cycles de récompense.
2. Indiquez la prise en charge d'un bout de chaîne particulier.
3. Spécifier l'adresse Bitcoin pour recevoir les récompenses.

Ces messages peuvent être diffusés soit sur la chaîne Stacks, soit sur la chaîne Bitcoin. S'ils sont diffusés sur la chaîne Stacks, ces messages doivent être confirmés sur la chaîne Stacks avant le bloc d'ancrage pour la période de récompense. S'ils sont diffusés sur la chaîne Bitcoin, ils peuvent être diffusés pendant la phase de préparation, mais doivent être inclus avant la fin de la phase de préparation.

Ces messages signés sont valables pour un maximum de 12 000 blocs Bitcoin (12 cycles de récompense ou 3 mois). Si le message signé spécifie une période de blocage x inférieure à 12 000 blocs, alors le message signé n'est valable que pour la participation cumulée pour les cycles de récompense d'étage (x/1 000) (la longueur minimale de participation est d'un cycle : 1 000 blocs).

## 3.3 Délégation de signalisation des participants

Le processus de délégation permet à une adresse de portefeuille Stacks (l'adresse représentée) de désigner une autre adresse (l'adresse du délégué) pour participer au protocole de récompenses PoX. Cette adresse de délégué, aussi longtemps que la délégation est valide, est capable de signer et de diffuser des messages de participation (c'est-à-dire des messages qui verrouillent Stacks, désignent l'adresse de récompense Bitcoin et signalent la prise en charge des pourboires de chaîne) au nom de l'adresse représentée. Cela permet au propriétaire de l'adresse représentée de contribuer à la sécurité du réseau en faisant en sorte que l'adresse du délégué signale la prise en charge des pointes de chaîne. Cette signalisation, comme la signalisation normale de participation au PoX, combat les attaques potentielles sur la stabilité de la blockchain par les mineurs qui peuvent tenter d'exploiter des forks cachés, de cacher des forks éventuellement invalides et d'autres formes de mauvais comportement des mineurs.

La délégation prise en charge ajoute deux nouveaux types de transactions à la blockchain Stacks :

Déléguer des fonds. Cette transaction initie une relation représenté-délégué. Il transporte les données suivantes :

- Adresse du délégué
- End Block : la hauteur du bloc Bitcoin à laquelle cette relation se termine, à moins qu'une transaction de fonds déléguée ultérieure ne mette à jour la relation. Il n'y a pas de limite supérieure pour ce bloc d'extrémité.
- Montant délégué : le montant total de STX de cette adresse pour lequel l'adresse du délégué pourra émettre des messages de pile au nom de.
- Adresse de récompense (facultatif) : une adresse Bitcoin qui doit être désignée comme destinataire des fonds dans les messages Stacking du délégué. Si elle n'est pas précisée, le délégué peut choisir l'adresse.

Terminer la délégation. Cette transaction met fin à une relation représenté-délégué. Il transporte les données suivantes :

- Adresse du délégué

Notez qu'il n'existe qu'une seule relation active de délégué représenté entre une adresse représentée donnée et une adresse de délégué (c'est-à-dire que la paire (representedAddress, déléguéAddress) identifie de manière unique une relation). Si une relation représenté-délégué est toujours active et que l'adresse représentée signe et diffuse une nouvelle transaction de « fonds délégués », les informations de la nouvelle transaction remplacent la relation précédente.

Les deux types d'opérations de délégation doivent être signés à l'adresse représentée.
Il s'agit de transactions sur la blockchain Stacks, et seront implémentées via un contrat intelligent natif, chargé dans la blockchain lors du bloc de genèse de Stacks 2.0. Ces transactions sont donc des invocations « d'appel de contrat ».

# 4 Recherches en cours et futures

Nous sommes activement engagés dans des recherches plus approfondies sur plusieurs aspects du minage PoX et des récompenses de participation. Cette section aborde deux de ces sujets.

## 4.1 Aborder la consolidation des mineurs

PoX, lorsqu'il est utilisé pour des récompenses de participation, comme décrit, pourrait conduire à une consolidation des mineurs. Étant donné que les mineurs qui participent également en tant que détenteurs pourraient obtenir un avantage sur les mineurs qui ne participent pas en tant que détenteurs, les mineurs seraient fortement incités à acheter la nouvelle crypto-monnaie et à l'utiliser pour évincer les autres mineurs. Dans le cas extrême, cette consolidation pourrait conduire à une centralisation du minage, ce qui nuirait aux objectifs de décentralisation de la blockchain publique. Pendant que nous enquêtons activement

des mécanismes supplémentaires pour faire face à cette consolidation potentielle, nous proposons ici deux mécanismes :

