

# Comprendre la blockchain Bitcoin

# Histoire de la blockchain 1/2

- En 2008 suite à la crise financière, un cipherpunk ou un groupe de cypherpunk nommé Satoshi Nakamoto, excédé par la bêtise de la finance ‘moderne’ décide de créer une monnaie pair à pair.
- La règle de la monnaie pair à pair veut que l’émission soit contrôlée par le code.

# Histoire de la blockchain 2/2

- Satoshi Nakamoto a alors écrit son livre blanc disponible sur [bitcoin.org](https://bitcoin.org)
- Dans ce livre blanc il n'existe aucune mention de blockchain.
- La définition exacte se situe dans le terme ‘serveur d’horodatage distribué pair à pair’.
- En utilisant ce système Satoshi Nakamoto résout le problème principal d'une monnaie numérique qui est la double dépense.

# La notion de tiers de confiance

- Avant les blockchains, la notion de tiers de confiance était nécessaire dans les échanges monétaires pour éviter le principe de double dépense (banques, banque centrales, états, notaires, ...)

# La capacité de faire confiance à un tiers en question

- De nos jours pouvons nous encore faire confiance à nos institutions?
- La réponse doit rester personnelle mais quelques exemples :
  - Les camionneurs canadiens ont vu leurs comptes bancaires gelés pendant la crise du covid lors de leurs manifestations
  - Wikileaks s'est vu subir un embargo de Mastercard & Visa, ils ne pouvaient plus recevoir de dons.
  - Tout récemment, un homme qui disposait de 400 000 euros en liquide chez lui s'est vu se les faire confisquer par le trésor public, sous prétexte de ne pas pouvoir justifier de ces fonds.
  - N26 qui ferme les comptes bancaires sans rendre l'argent ...

# Couvrir des activités illégales avec les cryptos ?

- L'un des principaux arguments des cryptophobes se situent sur les activités illégales de type de blanchiment d'argent. Ce point n'est pas à nier. Mais on parle souvent d'anonymat dans les cryptos ce qui est faux.
- Nous devons parler de pseudonymat, en effet toutes les transactions sont stockées dans la blockchain et chaque adresse représente un compte 'bancaire'. Lorsque l'on utilise une plateforme d'échange nous devons nous authentifier par un KYC. Certaines vérifications sont plus poussées que certaines banques (Revolut ou N26 par exemple).
- L'une des activités de blanchissage d'argent les plus connues du moment sont les NFT, il y a encore quelques mois les NFT étaient considérés comme de l'art et soumis à une taxe faible pour son créateur (6%). Donc il suffisait de faire un gif de le poser sur la blockchain et le tour était joué vous êtes un artiste à succès aux yeux de l'état.
- Toutefois le blanchiment d'argent sale est toujours majoritairement effectué en \$ US

# Bitcoin, bitcoin ?

- Le Bitcoin désigne la technologie
- Le bitcoin désigne la monnaie
- Une simple histoire de majuscule.

# En quoi le bitcoin peut il avoir une valeur 1/2?

- La premiere chose à savoir est que bitcoin est divisible, jusqu' a  $10^{-8}$
- Sa plus petite unité est le satoichi. Donc  $100\ 000\ 000$  sat = 1 bitcoin.
- Sa quantité est définie à l'avance il n'y en aura que 21 millions. Le dernier bloc rémunérateur pour les mineurs devrait être miné aux alentours de 2140.
- Les autres monnaies tels que nous les connaissons sont ‘imprimable à l'infini’
- 



BRRRRR (même très connu des maximalistes du bitcoin)

# En quoi le bitcoin peut il avoir une valeur 2/2?

- Le transfert de valeur est extrêmement rapide quelque soit la région, le pays, le continent. Un virement bancaire international peut mettre plusieurs jours.
- Les frais de transferts sont toujours plus compétitifs en terme de temps, mais parfois plus élevés en terme de tarifs. ( Plus de 20euro de banque a banque a l'international et parfois plus de 15 jours)

