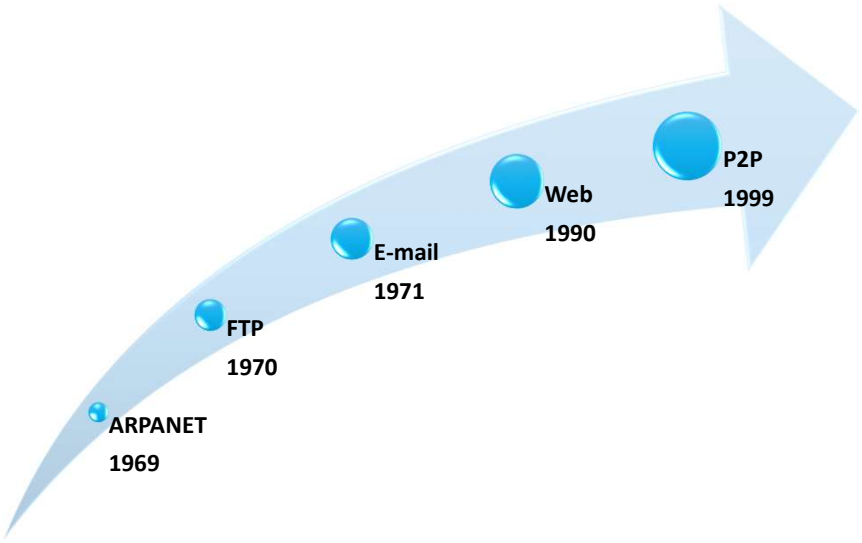
La technologie Blockchain

Dr. Marwa CHAIEB

HISTORIQUE:
L'INTERNET DE LA COPIE

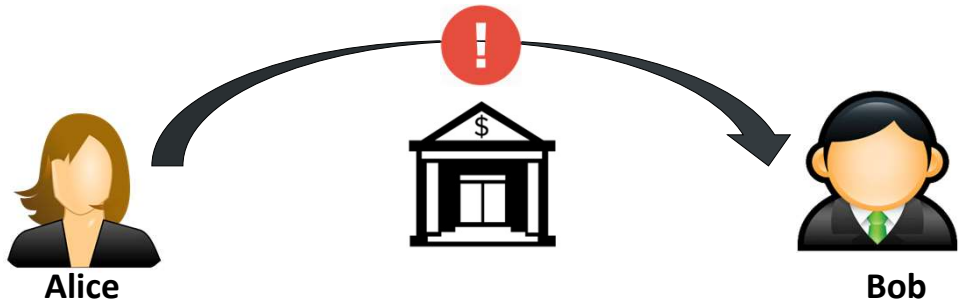
L'internet de la copie



De l'information à la valeur

- L'internet de la copie ne fonctionne pas pour tout: on ne peut pas copier un objet avec une valeur intrinsèque (une maison, une voiture, un animal…),
- L'internet actuel est construit autour d'un échange de l'information,
- Pour échanger des éléments de valeur, il faudrait un internet de la valeur,
  ➔ La technologie Blockchain

Echange de valeur en réalité



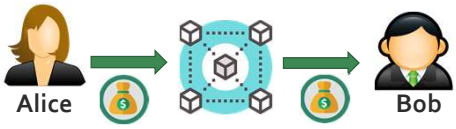
Physical Transaction

- ✓ Pas besoin d'un tier de confiance
- ✓ Transfert instantané
- ✓ Vérifiable
- ✓ Alice n'a plus la somme d'argent

Digital Transaction

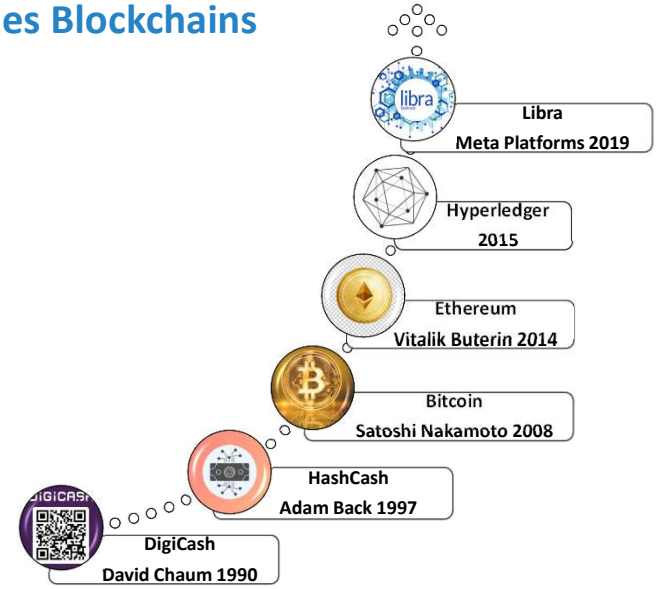
- ○ Comportement malveillant du tiers de confiance
- ○ Frais élevés
- ○ Non-disponibilité du service

