Mais alors, la blockchain, c'est quoi ?

Basiquement, c’est une sorte de grands livres de transactions sous forme encryptée. L’innovation réside dans la présence de ce registre. **De centralisée à distribuée**. C’est-à-dire ?

Aujourd’hui, lorsque l’on veut effectuer un virement au propriétaire de notre appartement (par exemple), on fait la demande à notre banque, qui va enregistrer cette demande, la transmettre à la banque de mon propriétaire et mettre à jour le solde de mon compte en déduisant ce virement. Ces données bancaires, j’y ai certes accès depuis mon ordinateur, mais *in fine* c’est la banque qui les stocke et qui détient le contrôle total sur elles. La banque est ici ce que l’on appelle un **tiers de confiance**. Mais tout le point qui présida à la naissance du bitcoin, c’est qu’avec la crise des subprimes en 2008 et la rupture de liquidités de nombreuses banques qui s’en est ensuivie, c’est précisément **cette confiance en des tiers qui s’est retrouvée considérablement touchée.**

La blockchain est venue apporter un remède à cette centralisation des transactions, en apportant par l’intelligence artificielle (puissance de calcul des ordinateurs) **la possibilité de sécuriser et authentifier les transactions pair-à-pair tout en fournissant une donnée pérenne, infalsifiable et distribuée**. Comment ? On ne rentrera pas trop longtemps dans la technique, promis !

Deux personnes veulent passer une transaction sur un réseau blockchain. Elles s’accordent sur les termes de l’échange et demandent au réseau de valider la transaction. Celui-ci va d’abord *hasher* l’information, c’est-à-dire la crypter. Les autres participants au réseau ne verront que cette version cryptée (qui, empiriquement, n’a jamais été déchiffrée), mais le réseau (en tant qu’algorithme) gardera en mémoire les changements de soldes respectifs des deux comptes ayant échangé. Mais avant que ce bloc ne soit accepté, il va falloir lui ajouter une **« preuve de travail»**. Concrètement, il rajoute au hash initial d’autres caractères, qui une fois traduits en binaire doivent remplir une condition (c’est-à-dire un certain nombre de 0 consécutifs). Trouver cette preuve requiert une très grande puissance de calcul : avec un ordinateur de bureau, elle prendrait quelques milliers d’années à être trouvée. D’où le recours à des ***mineurs***, c’est-à-dire pleins d’usagers du réseau qui mettent la puissance de calcul de leurs ordinateurs respectifs en concurrence pour trouver au plus vite cette preuve de travail.

Cela prend généralement une dizaine de minutes pour le réseau bitcoin mondial. Ensuite l'heureux gagnant sera rémunéré en crypto-monnaie. C'est ce point qui rend l'information **infalsifiable** : quelqu'un qui voudrait modifier les informations d'un bloc devrait calculer une nouvelle preuve de travail, ce qui changerait l'intégralité du codage du bloc (pas seulement la partie « preuve »). Or, chaque bloc comprend une petite partie du code du bloc précédent. Ainsi, le fraudeur ne devrait pas seulement retrouver une preuve de travail pour le bloc qu'il veut modifier, mais bien rattraper toute la chaîne qui suit … et ce juste avec sa propre puissance de calcul puisque les mineurs sont mis à contribution par le réseau uniquement pour la chaîne principale (c'est-à-dire celle sans fraude). C'est impossible.

Donc une fois cette preuve de travail fournie, le bloc est ajouté à la chaîne et stocké, non pas sur un serveur central, mais sur tous les ***nœuds du réseau***, c'est-à-dire l'ensemble des ordinateurs participants. L'information est donc effectivement **distribuée**.
Enfin, l'information sur les transactions est **pérenne** puisque l'ensemble de la chaîne est stockée sur tous les nœuds du réseau : un ordinateur et sa carte mémoire qui grillent n'enlèveront pas l'information de cette planète, puisqu'elle est stockée à l'identique sur nombre d'autres ordinateurs.
Voilà donc comment fonctionne basiquement la blockchain, et avec quel but :

Décentraliser les transactions en fournissant un système d'authentification, sécurisation et stockage des données pérenne, infalsifiable et distribué