Comprendre les concepts de base.

Pourquoi les blockchains ?

Lors d'une transaction traditionnelle entre deux personnes **d'une même banque**, la banque joue le rôle de tiers de confiance sur le fait que l'émetteur dispose des fonds, que les fonds aient bien été transférés et qu'il n'y a pas eu de **double dépense**. Pour ce faire la banque dispose d'un registre, **en anglais « ledger »**, avec la liste des comptes de ses clients, la somme d'argent disponible sur chaque compte etc. Le compte d'un client est lui-même un registre avec la liste de ses dépôts, retraits et dépenses, à qui, quand, combien, pourquoi etc. On peut donc dire que les comptes des clients sous des sous registres du registre de la banque.

Admettons maintenant que les deux personnes ne fassent pas partie de la même banque. Il faut alors que les deux banques commerciales fassent elle-même confiance à un tiers « supérieur », tel que celui de la banque de France, qui elle dispose des balances commerciales des deux banques.

Et si ces deux personnes se trouvent dans deux pays différents de la zone euro ? C'est la même chose mais avec la BCE qui agira en tiers de confiance entre les deux banques nationales.

Et si ces personnes se trouvent dans deux pays différents ? Ca se complique…

Mais sans aller plus dans le détail pour le moment, ce qu'il est important de comprendre ici c'est que l'économie actuelle est ordonnée sous la forme de registres (**Ledgers**) et de sous registres et que pour toute transaction entre deux personnes ou deux entités, un tiers de confiance est requis.

Du fait que l'on doive faire appel à un organisme central, ce système est dit centralisé.

La technologie des blockchains a été inventée dans le but de permettre à deux personnes de pouvoir se transférer de l'argent sans devoir faire appel à un tiers, telle qu'une banque.

Une blockchain garantit donc de façon décentralisée ce que les banques garantissent de façon centralisée.

- L'émetteur dispose des fonds
- Les fonds ont bien été versés
- La transaction est signée
- Il n'y a pas eu de double dépense

Dans un écosystème décentralisé, il existe plusieurs centaines voire milliers de validateurs sur le réseau. Ils doivent se mettre d'accord pour valider ou non une transaction. Tout d'abord, le solde de tous les comptes de la blockchain est connu de tous (vous, moi, tout le monde…), sans que l'on sache à qui ils appartiennent, ce ne sont que des numéros. Dès lors que des transactions sont demandées, elles sont enregistrées dans l'ordre chronologique par chaque validateur dans un fichier temporaire. Quand le fichier est plein elles sont enregistrées dans un nouveau bloc, bloc qui est ensuite soumis à la l'aval de tous les validateurs. Si tout le monde est d'accord le bloc est ajouté à la chaîne de façon irréversible.

Suivant la blockchain, le mécanisme de validation d'un nouveau bloc peut changer. Il en existe principalement 3. Le Proof of Work (PoW), le Proof of Stake (PoS) et le Proof of Consensus (PoC).

Si vous souhaitez aller un peu plus loin je vous invite à consulter la chaîne Youtube de Cryptoast. Ils expliquent par exemple très bien le Proof of Work dans cette vidéo : https://www.youtube.com/watch?v=6uYRN6b5EMU

Ce qu'il faut retenir

- Une blockchain est un registre ouvert à tous regroupant toutes les transactions ayant eues lieu depuis son commencement sous forme de blocs.
- Ce registre est inaliénable. On ne peut pas modifier un bloc après qu'il ait été ajouté à la blockchain.
- Les blockchains sont décentralisées dans la mesure le mécanisme de validation ne repose pas sur une entité centrale mais sur tous les acteurs, ou « nœuds » de la blockchain. 1 seule personne ou entité ne peut donc pas modifier ou cacher le contenu.
- Il existe plusieurs mécanismes de validation des blocs. PoW, PoS, PoC.

Enfin pour qu'une modification puisse être faîte sur une blockchain il faut que plus de 51% des « nœuds » s'accordent sur la modification. C'est démocratique. Si ladite blockchain est vraiment décentralisée, une entité malveillante (institution, personne, pays etc.) ne peut pas le faire. Sans rentrer encore trop dans le détail la Chine détient plus de 60% des validateurs du Bitcoin. Elle peut donc théoriquement inverser une transaction. Le Bitcoin a bien été conçu pour être décentralisé, mais son mécanisme de validation des blocs reposant sur la puissance de calcul, c'est à celui qui a le plus de puissance que revient le pouvoir. Sans même parler écologie et consommation d'électricité, c'est à mon sens un gros défaut de toutes les cryptomonnaies basées sur le Proof Of Work (ou PoW). Tout le monde n'est pas d'accord avec ça, à chacun de se faire son avis.

Investir dans les blockchains c'est donc promouvoir une technologie qui rend le pouvoir à la communauté et **qui permet de devenir sa propre banque**, rien que ça. Mes économies sont dans mon tiroir, et je peux envoyer de l'argent 7 jours sur 7, 24h sur 24, sans frais ou presque, à n'importe qui sur la planète, en quelques secondes. Essayez d'envoyer 100 euros à votre cousin au Chili avec votre banque. Bon courage ! 😉

Mais alors, pourquoi il y en a 9000 ?!

Pour simplifier au maximum comparez une blockchain à un train. Suivant le wagon on peut y mettre des passagers, des voitures, du gaz, des céréales etc.

Les blockchains c'est un peu la même chose. Au moment de la conception de la blockchain les développeurs se penchent sur un problème et essaient de le résoudre. Suivant le problème on n'y mettra pas les mêmes informations. Quelques exemples :

- Un passeport vaccinal, c'est d'actualité. Il faudra un n° de sécurité sociale, une date, le nom du médecin ayant fait l'injection etc.
- Dépôt des brevets : Qui ? quelle invention ? quand ? des plans de l'invention etc.
- Vote : Qui, quand, pour qui, où ?

➔ Souvenez-vous : inaliénable, public et décentralisé. Vous commencez à imaginer les possibilités ?

Mais méfiez-vous, énormément de blockchains aujourd'hui n'ont pas d'utilité, de cas d'usage. Pire, certaines sont juste des arnaques. Exemple : Le fondateur la crée, s'octroie une grande quantité de token, fait de la publicité mensongère, les gens en achètent, euphoriques, et le fondateur vend tout ce qu'il a à prix d'or. (#Sushicoin).

D'où l'importance de faire ses propres recherches !