Analyse de la complexité dans le réseau de Bitcoin

Nghia Hieu HOANG
Département Télécommunications Services et Usages
INSA Lyon
nghia.hoang@insa-lyon.fr

16 Mai 2023

1 Introduction

Bitcoin est une monnaie numérique décentralisée basée sur la technologie blockchain, qui a été introduite pour la première fois en 2008 par un pseudonyme, Satoshi Nakamoto. Au cœur de ce réseau se trouve le processus de minage, dans lequel les participants s'affrontent pour résoudre des énigmes mathématiques complexes afin de valider des transactions et d'ajouter de nouveaux blocs à la blockchain. Le paramètre de difficulté joue un rôle central dans la régulation de la vitesse à laquelle de nouveaux blocs sont ajoutés à la blockchain, garantissant une émission cohérente de bitcoins tout en maintenant la sécurité du réseau.

Le concept de difficulté est étroitement lié à la complexité du réseau Bitcoin, reflétant les complexités impliquées dans les opérations minières et la puissance de calcul sous-jacente requise. Au fur et à mesure que de plus en plus de participants rejoignent le réseau, la concurrence s'intensifie, entraînant des ajustements du niveau de difficulté pour maintenir un taux prédéterminé de génération de blocs. Cette interaction entre la difficulté, les opérations minières et la sécurité du réseau établit un domaine d'étude intrigant pour comprendre la complexité de l'écosystème Bitcoin.

Dans cette analyse, je me lance dans une analyse approfondie de la complexité du réseau Bitcoin, en me concentrant spécifiquement sur la nature dynamique du paramètre de difficulté. Mon objectif est de mieux comprendre comment fonctionne le mécanisme de ce réseau, comment révolutionne la complexité à l'intérieur, en explorant l'impact des ajustements de difficulté sur le réseau. Grâce à une étude compréhensive, je vise à démêler les interactions entre la difficulté, les opérations minières et les participants au réseau.

2 Evolution de la difficulté

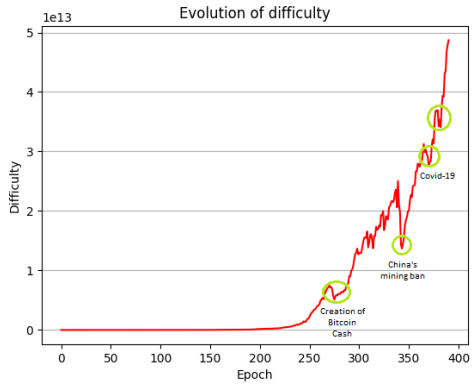
2.1 Aperçu général

Le mécanisme de consensus est le processus par lequel les participants s'accordent sur l'état actuel du registre de transactions sans avoir besoin d'une autorité centrale. Proof of Work (PoW) est le mécanisme utilisé dans le réseau de Bitcoin, donc un certain temps est nécessaire pour qu'un nouveau bloc soit ajouté dans la chaîne. Ce temps-là s'appelle **block pace**. Dans le cas de Bitcoin, un block pace est d'environ 10 minutes.

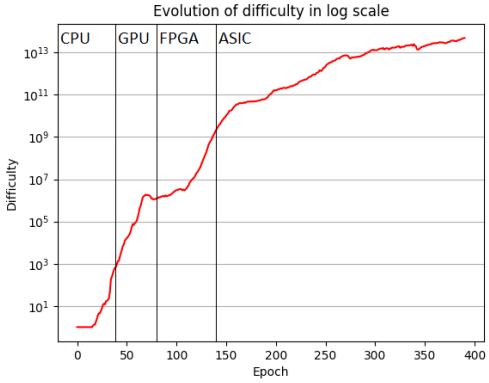
Bien sûr, ce délai n'est pas absolu, car la volatilité des participants affecte le temps nécessaire pour trouver un nouveau bloc, donc la notion de **difficulté** est mise en place pour maintenir la stabilité du réseau. Elle est une quantité lisible par l'homme qui détermine le niveau du problème mathématique requis pour miner un bloc. L'ajustement de la difficulté est fait après chaque époque de 2016 blocs, ce qui équivaut à 2 semaines si on prend une valeur cible de 10 minutes pour un block pace.

