

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN

------



HCMUTE

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

MỤC LỤC	i
DANH MỤC HÌNH ẢNH	ii
CHƯƠNG 1. SƠ ĐỒ LỚP	1
1.1. Mã nguồn	1
1.2. Sơ đồ lớp	1
1.3. Triển khai lớp Block	1
1.4. Triển khai lớp Blockchain	2
1.5. Proof-of-Work	2
1.6. Chain Validation	2
CHƯƠNG 2. GIAO DIỆN ỨNG DỤNG	3
2.1. Giao diện ứng dụng	3
2.2. Giao diện khi tiến hành tấn công	4

DANH MỤC HÌNH ẢNH

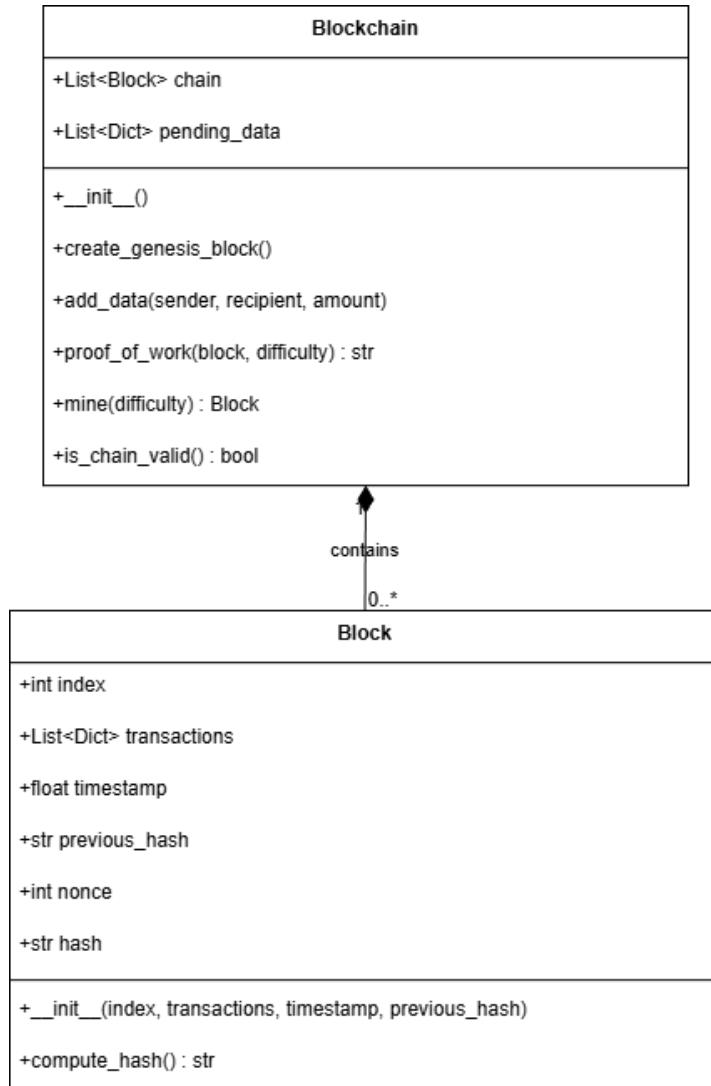
Hình 2.1. Giao diện ứng dụng khi mới truy cập	3
Hình 2.2. Giao diện khi thêm giao dịch.....	3
Hình 2.3. Giao diện khi tiến hành mining	4
Hình 2.4. Kiểm tra chuỗi khối hiện tại có hợp lệ hay không.....	4
Hình 2.5. Giao diện khi tiến hành thay đổi dữ liệu khối có index là 1	5
Hình 2.6. Giao diện khi kiểm tra chuỗi hợp lệ sau khi tấn công	5

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 khói được tạo.
- data: Dữ liệu giao dịch (ví dụ: "A chuyển cho B 10 coin").
- previous_hash: Dấu vân tay của khói 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 khói (`chain`).

