

CANADA

PROVINCE DE QUÉBEC
DISTRICT DE MONTRÉAL

DOSSIER R-4045-2018

ÉTAPE 2 (Éventuelle nouvelle catégorie de consommateurs, bloc dédié, éléments du processus de sélection, tarif dissuasif)

RÉGIE DE L'ÉNERGIE

TARIFS ET CONDITIONS DE SERVICE
D'HYDRO-QUÉBEC DISTRIBUTION (HQD)
POUR L'USAGE CRYPTOGRAPHIQUE
APPLIQUÉ AUX CHAÎNES DE BLOCS

HYDRO-QUÉBEC
En sa qualité de Distributeur

Demanderesse

-et-

LE REGROUPEMENT CREE,
constitué de :

LA PREMIÈRE NATION CRIE DE
WASWANIPi et
LA CORPORATION DE DÉVELOPPEMENT
TAWICH, une entité entièrement propriété de
la Première Nation Crie de Wemindji par une
société de gestion

Intervenantes

RÉPONSE À LA DEMANDE DE RENSEIGNEMENTS NO. 1, [C-FCEI-0013](#), DE LA FCEI

Monsieur Jean Schiettekatte, Analyste
Monsieur Jean-Claude Deslauriers, Analyste
M^e Dominique Neuman, LL.B., Procureur

Préparée pour:
La Première Nation crie de Waswanipi
La Corporation de développement Tawich (Wemindji)

Le 22 octobre 2018

RÉPONSE À LA DEMANDE DE RENSEIGNEMENTS NO. 1, [C-FCEI-0013](#), DE LA FCEI

Monsieur Jean Schiettekatte, Analyste
Monsieur Jean-Claude Deslauriers, Analyste
M^e Dominique Neuman, LL.B., Procureur

Préparé pour:
La Première Nation crie de Waswanipi
La Corporation de développement Tawich (Wemindji)

Le 22 octobre 2018

QUESTION 1 DE LA FCEI À CREE :**RÉFÉRENCE:**

- (i) [C-CREE-0016](#), p.31
- (ii) [C-CREE-0016](#), p. x
- (iii) [C-CREE-0016](#), p. xiv

PRÉAMBULE :

- (i) « *La durée de vie d'un modèle de cartes de calcul et de cartes graphiques utilisées dans les centres de calcul est en effet d'environ deux ans seulement après quoi la technologie doit être remplacée. (Cela signifie que, sur un éventuel contrat de 5 ans entre un « cryptomineur » et Hydro-Québec Distribution, la technologie du « cryptomineur » aura à être remplacée une ou deux fois). »*
- (ii) « *Le Regroupement CREE recommande à la Régie de l'énergie d'accepter de permettre à Hydro-Québec Distribution (HQD) de ne pas desservir les futurs clients d'usage cryptographique appliqué à des chaînes de blocs (de 50 kW et plus) sauf s'il s'agit d'abonnements pour du service non ferme, mais interruptible à seulement 90% (et non à 95 % comme HQD le propose) pour une durée totale annuelle maximale de 300 heures à la demande d'Hydro-Québec, moyennant un préavis de deux (2) heures à l'avance pour chaque limitation de puissance, sous peine d'un tarif dissuasif. »*
- (iii) « *Dans tous ces cas, les clients ne paieraient pas de surplus tarifaire mais paieraient simplement leur tarif déjà normalement applicable. »*

QUESTIONS 1.1 DE LA FCEI À CREE :

Relativement à la référence (i), veuillez indiquer la source de votre affirmation quant à la fréquence de remplacement des équipements dédiés au minage.