À partir de la naissance de Bitcoin, sa difficulté est initialisée à 1. 1 est également sa limite inférieure, et elle n'a pas de limite supérieure. Après chaque époque, la difficulté ne peut être augmentée que jusqu'à 4 fois et pas diminuée de plus de 4 fois par rapport à celle précédente pour éviter la soudaineté. La figure 1 montre l'évolution de la difficulté en fonction des époques, depuis le début avec l'époque 0 jusqu'à maintenant nous sommes à l'époque 391. D'après le graphique 1a, on peut voir qu'il y a des hauts et des bas et des tendances à la hausse tout au long du développement, indiquant que le système Bitcoin continue de croître régulièrement et progressivement. Par conséquent, il y a quelques endroits où il y a une baisse inhabituelle qui marque différents événements. Le premier événement a été des désaccords au sein de la communauté Bitcoin en 2017 qui ont conduit à un hard fork, aboutissant à la création de Bitcoin Cash (BCH), une crypto-monnaie distincte. L'interdiction d'exploitation minière en Chine vers juin 2021 a entraîné une baisse drastique des difficultés, après quoi il n'a fallu qu'environ six mois pour que le système revienne à son état d'origine avant que l'interdiction ne soit prononcée. Les récentes épidémies de Covid-19 l'ont également affecté.

L'échelle logarithmique de la figure 1b nous aide à mieux voir les progrès au fil du temps. Le **taux de hachage** total est une quantité estimée qui indique combien de hachages sont calculés par seconde dans l'ensemble du réseau, donc fondamentalement c'est une métrique pour mesurer la puissance du système. Cette mesure est proportionnelle à la croissance de la difficulté, on peut voir dans les premiers temps cette croissance est extrêmement forte. C'est parce que l'équipement minier a été développé très rapidement, du CPU au GPU, FPGA, et vers 2013-2014, ASIC. Chaque génération de nouvelles machines minières est plus rapide que la précédente, bien que cette augmentation ne soit pas régulière. Il est largement admis que le taux d'augmentation du taux de hachage s'essouffle, comme le montre la figure.



(a) Linear scale



(b) Log scale

Figure 1: Evolution of Difficulty

2.2 Comparaison avec block pace

Cette figure montre la relation entre la difficulté et le block pace. Pour mieux voir de détails, je n'ai tiré que les données à partir de l'époque 350. Il est assez clair qu'à chaque fois que le block pace passe sous l'objectif de 10 minutes, la difficulté diminue, et vice versa.

Donc, j'ai eu l'idée d'une formule pour calculer la difficulté, qui était bien évidemment intuitive : pour époque i

$$diff[i+1] = diff[i] * (2016*10)/(temps[i*2016-1] - temps[(i-1)*2016])$$

Dans la figure 2, on ne peut pas voir la courbe rouge, car la courbe verte correspond parfaitement à la courbe rouge, en d'autres termes, c'est la formule de calcul de la difficulté du réseau. Cependant, cette formule a un problème.

