

# Conception

## Systeme d'inscription

1. Insertion info user → username , password , email → generation de token pour l'user
2. Verification email → envoie de lien contenant le token de l'utilisateur → valider sur postman
3. Insertion user après verification email
4. Gestion des erreurs
  - a. email non existante

## Systeme de connection

1. Insertion username + password
2. Création de session pour la connexion
3. Envoie d'un code PIN d'identification email
4. Verification de l'email → gestion des erreurs
5. Gestion de la durée des sessions avec un listener
6. Gestion des erreurs → Limite \* 3
  - a. erreur mot de passe && PIN && email non vérifie
  - b. réinitialisation des tentative via email

## Action utilisateur

1. Inscription
2. Connection

3. Modification → username , password
4. Suppression → compte

## Lien api

- /api/auth/user/login → lien pour connection user ( method : post )
- /api/auth/user → lien pour les actions user avec token ( method : get , update , delete )
- /api/auth/user/register ( method : post )
- /api/auth/user/verify\_email?token=\*\*\*\*\* → lien pour vérification user ( method : get )

## Point important

- Gestion des sessions pour un utilisateur
- Documentation api Swagger
- Code sur github ou gitlab
- Docker ????

## Contenu Documentation Technique

- ✓ ~~MCD~~
- ✓ ~~Scénario d'utilisation~~
- ✓ ~~Fonctionnalités~~
- ✓ ~~Liste des membres (Nom , Prénom , ETU)~~

## A livrer

- ✓ ~~codes sources~~

- ☒ instruction pour lancer l'api
- ☒ collection postman
- ☐ to-do list avec membre
- ☒ Documentation

## A voir pour le V2:

Créer un site d'échange de crypto-monnaies implique une compréhension claire des étapes nécessaires pour gérer les transactions en toute sécurité et conformité. Voici les étapes principales à inclure :

---

### 1. Inscription et vérification des utilisateurs

- **Inscription** : Permettre aux utilisateurs de créer un compte.
  - **Vérification KYC (Know Your Customer)** : Collecte des informations personnelles pour vérifier l'identité des utilisateurs, comme des pièces d'identité et des preuves d'adresse.
  - **2FA (Authentification à deux facteurs)** : Ajouter une couche de sécurité supplémentaire pour les connexions.
- 

### 2. Dépôt de fonds

- **Fiat** : Permettre les dépôts via cartes bancaires, virements bancaires, ou autres moyens de paiement.
  - **Crypto** : Générer des adresses de portefeuille uniques pour chaque utilisateur pour recevoir des crypto-monnaies.
  - **Validation des dépôts** : Confirmer les transactions fiat/crypto et créditer les comptes utilisateurs.
- 

### 3. Mécanisme d'échange (Order Book ou AMM)

- **Prix en temps réel** : Intégrer des API pour récupérer les taux de change actuels des crypto-monnaies.
  - **Options de transaction** :
    - **Achat/Vente instantanée** : L'utilisateur achète ou vend au meilleur prix du marché.
    - **Ordres limités** : L'utilisateur peut définir un prix spécifique auquel il souhaite acheter ou vendre.
  - **Moteur de correspondance des ordres** : Faire correspondre les ordres d'achat et de vente.
- 

## 4. Transactions blockchain

- **Envoi de crypto** : Lorsque les utilisateurs achètent, l'échange doit envoyer les fonds achetés à leur portefeuille ou à celui de l'échange.
  - **Confirmation** : Vérification via la blockchain pour s'assurer que la transaction est validée.
- 

## 5. Retraits

- **Retraits fiat** : Autoriser les utilisateurs à retirer leurs fonds en monnaie fiduciaire vers leur compte bancaire.
  - **Retraits crypto** : Permettre les retraits vers des portefeuilles externes après confirmation et validation (via 2FA ou autre).
- 

## 6. Gestion des frais

- **Frais de transaction** : Appliquer un pourcentage ou un montant fixe pour les échanges, dépôts, et retraits.
  - **Transparence** : Montrer clairement les frais avant de finaliser chaque transaction.
- 

## 7. Sécurité

- **Stockage des fonds** :

