Economics of Bitcoin

Sunk cost, incentive mechanisms and dynamics of miners' pools

Othmane EL BELGHITI

ARTICLE INFO

Keywords:
Bitcoin
Dynamics
Blockchain
Miners
Pools
Incentives
Transaction
Migrations

ABSTRACT

En 2018, le cours du Bitcoin a fortement chuté en passant de 19499$/BTC à son pic au mois de décembre 2017 à 6839$/BTC au mois de février 2018. Cette chute du cours a provoqué, d'une part, une participation amoindrie des petits acteurs du minage des cryptomonnaies et d'autre part, des modifications majeures au sein des règles de répartition des revenus des pools de mineurs (groupes de mineurs), ce qui peut donc potentiellement engendrer des migrations de « mineurs » entre différents « pools ». C'est ainsi, que l'on cherche à montrer ici les motivations des mineurs à rejoindre un pool donné pour enfin expliquer les migrations des mineurs entre différents pools.

Introduction

Après plus de 10 ans d'existence, le Bitcoin qui est la crypto-monnaie décentralisée la plus utilisée s'installe comme une alternative aux monnaies traditionnelles contrôlées par les banques centrales étatiques. La stabilité, la fiabilité et la sécurité de cette monnaie repose sur le travail d'individus appelés « mineurs ».

Ces derniers ont tendance à se regrouper au sein de groupes nommées « pools » afin de maximiser leur espérance de gain et réduire la variance de leurs gains. Ainsi, la pratique du « minage » requiert des investissements importants et irréversibles. La complexité de la pratique du minage devrait être à l'origine d'un nombre limité de pools. Cependant, des pools émergent et disparaissent très rapidement. Ainsi, l'objectif de ce document est d'identifier les éléments relatifs au fonctionnement des pools pour ensuite expliquer ces fortes variations.

Pour appuyer cette démarche, les articles scientifiques utilisés traitent d'aspects différents relatifs au Bitcoin. Alors que le papier de Rosenfeld « Analysis of Bitcoin Pooled Mining Reward Systems » publié en 2011 s'intéresse aux règles de répartition des gains au sein d'un pool, d'autres articles scientifiques comme « Bitcoin: Economics, Technology, and Governance » de Rainer Böhme ou « SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies » de Joseph Bonneau publiés tous les deux en 2015 insistent sur le potentiel de cette monnaie à disrupter les systèmes de paiements actuels et la nécessité d'une gouvernance du Bitcoin. Enfin, le papier « Trends, Tips, Tolls : A Longitudinal Study of Bitcoin Transaction Fees » de Malte Moser publié en 2014 met en lumière le rôle des frais de transactions pour assurer la stabilité du Bitcoin et « The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries » publié en 2013 de Joshua A. Kroll explique en profondeur le mécanisme de mining. D'autres articles scientifiques ou sources ont été utilisées pour mener à bien cette revue littéraire et sont annotés dans la partie références.

Ce document se structure alors de la manière suivante. Après une première section expliquant le fonctionnement du protocole Bitcoin ainsi que ses composantes majeures, il s'agit ensuite d'expliquer les déterminants de la dynamique des « mineurs » au sein des « pools ».

1.1 Bitcoin et le minage

1.1.1 Bitcoin

Le Bitcoin[1],[2]est une monnaie électronique fiduciaire décentralisé utilisant la cryptographie et un réseau peer-to-peer.

Depuis sa création en 2009 par un groupe anonyme de développeurs (Nakamoto 2008), le Bitcoin[3] a servi pour environ 62.5 millions de transactions entre plus de 109 millions de comptes. (Chiffres de 2015).

Ainsi, alors que de nombreux observateurs ont jugé insignifiantes la montée des crypto-monnaies, les données montrent qu'en Avril 2017, le marché des crypto-monnaies[4] capitalise plus de 27 milliards de dollars. La répartition du marché a subi différentes variations au fil des ans. En effet, on peut noter une baisse de la part de marché du Bitcoin au détriment des autres crypto-monnaies entre 2015 et 2017.

On estime alors à 10 millions de personnes le nombre de personnes ayant possédé du Bitcoin en 2016 (CoinBase and ARK Research).

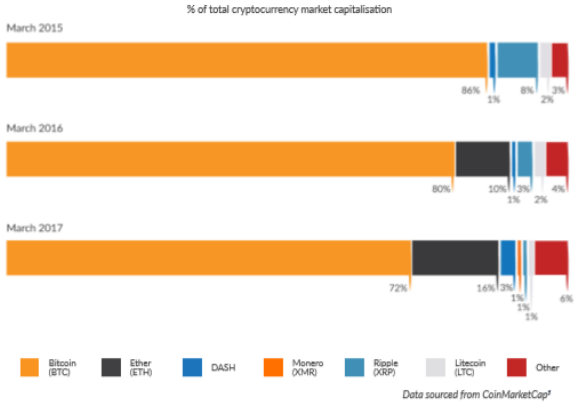

Fig 1 : Répartition du marché des cryptos[5]

Mais, il reste difficile d'estimer le nombre d'utilisateurs du Bitcoin[6], car un même individu peut posséder plusieurs portefeuilles chez différentes plateformes en même temps.

