un article sur le Bitcoin que j'avais écrit en 2018 et qu'il faut que je réactualise …

« Mon cher Jack,

Comme je te l'ai écrit dans ma dernière lettre, on se retrouvera début septembre à Skagway. J'ai raflé tout le stock chez le chinois de Market Street. Il était tout excité et m'a promis que cela tiendrait 14 Téra Hash mais tu ne sais jamais très bien avec lui… Et puis, j'ai aussi rassemblé suffisamment de chiens pour monter *nos vivres et toutes nos cartes ASIC. Notre claim est à trois jours du Chilkoot. Il y a plein de torrents autour et de quoi dresser des barrages pour donner du jus à nos cartes. Crois-moi, elles vont gentiment ronronner et nous tenir chaud pendant le blizzard et au printemps, on sera riche, Jack ! et cette fois-ci, je te prédis que nous traverserons Dawson sans verser une goutte d'alcool, sans même aller rendre une visite à Julia, nos poches gonflées de bitcoins, comme des seigneurs sous les étoiles.*

Bien à toi,

SF Juin 2018″

Et voilà, mon histoire s'arrête provisoirement ici. Comment vais-je parvenir à placer tous ces trucs de *hash*, de *nonce*, de *courbes elliptiques* ou de *peer-to-peer* ? La plume du grand *Jack* n'aurait pas tremblé, elle !

De la confiance

J'entendais parler du *bitcoin* depuis longtemps avec indifférence mais si je me rappelle bien, c'est en mai 2017, lorsque des *hackers* ont disséminé le virus *WannaCry* puis réclamé une rançon en *bitcoins* que, dans mon esprit, la légitimité de cette monnaie venait ironiquement d'être établie. J'entrevoyais que si le *bitcoin* permettait un

échange de valeur entre citoyens ordinaires d'une part et escrocs de l'autre, à la vue de tous, alors cette monnaie universelle était vraiment digne de confiance !

Ce qui me frappe aujourd'hui en observant le système *Bitcoin*, c'est sa robustesse. Faut-il que ce cela soit bien conçu pour fonctionner sans véritable accroc depuis sa création en 2009 ! C'est la plus fameuse *blockchain* que l'on puisse imaginer car elle est publique et cristallise sur sa technologie 130 Milliards d'Euros, ce qui représente un sacré tas de confiance.

Le *bitcoin* est le nom de la monnaie qui est produite par le système *Bitcoin* qui est, lui, un écosystème comprenant des développeurs, du logiciel, un protocole, une communauté d'intérêt à entrée libre. Le *bitcoin,* contrairement à l'or, ne possède aucune valeur intrinsèque. Il doit être considéré essentiellement comme un système de paiement. Il est progressivement perçu comme valeur refuge.

De l'énergie

Toute cette belle confiance fossilisée dans le *bitcoin* est basée *in fine* sur une dépense énergétique ahurissante. Ce 13 janvier 2023, au moment ou j'écrit ces lignes, des milliers de sites informatiques bourrés d'ordinateurs tournant à plein régime participent à un jeu de devinette à l'échelle mondiale en consommant l'équivalent de 127 TWh/an , soit 27% de la consommation Française d'électricité. Et c'est sur ce mécanisme incroyable à la fois absurde et génial que fonctionne le *bitcoin*. Pourquoi ? En raison d'un enchaînement de conséquences liées au caractère décentralisé d'une *blockchain* publique et donc du *Bitcoin* en particulier.

On va produire de la monnaie de façon décentralisée, mais cependant maîtrisée, et confier à un grand nombre de volontaires, appelés des *mineurs* dans le jargon *Bitcoin,* le soin de garder une copie du registre de tous les virements

effectués avec cette monnaie depuis sa date de démarrage en 2009. Allons-nous confier la tenue des comptes à de parfaits inconnus ? Oui, c'est exactement ce que l'on va faire sous la forme de ce qui peut s'apparenter à une franchise.

A cette fin, on élabore un Grand Livre comptable dans lequel sont enregistrés tous les mouvements de *bitcoins* d'une partie vers une autre, c'est à dire d'une personne privée ou morale, vers une autre. D'un point de vue technique, ce *Grand Livre* est matérialisé par un ensemble de fichiers organisés sous la forme d'une *blockchain*. C'est à l'intérieur de celui-ci que sont enregistrées toutes les transactions financières qui sont signées à l'aide de clefs asymétriques, puis regroupées en blocs qui sont tricotés ensemble à la manière d'une écharpe qui grandirait inexorablement. Toute tentative pour y introduire une opération frauduleuse qui ressemblerait à celle-ci : « *je verse, ex nihilo, un million de bitcoins à moi-même, le 16 avril* » est considérée d'un point de vue cryptographique comme quasiment impossible, quand bien-même le Grand Livre est accessible à tous.

Liberté ensuite, à qui le veut, de télécharger sur son ordinateur le logiciel *Bitcoin Core* qui récupérera une copie de cette *blockchain* puis de se déclarer comme volontaire (*mineur*) pour en assurer une réplication conforme à toutes les autres copies dans le monde. En échange du service qui est, concrètement, celui de maintenir un niveau de disponibilité indiscutable (en raison des milliers de répliques du Grand Livre), le système *Bitcoin* rétribue chaque *mineur* selon un barème évoluant dans le temps mais en assortissant le *deal* d'une autre contrepartie qui est celle de participer à un jeu coûteux en temps. Oui un jeu, une sorte de loterie !

