NDAChain

WHITEPAPER

Empowering Vietnam's Digital Future with Hybrid Decentralized Identity (Hybrid DID) System

2025

Mục lục

Cáo bạch NDAChain

Khai phóng Kỷ nguyên số của Việt Nam với Hệ thống Định danh Phi tập trung Lai (Hybrid DID)

Tóm tắt

Trong bối cảnh Việt Nam đẩy nhanh quá trình chuyển đổi số, nhu cầu về một hệ thống định danh số an toàn, có khả năng mở rộng và bảo vệ quyền riêng tư ngày càng trở nên cấp thiết. Hạ tầng định danh tập trung hiện tại, dù mang tính thẩm quyền cao, vẫn tồn tại những hạn chế về bảo mật, khả năng mở rộng và tính tương thích toàn cầu. NDAChain giới thiệu giải pháp Hệ Thống Định Danh Phi Tập Trung Lai (Hybrid DID), tận dụng công nghệ blockchain để nâng cấp khung định danh quốc gia. Bằng cách tích hợp mạng blockchain được kiểm soát (permissioned blockchain) với cơ sở dữ liệu quốc gia tập trung, NDAChain cho phép công dân kiểm soát dữ liệu cá nhân, tăng cường bảo mật và hỗ trợ các tương tác xuyên biên giới một cách liền mạch. Tài liệu này cung cấp cái nhìn chi tiết về NDAChain, bao gồm kiến trúc kỹ thuật, thông số giao thức, cơ chế đồng thuận, tiêu chí đánh giá hiệu năng, và sự tuân thủ các tiêu chuẩn quốc tế.

1. Giới thiệu

1.1. Bối cảnh và động lực

Sự phát triển kinh tế vượt bậc cùng quá trình chuyển đổi số của Việt Nam đòi hỏi một hạ tầng định danh số vững chắc. Hiện tại, Trung tâm Dữ liệu Quốc gia (NDC) quản lý hệ thống định danh tập trung cho hơn 100 triệu công dân, đóng vai trò nền tảng xác thực danh tính trong nhiều lĩnh vực. Tuy nhiên, tính chất tập trung của hệ thống này đặt ra các thách thức về bảo mật, quyền riêng tư, khả năng mở rộng và tính tương thích quốc tế.

1.2. Thách thức về hệ thống quản lý định danh số hiện tại

Hệ thống định danh số hiện tại đối mặt với các vấn đề chính sau:

- Rủi ro bảo mật: Lưu trữ dữ liệu tập trung tạo ra một điểm yếu duy nhất, làm tăng nguy cơ bị xâm phạm dữ liệu.
- Hạn chế về khả năng mở rộng: Hạ tầng hiện tại có thể không đáp ứng được nhu cầu ngày càng tăng của các dịch vụ số hóa.
- Hạn chế về tính tương thích toàn cầu: Thiếu sự đồng bộ với các tiêu chuẩn quốc tế gây cản trở cho các giao dịch xuyên biên giới.
- Quyền kiểm soát hạn chế của công dân: Công dân không có công cụ để kiểm soát dữ liệu cá nhân và cách thức dữ liệu được chia sẻ.

1.3. Hạn chế của những giải pháp hiện có

Hiện nay, một số giải pháp định danh đã tồn tại, nhưng chưa đáp ứng được yêu cầu cân bằng giữa mức độ tin tưởng của người dùng, quyền riêng tư, khả năng mở rộng và đáp ứng các tiêu chuẩn quốc tế:

- Hệ thống tập trung: Đảm bảo tính thẩm quyền nhưng yếu về bảo mật và khả năng mở rộng.
- Hệ thống liên kết: Phụ thuộc bên cung cấp thứ ba, gây lo ngại về chủ quyền dữ liệu.
- Định danh tự chủ (SSI): Trao quyền kiểm soát cho người dùng nhưng thiếu sự xác thực từ cơ quan có thẩm quyền và khả năng tuân thủ quy định.

1.4. Nhu cầu về NDAChain

NDAChain được phát triển với mục tiêu:

- Kết hợp hệ thống định danh tập trung với xác thực phi tập trung.
- Tăng cường bảo mật và quyền riêng tư thông qua các kỹ thuật mã hóa tiên tiến.
- Đảm bảo khả năng mở rộng hiệu quả để triển khai trên quy mô quốc gia.
- Tuân thủ các tiêu chuẩn toàn cầu để hỗ trợ tính tương thích quốc tế.
- Trao quyền cho công dân kiểm soát dữ liệu cá nhân của mình.

---

2. Tầm nhìn và Mục tiêu

2.1. Tăng cường bảo mật và quyền riêng tư

- Mã hóa tiên tiến: Triển khai các giao thức mã hóa mạnh mẽ.
- Xác thực phân tán: Giảm thiểu rủi ro liên quan đến hệ thống tập trung.

2.2. Trao quyền cho công dân

- Quyền sở hữu dữ liệu: Công dân có toàn quyền sở hữu và kiểm soát dữ liệu định danh của mình.
- Chia sẻ có chọn lọc: Sử dụng Bằng chứng không tri thức (Zero-Knowledge Proof) để chỉ chia sẻ chỉ những thông tin cần thiết.

2.3. Đạt được khả năng mở rộng hiệu quả

- Sự đồng thuận hiệu quả: Sử dụng thuật toán đồng thuận Bằng chứng quyền hạn (Proof of Authority) để đạt được thông lượng cao.
- Kiến trúc mô-đun: Cho phép mở rộng độc lập các thành phần của hệ thống.

