TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HỒ CHÍ MINH

KHOA CÔNG NGHỆ THÔNG TIN

BUILD A SIMPLE BLOCKCHAIN FROM SCRATCH

MÔN: BLOCKCHAIN VÀ ỨNG DỤNG

GVHD: TS. Huỳnh Xuân Phụng

HVTH: Trần Thị Minh Ánh

Phạm Đinh Quốc Hòa

Nguyễn Phương Thịnh

Thành phố Hồ Chí Minh, tháng 11 năm 2025

MỤC LỤC

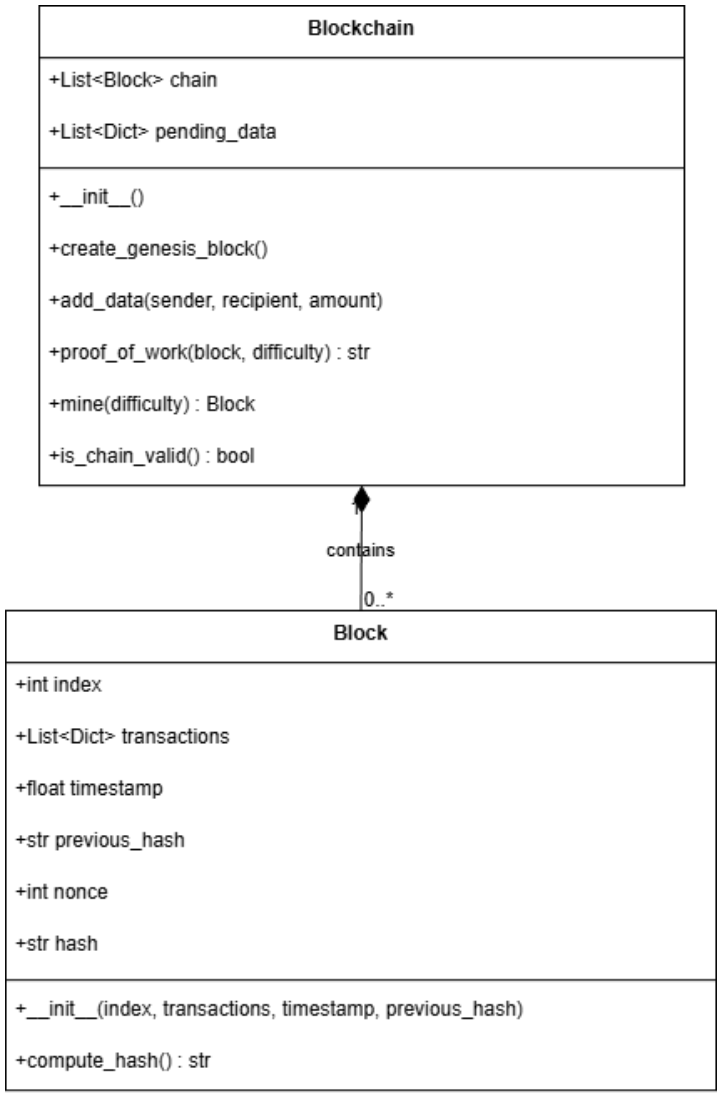
DANH MỤC HÌNH ẢNH

CHƯƠNG 1. SƠ ĐỒ LỚP

1.1. Mã nguồn

GitHub: https://github.com/hoadaknong101/bc_week_1

1.2. Sơ đồ lớp



Hình 1.1. Sơ đồ lớp

1.3. Triển khai lớp Block

Mỗi khối giống như một trang trong cuốn sổ cái. Nó phải chứa:

- index: Số thứ tự trang (0, 1, 2...).

- timestamp: Thời gian khối được tạo.
- data: Dữ liệu giao dịch (ví dụ: "A chuyển cho B 10 coin").
- previous_hash: Dấu vân tay của khối liền trước (đây là cái móc xích tạo nên chuỗi).
- nonce: Một số ngẫu nhiên dùng để đào (mining).

calculate_hash(): Hàm tạo dấu vân tay số (thường dùng thuật toán SHA-256) cho toàn bộ dữ liệu trên.

1.4. Triển khai lớp Blockchain

Quản lý danh sách các khối (`chain`).

