Les Cryptomonnaies et les NFT

Emmanuel Jeannot et Damien Robert

Unithé ou Café

5 juillet 2022

Comment faire? Exemple d'une caisse partagée

Registre (fichier partagé)

Paul verse 20€

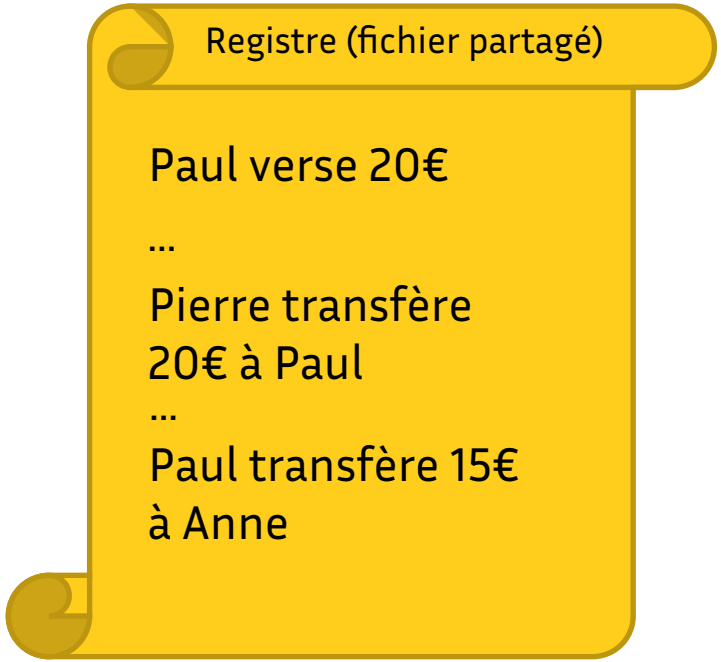
ère 15

0€

Problème résolu?

Connaître le solde d'une personne

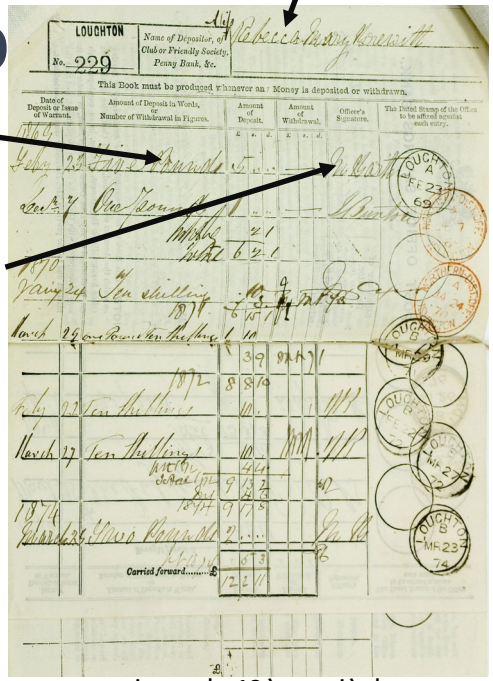
Il suffit de regarder l'historique des transactions



Empêcher une personne d'écrire n'importe quelle transactio

Le tiers de confiance : signe les transactions

Et si on a pas de tiers de confiance?



registre du 19ème siècle
Customer book deposit
(Wikipedia)

Un peu de cryptographique asymétrique

Propriétés de la signature cryptographique :

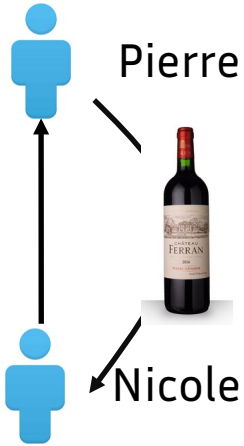
-Seule la clé publique peu **valider** un texte qui a été signé par la clé privée correspondante **(authentification)**

-Si le texte est modifié la validation échoue **(intégrité)**

-Seule la clé privée peut **signer** un texte qui sera validé par la clé publique correspondante **(non répudiation)**