Cependant, le Bitcoin reste la crypto-monnaie la plus largement utilisés à la vue du nombre de transactions journalières. Elle est suivie par l'Ethereum comme le montre la figure ci-dessus.

Le Bitcoin est également la crypto-monnaie la plus supportée[7] et utilisée par la majorité des plateformes d'échanges et services de paiement ce qui explique l'importance de son utilisation par rapport aux autres crypto-monnaies.

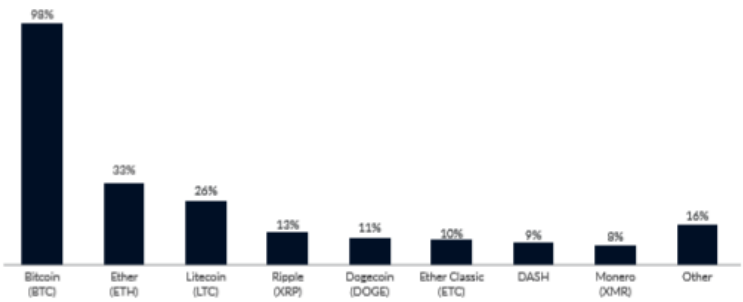

Fig 2 : Répartition des transactions[8]

Avant même la création du Bitcoin, et dès les années 90, plusieurs startups comme DigiCash[9] ou Peppercoin[10] ont essayé d'introduire des crypto-monnaies mais ont échoué une fois sur le marché. Ces monnaies intégraient déjà certaines briques actuelles du Bitcoin tels que la preuve de travail (« proof of work »).

En 2008, un papier expliquant le protocole Bitcoin a été publié sous le pseudonyme de Satoshi Nakamoto[11] et fut suivi par la publication du code source du client Bitcoin. Ainsi, le 1er bloc appelé « Block Genesis » a été validé le 3 Janvier 2009 et la 1ère utilisation du Bitcoin s'est déroulée en Mai 2010 lorsqu'une personne s'est fait livrer une pizza en échange de 10000 Bitcoins. Depuis, de nombreux commerçants ont adopté cette monnaie et le cours du Bitcoin s'est envolé jusqu'à atteindre 20 000$/Bitcoin en décembre 2017 pour rechuter à environ 4000$ fin 2018.

Ainsi, un Bitcoin correspond à un objet représenté par une chaine de signatures digitales[12] représentant les transactions pour lesquelles ce Bitcoin a été utilisé. Il est alors possible de vérifier la validité d'un Bitcoin en vérifiant la validité des signatures constituant son historique.
Chaque Bitcoin est détenu par une « Bitcoin address » qui n'est autre qu'une clé publique. Le propriétaire de Bitcoin (qui détient la clé privée liée à cette clé publique) peut créer une transaction en signant une déclaration où il signifie que des Bitcoins sont transférés d'une adresse à une autre.
La personne réceptionnant le Bitcoin peut vérifier alors que la transaction est valide, mais elle ne peut pas vérifier un « double spending ». Il ne peut pas savoir si ce Bitcoin a été utilisé pour payer quelqu'un d'autre auparavant. Pour éviter cela, le système de Blockchain intervient. Chaque transaction en Bitcoin est enregistrée sous forme de log au sein d'un bloc contenant un timestamp et un hash cryptographique correspondant au bloc précédent. Plusieurs transactions sont enregistrées au sein d'un même bloc. (Cf. exemple figure 3). Chaque bloc contient donc un lien au bloc précédent et ainsi de suite. C'est pour cela que l'on parle de blockchain. Ainsi, en parcourant la blockchain il est possible d'atteindre le 1er bloc (appelée genesis block).


```
{"hash":"00000000000000f38...",
 "prev_block":"00000000000000c6d...",
 "time":1354114900,
 "difficulty":436527338,
 "nonce":282240624,
 "tx":[
   {"hash":"5ca...",
     "in":[
      {"prev_out":
        {"hash":"000...",},
      }
     ],
     "out":[
       {"value":"50.53620000",
        "scriptPubKey":"27a1..."
       }
     ]
   },
   ---
 ]
}
```


Fig 3 : Un Bloc dans la blockchain[13] représenté en JSON

1.1.2 Minage et pool de mineurs

Pour assurer la stabilité de la blockchain, des participants appelés « mineurs » sont chargés de miner des blocs, c'est-à-dire de valider un bloc contenant une série de transactions.

Dans un premier temps, des nœuds dédiés du réseau (les « mineurs ») créent un nouveau bloc en regroupant des transactions récemment effectuées et en leur adjoignant un en-tête contenant notamment la date et l'heure, une somme de contrôle (« hash ») qui servira également d'identificateur unique du bloc, et l'identificateur du bloc précédent.

Dans un second temps, après avoir vérifié la validité de toutes les transactions que contient ce nouveau bloc et leur cohérence avec les transactions déjà enregistrées, chaque mineur l'ajoute à sa version locale du registre (ou chaîne de blocs).

