Cryptomonnaies, environnement et usage

Credit photo : Duncan Rawlinson

Au détour d'un tweet un peu troll mais avec un peu de fond quand même, je me suis fais sauter dessus par quelques twittos manifestement inlovewithbitcoin ces quelques derniers jours. Il y a 9 ans, quand je commençais à écrire sur le bitcoin, on ne parlait pas trop de smartcontracts, de proof of stake, … mais quasi tous les éléments du débat étaient déjà sur la table (voir les commentaires de l'article) :

- la conso énergétique / environnementale (le courant qu'il faut pour faire marcher le truc et les énergies et matières premières pour construire le matériel)
- l'adoption et l'usage bien peu « mainstream » de la chose
- les alternatives (avec, notamment, openUDC, ancêtre de Duniter qui a donné la June)

Full disclo : oui, j'ai eu plein de bitcoins en 2011, pour jouer avec, vu que ça « coûtait » entre 1 et 10 € en 2011 … Non je n'en ai plus tant que ça, oui c'est rageant, oui j'en ai encore qui sont coincés au Japon dans la faillite de MTGox, et oui j'ai aussi quelques autres cryptomonnaies. Une partie non négligeable des sous que j'ai de côté y sont rangés. Je les y laisse en grande partie parce que le fait de les rapatrier sur un compte en banque est un cauchemar au niveau déclaration fiscale.

Bien. Commençons !

La monnaie ça sert à quoi ?

A quantifier les échanges entre des personnes (physiques ou morales). En simplifiant à l'extrême, plutôt que de se demander combien de poireaux vaut un steak, on donne une valeur à chaque choses susceptibles de faire l'objet d'un échange.

Ça sert également de « réserve de valeur ». On sait déjà que l'argent ça ne se mange pas mais, partant du principe qu'on peut acheter du manger avec, garder l'argent de côté permet, en principe, de manger plus tard. Ça suppose trois choses :

- qu'il y ait du manger à vendre
- que la personne qui le vend accepte la monnaie qu'on lui présente
- qu'on ai assez de cette monnaie pour acheter le-dit manger

La crise du COVID a mis en lumière que ces trois prérequis sont loin d'être évidents : les capacités de production mondiales sont en chute libre (donc pas sur qu'il reste des choses à acheter) et il n'est pas impossible qu'une perte de confiance généralisée envers les monnaies de nos états déboule rapidement compte tenu de la quantité d'argent crée et déversée sur les marchés quotidiennement un peu partout dans le monde (plus d'argent en circulation + moins de choses produites + moins de choses achetées = baisse de la « valeur de l'argent » => il faut plus d'argent pour acheter la même chose)

Le nœud du problème : qui crée la monnaie et selon quelle règle ?

L'idée est d'avoir une quantité de monnaie en circulation qui soit juste suffisante pour permettre les échanges nécessaires. Ni trop (sinon les prix augmentent) ni trop peu (sinon les prix baissent). Au siècle dernier, la création de monnaie était indexée sur l'or. Un état devait avoir de l'or dans ses coffres pour pouvoir fabriquer des billets ou des sous sur un compte bancaire. L'immense majorité des pays a abandonné ce principe dans la seconde moitié du vingtième siècle.

Beaucoup ne le savent pas, faute de culture générale en économie, mais la monnaie dont on se sert tous les jours est crée par le crédit. Vous parvenez à convaincre votre banque de vous « accompagner » dans votre projet immobilier, vous signez un papier qui vous engage à rembourser, la banque invente les 200.000 € qu'elle crédite (d'où le terme « crédit ») sur votre compte, vous remboursez chaque mois une part de ce montant (qui est immédiatement détruite) et un peu d'intérêts (que la banque conserve bien au chaud : c'est cette somme qui constitue son chiffre d'affaire). A aucun moment la banque ne « prête » de l'argent qu'elle aurait par ailleurs en dépôt. Une fois votre maison achetée, les 200.000 € partent dans les mains du vendeur (ou du constructeur) qui va probablement rembourser lui même un bout de crédit précédent (donc une partie de cette monnaie est directement détruite), et se servir du reste pour faire ses courses (permettant, entre autre, au boucher de rembourser son crédit).

Nous avons aussi les banques centrales qui de plus en plus arrosent largement soit les banques commerciales directement, soit les marchés boursiers, soit les entreprises (les grosses hein, pas le boulanger du coin).