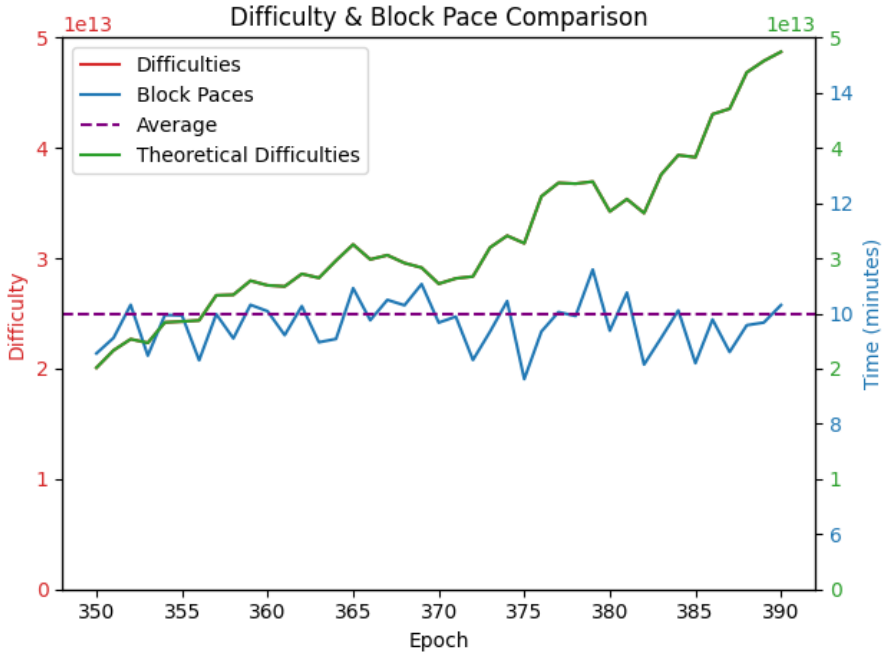


Figure 2: Difficulty and block pace comparison

La période utilisée pour le calcul ne comprend que la période des 2015 blocs, de bloc (i-1)*2016 à bloc i*2016-1. Le temps de passage entre le bloc i*2016-1 et bloc i*2016 est complètement oublié à chaque époque. Est-ce l'intention initiale ou est-ce un problème qui doit être résolu, puisque la période de cible utilisée dans la formule est toujours la période des 2016 blocs ?

3 Correlation entre le taux de hachage et le prix de Bitcoin

En étudiant la difficulté du système a soulevé une question dans mon esprit : la difficulté affecte-t-elle la valeur réelle de cette pièce ?

Parce que la difficulté ne change qu'après environ 2 semaines mais que la valeur du Bitcoin change quotidiennement, il est plus lisible de comparer le taux de hachage avec le prix quand on sait que le taux de hachage et la difficulté sont étroitement proportionnels l'un à l'autre.

Le taux de hachage est une approximation, pas une valeur exacte, car il n'est pas possible de mesurer avec précision toutes les machines de minage dans le monde ni le taux de hachage de chaque machine en raison de son mouvement continu et non stationnaire. Les chiffres du graphique sont obtenus via une API

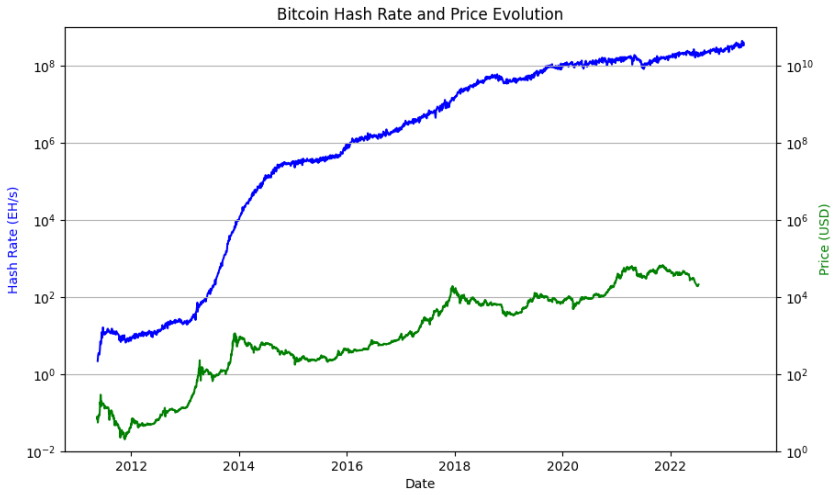


Figure 3: Price vs Hash Rate

qui fournit une approximation au jour le jour. En fait, cela ne nous dérange pas trop car le but ici est que nous pouvons avoir une idée générale de la façon dont ils changent.