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

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

1.5. Proof-of-Work

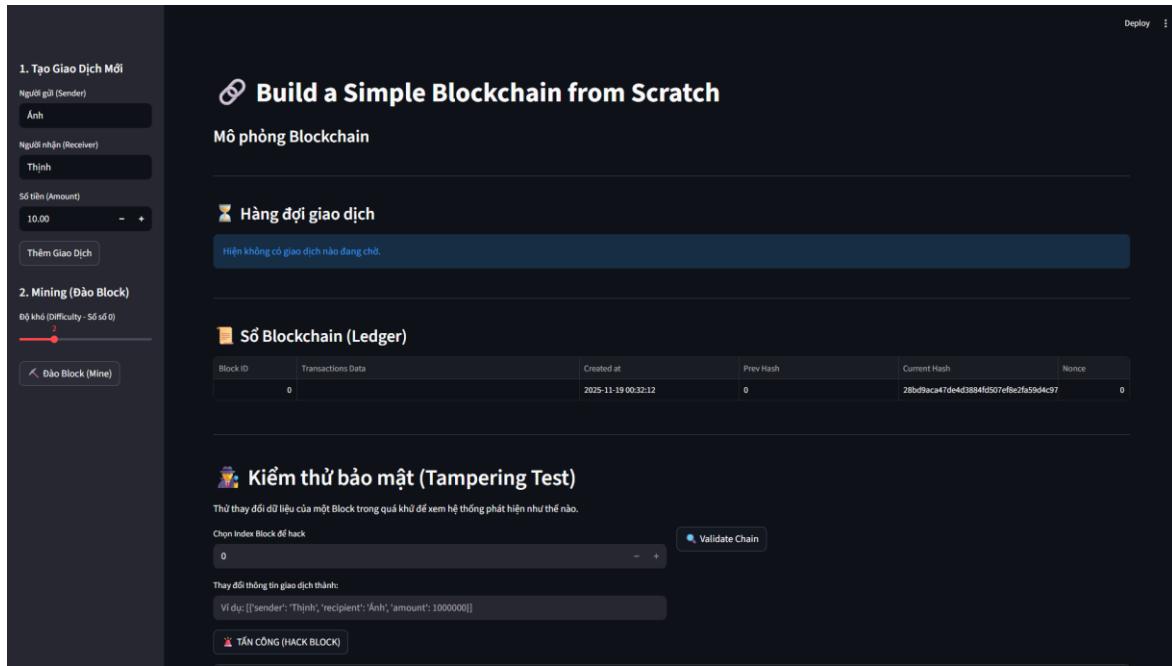
Đây là phần quan trọng nhất mô phỏng việc “đào coin”. `mine_block()`: Máy tính phải chạy một vòng lặp để tìm ra số `nonce` sao cho hash của khói bắt đầu bằng một số lượng số 0 nhất định (ví dụ: 0000abc...). Việc này tốn tài nguyên CPU, ngăn chặn kẻ gian spam block giả mạo.

1.6. Chain Validation

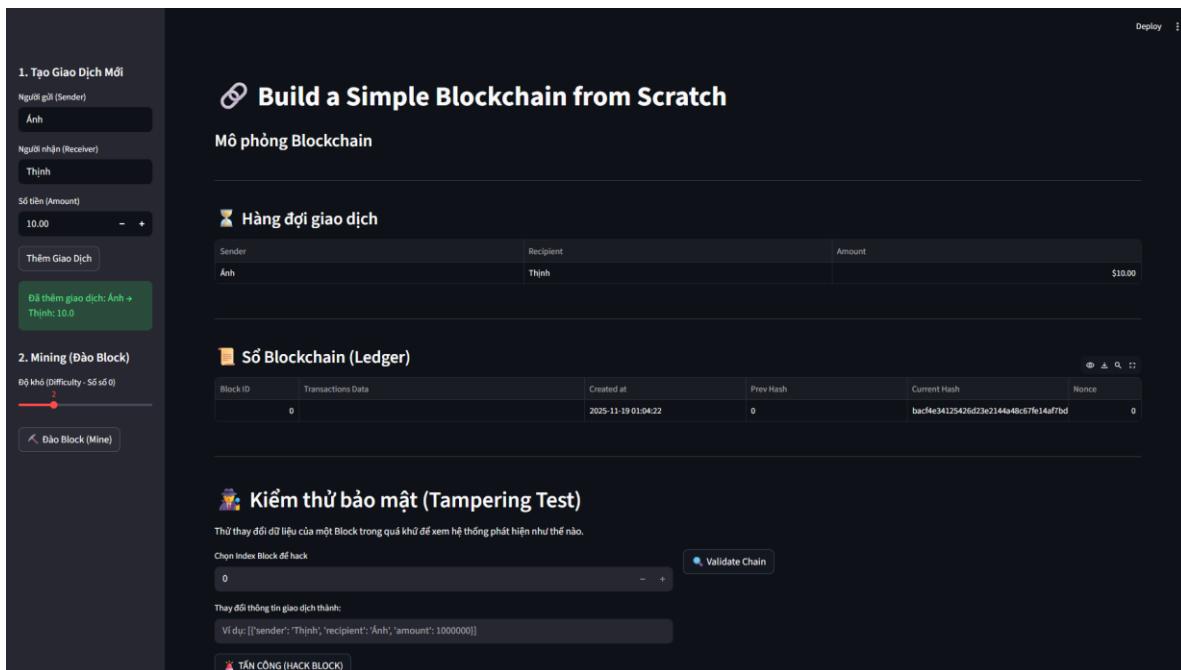
- `is_chain_valid()`: Duyệt lại toàn bộ chuỗi để đảm bảo:
- Hash của khói hiện tại là chính xác (dữ liệu không bị sửa).
- `previous_hash` của khói hiện tại khớp với hash của khói trước đó (chuỗi không bị đứt gãy).