2.4. Hỗ trợ tương thích toàn cầu

- Tuân thủ tiêu chuẩn: Tuân thủ tiêu chuẩn W3C về định danh phi tập trung (DID) và chứng chỉ có thể xác minh (Verifiable Credentials)

- Nhận diện xuyên biên giới: Hỗ trợ sử dụng định danh số trên phạm vi quốc tế.

2.5. Đảm bảo tuân thủ quy định

- Quy định quốc gia: Tuân thủ các luật bảo vệ dữ liệu của Việt Nam.
- Quy định quốc tế: Phù hợp với GDPR và các tiêu chuẩn toàn cầu khác.

---

3. Giải pháp NDAChain

3.1. Tổng quan về hệ thống định danh phi tập trung lai (Hybrid DID)

NDAChain tích hợp một mạng blockchain được kiểm soát (permissioned blockchain) với cơ sở dữ liệu quốc gia để tạo ra một hệ thống định danh phi tập trung lai (Hybrid DID):

- Định danh tập trung: Cơ sở dữ liệu quốc gia vẫn là nguồn thông tin chính thức.
- Xác thực định danh phi tập trung: Blockchain cho phép thực hiện các hoạt động định danh an toàn và phi tập trung.
- Trao quyền cho người dùng: Công dân quản lý định danh của mình thông qua ví định danh phi tập trung (DID Wallet).

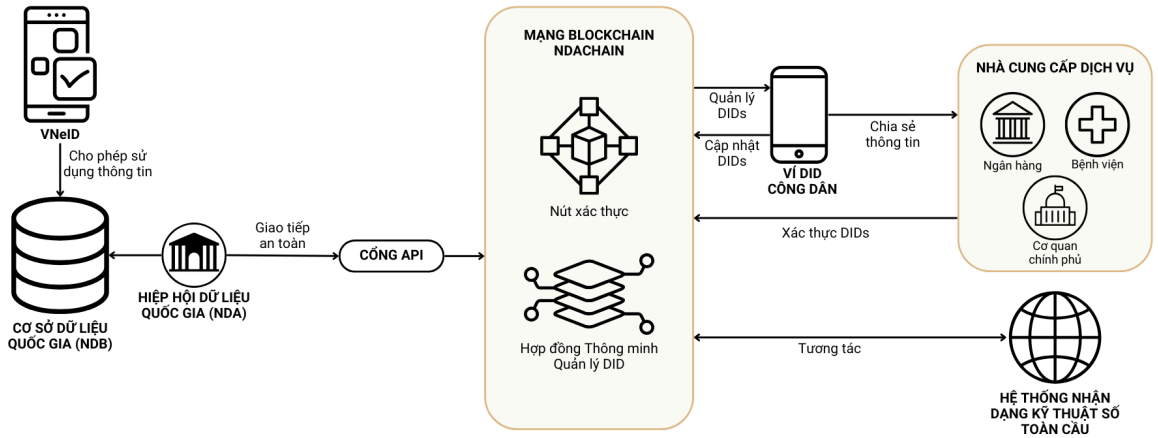
3.2. Các thành phần chính

1. Mạng blockchain được kiểm soát (Hyperledger Besu)
2. Nút xác thực và quản trị
3. Lớp quản lý định danh phi tập trung (DID) và hợp đồng thông minh
4. Tích hợp cổng API
5. Ví định danh phi tập trung (DID) của công dân

---

4. Kiến trúc Kỹ thuật và Thông số Giao thức

4.1. Kiến trúc hệ thống



Hình 1: Kiến trúc Hệ thống Chi tiết của NDAChain

Kiến trúc hệ thống bao gồm:

- VNeID: Ứng dụng có quyền truy cập vào cơ sở dữ liệu quốc gia và lấy sự đồng ý của công dân trước khi sử dụng dữ liệu của họ.
- Cơ sở dữ liệu quốc gia (NDB): Kho lưu trữ tập trung chứa dữ liệu định danh đã được xác minh.
- Hiệp hội Dữ liệu Quốc gia (NDA): Cơ quan chính phủ quản lý việc truyền dữ liệu từ NDB sang blockchain.
- Cổng API (APIG): Giao diện giữa NDA và blockchain, đảm bảo việc giao tiếp được thực hiện an toàn.
- Mạng blockchain NDAChain:
    - Nút xác thực (VNs): Các nút chịu trách nhiệm xác thực giao dịch.
    - Hợp đồng thông minh quản lý định danh (DIDSC): Xử lý các hoạt động liên quan đến đinh danh phi tập trung.
- Ví định danh phi tập trung công dân (CDW): Ứng dụng cho phép công dân quản lý định danh.
- Nhà cung cấp dịch vụ (SPs): Các tổ chức yêu cầu xác minh danh tính.

4.2. Cấu trúc dữ liệu và thuật toán

4.2.1. Cấu trúc dữ liệu

- Định danh phi tập trung (DID):

```
{
  "id": "did:pila:123456789abcdefghi",
  "publicKey": [ ... ],
  "authentication": [ ... ],
  "service": [ ... ],
  "created": "2023-01-01T00:00:00Z",
  "updated": "2023-01-01T00:00:00Z"
}
```

- Chứng chỉ có thể xác minh (VC):

```
{
  "@context": [ "https://www.w3.org/2018/credentials/v1" ],
  "id": "credential-id",
  "type": [ "VerifiableCredential", "IdentityCredential" ],
  "issuer": "did:pila:issuer-id",
```

```
  "issuanceDate": "2023-01-01T00:00:00Z",
  "credentialSubject": {
    "id": "did:pila:subject-id",
    "attributes": { ... }
  },
  "proof": { ... }
}
```

4.2.2. Thuật toán

- Thuật toán tạo định danh phi tập trung (DID):
    1. Đầu vào: Dữ liệu đăng ký người dùng từ NDB.
    2. Quá trình:
        - Tạo một DID duy nhất bằng cách sử dụng hàm băm mã hóa của khóa công khai của người dùng và các định danh khác.
        - Lưu trữ tài liệu DID trên blockchain thông qua hợp đồng thông minh.
    3. Đầu ra: DID được gán cho người dùng.
- Tạo Bằng chứng không tri thức (Sử dụng zk-SNARKs):
    1. Đầu vào: Các trường thông tin của người dùng cần được xác thực.
    2. Quá trình:
        - Tạo một bằng chứng zk-SNARK xác thực các trường thông tin nhạy cảm không thể tiết lộ.
    3. Đầu ra: Bằng chứng không tri thức (ZKP) được gửi đến người xác minh.

