RÉPONSES DE BITFARMS À LA DEMANDE DE RENSEIGNEMENTS N° 1 DE LA FCEI RELATIVE À LA DEMANDE DE FIXATION DES TARIFS ET DES CONDITIONS DE SERVICE POUR L'USAGE CRYPTOGRAPHIQUE APPLIQUÉ AUX CHAÎNES DE BLOCS

QUESTIONS ADRESSÉES À L'EXPERTE ÉLISABETH PRÉFONTAINE

Question 1 :

Références:

(i) C-Bitfarms-0013, p. 3
(ii) C-Bitfarms-0013, p. 10
(iii) C-Bitfarms-0013, p. 14
(iv) C-Bitfarms-0013, p. 16
(v) C-Bitfarms-0013, p. 3
(vi) C-Bitfarms-0013, p. 25

Préambule :

(i)
« Si l'on vise à identifier un sous-groupe de cryptomonnaie (celles qui sont énergivores), il faut savoir qu'elles ne présenteront des variations de consommation perceptibles que si leur réseau a du succès et reçoit des investissements massifs. Autrement dit, tenter de les isoler, créerait une tarification différente pour un même usage selon le niveau de succès du réseau de la cryptomonnaie en question. L'utilité de l'électricité dans le contexte d'un usage cryptographique appliqué aux chaînes de blocs doit d'abord être comprise. De plus, la définition de ce qu'est une chaîne de blocs, de son fonctionnement et des nuances qui existent est essentielle. Le manque de distinction entre les différents usages ou applications et le moment où la consommation énergétique devient élevée méritent d'être revisités.

Advenant des conditions de marchés défavorables, comme par exemple lorsque le prix du bitcoin est à la baisse et que le taux de hachage à la hausse, les entreprises qui ont accès à un tarif d'électricité non compétitif auront à éteindre de l'équipement informatique avant d'autres. Lorsque l'équipement est éteint, les revenus qui y sont associés cessent. Donc, un tarif non compétitif nuirait à la compétitivité des entreprises. »

(ii)
« Par ailleurs, comme le coût de l'énergie est la plus grande dépense des centres de calcul, les fournisseurs tels que les fabricants de puces ont tout intérêt à poursuivre leur R et D afin d'offrir de l'équipement toujours plus performant. Par exemple, au cours des 4.5 dernières années, le taux de hachage a augmenté de 300% annuellement. Mais au cours de la même période, l'efficacité des puces a augmenté en moyenne de 80% par année et le coût de la puce ($/TH/s) a diminué de 50% annuellement. Les centres de calcul ont intérêt à développer des procédés énergétiquement efficaces car l'impact de ces améliorations est directement lié à la profitabilité de leur entreprise.

L'évolution de l'équipement utilisé pour miner la devise bitcoin témoigne des progrès qui sont faits. Initialement, il était possible de miner avec des CPU (processeur standard d'ordinateur), puis avec des GPU (matériel informatique spécialisé disponible au détail). Il y a eu une brève période associée au FPGA après les GPU. Présentement ce sont les ASIC (Application-Specific Integration Circuit) qui sont utilisés. »

(iii)
« Le minage de bitcoins est l'une des rares industries où la rentabilité peut-être prédite avec précision lorsque toutes les variables économiques sont connues. Il y a donc peu de hasard puisque ces variables (prix du bitcoin, coût et efficacité de l'équipement et puissance de calcul) sont transparentes, accessibles et connues. »

(iv)
« Toutes les cryptomonnaies ne sont pas des clients dont la proposition est énergivore ou même fonctionnelle. Il est important de découpler le prix d'une cryptomonnaie en particulier du prix des cryptomonnaies dans leur ensemble. Le protocole Bitcoin a une dépense énergétique qui supporte la sécurité de son actif monétaire et a un schème de monétisation démontré. Cette phrase n'est pas applicable à l'ensemble des cryptomonnaies. »

(v)
« La première problématique est que la quantité élevée de MW demandés en électricité combinée à la manière simultanée dont ces demandes ont été présentées n'a pas tenu compte de la dynamique économique du minage de cryptomonnaie. Même si ces MW avaient été octroyés, il est peu probable qu'ils aient pu être déployés par les centres de calcul de cryptomonnaie de manière économiquement viable. De plus, même si ces MW avaient été octroyés, il est peu probable que l'équipement informatique nécessaire à ce déploiement énergétique ait été disponible. La dynamique économique et le défi de l'approvisionnement en équipements informatiques pointent vers une demande simultanée de différents clients et non pas vers la matérialisation du déploiement d'une telle demande énergétique. »

(vi)
« Donc même si on voulait isoler la preuve de travail, cela ne sera pas possible de manière équitable. Cela représenterait une forme de ségrégation à l'intérieur d'une catégorie mais aussi en fonction de la phase d'expansion du réseau. L'effet serait de favoriser financièrement les nouveaux réseaux (plus risqués) qui utilisent la preuve de travail (mais qui ne seraient pas détectables) et de pénaliser le succès des réseaux comme démontré par leur expansion. »

Questions :

1.1 Relativement à la référence (i), quel est présentement le revenu horaire marginal par kWh qui peut être généré par le minage de la cryptomonnaie Bitcoin en fonction des meilleurs équipements disponibles, du taux de hachage de la valeur du Bitcoin et, le cas échéant, des autres variables pertinents ? Voyez indiquer les hypothèses sous-jacentes à votre réponse.