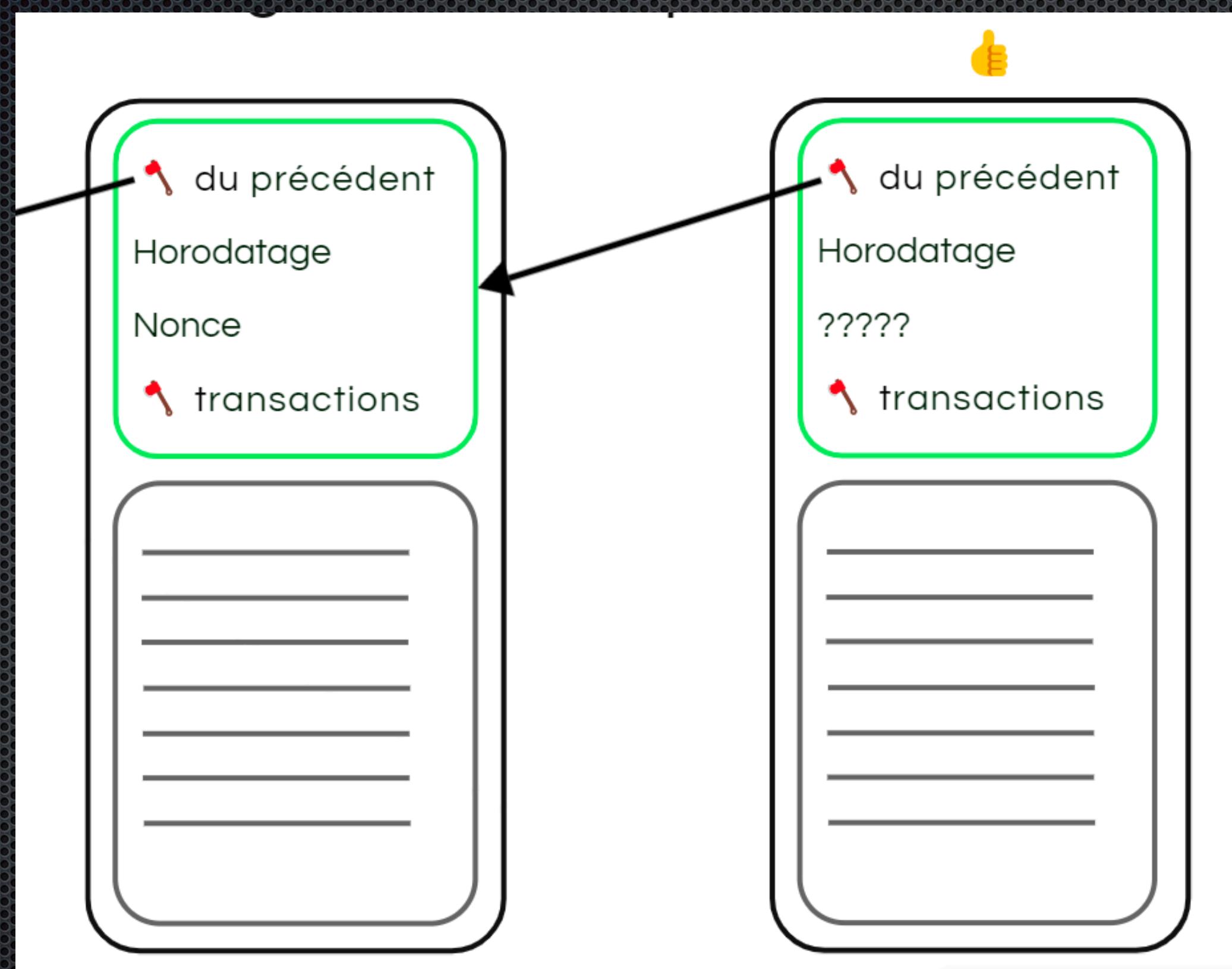
# Bitcoin l'or numérique?

- Souvent comparé à l'or, le bitcoin serait un or numérique:
  - Car nous le minons technologiquement (rigs de minage), grace à ce genre de machines
  - Il fait office de réserve de valeur(selon moi, mais peut être considéré comme trop volatile pour d'autres).
  - Contrairement à l'or celui ci n'a pas été encore testé sur des milliers d'années comme monnaie d'échange réserve de valeur.

# Le minage ?

- L'algorythme protégeant bitcoin est le sha256.
- Le minage sert avant tout à sécuriser les transactions qui ont été émises par les utilisateurs et les stocker finalement dans un block. Une fois ce bloc validé il sera immuable.
- Chaque bloc est dépendant du précédent si quelqu'un venait à modifier le bloc précédent pour alterer la blockchain, celui ci serait considéré comme invalide. Et au final si quelqu'un arrivait à modifier un block il faudrait une puissance de calcul incroyable car cela nécessite d'avoir 51 % de la puissance de calcul du réseau bitcoin.
- Explication technique du minage : <https://www.youtube.com/watch?v=3IFPqYZqlG0>

# Composition un block :



# Demos d'une blockchain

- Calcul de hash : <https://andersbrownworth.com/blockchain/hash>
- Une blockchain de test : <https://blockchain.nambrot.com/>
-

# Proof of ?

- Proof of work : preuve de travail, les mineurs valident les transactions (exemple bitcoin ravencoin dogecoin, ...)
- Proof of work : Les serveurs ayant un certain nombre de tokens de la blockchain valident les transactions (ethereum, Matic, ...)
- Proof of authority : maintenu par une autorité comme Binance, crypto.com... Qui permettent de piloter leurs propres blockchains.