Blockchain

Introduction

- Qui je suis ?
- De quoi on va parler ?
- Pourquoi vous avez besoin de ce cours ?

Plan de cours

Plan de cours

Chapitre 9

Chapitre 10

Chapitre 11

Chapitre 1 – Premiers pas

- 1.1 – Introduction
- 1.2 - Qu'est-ce que la blockchain ?
  - TP
- 1.3 - Les composants de la blockchain
  - TP
- 1.4 - Le White-paper Bitcoin
- 1.6 - Implémentation d'une blockchain

Introduction

But de ce chapitre : Savoir répondre à la question "Qu'est-ce exactement une blockchain ?"

Qu'est-ce que la blockchain ?

La blockchain n'est pas Bitcoin.

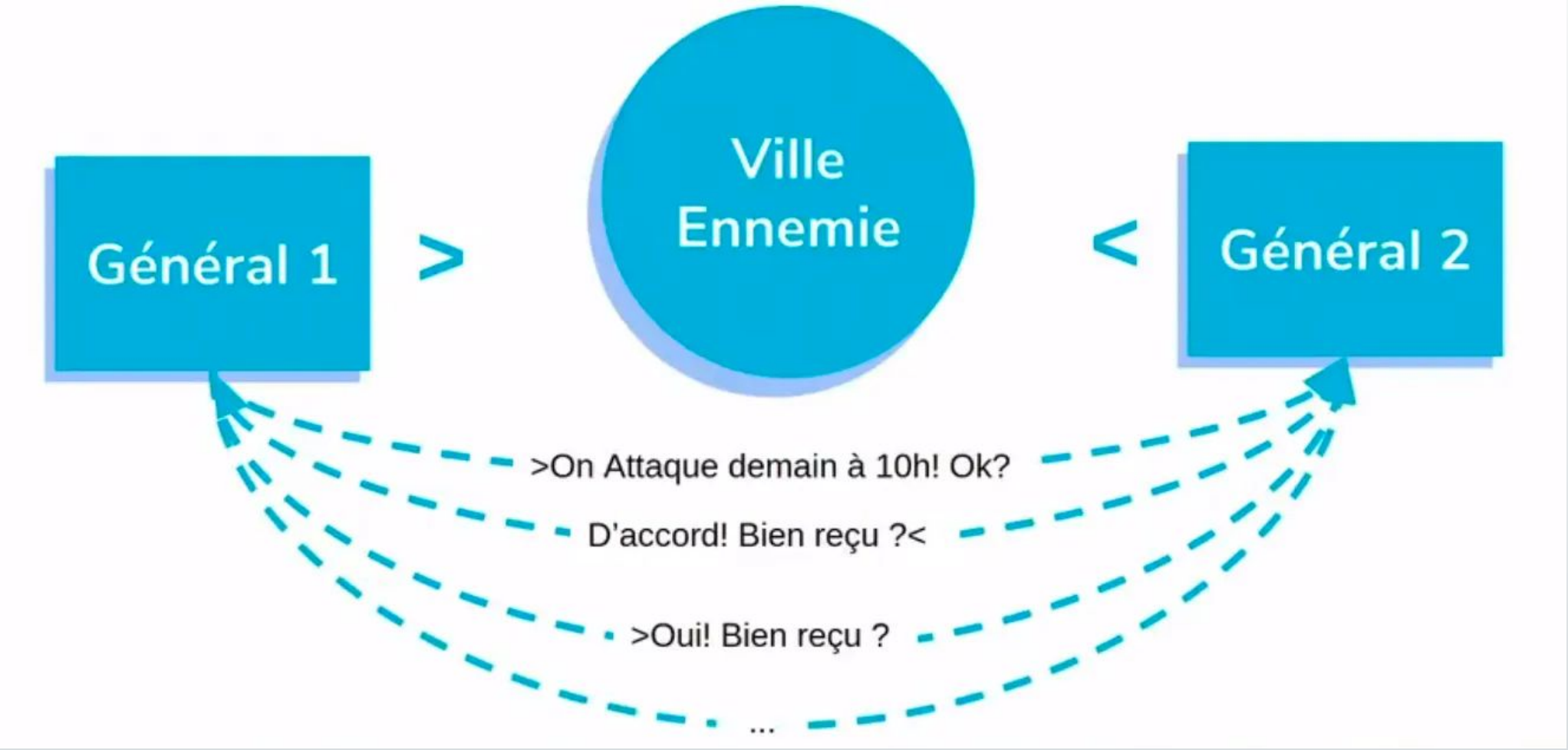
Blockchain : technologie qui permet de garantir la sécurité et la transparence dans un le but de créer un environnement de coopération dans lequel **personne ne se fait confiance**.

Problème des 2 généraux

2 généraux byzantins veulent prendre une ville ennemie, 1 seul général ne serait pas en capacité de le faire.

=> Les 2 généraux doivent se coordonner pour attaquer en même temps la ville ennemie.