Tout d'abord, nous pouvons immédiatement voir la ressemblance du taux de hachage avec la courbe de difficulté de la figure 1, confirmant ainsi l'hypothèse énoncée précédemment sur la relation entre la difficulté et le taux de hachage.

Comme la difficulté, le taux de hachage a initialement augmenté très rapidement, puis récemment, il a également ralenti. Avec la hausse des prix de l'électricité, l'augmentation des taux de hachage global dans le monde et la réduction de moitié des récompenses minières tous les 4 ans (6,25 bitcoins/bloc à l'heure actuelle) expliquent également en partie le phénomène.

De toute façon, en regardant attentivement le graphique, de petites fluctuations de prix et de taux de hachage sont proportionnelles. Ce n'est pas le cas des changements drastiques, car en théorie il n'y a pas de relation directe entre ces deux quantités et s'il y en a, ce n'est pas la seule quantité qui affecte la volatilité du prix. Cela peut être expliqué aussi bien que démontré : un taux de hachage élevé signifie qu'il y a plus de mineurs sur le système, ce qui augmente la difficulté, donc le prix augmente, attirant plus de personnes à participer au processus de minage, et vice versa.

4 Distribution du block pace

4.1 Étude et problème

Mon dernier résultat de recherche sur la complexité du système Bitcoin est la distribution du block pace. En fait, il existe de nombreux articles de recherche différents sur Bitcoin, dans de nombreux aspects tels que la sécurité, le système lui-même, l'impact environnemental, etc., utilisant les données pour leur analyse en assumant que la distribution du block pace est basée sur la loi de Poisson avec l'espérance de 10 minutes. Le plus typique d'entre eux est l'article original de la naissance de Bitcoin [1] : Il n'a pas dit explicitement que la distribution suivait cette loi, par contre, dans une section, pour effectuer des calculs, il a utilisé les paramètres qui étaient équivalents à l'hypothèse de la loi de Poisson. Cependant, il n'y a pas ou très peu d'articles liés à la preuve ou à la recherche de ce problème. Vous trouverez ci-dessous la figure 4 tracée sur les données pour les époques 0, 150, 300 et au fil du temps.

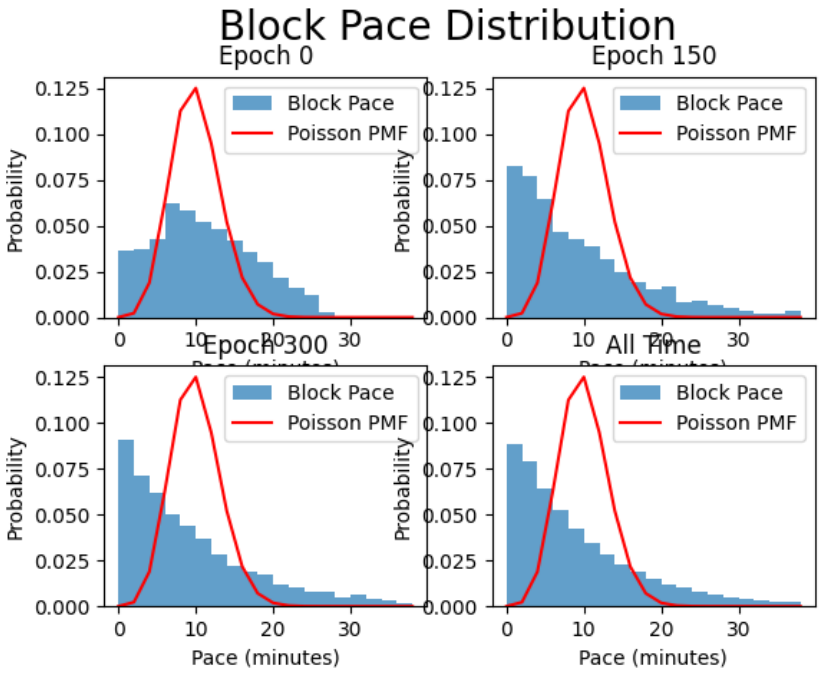
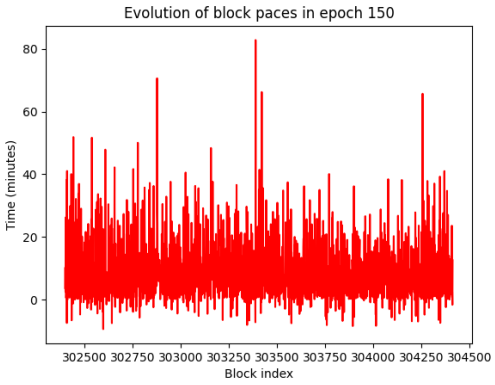