Réponse :

Voir la réponse donnée à la question 2.1 à la demande de renseignements #1 du Distributeur.

1.2 Veuillez indiquer l'information équivalente pour les autres cryptomonnaies , quel est présentement le revenu horaire marginal par kWh qui peut être généré par le minage de la cryptomonnaie Bitcoin en fonction des meilleurs équipements disponibles, du taux de hachage de la valeur du Bitcoin et, le cas échéant, des autres variables pertinentes ? Voyez indiquer les hypothèses sous-jacentes à votre réponse.

Réponse :

Voir la réponse donnée à la question 2.1 à la demande de renseignements #1 du Distributeur.

1.3 Si possible, veuillez également fournir une évaluation du revenu marginal horaire moyen historique et prospectif pour ces cryptomonnaies.

Réponse :

La représentation historique de la profitabilité du minage de différentes cryptomonnaie (BTC, ETH, BCH, LTC, DASH, XMR, etc.) est répertoriée par au moins un site Internet[1] qui offre plusieurs indicateurs d'analyse technique (données brutes, moyennes mobiles, RSI, etc.) et différentes périodes d'analyse (3, 6, 12 mois, all time). Par contre, ce type de calcul ne représente pas une lecture complète puisque de nombreuses variables spécifiques à la gestion des entreprises individuelles sont inconnues. Voici la représentation graphique de la profitabilité historique du minage des deux plus grandes cryptomonnaies (en termes de capitalisation) au cours de la dernière année:

[1] https://bitinfocharts.com/comparison/bitcoin-mining_profitability.html#1y (19/10/18)

1.4 Relativement à la référence (ii) et considérant la vitesse d'évolution technologique, à quelle fréquence les équipements de calculs doivent-ils être remplacés en général pour optimiser la rentabilité des opérations?

Réponse :

Dans un mode théorique et sans contrainte (économique ou de disponibilité), l'équipement serait continuellement remplacé par la version la plus efficiente. Le coût de l'énergie est la plus grande dépense des centres de calcul. Plus l'équipement est efficace, moins il consomme de joules d'énergie et plus il est profitable d'opérer ces équipements.

Dans un mode pratique, le centre de calcul maximisera l'utilité de son équipement. Il peut décider de l'utiliser jusqu'à ce que celui-ci ne soit plus rentable. Il peut aussi vouloir vendre son équipement sur le marché secondaire (pendant qu'il est encore rentable) et redéployer le capital ainsi généré sur l'acquisition de nouveaux équipements plus performants. Cette question touche donc à la gestion d'entreprise et aux choix stratégiques que fait cette dernière.

Pour renouveler son matériel informatique, l'entreprise doit pouvoir soit réinvestir ses capitaux propres ou avoir la possibilité d'emprunter pour faire ses achats. Une entreprise qui ne réinvestit pas ou n'accumule pas de capital et qui compte exclusivement sur l'appréciation du prix de la cryptomonnaie pour renouveler son équipement de minage pourrait se retrouver dans une situation financière précaire advenant des conditions de marchés défavorables.

Notons que l'équipement de minage le plus performant n'est pas nécessairement disponible au moment et en quantité voulue. La planification du remplacement est un enjeu d'entreprise.

1.5 À votre connaissance, à quelle fréquence les entreprises de minage remplacent-elles leurs équipements de minage.

Réponse :

Je ne dispose pas de cette information, mais il est possible de faire les hypothèses suivantes :

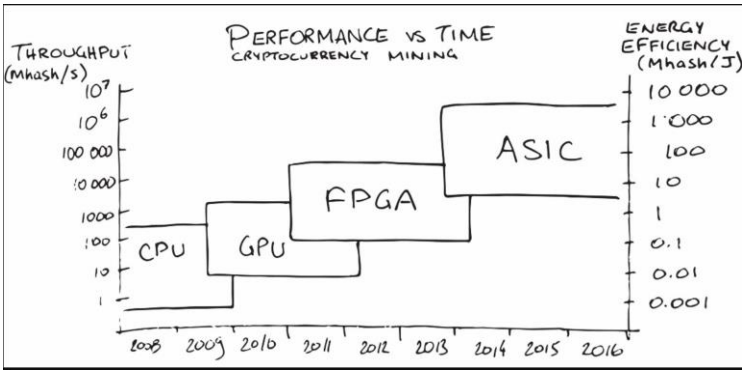
- Elles minent à 0$ de profit, mais pas à perte (mais pourraient décider de miner à perte).
- Elles visent à suivre le cycle d'évolution technologique.
- Le cycle de remplacement de l'équipement est lié à la progression du taux de hachage.
- Revoir la réponse à la question 1.4.

