

Première année

Cours 6: La blockchain

Les moyens de paiement évoluent et se multiplient – > inconvénients: délai d'attente, frais annexes, monopolisation des droits et autorisations sur les comptes, ...

Pour contrer les inconvénients les développeurs ont **créé un nouveau système**:

- rapide et efficace
- rentable
- fiable
- sécurisé

Blockchain

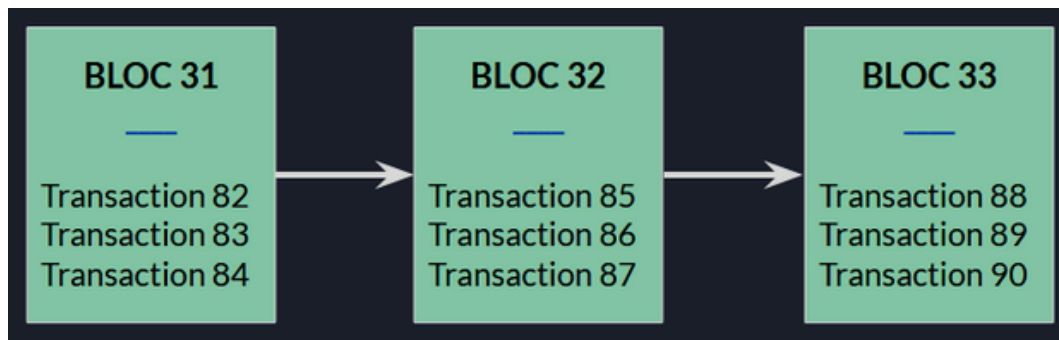
– > **Registre partagé et distribué destiné à faciliter le processus d'enregistrement des transactions et de suivi des actifs dans un réseau d'entreprises.**

Un **actif** peut être un **bien tangible** (maison, voiture, terrain), **ou intangible**, par exemple des éléments de propriété intellectuelle comme les brevets, les droits d'auteur ou les marques.

Un réseau Blockchain permet de **suivre et d'échanger pratiquement tout bien possédant une certaine valeur en réduisant les risques et en diminuant les coûts** pour tous les interlocuteurs concernés.

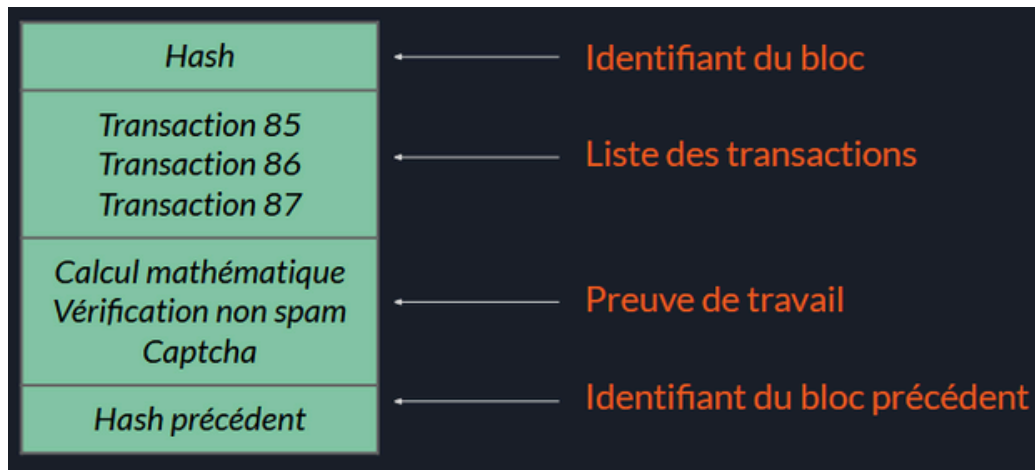
- Transactions publiques mais anonymes
- Transactions vérifiables par tous
- Transactions enregistrées et irréversibles
- Transactions infalsifiables
- Protège contre la fraude

Fonctionnement – > **un bloc contient une liste des transactions**



L'ensemble des blocs forment une chaîne de blocs.

Contenu d'un bloc:



Preuve de travail (proof-of-work - PoW) - > **processus de vérification automatisé**. Il doit être créé de façon à ce qu'il ne soit pas nécessaire de prendre du temps pour vérifier qu'il corresponde aux critères demandés. **Exemple:** Hashcash - > créée en 1997 par Adam Baker pour prévenir contre les spams.