La blockchain pour les nuls

Formation SellTix

Selltix.

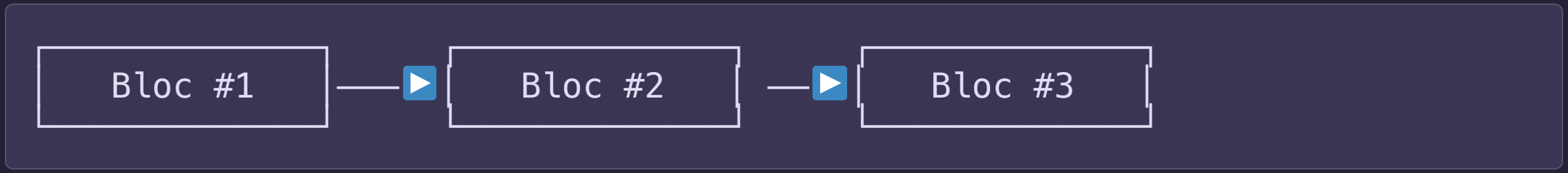
Sommaire:

Qu'est-ce que la blockchain ?

Définition et principes fondamentaux

La blockchain est une technologie de registre distribué qui permet de stocker et de transmettre des informations de manière:

- Transparente (tout est publique)
- Sécurisée
- Décentralisé (Sans organe central de contrôle)



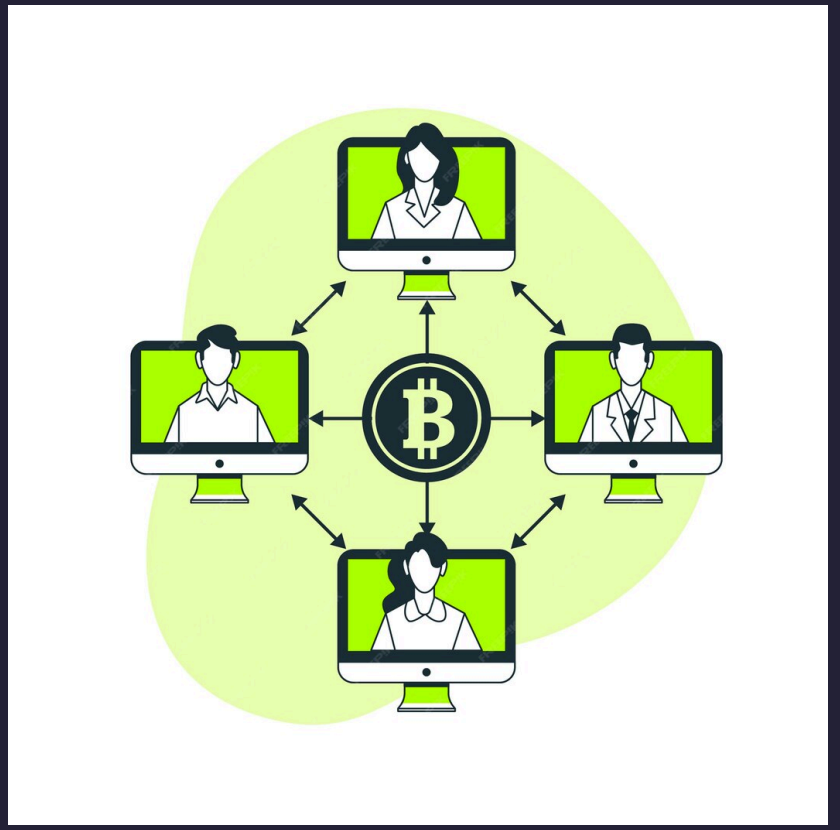
Historique et évolution

- **2008**: Publication du whitepaper Bitcoin par Satoshi Nakamoto
- **2009**: Lancement du réseau Bitcoin et premier bloc miné (bloc genesis)
- **2015**: Lancement d'Ethereum et introduction des smart contracts
- **2020-2023**: Explosion des cas d'usage: DeFi, NFTs, billetterie (SellTix)