1.6 Si possible, veuillez présenter l'évolution de la performance des équipements de calcul dans le temps.

Réponse :

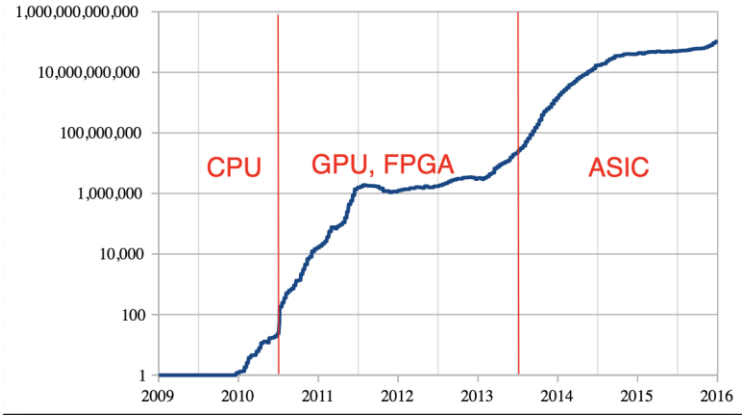
Bitcoin est le réseau ayant le plus long historique. Regarder son histoire permet de voir près de dix ans de progrès technologique dans la performance des puces informatiques. Remarquez dans les graphiques ci-dessous, les périodes de superpositions entre les changements de technologies, la progression de la difficulté de calcul (throughput) et l'augmentation de l'efficacité énergétique des machines. Il s'agit d'une évolution constante. De nouveaux équipements qui sont plus performants ont récemment été annoncés.

Visuel 1[2]



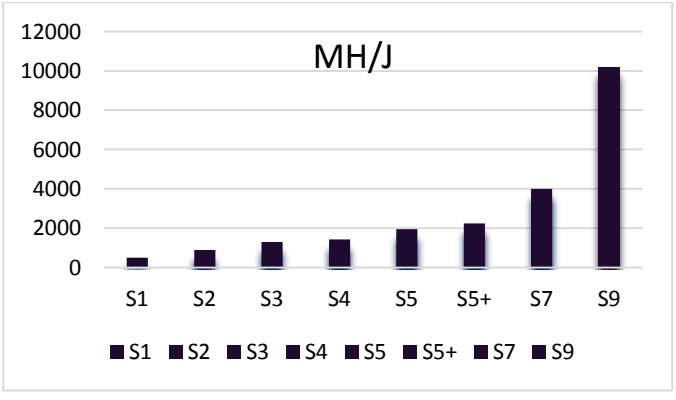
Visuel 2[3]

[2] https://en.bitcoinwiki.org/upload/en/images/c/c7/1%2AVcJKmqav8tcSRZLksc0jLA.jpeg (19/10/18)
[3]https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:History_of_Bitcoin_difficulty_and_mining_hardware.svg (19/10/18)



Voici un complément d'information qui vise à illustrer le progrès à l'ère ASIC en utilisant l'échantillon de machines de l'un des fournisseurs[4].

Modèle	Taux de hachage MH/s	Consommation MH/joules	Watts
Antminer S1	180 000	500	360
Antminer S2	1 000 000	900	1 100
Antminer S3	441 000	1 300	340
Antminer S4	2 000 000	1 429	1 400
Antminer S5	1 155 500	1 957	590
Antminer S5+	7 722 000	2 247	3 436
Antminer S7	4 860 000	4 000	1 210
Antminer S9	14 000 000	10 182	1 375



1.7 Relativement à la référence (iii), veuillez expliquer les liens entre les différents concepts suivants : le nombre de transactions, la valeur des transactions, le nombre de blocs, le niveau

[4] https://en.bitcoin.it/wiki/Mining_hardware_comparison (19/10/18)

de difficulté, le nombre de preuves de travail, la puissance de calcul requise, le nombre d'équipements de calcul en opération, la rémunération des calculs, la demande énergétique.

Réponse :

La réponse varie en fonction de la cryptomonnaie en question. J'utilise l'exemple du réseau Bitcoin car il s'agit de la première cryptomonnaie, mais aussi la plus pertinente dans le cadre du dossier R-4045-2018 puisqu'elle représente la plus grande consommation énergétique.

Block #546460 C

Summary		
Number Of Transactions	2708	A
Output Total	3,277.0526798 BTC	B
Estimated Transaction Volume	485.00968871 BTC	
Transaction Fees	0.07757484 BTC	F
Height	546460 (Main Chain)	
Timestamp	2018-10-19 19:46:49	
Received Time	2018-10-19 19:46:49	
Relayed By	AntPool	
Difficulty	7,182,852,313,938.32	D
Bits	388444093	
Size	1162.128 kB	
Weight	3992.322 kWU	
Version	0x20000000	
Nonce	2764308144	
Block Reward	12.5 BTC	F

- Nombre de transactions (A) : nombre de transactions individuelles qui sont regroupées dans un bloc. Dans l'exemple ci-dessous il y a eu 2 708 transactions dans le bloc.

