CÁO BẠCH

NDAChain

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

2024

Mục lục

Cáo bạch NDAChain

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

Tóm tắt

Khi Việt Nam đẩy nhanh quá trình chuyển đổi số, nhu cầu về một hệ thống nhận diện số đảm bảo an toàn, khả năng mở rộng và bảo vệ quyền riêng tư trở nên vô cùng cấp thiết. Hạ tầng nhận diện tập trung hiện tại, mặc dù mang tính thẩm quyền, vẫn tồn tại những hạn chế về bảo vệ quyền riêng tư, khả năng mở rộng, và tính tương thích toàn cầu. NDAChain giới thiệu Hệ thống Danh tính Phi tập trung Lai (Hybrid DID) dựa trên công nghệ blockchain nhằm nâng cao khung nhận diện quốc gia. Bằng cách tích hợp mạng blockchain phân quyền được kiểm soát với Cơ sở Dữ liệu Quốc gia tập trung, NDAChain cho phép công dân kiểm soát dữ liệu cá nhân của họ, tăng cường an ninh và hỗ trợ tương tác xuyên biên giới một cách liền mạch. Cáo bạch này cung cấp cái nhìn chuyên sâu về mặt kỹ thuật của NDAChain, bao gồm các thông số giao thức chính 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 tăng trưởng kinh tế nhanh chóng và chuyển đổi số của Việt Nam đòi hỏi một hạ tầng danh tính kỹ thuật số vững chắc. Trung tâm Dữ liệu Quốc gia (NDC) hiện đang quản lý một hệ thống danh tính tập trung cho hơn 100 triệu công dân, đóng vai trò là nền tảng cho việc xác minh danh tính trong nhiều lĩnh vực. Tuy nhiên, tính chất tập trung của hệ thống này đặt ra những thách thức về quyền riêng tư, khả năng mở rộng và khả năng tương tác.

1.2 Thách thức về Danh tính Kỹ thuật số

Các thách thức chính bao gồm:

- Rủi ro về Quyền riêng tư Dữ liệu: Lưu trữ tập trung tạo ra một điểm thất bại duy nhất, làm tăng khả năng bị vi phạm dữ liệu.
- Hạn chế về Khả năng mở rộng: Hạ tầng hiện tại có thể không hỗ trợ nhu cầu ngày càng tăng về dịch vụ kỹ thuật số.
- Hạn chế về Khả năng tương tác Toàn cầu: Thiếu sự phù hợp với các tiêu chuẩn quốc tế cản trở các tương tác xuyên biên giới.
- Kiểm soát của Công dân Hạn chế: Công dân có quyền kiểm soát tối thiểu đối với dữ liệu cá nhân của họ và cách thức dữ liệu được chia sẻ.

1.3 Các Giải pháp Hiện có và Hạn chế của Chúng

Mặc dù có một số giải pháp danh tính tồn tại, nhưng chúng thường không đạt yêu cầu trong việc cân bằng giữa niềm tin, quyền riêng tư, khả năng mở rộng và tuân thủ:

- Hệ thống Tập trung: Gặp phải các vấn đề về quyền riêng tư và khả năng mở rộng.
- Hệ thống Liên kết: Phụ thuộc vào các nhà cung cấp bên thứ ba, làm dấy lên những lo ngại về chủ quyền dữ liệu.
- Danh tính tự chủ (SSI): Cung cấp quyền kiểm soát cho người dùng nhưng có thể thiếu xác minh có thẩm quyền và tuân thủ quy định.

1.4 Nhu cầu về NDAChain

NDAChain nhằm mục đích:

- Kết hợp niềm tin tập trung với xác minh phi tập trung.
- Tăng cường quyền riêng tư thông qua các kỹ thuật mã hóa tiên tiến.
- Mở rộng hiệu quả để hỗ trợ triển khai quốc gia.
- Phù hợp với các tiêu chuẩn toàn cầu về khả năng tương tác.
- Trao quyền cho công dân kiểm soát dữ liệu của họ.

---

2. Tầm nhìn và Mục tiêu

2.1 Trao quyền cho Công dân

- Quyền sở hữu dữ liệu: Công dân có quyền sở hữu và kiểm soát hoàn toàn dữ liệu danh tính của họ.
- Tiết lộ có chọn lọc: Việc sử dụng Chứng minh không biết (ZKPs) cho phép chia sẻ chỉ thông tin cần thiết.

