API Documentation

Overview

This API provides authentication and wallet management functionality. Authentication is handled via a JWT stored in an HTTP cookie named **sid**.

Base URL
http://localhost:PORT

Authentication

After successful registration or login, a JWT is issued and stored in a cookie named **sid**. Protected routes require this cookie to be present. Frontend requests must include credentials.

Auth Endpoints

POST /auth/register

Creates a new user account.

Request Body:
- name (string, required)
- email (string, required, unique)
- password (string, required)
- username (string, required, unique)

POST /auth/login

Authenticates a user and sets the JWT cookie.

Request Body:
- email (string, required)
- password (string, required)

GET /auth/me

Returns the currently authenticated user.

Authentication: Required (JWT via sid cookie)
Request Body: None

Wallet Endpoints

GET /wallet/getWallets

Returns wallets for the authenticated user.

Authentication: Required
Request Body:
- name (string, required)
Middleware: req.user.id

POST /wallet/create

Creates a new wallet.

Authentication: Required
Request Body:
- page (number, required)
- pageSize (number, required)

DELETE /wallet/delete/:walletId

Deletes a wallet by ID.

Authentication: Required
URL Params:
- walletId (string, required)
Middleware: req.user.id