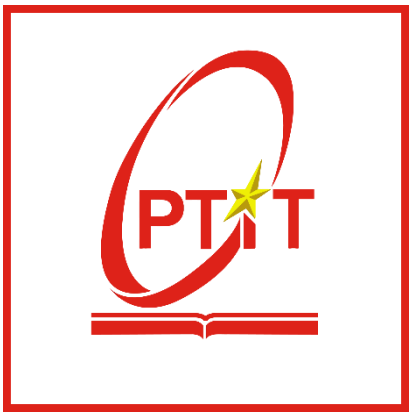
BỘ KHOA HỌC VÀ CÔNG NGHỆ
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÁO CÁO BÀI TẬP LỚN

CHUYÊN ĐỀ:
PHÂN TÍCH AN TOÀN THÔNG TIN CHO MODULE BLOCKCHAIN TRONG HỆ THỐNG PEPE

-NHÓM 4-

Môn học: Cơ sở an toàn thông tin

Giảng viên PGS.TS Đỗ Xuân Chợ

Thành viên	Trần Vũ Tiến Minh	B23DCCE067
	Phạm Quốc Hùng	B23DCVT188
	Trần Hoàng Nam	B23DCCE070
	Phạm Thanh An	B23DCCE004
	Phạm Đào Thanh Tùng	B23DCVT449

Lớp: D23CQCE04-B

Hà Nội, Tháng 12/2025

LỜI NÓI ĐẦU

"Trong bối cảnh chuyển đổi số toàn cầu, công nghệ Blockchain nổi lên như một giải pháp đột phá về tính minh bạch và khả năng chống sửa đổi dữ liệu. Tuy nhiên, một quan niệm sai lầm phổ biến là các hệ thống dựa trên Blockchain mặc nhiên an toàn tuyệt đối. Thực tế cho thấy, các lỗ hổng trong smart contract (hợp đồng thông minh), giao thức đồng thuận hay các module tích hợp vẫn là mục tiêu tấn công ưa thích của tội phạm mạng.

Đối với hệ thống **PEPE**, module Blockchain đóng vai trò là xương sống trong việc vận hành và lưu trữ các giao dịch quan trọng. Bất kỳ sơ suất nào trong khâu bảo mật tại module này đều có thể dẫn đến hậu quả nghiêm trọng về tài sản và uy tín của toàn hệ thống. Xuất phát từ tính cấp thiết đó, bài báo cáo **'PHÂN TÍCH AN TOÀN THÔNG TIN CHO MODULE BLOCKCHAIN TRONG HỆ THỐNG PEPE'** được thực hiện nhằm nhận diện các bề mặt tấn công, đánh giá rủi ro và đề xuất các biện pháp củng cố an ninh, đảm bảo tính bí mật, toàn vẹn và sẵn sàng cho hệ thống."

NHẬN XÉT ĐÁNH GIÁ CHO ĐIỂM
(Của giảng viên hướng dẫn)

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

Điểm: ..... (bằng chữ……)

Hà Nội,...ngày... tháng 12 năm 2025.
CÁN BỘ, GIẢNG VIÊN HƯỚNG DẪN
(ký, họ tên)

NHẬN XÉT ĐÁNH GIÁ CHO ĐIỂM
(Của giảng viên phản biện)

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

Điểm: ..... (bằng chữ…….)

Hà Nội,...ngày... tháng 12 năm 2025.

CÁN BỘ, GIẢNG VIÊN PHẢN BIỆN

(ký, họ tên)