Concepts clés: Décentralisation

La blockchain fonctionne sur un réseau pair-à-pair (P2P):

- Pas d'autorité centrale
- Chaque nœud du réseau possède sa propre copie de la blockchain
- Consensus distribué pour valider les transactions (POW,POS)



Concepts clés: Transparence

Toutes les transactions sont:

- **Publiques** et visibles par tous
- **Traçables** de leur origine à leur destination
- **Vérifiables** par n'importe quel participant

```
Explorer: https://etherscan.io
```

Concepts clés: Immuabilité

Une fois qu'une transaction est validée et ajoutée à un bloc:

- Elle ne peut plus être modifiée
- Elle est liée cryptographiquement aux transactions précédentes
- Toute tentative de modification serait immédiatement détectée

Application à SellTix

SellTix utilise la blockchain pour:

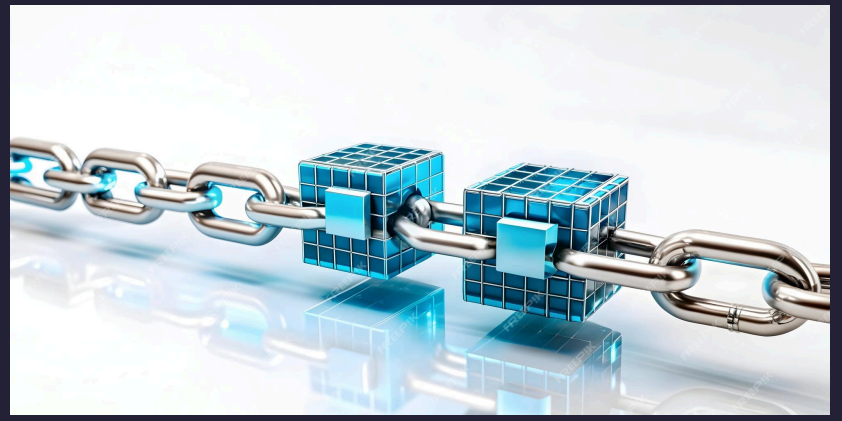
- Créer des tickets sous forme de NFTs (jetons non fongibles)
- Garantir l'authenticité des billets
- Permettre des transferts sécurisés entre utilisateurs
- Éliminer la contrefaçon et la revente frauduleuse

Comment fonctionne la blockchain ?

Blocs, transactions et chaîne

La blockchain est une **chaîne de blocs** liés cryptographiquement:

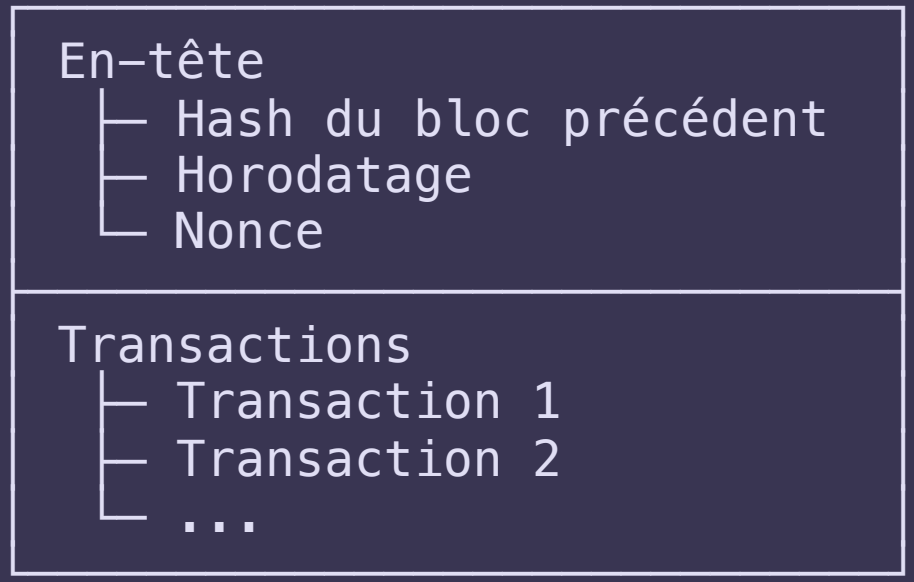
- Chaque bloc contient un ensemble de **transactions**
- Les blocs sont liés par des **hachages cryptographiques**
- Chaque bloc contient le hachage du bloc précédent



