Blockchain
Cours 2

Objectif de cours

Les inconvénients des systèmes de transactions existants
Blockchain et digitalisation : Pourquoi la Blockchain est-elle appropriée pour les entreprises ?

Optimisation du Traitement de Fichiers Avant l'Invention des SGBDR

Redondance et inconsistance des données

– certaines info se trouvent sur plusieurs fichiers

Difficulté d'accès aux informations non prévues

– nécessité d'écrire de nouveaux prog. d'accès

Dépendance : rep. interne / Applications

– changement de structure -> re-programmation des App

Atomicité et pb de concurrence

– erreur, pannes, accès concurrents -> introduisent des inconsistances

1960: les SGFs

➲Problème de surcharge ☹
➲Comment libérer le programmeur ?

⇒ SGBD ☺

- **1970**: Codd paper; les fondements des BDR
- **1980**: Les SGBD-R sur le marché

Évolution du système de base de données:
~ Une longue histoire

History Repeats Itself

"Relational vs. CODASYL".

The "SQL vs. NoSQL"

One Size Fits All
An Idea Whose Time Has Come and Gone
by
Michael Stonebraker

MICHAEL STONEBRAKER, 2014
-Research and products are central to many relational database systems

In Science
- Turing Awardees

1960S – IBM IMS → Hierarchical data model.

1970s – RELATIONAL MODEL

1980s – The relational model wins

Transaction processing **1998**

2000s – INTERNET BOOM

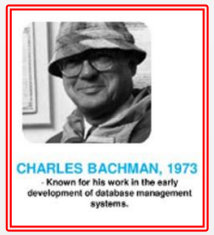
2000s – DATA WAREHOUSES

2009– NoSQL

2010s – NewSQL

2010s – HYBRID SYSTEMS

- **NoSQL projects**
- Graph DB Neo4j (2000)
- CouchDB (2005)
- MongoDB (2007)



CHARLES BACHMAN, 1973
- Known for his work in the early development of database management systems.

EDGAR CODD, 1981
-Invented Relational model (RM), the theoretical basis for relational databases and relational database management systems.

Gray Stonebraker Ellison

JAMES GRAY, 1998
-For seminal contributions to database and transaction processing research

DB-Engine*: **316** DBMS en 2016
*http://db-engines.com/en/ranking

Le concept de transaction

- **Définition:**
  - Une **transaction** est une séquence d'opérations (lecture/ écriture) qui forment une seule unité de travail.
  - **Exemple:** Virements en banque, achats en ligne, inscription aux cours
  - Une transaction est souvent déclenchée par un programme d'application

    - commencer une transaction **START TRANSACTION**
    - Accès à la base (lire/écrire)
    - Calculs en MC
    - fin transaction : Une instruction COMMIT ou ROLLBACK est exécutée.

```
BEGIN TRANSACTION
   [SQL statements]
COMMIT     or
ROLLBACK (=ABORT)
```

Challenges

- Voulez-vous exécuter plusieurs applications simultanément
  - Toutes ces applications lisent et écrivent des données dans la même BD
- **Solution simple**: ne servir qu'une application à la fois
  - Quel est le problème?

- Voulez-vous que plusieurs opérations soient exécutées de manière atomique sur le même SGBD?

C'est quoi le problème ?

Account 1 = $100
Account 2 = $100
Total = $200

- **App 1:**
  - Set Account 1 = $200
  - Set Account 2 = $0
- **App 2:**
  - Set Account 2 = $200
  - Set Account 1 = $0
- At the end:
  - Total = $200

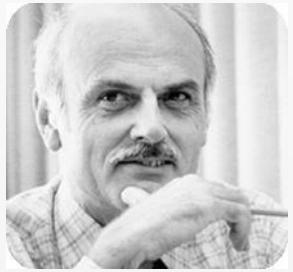
- **App 1**: Set Account 1 = $200
- **App 2**: Set Account 2 = $200
- **App 1**: Set Account 2 = $0
- **App 2**: Set Account 1 = $0
- At the end:
  - Total = $0

C'est ce qu'on appelle la mise à jour perdue aka conflit WRITE-WRITE

Turing Awards in Data Management

Charles Bachman, 1973

IDS and CODASYL



Edgar Frank Codd, 1981

Relational model

Jim Gray, 1998

Transaction processing

Michael Stonebraker, 2014

INGRES and Postgres

Responsabilité du SGBD

➲ SGBD doit vérifier les propriétés règles **ACID** (*atomicity*, *consistency*, *isolation* et *durability*)