MỤC LỤC

BẢNG PHÂN CÔNG CÔNG VIỆC

Mã sinh viên	Thành viên	Công việc
B23DCCE067	Trần Vũ Tiến Minh	• Thiết kế Database • Sửa lỗi và kiểm thử hệ thống • Phê duyệt code cuối cùng • Phụ trách phần tính năng Download tài liệu tích hợp blockchain • Kiểm thử smart contract (test case), kiểm tra logic & bảo mật cơ bản, mô phỏng các tương tác người dùng với contract (gọi hàm, kiểm tra dữ liệu). • Phát triển và tối ưu back-end cho toàn hệ thống
B23DCVT188	Phạm Quốc Hùng (Trưởng nhóm)	• Thiết kế Database của app Forum • Xử lí front-end và back-end của Forum • Phụ trách tính năng làm test tích hợp block chain • Phân tích và thiết kế nghiệp vụ logic, bảo mật • Kiểm thử tính năng
B23DCCE070	Trần Hoàng Nam	• Thiết kế mô hình kiến trúc cho dự án • Thiết kế Database của app account và wallet • Xử lí front-end và back-end của account và wallet • Phụ trách phần kết nối Web3, kết nối ví, đọc/ghi dữ liệu từ smart contract.
B23DCCE004	Phạm Thanh An	• Phụ trách phần Chatbot • Hỗ trợ kết nối back-end với smart contract • Phụ trách tính năng giới thiệu thưởng token • Phát triển và tối ưu front-end cho toàn hệ thống • Hỗ trợ viết báo cáo • Thiết kế Database của app Home • Xử lí front-end của app Home
B23DCVT449	Phạm Đào Thanh Tùng	• Thiết kế điểm danh hệ thống PEPE • Viết báo cáo

GIỚI THIỆU CHUNG WEB PEPE
– HỆ SINH THÁI HỌC TẬP & KẾT NỐI DÀNH RIÊNG CHO SINH VIÊN PTIT

Chào mừng bạn đến với WEB PEPE – Diễn đàn học thuật và kết nối cộng đồng sinh viên Học viện Công nghệ Bưu chính Viễn thông (PTIT). Hơn cả một kho tài liệu, WEB PEPE là nơi tri thức được sẻ chia, tinh thần tự học được khích lệ và những nỗ lực đóng góp được ghi nhận xứng đáng. Tại đây, chúng tôi xây dựng một môi trường "Win-Win", nơi người học tìm thấy tài liệu chất lượng, và người chia sẻ nhận được sự ủng hộ thiết thực.

Cơ chế hoạt động & Hệ thống Token: Tại WEB PEPE, Token không chỉ là điểm số, nó là đơn vị đo lường sự chăm chỉ và đóng góp của bạn:

Điểm danh mỗi ngày (+5 Token): Duy trì thói quen học tập hàng ngày để tích lũy tài nguyên miễn phí.

Mở khóa tài liệu học tập trong bài đăng (-5 Token): Sử dụng Token để tải xuống các tài liệu, đề thi chất lượng cao đã được chọn lọc.

Ủng hộ người làm ra bài kiểm tra (-1 Token/lượt test): Khi bạn thực hiện một bài kiểm tra, 1 Token của bạn sẽ được chuyển trực tiếp cho người tạo ra đề thi đó.

Giới thiệu bạn bè (Referral): Giới thiệu WEB PEPE đến bạn bè, người giới thiệu sẽ nhận được phần thưởng Token hấp dẫn.

WEB PEPE – Kết nối đam mê, sẻ chia tri thức!

Phần I.
TỔNG QUAN VỀ KIẾN TRÚC BLOCKCHAIN TRONG PEPE

1. TỔNG QUAN VỀ KIẾN TRÚC BLOCKCHAIN TRONG PEPE

Mô hình hiện tại của dự án PEPE là một kiến trúc **Lai Tập trung (Custodial Single-Ledger)**. Dự án sử dụng Blockchain như sổ cái duy nhất cho tài sản (Token STK) nhưng duy trì sự kiểm soát tập trung đối với khóa riêng của người dùng.

1.1. Mô hình Tập trung (Custodial) và Sổ cái Đơn

Bản chất: Mô hình là **Custodial** (Giữ hộ), vì Server PEPE giữ **Private Key (PK)** của người dùng, biến Server thành điểm tin cậy duy nhất và là mục tiêu tấn công chính.
Ledger: Hệ thống tập trung hoàn toàn vào **Token STK** trên Blockchain (Sổ cái Phân tán) để xử lý mọi logic tài chính, bao gồm cả các nghiệp vụ có thể thực hiện off-chain trước đây (ví dụ: thưởng điểm danh, chuyển tiền nội bộ).