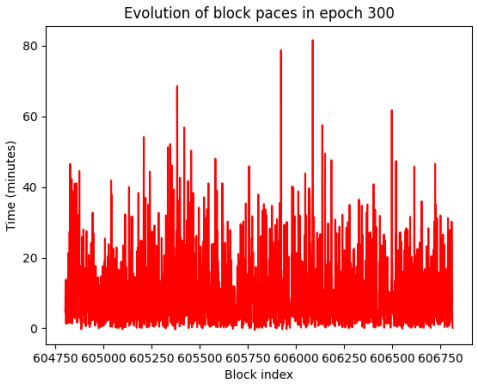
Figure 4: Price vs Hash Rate

On voit immédiatement qu'ils n'obéissent pas du tout à la loi de Poisson, même si je les ai laissés dans la même époque, c'est-à-dire que leur difficulté est la même, la condition en termes de probabilité aléatoire peut être garantie. Il y avait beaucoup de blocs trouvés avec un temps beaucoup plus court que le temps prévu de 10 minutes. Ensuite, j'ai essayé de regarder de plus près les

données des block paces à une époque donnée :



(a) Epoch 150



(b) Epoch 300

Figure 5: Evolution of block paces in one epoch

Le premier point d'absurdité quand on regarde la figure 5 est qu'il y a des moments où le block pace est négatif ! C'est complètement absurde, car l'ordre des blocs sur la blockchain est strictement défini, puisque nous avons des informations sur le hachage du bloc immédiatement précédent enregistré dans l'en-tête du bloc actuel. Ainsi, la première raison qui pourrait expliquer le phénomène au sommet est que la rétention des timestamps sur le réseau n'est pas fiable. Ce problème a été amélioré récemment, alors que dans la figure 5b, il ne reste que quelques valeurs négatives. Bien qu'on ne puisse pas leur faire confiance, comme je l'ai démontré dans la section 2, cet intervalle de temps est toujours utilisé pour calculer la prochaine difficulté. Est-ce un autre problème à résoudre ?

Une autre hypothèse que j'ai faite est que la période de changement de

difficulté est assez longue, environ 2 semaines en moyenne. D'après la figure 3, nous pouvons voir que le taux de hachage fluctue considérablement d'un jour à l'autre, en particulier dans les premiers stades. Cela veut-il donc dire qu'à la fin d'une époque le temps pour miner un bloc est plus rapide qu'au début, car en temps réel la vraie quantification qui affecte le processus des probabilités aléatoires est le taux de hachage réel et plus seulement la difficulté ?

