ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO TIẾN ĐỘ

MÔN HỌC: MẬT MÃ HỌC

Đề tài: Ứng dụng Zero Knowledge Proofs và thuật toán hậu lượng tử (Post Quantum Cryptography) vào việc bảo vệ tài sản và xác minh danh tính trong mạng Blockchain liên ngân hàng

Giảng viên hướng dẫn: TS. Nguyễn Ngọc Tự

Lớp: NT219.Q12.ANTT

Sinh viên thực hiện: Nguyễn Hoàng Quý – 24521494
Huỳnh Nhật Duy – 24520375

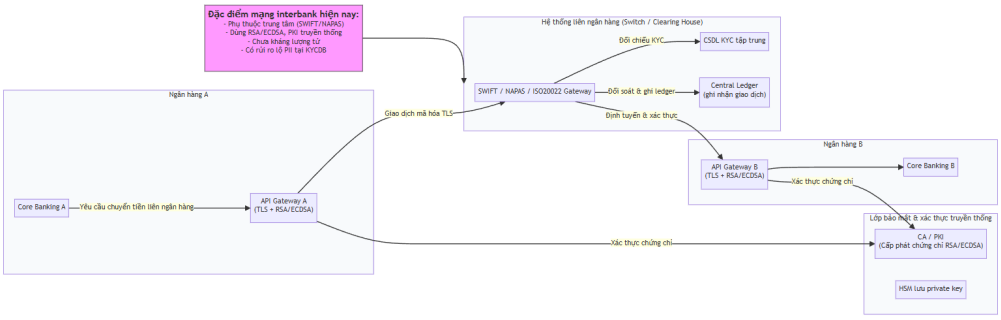
Thành phố Hồ Chí Minh, tháng 09 năm 2025

Mục lục

1 Ngữ cảnh (Context)

Công nghệ **Blockchain** đã trở thành nền tảng quan trọng trong lĩnh vực tài chính, đặc biệt là đối với các hệ thống ngân hàng và liên ngân hàng, nhờ vào các đặc tính nổi bật như *tính minh bạch*, *toàn vẹn dữ liệu* và *phi tập trung*. Tuy nhiên, sự phát triển nhanh chóng của **máy tính lượng tử** [**?**] đang đặt ra thách thức lớn đối với các thuật toán mật mã hiện hành như **RSA** và **ECDSA**. Những thuật toán này có thể bị phá vỡ khi năng lực tính toán lượng tử đạt đến ngưỡng nhất định, dẫn đến nhu cầu cấp thiết trong việc nghiên cứu và triển khai các **thuật toán mật mã hậu lượng tử (PQC)** để đảm bảo an toàn cho các giao dịch trên blockchain.

Bên cạnh mối đe dọa từ máy tính lượng tử, các quy trình nghiệp vụ truyền thống trong ngân hàng, chẳng hạn như *rút tiền* hay *sao kê tài khoản*, vẫn còn phức tạp và tiềm ẩn nhiều rủi ro bảo mật. Cụ thể, khách hàng thường phải cung cấp các giấy tờ định danh như **CCCD** hoặc **hộ chiếu** trong mỗi giao dịch, làm tăng nguy cơ **lộ lọt thông tin cá nhân**. Điều này không chỉ ảnh hưởng đến quyền riêng tư của người dùng mà còn có thể dẫn đến việc **kẻ tấn công lợi dụng dữ liệu bị rò rỉ để tạo và ghi nhận các giao dịch giả mạo** trong hệ thống.



Hình 1: Quy trình giao dịch của mạng liên ngân hàng hiện nay

Trước thực tế đó, nhu cầu đặt ra là phải xây dựng một giải pháp vừa có khả năng **kháng lượng tử** để bảo vệ an toàn cho hệ thống, vừa **tăng cường quyền riêng tư và tính xác thực của giao dịch**. Giải pháp này sẽ góp phần củng cố niềm tin của khách hàng, đồng thời thúc đẩy quá trình chuyển đổi số an toàn trong lĩnh vực ngân hàng và liên ngân hàng.

2 Tài sản cần bảo vệ (Assets to Protect)

2.1 Dữ liệu khách hàng (Customer Data)

Tài sản quan trọng nhất là dữ liệu định danh cá nhân (PII) và dữ liệu tài chính nhạy cảm của khách hàng. Hệ thống phải bảo vệ các thông tin sau:

- **Thông tin định danh cá nhân (PII)**: Căn cước công dân (CCCD), hộ chiếu, email, số điện thoại.
- **Dữ liệu tài chính nhạy cảm**: Số dư tài khoản, chi tiết và lịch sử giao dịch, các thông tin liên quan đến nghiệp vụ ngân hàng.