Signature du registre

Nicole signe sa transaction:
-Non-repudiation
-Autentification
-Intégrité

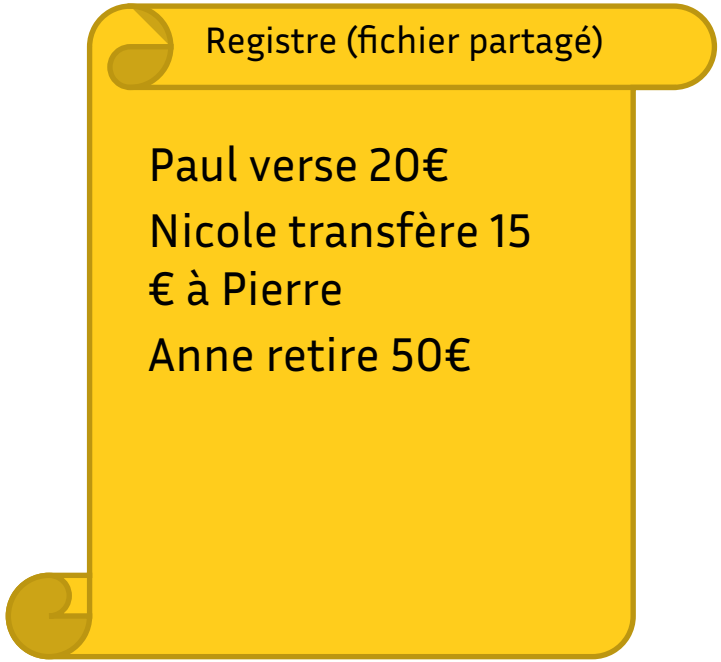


Registre (fichier partagé)

Nicole transfère 15 € à Pierre ; qàU4hduz7!
n

Un système centralisé

Quels sont les problèmes liés à un système centralisé ?



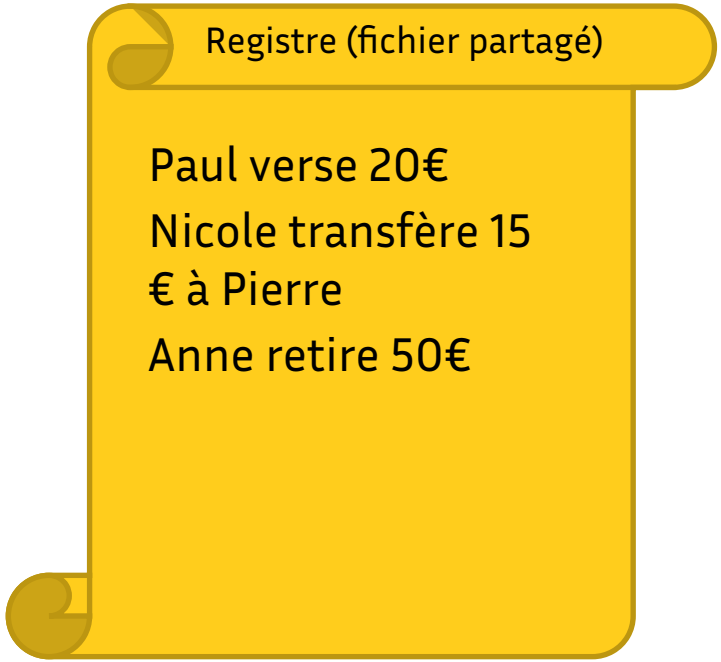
Un système centralisé

Avoir un seul registre pose un problème de centralisation :

-Quelle confiance?

-Quelle résistance aux pannes?

