**Rapport :**

**Création d’une blockchain proof of work au niveau local**



Crée par :

Mohamed KHACHLAA

Mohamed Jad LACHKHAM

Encadré par :

Prof. Mehdi TMIMI

Résumé du projet :

Ce projet consiste à développer une blockchain locale simplifiée, intégrant un mécanisme de Proof-of-Work. L'objectif principal est d'explorer les fondements de la technologie blockchain, notamment la création de blocs, la gestion des transactions, la signature numérique manuelle, la mempool et la sécurité des portefeuilles. Le système est composé d’un serveur Express qui gère la chaîne de blocs, les transactions et le minage, d’un client Node.js qui joue le rôle de mineur et d’expéditeur de transactions, ainsi que d’une interface web permettant de visualiser les blocs, les portefeuilles et d’interagir avec les transactions. Chaque mineur tente de résoudre un puzzle cryptographique pour valider un bloc, et reçoit une récompense en uemfCoins. Ce projet offre une compréhension pratique et progressive du fonctionnement d’une blockchain, tout en mettant en place une application web interactive pour la visualisation et la manipulation du système.

Technologies utilisées :

Pour ce projet nous avons opté à utiliser principalement node.js pour la création du serveur, ainsi que html et css pour le coté client a fin de créer des pages web qui seront comme interface pour les utilisateurs souhaitons utiliser nos services :

Node.js :

Node.js® est un environnement d'exécution JavaScript gratuit, open-source et multiplateforme qui permet aux développeurs de créer des serveurs, des applications web, des outils en ligne de commande et des scripts.

Html :

HTML signifie « HyperText Markup Language » qu'on peut traduire par « langage de balises pour l'hypertexte ». Il est utilisé afin de créer et de représenter le contenu d'une page web et sa structure.

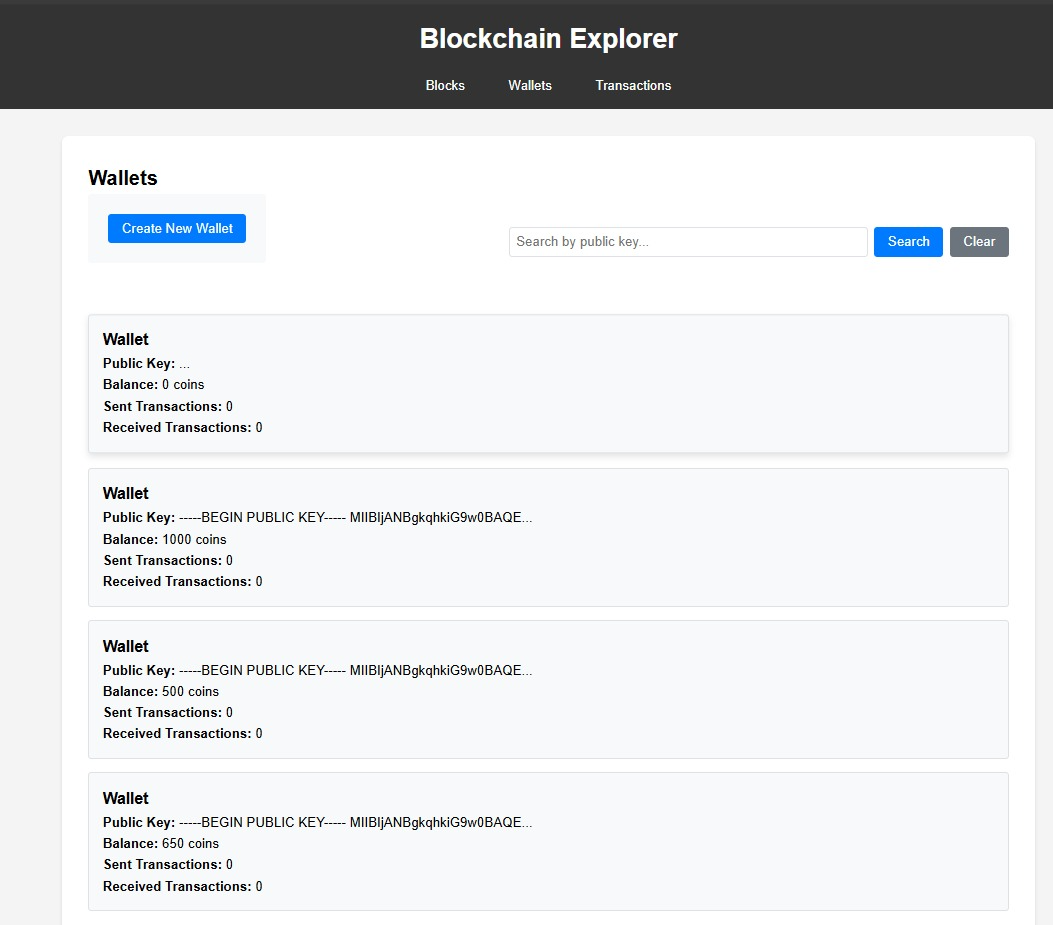
Css :

