Digital Wallet API Documentation

Auth Middleware

- All protected routes require authentication.
- `req.user` contains authenticated user info (e.g., `_id`, `email`).

Wallet Routes

Method	Endpoint	Description	Request Body	Response
POST	`/wallet`	Create or get wallet for currency	`{ currency: "USD" }`	Wallet object
GET	`/wallets`	Get all wallets for logged user	None	Array of wallet objects

---

Transaction Routes

Method	Endpoint	Description	Request Body	Response
POST	`/transaction`	Create a new transaction	`{ fromWallet, toWallet, amount, currency, type }`	Transaction object
GET	`/transactions`	Get transactions for logged user	None	Array of transactions
DELETE	`/transaction/:id`	Soft delete a transaction	None	Success message / error

Admin Routes

Method	Endpoint	Description	Request Params	Response
GET	`/admin/flagged`	List all flagged suspicious transactions	None	Array of flagged transactions
GET	`/admin/totals`	Get total balances by currency	None	Array of `{_id: currency, total: balance}`
GET	`/admin/top-users`	Get top 5 users by total balance	None	Array of `{_id: userId, total: balance}`

Fraud Detection & Bonus Features

- **Daily Fraud Scan:**
  Runs automatically every day at midnight using a cron job to find flagged transactions and trigger mock email alerts.

- **Soft Delete:**
  Transactions are soft deleted (using `isDeleted` flag), so data is not permanently removed.

- **Email Alerts:**
  Mock email alerts are sent for large or suspicious transactions (logged to console to simulate real email sending).

Notes

- All responses return JSON.
- Error handling returns appropriate HTTP 4xx or 5xx status with error message.
- Authentication required for all user-specific routes.
- Admin routes should be protected with role-based middleware.