**Bdd -> centralisé**

Désavantage : - Plus grand plus lourd plus lent

**Blockchain – décentralisé – distribué – pear to pear :**

**Avantage** : - Peu de chance d’avoir des pertes de données. Plus grand = Plus robuste

**Désavantage** : - La Synchronisation – Activité Criminel (Blanchir de l’argent)

C’est un stockage de donnée en crypté c’est ce qui fait sa force en termes de sécurité cela est très safe

**Blockchain** = **Liste** **d’éléments** : - Liste chainé par ce qu’on a des infos du block précédents

Les informations sont toutes consultables dans les blockchains et elles ont toutes leur intégrité, on ne peut pas douter de son authenticité

Tous les nœuds sont des mineurs mais tous les mineurs ne minent pas.

La complexité du hash c’est de trouver le ‘Nonce’ = Un Nouveau champ dans le block donc le hash change

Chaque block Hashage est relié entre eux

TP : Créer une blockchain pas du top 5 (expliquez pourquoi elle est bien, (pas plus de 5 lignes))

**Mineurs :**

POS – proof of stake (on fait confiance au validateur)

Cela est plus rapide.

Il faut toujours de la puissance de minage pour valider le block suivant

Solidity langage de programmation

NFT :

**En partant de la blockchain donnée les différences entre un erc20 et erc721 point de vue code**

Indice : Regarder les interfaces, classes

Consignes : modifier des métas données, Candy Machine v2(Metaplexdoc)

Bloc de construction c’est la classes 🡪 Dans une usine

La voiture qui sort de l’usine c’est objet

Pour une voiture un contrat c’est une berline qui s’engage d’avoir certaines caractéristiques

Une interface (contrat) c’est comme une classe qui s’engage d’implémenter la méthode associée à la voiture

……………………………………………………………………………………………..

BDD -> centralisé

Blockchain -> décentralisé -> p2p

- C'est une technologie qui interdit la redondance des informations -> interdit de modifier

- Stockage de donnée cryptographié

#1 Principes

>> Partager le registre entre plusieurs opérateurs

>> Chaque participant à la transaction à accès au registre

>> Une transaction enregistré ne peut etre modifiés elle doit etre "annulée"

si nécessaire auquel cas cette opération est une transaction aussi

>> Accord de tous les participants

>> Traçage du "Bien" et des participants

>> Transaction enregistrée de façon "immuable"

>> Enregistrement dans un seul registre unique partagé, accessible aux partiicpants à la transaction

entre autre

#2 Identification et sécurité : cryptographie : Rappel des Principes

>> Encodes des informations de façon que qeuls les emetteurs et destinataires qui sont propriétaires de ces

informations puissent en disposer

>> C'est-à-dire : Ecrire, Lire, Modifier, Supprimer selon des rgèles partagées et acceptées

>> La principale technologie utilisée est : la crypto asymétrique par opposition à la crypto symétrie

-Clé symétrique

>> Meme clé pour chiffrer et déchiffrer

=> Comment trensmet on la clé depuis l'émetteur vers le destinataire ? On l'encrypte avec une clé ?

-Clé asymétrique

>> Si vous voulez recevoir un message crypté d'un destinataire, pour le crypter il lui faudra votre clé publique, celle que vous donnez

>> Pour déchiffrer le message, il faut une seconde clé

#3 Hashage en crypto, clé

>>Fonction dite à "sens unique" et à "porte secrète"

#4 Principes

>> Bloques ont un ID unique

>> Hash du block précedents et plein d'infor que l'on appel des transactions

>> La casi-totalité des transaction sont publique et peuvent lu par tous le monde

=> Application : chainé les informations personnelles

#5 Composants BLOCK CHAINE

>> Noeuds légers ou complets : infrastructure

>> Réseau d'ordinateurs de servers -> interconnectés

>> Contiennent une copie de la BC si noeud complets

>> Se synchronisent entre eux

>> Les mineurs acteurs + infrastructure

>> Qui mettent à disposition une puissance de calcul

>> Sont motivés financièrement

>> Sont controlés

>> Outre leurs fonction de Noeuds, ils créent les blocks

>> Tous les noeuds ne sont pas "mineurs"

>> Chaque Mineur est différentiable : Les blocks qu'il crée sont

indentifiables et propre à chaque mineur

>> La création d'un nouveau Block doit etre validée par le réseau, d'ou un gap temporel

>> Avant de créer un nouveau block, le mineur doit récupérer les transactions qui ne sont pas encore

incluses dans un block

>> Puis pour créer ce nouveau Block le mineur doit résoudre un "puzzle cryptographique". Le mineur le plus

rapide gagne et peut donc l'inscrire dans la BC

>> Controle

>> Le minuer le plus rapide pour solutoinner transmet sur le réseau et sa solution et son block

