STAKEPOOL

Proof Of Stake Mining Cryptocurrency
10 octobre 2017

Résumé

StakePool (POOL) est un jeton Ethereum ERC-20 qui représente un droit aux bénéfices tirés de la puissance de minage par preuve d'enjeu (Proof Of Stake, POS) de l'infrastructure de StakePool.co. Le réseau StakePool.co utilise la preuve d'enjeu (POS) sur plusieurs types de masternodes pour maximiser le retour sur investissement. Le jeton sera disponible durant la levée de fond (ICO) qui durera 60 jours. Durant la première vague, 50 millions de jetons au maximum seront vendus. Durant la deuxième vague, 100 millions seront vendus, puisque de plus en plus de crypto-monnaies migreront vers la preuve d'enjeu, dont l'Ethereum. Cette deuxième vague aura lieu entre 60 et 90 jours avant la bascule d'Ethereum vers la preuve d'enjeu (mise à jour Casper). Les jetons restants seront gardés de côté pour d'éventuels d'autres migrations vers la preuve d'enjeu ou masternodes. Une troisième vague n'aura lieu plus tard qu'en cas de besoin d'investissements supplémentaires. Dans le cas contraire, les jetons restants seront brûlés.

1 The StakePool project

Qu'est ce que StakePool : Le projet StakePool, issu d'une société américaine (POS Mining Co.) basée en Ontario (Canada), maintient des portefeuilles POS et des masternodes pour les crypto-monnaies à preuve d'enjeu (POS). 25% de notre approvisionnement en éléctricité est issu de l'énergie solaire. Chaque jeton POOL représente un pourcentage des profits générés par le minage, et est payé mensuellement en ETH, directement dans le portefeuille des détenteurs de jetons. Comme pour la plupart des jetons, les jetons POOL devraient être listés sur plusieurs place d'échange.

La philosophie de la preuve d'enjeu est non pas "la sécurité vient de l'énergie dépensée", mais plutôt "la sécurité vient de l'immobilisation d'un bien économique". [1]

1.1 Notre vision

1.1.1 Histoire du projet

Les fondateurs de StakePool ont maintenu des portefeuilles POS et des masternodes pour plusieurs clients depuis plus de deux ans maintenant. En commençant par DASH, Blackcoin, Diamond, NEM et Reddcoin, puis avec OkCoin, Stratis et Decred, ils ont commencé à regrouper les «coins» de leurs amis, leur famille, et de personnes rencontrés sur le net, afin d'augmenter les chances de récompenses. Comme les fonds continuaient à croître, ils ont commencé à miner de plus en plus de crypto-monnaies. Contrairement à la preuve de travail (Proof of Work, POW), l'investissement est entièrement sur la monnaie. Les coûts électriques et de matériel restent minimes.

1.1.2 Sécurité

Le minage par preuve d'enjeu (POS) a ses propres challenges de sécurité. Pour le minage par preuve de travail (POW), les «coins» peuvent être stockées hors ligne dans un portefeuille papier ou matériel pour les protégér du vol. Pour le minage par preuve d'enjeu, les «coins» doivent être en ligne sur un portefeuille non verrouillé. StakePool a mis en place différentes mesures de sécurité physiques et logicielles pour éviter les intrusions. StakePool utilise un solution professionnelle d'atténuation d'attaque pas déni de service (DDOS).

1.1.3 Transparence

Nous nous efforcerons d'être aussi transparents que possible, tout en gardant la sécurité comme premier objectif. À partir du 1er novembre, les adresses des pourtefeuilles seront postées en ligne, aussi bien pour les preuve d'enjeu (POS) que pour les masternodes.