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

The screenshot shows a blockchain application interface. On the left, there's a sidebar with two sections: "1. Tạo Giao Dịch Mới" (Create New Transaction) and "2. Mining (Đào Block)". Under "1.", fields are shown for "Người gửi (Sender)" (Anh), "Người nhận (Receiver)" (Thịnh), and "Số tiền (Amount)" (10.00). Under "2.", a "Độ Khó (Difficulty - Số số 0)" slider is at 0, and buttons for "Đào Block (Mine)" and "Đã đào xong Block #1!" are visible. A note says "Thời gian đào: 0.0051 giây" and shows a hash: "Hash: 00af3e1b2f6bd8b297". On the right, the main area is titled "Build a Simple Blockchain from Scratch" and "Mô phỏng Blockchain". It shows a "Hàng đợi giao dịch" (Transaction Queue) with the message "Hiện không có giao dịch nào đang chờ.". Below it is a "Số Blockchain (Ledger)" table:

Block ID	Transactions Data	Created at	Prev Hash	Current Hash	Nonce
0		2025-11-19 01:04:22	0	bacf4e34125426d23e2144a48c67fe14af7bd	0
1	Anh → Thịnh: \$10.0 / Anh → Thịnh: \$10.0 / Anh → Thịnh: \$10.0 / Anh →	2025-11-19 01:05:46	bacf4e34125426d23e2144a48c67fe14af7bd	00af3e1b2f6bd8b2972f43b3306e88a6bd38k	231

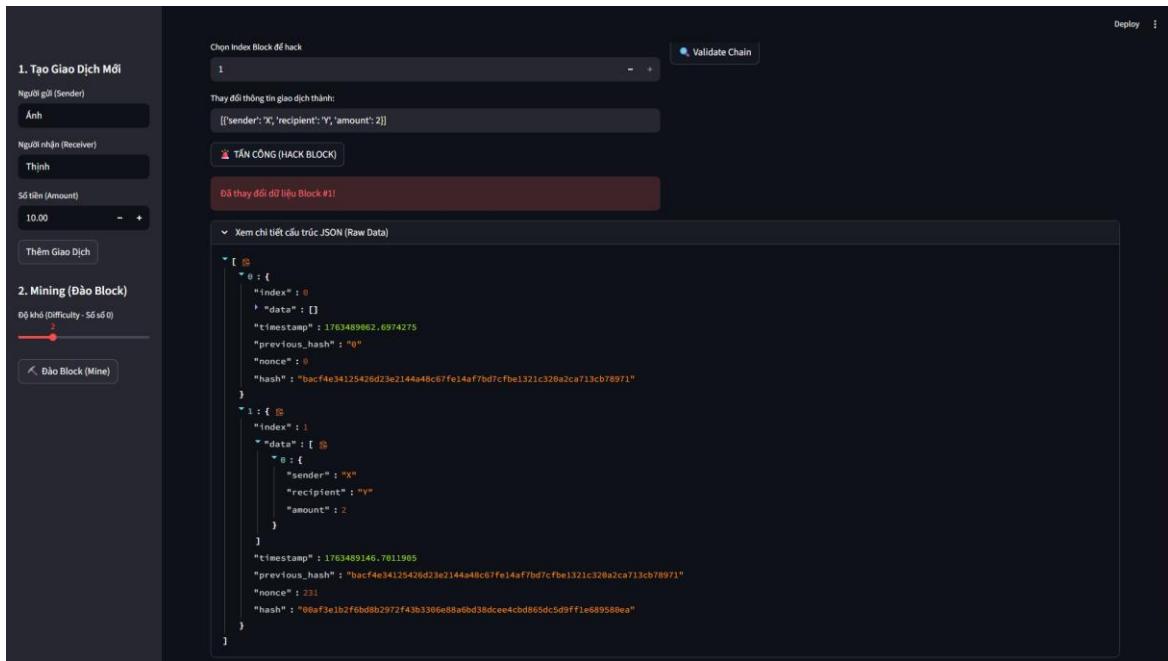
Below the ledger is a "Kiểm thử bảo mật (Tampering Test)" section with a note: "Thay đổi dữ liệu của một Block trong quá khứ để xem hệ thống phát hiện như thế nào." It includes a dropdown for "Chọn Index Block để hack" (Select Block Index to Hack) set to 0, a "Validate Chain" button, and a text input for "Thay đổi thông tin giao dịch thành:" with placeholder "[{"sender": "Thịnh", "recipient": "Anh", "amount": 1000000}]". At the bottom is a red button labeled "TẤN CÔNG (HACK BLOCK)".