4.3. Cơ chế đồng thuận: Bằng chứng quyền hạn (PoA)

4.3.1. Lý do và so sánh

- Ưu điểm của PoA:
    - Hiệu suất: Độ trễ thấp hơn và thông lượng cao hơn so với Bằng chứng công việc (Proof of Work - PoW).
    - Tiêu thụ năng lượng: tiết kiệm năng lượng đáng kể so với PoW.
    - Kiểm soát: Cho phép quản lý tập hợp các nút xác thực, phù hợp với các yêu cầu quy định.
- So sánh với các cơ chế khác:
    - Bằng chứng cổ phần (Proof of Stake - PoS): Mặc dù PoS mang tính phi tập trung, nhưng không cung cấp mức kiểm soát cần thiết để tuân thủ quy định.
    - Bằng chứng cổ phần được ủy quyền (Delegated PoS - DPoS): Gây phức tạp trong quản trị và tiềm ẩn rủi ro tập trung hóa.

4.3.2. Hoạt động kỹ thuật

- Lựa chọn nút xác thực:
    - Tiêu chí: Tuân thủ các tiêu chuẩn bảo mật, độ tin cậy và năng lực vận hành.
    - Quy trình tham gia: Các nút xác thực được thêm vào thông qua hợp đồng thông minh đa chữ ký, yêu cầu sự chấp thuận từ các nút xác thực hiện có.
- Sản xuất khối:
    - Các nút xác thực luân phiên sản xuất các khối theo hình thức vòng tròn.
    - Thuật toán:

```
Đối với mỗi khối có độ cao h:
    Nút xác thực V_i = V_h mod N
    V_i đề xuất khối B_h
    Các nút xác thực khác thực hiện xác thực B_h
    Nếu B_h hợp lệ, thêm vào blockchain
```

- Quy trình đồng thuận:
    - Điều kiện bình thường: Các nút xác thực tuân theo giao thức, và các khối được xác nhận nhanh chóng.
    - Điều kiện Byzantine: Nếu một nút xác thực có hoạt động sai lệch, khối sẽ bị từ chối bởi các nút khác.
- Khả năng chịu lỗi:
    - Mạng có thể chịu được tối đa (N-1)/3 nút xác thực lỗi.
    - Triển khai cơ chế phạt hoặc loại bỏ các nút xác thực sai lệch.

4.4. Quản lý định danh phi tập trung và hợp đồng thông minh

- Hợp đồng đăng ký định danh phi tập trung:
    - Chức năng:
        - `registerDID(didDocument)`
        - `updateDID(didDocument)`
        - `revokeDID(did)`
- Biện pháp bảo mật:
    - Kiểm soát truy cập dựa trên vai trò.
    - Xác minh đầu vào để ngăn chặn tấn công tiêm mã.

4.5. Triển khai Bằng chứng không tri thức

- Giao thức ZKP:
    1. Phân loại: zk-SNARKs (Bằng chứng không tri thức ngắn gọn, không tương tác về kiến thức)

2. Các đặc tính:
    - Tính đầy đủ: Các bằng chứng đúng luôn được chấp nhận.
    - Tính hợp lệ: Các bằng chứng sai bị từ chối.
    - Không tiết lộ: Không có thông tin nào về dữ liệu gốc được tiết lộ.

- Các bước triển khai:
    1. Thiết lập: Tạo các tham số công khai (thiết lập tin cậy).
    2. Bằng chứng: Người dùng tạo bằng chứng cho một tuyên bố (ví dụ: tuổi trên 18).
    3. Xác thực: Bên xác thực kiểm tra bằng chứng bằng cách sử dụng các tham số công khai.

4.6. Tích hợp với các hệ thống hiện có

- Thông số kỹ thuật cổng API:
    - Giao thức: API RESTful với mã hóa TLS.
    - Xác thực: OAuth 2.0 với mã thông báo JWT.
    - Điểm cuối:
        - `/register`: Để đăng ký định danh mới.
        - `/update`: Để cập nhật các trường thông tin định danh.
        - `/revoke`: Để thu hồi định danh.
- Đồng bộ dữ liệu:
    - Cập nhật theo thời gian thực thông qua kiến trúc dựa trên sự kiện.
    - Sử dụng hàng đợi tin nhắn để đảm bảo độ tin cậy.

---

5. Phân tích Bảo mật

5.1. Các mối đe dọa

- Tấn công từ bên ngoài: Cố gắng truy cập trái phép vào dữ liệu hoặc làm gián đoạn hoạt động của mạng.
- Tấn công nội bộ: Nút xác thực sai lệch hoặc người trong cuộc làm tổn hại tính toàn vẹn hệ thống.
- Các đe dọa về quyền riêng tư: Liên kết trái phép định danh người dùng hoặc các thông tin bị tiết lộ.