RÉPONSE 1.1 DE CREE À LA FCEI :

Tel que nous l'indiquons à la section 7.1 de notre mémoire [C-CREE-0016](#) :

*38 - [...] La durée de vie d'un modèle de cartes de calcul et de cartes graphiques utilisées dans les centres de calcul est en effet d'**environ deux ans seulement** après quoi la technologie doit être remplacée. (Cela signifie que, sur un éventuel contrat de 5 ans entre un « cryptomineur » et Hydro-Québec Distribution, la technologie du « cryptomineur » aura à être remplacée une ou deux fois). Il existe **deux grands modèles de technologie** dans le domaine : D'une part, ASIC (utilisant des cartes de calculs spécialisées) et d'autre part GPU (utilisant la puissance de calcul des cartes graphiques). Il existe une possibilité qu'un de ces deux modèles technologiques ne vienne à dominer le marché et remplacer l'autre modèle à terme, ce qui aurait deux effets : d'abord les centres de calculs qui se seront exclusivement fiés au modèle « perdant » deviendront obsolètes et, d'autre part, la domination d'un seul type de modèle pourrait amener une hausse des prix des systèmes et donc poser un défi économique à certains cryptomineurs moins préparés à ce changement. Dans tous les cas, la survie des cryptomineurs et de leurs centres de calcul dépendra de leur capacité à s'adapter continuellement à l'évolution de la technologie et au remplacement, environ tous les deux ans, des cartes ou des systèmes. [Caractère gras dans le texte]*

Tel qu'expliqué en section 7.8 de ce même mémoire, la *Première Nation Crie de Waswanipi* et la *Corporation de développement Tawich* (dont le projet qui est exemplaire à de nombreux égards et dont nous recommandons à la Régie l'acceptation préliminaire notamment pour ce motif) se sont prémunies contre le risque d'obsolescence d'une des deux technologies en **incluant simultanément ces deux technologies dans son Projet** (une manière de faire qui avait d'ailleurs déjà été employée, par exemple, par Hydro-Québec Production dans plusieurs de ses investissements majeurs) :

137 - [...] Afin de parer au risque qu'un des deux modèles technologiques ne vienne à dominer le marché et remplacer l'autre modèle, à terme, il a été convenu dès à présent de s'associer avec un partenaire leader pour chacune de ces deux technologies (ASIC et GPU), ce qui contribue à assurer la pérennité du Projet.

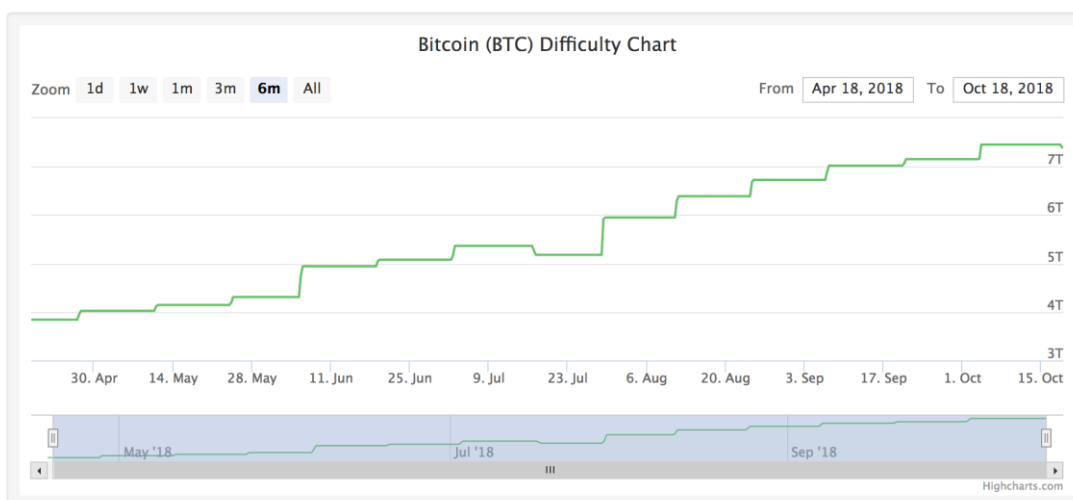
Dans son livre *“Mastering Bitcoin: Programming the Open Blockchain”*, M. Andreas M. Antonopoulos, mentionne que même en participant à un « pool » de cryptomineurs :