Anatomie d'un bloc

Un bloc contient:

- **En-tête**: hachage du bloc précédent, horodatage, nonce
- **Transactions**: liste des transferts de valeur ou d'informations
- **Métadonnées**: informations supplémentaires spécifiques au réseau



Consensus et validation

Le consensus est le mécanisme qui permet aux nœuds de s'accorder sur l'état de la blockchain:

Proof of Work (PoW)

- Utilisé par Bitcoin
- Les mineurs résolvent des problèmes cryptographiques
- Consommation énergétique importante

Proof of Stake (PoS)

- Utilisé par Ethereum 2.0, Polygon, Solana
- Les validateurs mettent en jeu des crypto-monnaies
- Plus écologique que PoW

Processus de validation d'une transaction

1. **Création**: Un utilisateur crée et signe une transaction
2. **Propagation**: La transaction est diffusée sur le réseau
3. **Vérification**: Les nœuds vérifient la validité de la transaction
4. **Inclusion**: La transaction est incluse dans un bloc
5. **Validation**: Le bloc est validé par consensus
6. **Confirmation**: Le bloc est ajouté à la chaîne

Smart contracts et dApps

Smart Contracts

- **Programmes autonomes** qui s'exécutent sur la blockchain
- Exécution automatique lorsque certaines conditions sont remplies
- Immuables et transparents

Applications Décentralisées (dApps)

- Applications construites sur la blockchain
- Interface utilisateur + smart contracts
- Exemples: SellTix, Uniswap, OpenSea

```
// Exemple simplifié d'un smart contract de ticket
contract Ticket {
    address public owner;

    constructor() {
        owner = msg.sender;
    }

    function transfer(address newOwner) public {
        require(msg.sender == owner);
        owner = newOwner;
    }
}
```

SellTix: Smart Contracts en action

SellTix utilise plusieurs smart contracts pour:

- Créer et gérer des événements
- Émettre des tickets sous forme de NFTs
- Gérer les transferts de propriété
- Vérifier l'authenticité des billets

Ces contrats garantissent que:

- Seuls les tickets légitimes sont acceptés
- Les transferts sont traçables et sécurisés
- Les règles de l'événement sont respectées

Les cryptomonnaies

Différence entre tokens et coins

Coins (Pièces)

- Possèdent leur propre blockchain
- Fonctionnent comme moyen d'échange
- Exemples: Bitcoin (BTC), Ether (ETH), Solana (SOL)

Tokens (Jetons)

- Construits sur des blockchains existantes
- Représentent des actifs ou des utilités
- Exemples: USDT (Tether), LINK (Chainlink)

Standards de tokens

ERC-20

- Standard pour les tokens fongibles : non unique / interchangeable
- Utilisé pour la plupart des tokens Ethereum
- Exemple: USDT, DAI, LINK

ERC-721

- Standard pour les tokens non-fongibles (NFTs)
- Chaque token est unique et non interchangeable
- **Utilisé par SellTix pour les tickets**

ERC-1155

- Standard multi-tokens (fongibles et non-fongibles)
- Permet des transactions plus efficaces
- Utilisé pour les jeux et certaines places de marché