➲ Garantir l'exécution correcte des transactions

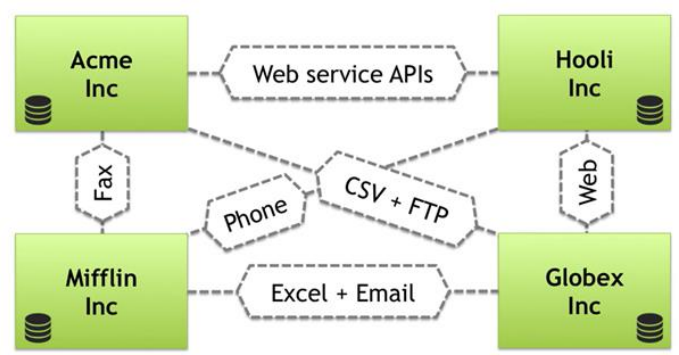
➲ Gérer l'exécution concurrente des transactions

❑ Implémentation d'un ordonnanceur

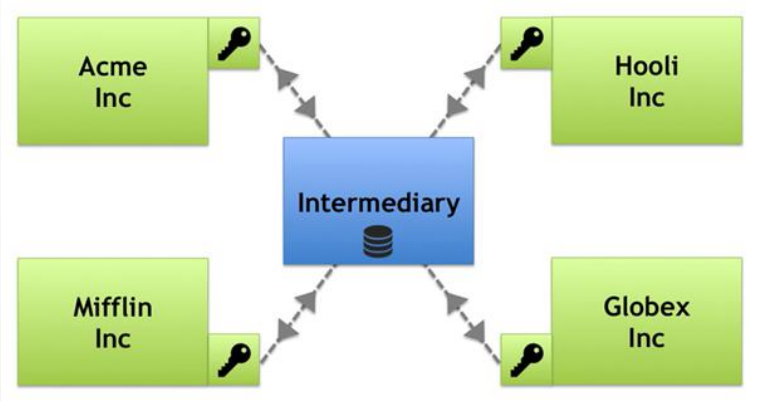
- 2PL : Two-Phase Locking
- 2PL Strict : Strict Two-Phase Locking
- 2PC : Two-Phase Commit
- 3PC : Three-Phase Commit