- **Hot wallets** : Pour les transactions quotidiennes.
  - **Cold wallets** : Pour stocker la majorité des fonds hors ligne.
  - **Audit des transactions** : Suivi et enregistrement des transactions pour éviter les fraudes.
  - **Détection d'activité suspecte** : Utiliser des systèmes pour identifier les activités anormales.
- 

## 8. Historique et tableau de bord

- **Historique des transactions** : Permettre aux utilisateurs de voir toutes leurs transactions passées.
  - **Portfolio** : Afficher le solde de chaque crypto et son équivalent en fiat.
- 

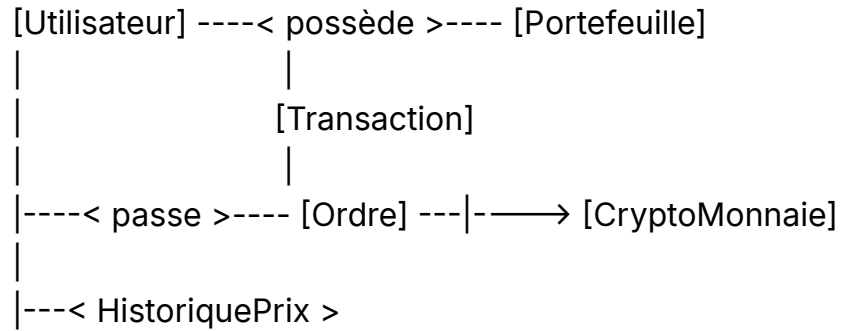
## 9. Conformité légale

- **Licence** : Obtenir une licence pour opérer un échange (les exigences varient selon le pays).
  - **AML (Anti-Money Laundering)** : Mettre en place des politiques pour détecter et prévenir le blanchiment d'argent.
  - **Reporting** : Fournir des rapports de transactions aux autorités fiscales si nécessaire.
- 

## 10. Assistance client

- **Support** : Ajouter un système de tickets ou chat pour répondre aux préoccupations des utilisateurs.
  - **Éducation** : Fournir des guides sur la sécurité et l'utilisation de la plateforme.
- 

Ces étapes garantissent un site d'échange fonctionnel, sécurisé et conforme. Envisagez également de travailler avec des experts juridiques et techniques pour lancer une plateforme conforme et fiable.



- **Utilisateur**

- IdUtilisateur (PK)
- Nom
- Prénom
- Email
- MotDePasse
- Adresse
- NuméroTéléphone
- DateInscription
- Vérifié (booléen pour KYC)

- **Portefeuille**

- IdPortefeuille (PK)
- IdUtilisateur (FK vers Utilisateur)
- SoldeFiat
- SoldeCrypto

- **Transaction**

- IdTransaction (PK)
- IdUtilisateur (FK vers Utilisateur)

- TypeTransaction (achat, vente, dépôt, retrait)
- MontantFiat
- MontantCrypto
- DateTransaction
- StatutTransaction (en cours, confirmé, échoué)
- **CryptoMonnaie**
  - IdCrypto (PK)
  - NomCrypto
  - SymboleCrypto
  - ValeurEnFiat (prix actuel)
- **Ordre**
  - IdOrdre (PK)
  - IdUtilisateur (FK vers Utilisateur)
  - IdCrypto (FK vers CryptoMonnaie)
  - TypeOrdre (achat, vente)
  - PrixUnitaire
  - Quantité
  - StatutOrdre (ouvert, exécuté, annulé)
  - DateCréation
- **HistoriquePrix**
  - IdHistorique (PK)
  - IdCrypto (FK vers CryptoMonnaie)
  - DatePrix
  - ValeurFiat
- **CryptoMonnaie** (mise à jour avec des informations supplémentaires)
  - IdCrypto (PK)

- NomCrypto
- SymboleCrypto
- Description
- DateCréation
- **PrixCrypto** (entité pour stocker les prix actualisés)
  - IdPrixCrypto (PK)
  - IdCrypto (FK vers CryptoMonnaie)
  - Devise (USD, EUR, etc.)
  - PrixActuel
  - DateDernièreMiseÀJour
- **TauxChange** (pour gérer les conversions entre cryptos et fiat)
  - IdTauxChange (PK)
  - IdCrypto1 (FK vers CryptoMonnaie)
  - IdCrypto2 (FK vers CryptoMonnaie ou devise fiat)
  - Taux
  - DateDernièreMiseÀJour