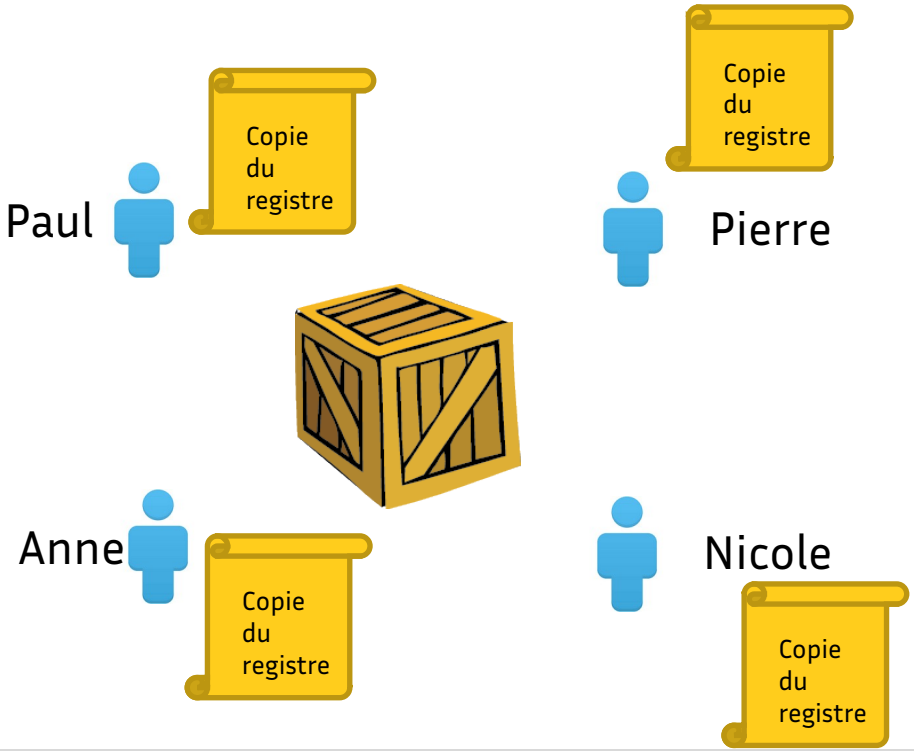
-Quelle résistance aux attaques?



Un système décentralisé

On distribue une copie du registre

Quels sont les problèmes liés à un système décentralisé ?



Un système décentralisé

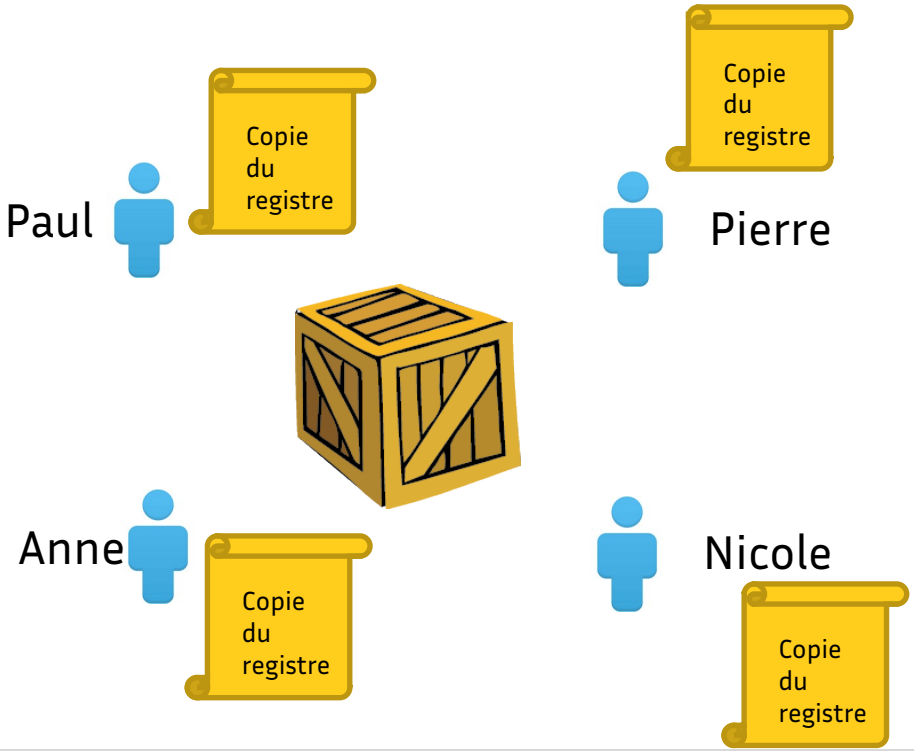
On distribue une copie du registre

Pb :

- comment être sûr que tout le monde possède **la même copie**?

- Comment tout le monde se met d'accord sur le contenu du registre (consensus?)

Comment resister aux attaques ?

