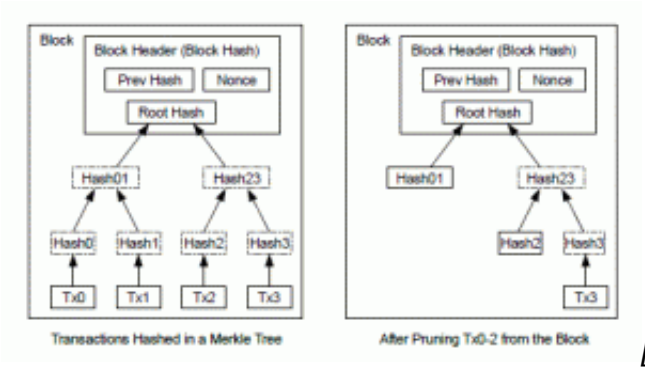
La banque et la désintermédiation



[j'avais fait figure d'early adopter lors de quelques articles sur la blockchain en 2013, j'ai continué à m'y intéresser entre temps, et avec tout ce qui bouillonne dans ce milieu qui n'est plus si petit que ça, ça vaut la peine de passer un peu de temps à faire le point. Full disclo : j'ai, bien malgré moi, plus de sous en cryptomonnaie que de sous à la banque à l'heure actuelle]

Si vous ne voulez pas vous taper beaucoup de littérature ni comprendre les fondamentaux techniques de la chose, il suffit de savoir que la blockchain permet de créer et d'échanger des bidules numériques. Là ou internet permettait jusqu'à présent de copier indéfiniment des choses (quand je t'envoie une vidéo de chatons, tu as la vidéo de chatons et je l'ai aussi : elle a été copiée), la blockchain permet, au travers du réseau, d'envoyer un bidule numérique d'une personne à une autre. Après l'envoi, le destinataire a le bidule numérique et l'émetteur ne l'a plus.

Cette possibilité ouvre des champs jusqu'à présent inexplorés. Lorsque ~~le secteur de la culture~~ l'industrie du divertissement a commencé à couiner que le peer2peer allait lui bouffer tout le gâteau parce que les gens ils achetaient plus les disques et préféraient pirater (scoop : c'est pas vrai), les banquiers se marraient, se croyant à l'abri, puisque le principe de base de l'argent, c'est que ça ne se copie pas. Ceux qui leur prédisaient le même sort étaient raillés.

Eh ben les copains, on y est.

Petit mémo sur ce à quoi sert une banque : non, elle n'est pas là pour garder des tonnes d'or bien au chaud dans ses coffres et faire circuler des pièces et des billets à la place (parce qu'un lingot d'or, ça pèse un kilo. En billet de 500, ça ne fait plus que 100 grammes .. c'est plus pratique à transporter, à échanger, à découper en petits morceaux). L'année prochaine, ça fera tout pile 50 ans que les dollars ne sont plus indexés sur l'or.

Une banque, c'est un bidule qui, aujourd'hui, sert à inventer des sous en échange de reconnaissances de dettes. J'ai l'impression de le dire 12 fois par semaine et donc j'ai tendance à croire que tout le monde le sait, mais non. Donc : l'argent que ta banque t'as filé pour acheter ta baraque ou ta bagnole, elle ne l'a pas sorti du livret A de ton oncle. Elle l'a inventé *pouf* comme ça. Quand tu rembourse, elle détruit l'argent *pouf* comme ça et se garde les intérêts dans le fond de la poche. Parce qu'elle peut. C'est le rôle que le monde entier leur a confié. Et cet argent fabriqué quand tu fais un crédit (enfin, pas que toi hein, le

gouvernement américain aussi) et détruit quand tu le rembourse, ça représente 95% du pognon en circulation dans le monde (à peu près hein, tout le monde n'est pas d'accord sur le chiffre, mais ce qui est certain c'est que c'est la majorité).

Quand on voit ce que certains états font à leur économie en faisant n'importe quoi, on peut se dire qu'il était finalement sage de confier ça au privé avec des règles strictes. (scoop : non, en fait, le privé, tout ce qui l'intéresse, c'est de se remplir la poche). En prime, on comprend bien aussi que, dans le système tel qu'il fonctionne actuellement, vouloir à tout prix résorber une dette (que ce soit la tienne perso pour ta télé 4K ou celle de l'état Français pour toutes les télé 4K des ministère), c'est un peu comme se tirer une balle dans le pied : s'il n'y a plus de dettes, il n'y a plus de pognon en circulation, du coup, on n'a plus d'outil pour échanger.