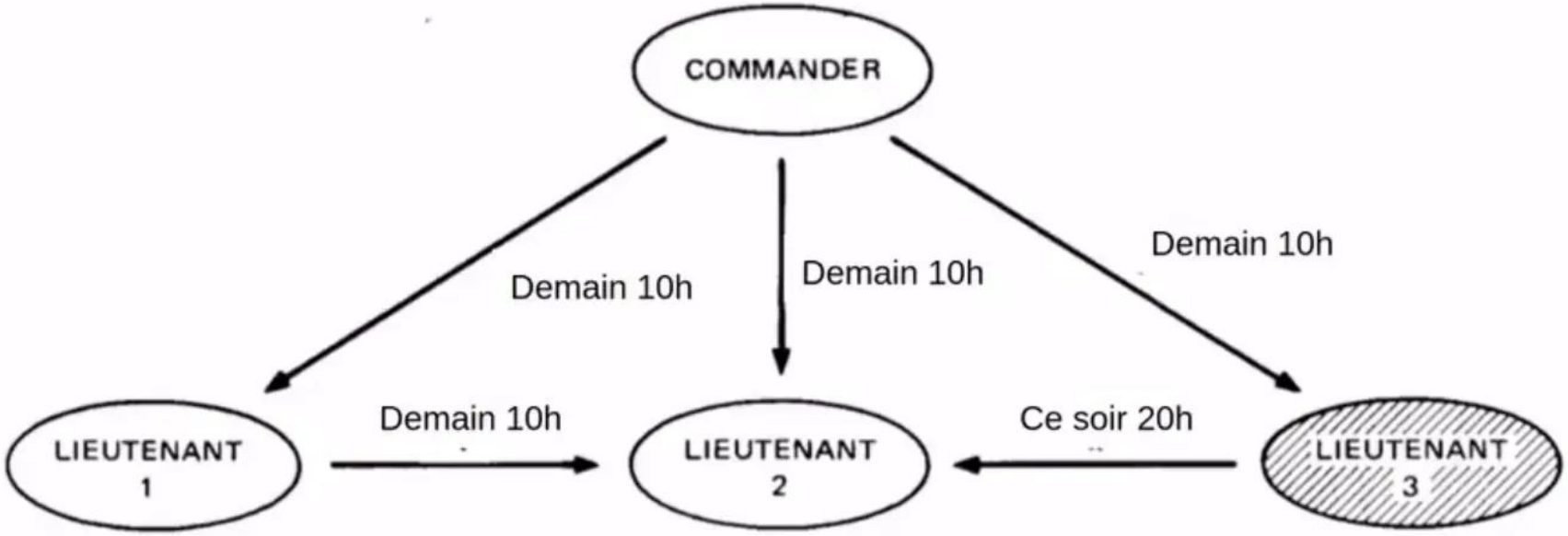
Problème des 2 généraux



Le problème des généraux byzantins

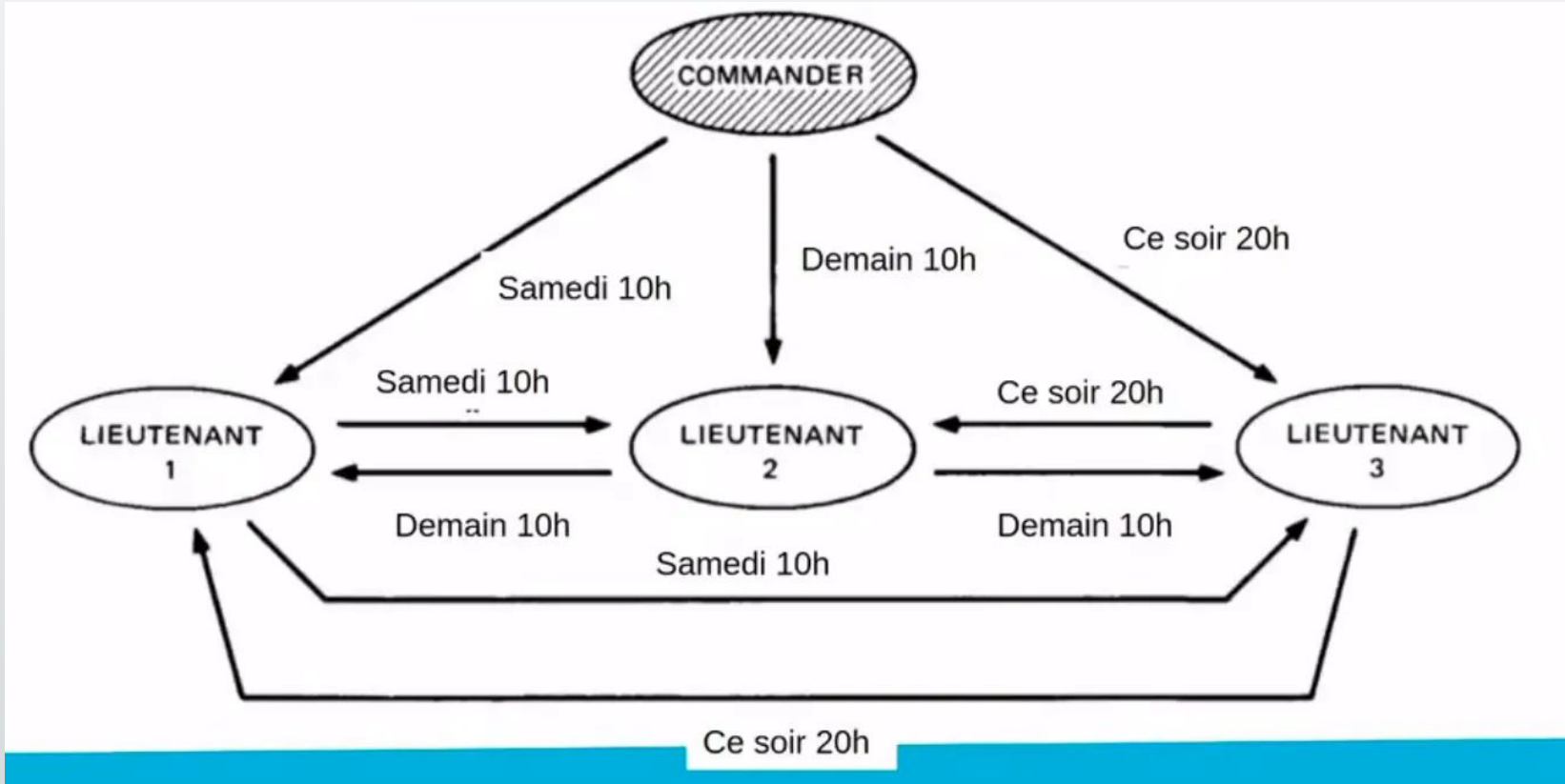
2 sous-problèmes :

- de 2 généraux doivent se coordonner,
- Un ou plusieurs généraux peuvent être des traîtres.



Le problème des généraux byzantins

=> Le problème est soluble si plus de la moitié des généraux sont honnêtes.



La tolérance aux pannes byzantines

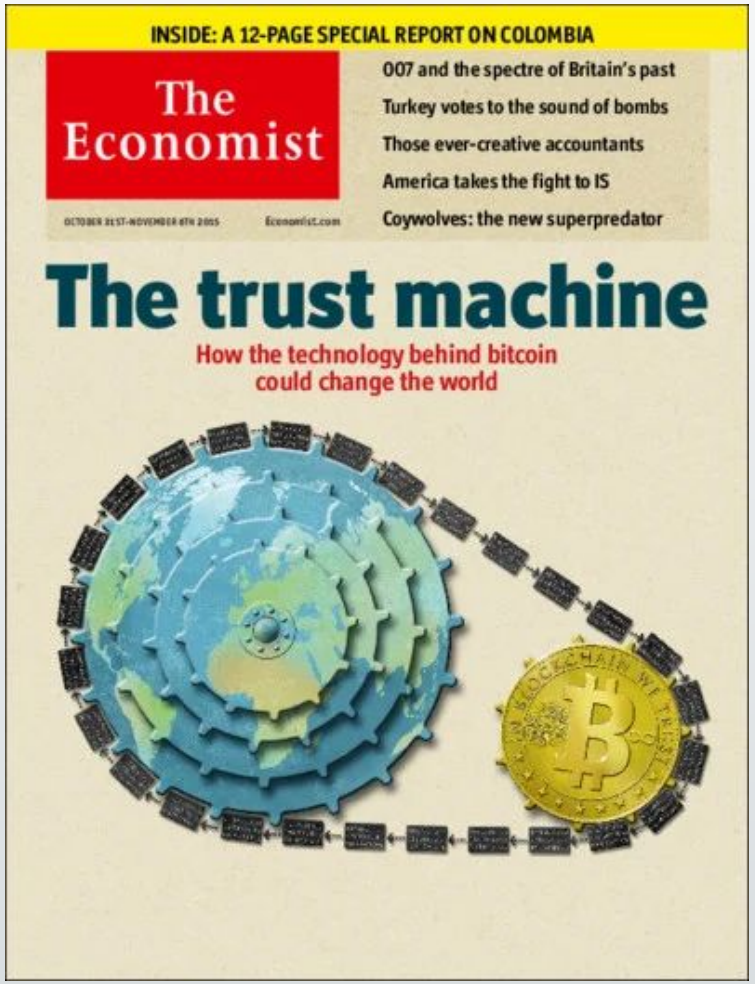
=> La Tolérance aux pannes byzantines, est la capacité d'un système informatique distribué à résister aux défauts byzantins

=> C'est la classe de panne la plus difficile car elle n'implique aucune restriction et ne fait aucun hypothèses sur le type d'erreur qu'un noeud peut avoir.