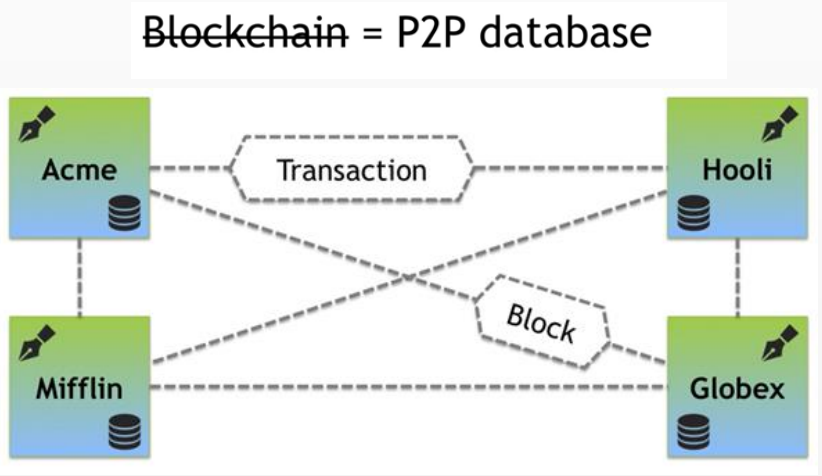
~~Blockchain~~ = P2P database

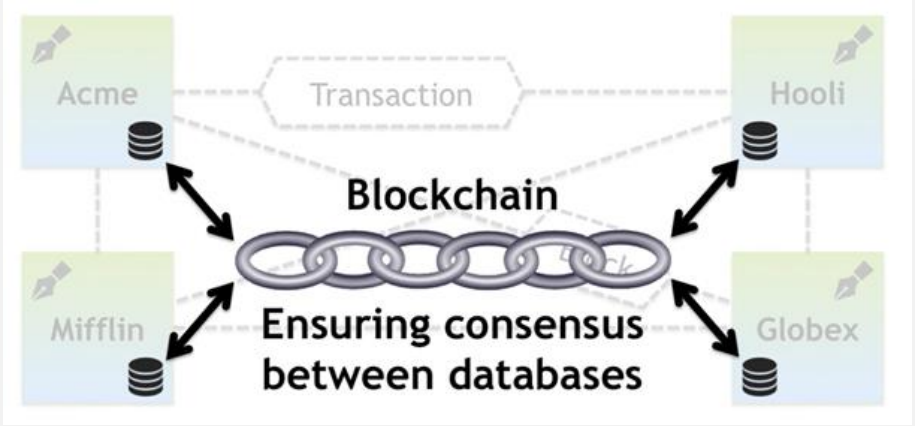
Coordination par les données



L'intermédiaire de confiance





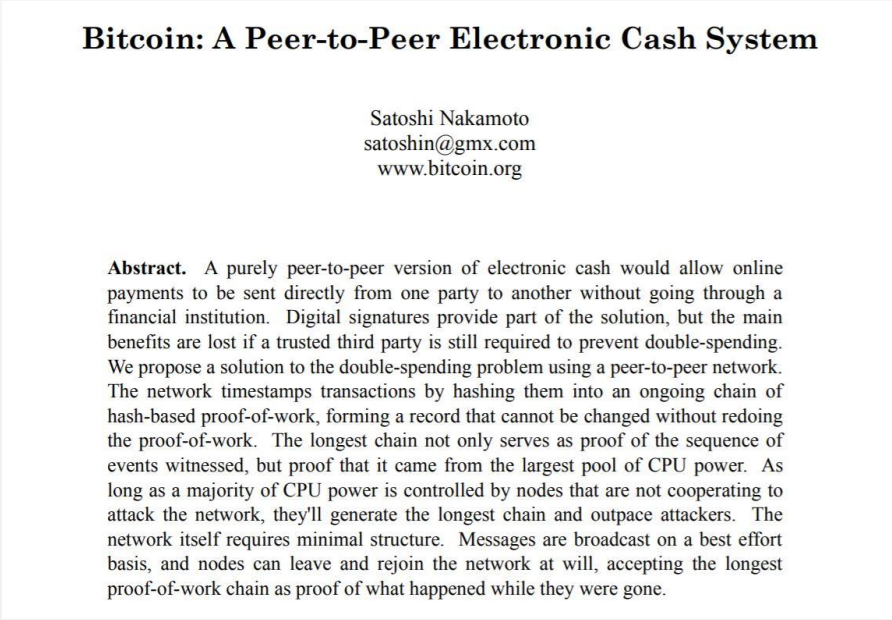


Problèmes et solutions: Gérer la confiance

- **Transmettre la confiance** est un problème connu et recherché en informatique depuis le début des années 1990s
- Les obstacles techniques à transmission de la confiance ont pu être partiellement résolus grâce à la cryptographie
  - ➢ Comment faire confiance à un groupe d'individus qu'on ne connait pas ?
  - ➢ Comment formaliser la confiance ?

En 2008, Satoshi Nakamoto publie un papier *Bitcoin: A Peer-to-Peer Electronic Cash System* qui présente une solution à ce problème. (Accessible à https://bitcoin.org/bitcoin.pdf)

La publication fait suite à la crise financière de la même époque, et de la perte de confiance dans les institutions bancaires.