Các dữ liệu này phải được bảo vệ khỏi mọi hành vi truy cập, đọc trộm hoặc sửa đổi trái phép, cả khi lưu trữ (at-rest) và khi truyền tải (in-transit).

2.2 Tính toàn vẹn và xác thực giao dịch (Transaction Integrity & Authenticity)

Tài sản ở đây là sự thật và tính bất biến của sổ cái (ledger). Hệ thống phải đảm bảo:

- **Tính xác thực (Authenticity)**: Mọi giao dịch trên blockchain phải được chứng minh xuất phát từ đúng chủ tài khoản thông qua chữ ký số hợp lệ.
- **Tính toàn vẹn (Integrity)**: Dữ liệu giao dịch đã xác nhận và ghi vào khối không thể bị thay đổi, chỉnh sửa hay xóa bỏ bởi bất kỳ bên thứ ba nào.

2.3 Thông tin bảo mật liên quan đến khóa (Key-related Security Information)

Khóa bí mật (private key) của ngân hàng là tài sản cốt lõi cho việc tạo chữ ký số và thực hiện giao dịch. Hệ thống phải đảm bảo:

- Khóa riêng không bị lộ hoặc bị phá bởi các cuộc tấn công cổ điển như dò tìm hay tấn công vét cạn.
- Khóa riêng phải **kháng lượng tử (quantum-resistant)**, nghĩa là không thể suy ra từ khóa công khai (public key) ngay cả khi kẻ tấn công sử dụng máy tính lượng tử (ví dụ thuật toán Shor).

3 Phân tích rủi ro bảo mật (Security Risk Analysis)

3.1 Tính an toàn của các loại mã hóa hiện đại trước máy tính lượng tử (Post-Quantum Vulnerabilities of Current Cryptography)

Các hệ thống blockchain hiện nay, bao gồm cả các ứng dụng trong ngân hàng, chủ yếu dựa vào thuật toán mật mã bất đối xứng như **RSA** (dùng trong một số hạ tầng PKI) và **ECDSA** (phổ biến trong Bitcoin và Ethereum) để tạo chữ ký số và xác thực giao dịch.

Các thuật toán này dựa trên độ khó của hai bài toán:

- **RSA**: Phân tích một số nguyên lớn ra thừa số nguyên tố.
- **ECDSA**: Logarit rời rạc trên đường cong elliptic (ECDLP).

Tuy nhiên, cả hai bài toán này có thể bị giải quyết hiệu quả bởi **thuật toán Shor** nếu sử dụng máy tính lượng tử đủ mạnh .Khi đó, kẻ tấn công có thể:

- **Phá khóa riêng (Private Key)**: Suy ngược từ khóa công khai (public key) để chiếm quyền kiểm soát tài khoản.
- **Giả mạo giao dịch**: Tạo và ký các giao dịch giả mạo.
- **Phá vỡ tính toàn vẹn của chuỗi**: Thay đổi lịch sử giao dịch và ký lại các khối.

3.2 Rủi ro lộ thông tin cá nhân trong quá trình giao dịch (Personal Data Leakage Risks During Transactions)

Các quy trình ngân hàng, ngay cả khi số hóa, vẫn yêu cầu khách hàng cung cấp thông tin định danh nhạy cảm (PII) như **CCCD** hoặc **hộ chiếu** để thực hiện KYC (Know Your Customer).

Rủi ro gồm:

- **Tập trung hóa dữ liệu**: Dữ liệu PII lưu trong cơ sở dữ liệu tập trung, nếu bị tấn công sẽ dẫn tới rò rỉ thông tin.
- **Lạm dụng thông tin**: Kẻ tấn công có thể mạo danh khách hàng và thực hiện giao dịch gian lận (thực hiện lại các giao dịch đã được xác minh hợp lệ - thực hiện một giao dịch nhiều lần).

- **Thiếu quyền riêng tư**: Khách hàng phải tiết lộ toàn bộ thông tin cá nhân, ngay cả khi chỉ cần xác thực một thuộc tính đơn lẻ.