Du consensus

L'objectif primordial, dans un système décentralisé, est d'obtenir un consensus sur un

exemplaire VRAI et donc unique du Grand Livre tout en évitant un emballement du nombre de synchronisations (*peer-to-peer*) entre les comptables (les *mineurs*) pour savoir quelle est la bonne version et en évitant également la formation d'une situation monopolistique (> 51% de *mineurs* complices).

Venons-en à ce que je considère comme la plus grande et géniale monstruosité qui constitue un sérieux défi à l'entendement: On introduit un mécanisme de ralentissement qui vise à garder à la fois un nombre raisonnable de *mineurs* et un nombre raisonnable d'échanges entre eux pour ne pas saturer le réseau. C'est cette même mécanique qui permet, indirectement, de réguler la rareté de façon déterministe puisque le nombre de *bitcoins* à atteindre, selon les statuts de départ, est de vingt-et-un millions, pas un de plus, selon une cadence programmée jusqu'en 2040. On va donc obliger les *mineurs* à perdre du temps dans un jeu de devinette. Celle-ci nécessite que chaque *mineur* soit équipé d'un ordinateur, d'un accès au réseau internet et d'un logiciel spécialisé, le *Bitcoin Core*. L'émergence du consensus est ainsi acquise à l'aide du mécanisme précédent désigné par l'expression « *preuve de travail* » (POW). C'est également le cas pour Ethereum qui est une autre *blockchain* très populaire. La question est de savoir comment objectiver cette quantité de « travail » et c'est maintenant qu'il faut rappeler les vertus du *hash*.

Du hash

« *De toute ma vie, je n'avais jamais vu une telle quantité de hash partir en fumée!* «

Le système *Bitcoin* est conçu pour « fatiguer » les machines des *mineurs,* éprouver leur détermination pour ainsi dire. *Bitcoin* utilise *ad nauseum* la technique de *hashing*. Il s'agit d'un procédé logiciel qui consiste à produire, à partir de n'importe quoi (un texte, des nombres, une image, un livre complet) une suite de

caractères d'une longueur fixe de 256 bits qui représente un condensé unique appelé *hash*. Ce dernier se présente soit comme une suite de deux cent cinquante-six chiffres 1 et 0, soit comme une chaines de trente-deux chiffres ou lettres. C'est juste une affaire de représentation.
SHA256 est l'une des variantes de ce procédé. C'est un beau bijou logiciel digne d'une montre à complications et qui mériterait lui aussi d'être porté au poignet. En décrire le fonctionnement sort du cadre de cet article mais je peux simplement dire que, si deux choses auxquelles on applique le *hashing* présentent une différence, aussi insignifiante soit-elle, alors les valeurs de *hash* obtenues seront totalement différentes. Par exemple, si je modifie un seul caractère du texte de la Bible, une autre personne peut le détecter immédiatement en constatant que la nouvelle valeur de *hash* vient de changer radicalement. C'est donc très pratique pour garantir l'inviolabilité d'une information. A contrario, je mets au défi quiconque de trouver, à partir d'une valeur de *hash* prise au hasard, quelle est la chose qui lui a donné « naissance ».
Cependant …cependant … il est de l'ordre du possible de lancer un challenge qui ressemblerait à celui-ci : « T*rouver une chose dont la valeur de hash commence par une série de 18 zéros.* »
C'est exactement ce genre de devinette qui sera soumise aux ordinateurs !! Après des milliards de milliards de « coups de hachoir », si on parvient à obtenir un *hash* présentant cette caractéristique, le jeu de devinette est gagné. S'il faut augmenter la difficulté, le défi deviendrait simplement : « *Maintenant, encore plus fort: c'est 17 zéros et non plus 18.* « .

Si on se relie à nouveau à notre Grand Livre, le principe de la devinette évoquée plus haut consiste à « tomber » par chance sur un nombre appelé *nonce,* (2) tel que, combiné avec le contenu d'une nouvelle page du Grand Livre contenant les enregistrements des toutes dernières transactions, celui-ci produise à l'issue d'un *hashing* une valeur de *hash* présentant des caractéristiques morphologiques

précises (*Target*) comme illustré précédemment.

Pour donner une idée, il faut environ actuellement un trillion d'essais, environ, avant de tomber sur un bon nombre. Tout dépend si on a de la chance, mais disons que c'est calibré pour durer environ dix minutes. Le logiciel de *Bitcoin* communément utilisé par chacun des *mineurs* agit ainsi à la manière d'un *pacemaker* qui fixe le niveau de rareté en fonction du nombre de *mineurs* à un instant donné et de la puissance intrinsèque des ordinateurs qui, elle, progresse régulièrement en raison des progrès de la technologie. La difficulté augmente tous les 2016 blocs, c'est à dire toutes les deux semaines environ.