- Valeur des transactions (B) : somme de la valeur monétaire des transactions qui sont regroupées dans un bloc. Cette valeur est exprimée en BTC.

- Le nombre de blocs (C) : il y a un nouveau bloc ajouté à la chaîne de bitcoin aux +/- dix minutes et ce depuis près de dix ans. Le dernier bloc à avoir été miné au moment d'écrire ces lignes est le # 546 460. Autrement dit, le 546 460e bloc de la chaîne de blocs de bitcoin.

- Le niveau de difficulté (D) : c'est une mesure qui indique à quel point un bloc est difficile à trouver. À chaque 2016 blocs, la difficulté de calcul est ajustée à la hausse ou à la baisse selon qu'il y a eu plus ou moins de puissance de calcul fournie au réseau. Ceci permet de remettre la vitesse des blocs à dix minutes. Le taux de hachage correspond au nombre de tentatives à la seconde pour résoudre le problème mathématique selon la difficulté de calcul. Relire au besoin la section 1.2 du document C-Bitfarms-0013.

- La puissance de calcul requise (E) : la puissance requise qui sera fournie par l'équipement informatique pour effectuer le calcul selon la difficulté actuelle du réseau. Voir les outils de calcul à la réponse 1.1 du présent document.

- La rémunération des calculs (F): la rémunération est composée de la récompense du bloc (actuellement de 12,5 BTC) et des frais de transactions qui composent le bloc.

Autres demandes :

- Le nombre de preuves de travail : il y a une preuve de travail à chaque bloc par équipement branché. Ce concept est essentiel. C'est la preuve que quiconque propose un nouveau bloc a travaillé pour le faire. C'est ce qui assure la sécurité informatique du réseau sans intermédiaire de confiance. Il n'y a pas de façon abordable de réécrire l'histoire.

- Le nombre d'équipement de calcul en opération : il n'est pas possible de le savoir avec certitude. C'est pourquoi un estimé en fonction des données disponibles sur l'équipement encore rentable est utilisé. Une fourchette est généralement présentée pour refléter l'écart entre les machines les plus et les moins performantes. Revoir l'annexe 2 du document C-Bitfarms-0013.

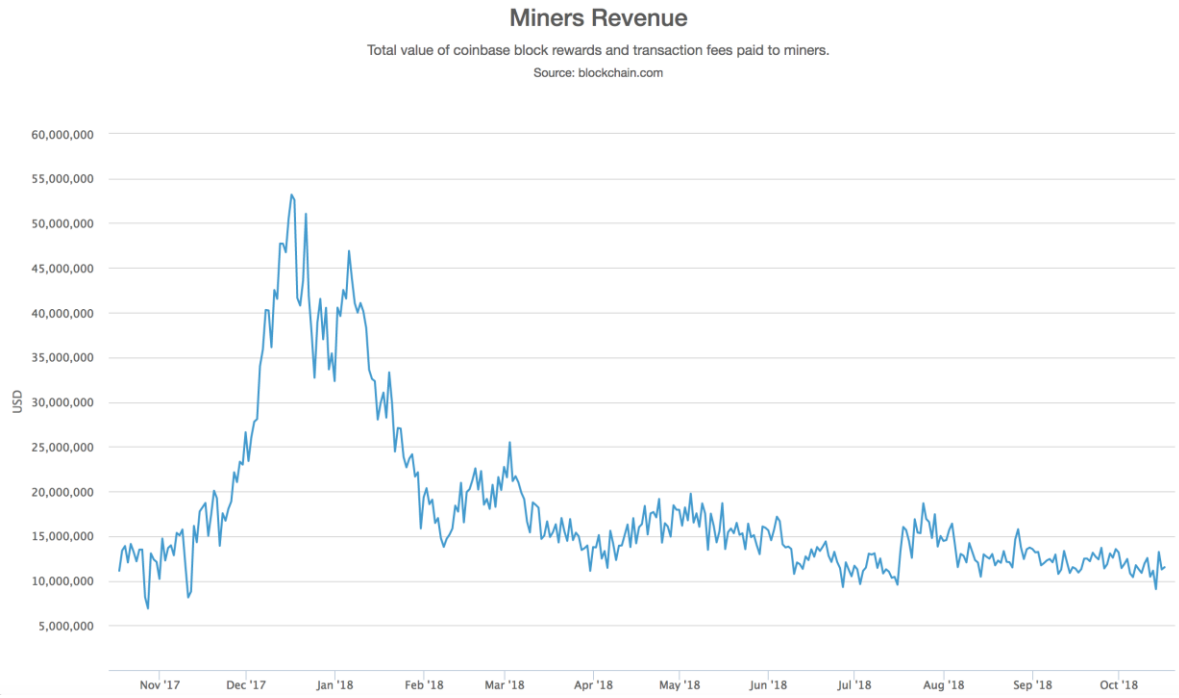
- La demande énergétique : plus une machine à miner est efficace d'un point de vue énergétique, plus elle est rentable car elle consomme moins d'énergie pour le même calcul. Revoir l'annexe 2 du document C-Bitfarms-0013.

