

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

**RAPPORT D'ANALYSE PRÉSENTÉ À LA RÉGIE DE L'ÉNERGIE PRÉPARÉ POUR BITFARMS PAR
MME ELISABETH PRÉFONTAINE DE LA FIRME OCTONOMICS**

1. Référence(s) : (i) Pièce C-Bitfarms-0013, pages 25 et 26

Préambule :

- (i) « Les définitions proposées sont problématiques, car des nuances essentielles sont présentes à l'intérieur de la catégorie de clients proposés. L'hypothèse selon laquelle tous les clients de la catégorie sont énergivores est incorrecte. La facturation séparée et les outils de surveillance ne pourront être implantés comme envisagé.

Même s'ils l'étaient, ils créeraient des injustices basées sur l'utilisation et les applications. Rappelons que les technologies utilisées ne sont pas nouvelles, que la nouveauté réside dans l'assemblage qui en est fait.

Imaginez un centre de données qui fait de la R et D sur un usage cryptographique appliqué à la chaîne de blocs et qui n'utilise pas la preuve de travail. Son profil de consommation énergétique ne sera pas identifié. Pourquoi accepterait-il volontairement de payer un tarif supérieur à celui auquel il a accès dans le cours normal de ses activités?

Par ailleurs, un centre de données peut héberger un centre de calcul. Veuillez consulter l'annexe 6 qui traite de la convergence entre les centres de données et les centres de calcul.

Pour sa part, le centre de calcul est le consommateur énergivore qui génère un actif monétaire. C'est ce type de client qui a un schème de revenu confirmé lui permettant de s'acquitter de sa facture d'électricité et qui peut réinvestir une partie de ses bénéfices en R et D. Un tarif non compétitif aura l'effet de diminuer sa compétitivité, de dissuader l'établissement local de ces entreprises (vente d'électricité, impôts corporatif et foncier, création d'emploi) et d'étouffer le réinvestissement local en R et D (effet multiplicateur pour le développement économique du Québec). »

Demande(s) :

- 1.1. Veuillez proposer des définitions des termes « usage cryptographique » et « chaîne de blocs » qui répondent aux préoccupations exprimées dans votre rapport. Veuillez proposer d'autres définitions si vous l'estimez approprié.

Réponse :

Proposer une définition qui englobe « usage cryptographique » et « chaîne de blocs » dans le contexte d'une catégorie de clients énergétiques est difficile, voire impossible. Voici quelques raisons qui expliquent cette difficulté :

- Tenter de définir le terme chaîne de blocs est hasardeux, car trop large et ce, peu importe le contexte (énergétique, réglementaire, commercial, etc.). Pour être utile, la définition devrait être simple et générale, mais les nuances l'empêchent.

À sa plus simple définition, « *a blockchain is a chain of blocks* ». D'un point de vue technique, une chaîne de blocs est une liste de blocs qui sont liés les uns aux autres et un bloc est une liste de transactions ordonnées. C'est une structure de données. L'expression chaîne de blocs confond les termes suivants: chaînes publiques, privées, à permissions et technologies de registres distribués.

L'université de Cambridge a tenté de répondre au problème des définitions avec la publication d'un rapport de 97 pages en août 2018.

Précisons par ailleurs, que le White Paper à l'origine de Bitcoin n'utilise pas le mot Blockchain.

« The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. »

Satoshi Nakamoto, 31 octobre 2008

Il s'agit d'une industrie qui est en constante évolution et une catégorie englobante ne saurait définir de manière inclusive, simple et stable à travers le temps l'ensemble des clients autour de caractéristiques communes. Par exemple, le système de validation qui est utilisé est une différence fondamentale entre les différents projets et propositions. Des systèmes de validation comme la preuve de travail (proof-of-work), la preuve d'enjeu, la preuve d'enjeu délégué, permissions d'un consortium, etc. n'ont pas le même profil de consommation énergétique, n'offrent pas le même niveau de sécurité, visent des propositions commerciales différentes et leur déploiement diffère.

- L'usage cryptographique s'applique à autre chose que la cryptomonnaie et tenter de le circonscrire pourrait avoir des impacts sur d'autres types de clients qui ne sont pas liés à la cryptomonnaie ou aux chaînes de blocs.

La cryptographie sert à protéger des messages en les rendant inintelligibles sauf pour le destinataire et assurer ainsi l'authenticité de ceux-ci. Il s'agit d'une discipline qui n'est pas nouvelle et qui évolue à travers le temps en fonction des avancées en sciences informatiques et mathématique.