2.2 Tăng cường An ninh và Quyền riêng tư

- Mã hóa tiên tiến: Triển khai mã hóa mạnh mẽ và các giao thức mã hóa.
- Niềm tin phân tán: Giảm thiểu rủi ro liên quan đến sự tập trung.

2.3 Đạt được Khả năng mở rộng và Hiệu quả

- Đồng thuận hiệu quả: Sử dụng Chứng minh quyền hạn (PoA) để đạt được thông lượng cao.
- Kiến trúc mô-đun: Cho phép mở rộng độc lập các thành phần của hệ thống.

2.4 Kích hoạt Tính tương tác Toàn cầu

- Tuân thủ Tiêu chuẩn: Tuân thủ tiêu chuẩn W3C về DID và Chứng chỉ có thể xác minh.

- Nhận diện Xuyên Biên giới: Tạo điều kiện cho việc sử dụng danh tính kỹ thuật số quốc tế.

2.5 Đảm bảo Tuân thủ Quy định

- Quy định Quốc gia: Tuân thủ các luật của Việt Nam về bảo vệ dữ liệu.
- 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 Danh tính Phi tập trung Lai (Hybrid DID)

NDAChain tích hợp một blockchain có quyền truy cập với Cơ sở Dữ liệu Quốc gia để tạo ra một hệ thống Hệ thống Danh tính Phi tập trung Lai (Hybrid DID):

- Xác minh Tập trung: Cơ sở Dữ liệu Quốc gia vẫn là nguồn thông tin chính thức.
- Quản lý Danh tính Phi tập trung: Blockchain cho phép các hoạt động danh tính an toàn và phân tán.
- Trao quyền cho Người dùng: Công dân quản lý danh tính của họ thông qua ví DID.

