Blockchain et Applications

Chapitre 1

Qu’est-ce que la Blockchain ?

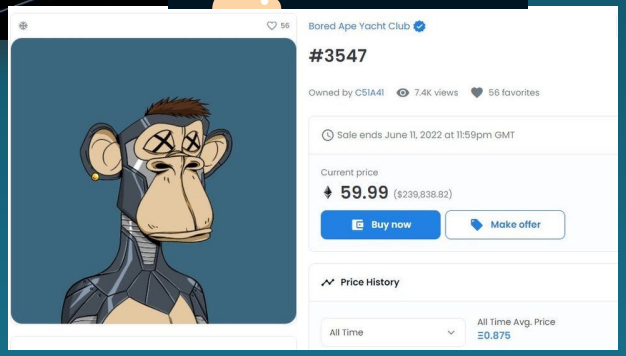
Clement Germanicus

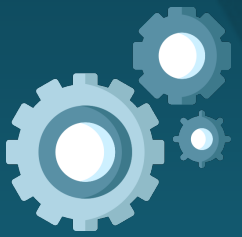
CENTRALE PARIS — EPFL — 2017

Acid Cousins — Co-fondateur

2020

Ce que vous aurez/n'aurez pas dans ce module





Découpage du module

10/01
Intro

17/01
Structure

24/01
Consensus

7/02
Noeuds

Blockchains

DApps

14/02
Smart Contracts

28/02
Ouverture

Déroulement des cours et évaluation

Chaque cours

Quiz noté sur le TD du cours précédent
+
50% Présentation avec quiz interactif
+
50% Travaux dirigés (TD)

Avant la séance suivante

Soumission de votre TD

50%

Projet DApp

Création d'une application décentralisée

20%

Examen final

QCM

30%

Déroulement des cours et évaluation

Chaque cours

Quiz noté sur le TD du cours précédent
+
50% Présentation avec quiz interactif
+
50% Travaux dirigés (TD)

Avant la séance suivante

Soumission de votre TD

50%

Projet DApp

Création d'une application décentralisée

???????

20%

Examen final

QCM

30%

Déroulement des cours et évaluation

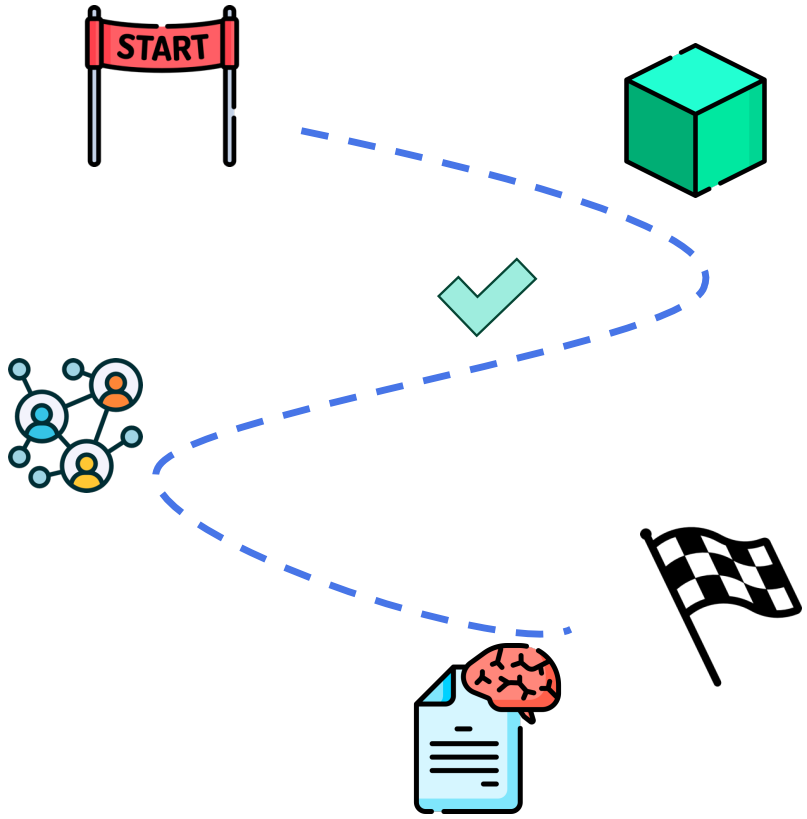
Chaque cours

Quiz noté sur le TD du cours précédent
+
50% Présentation avec quiz interactif
+
50% Travaux dirigés (TD)

Avant la séance suivante

Soumission de votre TD

50%



Règles du module

- Retards
  - 5 min ok
  - Entre 5 min et la fin du quiz noté : vous attendez dehors la fin du quiz
  - Après le début du cours : vous ne rentrez pas
- TDs
  - Exclusivement en Python
  - Vous devrez me rendre un notebook + votre code
  - Votre code sera soumis à un test de robustesse (noté)
  - Entraide ok, plagiat interdit (0) : votre code sera analysé
  - ChatGPT autorisé, mais à vos risques et périls !
  - Un rendu inachevé vaut mieux qu'un rendu plagié
- Contactez-moi !
  - Par mail : clement.germanicus@ext.junia.com
  - Sur Teams

Quand est née la technologie Blockchain ?

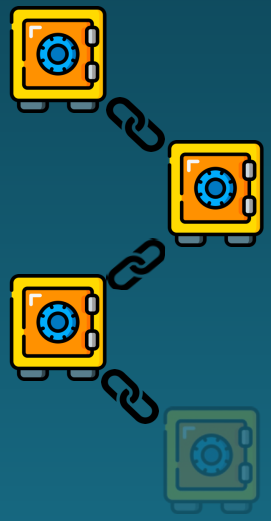
David Chaum – 1982

Cash électronique

Anonymat lors du paiement

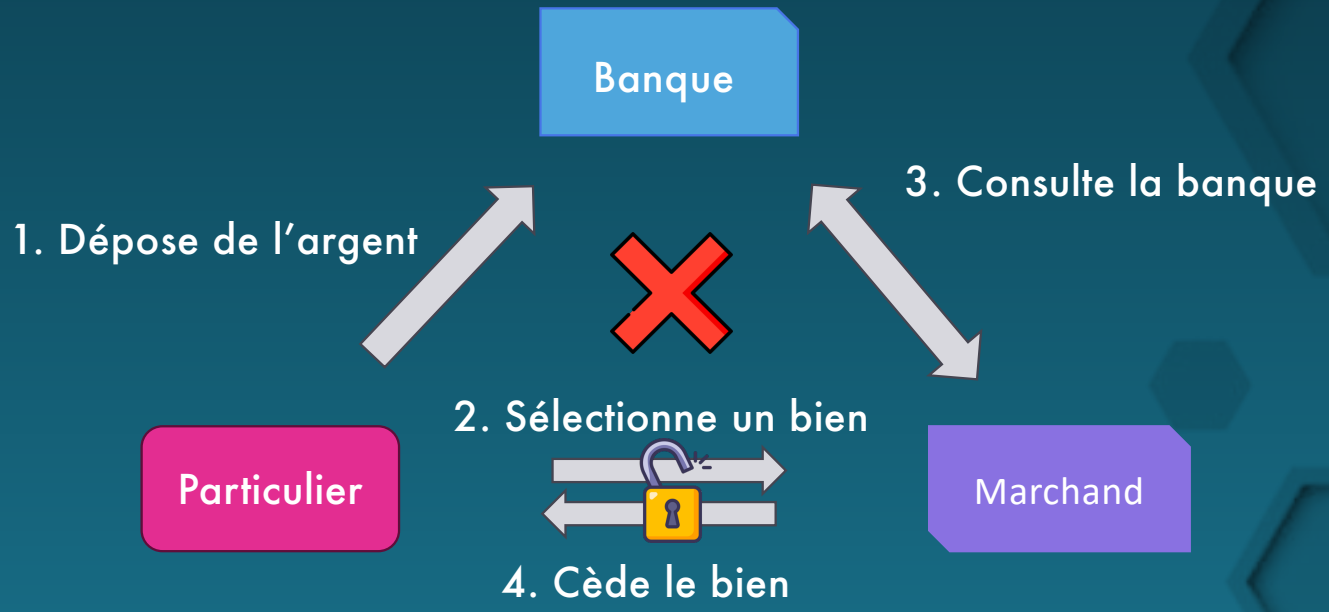
David Chaum – 1982

1982 – "Systèmes informatiques établis, maintenus et approuvés par des groupes mutuellement méfiants"