Dès qu'un *mineur* trouve une combinaison correcte, son logiciel avertit tous les autres (*peer-to-peer*). A partir de ce moment là, tous les autres *mineurs* sont tenus de vérifier que le nombre est effectivement correct, et s'inclinent alors en acceptant la victoire du compétiteur et ajoutant au Grand Livre la nouvelle page, c'est à dire le bloc qui vient d'être validé par le vainqueur. Résultat: 6,25 *bitcoins* dans la poche de celui qui a trouvé le nombre, plus une petite rémunération associée (*fee*) à chacune des transactions enregistrées dans le bloc, et on est reparti pour le tour suivant ! Précisons que c'est uniquement à ce stade qu'a lieu le processus de création monétaire. Au 23 janvier 2024, le *bitcoin* (BTC) s'échange contre 46.430 € et donc le gagnant ramasse environ 290 187 €. De l'électricité est consommée (il vaut mieux être en Chine), de la chaleur produite (il vaut mieux être en Islande) , du bruit n'en parlons pas (il vaut mieux être sourd) , tout cela pour être le premier à lever le doigt. C'est complètement idiot, non ? C'est à la fois absurde et génial. C'est le prix à payer pour obtenir un consensus dans une communauté d'intérêts dénuée de confiance (*trustless*). Il existe d'autres méthodes sur lequel le système *Bitcoin* aurait pu s'appuyer pour obtenir un consensus, mais celle-ci s'avère très robuste lorsque l'environnement ressemble d'avantage au Far-West qu'à une association diocésaine.

Dans ce qui précède, j'ai eu recours à un peu d'anthropomorphisme en parlant de *mineurs*, mais j'aurais dû employer le terme plus exact de « logiciel *Bitcoin* utilisé par le *mineur*« .

La ruée

Inutile d'insister sur les enjeux ni de préciser qu'il existe une course aux armements en matière de puissance de calcul. Les processeurs classiques sont désormais hors jeu dans cette compétition. On détournait encore très récemment l'usage des cartes graphiques élaborées (celles utilisées par d'autres vrais *gamers*) pour leur faire exécuter ces fameuses opérations de *hashing*, mais elles sont désormais supplantées par des circuits spécialisés (ASIC) qui ne savent rien faire d'autre que du *hashing*.

Une carte spécialisée ASIC telle que *Bitmain Antminer S19 XP* effectue 140 Teras, soit environ 140.000 milliards d'opérations de *hashing* en une seconde. Une machine de ce type vaut 3.500 €. Comme il faut concentrer beaucoup de puissance pour se garantir un niveau de rémunération qui ne soit pas trop aléatoire, beaucoup de mineurs se contentent de rejoindre des sortes de coopératives (*mining pool*) et le butin, s'il y en a, est partagé selon des règles propres à la coopérative. La puissance totale recensée au mois d'avril 2018 est de l'ordre de 671 millions de Tera H/s, soit 671 Peta TH/s. C'est ce qu'on appelle le *Hashrate*. Le logiciel *Bitcoin Core* tient compte de cette information pour moduler le niveau de difficulté. En avril 2018, la Chine où le charbon est abondant et par conséquent l'électricité bon marché (0.11 $ /kwh), concentrait plus de 51% des *pools* de mineurs (AntPool, F2Pool, BTCC). Ce dernier point ne signifie pas que nous sommes en présence d'une situation monopolistique mais entraîne cependant des interrogations. Le système *Bitcoin* n'est de toute façon qu'une interminable liste de « que se passerait-il si… ».

De la raison

le *Bitcoin* est donc cette expérience révolutionnaire qui se déroule sous nos yeux en temps réel et qui est passée directement du stade de *white paper* en 2009 à celui de laboratoire puis celui de banque alternative crédible. Le *Bitcoin* a popularisé l'emploi d'une approche décentralisée pour réinventer des modèles d'échange de valeurs, et affronter de nouvelles classes de besoins que notre esprit conformiste ou notre fameux bon sens nous aurait empêcher d'envisager sous une autre forme que celle passant par le « nécessaire » tiers de confiance. C'est le plus bel exemple de *blockchain* en activité.

» *Est-ce bien ce monde meilleur que tu souhaitais Jack ? »*

---

(1) Les avis sur cette cryptomonnaie sont partagés, évidemment. Des économistes prétendent qu'elle alimente une bulle spéculative et fait courir des risques importants au système financier. Le prix Nobel JeanTirole ou bien Jamie Dimon (JP Morgan) ont écrit récemment des articles très négatifs sur le *bitcoin*. Ce dernier est un « objet » tellement révolutionnaire et échappant à toute expérience passée que même des économistes chevronnés ne parviennent pas à s'accorder pour dire, par exemple, si le *bitcoin* est assimilable à une pyramide de Ponzi ou non.

(2) Devant la montée en puissance des processeurs spécialisés (ASIC) en *hashing*, il a fallu se libérer de la valeur du *nonce* qui permettait de monter à « seulement » quatre milliards en lui ajoutant d'autres combinatoires. Ce fut l'objet du protocole stratum qui permet à un *pool de mineurs* de travailler efficacement en partageant des « plages de calcul »