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

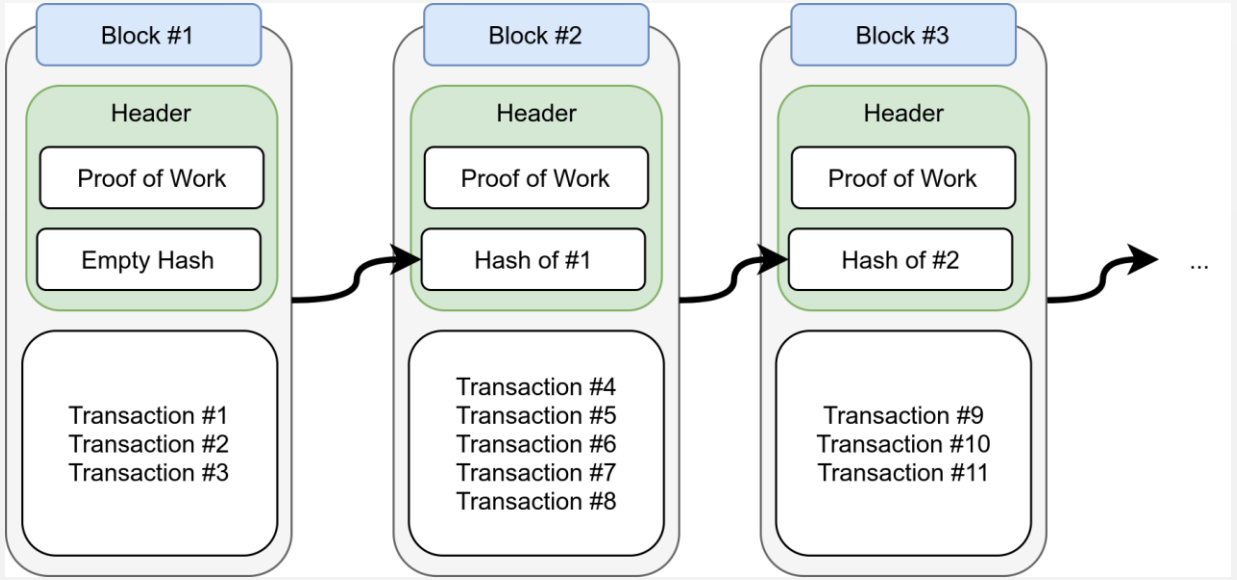
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Problèmes et solutions: Gérer la confiance

- **Problème d’intégrité:**
  - Chaque utilisateur possède une clé pour signer ses messages et en assurer l’intégrité
- **Problème de confiance:**
  - Un algorithme de consensus s’assure que les décisions sont prises par les entités de confiance
- **Problème de centralisation**
  - Les participants sont répartis, et la suppression d'une partie d'entre eux n'empêche pas la blockchain de continuer à fonctionner.

Qu'est-ce que la technologie blockchain?

La technologie blockchain est une forme de **registre numérique distribué**, sécurisé et immuable. Elle fonctionne sur la base de blocs de données connectés de manière cryptographique, assurant la transparence et la sécurité des transactions. La décentralisation et l'absence d'intermédiaires en font un élément clé de confiance pour diverses applications



Qu'est-ce que la technologie blockchain?

- **Techniquement**, la blockchain est une base de données backend qui maintient un grand livre distribué pouvant être inspecté ouvertement.
- **Sur le plan commercial,** la blockchain est un réseau de changement permettant de transférer des transactions, de la valeur et des actifs entre pairs sans l'assistance d'intermédiaires.
- **Sur le plan légal**, les blockchains valident les transactions, remplaçant ainsi les entités de confiance précédemment établies.

Pourquoi adopter la technologie blockchain ?

Manque de transparence

Les plateformes en ligne ne fournissent pas toujours des données ouvertes et accessibles concernant les résultats et les transactions.

Manipulation potentielle des résultats résultats

Les utilisateurs redoutent que les opérateurs opérateurs puissent truquer les résultats ou ou ajuster les cotes afin de favoriser certains certains résultats.

Problèmes de sécurité et de confidentialité des données

Les utilisateurs risquent l'exposition de leurs leurs données personnelles et financières en en raison de la vulnérabilité des plateformes plateformes traditionnelles.

Manque de confiance dans les résultats

Les désaccords sur les résultats ne sont pas pas toujours résolus de manière transparente, transparente, ce qui réduit la confiance des des utilisateurs.

Avantages de la Blockchain pour les Entreprises

1

Transparence/traçabilité et immuabilité

La blockchain assure une transparence totale et une immuabilité des enregistrements, ce qui réduit le risque de fraude.

Amélioration de la confiance des clients

Suivi des transactions en temps réel

Amélioration de la confiance des clients

2

Contrats intelligents

Les contrats intelligents automatisent les transactions et garantissent l'exécution des l'exécution des accords sans intervention humaine.

Définition et fonctionnement

Cas d'utilisation dans le monde des affaires

3

Répartition équitable des gains

La technologie blockchain permet une répartition équitable des gains directement directement entre les participants, sans intermédiaires.