1.2 Aspects techniques

1.2.1 Pourquoi la preuve d'enjeu (POS) ?

En 2015, la quantité d'électricité nécessaire au minage d'un bloc Bitcoin aurait suffit à alimenter 1,6 maison états-unienne pendant un jour. En 2016, c'était 2,5 maisons par bloc. Dans un papier récent, des chercheurs ont estimé que les transactions Bitcoin consommeront autant d'électricité que le Danemark d'ici 2020. Alors que l'adoption des crypto-monnaies s'accélère, c'est tout à fait contraire aux objectifs écologiques indispensables à notre planète

Les développeurs d'Ethereum se sont sentis concernés par ce problème et ont présenté une méthode de consensus plus écologique, qui avec la mise à jour vers la version Casper, migrera de la preuve de travail (POW) vers la preuve d'enjeu (POW). Ethereum rejoindra alors les nombreuses autres crypto-monnaies qui utilisent déjà la preuve d'enjeu (POS) depuis 2012.

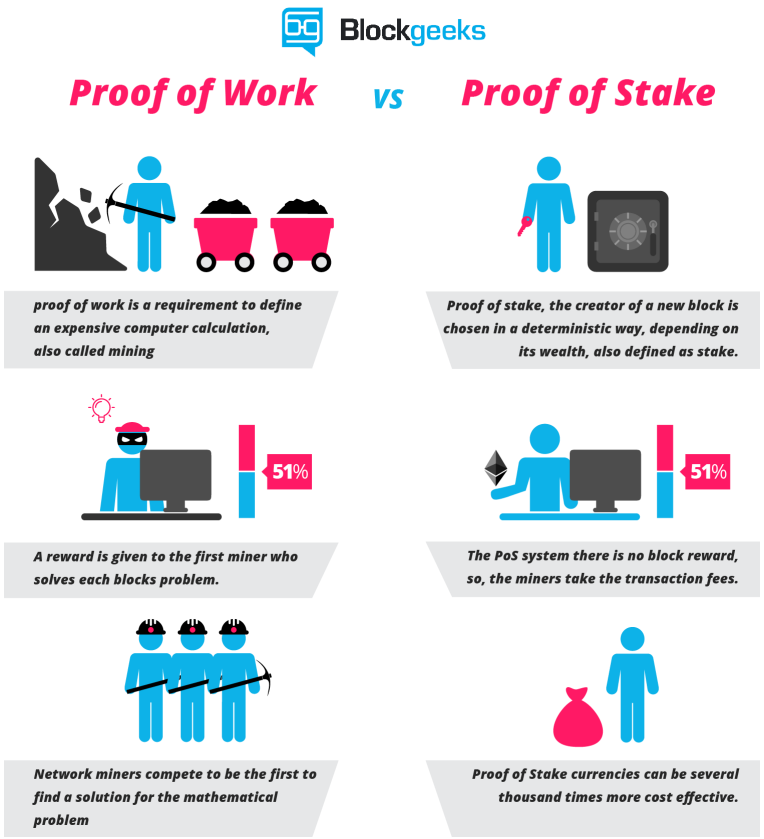
La preuve d'enjeu n'est pas seulement un système plus juste, il est aussi des milliers de fois moins coûteux. Les propriétaires laissent simplement leurs «coins» sur leur portefeuille sur le réseau afin qu'ils maturent. Les investisseurs qui immobilisent ainsi leur «coins» peuvent gagner des récompenses — un peu comme s'il engrangaient des intérêts de leurs avoirs. La preuve d'enjeu ne requérant donc pas de matériel spécifique de minage (GPU,...), elle est plus juste, plus écologique, et évite une centralisation du minage, dangereuse pour le réseau.

However, there is one SHA256 alternative that is already here, and that essentially does away with the computational waste of proof of work entirely: proof of stake. Rather than requiring the prover to perform a certain amount of computational work, a proof of stake system requires the prover to show ownership of a certain amount of money. [2]

1.2.2 Qu'est ce que la preuve d'enjeu (POS)

Le concept de la preuve d'enjeu (POS) repose sur le fait qu'une personne peut valider un bloc en fonction du nombre de «coins» dans son portefeuille. Plus on a de «coins», plus on a de puissance de minage. Le principe du minage par preuve d'enjeu est de garder les «coins» sur un portefeuille ouvert sur le réseau (donc pas sur un portefeuille matériel). Les portefeuilles forment ainsi un résau P2P, au travers duquel les transactions sont confirmées, et les récompenses correspondantes accordées. Ces récompenses sont les dividendes qui seront reversés au détenteurs de jetons POOL tous les mois.