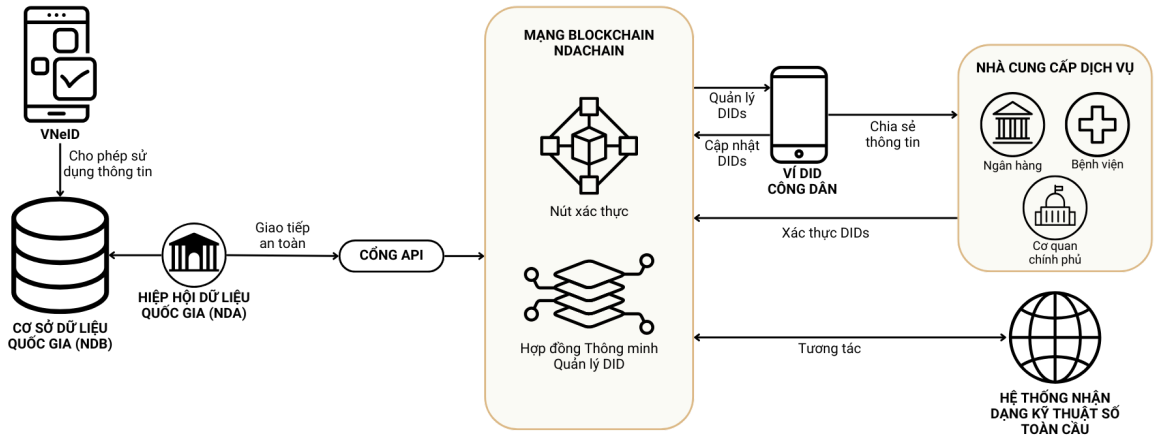
3.2 Các Thành phần Chính

1. Mạng Blockchain Có quyền truy cập (Hyperledger Besu)
2. Nút xác thực và Quản trị
3. Lớp Quản lý DID và Hợp đồng thông minh
4. Tích hợp Cổng API
5. Ví 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 danh tính đã được xác minh.
- Hiệp hội Dữ liệu Quốc gia (NDA): Một cơ quan chính phủ chịu trách nhiệm quản lý việc truyền dữ liệu từ Cơ sở Dữ liệu Quốc gia (NDB) sang blockchain.
- Cổng API (APIG): Một giao diện giữa NDA và blockchain, đảm bảo việc giao tiếp được an toàn.
- Mạng Blockchain NDAChain:
    - Nút Xác thực (VNs): Các nút xác thực giao dịch.
    - Hợp đồng Thông minh Quản lý DID (DIDSC): Các hợp đồng xử lý các hoạt động DID.
- Ví DID Công dân (CDW): Ứng dụng cho công dân để quản lý danh tính.
- Nhà cung cấp dịch vụ (SPs): Các thực thể 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 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 mật mã của khóa công khai của người dùng và các định danh khác.
        - Lưu trữ Tài liệu DID trên chuỗi thông qua hợp đồng thông minh.
    3. Đầu ra: DID được gán cho người dùng.
- Tạo Chứng minh Không biết (Sử dụng zk-SNARKs):
    1. Đầu vào: Thuộc tính của người dùng cần chứng minh.
    2. Quá trình:
        - Tạo một chứng minh zk-SNARK xác minh thuộc tính mà không tiết lộ nó.
    3. Đầu ra: ZKP được gửi đến người xác minh.

4.3 Cơ chế Đồng thuận: Chứng minh 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 Proof of Work (PoW).
    - Tiêu thụ năng lượng: Ít tốn năng lượng hơn đáng kể so với PoW.
    - Kiểm soát: Cho phép một tập hợp các nút xác thực được kiểm soát, phù hợp với các yêu cầu quy định.
- So sánh với các cơ chế khác:
    - Proof of Stake (PoS): Mặc dù PoS cung cấp sự phân quyền, nhưng có thể không cung cấp kiểm soát cần thiết cho việc tuân thủ.
    - Delegated PoS (DPoS): Giới thiệu các phức tạp trong quản trị và rủi ro tập trung tiềm ẩn.

4.3.2 Hoạt động Kỹ thuật

- Lựa chọn nút xác thực:
    - Tiêu chí: Tuân thủ các tiêu chuẩn an ninh, độ tin cậy và khả năng hoạt động.

    - Quy trình gia nhập: Các nút xác thực được thêm vào thông qua một 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 lần lượt 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 hành vi bất thường, khối sẽ bị từ chối bởi những bên khác.
- Khả năng chịu lỗi:
    - Mạng có thể chịu đựng tối đa (N-1)/3 nút xác thực bị lỗi.
    - Triển khai các cơ chế để cắt giảm hoặc loại bỏ các nút xác thực bất thường.

4.4 Quản lý DID và Hợp đồng thông minh

- Hợp đồng Đăng ký DID:
    - Chức năng:
        - `registerDID(didDocument)`
        - `updateDID(didDocument)`
        - `revokeDID(did)`
- Biện pháp bảo mật:
    - Kiểm soát truy cập thông qua quyền dựa trên vai trò.
    - Xác thực đầu vào để ngăn chặn các cuộc tấn công tiêm.

4.5 Triển khai Bằng chứng Không biết

- Giao thức ZKP:
    1. Loại: zk-SNARKs (Bằng chứng Không biết Ngắn gọn Không tương tác về Kiến thức)
    2. Các thuộc tính:
        - Tính đầy đủ: Các chứng minh trung thực luôn được chấp nhận.

        - Tính hợp lệ: Các chứng minh sai bị từ chối.
        - Không biết: Không có thông tin nào về dữ liệu cơ sở được tiết lộ.
- Các bước triển khai:
    1. Thiết lập: Tạo các tham số công khai (thiết lập tin cậy).
    2. Chứng minh: Người dùng tạo một chứng minh cho một tuyên bố (ví dụ: tuổi trên 18).
    3. Xác minh: Người xác minh kiểm tra chứng minh 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 danh tính mới.
        - `/update`: Để cập nhật thuộc tính danh tính.
        - `/revoke`: Để thu hồi danh tính.
- 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

- Sự tấn công bên ngoài: Cố gắng truy cập trái phép vào dữ liệu hoặc làm gián đoạn hoạt động của mạng.
- Sự tấn công từ nội bộ: Các nút xác thực bất thường hoặc người trong cuộc làm tổn hại đến tính toàn vẹn của hệ thống.
- Các đe dọa về quyền riêng tư: Liên kết trái phép các danh tính người dùng hoặc tiết lộ thuộc tính.