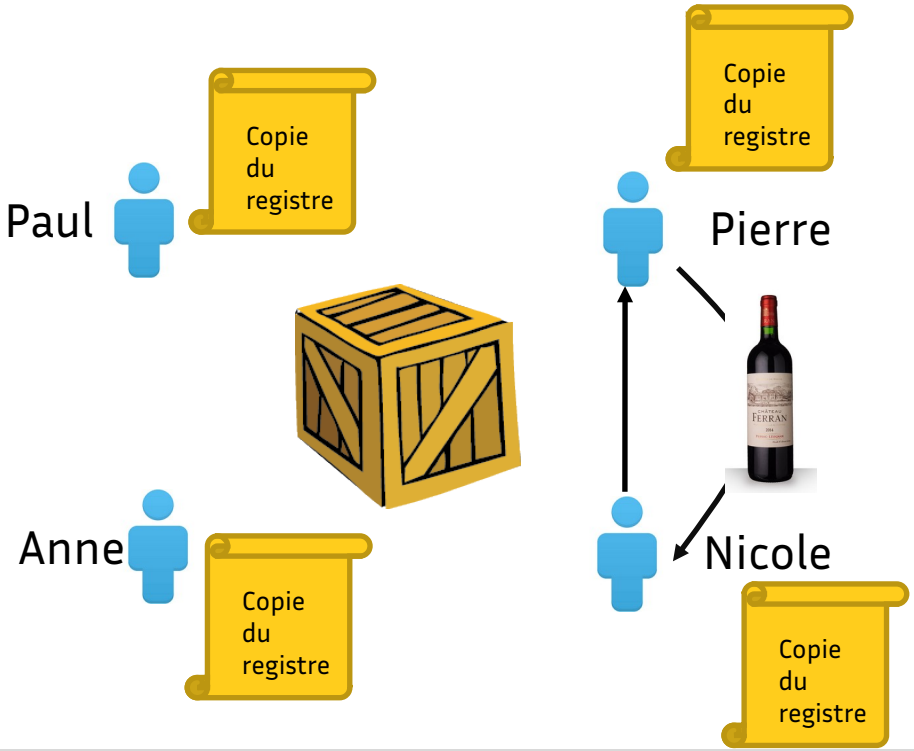


Diffusion des transactions

- **Nicole diffuse sur le réseau: “Nicole transfère 15 € à Pierre ; qàU4hduz7!n”**
- **Chacun ajoute cette transaction à son registre**

Problème :

- **Ordre des transactions**
- **Quelqu’un peut avoir manqué la diffusion**

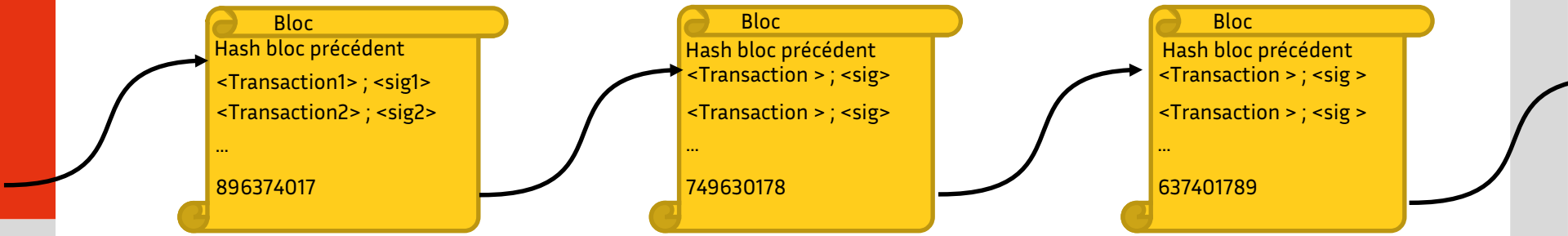


Solution 1 : le consensus majoritaire

- On garde en mémoire toutes les transactions dans le registre : nécessaire pour savoir quelle transaction a été prise en compte
- Les transactions validées sont celles qui sont présentes dans la majorité des noeuds.
- Pb : pour Bitcoin, le registre fait 390GB et il y a environ 50000 nœuds…
- Vérifier rapidement que les registres sont les mêmes ?

