Du bon jus de BTC pour ta finance

[Un trollud croisé entre twitter et reflets m'oblige à zapper mon film du lundi soir pour pondre quelques explications. A force de lire des âneries partout dans la presse depuis un an, de toute façon, il fallait bien que j'use de nouveau mon joli clavier. Disclamer : j'ai des bitcoins, des ether, des bitcoin cash, quelques litecoins, une jolie pelle de ?1 et probablement 2/3 autres cryptos. Ouais, j'aime ça. Non, je suis pas riche.]

Le bitcoin, les bases.

Bon, non, je vais pas vous les refaire, y'a un tas de littérature en ligne sur le sujet, et si vous voulez rester dans les parages, j'ai commis quelques articles également.

Bon alors, le jus de BTC, comment on fait ?

CC BY SA strelitzia

Si t'as tout bien lu et compris les articles qu'on peut trouver ici ou ailleurs, tu sais déjà que les bitcoins n'existent pas matériellement et ne sont qu'une succession de blocs qui gravent des transactions dans le marbre et, au passage, créent de nouvelles unités monétaires. Ce n'est pas spécifique au bitcoin, toutes les cryptomonaies fonctionnent comme ça : les blocs créent de la monnaie et servent à la faire voyager d'un compte à un autre.

La grosse critique du moment affirme que le bitcoin est une hérésie écologique à cause du courant consommé par transaction. Et du coup, là, je dis : NAN.

Le jus de BTC, ça ne se fabrique pas en se basant sur les transactions. Autrement dit, ce n'est pas parce qu'il y aura 2 fois moins de transactions que le réseau bitcoin consommera deux fois moins d'énergie, pas plus qu'il n'en consommera 10 fois plus si on décuple les transactions.

Du coup, l'argument « Tant de kW/h par transaction » est une ânerie.

Mais alors, d'où qu'elle vient, la conso du bitcoin ?

Pour faire simple, elle vient de l'avidité humaine.

Reprenons au début : un bloc est, à l'origine, miné pour enregistrer des transactions. Il se trouve, dans le cas du bitcoin et de pas mal d'autres cryptos, que pour éviter que l'ensemble de la monnaie ne soit crée au début, il a été convenu que chaque bloc en créait un peu. C'est une façon de répartir la création de la monnaie sans connaître les futurs acteurs et de la faire émerger au cours du temps. Mais la fonction de base du bloc est bel et bien d'enregistrer des mouvements entre comptes. Il se trouve que le bitcoin limite en gros le nombre de transactions dans un bloc à ~2000 (en vérité, un bloc ne peut pas faire plus d'1Mo et il se trouve qu'une transaction fait aujourd'hui en gros un demi Ko) et que la personne qui trouve le bloc récupère les frais de transaction associées à celles qu'il inscrit dans son bloc (entre 1 et 4 BTC par bloc de nos jours). Sauf qu'avec un bitcoin à 16000 euro et quelques, la rémunération actuelle de 12.5 BTC de nouvelle monnaie crée pour chaque bloc attire pas mal (oui, on a bien lu : ~3 BTC de frais de transaction + 12.5 BTC de monnaie crée, soit pas loin de 250k€ toutes les 10 minutes au cours actuel).

Du coup, c'est une bête course à l'échalote : pour avoir le plus de chance de trouver le prochain bloc, il faut aligner la plus grosse puissance de calcul. Et la puissance de calcul, ça se trouve de deux façons : en alignant tout le matos que tu peux comme un porc qui va tirer un courant de barjo ou bien en faisant de la R&D pour sortir des puces (on dit des « ASICs ») spécialisées dans le calcul idiot nécessaire à la création de blocs, et donc consommer des ressources rares pour créer des engins dans le seul et unique but de faire un calcul qui n'a aucune autre fonction que de s'assurer qu'on a aligné des ressources matérielles pour créer des blocs.

Donc c'est pas bien dur : plus le BTC vaut cher, plus il attire des gens qui voudraient en avoir, plus il y a du matos qui est fabriqué et branché au courant.

Du coup, suffit de faire baisser la valeur, et PAF, ça consomme moins !

C'est l'idée … Sauf que des cryptomonnaies, il y en a des milliers et que les mineurs passent leur temps à switcher d'une chaîne à une autre en fonction de la rentabilité très court terme (de l'ordre de l'heure, il y a mêmes des sites faits pour ça). Donc dézinguer le bitcoin (par exemple en arrivant à convaincre les frères Winklevoss d'inonder le marché en vendant leur trésor de guerre) ne fera que faire se reporter la puissance de minage sur d'autres monnaies qui vont du coup grimper à une vitesse folle. Eh ouais, le matos pour miner, il existe, il est là, il est branché, il tourne, il faut qu'il mine.

On est foutus alors ?

Pas mal oui. Des industrie fondent à tour de bras des ASICs et des GPUs de minage et ça

aligne du rayonnage à mort dans des pays ou le courant coûte pas grand chose. Le seul salut dans l'histoire est de voir émerger des cryptos utilisant des calculs ne pouvant pas être (mieux) gérés par des ASICs ou des GPUs … du coup, les industriels du secteurs pourraient se reconvertir vers des activités plus utiles, comme héberger des contenus. Mais dans cette belle industrie, tenue par une grosse vingtaine d'entreprises en ce bas monde, QUI va vouloir se tirer une balle dans le pied pour le bien commun ?

Guess who !

Personne.

Du coup, on fait quoi ?

On peut simplement attendre. A un moment, les bitcoins crées en même temps que les blocs vont se réduire à peau de chagrin (le 8 juin 2020 on passera de 12.5 à 6.25, et ainsi de suite tous les 210000 blocs, soit une division par deux environ tous les 4 ans) … sauf qu'il n'y aura toujours que 2000 transactions par bloc, donc fort intérêt à augmenter les frais de transactions si on veut qu'elles passent rapidement … sauf que peut être que le lightning network (une méthode hors blockchain pour effectuer des transactions rapides) va peut être calmer le jeu … ou bien l'un des nombreux forks de la chaîne (comme le bitcoin cash, existant depuis cet été, ou le bitcoin gold, qui a lamentablement échoué à la rentrée dernière). Sans compter que là dedans, on trouve aussi des monnaies qui ne fonctionnent pas sur le principe de « j'ai une plus grosse puissance de minage, j'te nique » qui montent doucement mais sûrement.

En bref, c'est un écosystème plutôt archi complexe qui peut être déstabilisé d'une minute à l'autre … Et même si ça tire du TW/h à fond, c'est une expérience qui me semble nécessaire, d'une part pour s'assurer que les gens sont toujours globalement aussi cons, mais aussi parce qu'il faudra bien abattre les banques et que ça peut être un moyen.

Et à part attendre ?

On ouvre un portefeuille ?1, on va rencontrer son prochain, on se fait certifier, et on essaie une monnaie basée sur la blockchain, mais libre et à dividende universel ? C'est probablement pas encore la bonne qui changera le monde, mais elle consomme beauuuucoup moins de ressources et aide à se poser les bonnes questions sur la façon dont on crée la monnaie aujourd'hui et comment elle est distribuée et utilisée.

Allez, chiche ! :)