Suppression des intermédiaires

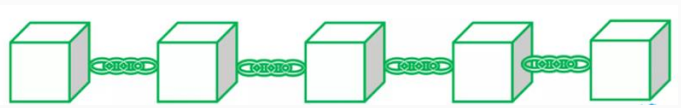
Efficacité opérationnelle

4

Amélioration de la sécurité

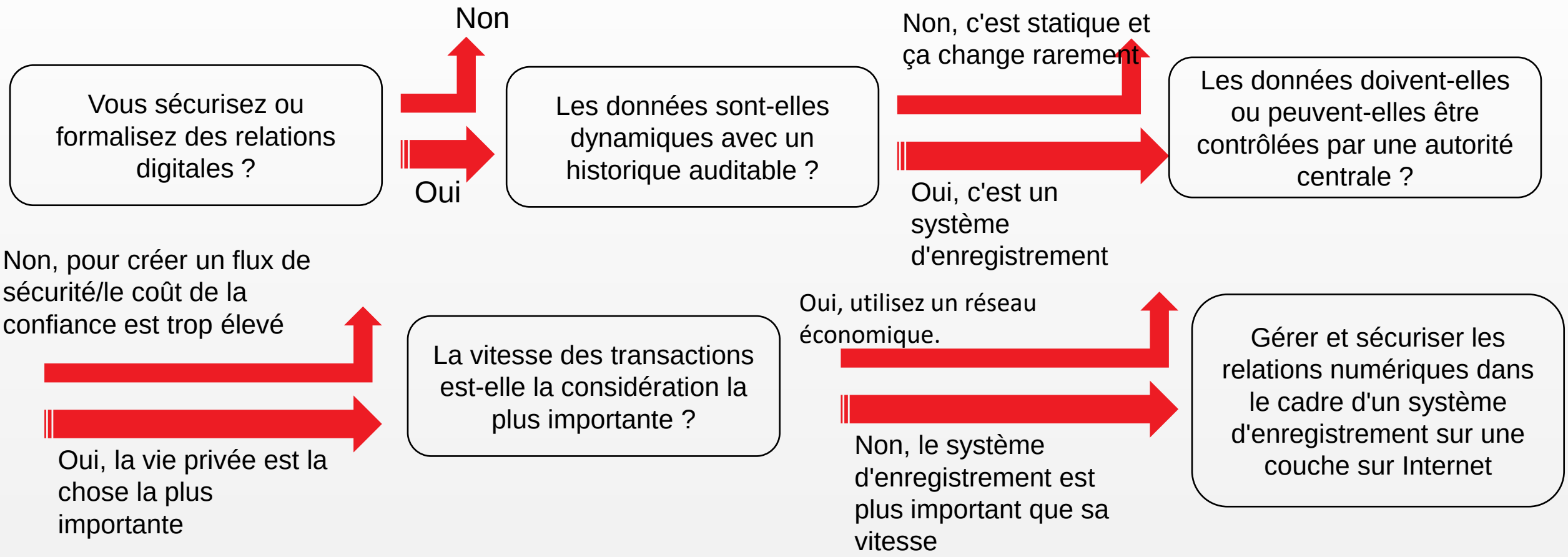
Cryptographie avancée, Résilience face aux fraudes

Principes Fondamentaux de la Blockchain : Concepts Clés à Retenir



- **Registre distribué :** Une base de données partagée et sécurisée, répartie sur un réseau d'ordinateurs.
- Une fondation pour l'internet futur et un outil pour la décentralisation.
- La confiance est établie par le protocole.
- Transactions immuables et irréversibles.
- Décentralisation totale.
- Transparence complète.
- Résilience élevée.
- Vérification de chaque transaction.
- Réseaux pair-à-pair mondiaux sans autorité centrale.
- Renforcement de la collaboration grâce à la cryptographie.
- Suppression des intermédiaires grâce aux applications blockchain.

Quand avons-nous besoin d’utiliser la Blockchain ?



Quand avons-nous besoin d'utiliser la Blockchain ?

Exercice: Les avantages de l'utilisation de la blockchain dans les paris sportifs en ligne

Transparence

La blockchain permet-elle une transparence accrue des transactions, renforçant ainsi la confiance des utilisateurs envers les applications en ligne ?

Sécurité

La technologie blockchain offre-t-elle un elle un niveau élevé de sécurité, protégeant ainsi les données personnelles et les fonds des utilisateurs utilisateurs contre les fraudes et les manipulations ?

Réduction des Frais

L'utilisation de la blockchain pour les paris sportifs en ligne permet-elle de réduire les frais frais de transaction, améliorant ainsi le rendement financier des utilisateurs ?

Les défis et les limites de l'adoption de la technologie blockchain dans les applications

Fiabilité et Scalabilité

La blockchain doit être suffisamment rapide et rapide et évolutive pour gérer les paris en temps temps réel.