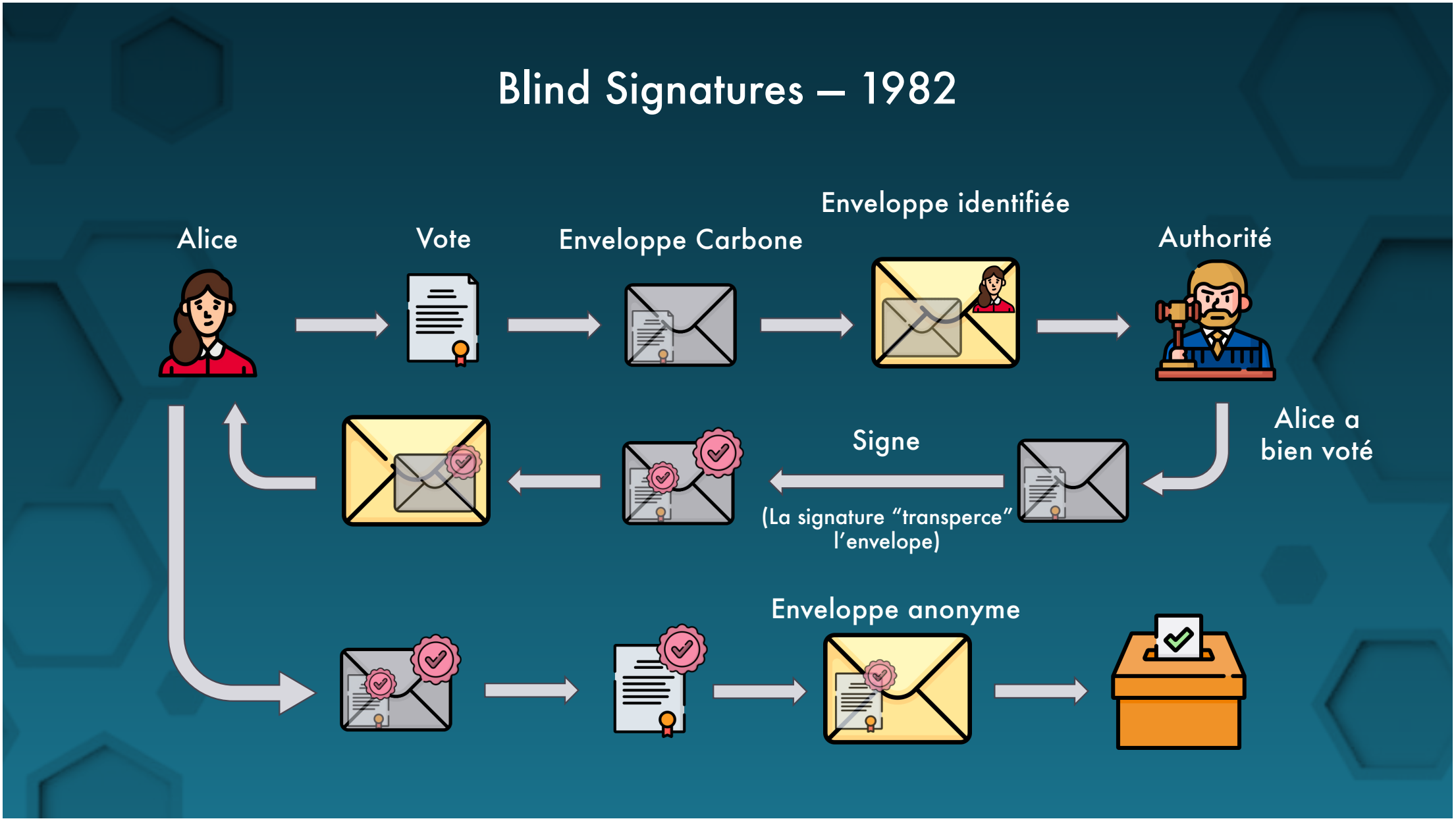


David Chaum – 1982

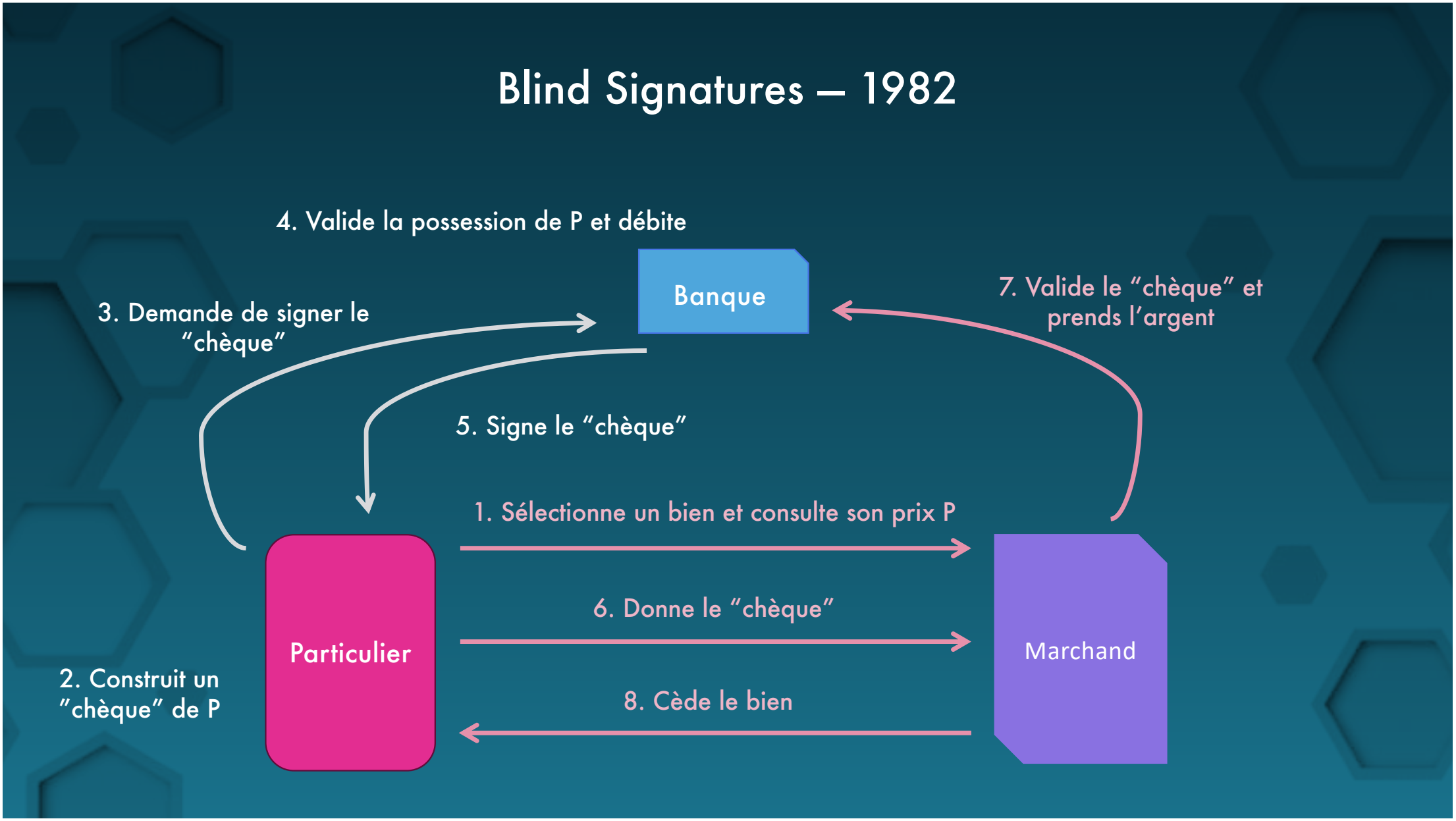
1982 – Blind signatures



Blind Signatures – 1982



Blind Signatures – 1982



David Chaum – 1982

1989 – Création de DigiCash

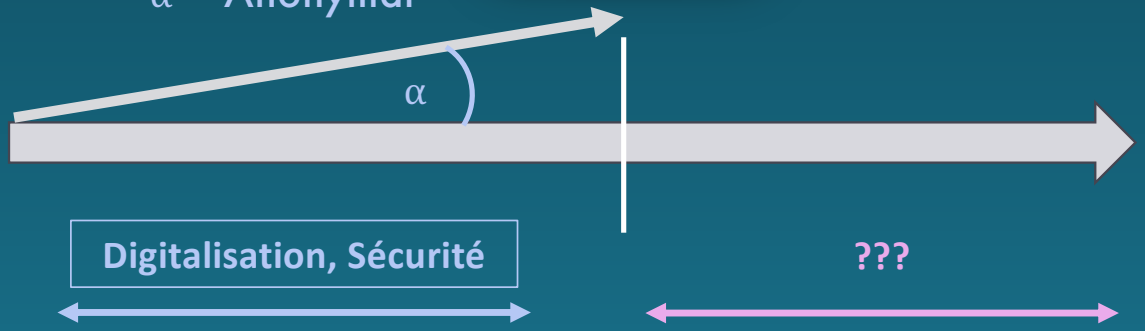
- Logiciel permettant au particulier de “retirer” une note certifiant de la possession d’une certaine somme auprès de sa banque (un “chèque”).
- Implémente la signature aveugle dans son protocole
- Utilise des “cyberbucks”
- Partenariat avec The Mark Twain Bank (Missouri), Deutsche Bank (Allemagne), Crédit Suisse, +3 autres

David Chaum – 1982

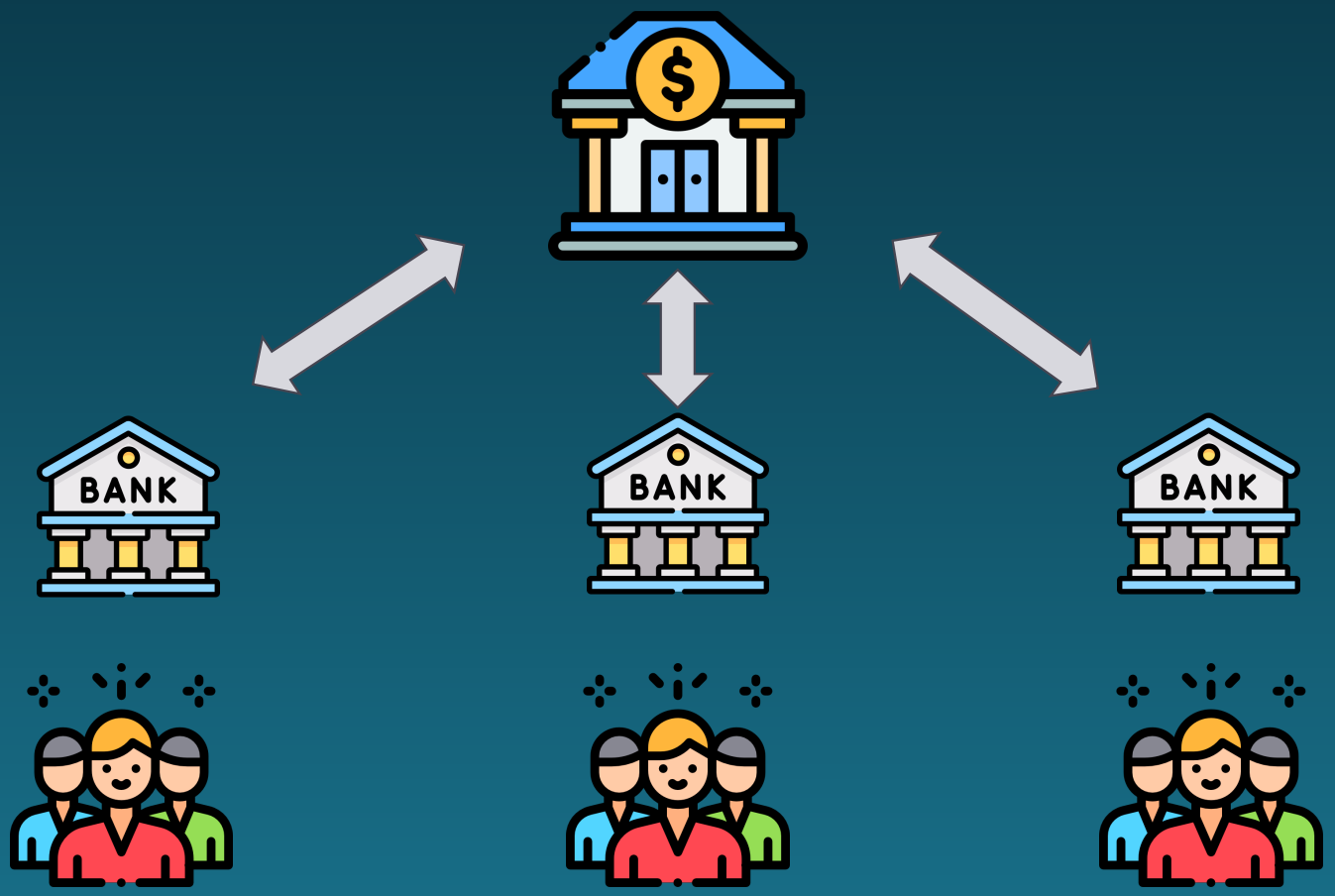
1998 – Faillite !

- N'a pas réussi à être à la hauteur de son succès, aucun vrai business model
- Émergence de Paypal
- Certains dénoncent le côté "paranoïaque" de Chaum qui aurait refusé d'importants partenariats
- Chaum affirme que c'est un problème type "l'oeuf ou la poule" : les marchands ne l'adoptent que s'il y a des clients, qui eux l'adoptent si il y a des marchands.

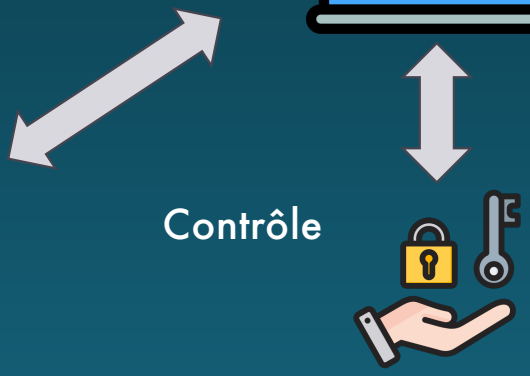
Des banques jusqu'aux cryptomonnaies



Économie centralisée



Économie centralisée

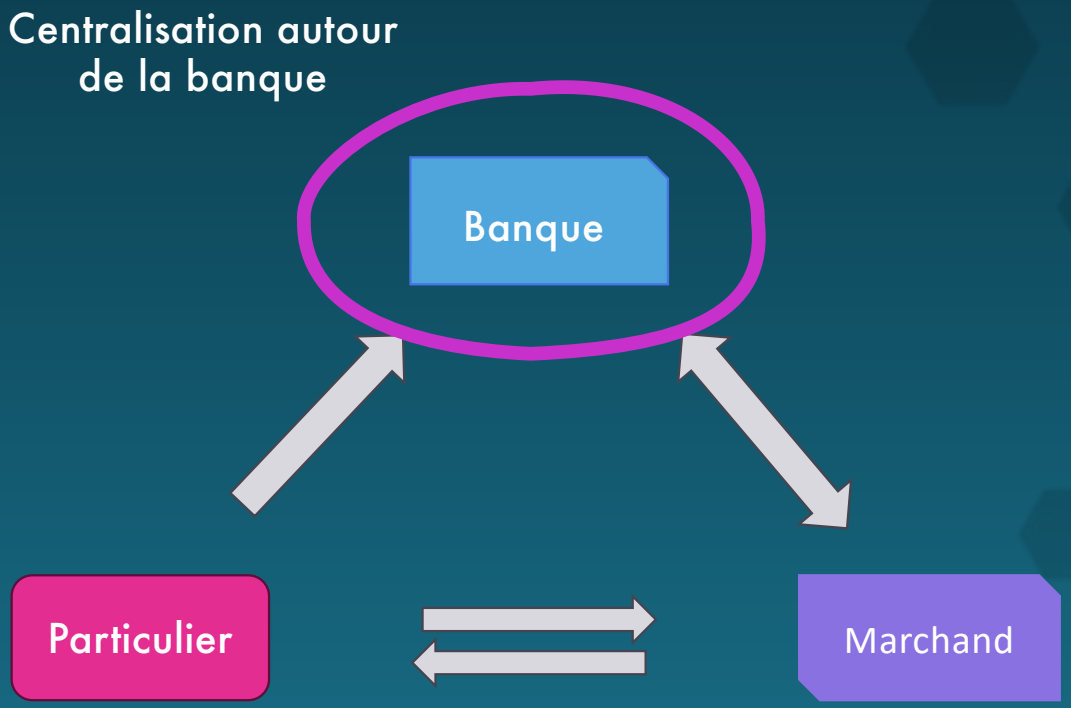


Observation

Contrôle

Effondrement

Modèle de David Chaum – Un paradoxe ?