  Fonction de hachage !
- Sha256 ‘inria’ : a453e547985b58162cef59f13ed9a70dbfa3db0ea5eb604914886841890e69d7
- Sha256 ‘Inria’ : eaa1add8592f0e71604e031b90d2b39e581777ef5a0f7d631ecb7ac184d9709c

Du registre à la chaîne de blocs



”Impossible”:

-Changer l’ordre des blocs

-Changer une transaction

Le (hash du) dernier block suffit à valider toute la chaîne !

Consensus sur l’ajout d’une transaction (attaque des clones)?

Solution 2 : Preuve de travail

J'ai trouvé un nombre spécial tel que :

-Ajouté à la fin du registre

-SHA256 (registre) : commence par 30 zero.

-1/2^30 ~ 1/10^9 chance de trouver le bon nombre

-Donc j'ai du essayer environ 1 millard de nombres

-Mais c'est facile à verifier : tout le monde peut le faire en appliquant SHA256

-Si on change/ajoute une transaction, il faut refaire le travail

-Le travail est rémunéré !

-Consensus : chaîne de bloc la plus longue

Critique de la solution

Nombre de transactions par secondes

Bitcoin :

- 1 bloc toutes les 10 minutes (600s)
- 1 bloc : 2048 transaction en Moyenne
- Donc : 2048/600 ~ 3,4 transaction par seconds (tps)

=> Actuellement 10 000 000 transaction par mois = 3,85 tps

Carte bancaire/swift :

- CB en France 400 tps
- Visa (monde) : 1700 tps (maximum entre 24 000 et 54 000)
- SWIFT : environ 400 tps (2019)

Délais d'une transaction

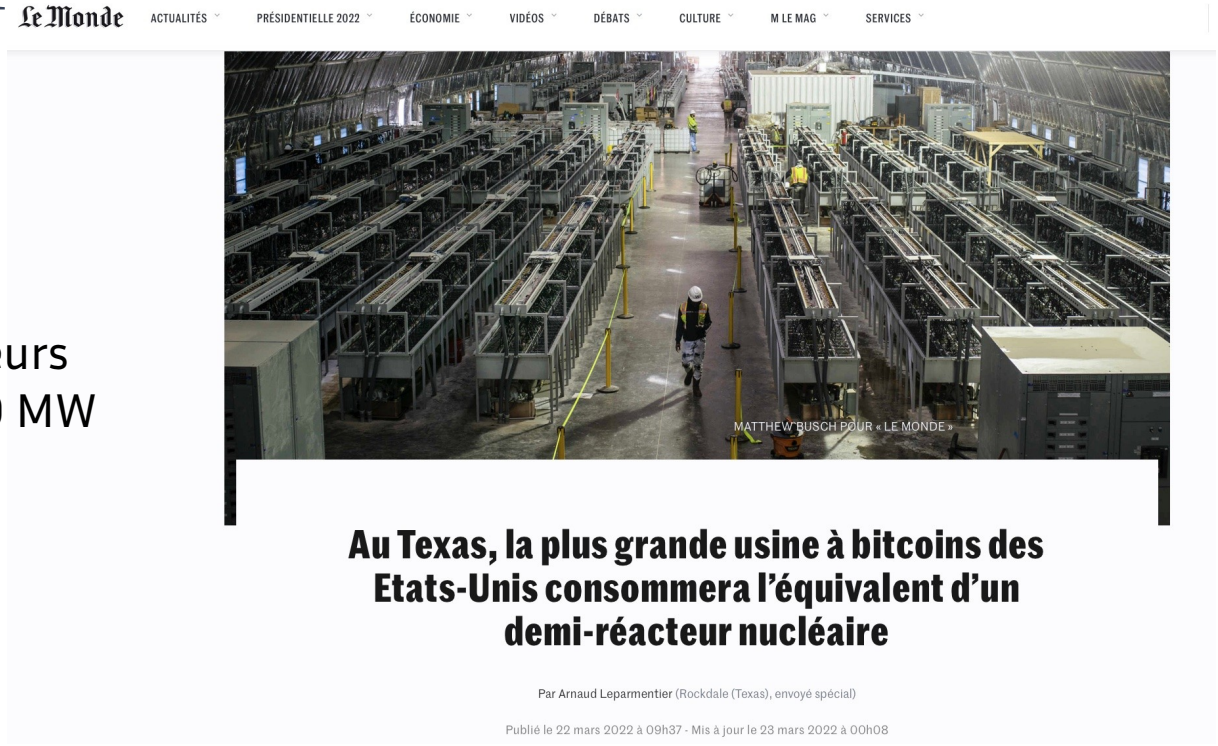
- Il faut attendre plusieurs blocs pour être sûr que la transaction va rester dans la châine : 6 blocs * 10 minutes ~ **1 heure d'attente**
- **SWIFT : 24h**
- **CB : quelques secondes**