1.8 Selon vous, quelle proportion des équipements actuellement en place mondialement cesseraient d'opérer si le revenu marginal horaire du minage du Bitcoin diminuait de 20%?

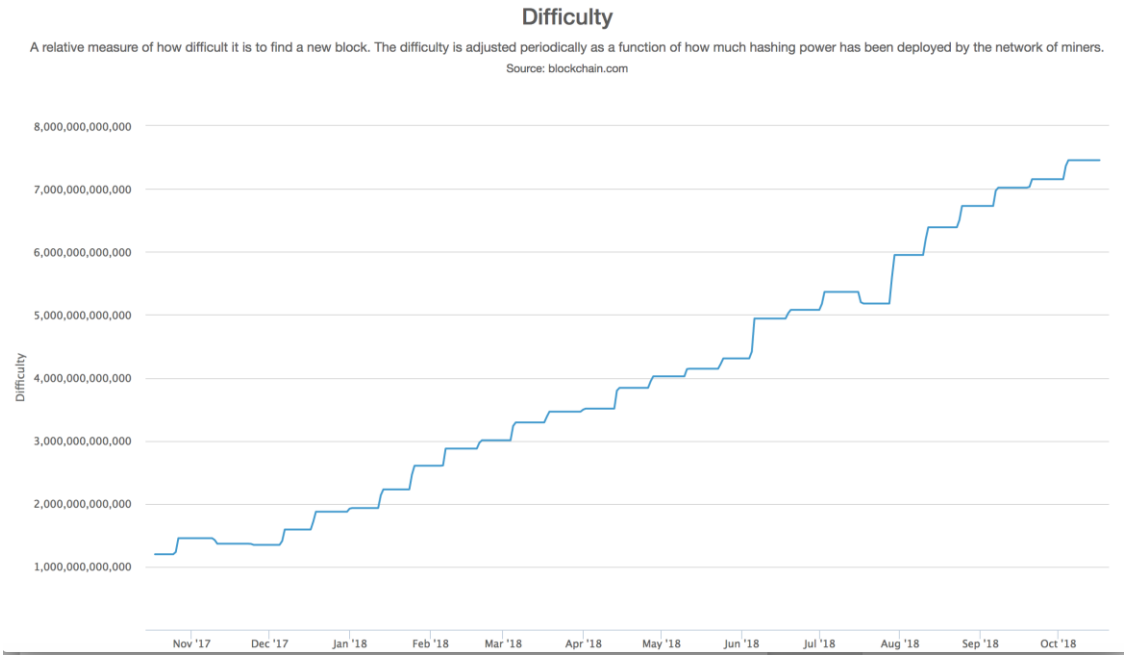
Réponse :

Je ne suis pas en mesure de répondre à cette question. Considérer uniquement la baisse du revenu marginal horaire est une donnée insuffisante. Il faut aussi estimer ce qui arriverait à la difficulté de calcul. Il faudrait émettre des hypothèses sur le nombre et le type de tous les équipements branchés mondialement sur le réseau ainsi que le tarif d'électricité (toutes sources confondues) auxquels les différents mineurs ont accès.

Puisque le contexte de marché est actuellement défavorable aux mineurs, il est possible d'utiliser l'historique récent pour répondre à la question soumise. Remarquez la baisse de revenus des mineurs[5] au cours de la dernière année. Remarquez pourtant, la hausse de la difficulté de calcul au cours de la même période. Ceci indique que, malgré la baisse de revenus, il y a de la puissance supplémentaire est a été fournie au réseau (c'est ce qui fait augmenter la difficulté de calcul). C'est un signal qui indique que les entrepreneurs continuent à investir malgré la baisse des revenus de leur activité.



[5] www.blockchain.com (19/10/18)



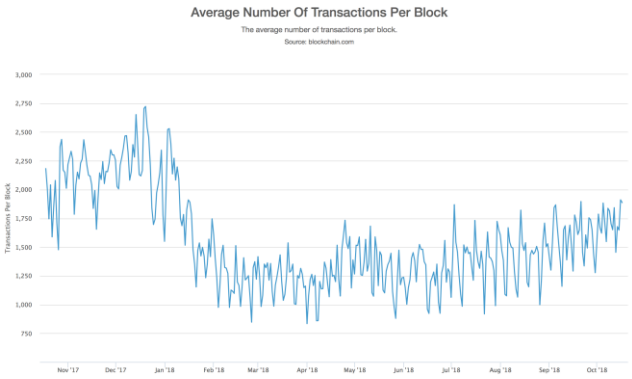
1.9 Quelle proportion des équipements actuellement en place devraient cesser d'opérer si le nombre de transactions diminuait de moitié?