3.3 Rủi ro về quyền riêng tư trên sổ cái (On-chain Privacy Risks)

Bản chất blockchain là **minh bạch**. Mặc dù các địa chỉ ví thường là giả danh, nhưng khi liên kết với danh tính thực (qua KYC hoặc phân tích dữ liệu), toàn bộ hoạt động tài chính của khách hàng (số dư, lịch sử giao dịch, đối tác giao dịch) đều có thể bị theo dõi, gây vi phạm quyền riêng tư tài chính.

4 Mục tiêu bảo mật (Security Objectives)

4.1 Xác minh giao dịch (Transaction Validity)

Mọi giao dịch phải được kiểm tra bởi các node với các yêu cầu sau:

- **Xác thực chữ ký**: Chữ ký của giao dịch phải hợp lệ và được tạo từ khóa riêng tương ứng với địa chỉ người gửi. Trong môi trường hậu lượng tử, chữ ký này được tạo bằng **PQC Dilithium** để chống giả mạo từ các kẻ tấn công lượng tử.
- **Kiểm tra số dư**: Người gửi phải có đủ số dư để thực hiện giao dịch.
- **Ngăn chặn chi tiêu lặp (Double-Spending)**: Mỗi giao dịch được gán một **nonce** duy nhất cho tài khoản gửi. Node từ chối các giao dịch có cùng nonce đã được sử dụng, đảm bảo cùng một lượng tài sản không thể chi tiêu nhiều lần.
- **Chống tấn công phát lại (Replay Attack)**: Giao dịch từ một mạng lưới không thể được gửi lại trên mạng lưới khác hoặc lặp lại trên cùng mạng nhờ kiểm tra **nonce** và chữ ký. Node xác minh tính duy nhất của nonce kết hợp với địa chỉ người gửi để từ chối các giao dịch lặp lại.

4.2 Tính bất biến của sổ cái (Immutable Ledger)

Các giao dịch sau khi xác minh sẽ được ghi vào các khối (blocks). Các khối được liên kết bằng **cryptographic hashes** tạo thành chuỗi (ledger) không thể thay đổi.

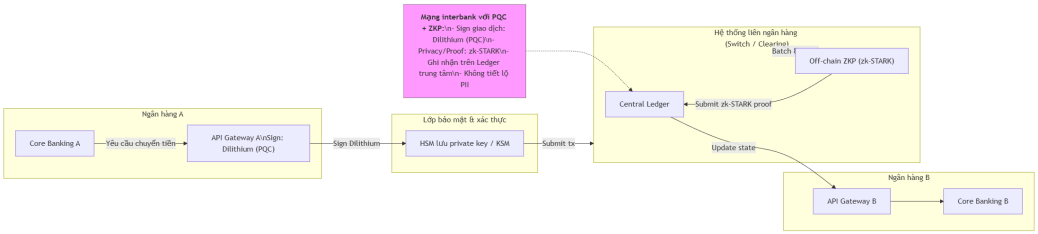
- Thay đổi dữ liệu trong khối cũ sẽ làm sai giá trị hash và phá vỡ toàn bộ chuỗi.
- **ZKP ZSTARKs** được áp dụng để bảo vệ quyền riêng tư trên blockchain: các node có thể xác minh tính hợp lệ của giao dịch mà không cần tiết lộ các thông tin nhạy cảm (số tiền, địa chỉ người gửi/nhận).

4.3 Kháng tấn công lượng tử (Quantum Resistance)

- Hệ thống sử dụng các thuật toán mật mã hậu lượng tử (**PQC**), ví dụ **Dilithium**, để tạo chữ ký số, đảm bảo rằng các giao dịch vẫn an toàn ngay cả trước máy tính lượng tử.
- Khóa riêng được tạo, lưu trữ và trao đổi bằng cơ chế kháng lượng tử.

4.4 Tăng cường quyền riêng tư và ẩn danh tính (Enhanced Privacy & Anonymity)

- **Xác thực không tiết lộ thông tin (ZKP)**: Khách hàng chứng minh quyền sở hữu tài khoản hoặc đáp ứng điều kiện KYC mà không tiết lộ CCCD hay các PII.
- **Bảo mật giao dịch trên chuỗi**: Áp dụng **ZSTARKs** để che giấu chi tiết nhạy cảm của giao dịch (số tiền, địa chỉ người nhận) trong khi vẫn cho phép xác thực hợp lệ.