Besoin de centraliser

Bob me doit 3 euros

Oui, en effet

Ok

Besoin de centraliser

Hein ?? C’est totalement faux !

Je ne sais pas qui croire…

Alice me doit 150.000 euros

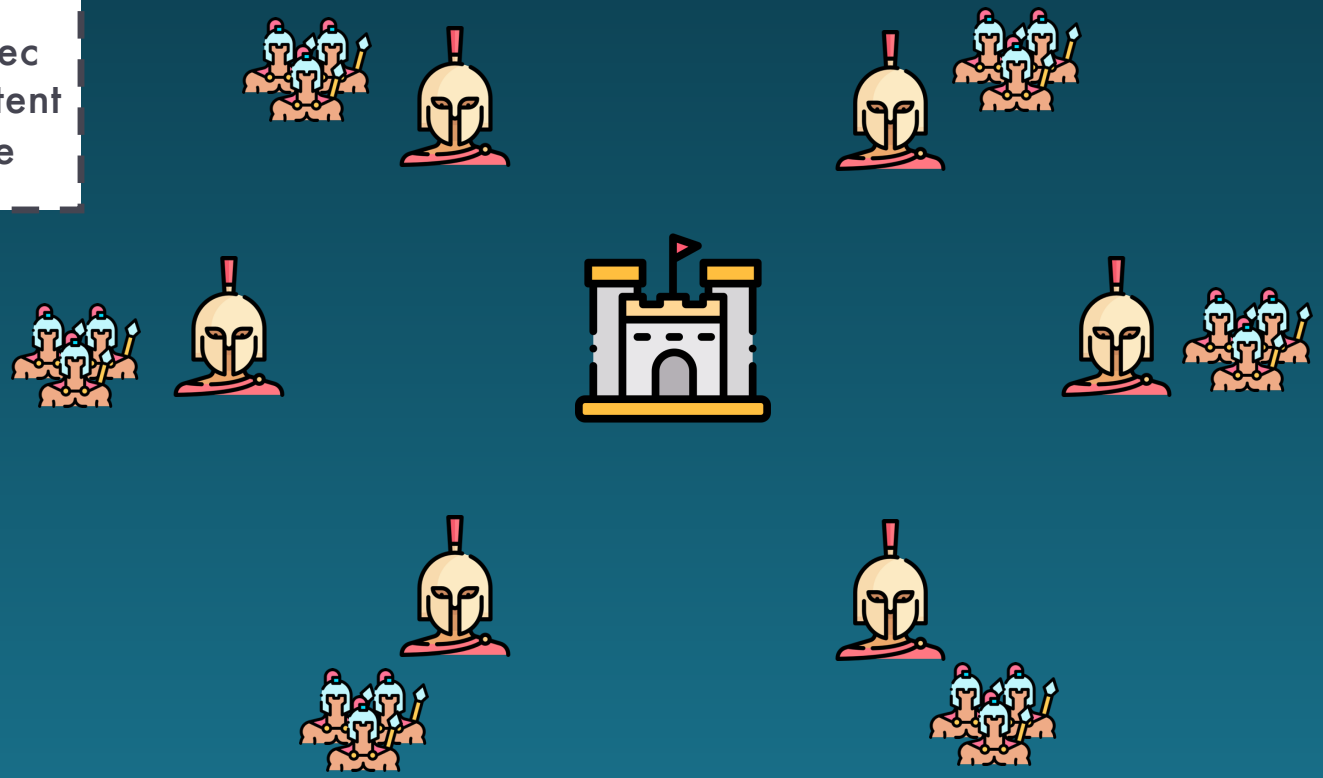
Byzantine Fault Tolerance (BFT)

Un système BFT doit se mettre d'accord sur l'état d'une entité malgré certains participants malicieux ou défectueux

Leslie Lamport, Robert Shostak et Marshall Pease – 1982

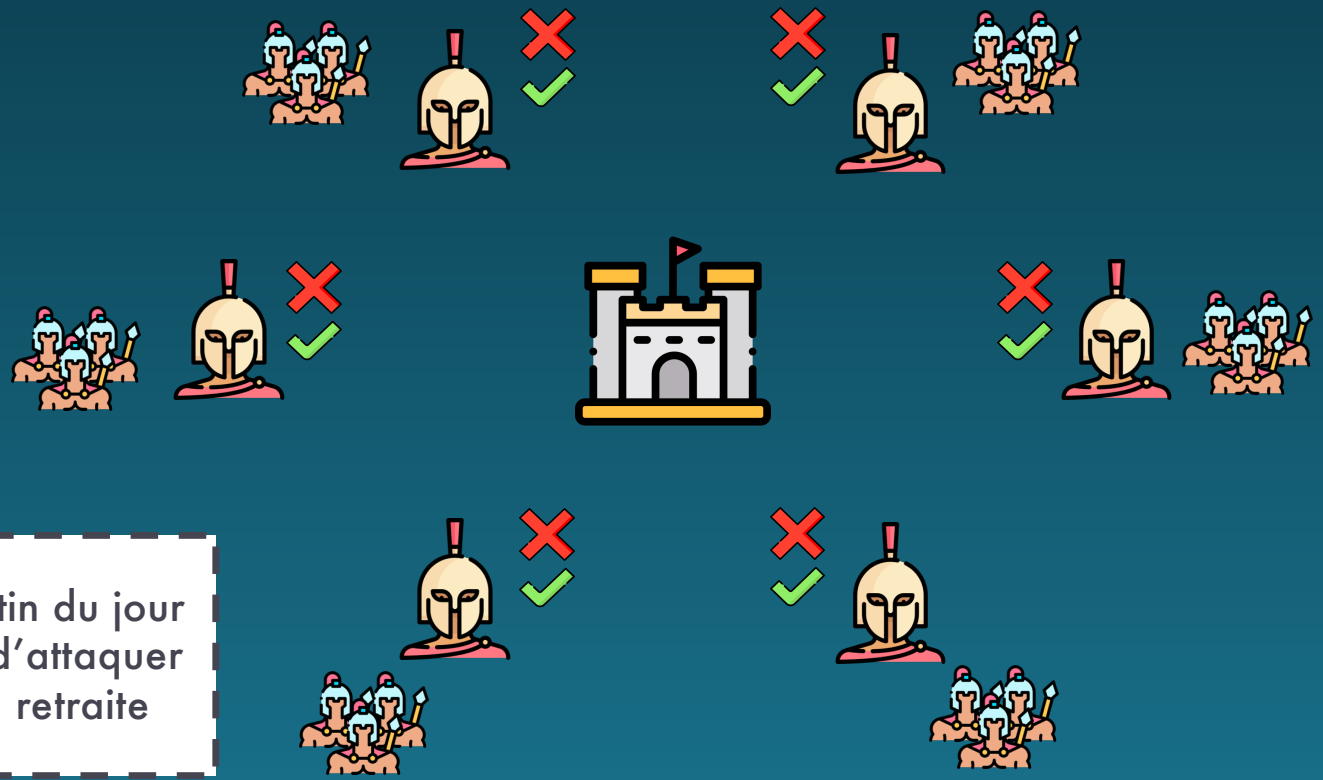
Problème des généraux byzantins

Des généraux (avec leur armée) souhaitent attaquer Byzance



Leslie Lamport, Robert Shostak et Marshall Pease – 1982

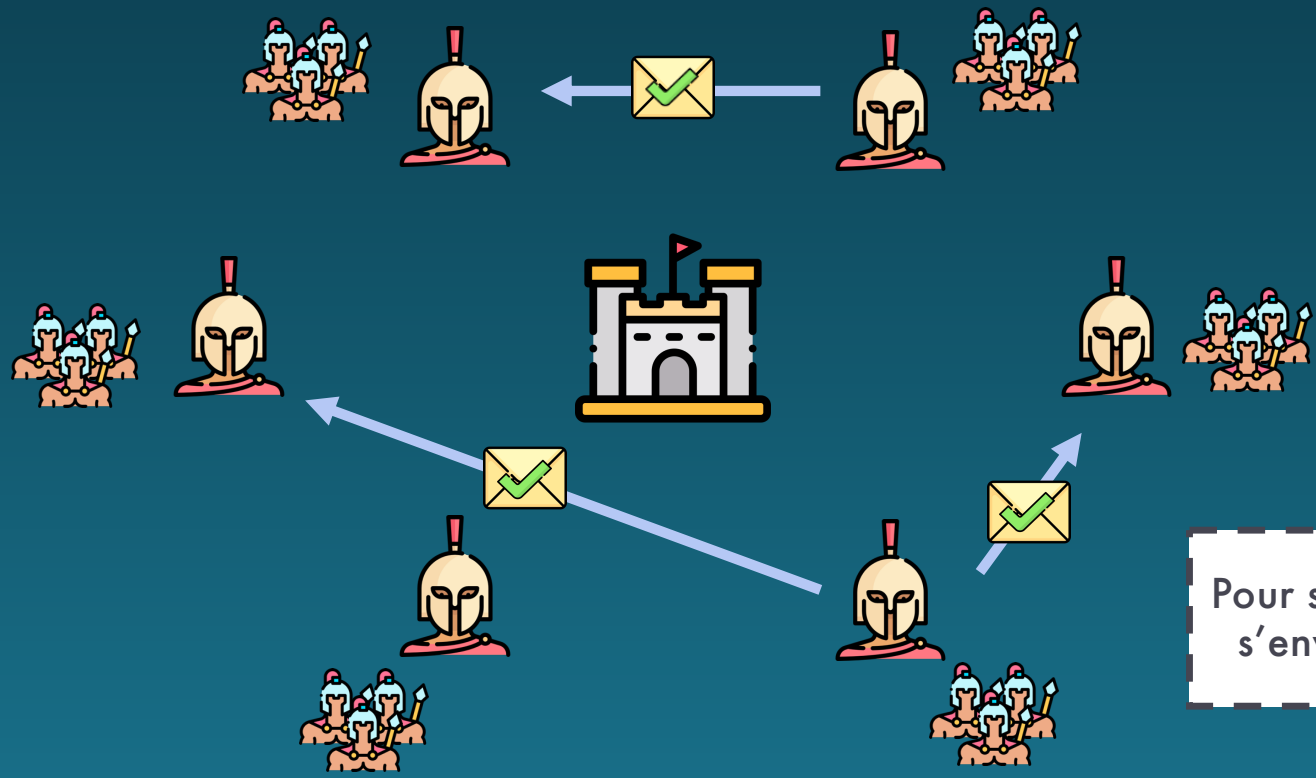
Problème des généraux byzantins



Ils doivent, le matin du jour suivant, décider d'attaquer ou de battre en retraite