Réponse :

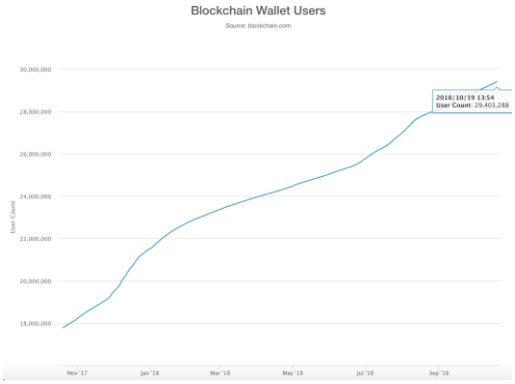
Je ne suis pas en mesure de répondre à cette question directement et ma réponse serait de nature spéculative. Je devrais notamment spéculer sur l'impact de la difficulté de calcul et pour y arriver, je devrais estimer quels équipements fournissent de la puissance de calcul au réseau et le tarif d'électricité (toutes sources confondues) en vigueur. Par contre, j'aimerais préciser que :

- Les frais de transactions sont actuellement faibles comparativement à la récompense d'un bloc. Prenons l'exemple de la question 1.7, la récompense est de 12,5 BTC alors que les frais de transactions de ce bloc sont de 0,07757484 BTC. Ces frais sont variables. Plus il y a de transactions, plus les frais peuvent augmenter car il y a une taille maximale à un bloc. Dans cet exemple, les frais représentent 0.62% de la rémunération totale du bloc.

- Le nombre de transactions a diminué de moitié au cours de la dernière année. L'augmentation de la difficulté de calcul démontre qu'il n'y a pas eu de retrait net d'équipements mais au contraire plus de puissance de calcul a été apportée au réseau.



- Le nombre d'utilisateurs de Wallet Blockchain montre une progression haussière soutenue.



1.10 Veuillez commenter sur l'intérêt relatif des mineurs envers des tarifs d'électricité essentiellement fixe (coût de puissance représente une part importante de la facture) ou essentiellement variable (coût de l'énergie représente une part importante de la facture).

Réponse :

Je ne suis pas une experte en électricité et je ne peux donner une réponse applicable à l'ensemble d'une industrie composée d'entreprises différenciées.

1.11 Relativement à la référence (iv), à votre avis, les clients qui ont présenté des demandes de puissance sont-ils susceptibles de viser des cryptomonnaies non énergivores et si oui pourquoi alors avoir demandé cette puissance. Suggérez-vous que des clients demandent de la puissance dont ils n'ont pas besoin où qu'ils n'ont pas l'intention de s'en servir pour une raison ou pour une autre?

Réponse :

Je pense que les demandes qui ont été formulées au Distributeur sont des demandes pour des cryptomonnaies énergivores et que celles-ci ont été présentées de manières simultanées un peu

comme un « gold rush ». Je pense également qu'il peut y avoir des doublons dans les demandes formulées, qu'une certaine partie des demandes peut venir d'un déplacement d'installations actuellement déployées ailleurs dans le monde et qu'une autre partie représente de la nouvelle puissance que l'on veut brancher aux réseaux qui reposent sur la preuve de travail.

Il est possible que certains spéculateurs aient voulu profiter du « gold rush » sans être directement impliqués dans l'activité de minage de cryptomonnaie. Il est possible que certaines demandes d'électricité aient été formulées avec un objectif de revente.

Je ne crois pas que les demandes de puissance ont visé des cryptomonnaies non-énergivores. Par contre, la définition de la catégorie proposée par le Distributeur les englobe. Les cryptomonnaies dites non-énergivores consomment quand même de l'électricité mais sont basées sur une méthode de consensus différente et elles sont à différentes étapes de développement. Certaines n'ont pas de chaînes de blocs et sont encore à l'étape de la conception. D'autres ont lancé leur chaîne et sont à bâtir leur courbe d'adoption, à démontrer leur viabilité commerciale, leurs cas d'utilisations et leur proposition à valeur ajoutée. Ceci dit, le niveau de sécurité offert par ces autres chaînes est différent. Pour simplifier, par exemple, le besoin de sécurité et de décentralisation pour une monnaie n'est pas comparable à celui d'un jeton de fidélité.

J'aimerais rappeler que la dépense énergétique n'est pas un défaut, mais bien une propriété et que celle-ci assure, en résumé, la sécurité et l'immuabilité du réseau en question. Cette notion est essentielle. La preuve de travail est la seule solution actuellement trouvée et applicable à grande échelle pour répondre au problème ouvert en sciences informatiques de la double dépense (appelé problème des généraux byzantins). Au besoin, je vous invite à consulter le document de travail[6] publié par la Banque du Canada en juillet 2018 qui traite de la preuve de travail et trace des certaines conclusions relativement aux autres méthodes de consensus.

1.12 Relativement à la référence (v), à votre avis, quel est le potentiel de croissance totale de la demande énergétique (énergie et puissance) au Québec si le Distributeur avait accepté les demandes de tous les clients s'étant manifestés en fonction des conditions tarifaires existantes?

Réponse :

Si la question demande le taux d'absorption du déploiement énergétique en fonction de la dynamique économique du réseau, je n'ai pas les ressources pour formuler une réponse adéquate à une question de cette ampleur. Des paramètres et des hypothèses de recherche devraient également être préalablement établis afin de circonscrire l'analyse de sensibilité demandée. Dans une telle éventualité, une hypothèse qui risque d'être difficile à formuler, voire impossible mais qui pourtant, est importante dans ce type d'analyse est le tarif d'électricité (peu importe la source) auquel ont accès les autres membres branchés sur le réseau mondialement.