Bilan des courses : si plus personne ne fait de nouveaux crédits, la monnaie disparaît petit à petit au fur et à mesure des remboursements des anciens. Si, pris à la gorge, les gouvernements tentent de soutenir l'économie défaillante (comme en ce moment) à grand coups de milliards inventés de nulle part, éventuellement même parachutés directement sur les comptes en banque de chacun (comme aux États-Unis) mais puisqu'il n'y a rien à acheter avec (parce que les usines, restaurants, etc. sont toujours en berne), l'argent va très naturellement partir dans le remboursement des dettes, et donc réduire encore plus la masse monétaire globale.

Les spécialistes me pardonneront les énoooormes raccourcis que j'ai pris, mais c'était pour illustrer la galère monétaire dans laquelle nous entrons. Je recommande vivement la chaîne Youtube Heu?reka à ceux qui veulent creuser le sujet.

Comment faire autrement ?

Pourquoi diable a-t-on confié à des banques privées le soin de réguler notre masse monétaire ? Pourquoi via le crédit et pas une autre règle de fonctionnement ? Quelles sont les alternatives ? Sont-elles plus justes et équitables ? A-t-on vraiment pensé à tout ?

Dans le troll dans lequel je me suis moi même jeté, le point sur lequel j'insistai était la gabegie énergétique que représente aujourd'hui le bitcoin. Quelqu'un a fort justement souligné, un peu plus tard, qu'il y avait aussi des matières premières et de l'énergie lors de la fabrication du matériel qui devaient rentrer dans les calculs. On va faire un rapide rappel du fonctionnement du bitcoin en terme de création monétaire :

- le protocole édicte que la chaîne consignant les transaction doit grandir en moyenne au rythme d'un bloc toutes les 10 minutes.
- un bloc est constitué d'une liste de transaction, d'une référence au bloc précédent (d'où le concept de chaîne) et d'un nombre aléatoire. Un « mineur de bitcoin » vérifie la validité des transactions, puis effectue la combinaison de ces trois information et la passe dans une moulinette (hachage) pour obtenir un chiffre qui doit comporter, au début, un certain nombre de 0 pour que le bloc soit désigné comme valide et ajouté à la chaîne
- plus il y a de gens qui font tourner des ordinateurs à ce petit jeu, plus la probabilité qu'un bloc valide soit trouvé augmente
- la difficulté de trouver un bloc est ajustée automatiquement de façon régulière en fonction de la fréquence d'apparition des derniers blocs trouvés. Cette difficulté consiste juste à imposer que le résultat du hachage du bloc contienne plus ou moins de zéros afin de réguler l'apparition de nouveaux blocs.
- le mineur qui « trouve un bloc » valide se voir remercié par l'encaissement des frais de transactions et par la création nouvelle de monnaie par la simple existence du-dit bloc, et qui lui est directement attribuée
- tout le monde veut donc gagner de l'argent et aligne du matériel pour avoir plus de chance de trouver des blocs valides
- plus on ajoute du matériel pour chercher des blocs, ça devient plus dur d'en trouver, si on en enlève, c'est plus facile
- la part du travail consistant à vérifier les transaction est minime (quelques millisecondes) par rapport à celle consistant à tirer des chiffre au sort et à passer le tout dans une fonction de hachage pour trouver un certain nombre de zéro (l'ensemble du réseau développe actuellement une capacité de hachage d'environ 100EH/s – 100 exahash par seconde – 100 000 000 000 000 000 000 opérations de hachage de bloc par seconde. Soit un bloc toutes les 10 minutes, le réseau bitcoin effectue donc en moyenne 6×10^{22} opérations « pour rien » pour une « bonne opération »
- s'il est important que plusieurs acteurs travaillent à la validation pour que le réseau reste décentralisé, l'empilement de matériel coûteux en ressources et gourmand en

> énergie ne présente aucun autre intérêt que de départager les participants : c'est celui qui a le plus de matos qui a la plus grande probabilité de bénéficier directement de la création monétaire

Nous avons donc un choix algorithmique qui a un impact environnemental et énergétique direct. Valider que les transactions sont légitimes peut se faire avec la capacité de calcul d'un Raspberry PI 3 à 20$.