[TRADUCTION] « l'équipement de minage sera quand même obsolète dans un ou deux ans ». ¹

On peut comprendre assez facilement si on regarde le graphique suivant de l'évolution du niveau de difficulté pour résoudre la chaîne de blocs de Bitcoin. Ce niveau de difficulté a doublé durant les 6 derniers mois. ²



Bitcoin Difficulty Chart and Graph



Évolution du niveau de difficulté pour résoudre la chaîne de blocs Bitcoin

- ¹ **ANDREAS M. ANTONOPOULOS**, *Mastering Bitcoin: Programming the Open Blockchain*, O'Reilly, https://books.google.ca/books?redir_esc=y&hl=fr&id=tponDwAAQBAJ&q=obsolete#v=snippet&q=obsolete&f=false, Page 215, Paragraphe 1.
- ² **COINWARZ**, *Bitcoin Difficulty Chart and Graph*, <https://www.coinwarz.com/difficulty-charts/bitcoin-difficulty-chart>.

Steven Ehrlich, collaborateur à Forbes, explique que cette croissance exponentielle du niveau de difficulté du cryptominage requiert que les mineurs accroissent continuellement leur puissance cryptographique (soit en accroissant le nombre de leurs ordinateurs, soit en accroissant la puissance de chacun, par remplacement de ces ordinateurs ou de leurs cartes :

2.By Design, Mining is Not an Efficient Process

*The Proof of Work algorithms employed by Bitcoin, Litecoin, Ethereum, and other blockchains require a process known as 'brute force computing'. This means that solving the complex computational problem that gives a miner the right to add a block to a network can only be done by randomly guessing solutions as fast as possible. **There is no way to game the process or get an advantage over the competition other than by buying a higher number of more powerful computers.** Furthermore, solving one block does not give a miner an advantage over the competition when it comes to a subsequent or future block.*

It is also important to note that under Proof of Work blocks are added to their respective chains under specific time intervals, regardless of how much computing power is on the network. For example, Bitcoin adds a block on average every 10 minutes. To maintain this pace, the network automatically adjusts/increases the difficulty of the computational problem that miners are trying to solve. Simply put, there are no economies of scale when it comes to mining.³

On peut aussi voir les inquiétudes de plusieurs usagers dans le blogue « *How long until an Antminer S9 becomes obsolete and should be replaced ?* »⁴ qui confirme la sensibilité de cette industrie au changement technologique. Selon ce blogue, la rapidité de l'obsolescence des équipements de cryptographie appliqués aux chaînes de blocs varierait entre 8 mois et deux ans :

« some forums suggest 8-12 months, while others suggest it might be as long as 2 years ».

La compétition entre les deux principales technologies sur le marché amène un risque constant

³ **Steven EHRlich** , "After Bitmain's IPO Filing, Here's What Everyone Should Know About Crypto Mining", *Forbes*, Oct 1, 2018, <https://www.forbes.com/sites/stevenerlich/2018/10/01/after-bitmains-ipo-filing-heres-what-everyone-should-know-about-crypto-mining/#41fd62415968> .
Souligné en caractère gras par nous.

⁴ **CANADA BITCOIN COMMUNITY (Maadiah)**, *How long until an Antminer S9 becomes obsolete and should be replaced?*, <https://coinforum.ca/discussion/4841/how-long-until-an-antminer-s9-becomes-obsolete-and-should-be-replaced>,

d'obsolescence et un besoin continu de remplacements fréquents, ce à quoi s'ajoute la tendance vers la re-centralisation de l'usage cryptographique dont nous avons fait état à la section 5.1 de notre mémoire [C-CREE-0016](#) (ce qui constitue le plus important risque de changement technologique, plaçant ainsi à risque l'ensemble du modèle actuel décentralisé de cryptominage) :