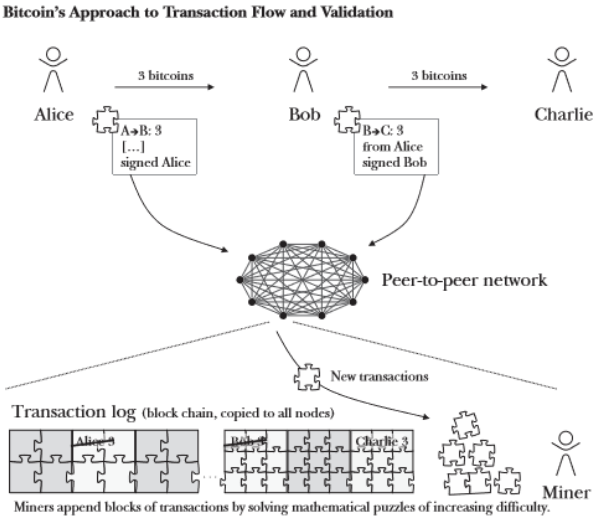

Fig 4 : Ajout d'une transaction à la blockchain[14]

Il s'agit de résoudre un puzzle difficile à résoudre mais facile à vérifier à la manière d'un Sudoku. On parle de « proof-of-work » ou preuve de travail[15].

Un bloc peut contenir un nombre quelconque de transactions, en général entre 1 000 et 2 000, sans toutefois que la taille du bloc puisse dépasser 1 mégaoctet (pour le système Bitcoin Core).

Au sein d'un bloc, les transactions sont stockées sous la forme d'un arbre de Merkle.

La somme de contrôle (ou empreinte) du bloc est calculée en appliquant deux fois un hashage SHA-256[16] au sextuplet constitué :

- Du numéro de version du logiciel,
- De l'empreinte de l'en-tête du bloc précédent,
- De la racine de l'arbre des transactions du bloc (qui est lui-même une empreinte indirecte de l'ensemble des transactions du bloc),
- De l'horodatage (temps écoulé depuis le 1er janvier 1970 0 h, en secondes),
- De la difficulté,
- Du nonce.

Le calcul de cette empreinte est rendu intentionnellement difficile par l'exigence d'être inférieure à une certaine valeur (la « difficulté »), qui se matérialise par une représentation binaire commençant par un certain nombre de zéros. À cette fin, l'empreinte contient parmi ses composants, un nombre arbitraire de 32 bits, le « nonce ».

Même si l'on connaît les empreintes correspondant à certains nonces, le hachage fait qu'il est impossible de déterminer la valeur de l'empreinte pour un nouveau nonce sans exécuter à nouveau l'algorithme. On ne peut donc trouver le nonce approprié à l'exigence de borne sur la valeur de l'empreinte qu'en faisant plusieurs essais.

Pour une valeur donnée du nonce, la probabilité de calculer une empreinte inférieure à la difficulté est très faible, de sorte que de nombreuses tentatives doivent être effectuées avant d'y parvenir. Entre 2014 et 2016, le nombre moyen de nonces que chaque mineur a dû tester

entre chaque création de blocs est passé de 1 milliard à 200 milliards. Ce calcul consiste[17] à effectuer un très grand nombre de fois le même calcul à partir de données différentes, il se prête donc bien au calcul parallèle.

La difficulté est réajustée tous les 2016 blocs pour tenir compte de la puissance de calcul réelle du réseau et permettre en moyenne d'ajouter un bloc toutes les 10 minutes, ce qui revient à dire que la durée probable de calcul d'une empreinte valide est de 10 minutes pour l'ordinateur ou le groupe d'ordinateurs le plus puissant du réseau.

Ainsi, chaque mineur possède une probabilité de trouver le prochain bloc de la blockchain proportionnel à sa part de la puissance totale de hash des mineurs.

De plus, le mécanisme de minage possède la propriété suivante. S'il existe deux branches de la blockchain avec deux groupes de mineurs en train de faire croitre chacune des deux branches, seule la branche avec les mineurs ayant la plus grosse capacité de calcul va grandir plus vite. Ainsi, seule la plus longue branche peut être considéré comme valide.

D'autre part, il faut savoir que la création d'un Bitcoin ne peut se faire qu'à l'aide du mécanisme de minage. En effet, lorsqu'un nouveau bloc est miné une transaction spéciale se rajoute à ce block qui permet de payer le mineur en Bitcoin. On parle de « block reward ». Cela introduit une incitation pour encourager le minage. Le nombre de Bitcoin créé par ce moyen est ajusté selon un calendrier prédéterminé pour lequel la récompense diminue de moitié chaque 210 000 block miné sachant que lors du lancement du Bitcoin le « mining reward » était de 50 Bitcoin par bloc.

1.2 Les déterminants de la dynamique des pools de mineurs

1.2.1 Block rewards et transaction fees

1.2.1.1 Block rewards

Aujourd'hui, on recense[18] plusieurs milliers de crypto-monnaies. Le point commun de ces crypto-monnaies est l'utilisation d'un « block reward » comme motivation pour les participants afin de maintenir en activité le réseau en l'absence de nœud central.

Joshua et Ian de l'université Princeton utilise le modèle[19] suivant pour mieux comprendre le mécanisme de minage.