5.2 Các thuộc tính Bảo mật

- Bảo mật: Được đảm bảo thông qua mã hóa và ZKPs.
- Tính toàn vẹn: Được bảo vệ bởi tính không thay đổi của blockchain và các cơ chế đồng thuận.
- Tính khả dụng: Đạt được thông qua sự dư thừa mạng 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 minh Chính thức

- Xác minh 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 minh Giao thức:
    - Phân tích Giao thức Bảo mật:
        - Xác minh các thuộc tính như bí mật và xác thực bằng cách sử dụng các công cụ như ProVerif.
- Xác minh tuân thủ:
    - Kiểm toán định kỳ để đảm bảo tuân thủ các tiêu chuẩn và quy định.

---

6. Các chỉ số hiệu suất

6.1 Thông lượng giao dịch và độ trễ

6.1 Khả năng Xử lý 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:
    - Khả năng xử lý: 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 Các bài 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 khả năng 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 PoA và mạng lưới có quyền truy cập.
- 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. Các trường hợp sử dụng

7.1 Truy cập dịch vụ công

Kịch bản: Nguyễn, một cư dân của Hà Nội, cần gia hạn giấy phép lái xe của mình trực tuyến. Thông thường, quy trình này yêu cầu nhiều lần đến các văn phòng chính phủ và nhiều giấy tờ.

Quy trình với NDAChain:

1. Xác thực:
    - Nguyễn đăng nhập vào ứng dụng VNeID, trong trường hợp này đóng vai trò như Ví DID của anh, được bảo mật bằng xác thực sinh trắc học.
2. Tiết lộ có chọn lọc:
    - Thông qua Ví DID của mình, anh đồng ý chia sẻ chỉ những thông tin cần thiết cho việc gia hạn giấy phép, chẳng hạn như chứng minh danh tính và thông tin giấy phép hiện tại.
    - Nền tảng tạo ra một Chứng minh không biết (ZKP) xác thực Nguyễn đủ điều kiện đăng ký mà không tiết lộ dữ liệu cá nhân.
3. Xác minh:
    - Hệ thống chính phủ xác minh ZKP qua NDAChain, xác nhận danh tính và điều kiện của Nguyễn.
    - Quá trình xác minh được ghi lại trên blockchain để phục vụ cho mục đích kiểm toán.
4. Xử lý Đơn xin:
    - Đơn xin được xử lý tự động, và bất kỳ cập nhật cần thiết nào cũng được thực hiện đối với Tài liệu DID của Nguyễn.
5. Thông báo:
    - Nguyễn nhận được thông báo kỹ thuật số về giấy phép đã được gia hạn của mình, điều này cũng được phản ánh trong Ví DID của anh ấy.

Lợi ích:

- Hiệu quả: Giảm thời gian xử lý từ vài ngày xuống còn vài phút.
- Riêng tư: Bảo vệ dữ liệu cá nhân thông qua ZKPs.
- Khả năng kiểm toán: Cung cấp một bản ghi không thể thay đổi của giao dịch.

7.2 Đơn giản hóa Giao dịch Tài chính

Kịch bản: Linh muốn xin vay tiền từ ngân hàng để bắt đầu kinh doanh nhỏ của mình.

Quy trình với NDAChain:

1. Khởi đầu:
    - Linh truy cập cổng thông tin trực tuyến xin vay tiền của ngân hàng.
2. Xác minh Danh tính:
    - Sử dụng Ví DID của cô ấy để chia sẻ các chứng chỉ có thể xác minh cần thiết mà ngân hàng yêu cầu, chẳng hạn như chứng minh danh tính và lịch sử tín dụng.
3. Sử dụng ZKP:
    - Tạo ra ZKPs để chứng minh mức thu nhập và khả năng tín dụng của cô mà không tiết lộ thông tin tài chính chi tiết.
4. Xác minh Thời gian Thực:
    - Ngân hàng xác minh 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 khoản vay.
- 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 người nộp đơn.

7.3 Tăng cường Tương tác Xuyên biên giới

Kịch bản: Anh là một doanh nhân đang có kế hoạch mở rộng kinh doanh ra quốc tế. Anh cần thiết lập danh tính của mình với các đối tác nước ngoài.