Mais du coup, maintenant, on a des cryptomonnaies. On n'a plus besoin de faire confiance à un banquier pour décider à quel rythme on crée le pognon et à qui on le file : on peut avoir un algorithme qui s'occupe de ça, selon des règles qu'on aura décidé à l'avance et avec lesquelles (à priori) personne ne peut tricher. Dans certains cas on peut même voter pour changer l'algorithme en cours de route (toujours selon des règles précises et connues à l'avance).

Mais vous verrez plus loin que c'est même pas grave pour le banquier : on a toujours besoin d'eux pour d'autres choses.

> Ah ouaaais, j'te vois venir, tu va conseiller à tout le monde de vider son compte en banque pour acheter des bitcoins et devenir millionnaire à noël prochain ! Mais c'est trop tard, c'était en 2010 qu'il fallait faire ça !

Mmmmhh ouais, je pourrais faire ça, et mettre quelques liens d'affiliation dans l'article pour gagner des sous ! En plus, si ça s'trouve, c'est pas impossible que ça arrive (les liens d'affiliation dans mes articles *et* le fait de devenir millionnaire en achetant quelques bitcoins aujourd'hui)

Non, je ne me fais pas chier à pondre un article pour parler de (et encore moins encourager) la spéculation. Oui, les cryptomonnaies, en tout cas les plus grosses, ça valse dans tous les sens et c'est clairement pas l'idée du siècle que de conseiller à mamie d'y placer son bas de laine. Par contre, ça peut être une bonne idée d'en avoir un peu sous le coude … Non pas dans l'espoir que leur valeur soit multipliée par 10 après demain, mais surtout pour prendre un peu l'habitude de les manipuler et pour en avoir un peu à dépenser si jamais on n'a plus d'euro, qu'il se met à ne plus rien valoir ou que la banque nous interdit d'y accéder.

> Ouiiii mais c'est de la merde, ça consomme des gigawatts pour rien, mon oncle y me l'a dit à noël !

Alors oui et non. Il ne faut pas confondre blockchain (la technologie de stockage de l'information), les cryptomonnaies (une application donnée de la blockchain), et le bitcoin (la

première cryptomonnaie .. il en existe des milliers aujourd'hui)

Oui, le bitcoin consomme beaucoup d'énergie. Non pas pour « faire des calculs très compliqués destinés à sécuriser la blockchain », mais pour réguler la création monétaire : comme c'est celui qui a le plus gros flingue qui a la plus grande probabilité de trouver le prochain bloc de la chaîne, et comme, dans le bitcoin, la monnaie est crée *pouf* comme ça par chaque bloc, tout le monde essaie d'avoir la plus grosse pour trouver le prochain bloc et toucher les nouveaux sous. Du coup, plus ça va, plus il y a de la puissance dispo pour trouver des blocs.

Corollaire, la probabilité d'en trouver plus vite augmente. Mais comme le protocole prévoit un bloc toutes les 10 minutes en moyenne, l'algorithme diminue la probabilité de trouver des blocs (augmente la difficulté) à mesure que la puissance mise à disposition augmente. On parle de « preuve de travail » : le calcul compliqué qui est effectué n'a aucun but de sécurisation mais sert simplement à prouver qu'on a tout un bordel de matériel qui tourne, qui coûte fort cher, et que donc on est quelqu'un de bien en qui on peut avoir confiance pour écrire le prochain bloc.

Si tous les gens qui créent des blocs de la chaîne bitcoin se mettaient d'accord pour n'utiliser chacun qu'un iphone 3 (la blague pourrait peut être même marcher avec un 486DX2 pour les plus âgés d'entre nous), bitcoin pourrait fonctionner en ne consommant que quelques kilowatts en tout et pour tout. Mais l'avidité humaine l'interdit. Et puis il faudrait aussi un peu de stockage, la blockchain bitcoin pesant aujourd'hui un peu plus de 260Go.

Du coup, d'autres cryptomonnaies ont une création monétaire qui fonctionne autrement. Quitte à considérer que c'est celui qui a la plus grosse (et donc le plus riche) qui touche les nouveaux sous, ne pourrait-on pas imaginer de zapper l'étape « calcul compliqué » pour dépenser moins d'énergie ? C'est le principe de la « preuve d'enjeu » : la probabilité de trouver le prochain bloc n'est plus liée à un calcul mathématique mais à la quantité d'argent qu'on a bloqué dans la chaîne en guise de bonne foi. La seconde cryptomonnaie du marché (Ethereum) va passer d'un fonctionnement « preuve de travail » à un fonctionnement majoritairement « preuve d'enjeu » dans les quelques années à venir.