En effet, si l'on prend un mineur donné. Il décide d'investir des ressources (équipements et électricité …) pour miner à un coût C dollars par secondes. Cet investissement va lui permettre de faire P=f (C) puzzles essais (hashes) par seconde. Sachant qu'il faut G essais pour résoudre un puzzle et avoir une récompense sous forme de Bitcoin d'une valeur V, on obtient la relation suivante : $C < \frac{P*V}{G}$. Le mineur va donc miner si $G < \frac{P*V}{C}$.

Lorsque l'on considère N mineurs, on a à un instant t donnée : $R = \sum_{i=1}^{N} \frac{P_i}{G}$ Avec R le nombre de nouveau blocks minés. Si P est le nombre total de hashes (essais) par secondes, le numérateur de cet expression et C le cout total dépensé dans le minage tel que $C = \sum_{i=1}^{N} C_i$ .On a alors : $G = \frac{P}{R}$. Ainsi, une personne décidera de miner si :

$$\frac{P}{R} < \frac{P*V}{C} \equiv C < R*V$$

Il y a donc un équilibre global pour lequel la récompense totale (en dollars) de minage par seconde est égale au coût global de minage. : $C = R*V$

Or, comme la valeur du « mining reward » V fluctue avec la valeur d'échange du Bitcoin, si le cours du Bitcoin chute, cela réduit les motivations de miner. Cela peut donc conduire à un cercle vicieux pour lequel la baisse de confiance dans le Bitcoin diminue le nombre de mineurs ce qui rend la monnaie plus vulnérable et donc réduit la confiance en cette monnaie etc …

D'autre part, lorsqu'un mineur mine et investit un montant C pour avoir une puissance P=f (C) hashes par secondes, ce dernier cherche à maximiser son utilité sans forcément suivre les règles énoncées pour le bon fonctionnement du Bitcoin.

A priori un mineur lambda peut créer un nouveau bloc sur n'importe quelle branche ou même crée une nouvelle branche sur un arbre existant. Les règles énoncent que les mineurs sont supposés étendre la plus longue branche, mais cette règle peut ne pas être respecté. Ainsi, comme le mineur reçoit un « block reward » si et seulement s'il rajoute un bloc à la chaîne la plus longue et que chaque mineur cherche à maximiser son profit, les mineurs vont se mettre d'accord pour utiliser la même stratégie et donc étendre la même branche de la blockchain ce qui va donc constituer un équilibre de Nash[20].

C'est ainsi que le réseau de vérification du Bitcoin est plus puissant que la puissance combinée des 500 meilleurs super ordinateurs au monde[21]

Enfin, comme les puzzles à résoudre par les mineurs sont devenues de plus en plus dur[22] au fil du temps et que le risque d'utiliser des ressources pour finalement ne recevoir aucun reward devient de plus en plus important, de nombreux mineurs indépendants décident de partager leurs ressources respectives au sein d'un groupe (appelée pool)[23] afin de réduire la variance de leurs revenus en partageant les « rewards » avec les autres mineurs.

En général, les pools sont administrés par un opérateur qui pour une légère commission collecte les « mining rewards » des blocks validés minées par les autres participants et effectue le partage entre les différents membres.
Ainsi, le système de reward (25 BTC par block reward en 2014) est un des facteursde succès de l'adoption du Bitcoin[24].

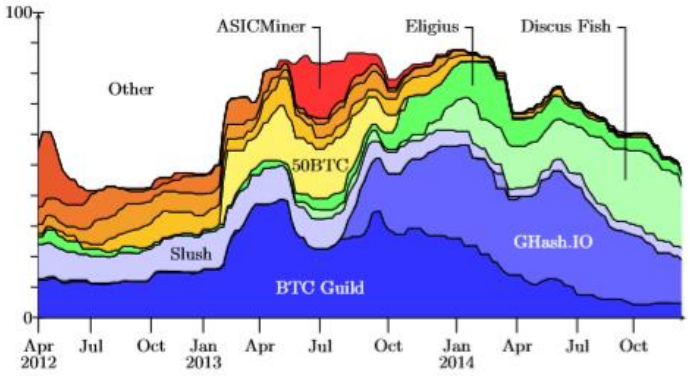

Fig 5 : Parts de validation des blocs par pools[25]

Cependant, cette récompense n'est pas compatible avec la limite prévue de la production de monnaie (21 000 000 blocs) qui constitue une autre règle du Bitcoin. Pour faire face à cette limite, le protocole propose également que l'émetteur d'une transaction offre des frais de transactions (transaction fee) au mineur ayant miné le bloc contenant cette transaction.

1.2.1.2 Transaction fees

La différence entre la valeur payée d'une transaction et la valeur reçu par le destinataire correspond au « transaction fee »[26], ce dernier est collecté par le mineur ayant miné le bloc contenant cette transaction. Il s'agit d'une sorte de pourboire pour le mineur.

Il faut savoir également comme l'explique Malte et Rainer que les mineurs sont libres d'accepter une transaction et de l'inclure dans la blockchain, ou de l'ignorer. Cela crée donc un marché qui permet de déterminer le coût d'une transaction en Bitcoin.