Lớp Kiến trúc	Thành phần	Nơi Lưu trữ	Mô tả/Mục đích
Layer 1: Blockchain (Token On-chain)	**Simple Token (STK)**	Blockchain (Ví người dùng)	**Toàn bộ Logic Tài sản:** Nạp/Rút Token, Điểm danh, nhận thưởng, mua nội dung/bài kiểm tra, nhận thưởng giới thiệu, Chuyển P2P.

Layer 2: Dữ liệu Vận hành	**Encrypted Private Key**	Database (students.encrypted_private_key)	**Bằng chứng ủy quyền:** Server giải mã và sử dụng PK để ký (sign) giao dịch burn và transfer on-chain thay mặt người dùng.

Triển khai các Nghiệp vụ Cốt lõi (Server Ký):

Logic: Người dùng nhập địa chỉ và PK. PK được mã hóa (encrypt_key) và lưu vào DB. Khi giao dịch (ví dụ: Nạp Token), Server giải mã (decrypt_key) PK và sử dụng nó để ký giao dịch (user_burn_tokens) và gửi lên Blockchain.

1.1. Ưu điểm và nhược điểm

Khía cạnh	Mô tả
Ưu điểm (Pros)	**Tiện ích (UX) cao:** Người dùng không cần tự ký thủ công (MetaMask) hoặc nhập PK mỗi lần. Server xử lý việc ký, tạo ra trải nghiệm liền mạch.
Nhược điểm (Cons)	**Rủi ro Tính Bí mật (FATAL):** Server giữ Private Key của TẤT CẢ người dùng. Nếu Server bị tấn công, hoặc khóa giải mã bị lộ, **toàn bộ tài sản STK của User sẽ bị đánh cắp**, vi phạm nghiêm trọng Tính Bí mật.

1.3. Điểm cần cải thiện về kiến trúc

Giải pháp Tốt hơn: Chuyển sang mô hình **Ủy quyền Admin (Delegated API/Relayer)** để loại bỏ việc Server lưu trữ PK của User. Đây là cách duy nhất để giải quyết rủi ro Custodial.

2. Công nghệ Nền tảng

Mạng lưới và Hợp đồng:

Hệ thống kết nối với một mạng blockchain thông qua API có địa chỉ là

https://hsc-w3oq.onrender.com/api.

Hợp đồng thông minh được sử dụng là **SimpleToken:**

Solidity Source Code:

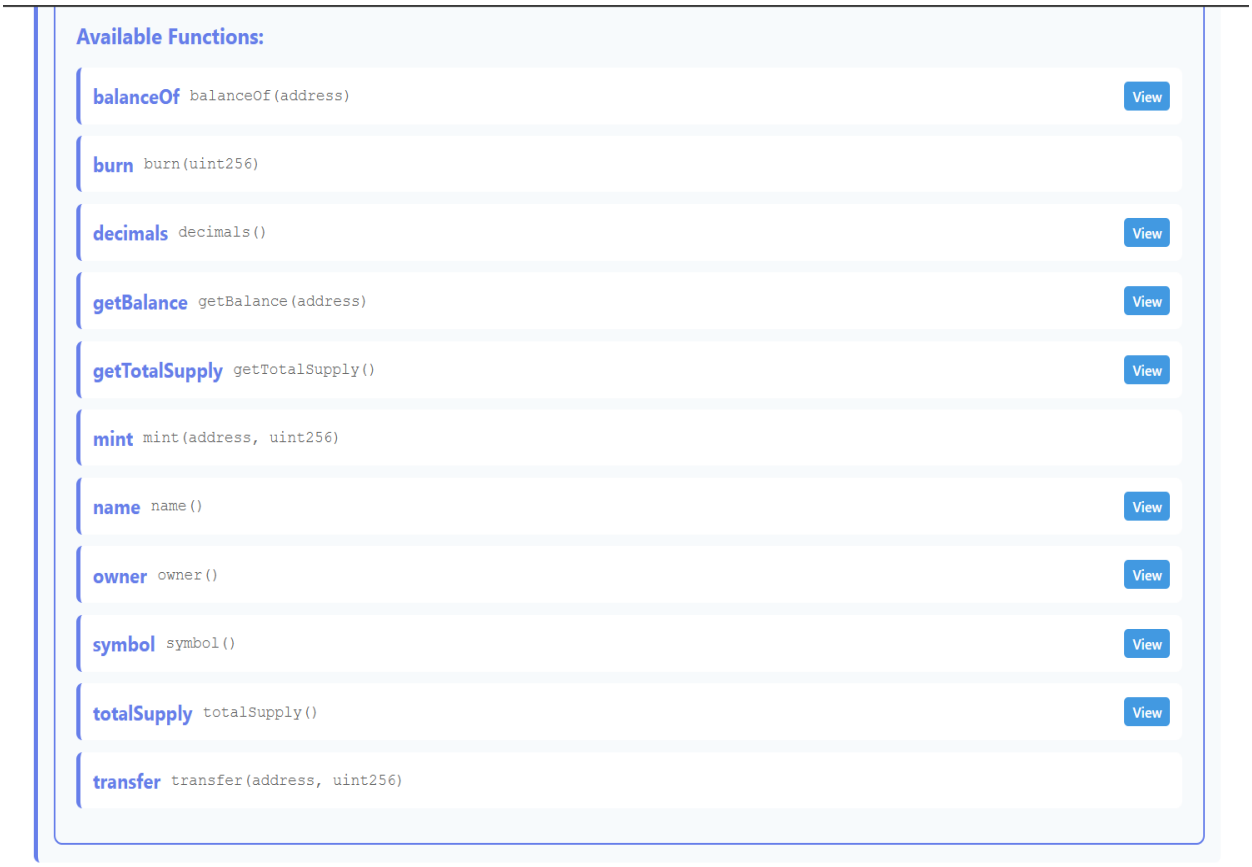
```
    // Chuyển token
    function transfer(address _to, uint256 _value) public returns (bool success) {
        require(_to != address(0), "Invalid address");
        require(balanceOf[msg.sender] >= _value, "Insufficient balance");

        balanceOf[msg.sender] -= _value;
        balanceOf[_to] += _value;

        emit Transfer(msg.sender, _to, _value);
        return true;
    }

    // Cộng token (mint) - chỉ owner có thể gọi
    function mint(address _to, uint256 _value) public returns (bool success) {
        require(_to != address(0), "Invalid address");
        require(msg.sender == owner, "Only owner can mint");

        totalSupply += _value;
        balanceOf[_to] += _value;

        emit Mint(_to, _value);
        emit Transfer(address(0), _to, _value);
        return true;
    }
    // Trừ token (burn)
    function burn(uint256 _value) public returns (bool success) {
        require(balanceOf[msg.sender] >= _value, "Insufficient balance");

        balanceOf[msg.sender] -= _value;
        totalSupply -= _value;

        emit Burn(msg.sender, _value);
        emit Transfer(msg.sender, address(0), _value);
        return true;
    }

    // Lấy số dư
    function getBalance(address _owner) public view returns (uint256) {
        return balanceOf[_owner];
    }

    // Lấy tổng cung
    function getTotalSupply() public view returns (uint256) {
        return totalSupply;
    }
}
```

Compile Contract | Deploy Contract

Compilation Successful!
Contract: SimpleToken
Bytecode: 6080604052604051806040016040528060b81526020017f53...

Available Functions:

- **balanceOf** `balanceOf(address)` — View
- **burn** `burn(uint256)`
- **decimals** `decimals()` — View
- **getBalance** `getBalance(address)` — View
- **getTotalSupply** `getTotalSupply()` — View



với địa chỉ hợp đồng là: 0x802c284f55030e4545d576b38a6da4c77dbf3fae

· Ví Admin (Mint/Cấp phát):

Một ví quản trị có vai trò là owner của hợp đồng Token, được sử dụng để thực hiện các giao dịch cấp phát Token khi người dùng rút Coin.

- Địa chỉ ví Admin: ***0x910df929197ce001f58fcd75290f934e012a5f03***.
- Private Key của Admin cũng được lưu trữ ở file .env không được public, tách biệt với database.