Ma critique consistait à souligner que le fait, pour quelques mineurs, de recourir, quand elle existe, à l'usage de la surproduction hydrolienne n'était pas suffisant pour prétendre que le bitcoin n'avait pas ou peu d'impact écologique. Ce qui n'enlève rien à ses qualités par ailleurs.

Remettre les choses en perspective

La capitalisation, toutes cryptomonnaies confondues, oscille ces derniers temps entre 100 et 300 milliards d'euro. Le bitcoin représente entre 60 et 70% de cette masse globale. L'utilité principale de l'ensemble de ces monnaies reste la spéculation. Une infime minorité des transactions concernent des opérations d'achat/vente de biens et de services.

Et quand on parle de capitalisation, on parle de la valeur de l'ensemble de ce qui circule si quelqu'un achetait l'ensemble au prix que ça vaut aujourd'hui. Sauf que le prix actuel, si quelqu'un déboule et veut acheter tout ce qui est à vendre, va monter en flèche. De même que si tout le monde se met à vouloir vendre à tout prix ce qu'il a, le prix va se casser la gueule jusqu'à 0 et même en dessous. Ce sont « les lois du marché ». Cette valeur ne correspond donc à rien de réel, mais on peut tout de même la comparer à la « valeur » du reste. Pour la zone euro, on parlait de 12000 milliards d'euro en 2018. Sans compter donc les États-Unis, la Russie, le Moyen Orient et l'Asie. Autant dire que les cryptomonnaies sont un shtroumpf au pays des géants.

Difficile de déterminer le coût énergétique et environnemental de gestion de ces 12000 milliards, mais si :

- on part du principe que les 21 millions de bitcoins maximum qui existeront remplacent des 12000 milliards d'euro
- que son cours, et donc l'intérêt pour des mineurs de mettre en route des infrastructures, suit la courbe d'adoption
- dans l'hypothèse d'une économie 100% bitcoin, on arrive à un cours de 570000 € / BTC (*57 par rapport à aujourd'hui)
- actuellement, le bitcoin consomme l'équivalent d'un pays de 8.5 millions d'habitants (pour environ 50 millions de portefeuilles contenant des bitcoins dont 7 millions sont réputés « actifs »)
- on aurait donc une conso finale de l'ordre de celle de 484 millions d'habitants
- la zone Euro compte 530 millions d'habitants

On parle donc de quasi doubler la consommation énergétique de la zone Euro. Uniquement

pour gérer la monnaie. Ou plus exactement pour limiter le rythme de sa création et diluer les frais de transaction entre de multiples acteurs.

Évidemment, ça n'arrivera jamais, mais ça illustre bien le doigt dans l'œil fourré jusqu'au coude de ceux qui prétendent que le bitcoin ne fait pas tant de mal que ça à la planète puisqu'il exploite en partie du courant généré par des installations type éolien, solaire et surtout hydrolien qui, par moment, sont en surproduction manifeste comparé à la demande.

C'est au mieux une vision court termiste : la nature (et le marché) ayant horreur du vide, si cette production hydrolienne existe et est utilisée, la probabilité qu'elle ne serve plus, ultérieurement, aux mines de bitcoin mais à des usages plus … utiles, est quasi nulle (tant que le bitcoin a une valeur, en tout cas)

There's got to be a better way

Bitcoin a eu l'avantage de révéler la blockchain et de proposer une façon moins sensible aux crises géopolitiques de créer et gérer la monnaie. C'est une bonne chose. Il permet, aujourd'hui, de diversifier un peu ses placements. Mais ça ne sera pas LA solution qui permettra de remplacer le système monétaire actuel par quelque chose de plus stable et juste, ne serait-ce que pour les raisons énergétiques exposées ci-dessus et parce qu'on sait comment termine un pays avec une monnaie qui passe son temps à fluctuer comme les directives gouvernementales françaises en ce moment (même si on peut espérer, avec un usage allant crescendo, une stabilisation du change bitcoin autre monnaie)

Dans l'univers de la blockchain (et de ses amis, nés après, comme le tangle ou le hashgraph), d'autres façons de faire sont apparues, dont :

Le pré-minage : l'ensemble de la masse monétaire est crée dès le début et sa gestion est confiée à un organe défini (souvent une fondation). Avantage : plus de course à l'échalote sur le matériel et l'énergie, problème : la répartition de la masse monétaire est laissée à l'appréciation d'une structure pilotée par des humains, donc faillible et corruptible.