En théorie, un mineur va inclure une transaction si sa « transaction fee » excède le coût marginal de son inclusion. Les coûts de production sont fixés par bloc (mais peuvent variées en fonction du matériel du mineur et son accès à l'électricité) et le protocole définie une capacité maximale de la taille d'un bloc. Les mineurs font du bénéfice seulement si les transactions sont en compétition pour faire partie de la blockchain. Ainsi, Houy indique qu'il est nécessaire d'avoir une taille maximale[27] pour chaque bloc ce qui assure la stabilité du Bitcoin.

En pratique, les « transactions fee » ont longtemps étaient considérés par les émetteurs d'une transaction comme une sorte de pourboire. En effet, leur valeur était souvent la valeur par défaut de la transaction tel que codé dans le logiciel client[28].

Cette figure montre que le montant total des transactions par bloc en dollars varie de la même façon que prix du Bitcoin en dollars, à l'opposé des biens et services payés en Bitcoin dont le prix en monnaie conventionnel reste fixe. Ainsi le BTC est l'unité dominante quand il s'agit de décider quel montant donnée pour une « transaction fee » contrairement à ce que l'on pourrait penser.

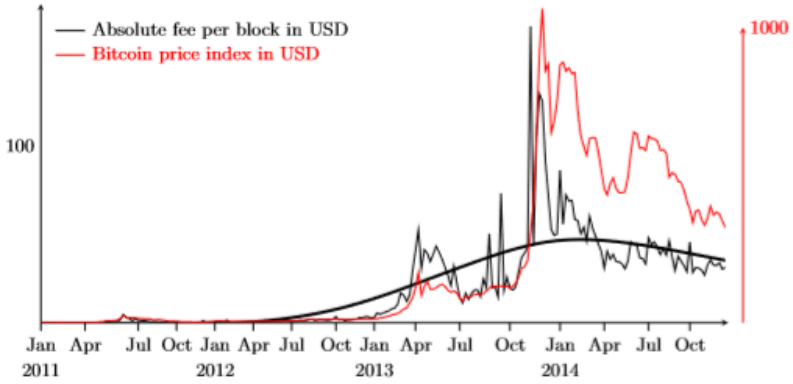

Fig 6 : Transaction fee par bloc (en dollars)[29]

D'autre part, comme l'expliquent Malte et Rainer, en 2014, une faible part des transactions n'offrait pas de transaction fee aux mineurs. Une large partie offrait la valeur par défaut et d'autres une valeur plus importante. Une hypothèse possible de cet écart serait le fait qu'une transaction fee élevé inciterait le mineur à mettre en priorité la transaction au sein de son bloc et donc accélérer la confirmation de la transaction. Si cela est vrai, les utilisateurs impatiens seraient plus enclins à augmenter leur « transaction fee ».

Ainsi, la table suivante montre les quantiles de la distribution des délais d'attentes des transactions avant leurs validation en fonction des « transaction fee ». Malte et Rainer remarquent alors que la moitié des transactions sans frais attendent plus de 20 minutes (1339 secondes) avant leur 1ère validation. Parallèlement, le fait de payer 0.0005 BTC conduit à une validation en moins de 10 minutes (600 secondes) pour 50 % des transactions.

		Quantiles of the latency distribution				
Fee	# Tx	10 %	25 %	50 % (median)	75 %	90 %
0	1503	180	444	1339	4270	13927
0.0005	5735	106	255	600	1244	2440
0.001	1905	90	212	520	1129	2135

Sample period: June 2012 to May 2013. See text for details.

Fig 7 : Délai d'attente d'une transaction par Transaction fee (en dollars)[30]

L'hypothèse est donc vérifiée, les utilisateurs impatients sont plus enclins à émettre des « transaction fee » plus importants.

Enfin, si l'on suit l'activité des pools et leur rapport vis-à-vis des « transaction fee », on peut noter que certains pools ont une politique plus restrictive avec les zero-fee transaction comme Discus Fish ou Eligius.

Rainer et Malte remarquent alors que que ces 2 pools ont vu leur part de marché progresser par rapport à d'autres pools comme BTC Guild acceptant les transactions sans frais (cf. fig. 5 plus haut). On en conclut que la politique des pools vis-à-vis des « transaction fee » consitue un facteur important de l'adhésion d'un mineur au sein d'un pool.

		% of zero-fee transactions		% of blocks w/o any zero-fee transaction	
Blocks solved (%)		Apr 2012–	Jan 2014–	Apr 2012–	Jan 2014–
All miners	100.0	7.2	2.7	8.5	17.7
BTC Guild	18.0	6.5	2.2	1.5	4.1
GHash.IO	13.0	4.0	3.4	2.0	2.3
Slush	7.2	5.6	3.4	6.9	2.7
Discus Fish	7.0	0.7	0.3	66.3	72.5
Eligius	5.2	4.1	0.7	26.1	29.2
50BTC	3.9	8.2	11.9	0.4	3.3
BitMinter	3.5	10.4	14.9	3.5	0.8
EclipseMC	3.3	22.3	3.8	2.0	2.6
OzCoin	2.8	8.0	3.3	1.2	7.7
ASICMiner	1.9	8.8	5.9	1.7	0.0

Excluding coinbase transactions. Pool data before Apr 2012 is unreliable.