Une fonction de hachage calcule une empreinte à partir d'une donnée fournie et cette empreinte sert à identifier rapidement, même si incomplète, la donnée initiale. Une fonction de hachage est, entre autres, utile pour la cryptomonnaie, mais aussi pour gérer des structures de données et pour lutter contre la contrefaçon. Un exemple de fonction de hachage cryptographique reconnu et largement utilisé sur Internet en général est SHA-256. Par exemple, les sites transactionnels (banques, commerces, gouvernements, autres) sont sécurisés par la cryptographie. Par conséquent, cibler l'usage cryptographique a des répercussions bien plus larges que la cryptomonnaie et chaîne de blocs puisque cela touche entre autres, à l'Internet.

- Le contenu d'un bloc peut varier

Un bloc, c'est de l'espace d'information. Prévoir à l'avance l'ensemble de ce que cet espace contiendra ou pourrait contenir est hors de ma portée. Par contre, avec le temps, d'autres cas d'utilisations pourraient être développés. Au besoin, veuillez vous référer aux sections 3 et 4 de la pièce C-Bitfarms-0013.

Par conséquent, proposer des définitions (usage cryptographique et chaîne de blocs) pour englober les clients en fonction de leur usage n'est pas simple, peut avoir des répercussions sur d'autres types de clients et n'est possiblement pas stable dans le temps puisqu'il s'agit d'une industrie en constante évolution. Ce qui pourrait simplifier la catégorisation des clients est de les considérer en fonction de leur consommation au même titre, par exemple, qu'un centre de données et non en fonction de leur usage. L'analogie est fortement simplifiée, mais un centre donné n'a pas une tarification énergétique en fonction du type d'hébergement de clients qu'il dessert. La tarification énergétique est la même si le centre entrepasse des données de Facebook, d'une institution financière, d'un gouvernement ou d'un jeu en ligne.

- 2. Référence(s) :**
- (i) Pièce C-Bitfarms-0013, page 56
 - (ii) Pièce C-Bitfarms-0013, page 49
 - (iii) Rapport de la firme KPMG, pièce B-0008, page 9.

Préambule :

- (i) « • *«Au début 2018, pour une installation au Québec, les experts estimaient que le seuil de rentabilité correspondait à un prix de bitcoin se situant entre 3 000 et 4 000\$ pour un opérateur existant.» (note omise)*

Il aurait été intéressant d'obtenir les sources et les hypothèses utilisées (efficacité des machines et taux de hachage en vigueur lors de cette estimation). Le taux de hachage est ajusté à chaque 2016 blocs et par conséquent le seuil de rentabilité également. »

- (ii) «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. La donnée manquante actuellement est le prix de l'électricité. »

Demande(s) :

- 2.1. Quel est le seuil de rentabilité, exprimé en valeur du cours du Bitcoin (\$), d'une entreprise située au Québec menant des activités de minage de cette cryptomonnaie, selon que le tarif d'électricité applicable est :
- a. le tarif M ;
 - b. le tarif LG ;
 - c. le tarif LG dont la composante en énergie est majorée de 1 cent/kWh ;
 - d. le tarif LG dont la composante en énergie est majorée de 2 cents/kWh ;
 - e. le tarif LG dont la composante en énergie est majorée de 3 cents/kWh ;
 - f. le tarif LG dont la composante en énergie est majorée de 4 cents/kWh ;
 - g. le tarif LG dont la composante en énergie est majorée de 5 cents/kWh.

Veuillez fournir l'information demandée à la fois pour un opérateur existant et pour un nouvel opérateur.

Réponse :

La réponse à la question nécessite l'intégration de plusieurs facteurs et ceux-ci varient dans le temps et varient d'une entreprise à l'autre. D'un point de vue théorique, il est possible d'écrire la formule du seuil de rentabilité, mais dans la pratique, les spécificités propres à chaque entreprise feront varier le résultat. La vision, le positionnement stratégique, les contrats de services, les décisions de gestion et les différentes politiques internes liées à la gestion de l'entreprise auront une incidence sur le calcul.

Par conséquent, il y a trop de variables inconnues pour répondre au seuil de rentabilité d'une industrie composée de plusieurs entreprises gérées de manière différente. Je n'ai pas d'autre exemple (provenant d'autre industrie) sur lesquels me reposer pour tracer un parallèle où la rentabilité est calculée en lien avec la tarification énergétique.

Le seuil de rentabilité d'une entreprise ne semble pas être une donnée pertinente pour l'établissement d'un tarif énergétique. Par exemple, un centre de données, une mine d'or ou un restaurant n'ont pas une tarification basée en fonction de leur rentabilité.

De plus, le calcul de profitabilité varie dans le temps. Par exemple, comme le taux de hachage est ajusté à chaque 2016 blocs, même si l'on gardait toutes les autres variables fixes, le calcul de profitabilité varierait quand même toutes les deux semaines (2016 blocs de +/- dix minutes).