`create_genesis_block()`: Tạo khối đầu tiên (Khối nguyên thủy) vì khối này không có khối trước nó.

`add_block()`: Thêm một khối mới vào danh sách sau khi đã đào xong.

1.5. Proof-of-Work

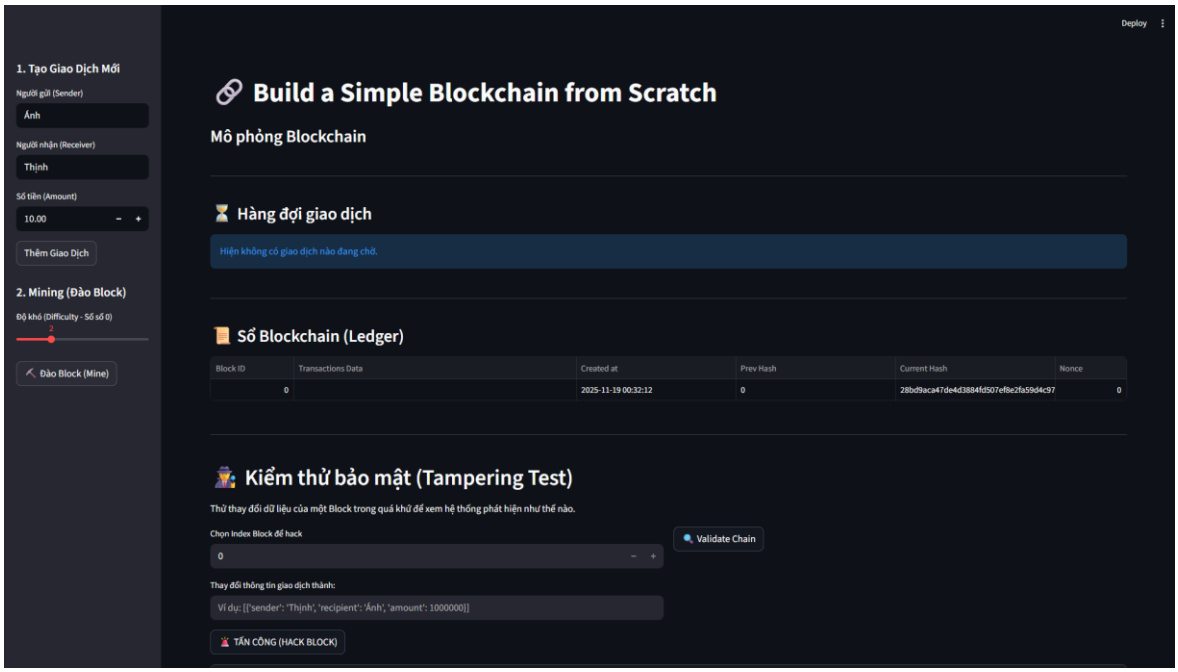
Đây là phần quan trọng nhất mô phỏng việc "đào coin". `mine_block()`: Máy tính phải chạy một vòng lặp để tìm ra số `nonce` sao cho hash của khối bắt đầu bằng một số lượng số 0 nhất định (ví dụ: `0000abc...`). Việc này tốn tài nguyên CPU, ngăn chặn kẻ gian spam block giả mạo.