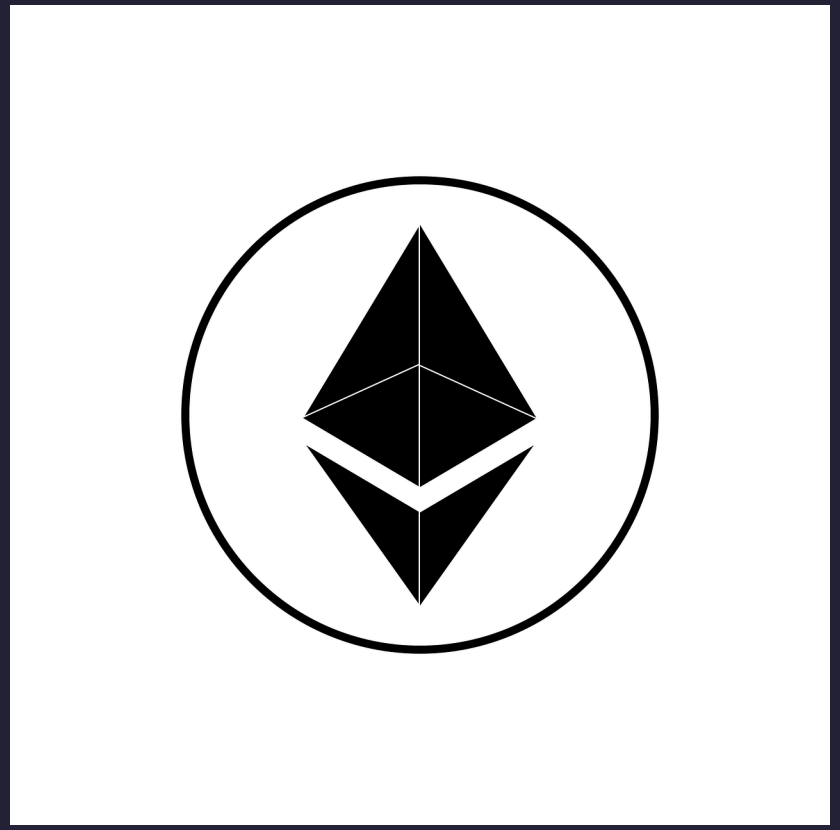
Principaux réseaux blockchain

Ethereum

- Premier réseau avec smart contracts
- Écosystème le plus développé

Polygon

- Solution de mise à l'échelle pour Ethereum
- Frais de transaction réduits
- Compatible avec les outils Ethereum
- Utilisé par SellTix pour ses tickets NFT



Autres réseaux importants

- Binance Smart Chain (BSC)
- Solana
- Avalanche

Frais de transaction (Gas)

Qu'est-ce que le gas?

- Unité de mesure pour le coût de calcul sur la blockchain
- Payé en cryptomonnaie native du réseau (ETH pour Ethereum)
- Varie selon la congestion du réseau

Impact sur l'expérience utilisateur

- Coût supplémentaire pour chaque transaction
- Peut être élevé sur Ethereum pendant les périodes de forte demande
- Solutions: Layer 2 (Polygon), optimisation des contrats

Cas d'usage dans SellTix

Tickets sous forme de NFTs

- Chaque ticket est un token ERC-721 unique
- Propriété vérifiable sur la blockchain
- Transfert sécurisé entre utilisateurs

Avantages pour les organisateurs

- Contrôle sur la revente des billets
- Élimination de la contrefaçon
- Possibilité de percevoir des royalties sur les reventes

Avantages pour les utilisateurs

- Propriété vérifiable du billet
- Transfert simple et sécurisé
- Conservation comme souvenir après l'événement

Qu'est-ce qu'un wallet crypto ?

Formation SellTix

Définition et rôle

Un wallet crypto (portefeuille) est:

- Une **interface** pour interagir avec la blockchain et consulter vos actifs numériques
- Un **gestionnaire** de vos clés cryptographiques
- Un outil pour **envoyer et recevoir** des cryptomonnaies et NFTs
- Un moyen d'identification **sécurisé et anonyme**

Ce n'est PAS un compte bancaire traditionnel!

Clés privées et clés publiques

Clé privée

- Séquence aléatoire de chiffres et de lettres
- Donne un contrôle total sur vos actifs
- Ne **JAMAIS** partager avec quiconque
- Souvent représentée par une phrase mnémonique

Clé publique / Adresse

- Dérivée mathématiquement de la clé privée
- Partageable sans risque (comme un IBAN)
- Format hexadécimal: 0x123...abc (42 carac.)