Phần II.

PHÂN TÍCH AN TOÀN THÔNG TIN THEO MÔ HÌNH CIA TRIAD

Mô hình bảo mật cốt lõi **CIA Triad** (Bí mật, Toàn vẹn, Sẵn dùng) được áp dụng để đánh giá module này:

1. Tính Bí mật (Confidentiality)

Mục tiêu: Đảm bảo **Private Key (PK)** của người dùng và Admin (là tài sản tối mật) được bảo vệ chống truy nhập, sử dụng, hoặc tiết lộ trái phép.

Biện pháp Bảo vệ và Quy trình Vận hành:

Mã hóa Dữ liệu Nhạy cảm: Thay vì lưu trữ Private Key dưới dạng văn bản thuần, hệ thống sử dụng thuật toán mã hóa đối xứng **Fernet** để mã hóa PK thành encrypted_private_key trước khi lưu vào database (bảng students).

Khóa Giải mã (Key Management): Khóa giải mã **Fernet** (PEPE_CRYPTO_KEY) được **tách biệt hoàn toàn** khỏi mã nguồn và database, được đọc từ môi trường hệ thống (Environment Variable). Điều này ngăn chặn việc giải mã hàng loạt PK nếu database và mã nguồn bị lộ đồng thời.

Quy trình Giải mã an toàn (Just-in-Time Decryption): PK chỉ được giải mã (bằng hàm decrypt_key) ngay trong bộ nhớ RAM của server, và được đưa vào inputdata mã hóathành hex-string gửi tới Hscoin.

Bảo vệ Khóa Admin: Tương tự, **Private Key Admin** (ADMIN_PRIVATE_KEY), vốn là một bí mật quan trọng, cũng được đọc từ Biến môi trường (PEPE_ADMIN_PK), loại bỏ rủi ro lộ PK Admin trong file cấu hình.

Vấn đề bảo mật:
Mặc dù đã mã hóa nhưng vẫn lưu trực tiếp trong DB
UPDATE students SET encrypted_private_key = %s
Thông tin nhạy cảm trong session

2. Tính Toàn vẹn (Integrity)

Tính toàn vẹn đảm bảo rằng dữ liệu tài sản (Token) và các giao dịch là chính xác, nhất quán và không bị làm giả.

a. Toàn vẹn trên Blockchain (On-chain Integrity)

Tính bất biến của Ledger: Các giao dịch chuyển tiền (transfer), nạp (burn) và rút (mint) được thực hiện trên Smart Contract SimpleToken. Một khi giao dịch đã được xác nhận trên blockchain, nó không thể bị sửa đổi hoặc xóa bỏ. Điều này đảm bảo lịch sử giao dịch là trung thực tuyệt đối.
Logic Smart Contract: Contract Solidity thực thi các quy tắc bất di bất dịch:
Không thể chuyển/burn quá số dư hiện có (require(balanceOf[msg.sender] >= _value)).
Chỉ owner (Admin) mới có quyền mint token mới.

b. Toàn vẹn dữ liệu:

Quy trình - Burn:

Hệ thống thực hiện **Burn Token trên Blockchain trước.**

Khi giao dịch thành công sẽ hiện block trên Hscoin và số dư Hscoin token sẽ bị trừ

Quy trình Mint:

User gọi lệnh mint và admin(sử dụng private key admin) sẽ mint (tạo) cho user 1 lượng token tương ứng.

Transaction hash tracking: Lưu tx_hash cho mọi giao dịch
Kiểm tra số dư: if current_coins < amount: trước khi rút

c. Toàn vẹn Bảo mật (Security Integrity)
Mã hóa khóa bí mật (Private Key Encryption):
Private Key của người dùng **không được lưu dưới dạng văn bản thuần (plaintext)** trong Database.

Hệ thống sử dụng thuật toán mã hóa đối xứng **Fernet (AES-128)** thông qua encrypt_key trước khi lưu và decrypt_key khi cần sử dụng. Điều này bảo vệ ví người dùng ngay cả khi Database bị lộ.

