**Blockchain :**

*Mounir BENDHAMANE*

Système de gestion de BDD **distribué**/décentralisé (inverse de centralisé comme SQL, NO SQL)

Mécanisme de P2P.

Avantage d’un réseau distribué :

Plus le réseau est grand, plus il est protégé car peer to peer.

Répartition des risques

Interdit la modification, suppression de l’information enregistrée

Technologie basée sur le cryptage

Désavantage :

Difficile à synchroniser

Existe depuis 40-50 ans

Smart contract (Contrat intelligent)

Crypto à clé symétrique -> Même “clé” pour chiffrer et déchiffrer

Crypto à clé asymétrique -> 2 clés, une clé privée et une publique

A donne sa clé publique à B et B donne sa clé publique à A

Liste chainée -> Chaque bloc possède l’information de celui d’après (ou parfois celui d’avant)

Intérêt blockchain -> infalsifiable et données publiques, disponibles à la vue de tous

Intégrité 100% fiable

Composants blockchain :

Nœud légers (%Tage de données) ou complets (100%) : infrastructure

* Réseau d’ordinateurs, de serveurs donc interconnectés
* Contiennent une copie de la BC si nœud complet
* Se synchronisent (ordinateur éteint) entre eux (Maj BC)

Les mineurs : acteurs + infrastructure

* Qui mettent à disposition une puissance de calcul (nœud)
* Sont motivés financièrement
* Sont contrôlés (“proof of stake”, mineur -> “Proof of work”)

Possible de falsifier une blockchain en ayant un PC + puissant que 51% de l’entièreté des PC du réseau.

Nouveau champ appelé “Nonce” (Number used Once)

Trouver le nonce qui donnera le hash -> c’est le minage

Contrôle des mineurs :

**Consensus :**

A la création d’un nouveau block, tous les nœuds l’enregistrent.

Problème de timestamp au niveau mondial -> resynchronisation à faire sur l’ensemble = consensus sur la genèse des documents

Si 2 blocks identiques créés en même temps -> celui ayant été reçu en premier par la majorité du réseau est gardé, l’autre est “destroyed”

PoS (proof of stake) : motivation

On fait confiance aux validateurs (ceux ayant bcp de blocks)

Block chain basée sur “la théorie des jeux”

Contrôle des mineurs :

Système de tirage au sort dans le pool :

* Durée de possession des bies mis dans le pool
* Tirage au sort des acteurs les plus réguliers

**Smart Contract (DAPP) :**

Contrat enregistré sous forme d’un code informatique -> programmation de conditions -> (si conditions réunies)

Smart contract -> class contract

Extension chrome -> Metamask

Ethereum.org / blockchain test ou dev

Coût en Ether (cryptomonnaie) de chaque transaction dépend de la complexité du code envoyé (plus les calculs sont longs/compliqués, plus le prix de la transaction augmente)

Token -> ERC20

**Partie NFT :**

Blockchain Solana -> pour les NFT (langage = RUST)

Etherum -> blockchain avec le + de développements associés

BTC = équivalent de l’or = valeur refuge

*Différence entre ERC20 et ERC721 (regarder interface)*

Class = assembler les objets (= plan de construction)

Objet = voiture qui sort de l’usine en se basant sur la class

Contrat = caractéristiques (3 portes, 5 portes...)

Interface = s’engager à avoir des fonctions qui ont tel nom ou tel nom

On implémente une interface et on hérite d’une class

IPFS -> système public en peer-to-peer pour stocker du média