Comment fonctionne un wallet

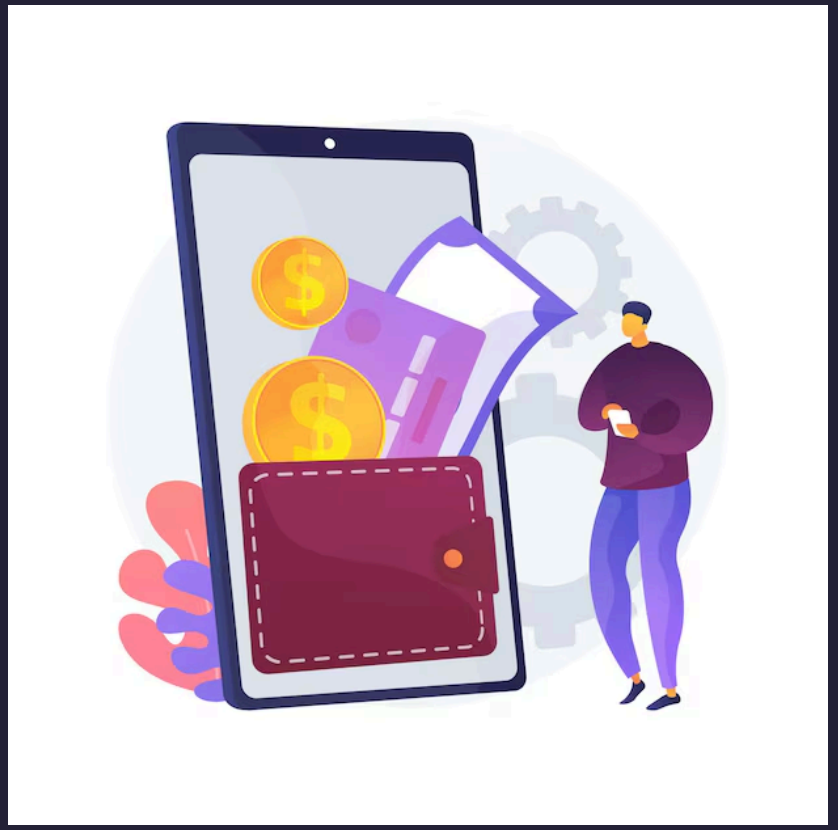
1. **Génération** de la paire de clés (privée/publique)
2. **Stockage sécurisé** de la clé privée
3. **Interaction** avec la blockchain via des transactions signées
4. **Suivi** du solde et de l'historique des transactions

Le wallet ne stocke pas vos cryptomonnaies - elles existent sur la blockchain!

Types de wallets: Hot vs Cold

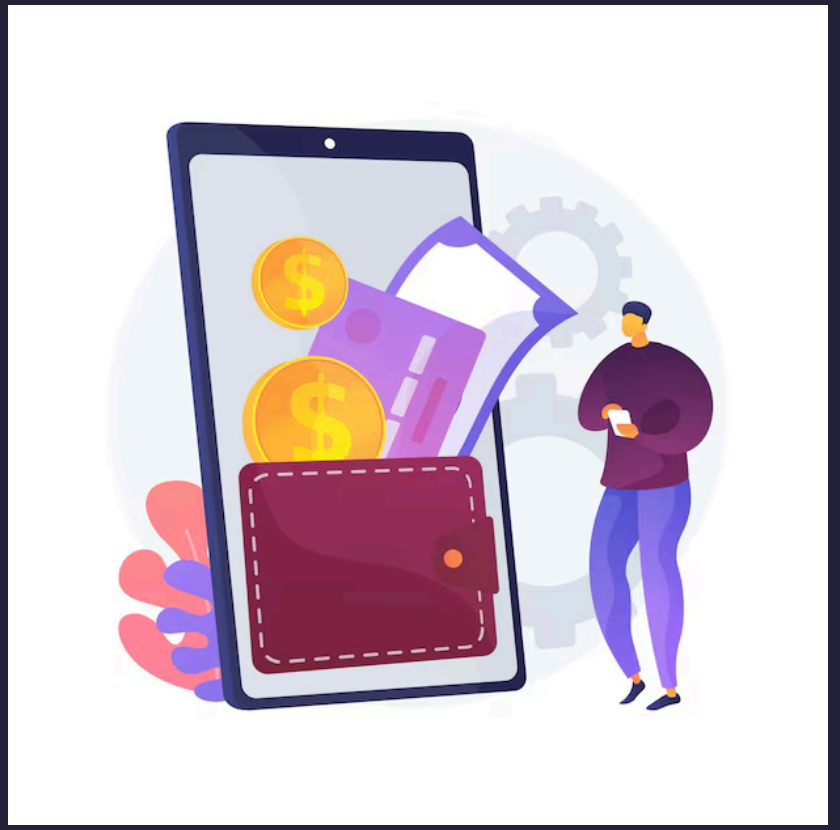
Hot Wallets (connectés)