3. Mining has Become an Arms Race

*There is a direct correlation between the computer or hashing power that a miner controls and their expected success rate. **This set off an arms race that has created exponential growth for companies like Bitmain, but which also threatens the overall decentralization and sustainability of networks like Bitcoin. When Bitcoin was first created nearly-ten years ago, blocks could easily be mined on basic computer Central Processing Units (CPUs). Eventually, it was discovered that Graphical Processing Units (GPUs) could be repurposed to mine crypto at a higher success rate than CPUs.** As the price of Bitcoin and other assets accelerated, developers in the community created Application Specific Integrated Circuits (ASICs), which are highly efficient microchips that are custom-built for one specific purpose, to randomly guess solutions to the PoW algorithm employed by any given blockchain. The top ASIC miners can run between 14-16 terahashes (guesses)/second and cost thousands of dollars.*

*Unfortunately, given the price appreciations throughout crypto in recent years, not to mention the gold rush that took place in late 2017, mining any sort of PoW cryptocurrency profitably requires the individual to either purchase an ASIC miner or join a mining pool that shares revenue based on allocated computer power. **It is also very helpful if the individual purchasing the miners is based in a cold climate to keep the machines cool and has access to cheap electricity,** as this cost directly impacts the overall profitability of any mining operation. Recent studies have shown that Bitcoin's energy consumption is analogous to the amount of electricity necessary to power a country like Switzerland for a year.*

According to Bitmain's IPO filing, the company earned \$2.25 billion in revenue in 2017 from mining hardware sales and brought in \$2.68 billion in sales during the first half of 2018. There is a saying that in a gold rush the only people who make money are those that sell the shovels; if that is the case then Bitmain is following this strategy perfectly.

4. Bitmain's Pole Position is Vulnerable

*Despite Bitmain's success to date, its executives may not [be] sleeping well at night for a number of reasons. For one, **their industry is becoming more competitive every day, and Bitmain must continue investing hundreds of***

millions of dollars in new ASIC chips to maintain its technological superiority and market share. For instance, one of Bitmain's top competitors – if there is such a thing – Innosilicon claims to now have an ASIC miner called the Terminator3 (T3) that is superior to any miner on the market today based on speed, profitability, and overall efficiency. The T3 will be released in December this year. Startups continue to target the industry as well, with companies such as Squire who just raised \$20 million to build ASIC miners.

That said, many crypto enthusiasts and interested parties do not feel that the answer to mining's shortcomings is more efficient and powerful miners. **There is a growing belief in the industry that mining should one day be avoided altogether, or at the very least the industry should become less reliant on ASICs, which as noted earlier consume huge amounts of energy and trend towards centralization. Parties looking for a complete shift away from Proof of Work typically advocate for a Proof of Stake (PoS) consensus mechanism. There are many variants of PoS, which are beyond the scope of this article, but in general the common denomination for any PoS system is that the nodes that add blocks place use a portion of their crypto holdings as collateral or a security deposit. If the validators do not act in appropriately in their role they risk losing all or a portion of their funds.** Peercoin is the first cryptocurrency that utilized PoS, and most notably Ethereum is looking to transition into a PoS system. New blockchains such as Cardano are also implementing PoS. PoS systems are designed to require significantly less energy than PoW while offering the same level of security. There are also proposed throughput and scalability benefits to a PoS model, though none of this is proven at scale.

The other main strategy being utilized is altering the hashing algorithm of PoW systems to make them ASIC-resistant. As noted above, ASIC chips are designed to be highly efficient at one very specific activity, which could be running a given hashing function. If developers introduce subtle changes to an existing algorithm, it would make every ASIC miner running the old function obsolete. This is a strategy that was undertaken by privacy-focused Monero earlier this year. Additionally, the team behind the Sia blockchain just announced that they would do the same. However, in an interesting twist they are not completely making their blockchain ASIC-resistant, just incompatible with large-scale miners such as Bitmain. It will remain to be seen how strategies like these will work as miners such as Bitmain continue to try and diversify the blockchains that their miners can support. Most likely, it will turn into a bit of a cat and mouse game.⁵