1.6. Chain Validation

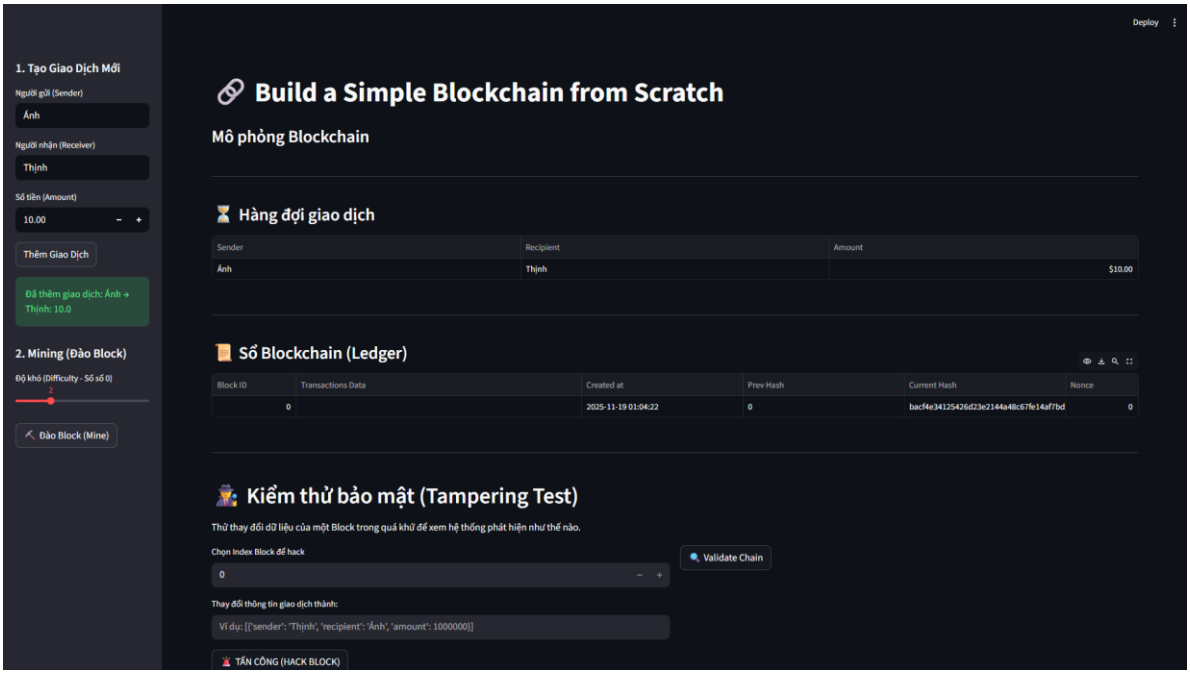
- is_chain_valid(): Duyệt lại toàn bộ chuỗi để đảm bảo:
- Hash của khối hiện tại là chính xác (dữ liệu không bị sửa).
- previous_hash của khối hiện tại khớp với hash của khối trước đó (chuỗi không bị đứt gãy).