5.2. Các thuộc tính bảo mật

- Bảo mật: Được đảm bảo thông qua mã hóa và Bằng chứng không tri thức (ZKPs).
- Tính toàn vẹn: Được bảo vệ bởi tính bất biến của blockchain và cơ chế đồng thuận.

- Tính khả dụng: Đạt được nhờ sự mạng dự phòng và khả năng chịu lỗi.
- Không thể phủ nhận: Các giao dịch được ký và có thể xác minh.

5.3. Các phương pháp xác thực chính thức

- Xác thực hợp đồng thông minh:
    - Sử dụng các phương pháp chính thức như TLA+ hoặc Isabelle/HOL để xác minh tính chính xác của hợp đồng.
    - Kiểm tra mô hình để phát hiện lỗi logic.
- Xác thực giao thức:
    - Phân tích giao thức bảo mật:
        - Xác minh các trường thông tin nhạy cảm cần giữ bí mật bằng cách sử dụng các công cụ như ProVerif.
- Xác thực tuân thủ:
    - Kiểm soát định kỳ để đảm bảo tuân thủ các tiêu chuẩn và quy định.

---

6. Đánh giá Hiệu suất

6.1. Thông lượng giao dịch và độ trễ

- Môi trường kiểm thử:
    - Nút xác thực: 5 nút với cấu hình phần cứng khuyến nghị.
    - Nút hoàn chỉnh: 5 nút với cấu hình phần cứng khuyến nghị.
    - Điều kiện mạng: Độ trễ mô phỏng 50ms giữa các nút.
- Kết quả:
    - Thông lượng: Đạt trung bình 1,200 giao dịch mỗi giây (TPS).
    - Độ trễ: Thời gian xác nhận giao dịch trung bình là 1.5 giây.

6.2. Kiểm tra khả năng mở rộng

- Mở rộng tuyến tính:
    - Tăng số lượng nút xác thực từ 10 lên 50.
    - Quan sát sự gia tăng tỷ lệ thuận trong năng lực mạng.
- Kiểm tra tải trọng:
    - Mô phỏng tải đỉnh với 10,000 giao dịch đồng thời.
    - Hệ thống duy trì 95% thời gian hoạt động với sự suy giảm hiệu suất nhỏ.

6.3. Phân tích so sánh

- So với Ethereum (PoW):

    - TPS của Ethereum: Khoảng 15 TPS.
    - TPS của NDAChain: ~1,200 TPS, cao hơn đáng kể nhờ Bằng chứng quyền hạn (PoA) và mạng blockchain được kiểm soát (permissioned blockchain).
- So với Hyperledger Fabric:
    - TPS của Hyperledger Fabric: Lên đến 3,500 TPS trong điều kiện tối ưu.
    - TPS của NDAChain: Tương đương, với tiềm năng tối ưu hóa.

---

7. Trường hợp Sử dụng

7.1. Truy cập dịch vụ công

Kịch bản: Nguyễn, một cư dân Hà Nội, cần gia hạn giấy phép lái xe trực tuyến. Thông thường, quy trình này đòi hỏi nhiều lần đến các cơ quan chính phủ và giấy tờ phức tạp.

Quy trình với NDAChain:

1. Xác thực:
    - Nguyễn đăng nhập vào ứng dụng VNeID, đóng vai trò là ví DID, được bảo mật bằng xác thực sinh trắc học.
2. Chia sẻ có chọn lọc:
    - Thông qua ví DID, anh đồng ý chia sẻ các thông tin cần thiết (như chứng minh danh tính và thông tin giấy phép hiện tại).
    - Hệ thống tạo Bằng chứng không tri thức (ZKP) xác thực Nguyễn đủ điều kiện đăng ký mà không tiết lộ dữ liệu cá nhân.
3. Xác thực:
    - Hệ thống chính phủ xác thực ZKP qua NDAChain, xác nhận danh tính và điều kiện của Nguyễn.
    - Quá trình được ghi trên blockchain để kiểm soát.
4. Xử lý đơn:
    - Đơn được xử lý tự động, cập nhật tài liệu DID nếu cần.
5. Thông báo:
    - Nguyễn nhận thông báo số về giấy phép gia hạn. Thông tin này cũng được ghi nhận trong ví DID.

Lợi ích:

- Hiệu quả: Giảm thời gian xử lý từ vài ngày xuống còn vài phút.
- Quyền riêng tư: Bảo vệ dữ liệu cá nhân thông qua ZKPs.
- Khả năng kiểm toán: Cung cấp bản ghi bất biến của giao dịch.

7.2. Đơn giản hóa giao dịch tài chính

Kịch bản: Linh muốn vay vốn ngân hàng để khởi nghiệp kinh doanh nhỏ.

Quy trình với NDAChain:

1. Khởi đầu:
    - Linh truy cập cổng vay vốn trực tuyến của ngân hàng.
2. Xác thực danh tính:
    - Sử dụng ví DID để chia sẻ chứng chỉ cần thiết mà ngân hàng yêu cầu (như chứng minh danh tính và lịch sử tín dụng).
3. Sử dụng ZKP:
    - Tạo ZKPs chứng minh thu nhập và khả năng tín dụng mà không tiết lộ thông tin tài chính chi tiết.
4. Xác minh thời gian thực:
    - Ngân hàng xác thực các chứng chỉ và ZKPs qua NDAChain, đảm bảo tính toàn vẹn và xác thực của dữ liệu.
5. Phê duyệt khoản vay:
    - Sau khi xác minh thành công, ngân hàng nhanh chóng xử lý đơn xin vay.

Lợi ích:

- Tốc độ: Tăng tốc quá trình phê duyệt.
- Bảo mật dữ liệu: Các chi tiết tài chính nhạy cảm vẫn được giữ bí mật.
- Tin cậy: Xây dựng niềm tin vào tính xác thực của thông tin.