Et la blockchain dans tout ça ?

"Blockchain the trust machine" The Economist, Octobre 2015

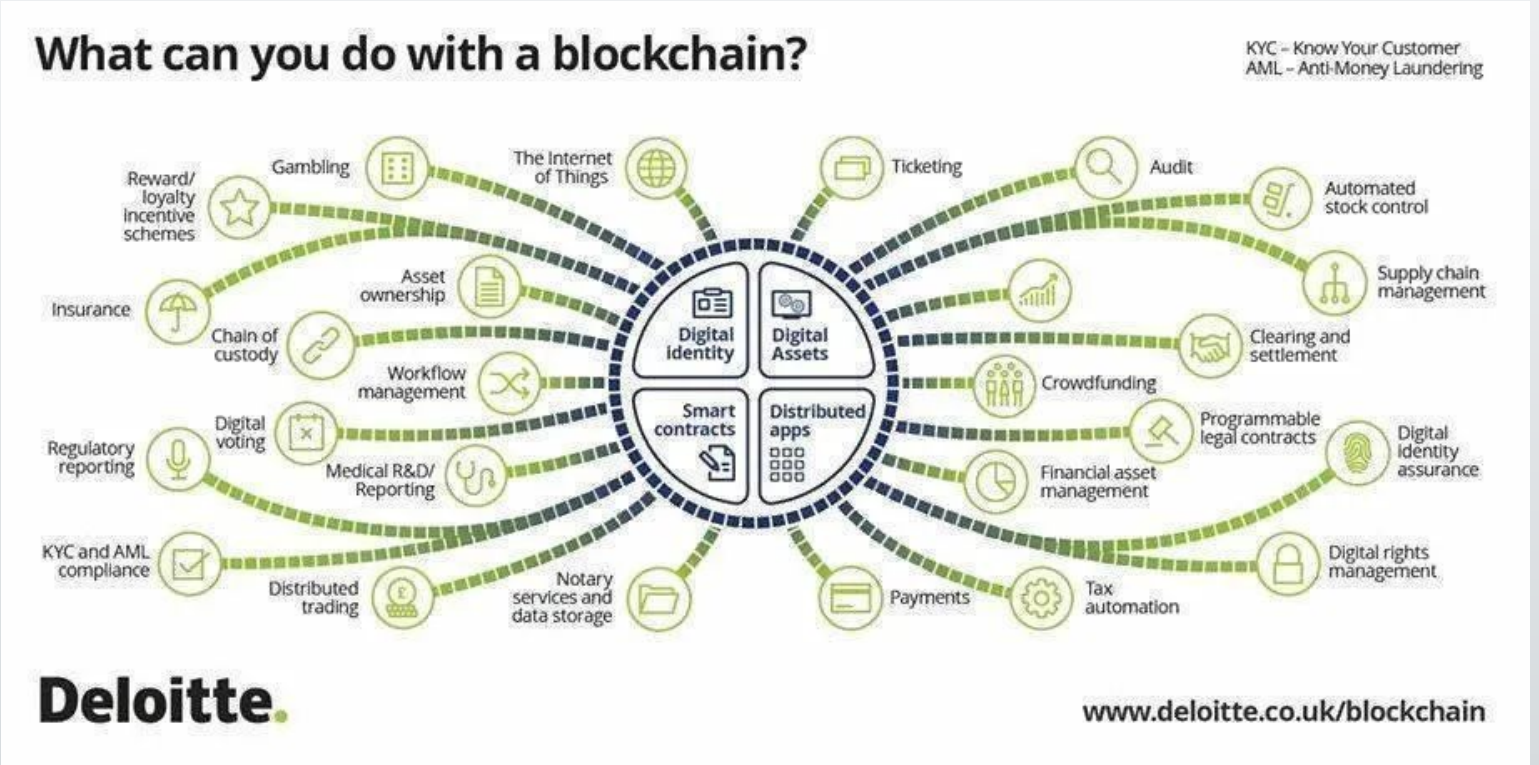
"L'innovation de la blockchain ce n'est pas l'argent, c'est la confiance." Ludwig Seigel (auteur de l'article)



Les promesses

=> Faire confiance aux informations sans faire confiance aux participants

=> Tous les participants du réseau participent ensemble à donner de la confiance aux informations.



Les potentielles applications

APPLICATION DE BLOCKCHAIN	ENTITÉ MENACÉE	POURQUOI
Paiements entre personnes ou sociétés	banques	plus rapide, plus fiable, jusqu'à 100 fois moins cher, frais de conversion bas, monnaie infalsifiable
Contrats entre personnes	notaires	plus rapide, plus fiable, jusqu'à 10 000 fois moins cher
Contrats entre sociétés	avocats	beaucoup plus fiable, jusqu'à 10 000 fois moins cher
Votes et élection	États, syndicats et partis politiques	plus fiable, plus rapide
Propriété intellectuelle	bureaux des brevets	beaucoup plus fiable, jusqu'à 50 000 fois moins cher

Exercice - La blockchain en application

Présentation orale en groupe avec visuel (diapo ou autre)

1. Trouver un projet existant autre que Bitcoin et faire l'analyse du besoin auquel le projet répond.
2. Expliquer pourquoi la blockchain est intéressant pour ce projet ? Ou pourquoi il n'est pas intéressant.

La présentation orale comprend :

- Présentation des principales données du projet/de la blockchain
- Quel problème est résolu ?
- Quelle solution est apportée ?
- Est-ce que la solution vous semble viable ?
  - Avantages
  - Inconvénients