- Connectés à Internet
- Faciles d'accès et pratiques
- Plus vulnérables aux attaques
- ***Exemples: MetaMask, Coinbase Wallet, Trust Wallet***



Cold Wallets (hors ligne)

- Non connectés à Internet
- Très sécurisés
- Moins pratiques pour les transactions fréquentes
- ***¡Exemples: Ledger, Trezor, KeepKey***



Comparaison des types de wallets

Type	Sécurité	Facilité d'utilisation	Cas d'usage
Mobile	Moyenne	Très facile	Usage quotidien
Extension	Moyenne	Facile	Navigation web, dApps
Hardware	Très haute	Modérée	Stockage long terme
Papier	Haute (si bien conservé)	Difficile	Backup, stockage froid
Web	Basse	Très facile	Petits montants

Importance de la phrase de récupération (seed phrase)

- Séquence de 12 à 24 mots dans un ordre spécifique
- Permet de restaurer l'accès à vos actifs
- **CRITIQUE**: si perdue, vos actifs sont perdus à jamais
- Si compromise, vos actifs peuvent être volés

Bonnes pratiques:

- Notez-la sur papier (jamais en numérique)
- Conservez-la dans un lieu sûr (coffre-fort)
- Envisagez des solutions de backup (plaque métallique résistant à un incendie)
- Ne la partagez JAMAIS

Utilisation avec SellTix

Votre wallet sur SellTix vous permet de:

- **Acheter** des billets sous forme de NFTs
- **Stocker** vos billets d'événements
- **Transférer** vos billets à d'autres utilisateurs
- **Accéder** aux événements avec vos billets

Selltix.

Démonstration

- Création d'un wallet
- Achat de crypto
- Transfert de crypto
- Connexion à une dAPP

NFTs et OpenSea

Formation SellTix

Comprendre les NFTs (Non-Fungible Tokens)

Définition

- Tokens **uniques** et **non interchangeables**
- Représentent la propriété d'un actif numérique ou physique
- Stockés sur la blockchain
- Chaque NFT possède un identifiant unique

Différence avec les tokens fongibles

- **Fongible**: interchangeable (ex: 1 ETH = 1 ETH)
- **Non-fongible**: unique, non interchangeable

Standards NFT

ERC-721

- Premier standard NFT sur Ethereum
- Un token = un actif unique
- Utilisé par SellTix pour les tickets

ERC-1155

- Standard "multi-token"
- Permet de gérer tokens fongibles et non-fongibles
- Plus efficace en termes de gas
- Utilisé pour les collections ou séries de tickets

Métadonnées et stockage

Métadonnées

Métadonnées

- Informations décrivant le NFT (nom, description, image...)
- Généralement au format JSON
- Peuvent inclure des attributs spécifiques (date, lieu, catégorie...)

Stockage

- **On-chain**: directement sur la blockchain (coûteux)
- **Off-chain**: stockage décentralisé comme IPFS
- SellTix utilise IPFS pour stocker les métadonnées des tickets

```
{
  "name": "Concert XYZ - VIP",
  "description": "Ticket VIP pour le concert XYZ",
  "image": "ipfs://Qm...",
  "attributes": [
    {"trait_type": "Date", "value": "2023-12-31"},
    {"trait_type": "Catégorie", "value": "VIP"}
  ]
}
```

Introduction à OpenSea

Qu'est-ce qu'OpenSea?