Hình 2: Kiến trúc hướng tới

5 Kiến trúc giải pháp (Solution Architecture)

Kiến trúc tổng thể của hệ thống được thiết kế để tích hợp chữ ký hậu lượng tử (**PQC**) và bằng chứng không tiết lộ kiến thức (**ZKP**) vào một mạng lưới consortium blockchain. Giải pháp được chia thành ba luồng (track) hoạt động song song:

5.1 Track A: Luồng chữ ký PQC (PQC Signatures)

1. **Wallet (Ví)**: Người dùng (khách hàng hoặc ngân hàng) khởi tạo giao dịch.

2. **Ký giao dịch**: Giao dịch được gửi đến **KSM (Key Simulation Module)**, mô phỏng HSM phần mềm, sử dụng thuật toán **Dilithium** để tạo chữ ký PQC.

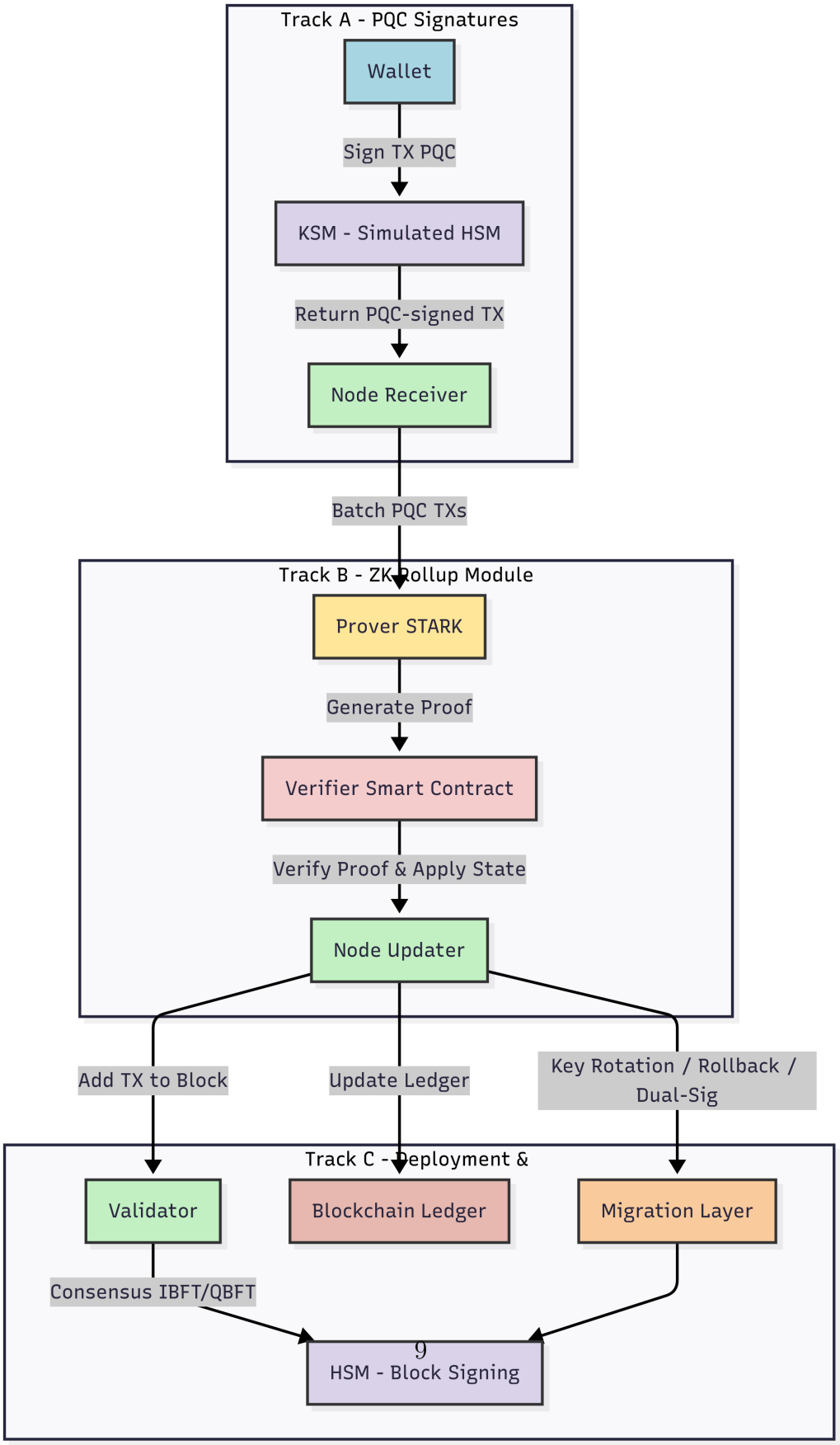
3. **Node Receiver**: Tiếp nhận các giao dịch đã ký PQC và đưa vào mempool chờ xử lý.