7.3. Tăng cường tương tác xuyên biên giới

Kịch bản: Thanh là một doanh nhân đang có kế hoạch mở rộng kinh doanh ra quốc tế và cần xác minh danh tính với đối tác nước ngoài.

Quy trình với NDAChain:

1. Trình bày chứng chỉ:
    - Thanh chia sẻ DID và các chứng chỉ liên quan với các đối tác quốc tế.
2. Tính tương tác:
    - NDAChain tuân thủ các tiêu chuẩn hệ thống định danh phi tập trung của W3C, cho phép đối tác xác minh qua hệ thống của họ.
3. Xác thực:
    - Đối tác xác minh tính xác thực của chứng chỉ qua các mạng lưới danh tính toàn cầu tương thích.
4. Giao dịch kinh doanh:
    - Thanh có thể tham gia an toàn vào các hợp đồng và giao dịch quốc tế.

Lợi ích:

- Công nhận toàn cầu: Tạo điều kiện cho các hoạt động kinh doanh xuyên biên giới.
- Bảo mật: Đảm bảo việc trao đổi danh tính an toàn và có thể xác thực được.
- Hiệu quả: Giảm thời gian và tài nguyên tiêu tốn cho việc xác thực danh tính.

7.4. Các trường hợp sử dụng bổ sung

7.4.1 Dịch vụ chăm sóc sức khỏe

Kịch bản: Minh, một bệnh nhân, cần chia sẻ hồ sơ y tế với bác sĩ mà vẫn giữ được quyền riêng tư.

Quy trình với NDAChain:

- Minh dùng ví DID tạo ZKPs xác nhận các thông tin cần thiết mà không tiết lộ toàn bộ lịch sử y tế.
- Bác sĩ xác thực thông tin qua NDAChain.

Lợi ích:

- Bảo vệ dữ liệu sức khỏe nhạy cảm.
- Tối ưu hóa quy trình tiếp nhận và tư vấn.

7.4.2 Xác thực bằng cấp học thuật

Kịch bản: Thảo, một sinh viên mới tốt nghiệp, nộp đơn xin việc và cần xác thực trình độ học vấn.

Quy trình với NDAChain:

- Thảo chia sẻ các chứng chỉ có thể xác minh về bằng cấp thông qua ví DID.
- Nhà tuyển dụng xác thực qua NDAChain, đảm bảo chúng không bị giả mạo.

Lợi ích:

- Ngăn chặn gian lận bằng cấp.
- Đơn giản hóa quy trình tuyển dụng.

---

8. Kế hoạch Triển khai

8.1. Chiến lược triển khai theo giai đoạn

Giai đoạn 1: Triển khai thí điểm

- Thời gian: Tháng 1-3
- Hoạt động kỹ thuật:
    - Thiết lập các nút xác thực ban đầu với tiêu chuẩn bảo mật cao.
    - Triển khai hợp đồng thông minh quản lý DID trên blockchain.

    - Phát triển và phân phối phiên bản beta của ví DID cho một nhóm kiểm soát.
    - Tích hợp cổng API với cơ sở dữ liệu quốc gia.
- Thiết lập hạ tầng:
    - Cấu hình môi trường mạng an toàn.
    - Thiết lập hệ thống giám sát và ghi log.
- Kết quả dự kiến:
    - Xác thực chức năng và bảo mật hệ thống.
    - Thu thập dữ liệu hiệu suất ban đầu.

Giai đoạn 2: Triển khai Khu vực

- Thời gian: Tháng 4-6
- Hoạt động kỹ thuật:
    - Mở rộng mạng lưới xác thực với các nút bổ sung.
    - Tối ưu hóa hợp đồng thông minh dựa trên phản hồi từ thí điểm.
    - Nâng cấp ví DID để cải thiện trải nghiệm người dùng.
- Cấu hình nút:
    - Triển khai cân bằng tải.
    - Đảm bảo tính dự phòng và khả năng sẵn sàng cao.
- Kết quả dự kiến:
    - Chứng minh khả năng mở rộng.
    - Tinh chỉnh hệ thống dựa trên mô hình sử dụng khu vực.

Giai đoạn 3: Triển khai toàn quốc

- Thời gian: Tháng 7-12
- Hoạt động kỹ thuật:
    - Thêm nhiều nút xác thực trên toàn quốc.
    - Tích hợp hoàn toàn với dịch vụ chính phủ và đối tác lớn trong khu vực tư nhân.
    - Triển khai biện pháp bảo mật tiên tiến, như HSM trên nút xác thực.
- Quản lý mạng:
    - Thiết lập trung tâm vận hành mạng quốc gia.
    - Triển khai quy trình phản ứng sự cố bảo mật toàn diện.
- Kết quả dự kiến:
    - Đạt được sự chấp nhận trên toàn quốc.
    - Thiết lập cấu trúc quản trị bền vững.

8.2. Kiểm tra và đảm bảo chất lượng

8.2.1. Kiểm tra chức năng

- Phạm vi:
    - Kiểm tra tất cả chức năng của hợp đồng thông minh.
    - Xác thực hoạt động của cổng API.
- Công cụ:
    - Sử dụng các framework kiểm tra như Truffle và Ganache cho hợp đồng thông minh.
    - Công cụ kiểm tra API tự động như Postman.

8.2.2. Kiểm tra hiệu suất

- Phạm vi: Đánh giá hệ thống dưới các điều kiện tải khác nhau.
- Công cụ: Công cụ kiểm tra tải như Apache JMeter.
- Chỉ số: TPS, độ trễ, mức sử dụng tài nguyên.