Voici un sommaire des éléments qui devraient être considérés pour effectuer le calcul.

Informations générales :

- Taux de hachage, difficulté du réseau Bitcoin¹.
- Prix de bitcoin en USD² : Il est recommandé d'utiliser la moyenne de plusieurs sources car le prix peut varier d'une source à l'autre.
- Prix de l'électricité en USD : le tarif M, LG, LG + 1, 2, 3, 4, 5 cents/kW/h.
- La courbe d'émission du bitcoin : la récompense actuelle est de 12,5 bitcoins par bloc. Cette récompense est divisée par deux à chaque 210 000 blocs. Le prochain "halving" est programmé pour le 21 mai 2020 à 21:01:39³.
- Taux de hachage et consommation en watt d'un équipement de minage donné.

À l'aide de ces données, il est possible d'utiliser un calculateur⁴ pour estimer la profitabilité et faire des projections quotidiennes, hebdomadaires, mensuelles ou annuelles. Par contre, plus ces projections sont éloignées dans le temps, plus leurs hypothèses sont instables car le taux de hachage, le prix de bitcoin, le progrès et la disponibilité de l'équipement informatique sont variables.

Informations spécifiques :

Au sujet de l'équipement utilisé :

- Quel type d'équipement est utilisé? Plusieurs machines sont disponibles et ont un taux de hachage et une consommation énergétique différente.
- Quel est le coût de l'équipement?
- Est-ce que l'équipement est financé et si oui, à quelles conditions?
- L'équipement utilisé dans la formulation de l'hypothèse est-il disponible et en quantité?

Au sujet de la récompense de chaque bloc :

- Quel est le volume de transactions et les frais associés dans chaque bloc?

¹ <https://www.blockchain.com/en/charts/hash-rate> et <https://www.bitcoinblockhalf.com/> (18/10/18)

² Des échanges tels que Coinbase et Kraken, ou des services tels que TradingView sont des exemples de sources.

³ <https://www.bitcoinblockhalf.com/> (18/10/18).

⁴ [https://www.cryptocompare.com/mining/calculator/btc?HashingPower=51141213&HashingUnit=TH%2Fs&PowerConsumption=107250000&CostPerkWh=0.03&MiningPoolFee=1\(18/10/18\)](https://www.cryptocompare.com/mining/calculator/btc?HashingPower=51141213&HashingUnit=TH%2Fs&PowerConsumption=107250000&CostPerkWh=0.03&MiningPoolFee=1(18/10/18)). D'autres calculateurs sont disponibles.

- Est-ce que l'entreprise s'est jointe à un pool de mineurs, et si oui quel en est le frais?

Au sujet des autres dépenses entourant l'activité :

- Quelles sont les taxes foncières?
- Quel est le coût des assurances?
- Est-ce qu'il y a un financement sur l'immeuble ou l'installation qui héberge l'équipement?
- Quel est le coût de refroidissement (s'il y a lieu)?
- Est-ce qu'il y a des frais de raccordement?

Au sujet de la gestion de l'entreprise

- Est-ce que l'entreprise développe son propre équipement?
- Quelle est la politique de réinvestissement pour le renouvellement du parc informatique?
- Quelle est la masse salariale à supporter?

Les entrepreneurs qui exercent dans ce domaine d'activité ont toutes les données à l'interne pour faire leur calcul de rentabilité avec précision. Ils ne connaissent toutefois pas les conditions particulières de leurs concurrents qui sont branchés sur le même réseau qu'eux, mais qui sont établis ailleurs dans le monde. Deux entreprises dans le même domaine peuvent avoir des performances financières complètement différentes.

2.2. Veuillez présenter et expliquer toutes les hypothèses utilisées pour la réponse à la question 2.1, notamment le taux de hachage.

Voir la réponse donnée à la question 2.1.

2.3. La durée de l'abonnement au service d'électricité est-elle considérée par les entreprises dans leur décision de démarrer ou maintenir des activités de minage de la cryptomonnaie Bitcoin ? Veuillez élaborer.

Réponse :

Oui. Il s'agit d'une décision d'entreprise individuelle qui comprend plusieurs éléments sur lesquels ses dirigeants doivent se prononcer.

2.4. Existe-t-il une durée minimale pour l'atteinte de la rentabilité des entreprises souhaitant démarrer ou maintenir des activités de minage de la cryptomonnaie Bitcoin en deçà de laquelle ces entreprises ne seraient pas intéressées à démarrer ou maintenir des activités ? Veuillez élaborer.

Réponse :

Voir la réponse fournie à la question 2.1.