>> Le réseau (tous les noeuds) vérifie que la solution est bonne et acceptées

L'instcription du nouveau block

#6 Puzzle

>> Composition : un hash est une valeur numérique isue d'une fonction de Hashage

>> Cette fonction est faire pour qu'il soit très difficile de retrouver sa valeur

en calcul brute

>> En block chain :

- Vérifier que le block n'a pas été modifié

- Lier ce block au suivant

>> Le hash prend en variables de transactions qui ont leurs propore hash, le hash du block

précédents... Toutes modifications du block modifie le hash

>> Rajoutons un nouveau champs "Nonce" Number used once, dans le B.C

>> Trouver le Nonce qui donnera ce nouveau hash

>> Le nonce est une contraine créee à la création de la B.C

>> Nonce => '0000...' ou > '10000'

#7 Controle des mineurs :

>> Deux block créés en meme temps

>> Proof of stake - PoS

>> Validateur : système de 'validation' des blocks concurrent ou complémentaire du PoW (proof of work)

>> PoW -> trouver un nouveau block -> validé -> récompense => pas performant

>> Rappel la B.C est basé aussi sur la théorie des jeux de Nash

>> Les validateurs sont des users qui parient qu'ils vont etre élus pour forger des blocks

>> Ils envoient des fonds dans le pool des validateurs ou ils sont bloqués tant que le validateur

n'a pas rempli son contrat à savoir forger des blocks

>> Les validateurs d'un block consiste à justifier d'un montant d'unité des 'biens' propre à la B.C

concernée

>> Donc le plus riche va etre choisi

>> Pour éviter ça, des procédures ont été crée

>> Tirage au sort

>> Deux méthodes de bases

>> PoW v PoS

>> PoW -> puissance de calcul

>> PoS -> basé sur la fortune des utilisateurs dans la B.C et de leurs 'enjeux'

#8 Smart Contract (DAPP)

Solidity -> JS + C;

ERC721 -> marche à suivre pour déployer les nft

## Résumé ##

>> Un token ERC20 peut être une monnaie, des actions d'une entreprise, des points de loyautés, etc...

>> Classes abtraites et interfaces ont chacune une fonction bien distincte : les classes abstraites

servent à factoriser du code, tandis que les interfaces servent à

définir des contrats de service.

>> Classe est un squellette d'un objet => Recette

>> Interface pour définir des contrats => Contrats => Comportements

>> Une interface ne peut étendre aucune autre classe et ne peut pas surcharger ou

implémenter des méthodes de classe abstraite. Une classe abstraite peut étendre

d'autres classes et peut également implémenter des interfaces.

>> Mint -> créer le token

>> Métadonnées -> caractériqtique de notre NFT - Doit etre accessible de partout

>> IPFS != B.C

>> Solidity -> Ether

>> DAPP -> application web classique (appelé décentralisé)

>> RUST -> language de programation -> Solana -> ERC721

>> Structure de la block chain Ether

>> Hash -> hexadecimal Il est associé à la fonction de hashage, un algorithme

mathématique qui consiste à convertir une chaîne de caractères en une valeur inférieure.

…………………………………………………………………………………………

Avantage d’un réseau distribué (Peer 2 Peer) : Il est appliqué partout donc + robuste car hébergé partout.

Inconvénient d’un réseau distribué : Etant donné qu’il est appliqué partout, il nous faudra une forte synchronisation. Car tout doit être disponible en même temps.

Qu’est-ce que la Blockchain :

- Technologie basée sur :

o Répartition des risques

o Accès à l’information par tous les membres du réseau

o Internet (Maillage, P2P)

o L’interdiction de la redondance des informations

o L’interdiction de la modification, suppression de l’information

o Cryptage

- Les blocks sont chaînés comme une liste chaînée restrictive. Chaque bloc possède :

o Le hash du bloc

o Le hash du bloc précédent

o Le hash de la transaction

 Chaque hash est une « adresse » différente afin que chacun des blocs soient uniques.

Le système de minage est un système de travail (trouver la solution au puzzle)

Les NFT’s ne sont pas dans la blockchain BTC car celle-ci n’a pas été prévue pour ça. C’est pourquoi ceux-ci sont dans la blockchain ETH.

Un NFT est un token.

En partant de la blockchain ETH, donnez les principales différences entre l’ERC20 et l’ERC721 :

- Tous les 2 sont des standards avec une interface différente.

-

Différence entre une interface et une classe :

- Classe :

o « Plan de construction » d’une variable (objet) ;

- Interface :

o Comme une classe mais uniquement avec les prototypes de fonction.

o On a que les en-têtes des fonctions, le comportement.