8.2.3. Kiểm tra bảo mật

- Phạm vi:
    - Kiểm tra xâm nhập trên các lớp mạng và ứng dụng.
    - Quét lỗ hổng của hợp đồng thông minh.
- Công cụ: Sử dụng các công cụ như Metasploit, Nessus và MythX để phân tích hợp đồng thông minh.

8.2.4. Kiểm tra chấp nhận người dùng (UAT)

- Phạm vi: Kiểm tra thực tế với người dùng cuối.
- Hoạt động: Thu thập phản hồi về tính khả dụng, hiệu suất và chức năng.
- Kết quả: Hoàn thiện giao diện cho người dùng và quy trình làm việc.

8.3. Chương trình nâng cao nhận thức và giáo dục cộng đồng

8.3.1. Chiến dịch giáo dục công dân

- Phương pháp:
    - Tạo nội dung giáo dục giải thích về NDAChain và những lợi ích của nó.
    - Tổ chức hội thảo trực tuyến và các buổi đào tạo.
    - Sử dụng các nền tảng mạng xã hội để mở rộng phạm vi tiếp cận.

8.3.2. Chương trình đào tạo nút xác thực

- Nội dung:
    - Đào tạo kỹ thuật về vận hành và bảo trì nút.

    - Thực hành các phương pháp bảo mật tốt nhất.
    - Yêu cầu về tuân thủ và quy định.

8.3.3. Hội thảo cho nhà cung cấp dịch vụ

- Mục tiêu:
    - Tạo điều kiện tích hợp với NDAChain.
    - Cung cấp tài nguyên và hỗ trợ kỹ thuật.
- Hoạt động:
    - Tổ chức các hội thảo thực hành.
    - Phát triển các bộ công cụ tích hợp và SDK.

8.4. Sự tham gia và hợp tác của các bên liên quan

- Cơ quan chính phủ:
    - Thiết lập các ủy ban liên ngành.
    - Đồng bộ hóa các chính sách và quy định.
- Đối tác khu vực tư nhân:
    - Hình thành quan hệ đối tác chiến lược.
    - Cùng phát triển các giải pháp tận dụng NDAChain.
- Cơ quan quản lý:
    - Tổ chức các cuộc tham vấn định kỳ.
    - Đảm bảo tuân thủ các quy định đang phát triển.
- Tổ chức quốc tế:
    - Tham gia các diễn đàn toàn cầu.
    - Đồng bộ hóa với các quy định thực hành quốc tế tốt nhất.

---

9. Triển vọng Tương lai và Lộ trình

9.1. Mở rộng mạng lưới xác thực

- Mục tiêu:
    - Tăng cường khả năng phục hồi và phi tập trung của mạng.
- Hành động:
    - Kết nạp thêm các tổ chức học thuật, NGO và tổ chức quốc tế.
    - Thực hiện phân phối và mở rộng các nút về mặt địa lý.

9.2. Tính năng bảo mật và quyền riêng tư nâng cao

- Mật mã học nâng cao:
    - Triển khai zk-STARKs để cải thiện ZKPs.
- Thuật toán chống lượng tử:
    - Nghiên cứu và tích hợp thuật toán mật mã chống lại các mối đe dọa từ máy tính lượng tử.
- Xác thực đa yếu tố và sinh trắc học:
    - Tăng cường bảo mật ví DID với tính năng xác thực đa yếu tố và các tùy chọn sinh trắc học nâng cao.

9.3. Tích hợp với tiêu chuẩn định danh số toàn cầu

- Áp dụng các tiêu chuẩn:
    - Kết hợp các tiêu chuẩn mới nổi như DIDComm để giao tiếp an toàn.
- Đối tác quốc tế:
    - Hợp tác với các sáng kiến định danh toàn cầu như ID2020.

9.4. Nâng cao trải nghiệm người dùng

- Khả năng tiếp cận:
    - Hỗ trợ nhiều ngôn ngữ.
    - Thiết kế cho người dùng khuyết tật.
- Chu trình phản hồi người dùng:
    - Thiết lập các kênh thu thập phản hồi liên tục từ người dùng để cải tiến.

9.5. Nghiên cứu và phát triển các trường hợp sử dụng nâng cao

- Tích hợp IoT:
    - Phát triển giải pháp định danh cho thiết bị trong các thành phố thông minh.
- AI và máy học:
    - Sử dụng AI để phát hiện bất thường và ngăn chặn gian lận.
- Tổ chức tự trị phi tập trung (DAO):
    - Khám phá mô hình quản trị sử dụng DAO cho quyết định do cộng đồng điều hành.

9.6. Cải tiến liên tục về tiêu chuẩn bảo mật và tuân thủ

- Giám sát quy định:
    - Theo dõi các cập nhật trong luật bảo vệ dữ liệu.
- Cân nhắc đạo đức:
    - Đảm bảo việc sử dụng dữ liệu và công nghệ một cách có đạo đức.

9.7. Tính bền vững và tầm nhìn dài hạn

- Mô hình tài trợ:
    - Khám phá các tùy chọn như phí dịch vụ, tài trợ và quan hệ đối tác công-tư.
- Lãnh đạo toàn cầu:
    - Định vị NDAChain là mô hình cho giải pháp định danh số toàn cầu.

---

10. Phân tích Rủi ro và Đề xuất Giải pháp

10.1. Rủi ro kỹ thuật

10.1.1. Tấn công vào cơ chế đồng thuận

- Rủi ro: Nút xác thực sai lệch thông đồng để cùng phá vỡ sự đồng thuận.
- Giải pháp:
    - Thực hiện các tiêu chí lựa chọn nút xác thực nghiêm ngặt.
    - Kết hợp các cơ chế phạt để trừng phạt hành vi sai trái.