Quy trình với NDAChain:

1. Trình bày Chứng chỉ:
    - Anh chia sẻ DID và các chứng chỉ có thể xác minh liên quan với các đối tác quốc tế.
2. Tính tương tác:
    - Vì NDAChain tuân thủ các tiêu chuẩn DID của W3C, các thực thể nước ngoài có thể xác minh chứng chỉ của anh bằng hệ thống của họ.

3. Xác minh:
    - Các đối tác xác minh tính xác thực của chứng chỉ của Anh qua các mạng lưới danh tính toàn cầu tương thích.
4. Giao dịch Kinh doanh:
    - Anh 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 minh.
- Hiệu quả: Giảm thời gian và tài nguyên tiêu tốn cho việc xác minh 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 một chuyên gia trong khi vẫn giữ được quyền riêng tư.

Quy trình với NDAChain:

- Minh sử dụng Ví DID của mình để tạo ra ZKPs xác nhận các điều kiện y tế cần thiết mà không tiết lộ toàn bộ lịch sử y tế.
- Chuyên gia xác minh thông tin qua NDAChain.

Lợi ích:

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

7.4.2 Xác minh bằng cấp học thuật

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

Quy trình với NDAChain:

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

Lợi ích:

- Ngăn chặn gian lận bằng cấp.
- Đơn giản hóa quy trình tuyển dụng cho nhà 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
- Các hoạt động kỹ thuật:
    - Thiết lập các nút xác thực ban đầu với tiêu chuẩn bảo mật cao.
    - Triển khai hợp đồng thông minh cho quản lý DID trên blockchain.
    - Phát triển và phân phối các 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 của hệ thống.
    - Thu thập dữ liệu hiệu suất ban đầu.

Giai đoạn 2: Triển khai Khu vực

- Thời gian: Tháng 4-6
- Các hoạt động kỹ thuật:
    - Mở rộng mạng lưới xác thực để bao gồm các nút bổ sung.
    - Tối ưu hóa hợp đồng thông minh dựa trên phản hồi từ thí điểm.
    - Nâng cao tính năng 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 các mẫu sử dụng khu vực.

Giai đoạn 3: Triển khai toàn quốc

- Thời gian: Tháng 7-12
- Các hoạt động kỹ thuật:
    - Tiến hành onboard thêm các nút xác thực trên toàn quốc.

    - Tích hợp hoàn toàn với các dịch vụ chính phủ và các đối tác lớn trong khu vực tư nhân.
    - Triển khai các biện pháp bảo mật tiên tiến, chẳng hạn như HSM trên các nút xác thực.
- Quản lý Mạng:
    - Thiết lập trung tâm vận hành mạng quốc gia.
    - Triển khai các quy trình phản ứng sự cố bảo mật toàn diện.
- Kết quả Dự kiến:
    - Đạt được sự chấp nhận trên toàn quốc.
    - Thiết lập các 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 các chức năng của hợp đồng thông minh.
    - Xác thực các 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 người dùng và quy trình làm việc.

8.3 Chương trình Nâng cao Nhận thức và Giáo dục Công chúng

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 Người xác thực

- Nội dung:
    - Đào tạo kỹ thuật về vận hành và bảo trì nút.
    - Các phương pháp bảo mật tốt nhất.
    - Các yêu cầu về tuân thủ và quy định.

8.3.3 Các buổi hội thảo cho Nhà cung cấp Dịch vụ

- Mục tiêu:
    - Tạo điều kiện tích hợp với NDAChain.
    - Cung cấp hỗ trợ kỹ thuật và tài nguyên.
- Hoạt động:
    - 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 các 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 vào các diễn đàn toàn cầu.
    - Đồng bộ hóa với các thực tiễn tốt nhất quốc tế.

---

9. Triển vọng tương lai và Lộ trình

9.1 Mở rộng Mạng lưới Người xác thực

- Mục tiêu:
    - Tăng cường khả năng phục hồi và phân quyền của mạng.
- Hành động:
    - Tiếp nhận các tổ chức học thuật, NGO và tổ chức quốc tế.
    - Thực hiện phân phối địa lý của các nút.