Hình 2.3. Giao diện khi tiến hành mining

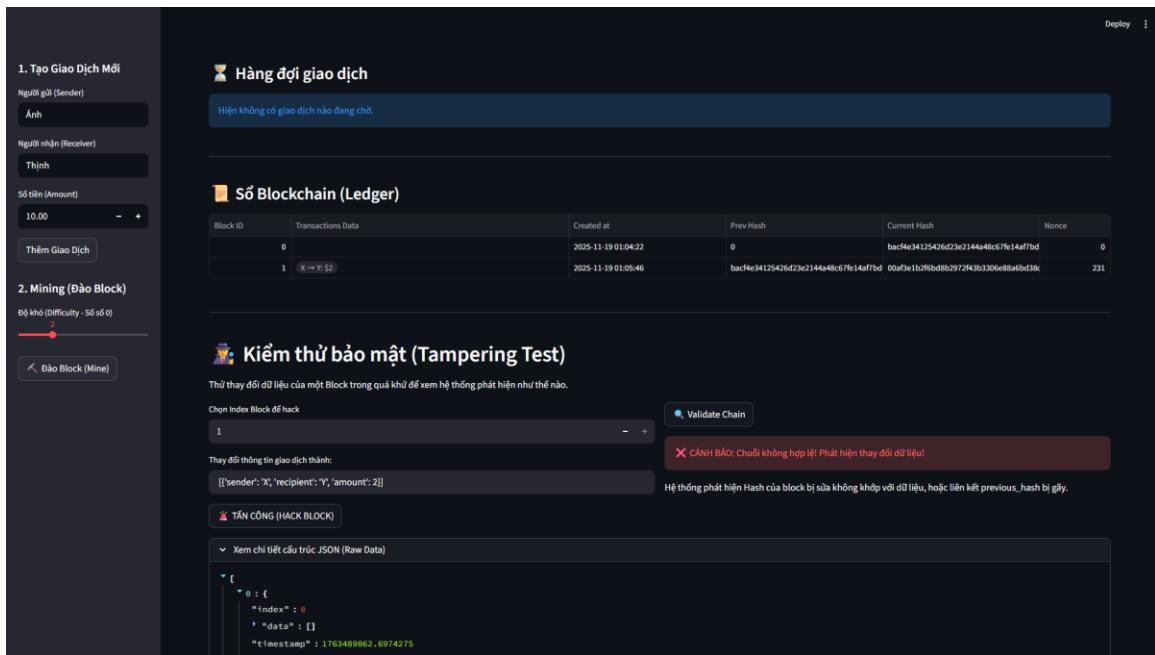
2.2. Giao diện khi tiến hành tấn công

This screenshot is identical to the one above, but the "TẤN CÔNG (HACK BLOCK)" button has been clicked. The "Validate Chain" button is now greyed out, and a green button labeled "Chuỗi hợp lệ (Blockchain Valid)." is visible. The ledger table remains the same.

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