10.1.2. Lỗ hổng mật mã

- Rủi ro: Những tiến bộ trong tính toán khiến các thuật toán mật mã hiện tại trở nên không an toàn.
- Giải pháp:
    - Cập nhật thường xuyên các giao thức mật mã mới.
    - Nghiên cứu và áp dụng các thuật toán chống lượng tử.

10.2. Rủi ro vận hành

10.2.1. Sự cố về nút

- Rủi ro: Nút xác thực bị mất kết nối ảnh hưởng đến hiệu suất mạng.
- Giải pháp:
    - Đảm bảo tính dự phòng.
    - Triển khai các cơ chế tự động chuyển đổi dự phòng.

10.2.2. Vấn đề đồng bộ dữ liệu

- Rủi ro: Sự không nhất quán giữa cơ sở dữ liệu quốc gia và NDAChain.
- Giải pháp:
    - Triển khai giao thức đồng bộ hóa mạnh mẽ.
    - Thực hiện kiểm toán định kỳ và kiểm tra tính nhất quán.

10.3. Rủi ro triển khai

10.3.1. Mức độ chấp nhận của người dùng

- Rủi ro: Người dùng không muốn áp dụng công nghệ mới.
- Giải pháp:
    - Tập trung vào thiết kế thân thiện với người dùng.
    - Cung cấp các ưu đãi và lợi ích rõ ràng.

10.3.2. Sự không đồng nhất giữa các bên liên quan

- Rủi ro: Xung đột lợi ích giữa các bên liên quan cản trở tiến trình.
- Giải pháp:
    - Thiết lập các cấu trúc quản trị rõ ràng.
    - Thúc đẩy giao tiếp minh bạch.

10.4. Rủi ro tuân thủ

10.4.1. Không tuân thủ quy định

- Rủi ro: Vô tình vi phạm luật bảo vệ dữ liệu.
- Giải pháp:
    - Hợp tác với các chuyên gia pháp lý.
    - Triển khai các công cụ giám sát tuân thủ.

10.4.2. Thách thức pháp lý quốc tế

- Rủi ro: Chia sẻ dữ liệu xuyên biên giới dẫn đến tranh chấp pháp lý.
- Giải pháp:
    - Thiết lập các thỏa thuận quốc tế rõ ràng.
    - Tuân thủ tiêu chuẩn bảo vệ dữ liệu quốc tế.

---

11. Tuân thủ và Căn chỉnh theo Tiêu chuẩn

11.1. Tuân thủ tiêu chuẩn quốc tế

- Tiêu chuẩn W3C về DID và VC:
    - Đảm bảo tương thích với các hệ thống định danh toàn cầu.
- ISO/IEC 27001:
    - Tuân thủ các tiêu chuẩn quốc tế về quản lý an ninh thông tin.
- ISO/TC 307:
    - Căn chỉnh với các tiêu chuẩn về blockchain và công nghệ sổ cái phân tán.

11.2. Tuân thủ quy định pháp luật

- Căn chỉnh theo GDPR:
    - Cơ sở pháp lý cho việc xử lý: Thu thập sự đồng ý cho việc xử lý dữ liệu.
    - Quyền của chủ thể dữ liệu: Cơ chế để truy cập, chỉnh sửa và xóa bỏ dữ liệu.
- Luật Bảo vệ Dữ liệu Việt Nam:
    - Tuân thủ Luật An ninh mạng và Nghị định về Bảo vệ Dữ liệu Cá nhân.

11.3. Quy định thực hành tốt nhất trong ngành

- OWASP Top 10:
    - Giảm thiểu các rủi ro bảo mật ứng dụng web phổ biến.
- Khung An ninh mạng NIST:
    - Áp dụng hướng dẫn để xác định, bảo vệ, phát hiện, phản ứng và phục hồi từ sự kiện an ninh mạng.
- Nguyên tắc bảo mật theo thiết kế:
    - Nhúng bảo mật vào kiến trúc và vận hành của hệ thống CNTT.

---

12. Kết luận và Lời kêu gọi Hành động

NDAChain đánh dấu bước tiến quan trọng trong lĩnh vực định danh số tại Việt Nam. Bằng cách kết hợp độ tin cậy của hệ thống tập trung với công nghệ phi tập trung, hệ thống mang đến giải pháp an toàn, có khả năng mở rộng và tập trung vào người dùng. Việc triển khai thành công NDAChain đòi hỏi sự hợp tác giữa các cơ quan chính phủ, đối tác khu vực tư nhân và công dân.

Chúng tôi kêu gọi tất cả các bên liên quan cùng tham gia hành trình chuyển đổi này, hướng tới một tương lai số an toàn và hiệu quả. Cùng nhau, chúng ta có thể biến NDAChain thành mô hình mẫu cho hệ thống định danh số toàn cầu.