Leslie Lamport, Robert Shostak et Marshall Pease – 1982

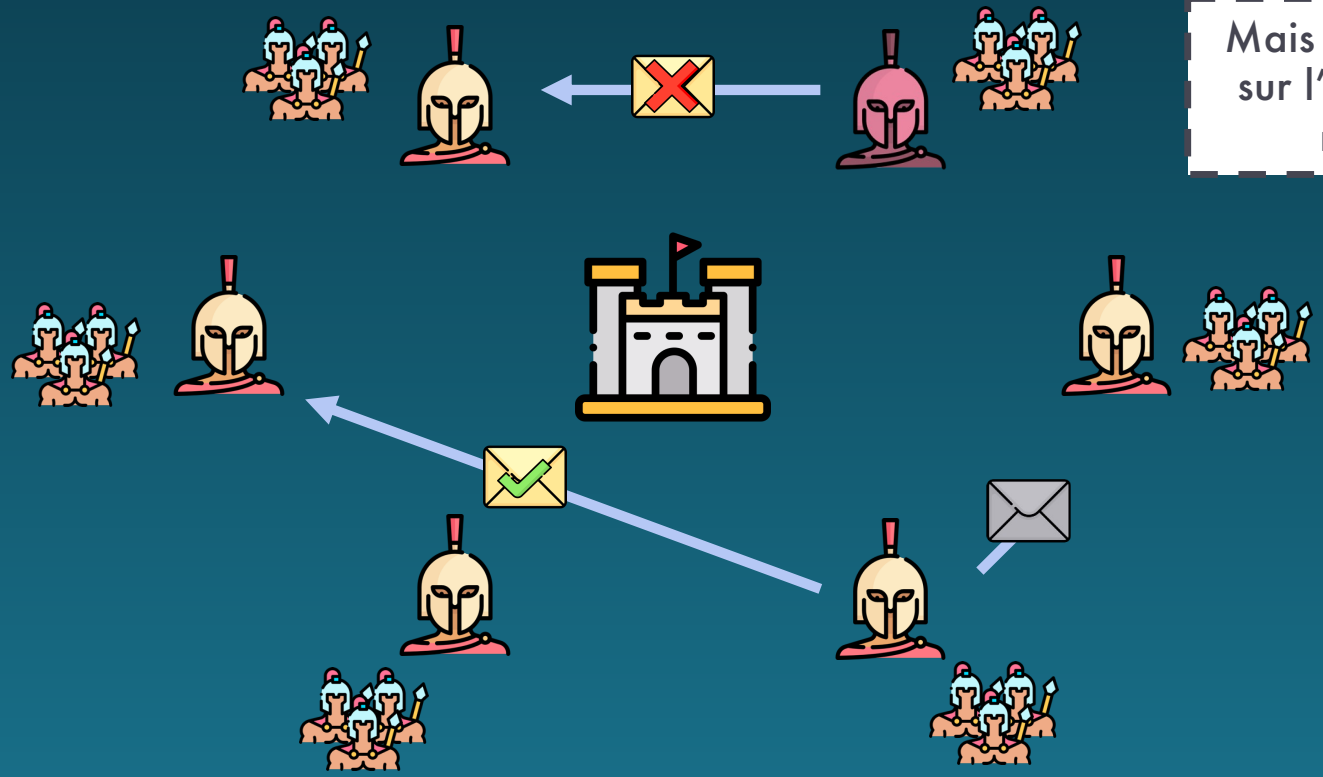
Problème des généraux byzantins



Pour se mettre d'accord, ils s'envoient des messages

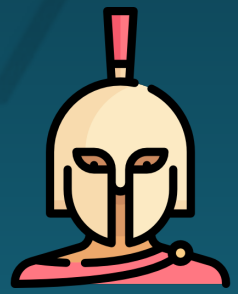
Leslie Lamport, Robert Shostak et Marshall Pease – 1982

Problème des généraux byzantins



Mais aucune garantie sur l'authenticité des messages...

Résolution du problème

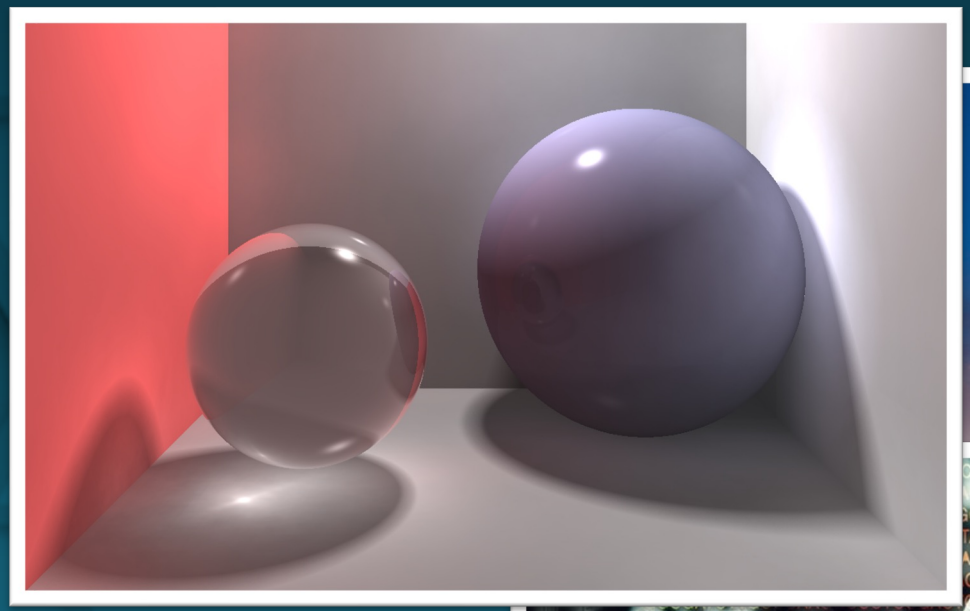


Barbara Liskov et Miguel Castro (1990)

Exact, mais 1/3 max de défectueux
Temps exponentiel...

Solution approchée ?

Solution probabilistique



Satoshi Nakamoto – 2008

Satoshi Nakamoto – 2008

31 Octobre 2008 – “Bitcoin: A Peer-to-Peer Electronic Cash System”

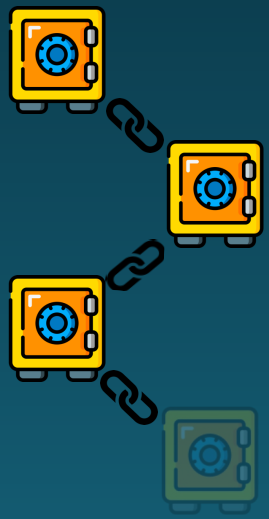
3 Janvier 2009 – Lancement du Bitcoin (block de genèse)

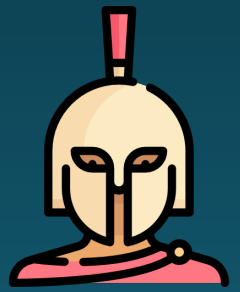
22 Mai 2010 – Premier achat en bitcoin (Deux pizzas pour 10.000 BTC)

Septembre 2021 – Buste de Satoshi Nakamoto à Budapest

bitcoin.org

Naissance de la technologie Blockchain



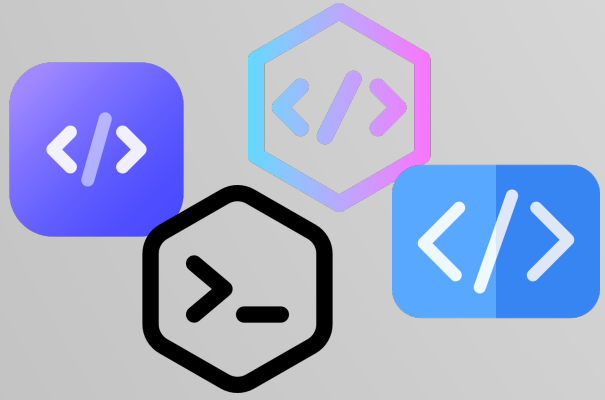


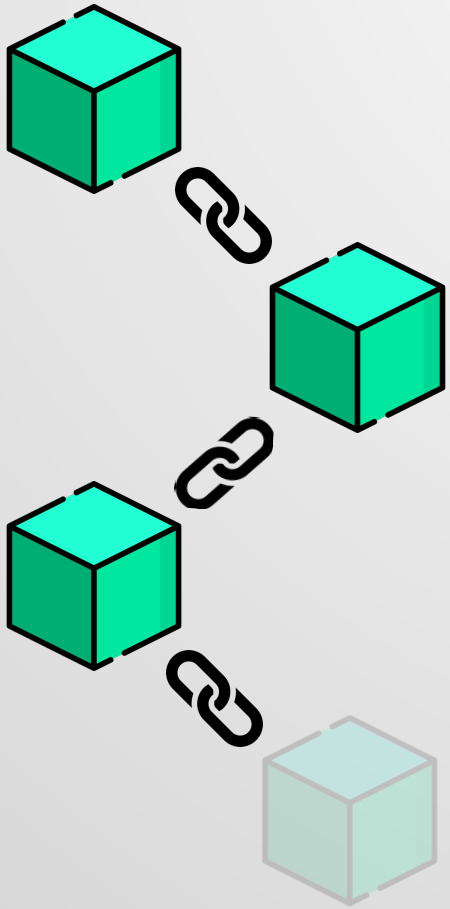
Blockchain ?

Block = Bloc

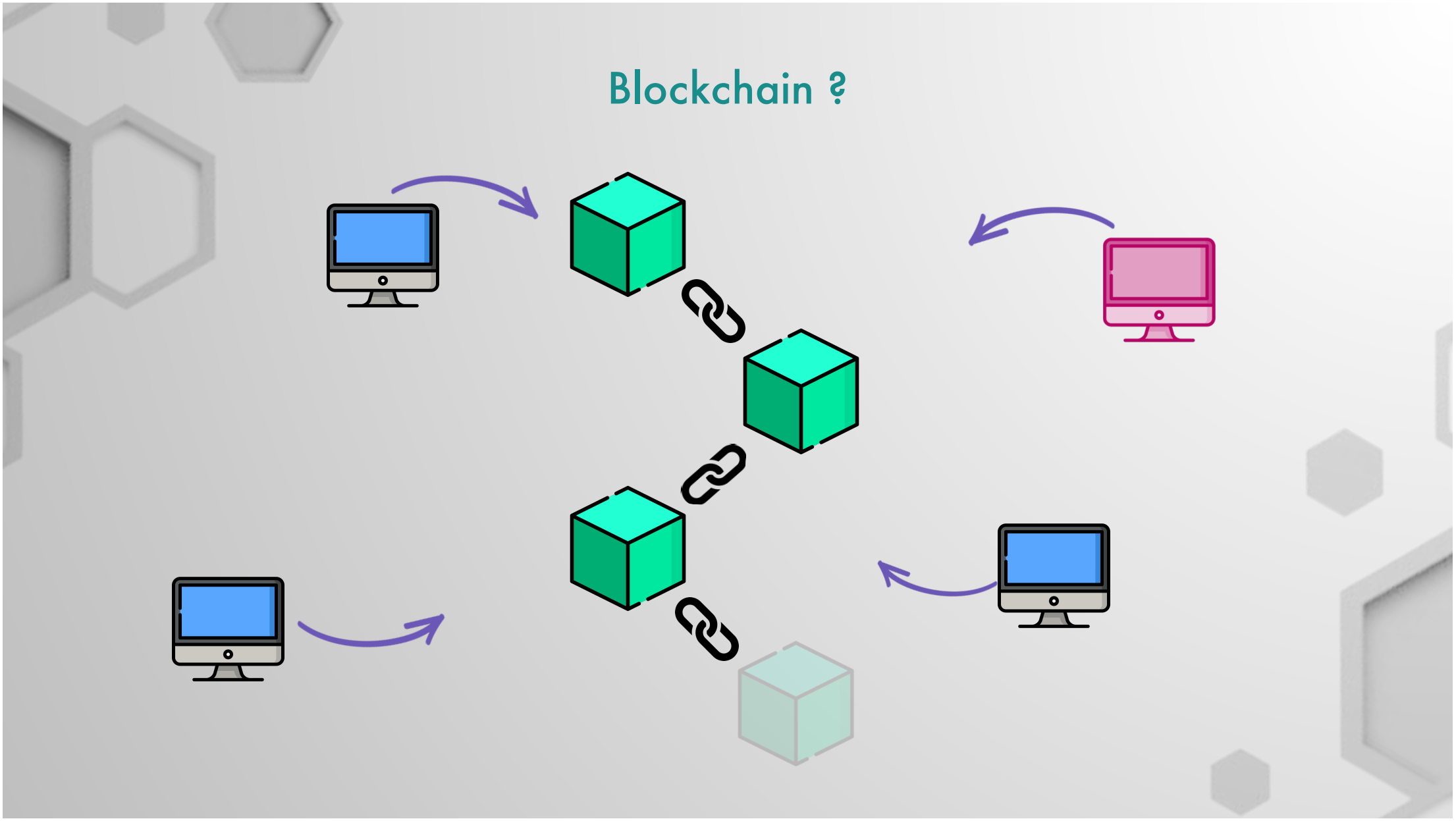
Chain = Chaîne

Chaîne de blocs



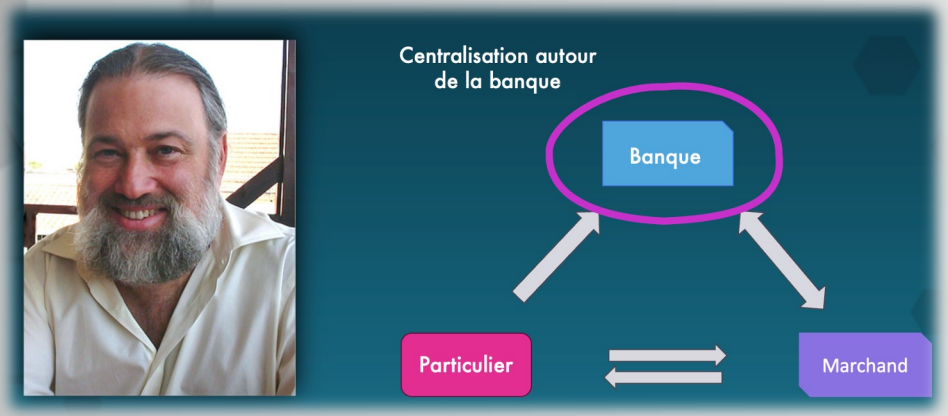


Blockchain ?