[6] https://www.bankofcanada.ca/2018/07/staff-working-paper-2018-34/ (19/20/18)

1.13 Relativement à la référence (vi), dans la mesure où les nouveaux réseaux seraient de petite envergure et donc impliqueraient une consommation faible, veuillez expliquer en quoi ils seraient risqués du point de vue du Distributeur.

Réponse :

J'aimerais d'abord préciser que cette réponse traite des nouveaux réseaux qui utiliseraient la preuve de travail. S'agit d'un lancement à partir de zéro, la consommation énergétique serait faible initialement et non perceptible mais augmenterait en fonction du succès. S'il s'agit d'un hard fork, cela va dépendre de la migration de la puissance de calcul vers le réseau « forké ». La valeur de la cryptomonnaie est attribuée spontanément par le marché. L'annexe 5 du document C-Bitfarms-0013 traite des facteurs qui font en sorte que Bitcoin est possiblement un phénomène unique et pourquoi il sera difficile de reproduire l'alignement des facteurs ayant permis son émergence.

Rappelons qu'initialement, il était possible de miner des bitcoins avec un ordinateur personnel et que la consommation du réseau était essentiellement imperceptible. Par contre, plus il y a de mineurs qui se branchent au réseau, plus la puissance de calcul nécessaire pour répondre à l'augmentation de la difficulté de calcul augmente. Donc un réseau (basé sur la preuve de travail) qui a du succès, a un taux de hachage à la hausse. Je vous invite à revoir au besoin les sections sur la preuve de travail et sur la dynamique économique présentées dans le document C-Bitfarms-0013.

Ceci dit, Bitcoin est un logiciel à l'architecture ouverte. Il est possible de copier le code et de lancer un nouveau réseau via un hard fork ou un airdrop.

Ces autres cryptomonnaies, qui s'inspirent de l'architecture de bitcoin, peuvent être plus risquées pour différentes raisons. Les principaux risques sont : la reconnaissance de la valeur par le marché (pérennité), une attaque 51% et le risque règlementaire potentiel.

- La pérennité d'un nouveau réseau repose sur la valeur qui lui est attribuée de manière spontanée par le marché. Est-ce que la proposition à valeur ajoutée, l'élément de différenciation ou le cas d'utilisation proposé est suffisamment intéressant pour diriger ou rediriger des ressources vers ce réseau ? Il est possible que le nouveau réseau ne soit pas supporté et donc sa viabilité à long terme serait questionnable.

- Le risque d'attaque 51% : il s'agit d'un type d'attaque contre une cryptomonnaie qui implique d'avoir le contrôle sur une majorité de la puissance de calcul pour pouvoir dépenser deux fois la même unité de cryptomonnaie. Quoi que ces attaques soient relativement rares, elles ciblent généralement des cryptomonnaies dont la capitalisation est plus faible. Plus le taux de hachage est faible, plus il est économiquement accessible de commettre ces attaques.

- Le risque règlementaire : Bitcoin n'a pas requis de capital pour être développé, ni pour être lancé. Il a été fonctionnel dès le premier jour et s'est développé organiquement sans

budget marketing ou efforts de vente. Le lancement d'un autre réseau, et ce peu importe la nouvelle proposition à valeur ajoutée, serait fort probablement planifié top down par une équipe et risquerait d'être classé à titre de valeurs mobilières. Ceci aurait possiblement des implications réglementaires auxquels devraient faire face l'équipe de lancement. La *Securities Exchange Commission*[7] a levé le doute sur la catégorisation du bitcoin (BTC) et d'ether (ETH) en spécifiant qu'elles ne sont pas des valeurs mobilières.

Ces raisons expliquent pourquoi ces réseaux sont plus risqués. Ils ne représentent qu'une petite portion par rapport à Bitcoin. Ceci dit, le choix de miner une cryptomonnaie ou une autre est une décision d'entreprise. Un centre de calcul ayant accès à une certaine quantité d'électricité peut décider de déployer sa capacité pour miner ce qu'elle veut, à supposer qu'elle a accès aux équipements informatiques requis. Le point à retenir ici est que différentes cryptomonnaies utilisent la preuve de travail. Qu'au début de la vie d'un réseau donné, la consommation est parfois faible (imperceptible) et que celle-ci augmente avec le succès dudit réseau. Plus on ajoute d'équipements au réseau, moins celui-ci est risqué. Tenter d'isoler la preuve de travail serait ardue et créerait des distorsions de prix en fonction du niveau de maturité et du succès commercial d'un réseau donné.

1.14 Veuillez confirmer la compréhension de la FCEI que les chaînes de bloc privées ne sont pas susceptibles d'être de grandes consommatrices d'énergie.

Réponse :

La réponse courte est oui. À supposer que ladite chaîne privée n'utilise pas la preuve de travail comme méthode de consensus, alors elle ne serait pas une grande consommatrice d'énergie.