---

13. Tài liệu Tham khảo

1. W3C Decentralized Identifiers (DID) v1.0
    - Liên kết đến Tiêu chuẩn
2. Mô hình dữ liệu Chứng chỉ có thể xác minh W3C phiên bản 1.1
    - Liên kết đến Tiêu chuẩn
3. Quy định về Bảo vệ Dữ liệu Chung (GDPR)
    - Liên kết đến Quy định
4. Luật An ninh mạng Việt Nam

    - Liên kết đến Luật
5. Tài liệu Hyperledger Besu
    - Liên kết đến Tài liệu
6. Bằng chứng không tri thức trong Blockchain
    - Tài nguyên Giáo dục
7. Quản lý An ninh Thông tin ISO/IEC 27001
    - Liên kết đến Tiêu chuẩn
8. Khung An ninh mạng NIST
    - Liên kết đến Khung
9. Mười rủi ro bảo mật hàng đầu OWASP
    - Liên kết đến Tài nguyên
10. Các quy định thực hành tốt nhất về bảo mật Blockchain
    - Liên kết đến Tài nguyên

---

14. Phụ lục

A. Từ điển

- Blockchain: Sổ cái phi tập trung ghi lại tất cả giao dịch trên mạng ngang hàng.
- Định danh phi tập trung (DID): Định danh duy nhất toàn cầu không yêu cầu cơ quan đăng ký tập trung.
- Bằng chứng không tri thức (ZKP): Phương pháp mật mã cho phép một bên chứng minh tuyên bố là đúng mà không tiết lộ thông tin ngoài tính hợp lệ của tuyên bố đó.
- Bằng chứng quyền hạn (PoA): Cơ chế đồng thuận trong đó giao dịch được xác thực bởi các tài khoản được phê duyệt (gọi là nút xác thực).
- Blockchain được kiểm soát (permissioned blockchain): Mạng blockchain mà quyền truy cập và tham gia được kiểm soát.
- Nút xác thực: Nút chịu trách nhiệm xác thực giao dịch và duy trì sổ cái blockchain.
- Hyperledger Besu: Ứng dụng Ethereum mã nguồn mở được thiết kế cho mục đích doanh nghiệp.
- Chứng chỉ có thể xác minh (VC): Chứng chỉ chống giả mạo, có thể được xác minh bằng mật mã.

B. Thông số giao thức chi tiết

B.1. Chức năng hợp đồng thông minh quản lý DID

- registerDID(address did, DIDDocument doc):
    - Đăng ký DID mới và liên kết với Tài liệu DID.

- Kiểm soát truy cập: Chỉ thực thể được ủy quyền mới có thể thực hiện việc này.

- updateDID(address did, DIDDocument doc):
  - Cập nhật Tài liệu DID liên kết với DID hiện có.
  - Xác thực: Đảm bảo người gọi có quyền thực hiện thay đổi.
- revokeDID(address did):
  - Thu hồi và vô hiệu hóa một DID đang có.
  - Mục đích: Ngăn chặn các hoạt động xác thực trong tương lai sử dụng DID này.

B.2. Cơ chế kiểm soát truy cập

- Kiểm soát truy cập dựa trên vai trò (RBAC):
  - Định nghĩa các vai trò như 'Bên xác thực', 'Bên phát hành', và 'Người dùng'.
  - Gán quyền dựa trên các vai trò.

C. Định nghĩa và thuật toán

C.1. Bằng chứng không tri thức (zk-SNARKs)

- Định nghĩa:
  - Một bộ `(G, P, V)` trong đó:
    - $G(1^\lambda) \rightarrow (pp, vk)$: Tạo tham số công khai và khóa xác thực.
    - `P(pp, x, w) → π`: Người chứng minh sử dụng tham số công khai, tuyên bố `x`, và nhân chứng `w` để tạo ra bằng chứng `π`.
    - $V(vk, x, \pi) \rightarrow \{0,1\}$: Người xác thực sử dụng khóa xác thực, tuyên bố, và bằng chứng để chấp nhận hoặc từ chối.
- Đặc tính:
  - Tính đầy đủ: Nếu `w` là một nhân chứng hợp lệ cho `x`, thì `V(vk, x, π) = 1`.
  - Tính chính xác: Nếu `V(vk, x, π) = 1`, thì tồn tại một `w` mà `P` có thể đã tạo ra `π`.
  - Tính riêng tư: `π` không tiết lộ thông tin nào về `w`.

C.2. Chính thức hóa thuật toán đồng thuận

- Mô hình hệ thống:
  1. Một tập hợp các nút xác thực `V = {v1, v2, ..., vn}`.
  2. Mỗi nút xác thực duy trì một bản sao cục bộ của blockchain `B`.
- Tính an toàn:
  1. Với hai nút xác thực trung thực bất kỳ `vi` và `vj`, blockchain tương ứng `Bi` và `Bj` đồng thuận về tất cả các khối cho đến khối đã xác nhận mới nhất.

- Tính sống động:
    1. Giao dịch từ khách hàng trung thực cuối cùng sẽ được đưa vào B.
- Các bước thuật toán:
    1. Đề xuất:
        - Nút xác thực v_p đề xuất một khối B_h tại độ cao h.
    2. Xác thực:
        - Các nút xác thực khác kiểm tra tính chính xác của B_h.
    3. Cam kết:
        - Nếu hợp lệ, thêm B_h vào blockchain cục bộ.

D. Dữ liệu đánh giá hiệu suất

D.1. Biểu đồ thông lượng giao dịch

- Mô tả: Biểu đồ hiển thị TPS theo thời gian dưới các mức tải khác nhau.
- Kết quả: TPS vẫn ổn định đến 80% công suất tối đa.

D.2. Biểu đồ phân phối độ trễ

- Mô tả: Biểu đồ histogram về thời gian xác nhận giao dịch.
- Kết quả: Phần lớn các giao dịch được xác nhận trong vòng 1-2 giây.

D.3. Cấu hình kiểm tra khả năng mở rộng

- Tham số kiểm tra:
    - Số lượng nút xác thực: 10, 20, 30, 40, 50.
    - Độ trễ mạng: Mô phỏng tại 50ms, 100ms.
- Tóm tắt kết quả:

Các nút xác thực	TPS	Độ trễ (Trung bình)
10	1,200	1.5s
20	1,800	1.7s
30	2,200	1.9s
40	2,500	2.1s
50	2,800	2.3s