PoX limitée dans le temps. Les récompenses de participation encouragent la consolidation des mineurs si les mineurs obtiennent des avantages permanents pour l'obtention de la nouvelle crypto-monnaie. Cependant, par En limitant la période de PoX, cet avantage diminue avec le temps. Dans ce schéma, un Un « bloc de coucher du soleil » serait défini pour les récompenses de participation x années après le lancement. À le bloc d'extinction, les récompenses de participation cesseraient et tous les mineurs fonctionneraient engagements en brûlant Bitcoin. Autrement dit, après le coucher du soleil, le système PoX transition vers PoB. Cette transition pourrait être linéaire dans le temps, la moitié de l'engagement Bitcoin serait brûlée et l'autre moitié serait transférée aux détenteurs, et ainsi de suite.

Les paramètres exacts d'une telle transition peuvent être ajustés et étudiés dans des simulations.

Ce système résoudrait le problème d'amorçage de la nouvelle blockchain, en offrant aux mineurs et aux détenteurs des incitations à participer dès le début au réseau.

Ensuite, à mesure que les cas d'utilisation naturels de la blockchain se développent et prennent de l'ampleur, le système PoX pourrait progressivement diminuer.

Ensemble de mineurs de confiance. La consolidation des mineurs grâce aux récompenses de participation n'est pas une menace s'il est interdit aux mineurs de participer en tant que détenteurs (c'est-à-dire que les mineurs ne peuvent pas recevoir PoX récompenses). Cependant, dans les systèmes ouverts et décentralisés, il n'est pas facile de déterminer si une adresse de portefeuille donnée appartient à un autre participant. Afin de fournir le garantir que les mineurs et les détenteurs sont séparés, une nouvelle blockchain pourrait limiter l'ensemble de mineurs potentiels vers un ensemble de confiance (qui pourrait être amorcé via un autre entité de confiance). Ces mineurs devraient être contrôlés par l'entité de confiance et nécessitera probablement d'autres systèmes pour garantir la conformité (par exemple, des contrats légaux). Pour nos besoins, un ensemble de mineurs de confiance nuirait à nos objectifs d'une blockchain publique ouverte, et la blockchain résultante commencerait à fonctionner davantage comme un système fédéré que notre système prévu.

## 4.2 Bande passante Bitcoin

Parce que les mineurs PoX doivent envoyer des transactions Bitcoin pour participer au consensus et envoyer des récompenses PoX, le minage PoX occuperait une partie de la bande passante des transactions Bitcoin. Étant donné que la bande passante Bitcoin est limitée par sa conception et compte tenu des exigences de sécurité, les nouvelles blockchains PoX doivent réduire leurs besoins en matière d'utilisation de la bande passante. Pour ce faire, SIP-007 limite le nombre de participants, en utilisant un seuil de détention STX.

D'autres moyens de résoudre les limitations de bande passante sont également possibles, par exemple les canaux d'éclairage. entre Bitcoin et la nouvelle blockchain. Optimisations des transactions Bitcoin

Une couche pourrait également être possible, ce qui réduirait la taille totale nécessaire aux transactions PoX. Nous explorons à la fois la réduction de la taille au niveau de la couche Bitcoin et les modifications potentielles de Lightning pour activer les canaux inter-chaînes.

# Références

[1] J. Nelson, « Les blockchains PoS nécessitent une subjectivité pour atteindre un consensus », 03 2017. https : //forum.blockstack.org/t/pos-blockchains-require-subjectivity-to-reach-consensus/762 .

[2] A. Poelstra, « Enjeu et consensus », 03 2015. https://download.wpsoftware.net/bitcoin/pos.pdf.

[3] Blockstack PBC, « Blockstack-core : v20.0.8.1 », 08 2019. https://github.com/blockstack/blocstack-core/tree/v20.0.8.1.

[4] BS Srinivasan, « Bitcoin devient le drapeau de la technologie », 1 2020. https://nakamoto.com/Bitcoin-devient-le-drapeau-de-la-technologie/.

[5] J. Nelson et A. Blankstein, « SIP 001 : Burn Election », https://github.com/blockstack/Blockstack-core/blob/develop/sip/sip-001-burn-election.md.

[6] M. Ali, J. Nelson, A. Blankstein, R. Shea et MJ Freedman, « Livre blanc technique Blockstack v2.0 », 05 2019. https://blockstack.org/whitepaper.pdf.

[7] M. Ali, A. Blankstein, MJ Freedman, D. Gupta, J. Nelson, J. Soslow et P. Stanley, « SIP 007 : Stack-ing Consensus », https://github.com/blockstack /blockstack-core/blob/develop/sip/ sip-007-stacking-consensus.md.