Exercice - Lecture du white-paper Bitcoin

30-45 minutes individuelle

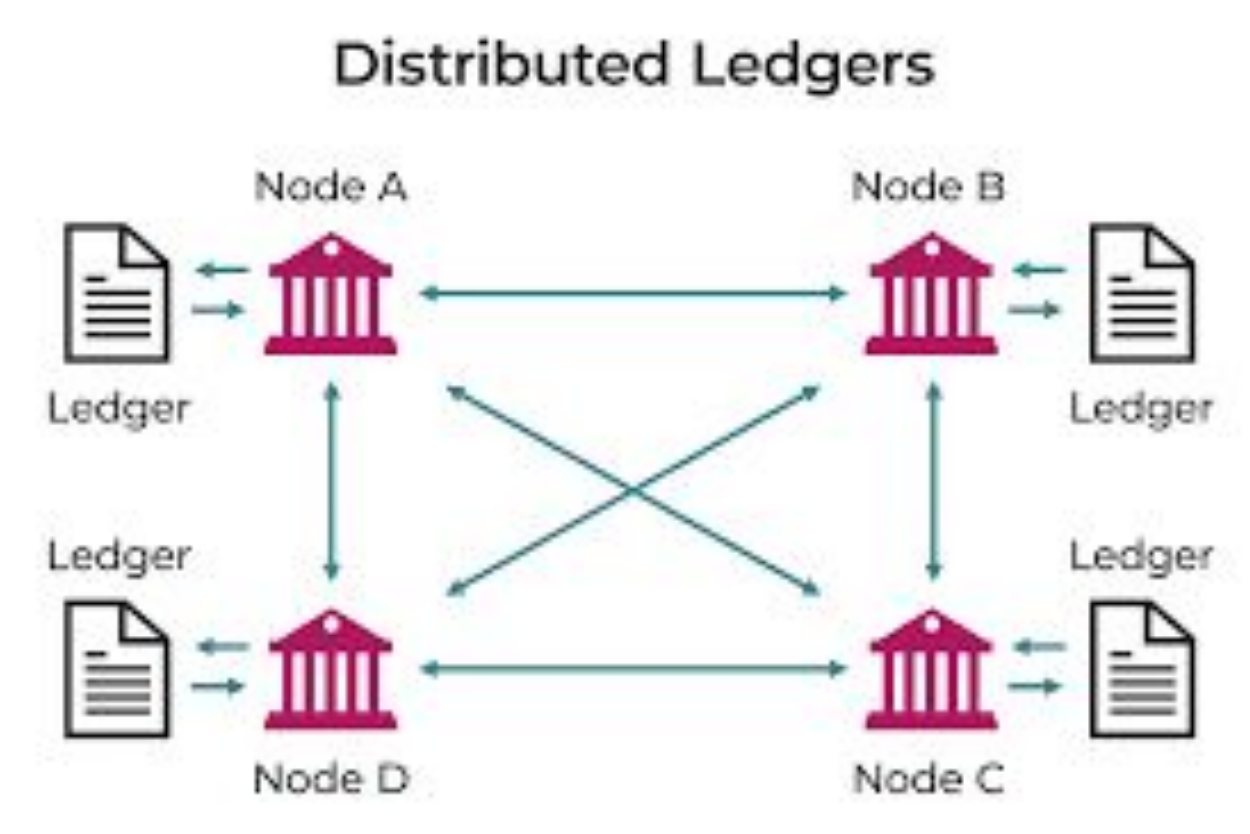
1. Lire le white-paper Bitcoin et lister les éléments que vous n'avez pas compris pour qu'on puisse en discuter.
2. Etablir la "recette de cuisine" de la blockchain Bitcoin ?
3. Répondre aux questions :
    1. Quel problème principal Satoshi Nakamoto cherche-t-il à résoudre avec Bitcoin ?
    2. Comment fonctionne la preuve de travail (Proof-of-Work) dans le système Bitcoin ?
    3. Qu'est-ce qu'un "double spending" et comment Bitcoin l'empêche-t-il ?
    4. Quel est le rôle des nœuds dans le réseau Bitcoin ?
    5. La conception de Bitcoin garantit-elle l'anonymat total des utilisateurs ? Expliquez.
    6. Comment les incitations économiques sont-elles intégrées dans le système de Bitcoin ?

Les composants de la blockchain

1. Un registre (ledger) distribué
2. une technique cryptographique pour sécuriser les échanges
3. un algo de consensus pour valider les transactions
4. un réseau pair à pair avec des participants