⁵ Steven EHRlich , “After Bitmain's IPO Filing, Here's What Everyone Should Know About Crypto Mining”, *Forbes*, Oct 1, 2018, <https://www.forbes.com/sites/stevenehrlich/2018/10/01/after->

Selon Nouriel Roubini, professeur d'économie à la Stern School Of Business de l'Université De New York, le principal changement technologique est l'inévitable conversion attendue des blockchain décentralisés vers des blockchains privés et centralisés, ce qui amène ainsi graduellement la réalisation de l'usage cryptographique dans des centres de données traditionnels :

Il est révélateur d'observer que toutes les blockchains « décentralisées » finissent tôt ou tard par devenir des bases de données centralisées, nécessitant un droit d'accès, lorsqu'elles sont effectivement mises en application. À ce titre, la blockchain n'a pas évolué depuis la feuille de calcul électronique standard, inventée en 1979.

Aucune institution sérieuse ne permettrait que ses transactions soient vérifiées par un cartel anonyme opérant dans la pénombre des kleptocraties les plus autoritaires de la planète. Il n'est donc pas surprenant que dans tous les cas ayant impliqué un environnement traditionnel de pilotage de la blockchain, celle-ci ait été soit jetée aux ordures, soit transformée en une base de données privée avec permission, jusqu'à ne devenir rien de plus qu'un tableau Excel ou une base de données au nom trompeur.⁶

bitmains-ipo-filing-heres-what-everyone-should-know-about-crypto-mining/#41fd62415968

Souligné en caractère gras par nous.

⁶ Nouriel ROUBINI, Professeur d'économie à la Stern School Of Business de l'Université De New York, *Le grand mensonge de la blockchain*, La Presse, le 22 octobre 2018, http://plus.lapresse.ca/screens/fdfcd171-3bbd-4bb9-993a-bfec82c70ec9_7C_0.html

Souligné en caractère gras par nous.

QUESTIONS 1.2 DE LA FCEI À CREE :

Selon vous, est-ce que l'implantation stable d'un client dans ce domaine à un endroit physique est remise en cause par cette fréquence de remplacement ?

RÉPONSE 1.2 DE CREE À LA FCEI :

Le remplacement, même fréquent, de cartes ou d'ordinateurs pour l'usage cryptographique est plus efficient que l'augmentation continue du nombre d'ordinateurs afin d'accroître la puissance de l'ensemble (ce qui requerrait un accroissement de l'espace utilisé). Ce remplacement, même fréquent, de cartes ou d'ordinateurs, tout en demeurant dans un centre de calcul, ne requiert pas de changement de local, avec la nuance qui suit. Selon nos propositions CREE-2-7.7, CREE-2-7.8 et CREE-2-7.9 des sections 2.7, 2.8 et 2.9 notre mémoire [C-CREE-0016](#) (et tout amendement de celui-ci), le client cryptographique qui désire être desservi par Hydro-Québec Distribution devra avoir déposé un plan d'affaires démontrant sa solidité technologique ainsi que sa capacité (financière notamment) à opérer les fréquents changements technologiques. Ceci implique que le local du centre de calcul devra avoir déjà prévu une certaine marge d'espace au cas où les futurs ordinateurs au cas où les futurs ordinateurs (qui sont empilés les uns sur les autres) seraient de tailles ou de formes légèrement différentes des précédents, sans être obligé à de coûteux réaménagements de locaux.