Mais ce n'est pas tout. Il existe aussi (au moins) une cryptomonnaie qui repose sur la confiance humaine pour autoriser la création des blocs (« j'ai été reconnu par plusieurs humains comme étant également humain et digne de confiance, une machine à qui je confie ma clé privée a donc le droit d'écrire des blocs dans la chaîne en mon nom ») et qui, surtout, décorrèle totalement la création de la monnaie de la création des blocs. Dans le cas de la June, première et seule (à ma connaissance) cryptomonnaie libre, la monnaie est crée chaque jour au premier bloc qui suit 13h00 et est attribuée de façon égalitaire à l'ensemble des humains identifiés comme digne de confiance par au moins 5 autres humains, qu'ils fassent tourner une machine qui trouve des blocs ou pas (en réalité c'est un brin plus compliqué que ça, mais vous vous renseignerez vous même sur la monnaie libre si le cœur vous en dit).

Il existe un tas colossal de cryptomonnaie dont l'ensemble de la masse monétaire existe déjà entièrement et qui sont distribuées selon des tas de critères (c'est notamment ce type de cryptomonnaie qui permet de faire des levées de fonds. Les jetons monétaires représentent en

réalité quelque chose qui s'approche du concept d'une action d'une entreprise, l'entreprise en crée un gros tas à l'instant T, en vends une partie à qui veut en acheter contre argent sonnant et trébuchant (comme une introduction en bourse, donc), puis on peut ensuite s'échanger ces jetons directement d'une personne à une autre sans passer par un intermédiaire financier, ce qui dicte la valeur des jetons en question.

Et enfin, on trouve les « stablecoin » qui sont spécifiquement crées pour avoir une valeur à peu près stable qui correspond à une valeur qu'on va retrouver dans le monde réel. On trouve par exemple 3 ou 4 stablecoins serieux qui sont stables par rapport au dollar US. Le principal problème de ces stablecoins, c'est que c'est une entreprise privée qui assure et garanti leur valeur. Si l'entreprise fait faillite et/ou que son patron se tire avec la caisse, pouf, vos économies s'envolent (les jetons existent toujours et sont en votre possession, mais plus personne n'en voudra : ils n'ont plus de valeur). Un peu comme quand des banques ont disparues en 2008, si vous vous souvenez bien, ou un peu comme quand il faut une brouette de billets pour acheter une baguette.

Ça pourrait ressembler à une blague, mais il existe des stablecoin aussi variés que celui qui réplique la valeur de boites de sardines de collection (que vous pouvez à tout moment échanger contre des sous ou … une boite de sardine) ou bien qui réplique la valeur d'une entreprise mexicaine qui cultive de l'agave (avis aux amateurs de tekila)

Tout ceci existe déjà et fonctionne. Et pas que « pour jouer ». Ces 24 dernières heures, plus de 12 milliards de dollars se sont échangés via l'USDT (le plus volumineux des stablecoin indexé au dollar US). Il serait bon que nos élus français et européens se saisissent du problème : si aucun stablecoin garanti par la banque centrale européenne n'est crée, l'ensemble de l'économie risque de dériver lentement mais sûrement vers du tout privé et géré par des gens potentiellement bien pire que des banques (certains on peut être entendu parler du projet Libra, porté par Facebook … perso, je préfère encore la BNP !)

Ceci étant, l'algorithmie n'a pas dit son dernier mot. Vous l'aurez compris, les cryptomonnaies non volatiles existent mais souffrent du fait qu'elles sont garanties par un tiers qui, s'il n'est pas à proprement parler une banque, joue quand même un rôle capital dans l'histoire et se doit de pouvoir échanger les jetons de stablecoin contre des vrais devises, actions, objets ou services (et donc de les avoir en compte / stock). Eh ben quelques furieux ont crée un stablecoin indexé sur le dollar US qui ne nécessite ni tiers de confiance ni stockage de la devise qui sert d'index (on parle de « collatéral »). Il possède d'autres défauts, mais on voit bien qu'on est loin d'avoir atteint la limite en terme de créativité dans ce domaine.