Fig 8 : Délai d'attente d'une transaction par Transaction fee (en dollars)[31]

1.2.2 Règles de répartition, Taille du pool et revenu du minage

1.2.2.1 Taille du pool et revenu

Comme expliqué précédemment le minage consiste à calculer des hashes d'une structure de données appelés « block header » également appelé « proof-of-work ». Lorsqu'un bloc est miné, le mineur est gratifié d'un montant B de Bitcoin.
En considérant que la fonction de hashage soit suffisamment complexe, ainsi que le nonce généré de façon pseudo-aléatoire lors de la construction du bloc, on peut supposer que le fait de trouver le hash peut être considéré comme un phénomène aléatoire. Soit la difficulté de minage d'un bloc notée D. Cette dernière est ajusté tel que chaque hash permet de valider un bloc avec une probabilité de $\frac{1}{2^{32}D}$.
Ainsi, pour modéliser le revenu d'un mineur seul, Rosenfeld utilise le modèle suivant[32].
Soit un mineur avec une puissance de hash h (nombre de hashs par secondes). Ce dernier va calculer h*t hashes pendant une période t et va donc trouver en moyenne $\frac{ht}{2^{32}D}$ blocs. Son revenu sera de $\frac{htB}{2^{32}D}$.
Par exemple, on considère que Bob achète un équipement qui lui permet d'atteindre une puissance de h=1 Ghash/s. On suppose qu'il l'utilise de manière continue soit 86400 secondes par jours. Si la Difficulté D est de 1 690 906 et le « block reward » de 50 BTC. Il va trouver en moyenne $\frac{10^9\ hash/s*86400s}{2^{32}*1690906} \simeq 0.0119$ blocs soit 0.0119*B = 0.595 BTC.

Lorsqu'un mineur valide des blocs seuls avec une puissance de hash h, le minage constitue une loi de Poisson de paramètre $\lambda = \frac{ht}{2^{32}D}$. Il s'agit également de la variance du nombre de blocs minés. La variance du gain est de $\lambda B^2 = \frac{htB^2}{2^{32}D}$. Ainsi si l'on reprend l'exemple de Bob, ce dernier a une variance de 0.0119*B^2=29.75 BTC^2. Et la probabilité que Bob reçoive un paiement au cours de sa journée de minage est de 1-exp (-λ) $\simeq 1.18\%$.

On peut voir que la variance du minage est grande et qu'un participant avec une puissance de calcul importante peut attendre jusqu'à 3 mois en moyenne pour recevoir son 1er paiement. Et comme ce processus est aléatoire, si le mineur a attendu plusieurs mois sans trouver de bloc, il n'est pas plus proche de l'obtenir que par rapport au début du minage et doit toujours attendre en moyenne 3 mois.
C'est ainsi que pour éviter cette incertitude de recevoir un paiement que les mineurs travaillent ensemble pour miner à plusieurs et ensuite partager les « blocks rewards » selon la participation de chacun. Ils forment alors un pool.

Mais est-il vraiment intéressant pour un mineur de miner au sein d'un pool ?
Rosenfeld nous montre à partir d'un calcul simple ce que va apporter le pool au mineur seul en termes d'avantages.
En effet, si l'on considère que la puissance de hash de tous les mineurs est de H, alors le pool va trouver en moyenne $\frac{Ht}{2^{32}D}$ blocs sur une période t et le gain total sera de $\frac{HtB}{2^{32}D}$. Un mineur seul ayant une puissance de calcul h=qH avec q une fraction de la puissance totale du pool devrait recevoir une fraction q du « reward » c'est-à-dire $q\frac{HtB}{2^{32}D} = \frac{htB}{2^{32}D}$, ce qui est exactement égal à son revenu s'il minait seul. Cependant, la variance du gain d'un mineur est beaucoup plus faible que s'il minait seul. En effet, la variance du gain total du pool est de $\frac{HtB^2}{2^{32}D}$, donc la variance individuelle du mineur est de $q^2\frac{HtB^2}{2^{32}D} = q\frac{htB^2}{2^{32}D}$ soit une fraction q de la variance de gain du mineur seul.
Ainsi, rejoindre un pool va permettre au mineur de considérablement réduire la variance de ces revenus. D'autre part, plus le mineur est petit et plus le pool est large, plus le bénéfice potentiel pour le mineur est important.
En pratique, un pool est géré par un opérateur qui peut demander des frais pour ces services. Il s'agit d'un pourcentage fixé f de chaque « block reward ».
Les paiements sont calculés pour différents rounds correspondant au temps entre un bloc miné par le pool et le suivant. A la fin de chaque round, lorsqu'un bloc est miné, le pool reçoit un gain B et l'opérateur garde le gain fB et le reste (1-f) B est partagé entre les mineurs selon leur contribution à la puissance de hash. Si un mineur à soumis n « shares »[1] durant ce round pour un total de N « shares » soumis par le pool, son gain va s'élever à $\frac{n}{N}(1-f)B$. Mais, cette répartition qui est dite proportionnelle du gain n'est pas toujours celle qui est utilisé au sein des pools. En pratique, il existe différentes règles de répartitions des gains que l'on détaillera dans le paragraphe suivant.

1.2.2.2 Règles de répartition

On cherche dans cette partie à montrer les différentes de règles de répartition des gains au sein d'un pool pour ainsi montrer si des différences de modèle entre les pools peuvent entraîner des migrations de mineurs entre différents pools.