Par contre, s'agit-il vraiment d'une chaîne de blocs ou plutôt d'une base de données? Ces chaînes privées ou à permissions sont mieux classifiées dans la catégorie des technologies de registres distribués (DLT).

Une base de données traditionnelle centralisée a besoin d'être écrite une seule fois, de vérifier les données une seule fois et de transmettre les données pour le stockage une seule fois. La chaîne de blocs doit être écrite des milliers de fois, vérifier les données des milliers de fois et transmettre les données des milliers de fois.

La principale distinction entre une chaîne de blocs et une base de données traditionnelle, est qu'il y a des règles spécifiques sur comment ajouter des données dans la base de données. La donnée :

- ne peut pas entrer en conflit avec d'autres données déjà présentes.
- peut seulement être ajoutée (immuable).
- est verrouillée par son propriétaire.
- est décentralisée, tous s'entendent sur l'état de la base de données sans autorité de contrôle.

[7] https://www.sec.gov/news/speech/speech-hinman-061418 (20/10/18)

Cette décentralisation est d'importance capitale car c'est elle qui fait en sorte qu'il n'y a pas de point central de défaillance et qu'aucune personne n'a le pouvoir de retirer de l'information ou de modifier l'historique. C'est cette propriété d'immuabilité qui attire l'attention sur les projets chaîne de blocs. Enlever la décentralisation et l'on obtient une base de données conventionnelle (centralisée) mais qui est possiblement plus lente et dispendieuse à opérer. La cohérence et la fiabilité des données peuvent être atteintes à moindre coût et beaucoup plus rapidement en utilisant des vérifications, des reçus et des sauvegardes. De plus, cette méthode traditionnelle peut avoir du ''down time'' pour la maintenance. Ce n'est pas le cas d'un système ouvert. C'est un peu le même concept selon lequel l'Internet ne ferme pas.

Pour que les données soient maintenues sans organe central de contrôle et sans qu'il n'y ait d'abus ou de corruption, il doit y avoir un incitatif à en préserver l'intégrité. Les données sont conservées par des milliers d'ordinateurs (nœuds) en même temps et il y a un consensus autour de la vraie version de l'histoire et un incitatif financier est nécessaire non seulement au début mais tout au long de la vie de la chaîne. Cet incitatif n'est pas orchestré ou imposé par un organe central de contrôle. Il est spontané, volontaire et adopté par consensus. L'incitatif (la récompense) doit être interne au protocole. Dit simplement, l'incitatif des validateurs à préserver l'intégrité d'un réseau comme celui de Bitcoin est que la récompense est exprimée en bitcoins. Une chaîne privée n'a pas ces caractéristiques et qualités de devise native au protocole. C'est-à-dire un incitatif financier offert aux validateurs puisque la validation est basée sur des permissions.

Le mot blockchain (chaîne de blocs) a attiré l'attention car plusieurs d'industries accusent un retard dans la mise à niveau de leur infrastructure informatique et beaucoup d'espoir y est fondé. La chaîne de blocs sera véritablement utile pour répondre à un besoin de décentralisation. C'est-à-dire pour retirer la tierce partie qui agit à titre d'intermédiaire de confiance. La simple organisation de la structure de données que propose une chaîne privée, sans l'utilisation de la preuve de travail (dépense énergétique) ou système de validation ouvert n'offre pas les bénéfices de décentralisation.

Les chaînes publiques, entre autres comme celles de Bitcoin et de Ethereum ne sont pas en compétition avec les chaînes dites privées. Elles poursuivent des objectifs complètement différents et ont peu de choses en commun.

QUESTIONS ADRESSÉES À BITFARMS

Question 2 :

Référence:

(i) C-Bitfarms-0014, p. 4

Préambule :

« Bitfarms estime la consommation mondiale pour la cryptomonnaie Bitcoin en date de mars 2018 à environ 4 000 MW. »

Questions :

1.1 Veuillez expliquer comment Bitfarms en arrive à cette estimation de 4 000 MW.

Réponse :

Bitfarms a effectué une estimation du nombre de MW utilisés par le réseau bitcoin en se basant sur la consommation énergétique des équipements les plus performants et les moins performants au moment du calcul. Le 4 000 MW correspond à la moyenne des deux extrêmes.

1.2 Veuillez indiquer si cette consommation correspond à l'opération simultanée de tous les équipements de calculs et si cela prévoit une utilisation totale ou partielle des équipements en place.

Réponse :

Oui. Le 4 000 MW prévoit une utilisation totale des équipements en place.

1.3 À la connaissance de Bitfarms, quel est approximativement le taux d'utilisation moyen (pourcentage des heures en opération) des équipements de calculs installés présentement dans le monde.

Réponse :

Les équipements installés dans les centres de calculs de Bitfarms fonctionnent 24 heures sur 24, tous les jours. Bitfarms estime qu'il en ait de même dans tous les centres de calculs. Toutefois, selon des informations publiques, plusieurs joueurs, notamment asiatiques, de ce secteur émergent possèdent des conteneurs équipés de ASIC en attente d'être branchés sur un réseau.