CHƯƠNG 2. GIAO DIỆN ỨNG DỤNG

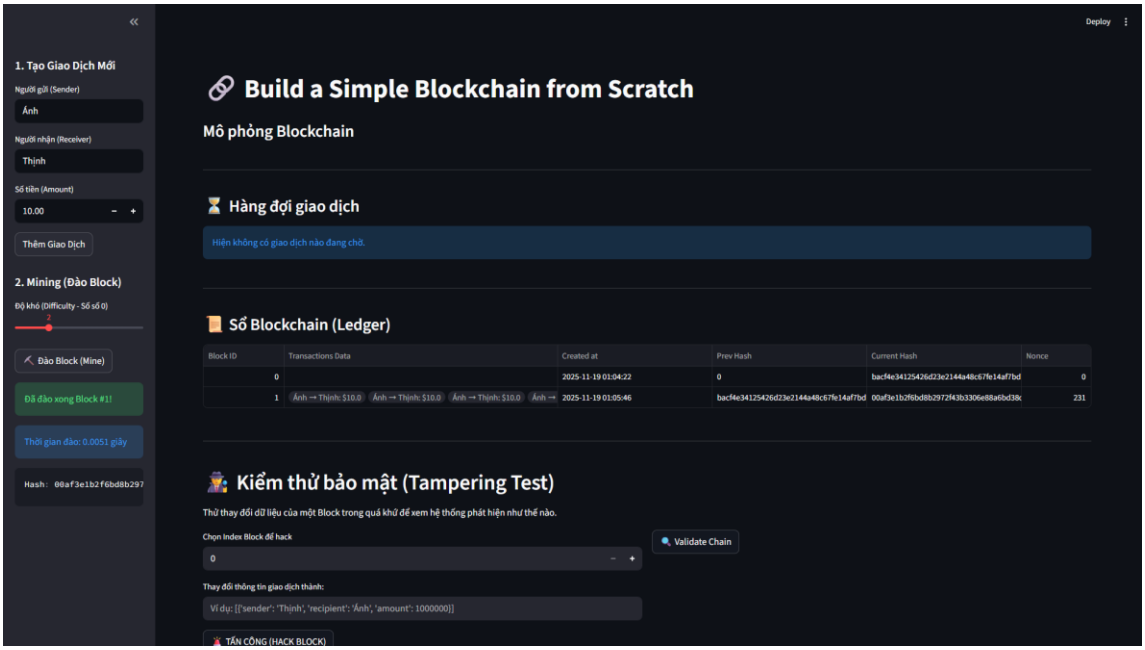
2.1. Giao diện ứng dụng



Hình 2.1. Giao diện ứng dụng khi mới truy cập

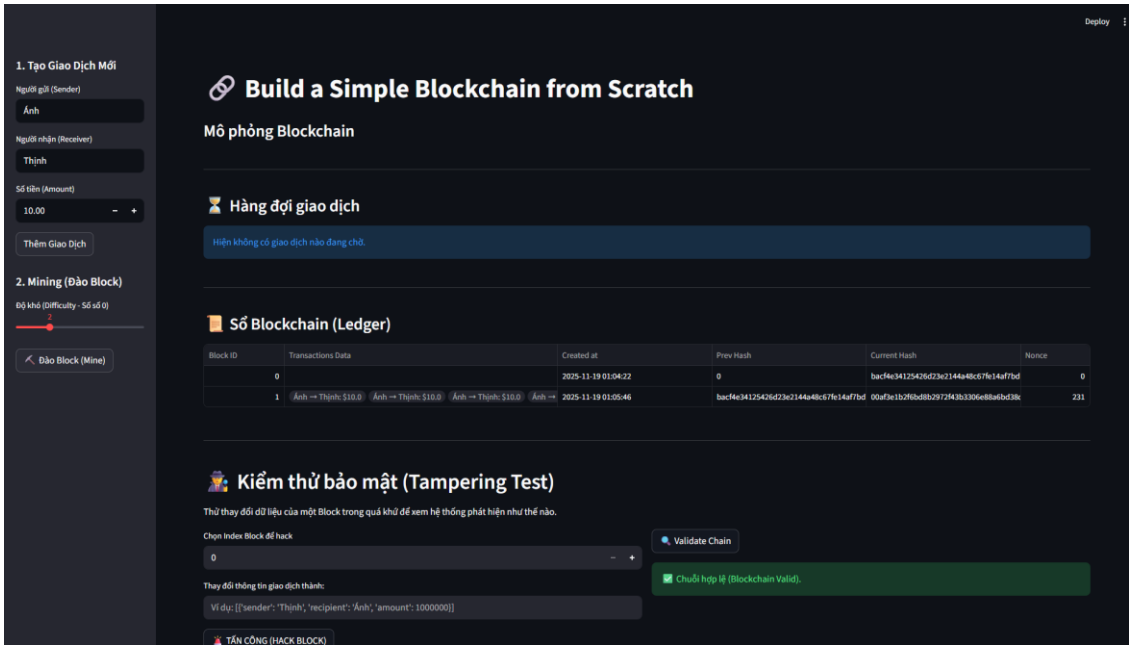


Hình 2.2. Giao diện khi thêm giao dịch

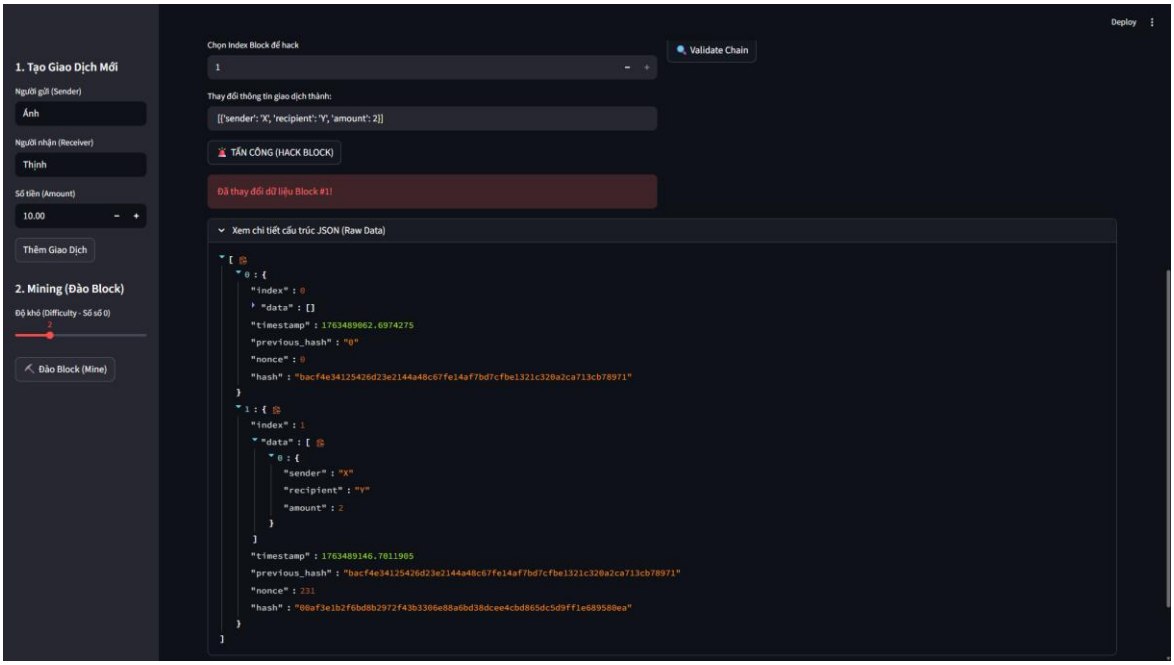


Hình 2.3. Giao diện khi tiến hành mining