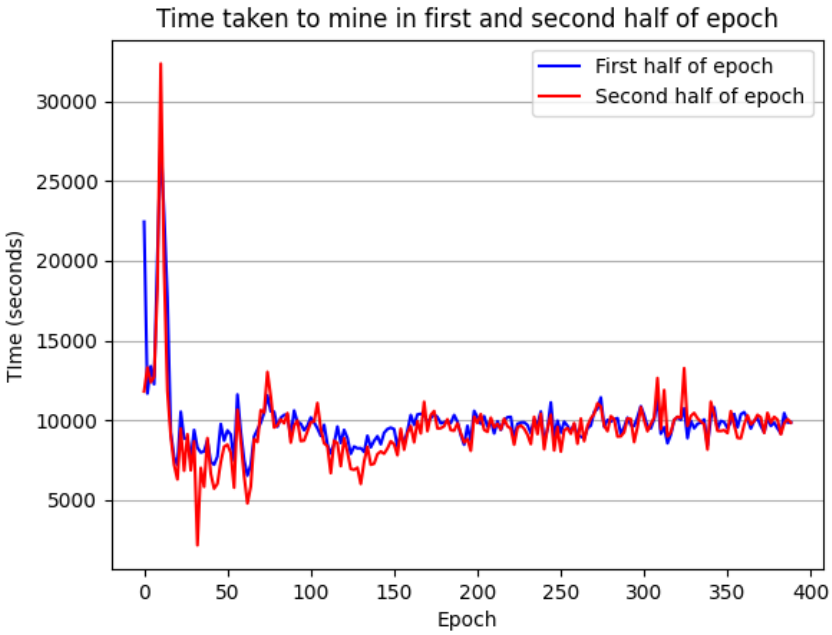


Figure 6: Time taken to mine in first and second half of epoch

La figure 6 confirme partiellement l'hypothèse ci-dessus, car dans les premiers stades, la courbe rouge a eu tendance à se situer en dessous de la courbe bleue. En fait, c'est aussi très raisonnable, car comme je l'ai mentionné plus haut, le taux de hachage n'augmente plus aussi fortement qu'avant, le fait que le temps pour miner dans les deux moitiés n'est plus si différent est assez évident.

La dernière hypothèse que j'avance est le phénomène de minage égoïste. C'est le phénomène que certains mineurs peuvent être incités à retarder ou à accélérer la création de nouveaux blocs, en fonction de la rentabilité de l'exploitation minière et d'autres facteurs, vise à faire plus de profit. Cependant, ce phénomène sort du cadre de cette étude, je ne vais donc pas en parler plus en détail.

4.2 Solution proposée / Travail ouvert

En fait, c'est peut-être une question qui mérite attention et résolution, car

elle peut affecter l'authenticité de nombreux autres articles scientifiques. Arrivant à la fin du projet PIR, j'ai une idée de comment on peut résoudre le problème ci-dessus. C'est que nous allons faire d'une manière pour que le bloc actuel ne vient pas à tous les nœuds de minage en même temps, mais il atteint progressivement les mineurs étant de plus en plus puissants. Pour le mettre en pratique, nous pouvons faire une simulation, et on a le taux que les mineurs reçoivent le bloc est proportionnel aux nombres de mineurs qui l'ont pas encore, ce qui crée un délai de bloc qui suit la loi exponentielle.

5 Conclusion

Cette étude scientifique se penche sur les aspects les plus fondamentaux du système en termes de complexité, y compris la difficulté et le temps d'arrivée de l'exploitation minière. Il y a encore des questions ouvertes derrière cette recherche, et pour moi personnellement, cette recherche a conduit à une meilleure compréhension du réseau bitcoin ainsi qu'à beaucoup d'intérêt académique.

Bibliographie

[1] Satoshi Nakamoto. Bitcoin : A Peer-to-Peer Electronic Cash System. Disponible sur : https://bitcoin.org/bitcoin.pdf?fbclid=IwAR0pWJT_foxYP1oOrnAW0z6Sd3uDjhlMdeH53i0NU3wnCn8KPASlnTxDbao (consulté le 16/03/2023)

[2] https://github.com/nhh1603/bc_complexity