Che giấu thông tin nhạy cảm trong Log:

Hàm call_hscoin có cơ chế tự động che giấu (masking) Private Key trong log hệ thống:

If 'privateKey' in log_payload: log_payload['privateKey'] = '***'.

Đây là một thực hành bảo mật tốt để đảm bảo tính toàn vẹn của hệ thống quản lý.

Vấn đề toàn vẹn:

Không có digital signature:

API calls không có signature verification

Dễ bị replay attack

Validate input chưa đủ mạnh:

3.Tính Sẵn dùng (Availability)

Tính **Sẵn dùng (Availability)** là yếu tố đảm bảo hệ thống và thông tin luôn có thể truy cập được cho người dùng hợp pháp khi họ yêu cầu.

Retry mechanism: Có retry cho HSCOIN API calls

Timeout settings: timeout=30 cho API calls

Error handling: Xử lý exception cơ bản

Fallback encoding: Có fallback khi không import được web3

a. Điểm Yếu Cốt Lõi: Phụ thuộc API bên ngoài

Các giao dịch quan trọng (Mint/Burn, Transfer Token) yêu cầu giao tiếp với API Blockchain bên ngoài (HSCOIN_API_BASE_URL).

Rủi ro: Nếu API HSCOIN_API_BASE_URL gặp sự cố mạng, bị tấn công từ chối dịch vụ (DoS/DDoS), hoặc ngừng hoạt động kéo dài, **toàn bộ chức năng ví sẽ bị tê liệt**.

b. Các Biện pháp Phòng vệ Hiện tại (Lớp 1)

Dự án đã có cơ chế cơ bản để giảm thiểu lỗi mạng tạm thời:

Cơ chế Thử lại (Retry): Hàm call_hscoin trong accounts/utils.py sử dụng **HTTP Adapter** và **Retry** :

```
from urllib3.util.retry import Retry

    retries = Retry(total=1, backoff_factor=0.5,
status_forcelist=[502,503,504], allowed_methods=["POST"],
raise_on_status=False)
```

Ưu điểm: Giúp phục hồi tự động khỏi các lỗi server tạm thời (502, 503, 504) và lỗi kết nối ban đầu, duy trì Tính Sẵn dùng trong các tình huống mạng chập chờn.
Hạn chế: Chỉ có thể thử lại **một lần** (total=1). Nếu API sập hẳn, cơ chế này không giúp ích được.

Vấn đề sẵn sàng:

API có thể bị DDoS

Ứng dụng phụ thuộc hoàn toàn vào blockchain availability

* Các Tính năng có tích hợp Blockchain *

1. Tính năng thưởng token điểm danh hằng ngày.

Đăng nhập mỗi ngày sẽ nhận được 5 token miễn phí bằng hàm mint trong contract.

Bảng users có trường last_checkin: DATE dùng để kiểm tra lần cuối người dùng đăng nhập và được UPDATE mỗi khi người dùng bấm "Điểm danh"

Backend của trang web PEPE sẽ gọi hàm mint viết ở trong smart contract và gửi post request tới api hscoin, cấp 5 token cho ví hscoin đã được liên kết của người dùng

2. Tính năng thưởng token khi người dùng mới được giới thiệu.

Người dùng mới khi tạo tài khoản có thể nhập tên người dùng của một người có sẵn trong database (trường username: TEXT trong bảng users).

Khi đăng kí thành công, người giới thiệu (đã liên kết với ví HSCoin) có thể nhấn nút "Nhận thưởng giới thiệu".

Web PEPE gọi hàm mint tới địa chỉ của tài khoản, cấp phát 50 token

3. Tính năng thưởng token khi người dùng trả lời đúng tất cả câu hỏi trong một bài kiểm tra.

Quy tắc: Người dùng A tạo ra một bài test, người dùng B lần đầu tiên làm bài test đó sẽ chuyển 1 token cho người dùng A để làm bài test, và ở những lần sau khi làm sẽ không phải trả phí.

Backend trang web PEPE sẽ gọi hàm transfer trong smart contract, hàm nhận 3 args là 2 địa chỉ người gửi người nhận, cùng với giá trị token sẽ chuyển.