Blockchain Transaction



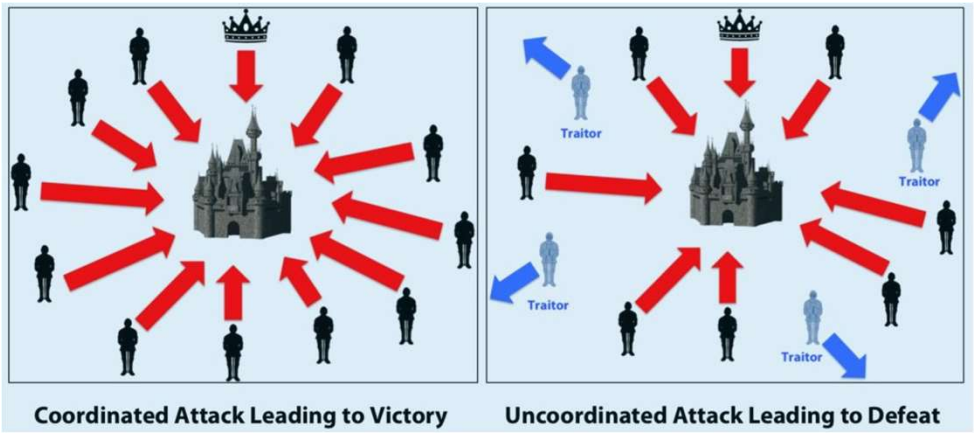
- ✓ La Blockchain n'est plus la propriété d'une entité centrale (architecture p2p).
- ✓ Vérification de bout en bout
- ✓ La Blockchain est sécurisé grâce au mécanisme de consensus.
- ✓ Les acteurs sont incités à agir honnêtement.

Naissance des Blockchains



https://bitcoin.org/bitcoin.pdf https://andersbrownworth.com/blockchain/

Problème de généraux Byzantins: Comment avoir confiance dans un message, sans avoir confiance dans le messager?



Types des Blockchains

	Public Blockchain	Private/Federated Blockchain
Access	- Permissionless	- Permissioned
Performance	- Slow transaction speed	- Lighter Blockchain - Fast transaction speed
Security	- Consensus mechanism - Proof of Work / Proof of Stake	- Pre-approuved participants - Voting / Multi-party consensus
Identity	- Anonymous	- Identities are known
Energy consumption	- Large	- Low
Transaction cost	- High	- Low
Trust	- No need to trust each other	- Trust is a must between nodes

HYPERLEDGER
FABRIC

Hyperledger Fabric

- La Fondation Linux a fondé le projet Hyperledger en 2015,
- Hyperledger Fabric est l'une des Blockchains proposées dans le cadre de ce projet,
- Cette Blockchain utilise des contrats intelligents (*appelé* ***chaincode***),
- C'est une Blockchain privée, les membres d'un réseau Hyperledger Fabric s'inscrivent par l'intermédiaire d'un fournisseur de services aux membres (***Membership Service Provider MSP***).

https://hyperledger-fabric.readthedocs.io/en/release-1.4/getting_started.html

Hyperledger Fabric: ChainCode (CC)

- *« Chaincode is a program, written in Go, node.js, or Java that implements a prescribed interface… »[1,2]*

- 2 types:
  - **ChainCodes utilisateur:** s'exécutent dans des conteneurs docker séparés, similaires aux smart contracts,
  - **ChainCodes système:** exécutent des fonctionnalités de configuration système, exemples: QSCC (Query System Chaincode), CSCC (Configuration System Chaincode) et LSCC (Lifecycle System Chaincode).