Par ailleurs, selon nos mêmes propositions CREE-2-7.7, CREE-2-7.8 et CREE-2-7.9 des sections 2.7, 2.8 et 2.9 notre mémoire [C-CREE-0016](#) (et tout amendement de celui-ci), le client cryptographique qui désire être desservi par Hydro-Québec Distribution devra, dans ce plan d'affaires ainsi déposé, avoir prévu que, d'ici environ 5 ans c'est-à-dire lorsque les centres de calcul seront en déclin), un autre usage générateur de chaleur sera établi au même emplacement. Si cet usage de remplacement est un « *centre de données* », le local initial devra pouvoir être agrandi et/ou démolir-reconstruit, afin de satisfaire aux besoins d'espace et de sécurité d'un tel « *centre de données* », tout en continuant d'alimenter, au même emplacement, l'usage de récupération de chaleur. Cela signifie également que, dans son plan d'affaires soumis à Hydro-Québec Distribution pour obtenir le droit d'être desservi, le client cryptographique devra avoir prévu que les autres conditions nécessaires au futur usage de remplacement seront également présentes (à savoir, selon le cas des lignes de télécommunication par fibre optique à grand débit si l'usage futur est centre de données, ou une alimentation en biomasse si l'usage futur est une usine de biomasse, etc.).

QUESTIONS 1.3 DE LA FCEI À CREE :

Relativement aux références (ii) et (iii), est-ce que, selon votre proposition, le « *tarif déjà normalement applicable* » serait conditionnel à ce que la charge soit interruptible sans rémunération ou ce caractère interruptible devrait-il être rémunéré comme c'est le cas pour l'option d'électricité interruptible ou la GDP affaires ?

RÉPONSE 1.3 DE CREE À LA FCEI :

Ce n'est pas notre proposition que de rémunérer l'interruption des clients cryptographiques visés par le présent dossier (ce qui, selon le champ d'application que nous proposons à notre recommandation CREE-2-7.1 de notre mémoire [C-CREE-0016](#) (et tout amendement de celui-ci), n'inclurait pas un « *centre de données* » effectuant des calculs cryptographiques).

Nous proposons que le tarif déjà normalement applicable G, M ou LG continue de s'appliquer à de tels clients cryptographiques « *qui auront le droit d'être desservis* » à l'issue du mécanisme qui sera décidé au présent dossier. Or, parmi les conditions donnant le droit d'être desservi à un tel client G, M ou LG, celui-ci doit accepter d'être interruptible sous certaines conditions, avec un **tarif dissuasif** (dont le calcul suivrait notre recommandation 2.8 du chapitre 8 de notre mémoire [C-CREE-0016](#) (et tout amendement de celui-ci). Il n'y aurait donc pas, en plus, de rémunération pour s'interrompre :

**RECOMMANDATION NO. CREE-2-8
LES TARIFS DISSUASIFS**

*Le Regroupement CREE recommande à la Régie de l'énergie d'édicter que les tarifs dissuasifs au présent dossier pour usage non autorisé (tant pour usage cryptographique sans avoir été sélectionné que pour défaut de s'interrompre) devraient être établis selon le **coût marginal** causé par cet usage non autorisé.*

Par ailleurs les clients cryptographiques G, M ou LG « *qui n'auront pas le droit d'être desservis* », à l'issue du mécanisme qui sera décidé au présent dossier, paieront aussi le tarif dissuasif pour usage non autorisé, tel que décrit également à notre recommandation 2.8 du chapitre 8 de notre mémoire [C-CREE-0016](#) (et tout amendement de celui-ci).

Enfin, les « centres de données » (qui effectuent, on l'a vu, des calculs cryptographiques), y compris ceux qui seront amenés d'ici environ 5 ans à remplacer certains centres de calcul cryptographiques (lorsque ceux-ci seront en déclin) paieront le tarif qui leur est normalement applicable (vraisemblablement le tarif LG, possiblement complété par le tarif de développement économique); Hydro-Québec Distribution est toujours tenue d'accepter un client de « centres de données » (sous réserve du seuil de 50 MW au-delà duquel l'article 10.6 des *Tarifs et conditions* lui donne le pouvoir de ne pas desservir). Mais par leur nature, de tels « centres de données » ne choisiront pas l'option de tarif interruptible ni le programme GDP Affaires. **En effet, un centre de données n'est pas interruptible.**