Figure 1: POW vs POS [3]



1.2.3 Masternodes

On peut le voir comme un serveur spécial, qui est maintenu en ligne 24h/24h. Les masternodes n'ont pas besoin de tiers de confiance, et sont décentralisés, à la manière des nœuds du réseau Bitcoin. Il y a quand même une différence majeure, puisque les masternodes Dash prennent part au protocole d'anonymisation Darksend. Les utilisateurs peuvent choisir d'envoyer des transactions anonymes directement depuis leur portefeuille Dash.

Chaque masternodes du réseau fourni un service d'anonymisation, s'assurant ainsi qu'il n'y a pas de point centralisé à attaquer ou à faire tomber. De plus, les masternodes assurent que les transactions sont validées en quasi temps-réel. Enfin, les opérateurs des masternodes Dash reçoivent une compensation financière pour le service rendu.

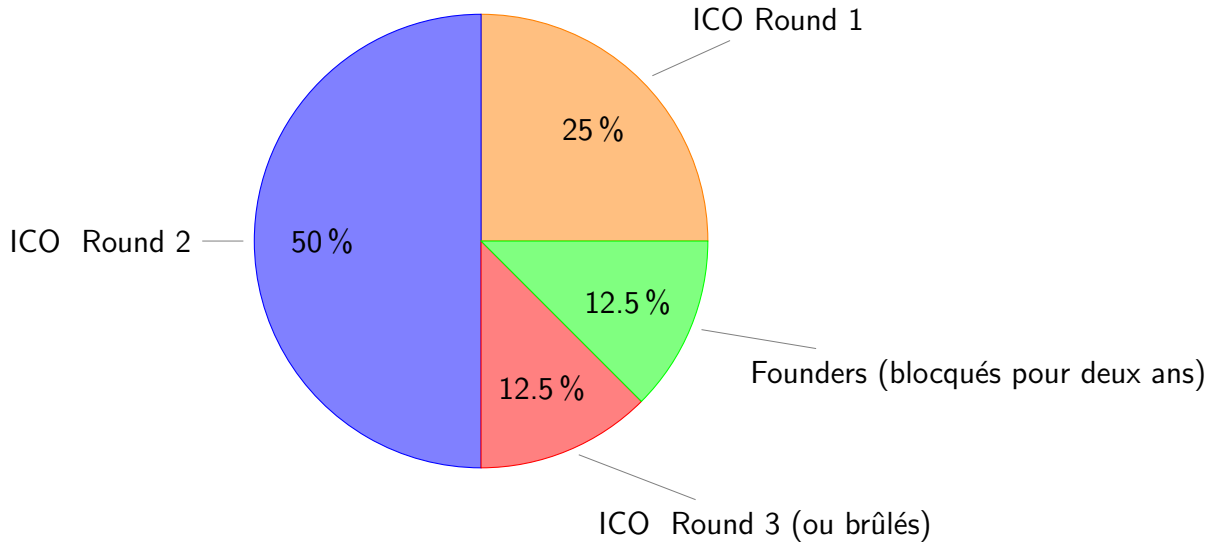
2 Émission des jetons

Les jetons POOL seront émis pendant une phase de pre-ICO pour les premiers investisseurs. Tous les fonds levés lors de la phase de pre-ICO seront utilisés pour acheter des «coins» POS. Un bonus de 10

La première vague de la levée de fond officielle ne commencera qu'une fois le premier paiement au détenteurs des jetons pre-ICO effectué. Elle durera deux mois. Les ethereum collectés durant la première phase seront là aussi consacré à l'achat de nouveaux «coins» à preuve d'enjeu. Cependant, 10

La seconde phase sera annoncée plus tard et sera consacrée à l'achat d'ETH pour préparer la bascule vers Casper.