Une des méthodes simples assez utilisé est la méthode PPS (Pay-per-share) qui consiste à faire absorber par le pool toute la variance auquel un mineur fait face, c'est-à-dire, donner comme gain (1-f) pB au mineur à chaque fois que ce dernier soumet un « share » et cela indépendamment de la quantité de bloc qu'il a validé.
Le paiement par « share » possède une valeur déterminée à l'avance ce qui procure plusieurs avantages pour les mineurs :

- Pas de variance pour le revenu par « share » et une variance très faible pour le nombre de « shares » obtenues par le mineur par unité de temps.
- Pas d'attente qu'un bloc soit validé pour obtenir un paiement (ce qui est le cas pour la répartition proportionnel)
- La valeur du revenu est connue à l'avance.
- Pas de risques de tricherie de l'opérateur ou d'autres parties prenantes.

Cependant, comme le rappel Rosenfeld[33], pour compenser l'absorption de cette variance de gain, et les pertes pour des rounds longs avec un nombre de « shares » plus élevé que la moyenne,

[1] Un share est un hash assez petit pour qu'il puisse être à l'origine d'un bloc valide. Ainsi, chaque hash a une probabilité égale à $\frac{1}{2^{32}}$ d'être un share. Et un share à une probabilité égale à p=$\frac{1}{D}$ d'être un bloc valide. Le nombre de shares obtenu par un mineur est proportionnel au nombre de hashes calculé par le mineur afin de valider un bloc.

le pool va faire payer des frais plus élevés qu'avec la méthode proportionnelle ce qui constitue donc un désavantage pour le mineur.
De plus, certains mineurs malhonnêtes font du « pool-hopping », une pratique qui consiste à arrêter d'envoyer des « shares » à un même pool si le round est trop long car la rentabilité est assurée d'être faible. Cela affecte alors les mineurs honnêtes qui reçoivent alors un gain plus faible.
Ainsi, pour contrer le « pool-hopping » un nouveau modèle de répartition a été implémenté dans « slush's pool[34] » qui consiste à établir un score pour chaque mineur dépendant du nombre de « shares » qu'il a envoyé et du temps passé une fois le round commencé. Plus le round est entamé, plus le score est important. De plus, le revenu distribué à la fin de chaque round dépend du score de chaque mineur ce qui permet alors de contrecarrer la pratique du « pool-hopping ».

La fonction de scoring est de forme exponentielle tel que s=exp (T/C) avec s le score correspondant à un share envoyé au temps T et C une constante.

Toutefois, il existe une autre méthode exposée par Rosenfeld qui se nomme méthode géométrique[35] inspiré par la méthode « slush » qui consiste à proposer un revenu fixe et un revenu variable. La partie fixe est un montant constant extrait du block reward tandis que la partie variable comprend un score établit au début du round et qui peut varier tout comme la méthode « slush » énoncé précédemment. Cela permet de faire en sorte qu'il n'y ait aucun avantage de miner au début ou à la fin du round et limite donc le « pool-hopping ».

Une autre méthode comme la PPLNS (Pay-per-last-N-shares) n'utilise pas les rounds pour effectuer la rémunération des mineurs. Cette dernière consiste à distribuer les revenues du minage seulement aux participants ayant soumis des shares récemment. Cela représente un système stable, juste, transparent ainsi que « hopping-proof » (c'est-à-dire résistant aux pratiques de « pool-hopping »).

Enfin, il existe d'autres méthodes de répartitions de revenus moins communes comme la rémunération par contrats. Ce système correspond à l'achat de « shares » par l'opérateur du « pool » par l'intermédiaire d'un contrat en échange d'un paiement en une fois ou à des dates prédéterminées en fonction du nombre de blocs trouvées par le pool et des méthodes utilisés.
Ainsi, au lieu de procéder à un paiement par « share » fixé à l'avance du type (1-f)pB, le pool va se protéger des risques avec des valeurs de p et B actualisés au termes du minage et éliminer la pratique de « pool-hopping ».
Enfin, il faut savoir qu'un même pool peut offrir des types de contrats différents en fonction de la spécificité du mineur. Comme nous l'explique Rosenfeld, cela s'établit concrètement par le fait que mineur peut customiser[36] ses propres paramètres de paiement et même choisir un type de répartition hybride par exemple 30% en « PPS reward » et 70% en « PPLNS reward ».

Conclusion

L'arrivée du Bitcoin en 2009 a constitué un point de départ pour mettre fin au monopole des banques dans l'émission de monnaies. Il s'agit d'un modèle économiquement disruptant les modèles centralisés utilisés de nos jours. Le Bitcoin se base alors sur le mécanisme de Blockchain ainsi que sur la participation des « mineurs » pour assurer sa stabilité et sa pérennité. Ainsi, on a pu montrer que les « mineurs » étaient au cœur de ce système et que sans leur participation, il était impossible de maintenir la stabilité de la blockchain.