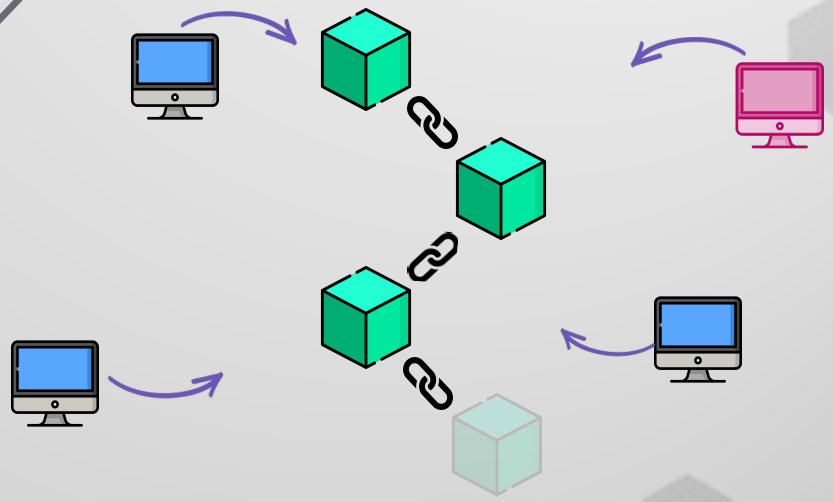
Miracle ?

Décentralisation

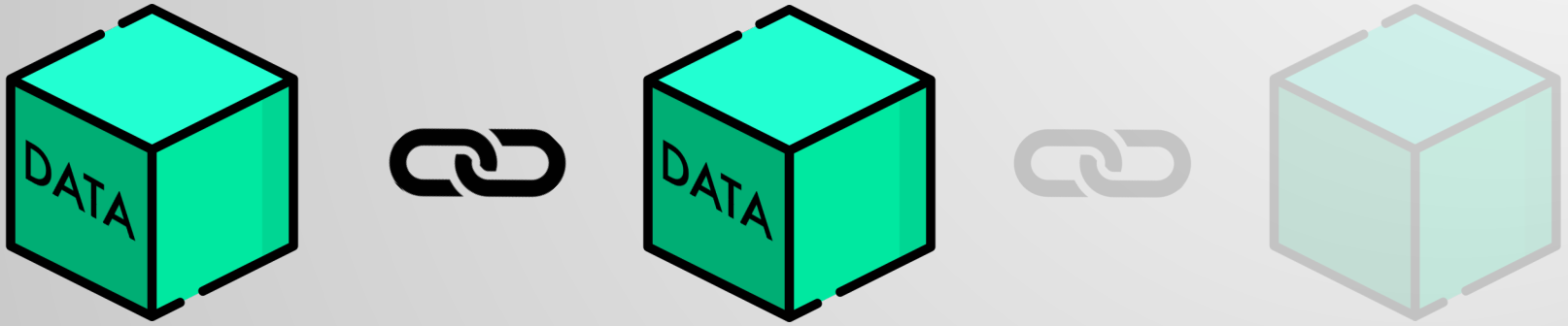


La banque est un médiateur et possède le véritable contrôle

Personne ne possède le contrôle

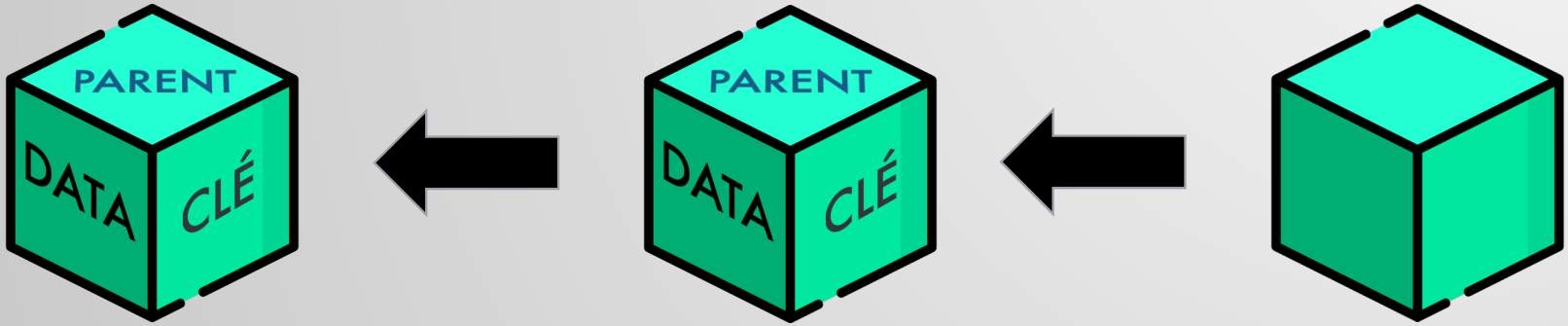


Concrètement



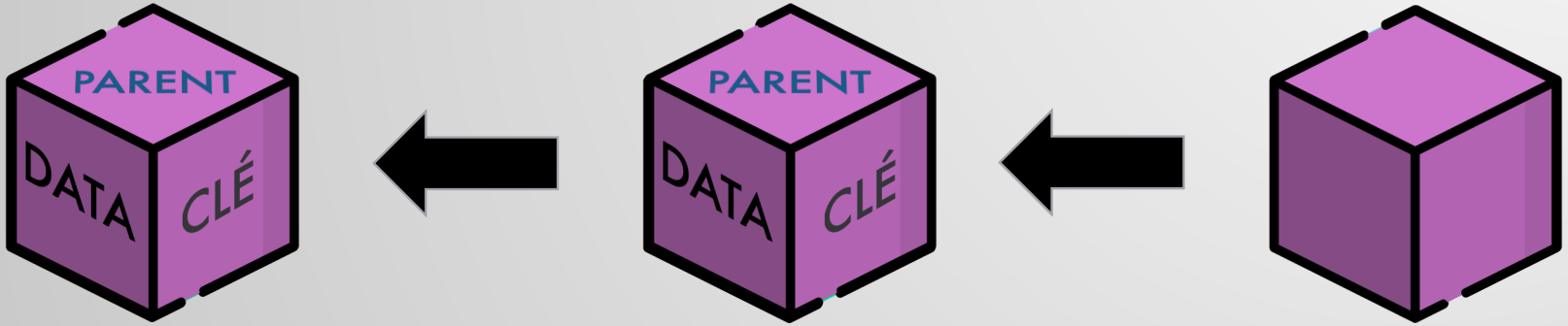
Base de donnée stockée sous la forme de blocs distincts, disposés les uns après les autres

Concrètement



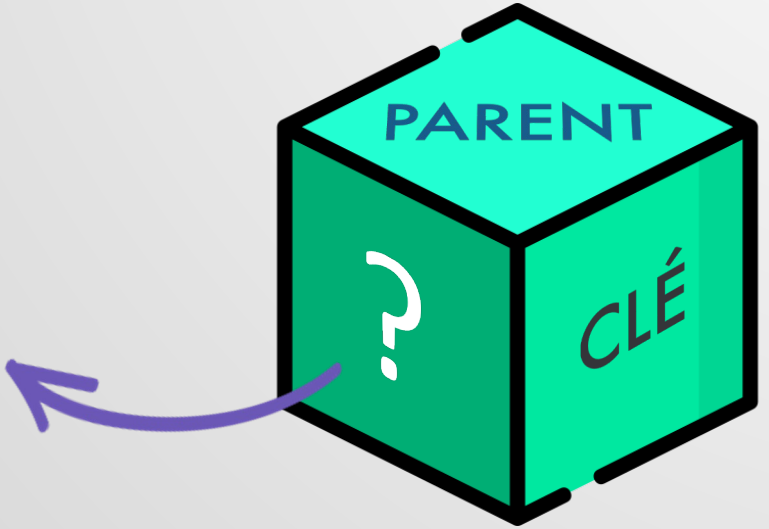
Chaque bloc pointe vers son prédecesseur

Concrètement



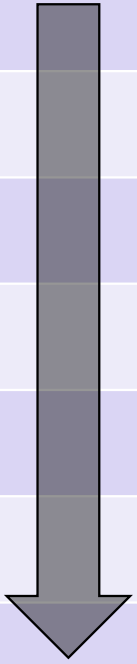
Un système cryptographique invalide
tous les enfants d'un bloc corrompu

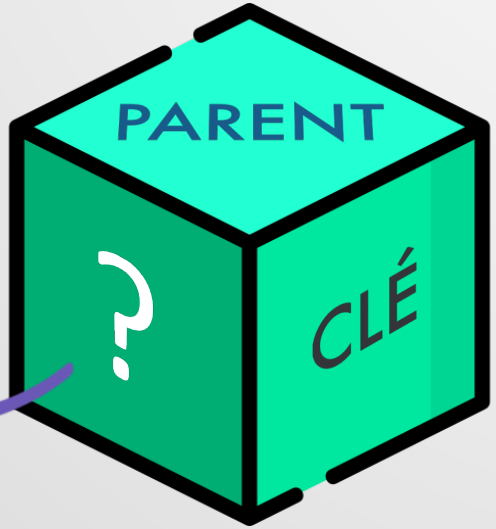
Le fameux “Ledger”



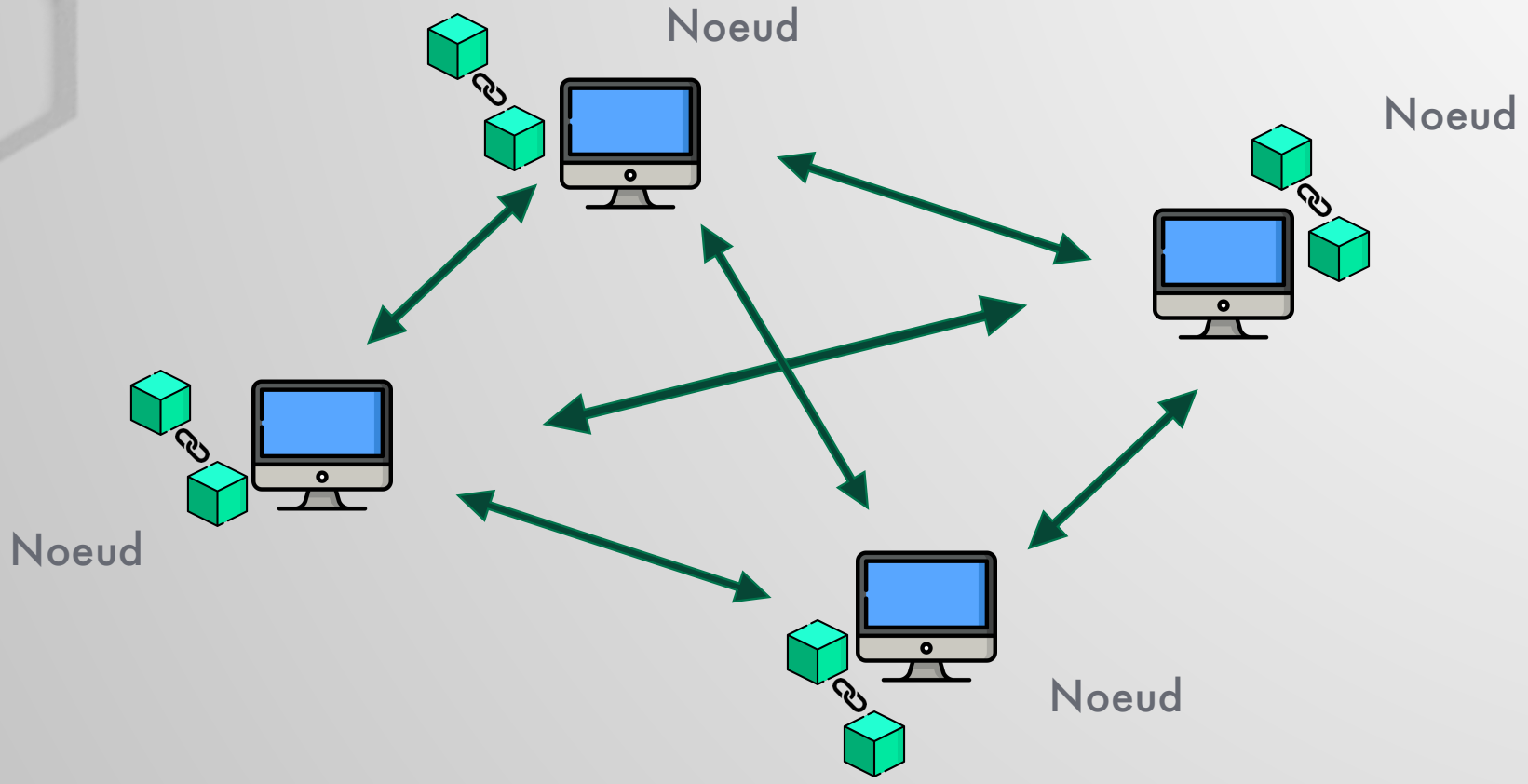
Le fameux "Ledger"