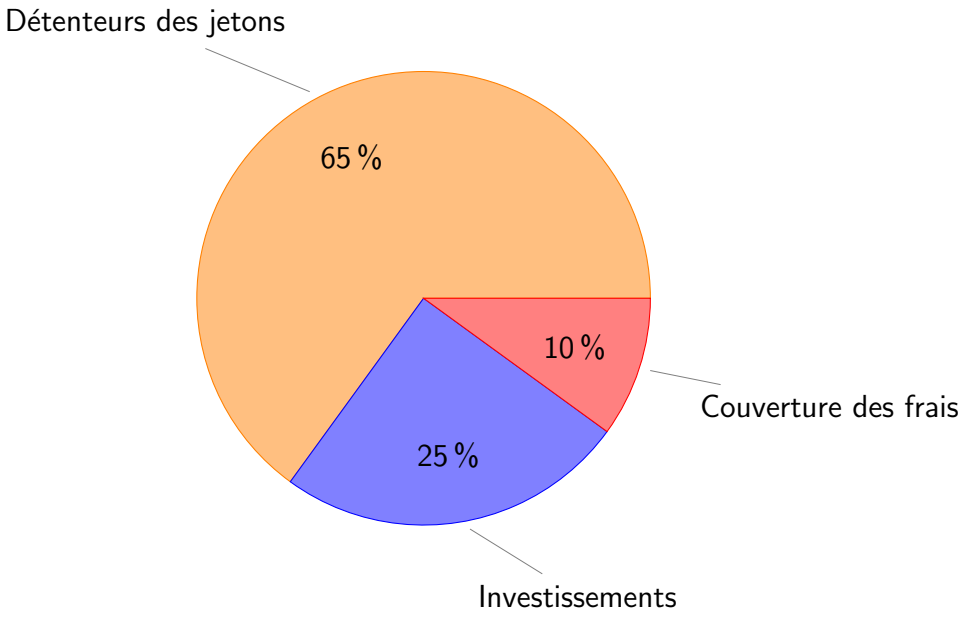
Figure 2: Distribution des jetons



3 Paiements

La dernière semaine de chaque mois, une annonce rappellera à tous les détenteurs de jetons de garder leur jetons POOL dans un portefeuille Ethereum et non sur une place d'échange. En début de mois suivant, une feuille de calcul Google Docs sera publiée et annoncée. Elle contiendra la liste des détenteurs à la date butoir, et le montant d'ETH distribué à chacun. Le paiment interviendra aux alentours du 10 du mois. Les profits seront répartis comme suit : 65% iront aux détenteurs de jetons, 25% seront réinvestis pour acheter plus de «coins» POS, et 10% couvreront les coûts opérationnels, les mises à niveau matériel, etc...

Figure 3: Distribution des dividendes



4 Feuille de route

Début août 2017	Publication du whitepaper
Août 2017	Annonce
7 septembre 2017	Lancement pre-ICO (bonus de 10%)
Début septembre 2017	Déménagement des serveurs
7 au 21 septembre 2017	Achat des «coins» pour commencer le minage POS
1er octobre 2017	Traitement du premier paiement des détenteurs de jetons pre-ICO
10 octobre 2017	Première vague de l'ICO (bonus 5%)
Octobre 2017	Lancement du masternode BOScoin
1er novembre 2017	Traitement du paiement des detenteurs de jetons
Novembre 2017	POOL token sur les places d'échange
1er décembre 2017	Traitement du paiement des detenteurs de jetons
2018	Deuxième vague de l'ICO
...	Les paiments continuent mensuellement

5 Contacts

Site web: `http://stakepool.co`

Twitter: `https://twitter.com/POSMiningCo`

BitcoinTalk: `https://bitcointalk.org/index.php?topic=2105630`

Facebook: `https://www.facebook.com/POS-Mining-Co-StakePoolco-136398393631970/`

Références

[1] Vitalik Buterin. A proof of stake design philosophy. *medium.com*, 2016. 1

[2] Vitalik Buterin. What proof of stake is and why it matters. *bitcoinmagazine.com*, 2013. 2

[3] BlockGeeks. Proof of work vs proof of stake: Basic mining guide. *blockgeeks.com*, 2017. 3