Việc kiểm tra đây có phải lần đầu người dùng làm sẽ dựa vào trường attemp_number: INTEGER trong bảng test_submission

4. Tính năng thưởng token khi tạo ra câu hỏi trong ngân hàng câu hỏi.

Quy tắc: mỗi khi người dùng tạo một câu hỏi trong ngân hàng

câu hỏi thì người dùng đó sẽ nhận được 0.5 token.

Trang web PEPE sử dụng hàm mint, cấp 0.5 token cho ví hscoin của người dùng

Cấp token ngay khi xác nhận câu hỏi không vi phạm kiểm tra đầu vào và được thêm vào database bảng questions

Phần III.

ĐẢM BẢO KHÔNG THỂ CHỐI BỎ

(NON-REPUDIATION)

Nguyên tắc Ký số: Mọi giao dịch quan trọng (burn, transfer) đều phải được ký bằng Private Key của chính người dùng.

Bằng chứng Blockchain: Blockchain cung cấp bằng chứng **Không thể chối bỏ**. Khi giao dịch được xác thực và ghi vào sổ cái, nó không thể bị thay đổi. Người dùng không thể phủ nhận việc mình đã gửi Token, vì chỉ có Private Key của họ mới có thể tạo ra chữ ký số hợp lệ cho giao dịch đó.

ABI Encoding: Các tham số giao dịch được đóng gói bằng **ABI Encoding** (encode_input_data) trước khi gửi, đảm bảo nội dung chính xác của lệnh gọi hàm (ví dụ: burn(amount)) được chuyển đến hợp đồng thông minh.

Phần IV.

ĐÁNH GIÁ RỦI RO VÀ BIỆN PHÁP KHẮC PHỤC

Rủi ro (Risk)	Phân tích Nguy cơ	Điểm yếu trong Mã nguồn	Khuyến nghị Khắc phục (Mitigation)
Tấn công Man-in-the-Middle	Mặc dù giao dịch được ký số, kênh truyền giữa Backend và API Blockchain (HSCOIN_API_BASE_URL) vẫn có thể bị tấn công.	Giao tiếp qua HTTPS/TLS giúp giảm thiểu rủi ro, nhưng cần kiểm tra tính xác thực API bằng HSCOIN_API_KEY.	Đảm bảo kết nối chỉ dùng HTTPS và kiểm tra chứng chỉ nghiêm ngặt.
Lỗi nghiệp vụ Nạp Coin	Nếu số Token trên ví người dùng không đủ, giao dịch burn sẽ thất bại.	Hàm user_burn_tokens có kiểm tra balance và trả về lỗi Insufficient balance trước khi gửi lệnh lên chuỗi.	Logic đã tồn tại, cần đảm bảo hàm kiểm tra số dư luôn chính xác.

LỜI CẢM ƠN

“Lời cuối cùng, nhóm chúng em xin được gửi lời cảm ơn chân thành đến Giảng viên Đỗ Xuân Chợ – người đã trực tiếp giảng dạy và hướng dẫn chúng em trong bộ môn Cơ sở An toàn thông tin.

Đối với chúng em, môn học này không chỉ mang lại những kiến thức lý thuyết về bảo mật, mã hóa hay an ninh mạng, mà còn rèn luyện cho chúng em tư duy cẩn trọng và cái nhìn đa chiều trước các vấn đề công nghệ. Đặc biệt, sự nhiệt tình và những chia sẻ thực tế của thầy đã tiếp thêm động lực rất lớn để nhóm mạnh dạn lựa chọn và triển khai đề tài phân tích an toàn cho hệ thống PEPE.

Quá trình thực hiện báo cáo cũng là khoảng thời gian quý báu để chúng em tự đánh giá lại năng lực và củng cố kiến thức. Nhóm rất mong nhận được sự chỉ bảo của thầy để khắc phục những hạn chế còn tồn tại trong bài làm.

Chúng em xin gửi đến thầy lời chúc sức khỏe và lời cảm ơn sâu sắc nhất!”