Nom	Donnée	Signature
Alice	…	
Alice	…	
Bob	…	

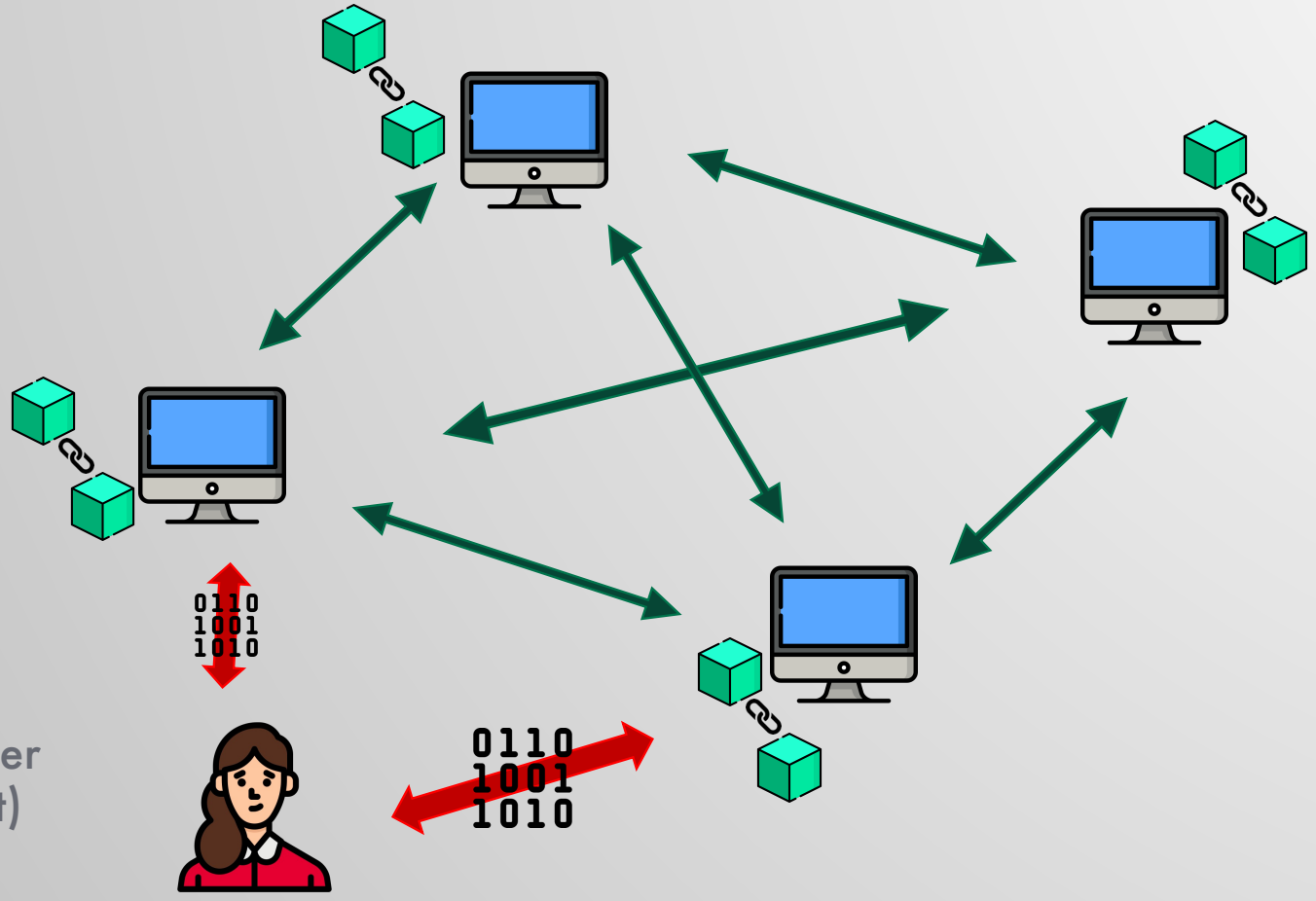




Base de données “distribuée”

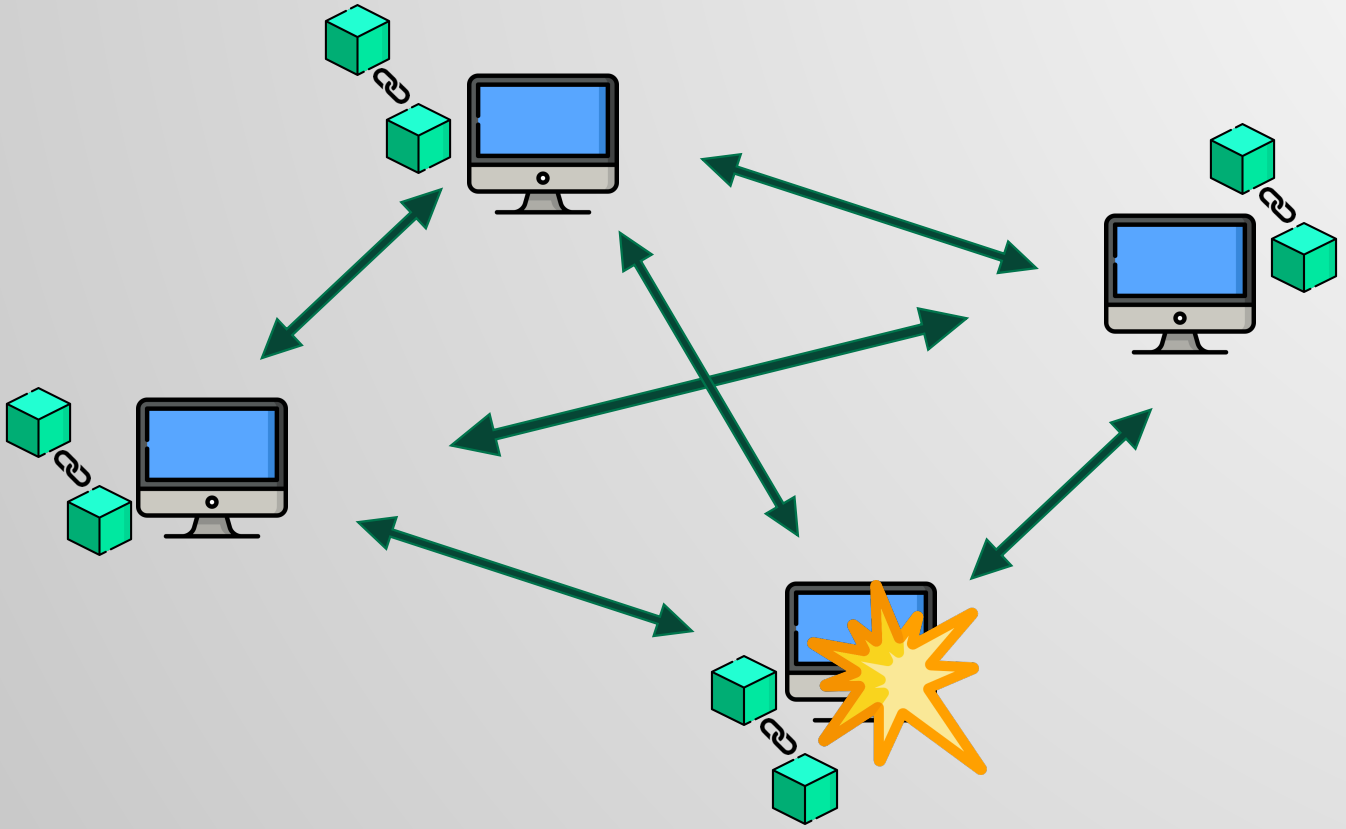


Base de données “distribuée”

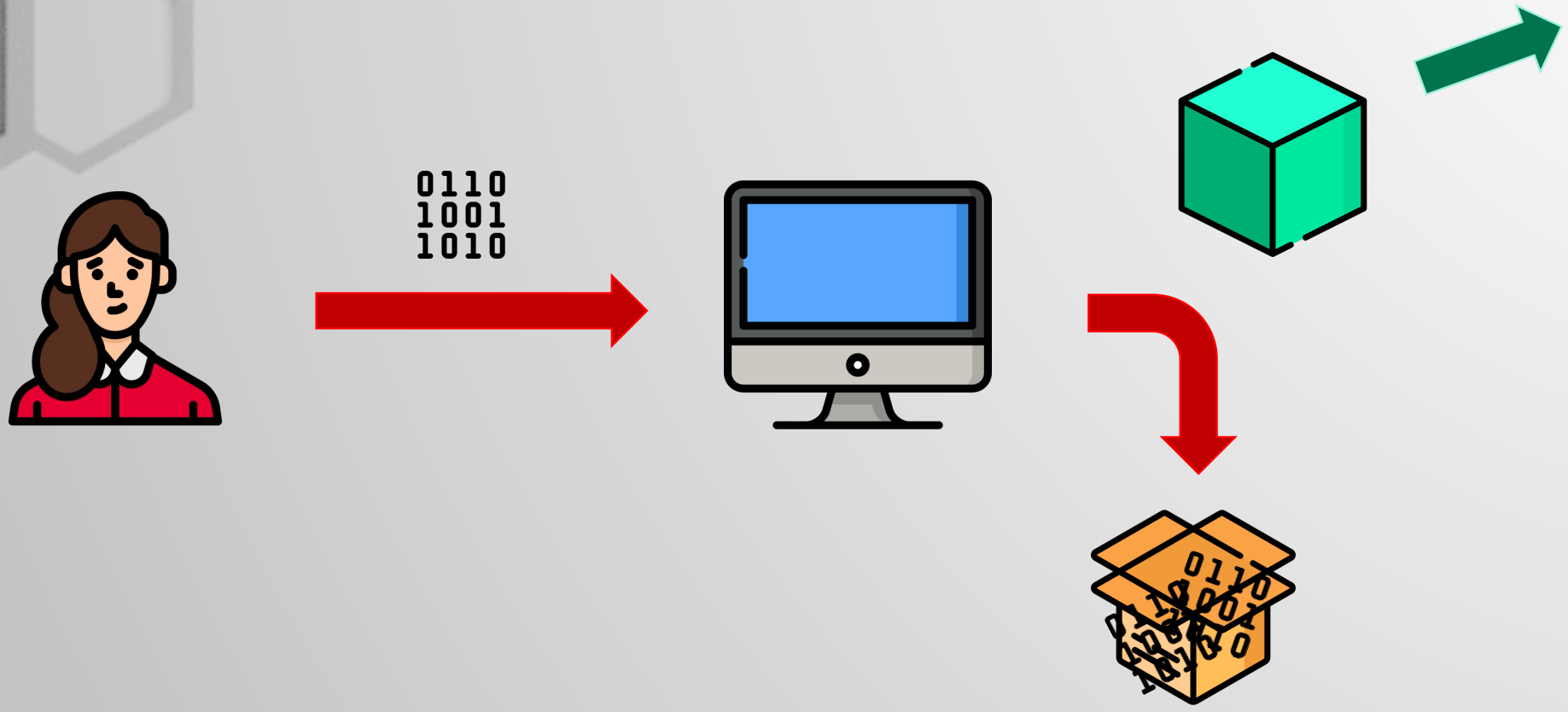


Particulier
(Wallet)