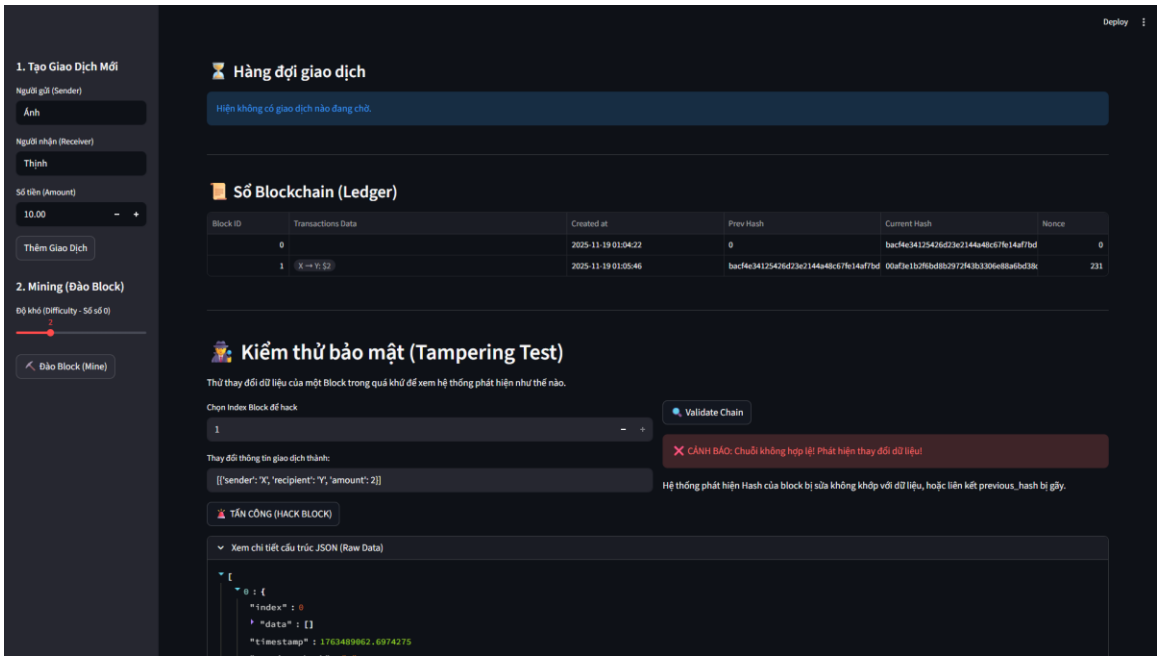
2.2. Giao diện khi tiến hành tấn công



Hình 2.4. Kiểm tra chuỗi khối hiện tại có hợp lệ hay không



Hình 2.5. Giao diện khi tiến hành thay đổi dữ liệu khối có index là 1



Hình 2.6. Giao diện khi kiểm tra chuỗi hợp lệ sau khi tấn công