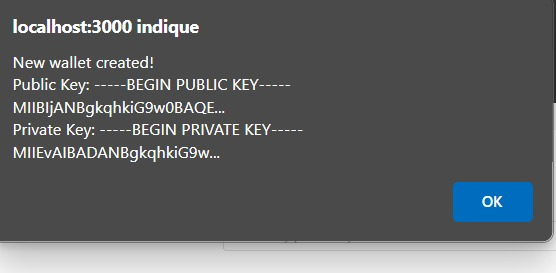
CSS (Cascading Style Sheets ou Feuilles de style en cascade en français) est un langage déclaratif utilisé pour décrire la présentation de pages web dans le navigateur. Le navigateur applique les déclarations de style CSS aux éléments concernés pour les mettre en forme.

Représentation du projet :

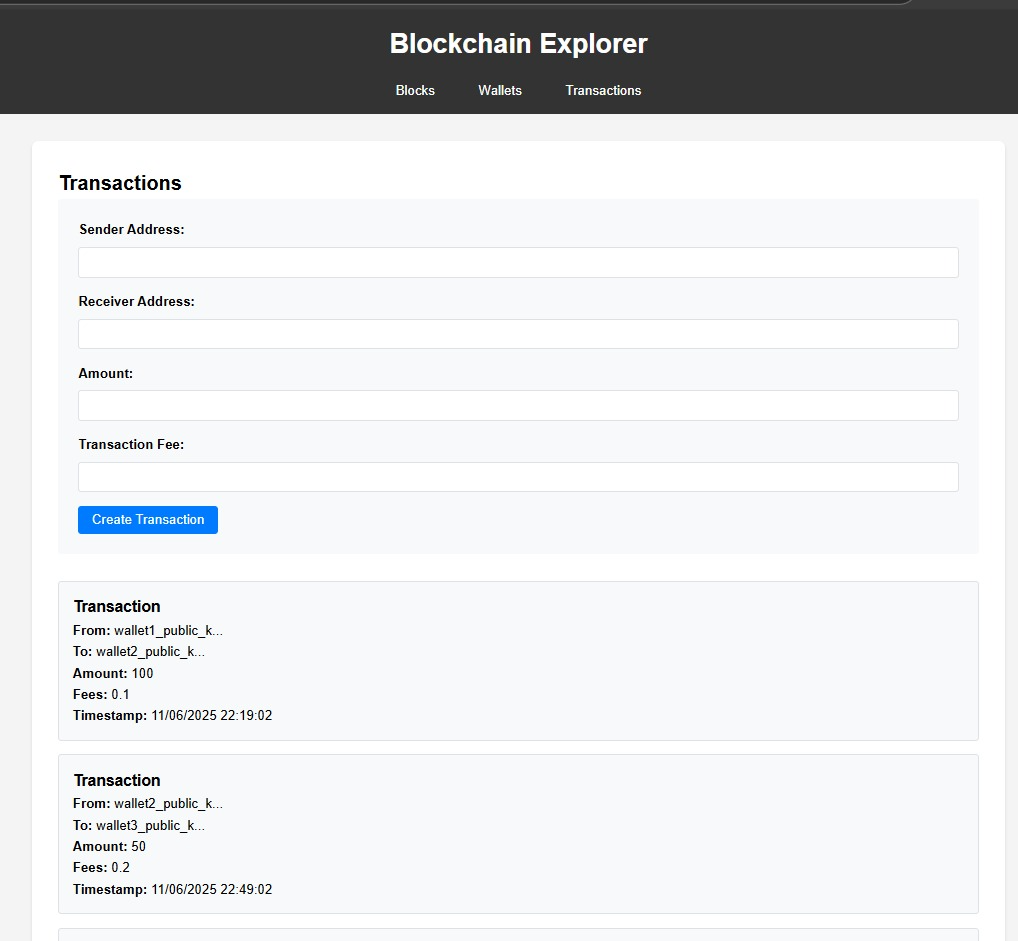
**Coté client :**

Page de création des wallets :