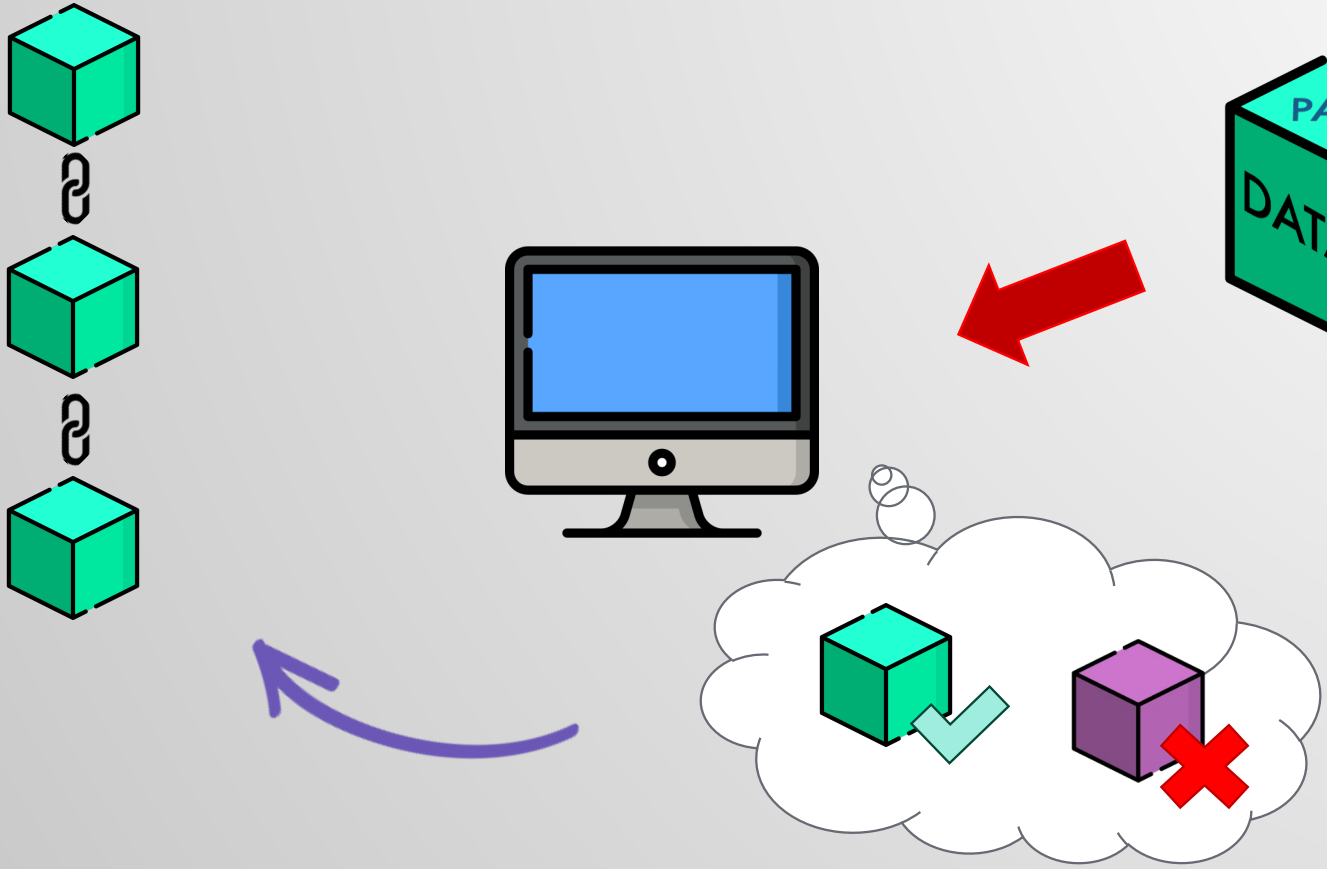
Base de données “distribuée”



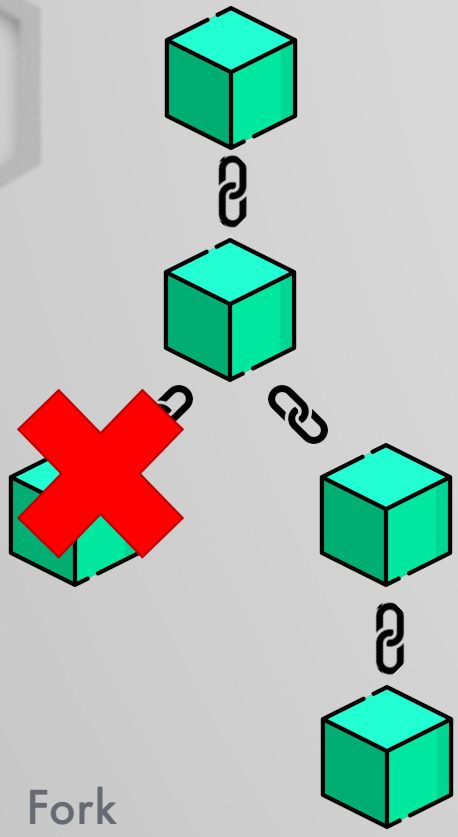
Synchronisation entre “Nodes”



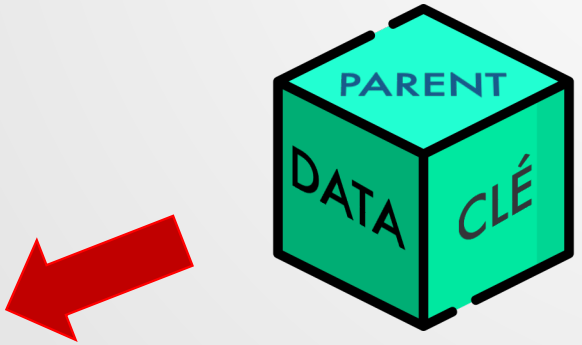
Synchronisation entre “Nodes”

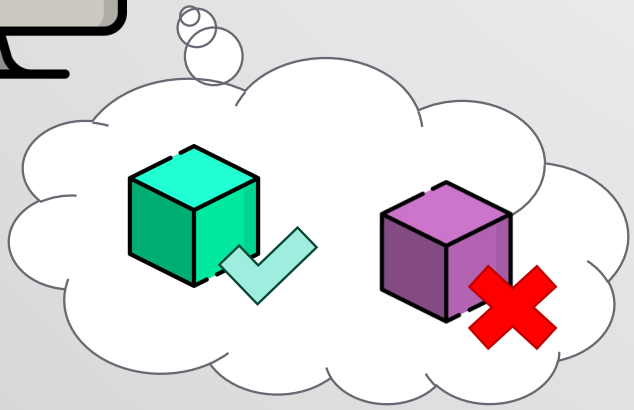


Synchronisation entre “Nodes”