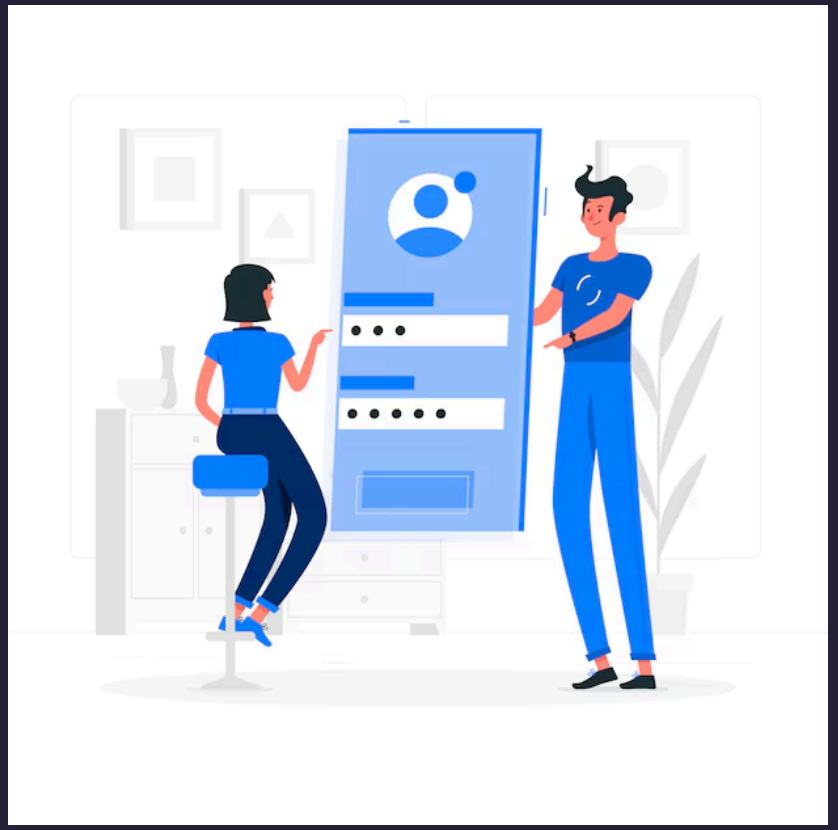
- Plus grande marketplace de NFTs au monde
- Permet d'acheter, vendre et découvrir des NFTs
- Compatible avec plusieurs blockchains (Ethereum, Polygon...)

Fonctionnalités principales

- Création et vente de collections NFT
- Enchères et achats directs
- Exploration par catégories
- Suivi des prix et de l'activité

Création d'un compte et connexion du wallet

1. Accédez à opensea.io
2. Cliquez sur l'icône de profil en haut à droite
3. Sélectionnez "Connect wallet"
4. Choisissez votre wallet (MetaMask, Coinbase Wallet...)
5. Suivez les instructions pour vous connecter
6. Acceptez la signature pour authentifier votre wallet



Navigation dans la marketplace

Exploration

- Page d'accueil: tendances et collections populaires
- Recherche par nom, collection ou attributs
- Filtres: prix, blockchain, catégorie...

Profil utilisateur

- Onglet "Collected": vos NFTs
- Onglet "Created": NFTs que vous avez créés
- Onglet "Favorited": NFTs que vous avez aimés
- Onglet "Activity": historique de vos transactions

Achat, vente et enchères de NFTs

Achat

- Achat direct ("Buy now")
- Faire une offre ("Make offer")
- Participer à une enchère

Vente

- Mise en vente à prix fixe
- Création d'une enchère
- Définition de royalties (% sur reventes)

Frais

- Frais de transaction (gas)
- Frais de marketplace (2.5% sur OpenSea)