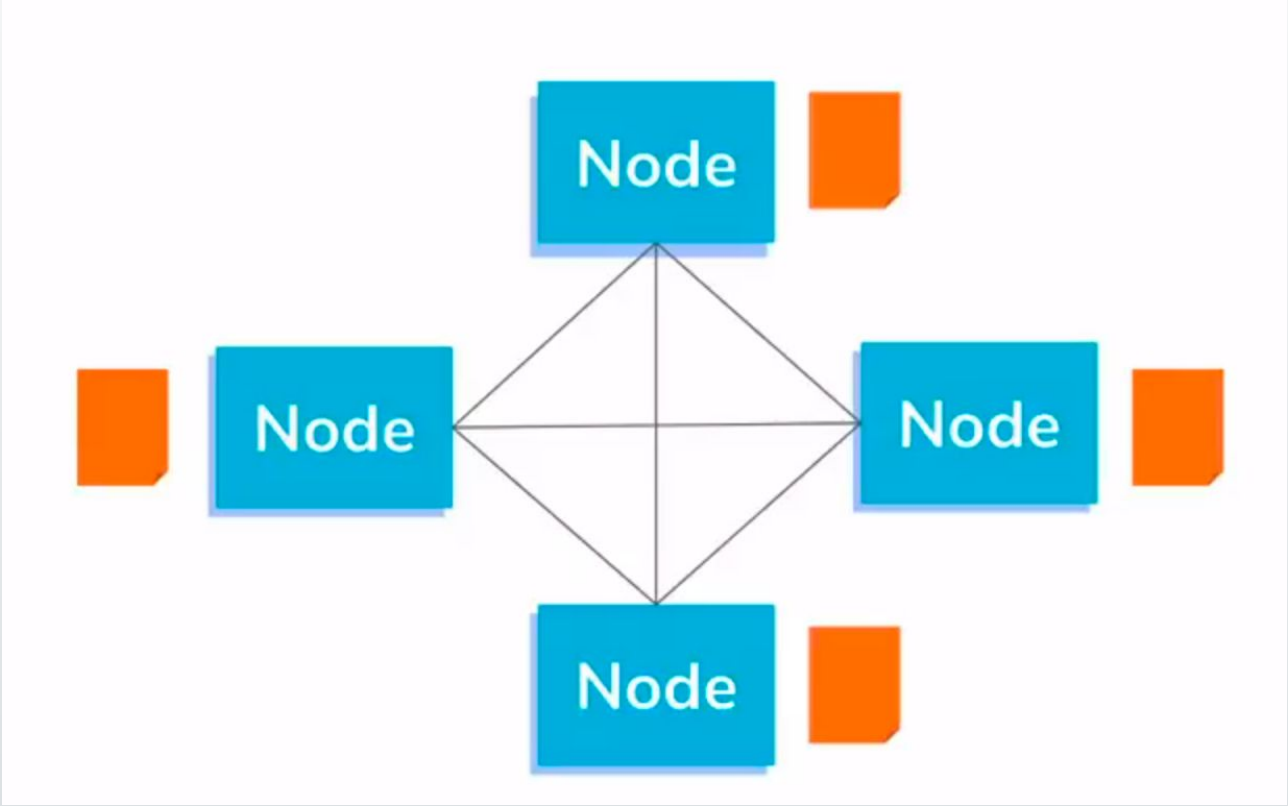
Le registre

Registre = grand livre de compte public décentralisé et partagé



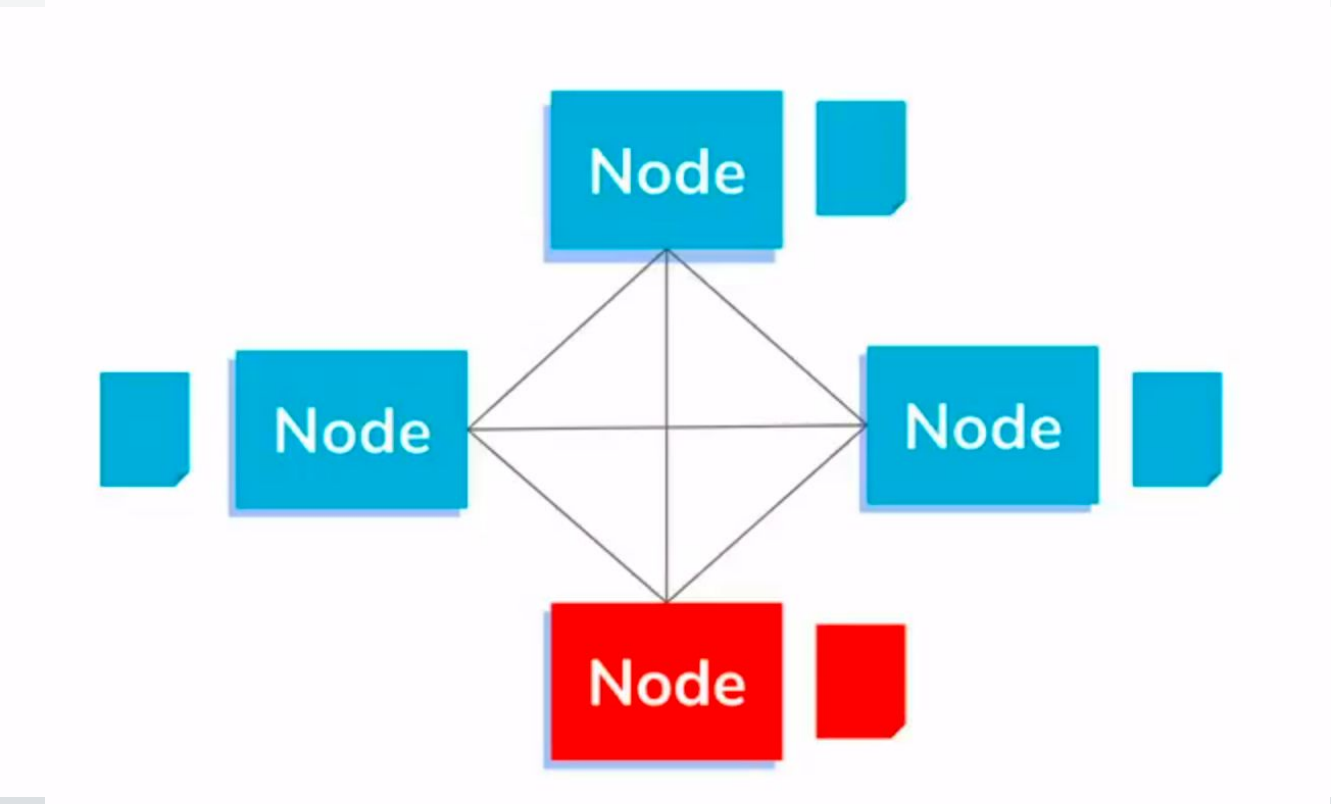
Le registre

Registre = grand livre de compte public décentralisé et partagé



Le registre

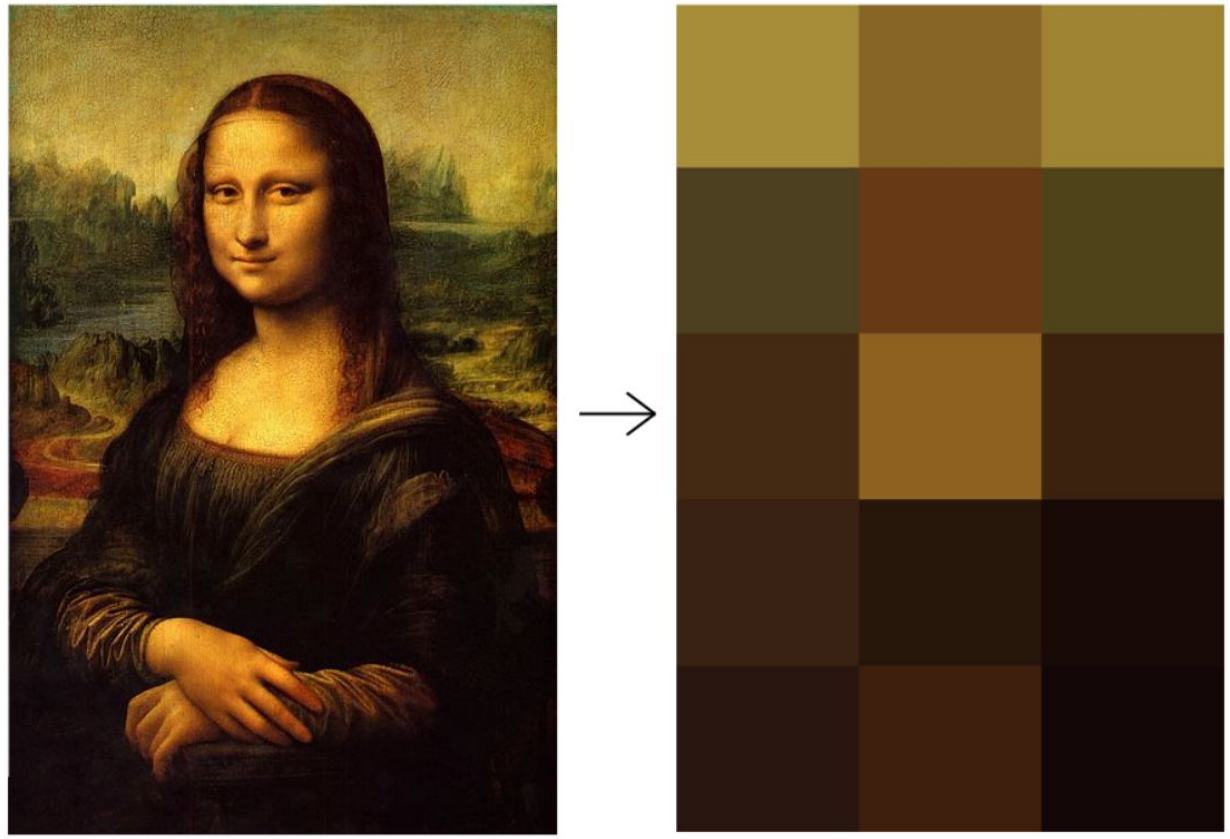
Registre = grand livre de compte public décentralisé et partagé



Une technique cryptographique

=> Fonction de hachage (SHA-256)