Réglementation et Conformité

Les défis juridiques et de conformité liés à l'adoption de la blockchain dans l'industrie des des applications.

Protection des Données Personnelles

La confidentialité des données des parieurs tout tout en assurant la transparence des transactions.

Accessibilité et Éducation

Assurer que les utilisateurs ont accès à la technologie et sont éduqués sur son utilisation. utilisation.

4 Key Concepts of Blockchain

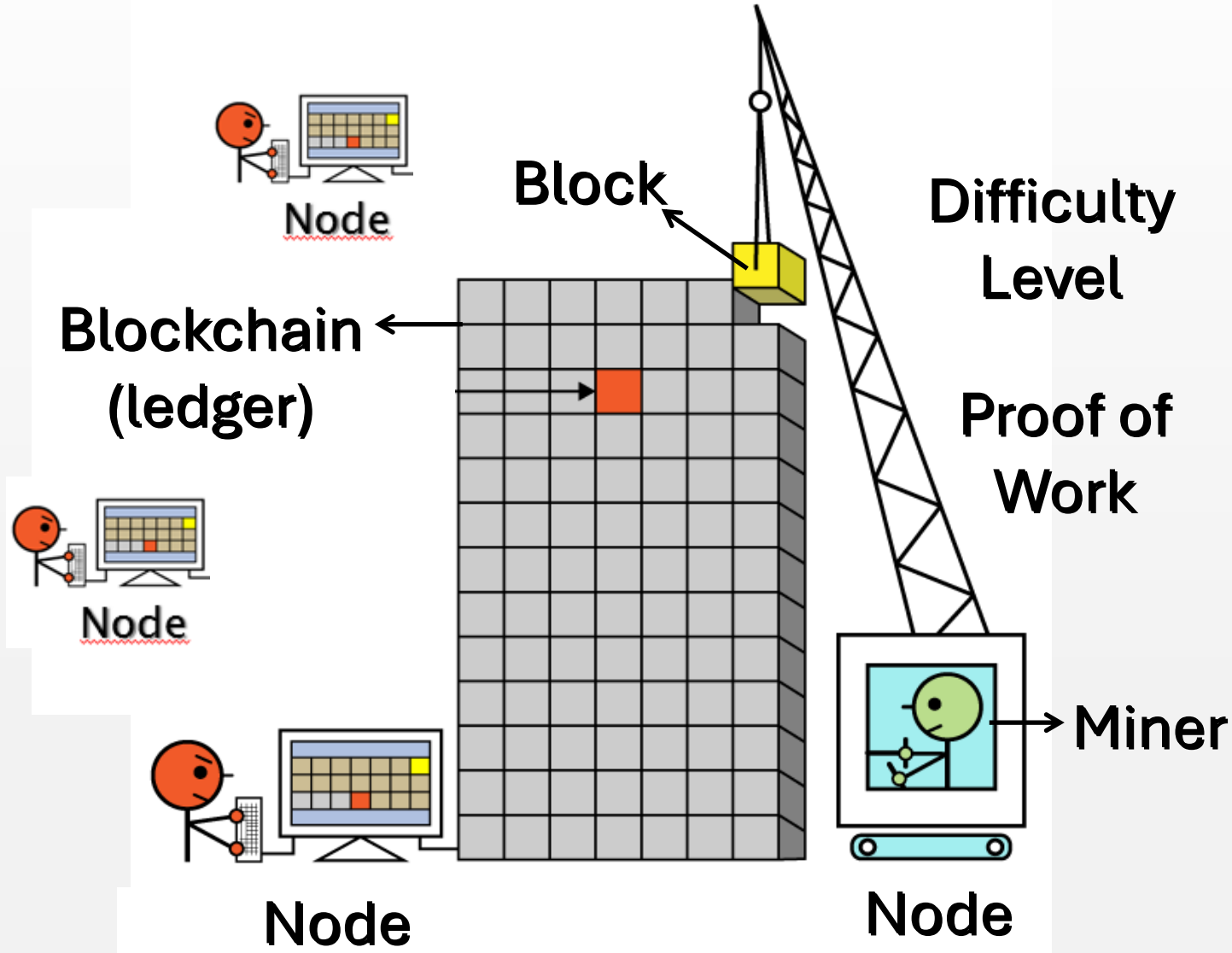
Distributed shared ledger

Cryptography

Consensus

Smart contracts

Blockchain: Blockchain Components

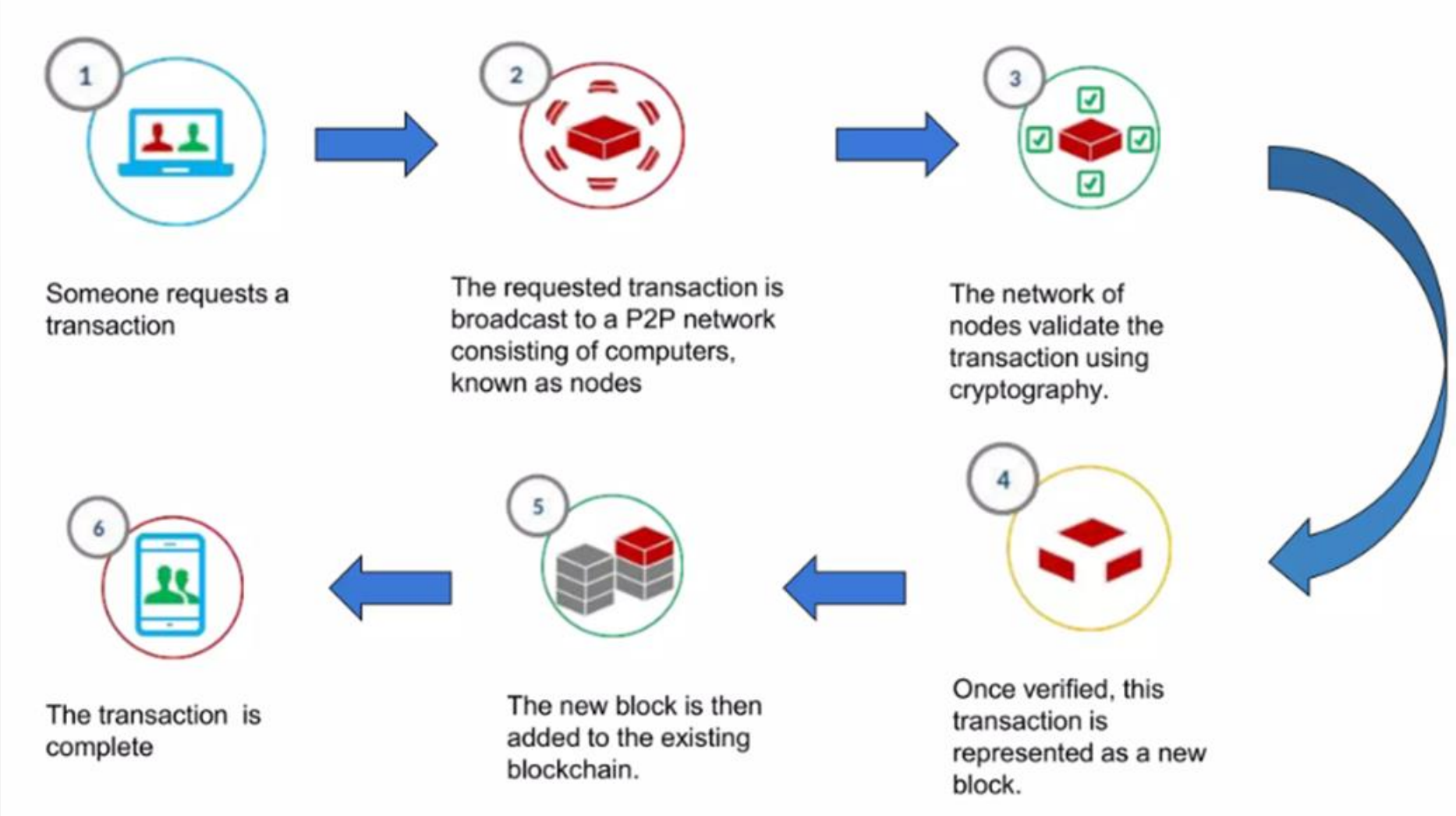


Double spending problem

Identifier le rôle d'un nœud dans un réseau

- ***Noeud complet***
  - Dispose d'un historique complet et à jour des transactions du réseau
  - Peut créer et vérifier de manière indépendante n'importe quelle transaction
  - Fait partie du système de consensus
- ***Miner***
  - Un nœud complet qui regroupe également les transactions validées dans un bloc candidat
  - Les mineurs rivalisent pour gagner le droit de créer un nouveau bloc complet en résolvant un problème mathématique complexe (preuve de travail)
  - Lorsque le mineur réussit à trouver la solution en premier, son bloc candidat devient un nouveau bloc valide

How Blockchain Transaction Works?