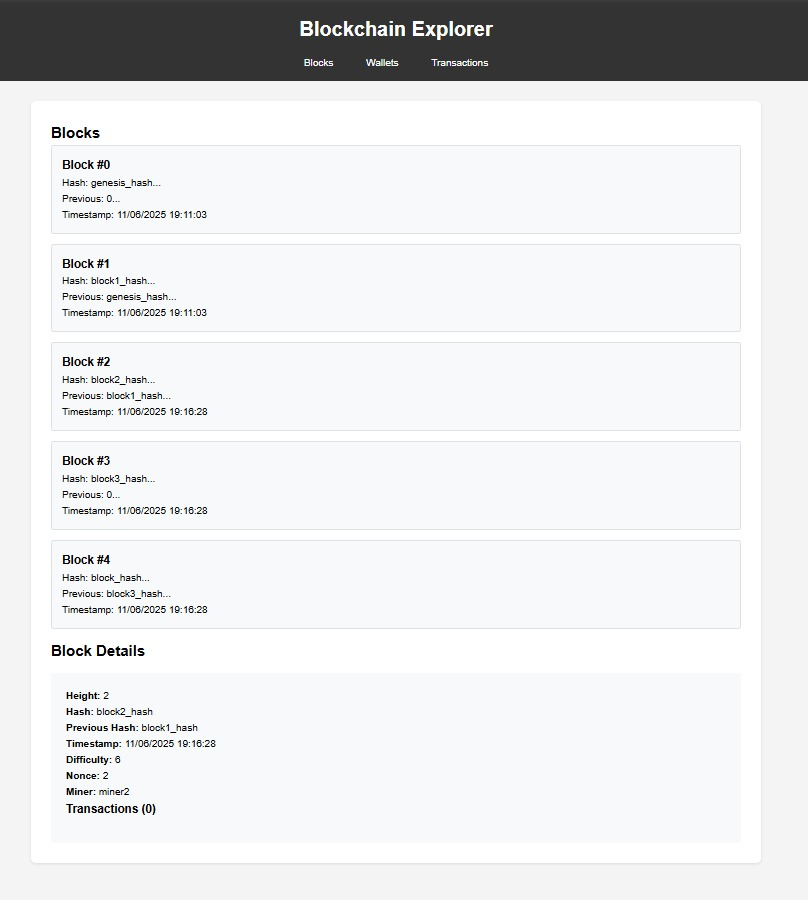




Page de création et validation des transactions :



Page des blocs :



**Coté serveur :**

Block :

Parametres :

**Height**: numéro du bloc dans la chaîne.

**hash** : empreinte unique du bloc.

**previousHash** : hash du bloc précédent.

**timestamp** : date et heure de création du bloc.

**difficulty** : complexité du calcul pour miner un bloc.

**blockReward** : récompense donnée au mineur.

**nonce** : nombre modifié pour trouver un hash valide.

**transactions** : liste des opérations validées dans le bloc.

Un bloc est une unité contenant un ensemble de transactions validées. Chaque bloc est lié au bloc précédent grâce à son hash, formant ainsi une chaîne sécurisée appelée blockchain. Il contient aussi des informations comme un horodatage, une preuve de travail (nonce), et la récompense du mineur. Cette structure garantit l’intégrité et la chronologie des données.

Mempool :

**signature** :C’est la signature numérique qui garantit que la transaction a été autorisée par le propriétaire du portefeuille (expéditeur). Elle sert à vérifier l’authenticité.

**feesAmount** :Montant des frais que l’expéditeur paie pour que la transaction soit traitée plus rapidement par les mineurs.

**Receiver** :Adresse ou identifiant du destinataire de la transaction, celui qui reçoit les fonds.

**Sender** :Adresse ou identifiant de l’expéditeur, celui qui envoie les fonds.

**mempool** :Référence ou état indiquant si la transaction est actuellement dans la mempool (pool des transactions en attente de validation).

**block** :Référence au bloc dans lequel cette transaction a été incluse une fois minée.

Une **transaction** représente le transfert de valeur d’un expéditeur à un destinataire sur la blockchain. Elle contient les informations nécessaires pour valider et enregistrer ce transfert dans un bloc, notamment la signature pour prouver l’authenticité, les frais payés au réseau, et les adresses des participants.

Wallets :

**pkey** :La clé privée du wallet, utilisée pour signer les transactions et prouver la propriété des fonds. C’est un élément secret à ne jamais divulguer.

solde :Le montant total de crypto-monnaie disponible dans ce wallet.

**ReceiveTransaction** :Une liste des transactions où ce wallet est destinataire (transactions reçues).

**SendTransaction** :Une liste des transactions où ce wallet est expéditeur (transactions envoyées).

Un **wallet** (portefeuille) est un objet qui représente un compte ou une adresse sur la blockchain. Il contient une clé privée permettant de signer les transactions, ainsi qu’un solde reflétant la quantité de crypto-monnaie détenue. Le wallet garde aussi la trace des transactions envoyées et reçues.