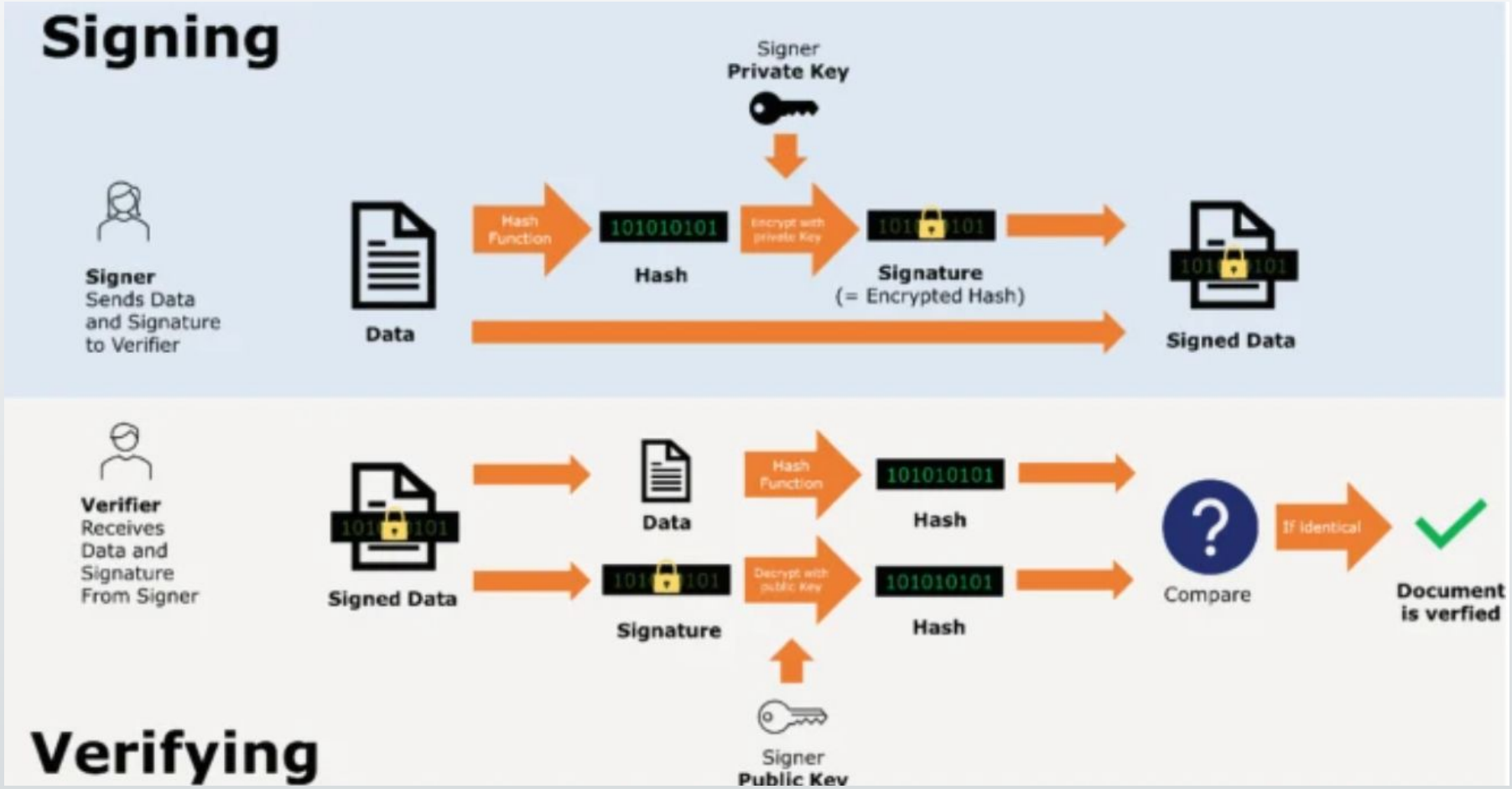
- Rien ne peut être supprimé du registre
- Rien ne peut être modifié dans le registre