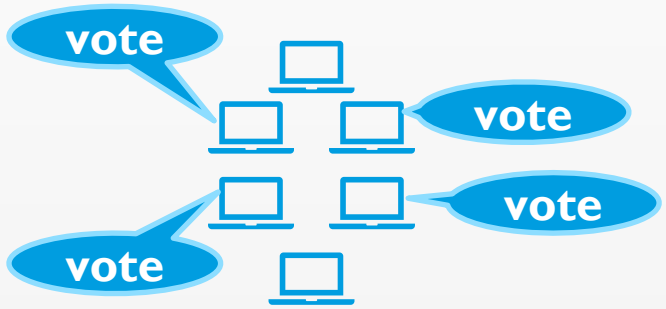


Differentiate between public, private and hybrid blockchains

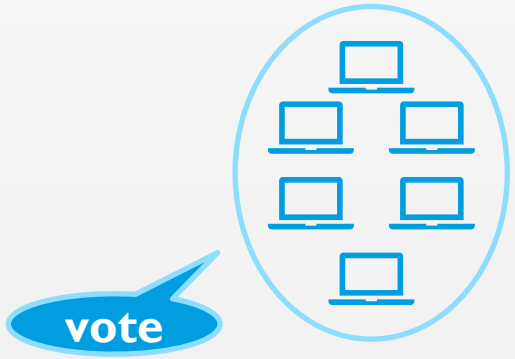
Il existe 3 principaux types de blockchains

- ***Blockchains publiques***
  - tout le monde peut voir toutes les transactions
  - n'importe qui peut ajouter des transactions au réseau
- ***Blockchains privées***
  - seules les parties de confiance peuvent exploiter la blockchain
  - l'identité sur le réseau est liée à l'identité réelle
- ***Hybrides***
  - contrôler qui peut participer et à quel niveau
  - par exemple : seules certaines parties de confiance peuvent ajouter des transactions au réseau, mais tout le monde peut visualiser les transactions

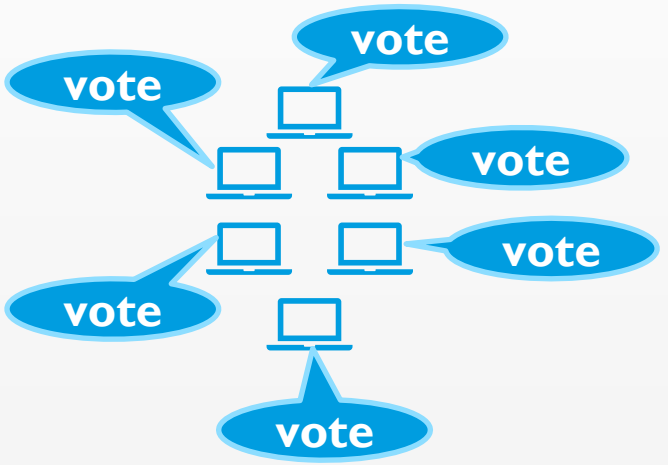
Differentiate between public, private and hybrid blockchains



Public : aucune restriction d'accès



Privé : autorisé



Hybride : combinaison

Cas d'utilisation de la blockchain

- HealthCare
- Supply-chain
- Banking
- Financial
- Fitech
- Government
- Identity
- Theft & Security
- Automotive
- Retail
- Fraud
- Voting
- Money transfer
- Cloud storage
- Education
- Marketing
- Direct selling
- Digital Payment
- Digital Currency
- Manufacturing
- Legal
- Insurance
- Media
- Energy
- Real Estate
- Charity
- Luxury Goods management
- Technology
- And More use cases

Cas d'utilisation de la blockchain

Blockchain dans la chaîne d'approvisionnement,
dans le domaine juridique,
dans le gouvernement, dans l'énergie,
dans l'alimentation, dans la vente au détail,
dans les soins de santé,
dans les assurances,
dans les voyages et l'hôtellerie,
dans le vote électronique,
dans le paiement des employés,
dans le stockage en nuage,
dans les contrats intelligents,

Questions ?!!