> Mouaaais bon ok je vais p'tet voir à jouer un peu avec pour pas avoir l'air trop con à noël prochain. Mais mon oncle y m'a aussi dit que les frais de transaction étaient super élevés … Moi j'veux bien mettre 100 balles pour apprendre comment ça marche, mais si y faut que je paie 70 balles pour jouer avec 30 et récupérer 2 à la fin, ça m'intéresse pas. Et puis d'abord, qui les touche, ces frais de transaction, puisque tu nous bassine en disant que y'a pas d'intermédiaire ?

Alors oui, fut un temps, une transaction, notamment en bitcoin, ça pouvait coûter fort cher. Je ne vais pas rentrer dans les détails du calcul des frais de transaction et de l'impact que ça a sur la vitesse de traitement, mais pour faire simple, les transactions étant écrites dans des blocs, c'est celui qui trouve le bloc ou ta transaction est inscrite qui va toucher les frais de transaction (pour lui dire encore plus merci que juste en lui donnant les nouveaux sous que le bloc a crée). Comme certaines cryptomonnaies (le bitcoin par exemple) ont une taille de bloc maximale définie et qu'il y a beaucoup de transactions, celui qui trouve un bloc doit parfois faire le choix de ne pas y inscrire telle ou telle transaction (qui restera donc en attente en espérant qu'un bloc suivant l'embarque). L'avidité fait donc tout naturellement que lorsqu'on est prêt à payer des frais élevés, on est quasi sûr d'avoir une transaction validée rapidement.

Ceci dit, avec 90% des blocs crées totalement pleins (et donc des transactions en attente possiblement de façon perpétuelle), j'ai dernièrement réalisé des transactions bitcoins à 5 ou 10 centimes de frais qui sont passés en moins d'une demi heure. Ce n'est pas encore idéal pour régler son café au bar, mais certaine cryptomonnaie ont un rythme de création de blocs beaucoup plus rapide (l'ethereum voit un bloc crée toutes les 12 secondes en moyenne et ma transaction de ce midi d'une valeur d'en gros 100$ m'a coûté 4 centimes .. soit quelque chose comme 1% des frais mensuel de tenue de compte dans une banque, donc de quoi faire trois transactions par jour pour un prix équivalent)

Certaines cryptomonnaies ont aussi des frais de transaction très légers, voir nulle (la monnaie libre, par exemple, puisque dans ce cas, il n'y a aucun gain financier prévu dans la blockchain quand on met à disposition du matériel chargé de trouver des blocs)

> Et le banquier dans tout ça ? Si on lui retire son privilège de création monétaire (que ce soit pour cramer des gigawatts avec bitcoin ou pour faire ça beaucoup plus intelligemment avec de la monnaie libre), il lui reste quoi ?

Si vous avez tout bien suivi, vous avez compris qu'avoir des cryptomonnaies, c'est comme avoir des sous au fond de votre poche. L'autre utilité du banquier, en dehors de vous prêter de l'argent qu'il a fait apparaître comme par magie, c'est de garder vos sous dans un endroit ou on vous les piquera pas quand vous dormez (dans une base de donnée, en fait). Il existe plein de moyens plus ou moins sûr de mettre à l'abri vos cryptomonnaies, mais pour une adoption grand public, il y aura sûrement des gens qui auront plus confiance dans un banquier que dans leurs propres capacités, ne serait-ce que parce que même si c'est assez simple, la manipulation de cryptomonnaies requiert un peu de manipulation technique qui peuvent rebuter.

Et puis même s'il y a aussi des algorithmes pour ça, un banquier pourrait toujours effectuer des prêts (pas avec de l'argent sorti de nulle part, du coup) en servant de tiers de confiance entre les prêteurs et les emprunteurs (et en étant rémunéré pour ça, sisi !)

Bref, c'est encore un secteur qui va se faire disrupter de gré ou de force. Voilà ce qui arrive quand on a la startupnation, Manu ! :)

PS : je ne mettrais pas de liens d’affiliation, mais si tu veux m’envoyer des brouzoufs une fois que t’aura joué avec des cryptomonnaies, t’as le choix :

- De la monnaie libre ?1 : CGnyAAKDSKDp5KUTCxd1mGp6Vp5SjH5TgSxA8GBdCioz
- De l’ethereum : 0x2F14003D82eC035a0878009F67ca1DEEF492aFEc
- Du bitcoin : 3KEgsnXRN2V5o8T92YJ1JhxqQDX8Kk8JA7