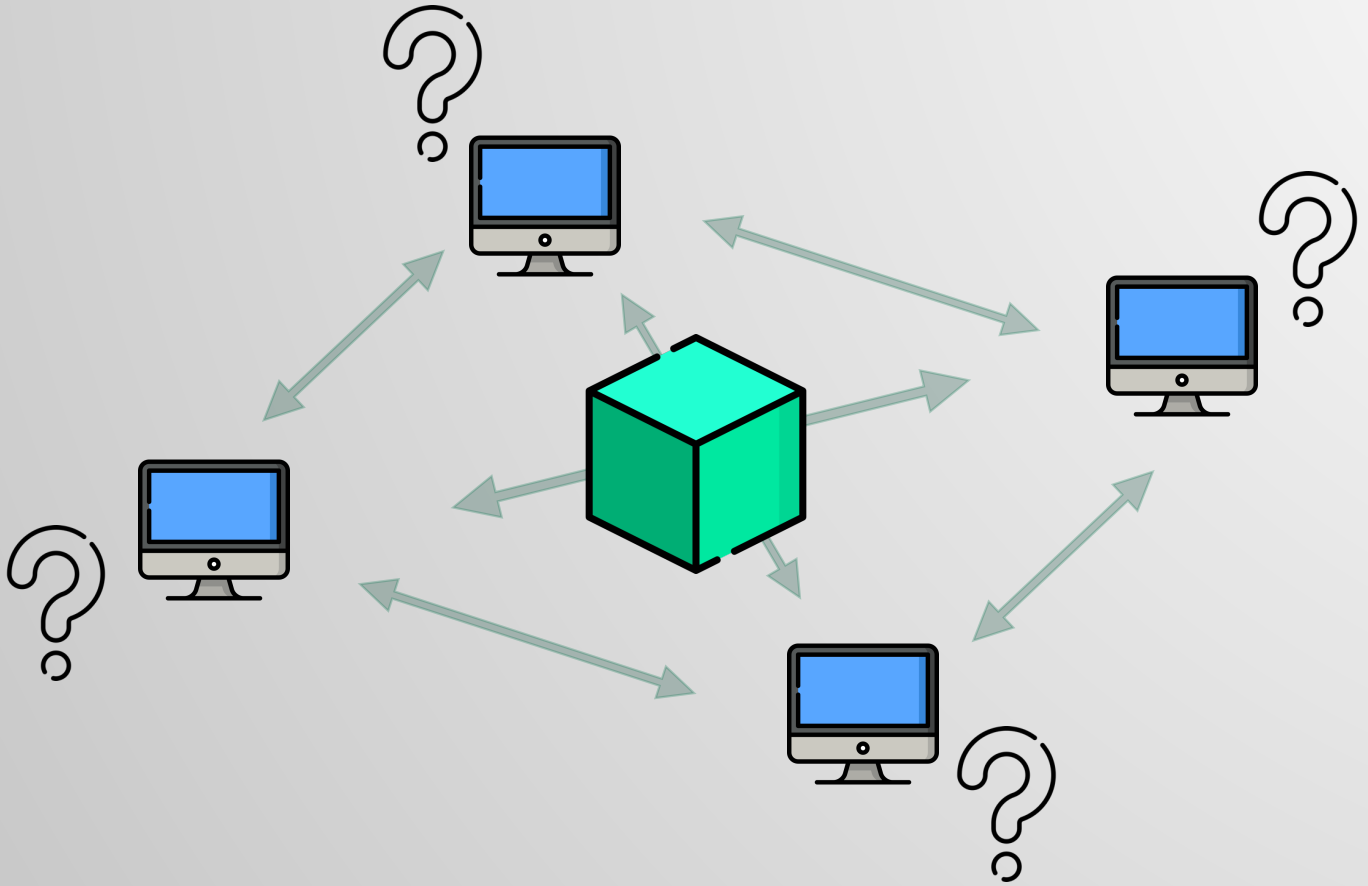


Fork

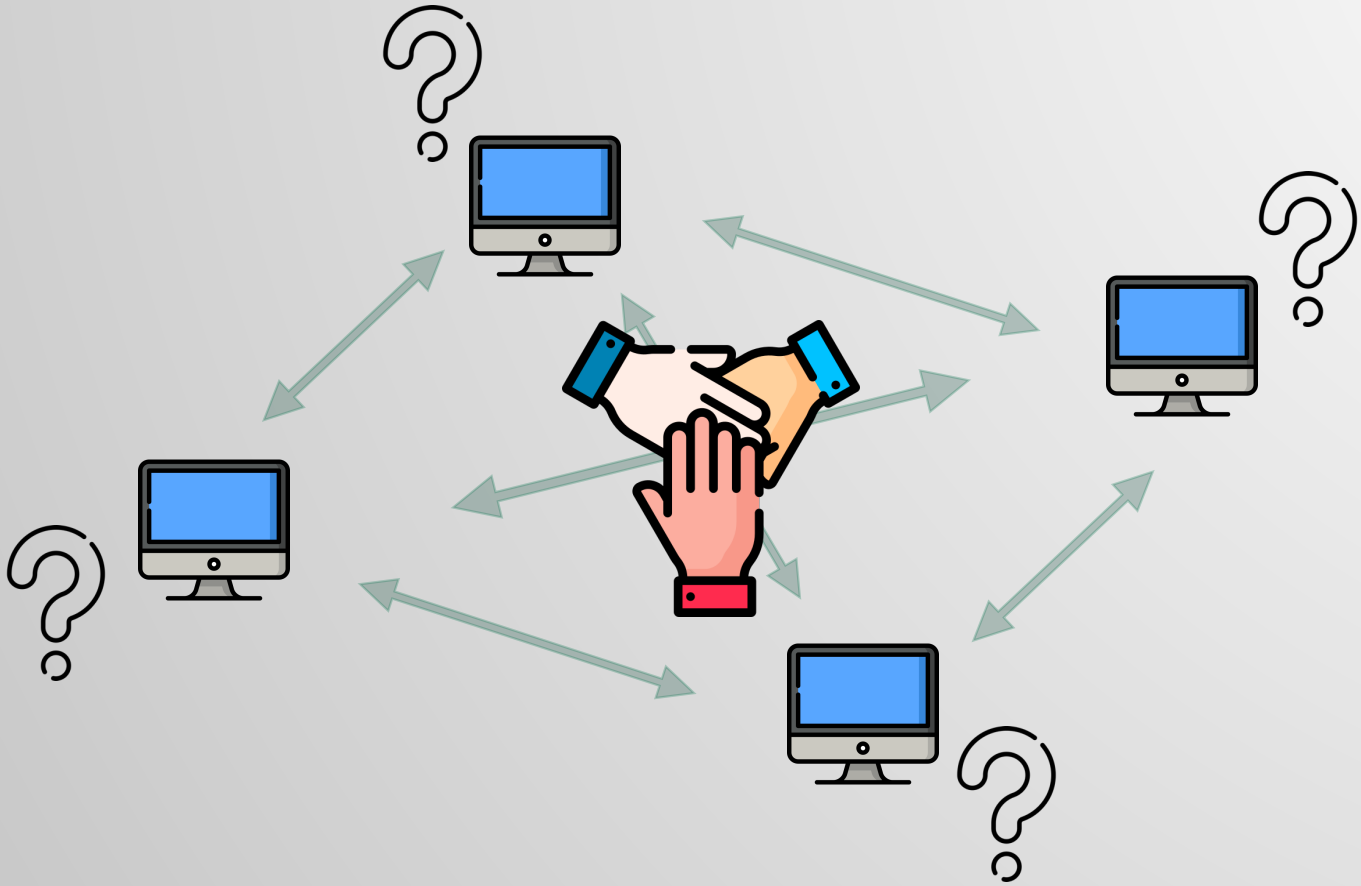




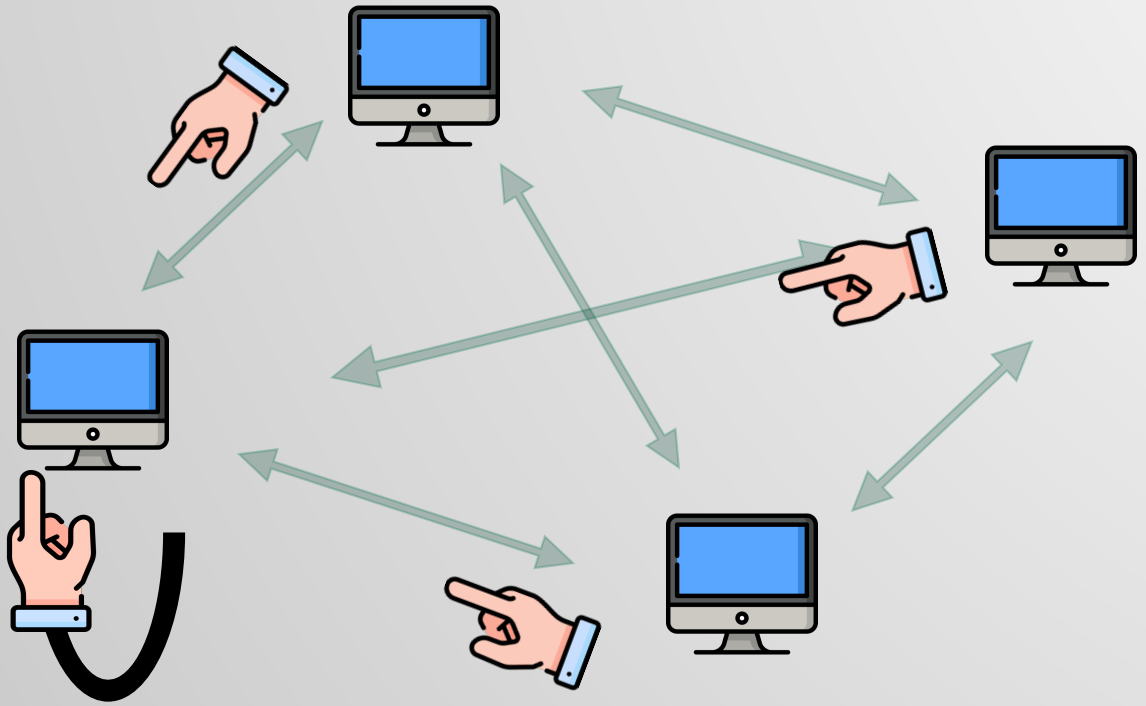
Consensus



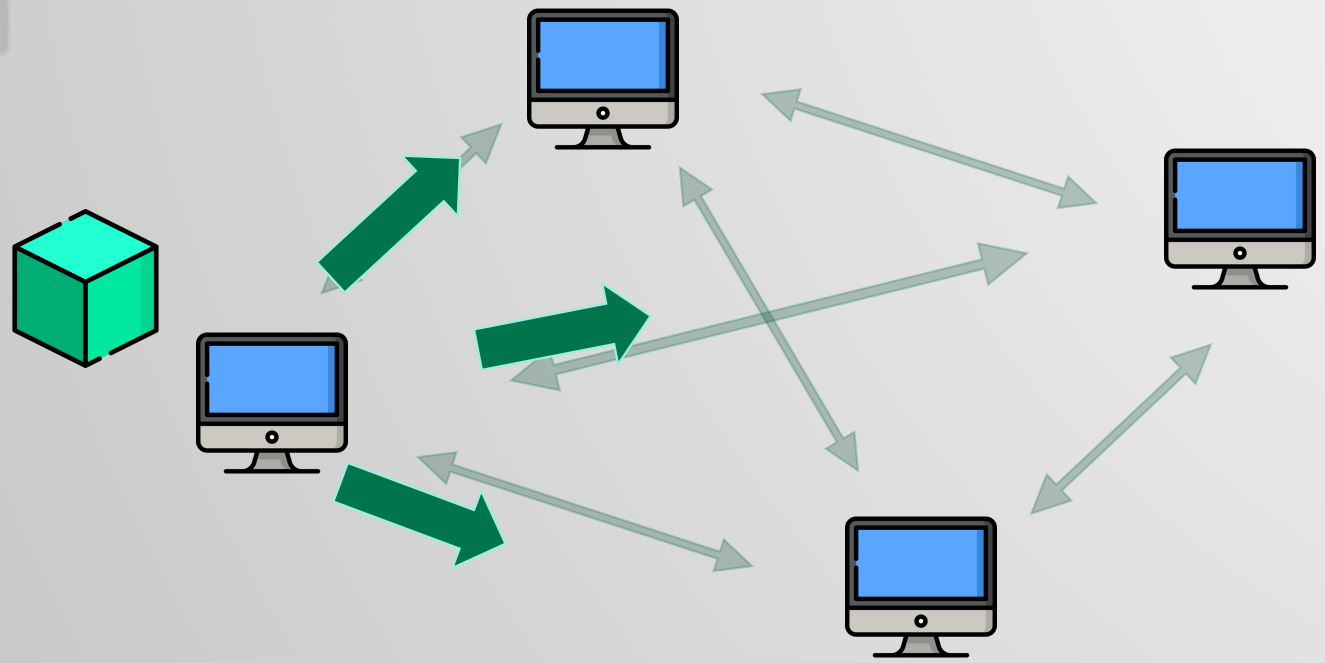
Consensus



Consensus



Consensus

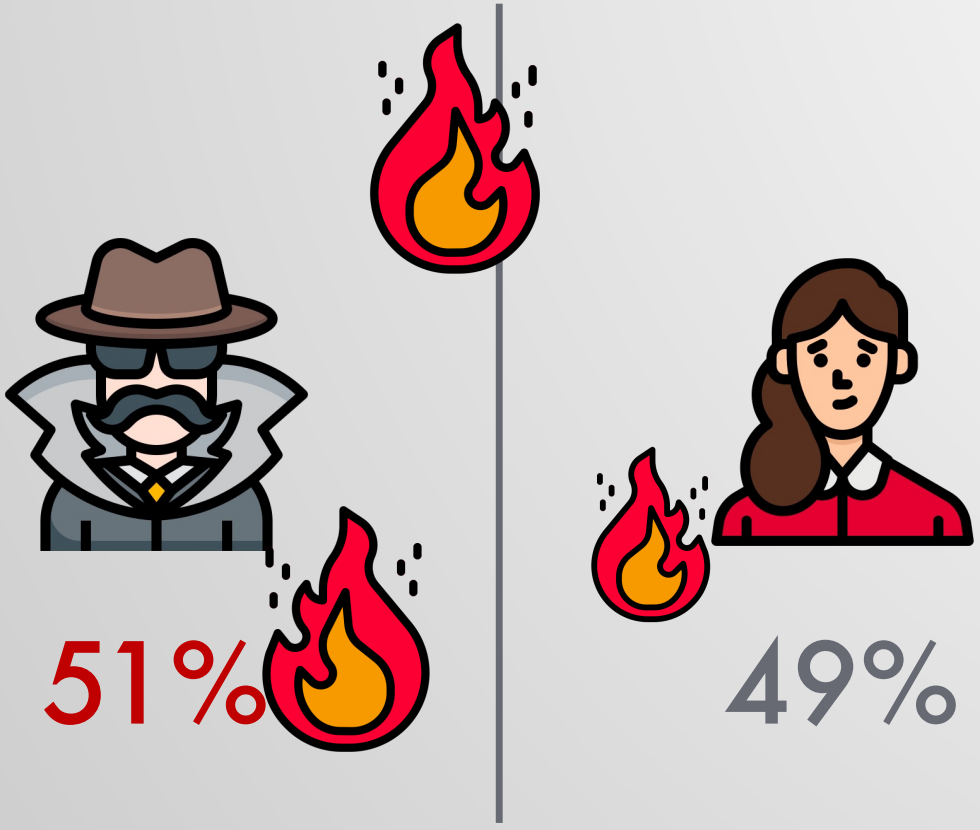


Retour aux généraux byzantins

13%

87%

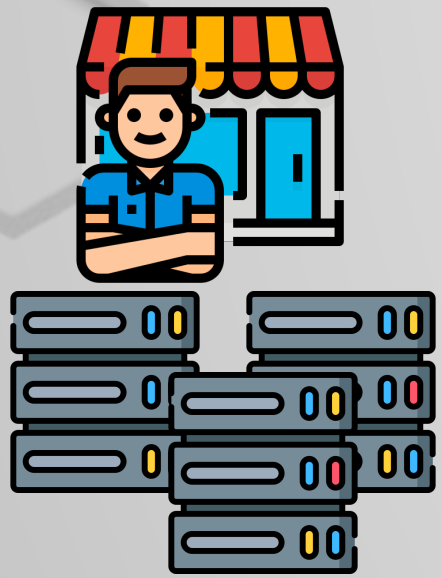
Retour aux généraux byzantins

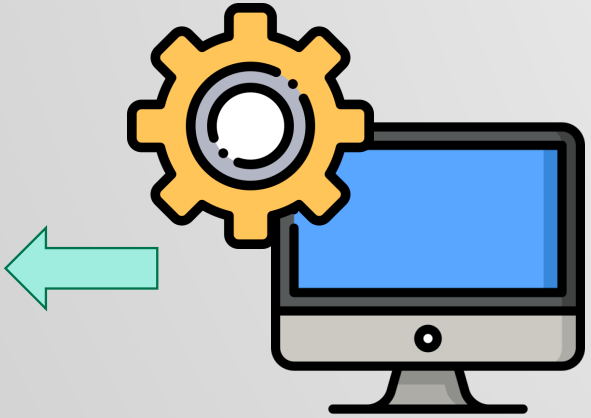


51%

49%

Motivation

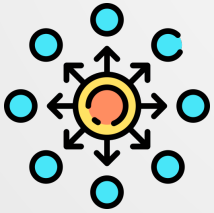




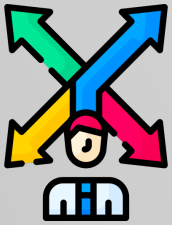
En résumé

Immutabilité

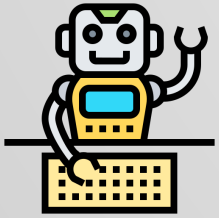
Sécurité



Décentralisation



Adaptabilité



Automatisation

SIMPLE !

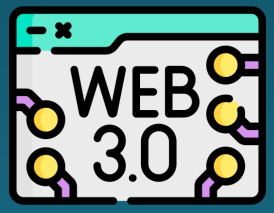
Enjeu international

Applications

Cryptomonnaies
(Bitcoin, Ethereum)

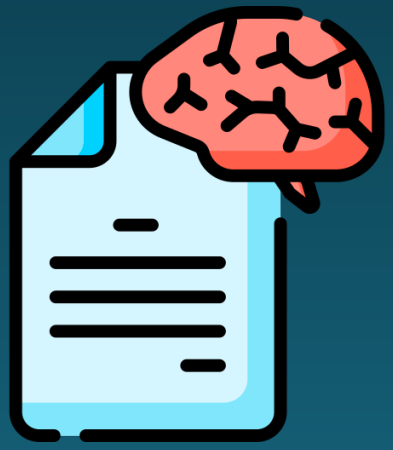
Médical

Vote



WEB 3

Applications



Smart Contracts

Exemples

Blockchain et Applications

Quiz 1

Qu’est-ce que la blockchain ?

Blockchain et Applications

TD 1

Un peu de Python