Pour garantir la participation des « mineurs », le protocole a introduit deux moyens de rémunération qui sont les « block rewards » ainsi que les « transaction fee ». Nous avons donc montré la nécessité de ce système de rémunération puis modéliser leur fonctionnement et le revenu de chaque mineur. Enfin, nous avons pu montrer quels étaient les incitations des mineurs de rejoindre des groupes appelés « pools ». Ainsi, ces derniers permettent de réduire la variance du revenu du mineur en échange de frais versé à l'opérateur du pool.

Enfin, on remarque alors que plusieurs facteurs influencent le mineur lorsqu'il s'agit de choisir un pool. Ces facteurs correspondent aux frais reversés au pool ainsi qu'aux règles de répartition des revenus du minage qui diffère selon les pools. Ainsi, les règles les plus simples consistent à partager de manière proportionnelle les revenus du minage en fonction de la participation du mineur au sein du pool tandis que d'autres utilisent des mécanismes plus complexes pour faire face à différents types de fraudes.

Références

[1] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating User Privacy in Bitcoin. In Proceedings of Financial Cryptography, 2013. (The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, page 1, 2013)

[2] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar. On Bitcoin and Red Balloons. In Proceedings of the 13th ACM Conference on Electronic Commerce, pages 56–73. ACM, 2012. (The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, page 1, 2013)

[3] Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore. Bitcoin: Economics, Technology, and Governance†, page 1, 2015.

[4] Dr Garrick Hileman & Michel Rauchs. Global Cryptocurrency Benchmarking Study, page 5, 2017.

[5] Dr Garrick Hileman & Michel Rauchs. Global Cryptocurrency Benchmarking Study, page 18, 2017.

[6] Dr Garrick Hileman & Michel Rauchs. Global Cryptocurrency Benchmarking Study, page 27, 2017

[7] Dr Garrick Hileman & Michel Rauchs. Global Cryptocurrency Benchmarking Study, page 20, 2017

[8] Dr Garrick Hileman & Michel Rauchs. Global Cryptocurrency Benchmarking Study, page 20, 2017

[9] B. Schoenmakers. Security aspects of the EcashTM payment system. State of the Art in Applied Cryptography, 1998. (SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, page 105, 2015)

[10] R. L. Rivest. Peppercoin micropayments. In Financial Cryptography, 2004 (SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, page 105, 2015)

[11] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. http: //bitcoin.org/bitcoin.pdf, 2008. (SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, page 105, 2015)

[12] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten. The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, page 3, 2013

[13] Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore. Bitcoin: Economics, Technology, and Governance†, page 4, 2015.

[14] Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore. Bitcoin: Economics, Technology, and Governance†, page 4, 2015.

[15] A. Back et al. Hashcash-a denial of service counter-measure. http://www. hashcash.org/papers/hashcash.pdf, 2002. (The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, page 5, 2013)

[16] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, page 107, 2015

[17] N. T. Courtois, M. Grajek, and R. Naik. Optimizing sha256 in bitcoin mining. In Cryptography and Security Systems, 2014. (SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, page 107, 2015)

[18] Dr Garrick Hileman & Michel Rauchs. Global Cryptocurrency Benchmarking Study, page 15, 2017.

[19] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten. The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, page 7, 2013

[20] B. Skyrms. The stag hunt and the evolution of social structure. Cambridge University Press, 2003. (The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, page 10, 2013)

[21] J. Becker, D. Breuker, T. Heide, J. Holler, H. Rauer, and R. B¨ohme. Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency. In Workshop on the Economics of Information Security, 2012. (The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, page 8, 2013)

[22] Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore. Bitcoin: Economics, Technology, and Governance†, page 10, 2015

[23] D. Schwartz, N. Youngs, and A. Britto. The Ripple Protocol Consensus Algorithm. https://ripple.com/consensus-whitepaper/, September 2014. (SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, page 108, 2015)

[24] Rainer B¨ohme. “Internet Protocol Adoption: Learning from Bitcoin”. In: IAB Workshop on Internet Technology Adoption and Transition (ITAT). Cambridge, UK, 2013. (Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees, page 3, 2014)
[25] Malte Möser and Rainer Böhme.Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees, page 12, 2014
[26] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten. The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, page 12, 2013
[27] Nicolas Houy. “The Economics of Bitcoin Transaction Fees”. Working Paper GATE 2014-07. 2014. (Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees, page 3, 2014)
[28] M. Sherif. The Psychology of Social Norms. New York: Harper, 1936. (Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees, page 3, 2014)
[29] Malte Möser and Rainer Böhme.Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees, page 8, 2014
[30] Malte Möser and Rainer Böhme.Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees, page 10, 2014
[31] Malte Möser and Rainer Böhme.Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees, page 12, 2014
[32] Meni Rosenfeld. Analysis of Bitcoin Pooled Mining Reward Systems, page 1, 2011
[33] Meni Rosenfeld. Analysis of Bitcoin Pooled Mining Reward Systems, page 6, 2011
[34] slush. Bitcoin pooled mining. http://mining.bitcoin.cz/. (Analysis of Bitcoin Pooled Mining Reward Systems, page 7, 2011)
[35] Meni Rosenfeld. Analysis of Bitcoin Pooled Mining Reward Systems, page 8, 2011
[36] Meni Rosenfeld. Analysis of Bitcoin Pooled Mining Reward Systems, page 27, 2011