La proof of stake : ou preuve d'enjeu, en bon français. L'idée est de ne plus confier la nouvelle monnaie crée à celui qui a le plus de matériel mais à celui qui a bloqué le plus de monnaie déjà existante. Avantage : pas de course à l'échalote non plus, problème : on reproduit un des travers du capitalisme qui tend à concentrer la masse monétaire entre peu de mains puisqu'il faut déjà avoir de la monnaie pour en obtenir plus et plus on en a, plus on en obtient.

La proof of authority : il s'agit ici de « monter patte blanche » avant d'être autorisé à créer des blocs et donc à percevoir la monnaie nouvellement crée (si tant est que la monnaie en question ne soit pas pré-minée). Avantage : on est sur la configuration qui requiert le moins de matériel, problème : la décentralisation en prend un coup puisqu'il faut être « membre du club » pour avoir le droit de jouer. Le système peut donc être aisément corrompu si les membres du club le décide.

La proof of existence : jugée utopiste, voir carrément dangereuse, développée notamment dans la Théorie Relative de la Monnaie, la proof of existence consiste à distribuer uniformément la création monétaire entre tous les humains. Avantage : on ne trouve à priori pas plus égalitaire, problème : une majorité de gens ont des difficultés à intégrer la possibilité d'usage d'une monnaie qui apparaît magiquement chaque jour sur tous les comptes (« mais alors on ne fait rien et on a de l'argent ? » – « oui, comme le banquier en somme .. ») et, s'agissant d'une monnaie numérique, elle exclue de facto tous ceux qui ne sont pas équipés en matériel, connectés au réseau et disposant petit socle de compétences techniques (mais c'est le lot de toutes les cryptomonnaies). On note par ailleurs que l'égalité en prend un petit coup puisqu'il est impossible de compter sur le fait que l'ensemble de l'humanité ou même plus simplement d'un pays ou d'un département, s'y mette en même temps. Ceci dit, le principe de création monétaire permanente engendre un phénomène d'érosion de la valeur : sur le long terme, les « premiers arrivés » ne sont pas mieux servis que les derniers.

On parle, dans tous ces cas, de la façon de créer de la monnaie. L'enregistrement ultérieur des transactions peut fonctionner sur un autre principe

Par exemple, dans la June, la monnaie est crée quotidiennement par la preuve d'existence mais les transactions sont validées par la preuve de travail avec une difficulté adaptée à participant du réseau fonctionnant, pour résumer, selon la règle « le prochain bloc trouvé le sera par le nœud qui en a le moins trouvé ces derniers temps ». Comme il n'y a aucun enjeu financier à trouver un bloc, nul besoin d'installer une masse de matériel informatique colossale pour que ça fonctionne.

Truth is out there

Je considère que nous en sommes encore aux balbutiements de cet univers numérique et ce qu'il deviendra, ne serait-ce que dans 10 ans, sera, à mon avis, fort différent de ce que nous voyons aujourd'hui.

Je ne vois pas les gouvernements se laisser déborder par une monnaie non contrôlée. Ils vont par contre se faire un plaisir d'utiliser les principes de la blockchain pour finir d'abattre le concept d'argent liquide et renforcer la traçabilité des transactions financières.

Dans le même temps, tout un tas d'usages spécifiques et de niches vont apparaître pour tout un tas de cryptomonnaies. Ça pullule déjà dans tous les sens, et quelques unes surnagent, chacune avec ses avantages et ses inconvénients.

Je vois venir quelques jours sombres pour la stabilité de nos réseaux électriques, donc également des réseaux de communication, et par extension de cet univers des cryptos.

J'estime que les crypto sont, pour bonne part, une manière alternative de spéculer et, de plus en plus, pour certaines, un moyen de mettre quelques noisettes à l'abri (mais il ne faut certainement pas toutes les y mettre) ou de participer à des levées de fonds pour financer des choses.

J’aime pas mal l’esprit de la June, et j’en attends beaucoup, non pas tant pour le côté monétaire (je ne pense pas que le monde soit prêt pour le concept de dividende universel) que pour la tendance qu’elle a à créer du lien entre les gens et donc à faire foisonner les idées et leurs concrétisations.

Conclusion

Si vous épluchez le looooong thread (très ramifié) qui suit mon tweet, vous apprendrez plein de choses sur les cryptos, l’énergie, la sociologie et les turpitudes humaines. C’est long, mais ça vaut le détour, promis !