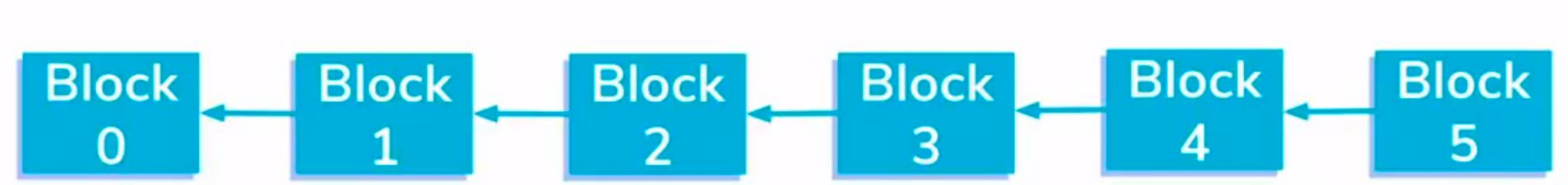
Une technique cryptographique

=> ECDSA

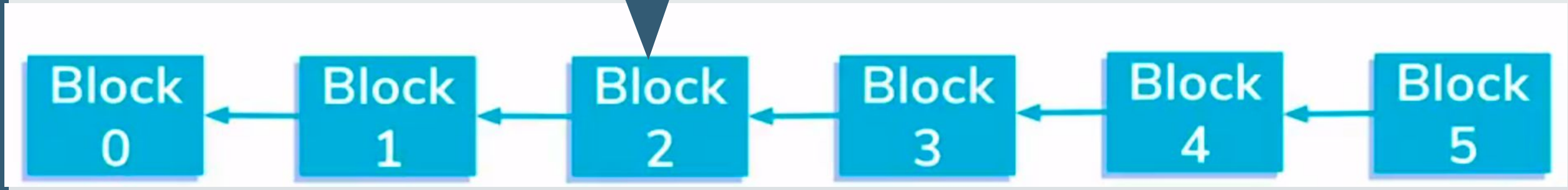
=> Usurpation d'identité



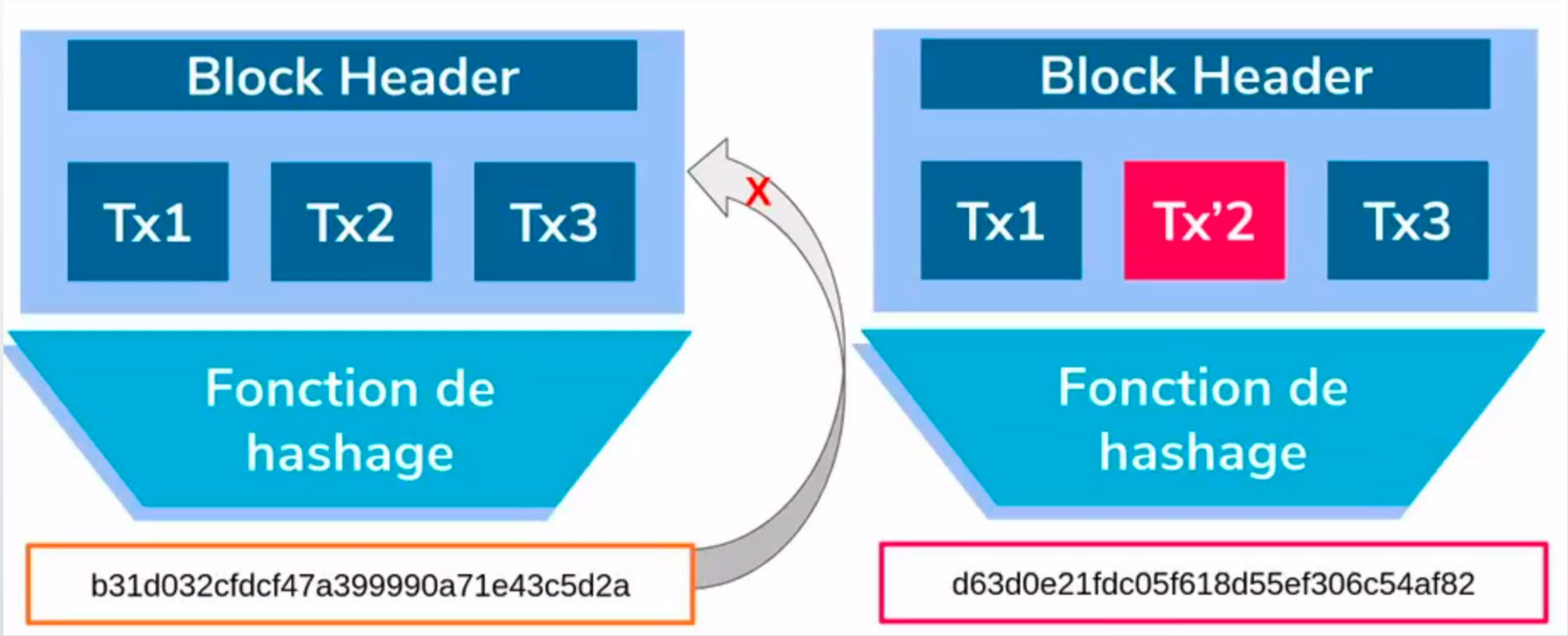
Une technique cryptographique



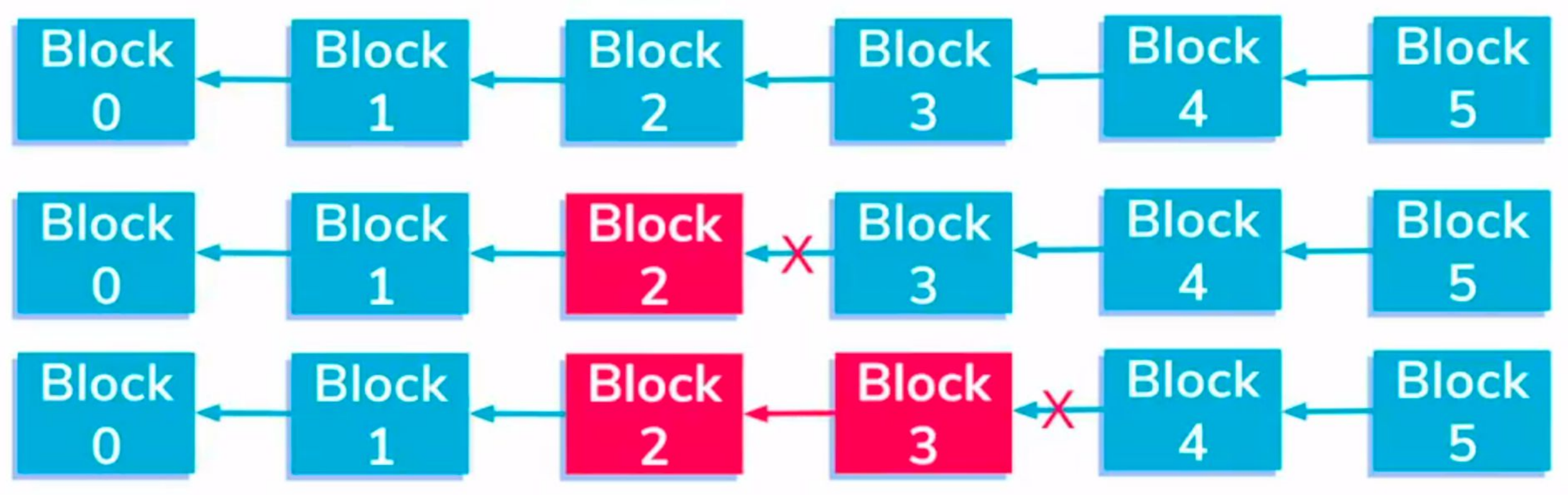
Une technique cryptographique



Une technique cryptographique



Une technique cryptographique

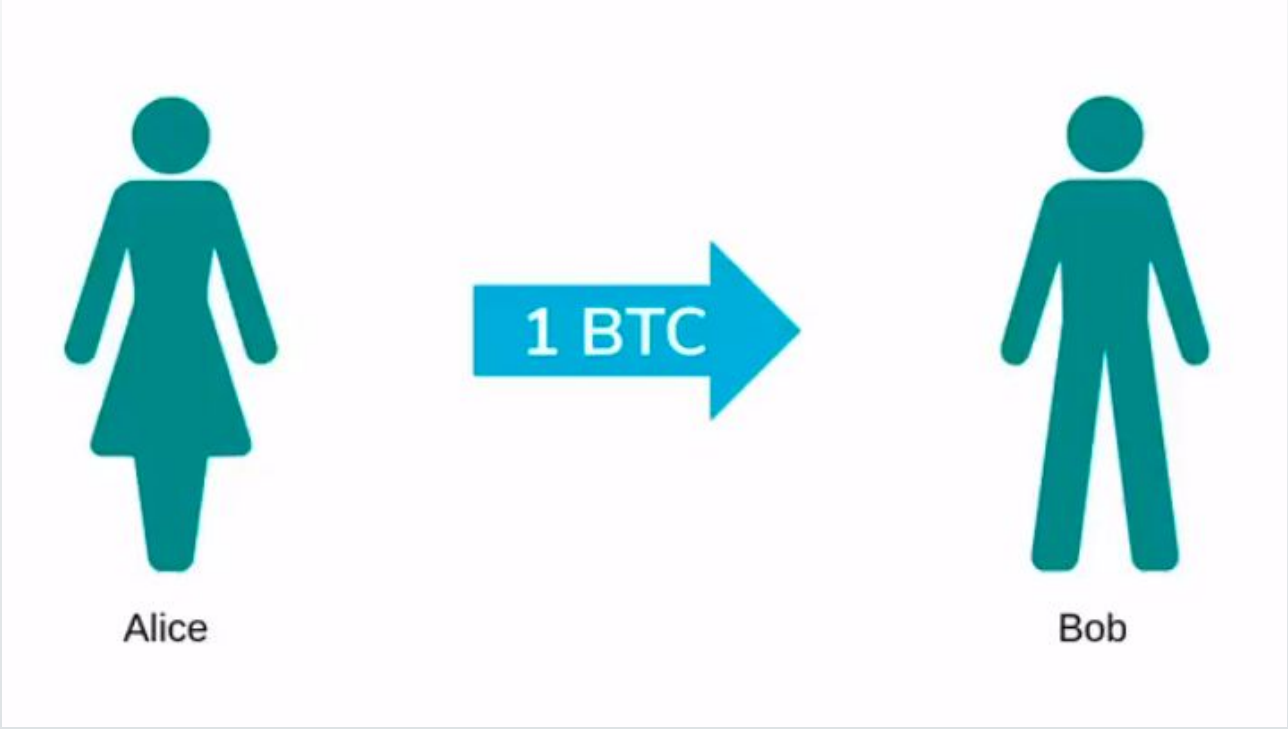


Déroulement d'une transaction

1. **Deux parties s'accordent sur les termes d'une transaction** (transfert d'argent, actifs, titres financiers, etc.)
2. **Le registre est scanné/analysé par les membres du réseau .** Par l'analyse de l'historique les membres du réseau s'assurent que le vendeur possède effectivement l'actif ou les fonds qu'il vend
3. **Si tel est le cas, la transaction est validée et ajoutée au dernier bloc de la chaîne**