Coût énergétique

- 50 à 150 TWh par an !
- ARENH : 42€/MWh
- 5000 à 15000 MW de puissance (1 EPR = 1650MW)
- Throughput de 1.75kB/s
- Donc 1 à 3 kWh par Octet, ie préparer 10 à 30L de thé !

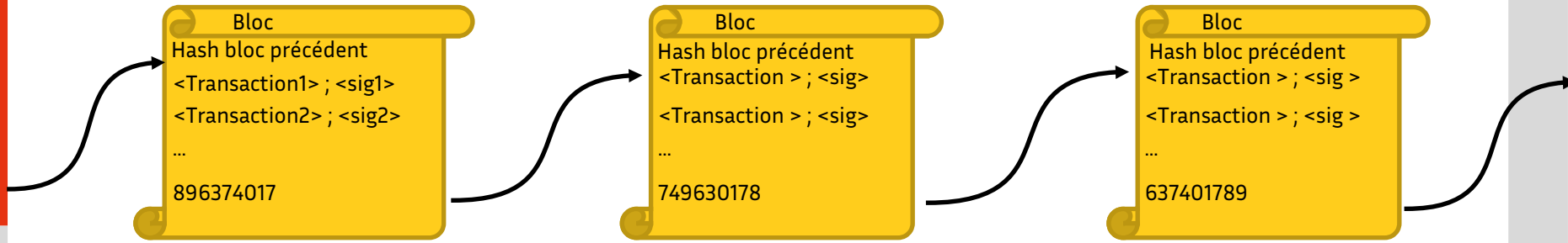
Ce n’est pas fini…

Whintson, TX
23000 ordinateurs
300 MW -> 700 MW



Autres utilisations de la chaîne de blocs

Rappel



- **Infalsifiable**
- **Authentification des transactions**
- **On a une base de donnée distribuée !**

Mettre autre chose que des transactions dans le chaîne de bloc?

Les transactions sont signées cryptographiquement.