[1] HYPERLEDGER FABRIC V1.4 https://hyperledger-fabric.readthedocs.io/en/release-1.4/chaincode.html
[2] HYPERLEDGER FABRIC V2.0 https://hyperledger-fabric.readthedocs.io/en/release-2.0/chaincode.html

Hyperledger Fabric: Confidentialité des ChainCode

- **ChainCode public:** déployés par les transactions publiques et peuvent être invoqués par tout membre du réseau.
- **ChainCode Confidentiel:** déployés par des transactions confidentielles et ne peuvent être invoqués que par des membres validants du réseau.
- **ChainCode à accès contrôlé:** déployés par des transactions confidentielles qui intègrent également les tokens des invocateurs approuvés. Ces invocateurs sont également autorisés à invoquer des chaincodes confidentiels même s'ils ne sont pas des validateurs.

Hyperledger Fabric: Transaction

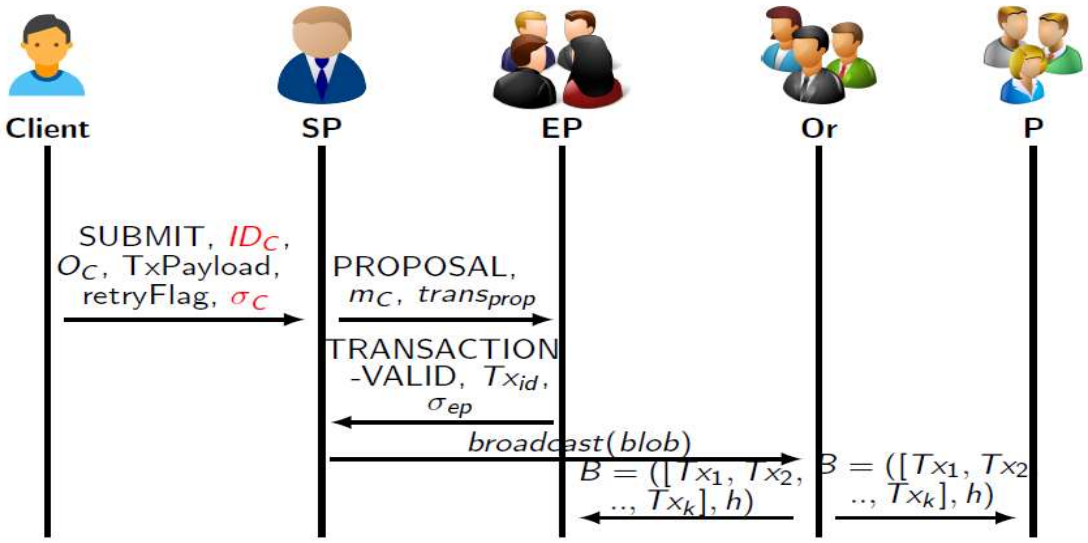
Types de transactions

- **Transaction de déploiement**
- **Transaction d'invocation**

Confidentialité des transactions

- **Transaction publique:** Son payload est public. Toute personne ayant accès à la Blockchain peut interroger les détails des transactions publiques,
- **Transaction confidentielle:** Son payload est chiffré, de sorte que personne d'autre que les parties prenantes à la transaction ne peut en interroger le contenu,
- **Transaction de ChainCode confidentiel:** Son payload est chiffré de telle sorte que seuls les validateurs peuvent le déchiffrer. La confidentialité du chaincode est déterminée au moment du déploiement. Si un chaincode est déployé en tant que chaincode confidentiel, les payloads de toutes les transactions d'invocation ultérieures de ce chaincode seront chiffrés.

Hyperledger Fabric: Consensus



Hyperledger Fabric: Channel

- Sous-réseau privé de communication entre deux ou plusieurs membres spécifiques du réseau, dans le but d'effectuer des transactions privées et confidentielles.
- Un canal est défini par des membres (organisations), SP par membre, un ou plusieurs CC et un ou plusieurs nœuds de sevice (Or).
- Chaque transaction sur le réseau est exécutée sur un canal, où chaque partie doit être authentifiée et autorisée à effectuer des transactions sur ce canal.
- Chaque pair qui rejoint un canal, a sa propre identité donnée par un MSP.

La technologie Blockchain

Dr. Marwa CHAIEB