4. **Le registre est diffusé à l'ensemble du réseau**

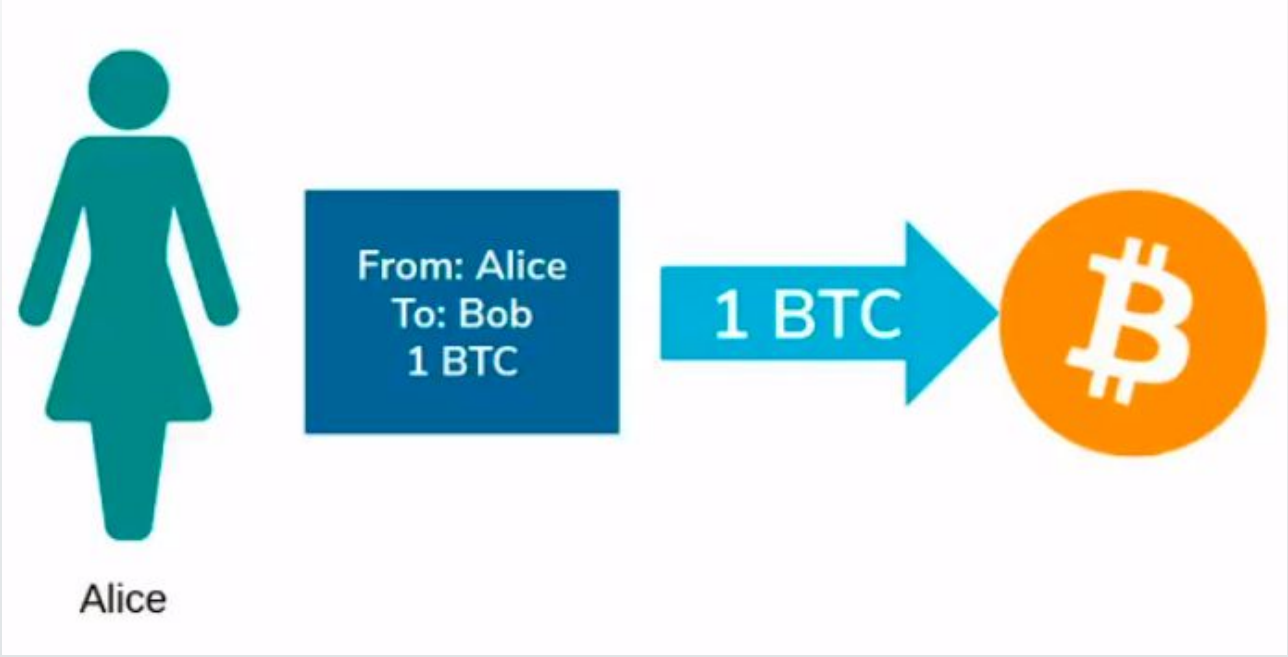
   son caractère distribué assure sa protection



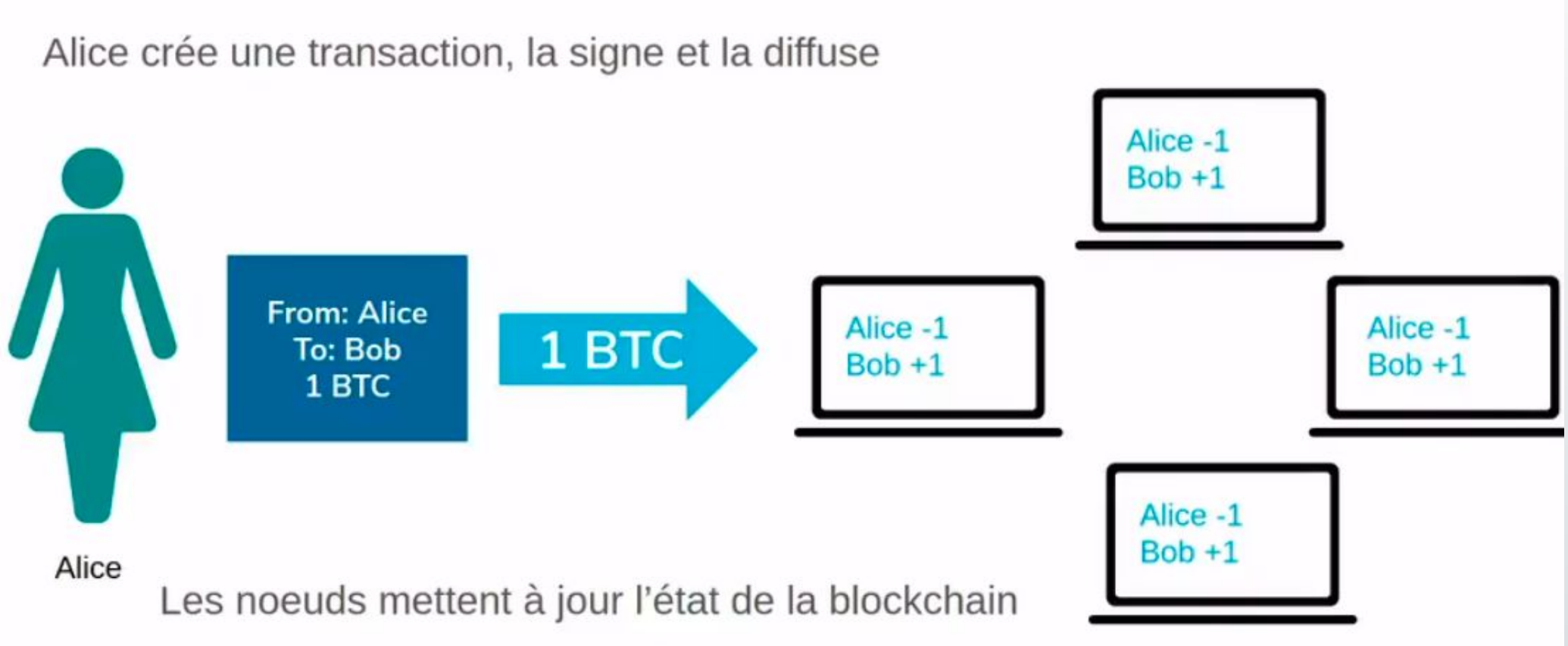
Déroulement d'une transaction

Une transaction à :

- Une adresse d'origine
- Une adresse de destination
- Metadata



Déroulement d'une transaction



Algo de consensus

- Le consensus désigne la capacité de chaque noeud au sein d'un réseau blockchain partagé, à se mettre d'accord sur l'état réel du réseau ainsi que l'ensemble des transactions valables.
- C'est le choix captial pour les blockchains
- Sur Bitcoin c'est du Proof of Work (souvent écrit PoW)