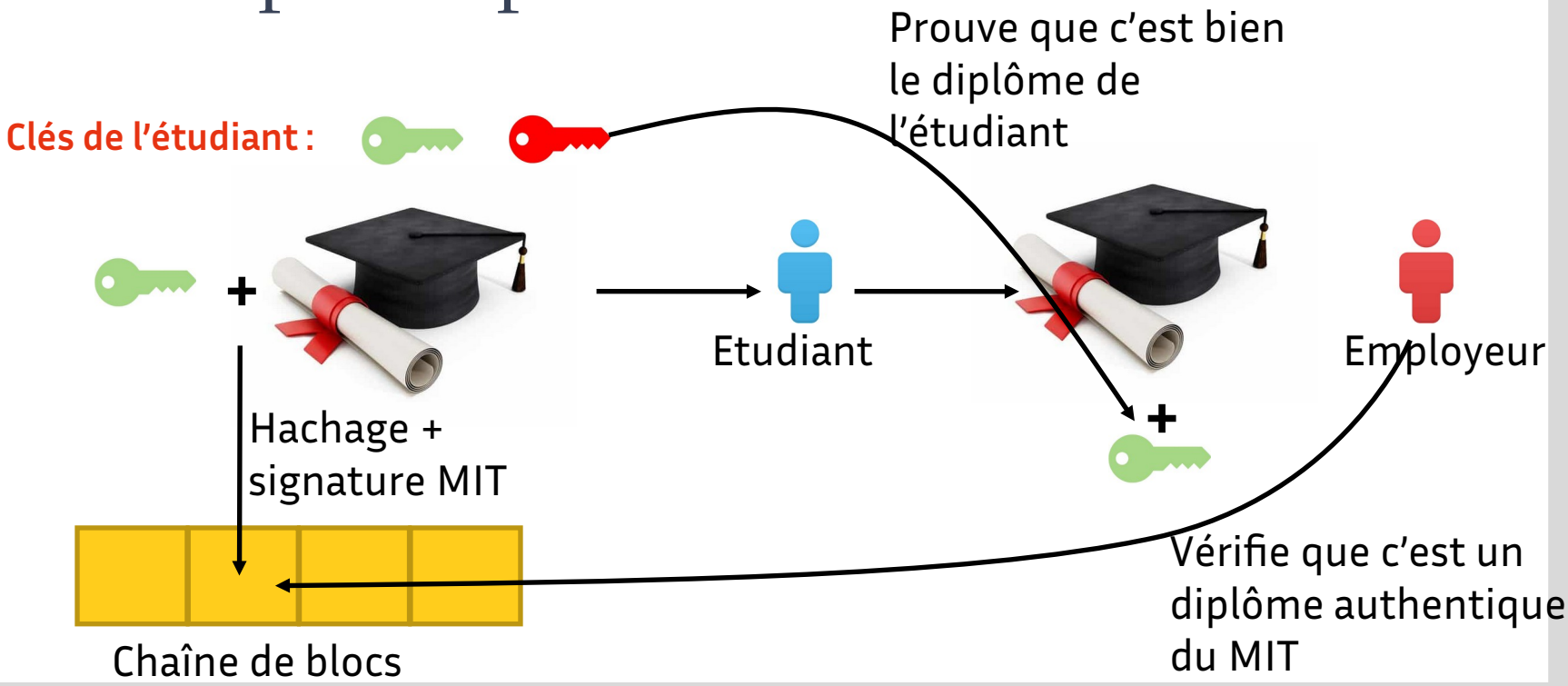
On pourrait mettre :

- **Du texte**
- **Une image**
- **Du code (smart contract, DeFi) !**

Bitcoin : les nœuds manipulent des tokens fongibles (monnaie).

NFT : tokens individualisés (Non Fongible Token)

Exemple : diplômes du MIT



Autres utilisations

- **Estonie : Chaine de blocs KSI pour stocker et identifier les transactions entre les bases de données de l'état**
- **Lutte contre la fraude dans les assurances**
- **Traçabilité des produits de la chaîne alimentaire**
- **General Electric : empreinte numérique des machines électriques**
- **ONG Bitland : cadastre virtuel du Ghana**
- **NFT**
- **Contrat intelligents…**

04

Conclusion

Conclusion

Bitcoin :

- **Solution à un problème informatique difficile**

Nouveaux problèmes :

- **Vitesse de transaction**
- **Coût énergétique catastrophique**

Nouveaux usages, par ex. :

- **Authentification des diplômes**
- **NFT , smart contract, decentalized finance (DeFi)**

Des algorithms plus efficaces ?

- Aggrégation de signatures (couplage sur courbes elliptiques)
- Proof of Stake
- Verifiable Random Functions (couplage sur courbes elliptiques)
- Verifiable Delayed Functions (isogénies sur courbes elliptiques)

Pour aller plus loin

- Le Bitcoin et la Blockchain (avec Heu?Reka) – science étonnante : https://www.youtube.com/watch?v=du34gPopY5Y
- 3Blue1Brown (en anglais) https://www.youtube.com/watch?v=bBC-nXj3Ng4

- **Le mystère Satoshi, Aux origines du Bitcoin**. Sur Arte.tv (6 épisodes)

- Une explication de Jean-Paul Delahaye de la preuve de travail : https://www.lemonde.fr/blog/binaire/2022/02/10/le-plus-gros-bug-de-lhistoire/
- Des vidéos Inria : https://www.lemonde.fr/blog/binaire/2017/05/17/podcast-bitcoin/

Merci !

Suivez-nous sur www.inria.fr