5.2 Track B: Luồng ZK-Rollup (ZK-Rollup Module)

1. **Batching**: Các giao dịch PQC từ Track A được gom lại thành một batch.
2. **Prover (Off-chain)**: Sinh **zk-STARK proof** cho toàn bộ batch bằng thư viện Winterfell mà không tiết lộ chi tiết giao dịch.
3. **Verifier Contract (On-chain)**: Nhận proof, xác minh và cập nhật trạng thái mới trên sổ cái nếu proof hợp lệ.

5.3 Track C: Luồng Tích hợp & Đồng thuận (Deployment & Consensus)

1. **Node Updater**: Ghi nhận trạng thái mới đã được verifier xác nhận vào ledger.
2. **Consensus**: Các Validator trong mạng consortium (IBFT2/QBFT) đạt đồng thuận về khối mới. Khối cũng được ký bằng khóa PQC từ KSM.
3. **Migration Layer**: Quản lý crypto-agility, cho phép quay vòng khóa (key rotation) hoặc chạy song song hai cơ chế (dual-sig).



Hình 3: WorkFlow

6 Môi trường và triển khai (Deployment)

6.1 Hạ tầng mạng và hệ điều hành (Network Infrastructure & OS)

- Hệ điều hành: Ubuntu 24.04 LTS cho tất cả các node (Validator, Prover, Node).
- Mô hình mạng: Consortium private blockchain (các ngân hàng thành viên vận hành node riêng).
- Bảo mật kênh truyền: Kết nối giữa các node được bảo vệ bằng mTLS; toàn bộ payload và proof mã hóa bằng AES-GCM trong TLS 1.3.

6.2 Các thành phần triển khai (Deployment Components)

- **Blockchain Core**: Hyperledger Besu (tương thích EVM), cơ chế đồng thuận IBFT2 hoặc QBFT.
- **Wallet**: Tạo giao dịch và gọi KSM để ký PQC (Dilithium).
- **KSM**: Mô phỏng HSM để sinh, lưu trữ an toàn và ký giao dịch bằng khóa PQC, hỗ trợ key rotation và dual-sig.
- **Prover (Off-chain)**: Gom batch giao dịch PQC và sinh zk-STARK proof (thư viện Winterfell).
- **Verifier (On-chain)**: Smart contract nhận và xác minh proof, cập nhật trạng thái ledger.

6.3 Kế hoạch thực thi và kiểm thử (Implementation & Testing Plan)

- **Tuần 1-4**: Xây dựng prototype PQC và ZKP; tích hợp ký/xác minh Dilithium trong ví và node; triển khai Verifier Contract mẫu.
- **Tuần 5-6**: Phát triển KSM nâng cao, hoàn thiện Verifier Contract, cơ chế replay protection, key rotation.
- **Tuần 7-10**: Tích hợp toàn bộ 3 luồng, kiểm thử cơ chế đồng thuận IBFT/QBFT, đánh giá bảo mật.

6.4 Kiểm thử (Testing Plan)

- **Hiệu năng**: Đo Tx size, CPU cost cho PQC; Proof generation time, Proof size và Verifier cost cho ZKP; End-to-end latency và TPS cho toàn hệ thống.
- **Bảo mật**: Đảm bảo chữ ký PQC và zk-STARK proof không hợp lệ bị từ chối; replay protection hoạt động; kiểm tra crypto-agility và key rotation.

7 Đánh giá định lượng (Evaluation Plan)

Nhóm đánh giá hệ thống triển khai dựa trên các tiêu chí sau:

- **E-Crypto:** Thử proof/chữ ký sai $\rightarrow$ bị từ chối 100%.
- **E-AuthN:** Thử ký sai khóa $\rightarrow$ bị từ chối; success $\geq$ 99%.
- **E-AuthZ:** Node không có quyền ghi ledger $\rightarrow$ bị deny 100%.
- **E-Cross:** Đo thời gian rotation khóa PQC (target $\leq$ 10 phút).