Prédiction des temps de validation des transactions dans la blockchain Ethereum

Arnaud Laurent[1], Luce Brotcorne[1], Bernard Fortz[1,2]

[1] Inria Lille, France {arnaud.laurent,luce.brotcorne,bernard.fortz}@inria.fr
[2] Université libre de Bruxelles, Belgium bernard.fortz@ulb.ac.be

Mots-clés : *Pricing, blockchain, Ethereum, gasprice, ether*

1 Présentation de la blockchain Ethereum

La blockchain est une technologie émergente utilisée en premier lieu pour servir de support à des crypto-monnaies. Cependant cette technologie peut aussi être le support pour des applications décentralisées et sécurisées. C'est l'objectif de la blockchain Ethereum [1] qui est à l'heure actuelle la deuxième blockchain la plus importante après la blockchain Bitcoin. Ethereum intègre un langage de programmation quasi-Turing complet, permettant la création et l'utilisation de "smart contract". Ces contrats sont exécutés automatiquement dans la blockchain sans nécessiter de tiers de confiance.

Comme son nom l'indique la blockchain est constitué d'une chaine de blocs. Chaque bloc contient le hashcode du bloc précédent, appelé bloc parent. Ainsi la chaine ne peut être brisée, car si quelqu'un essaie de modifier un bloc, le lien entre les blocs sera brisé. La chaine ainsi créée est représentée par la Figure 1.

Chacun de ces blocs contient les transactions qui ont été validées et qui impactent l'état du système. Dans Ethereum, un nouveau bloc est créé en moyenne toutes les 15 secondes. Les acteurs qui créent ces blocs sont appelés mineurs. Les mineurs choisissent les transactions qu'ils souhaitent ajouter à leur bloc. Ils peuvent sélectionner n'importe quelles transactions valides envoyées par les utilisateurs de la blockchain. Les mineurs récupèrent les frais liées aux transactions. En général les mineurs favorisent les transactions qui leur rapportent le plus.

Une des particularité de la blockchain Ethereum est son langage de programmation intégré quasi-Turing complet. Ce langage permet aux utilisateurs d'exécuter des applications décentralisées au sein de la blockchain. Cela entraine deux problèmes :

— Si une boucle infinie est exécutée par une transaction, les mineurs qui voudrons l'ajouter à leur bloc seront bloqués infiniment.
— Les transactions entrainant l'exécution d'applications décentralisées consomment plus de ressources que de simples transactions de fond et devraient donc payer des frais supplémentaires.

Pour répondre à ces problématiques, la mécanique de *gas* a été introduite. Le *gas* représente l'unité de consommation de ressources des transactions. Chaque opération provoquée par une

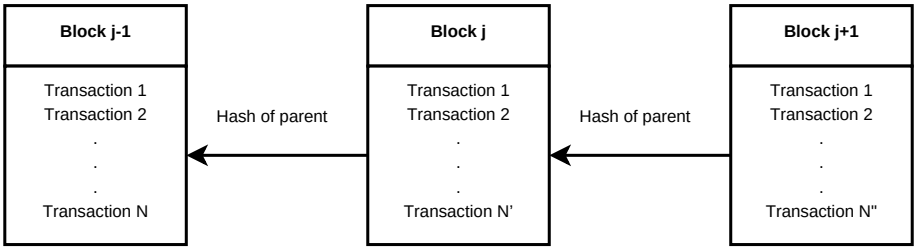

FIG. 1 – La chaine de blocs

transaction a un coût en *gas* [3]. Un bloc ne peut pas dépenser une quantité de *gas* supérieur à sa limite de *gas* par bloc.

L'utilisateur fixe deux paramètres pour chaque transaction envoyée :

— Le *gasLimit* qui est le montant maximal de gas que la transaction pourra dépenser. Au delà de cette valeur, la transaction sera annulée mais les frais seront tout de même payés aux mineurs. La quantité réellement consommée par une transaction n'est connue qu'une fois ajoutée à un bloc.

— Le *gasPrice* qui est le prix en ether (la monnaie associée à la blockchain Ethereum) pour chaque unité de *gas* consommé.

C'est cette deuxième valeur à laquelle nous allons nous intéresser. Le fait étant que plus le *gasPrice* d'une transaction sera élevé, plus une elle sera traitée rapidement par les mineurs. La question est donc de savoir quelle valeur minimum du *gasPrice* (1) va assurer la probabilité ϵ qu'une transaction tr soit minée avant la date T (2).

$$Min\ gp_{tr} \tag{1}$$

$$P(dateMining_{tr} < (T)) \geq \epsilon \tag{2}$$

2 Méthodes de résolution

Afin d'estimer la probabilité de minage d'une transaction dans un temps donné, nous proposons un modèle déterministe ainsi qu'un modèle stochastique. Le premier modèle a la particularité de pouvoir être résolu en temps polynomial contrairement au modèle stochastique. Cependant seul le modèle stochastique peut prédire efficacement ces probabilités. Afin de les approximer, nous proposons une méthode de Monte-Carlo [2] en fixant des valeurs aux variables aléatoires.

Une fois ces probabilités obtenues, on peut alors déterminer le gasprice gp minimal pour qu'une transaction donnée soit minée dans le temps T avec une probabilité λ.

3 Conclusion et perspectives

Les premiers résultats obtenus sont encourageants et intéressants. Les prédictions semblent légèrement pessimistes comparé à la réalité mais assez fiables pour donner une bonne prédiction des temps de minage.

Afin d'améliorer ces résultats, nous souhaitons perfectionner nos méthodes d'évaluation afin de cibler plus efficacement les potentielles améliorations de notre méthode. Enfin, nous souhaitons évaluer la performance de nos modèles en conditions réelles de mise en circulation de transactions en temps réel.

Références

[1] Vitalik Buterin et al. Ethereum white paper, 2014. *URL https ://github.com/ethereum/wiki/wiki/White-Paper*, 2013.

[2] Nicholas Metropolis and Stanislaw Ulam. The monte carlo method. *Journal of the American statistical association*, 44(247) :335–341, 1949.

[3] Gavin Wood. Ethereum : A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151 :1–32, 2014.