9.2 Tính năng Bảo mật và Riêng tư Nâng cao

- Mật mã Học nâng cao:
    - Triển khai zk-STARKs để có ZKPs hiệu quả hơn.
- Thuật toán Chống lượng tử:
    - Nghiên cứu và tích hợp các thuật toán mật mã chống lại các mối đe dọa từ máy tính lượng tử.
- MFA và Sinh trắc học:
    - Tăng cường bảo mật Ví DID với xác thực đa yếu tố và các tùy chọn sinh trắc học nâng cao.

9.3 Tích hợp với Các tiêu chuẩn Danh tính Kỹ thuật số Toàn cầu

- Chấp nhận 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 danh tính 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 của Người dùng:
    - Thiết lập các kênh để thu thập phản hồi liên tục từ người dùng và cải tiến.

9.5 Nghiên cứu và Phát triển cho Các Trường hợp Sử dụng Nâng cao

- Tích hợp IoT:
    - Phát triển các giải pháp danh tính cho các thiết bị trong các thành phố thông minh.

- AI và Học Máy:
    - Sử dụng AI để phát hiện bất thường và ngăn chặn gian lận.
- Tổ chức Tự trị Phi tập trung (DAO):
    - Khám phá các 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 thay đổi 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 như một mô hình cho các giải pháp danh tính kỹ thuật số trên toàn thế giới.

---

10. Phân tích rủi ro và chiến lược giảm thiểu

10.1 Rủi ro kỹ thuật

10.1.1 Các cuộc tấn công vào cơ chế đồng thuận

- Rủi ro: Các nút xác thực bất thường thông đồng để cùng phá vỡ sự đồng thuận.
- Giảm thiểu:
    - 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 Các 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.
- Giảm thiểu:
    - Cập nhật thường xuyên các giao thức mật mã.
    - Nghiên cứu và áp dụng các thuật toán chống lượng tử.

10.2 Rủi ro vận hành

10.2.1 Sự cố nút

- Rủi ro: Các nút xác thực bị ngắt kết nối ảnh hưởng đến hiệu suất mạng.
- Giảm thiểu:
    - 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.
- Giảm thiểu:
    - Triển khai các giao thức đồng bộ hóa mạnh mẽ.
    - Thực hiện kiểm toán định kỳ và kiểm tra tính nhất quán.

10.3 Rủi ro Thông qua

10.3.1 Sự Kháng cự của Người dùng

- Rủi ro: Người dùng không muốn áp dụng công nghệ mới.
- Giảm thiểu:
    - 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: Lợi ích mâu thuẫn giữa các bên liên quan cản trở tiến trình.
- Giảm thiểu:
    - 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: Vi phạm không cố ý các luật bảo vệ dữ liệu.

- Giảm thiểu:
    - Tham gia 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.
- Giảm thiểu:
    - Thiết lập các thỏa thuận quốc tế rõ ràng.
    - Tuân thủ các tiêu chuẩn bảo vệ dữ liệu quốc tế.

---

11. Tuân thủ và Căn chỉnh Tiêu chuẩn

11.1 Tuân thủ Tiêu chuẩn Quốc tế

- Tiêu chuẩn W3C về DID và VC:
    - Đảm bảo khả năng tương tác với các hệ thống danh tính 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 công nghệ blockchain và sổ cái phân tán.

11.2 Tuân thủ Quy định

- Căn chỉnh GDPR:
    - Cơ sở hợp pháp cho việc xử lý: Đã có 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.
- 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 Thực tiễn 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 các hướng dẫn để xác định, bảo vệ, phát hiện, phản ứng và phục hồi từ các sự kiện an ninh mạng.
- Nguyên tắc Bảo mật theo Thiết kế:
    - Nhúng bảo mật vào kiến trúc và hoạt động của các hệ thống CNTT.

---

12. Kết luận và Kêu gọi Hành động

NDAChain đại diện cho một bước tiến quan trọng trong lĩnh vực danh tính số của Việt Nam. Bằng cách kết hợp niềm tin tập trung với công nghệ phi tập trung, nó cung cấp một giải pháp an toàn, có thể 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, các đối tác khu vực tư nhân và công dân.

Chúng tôi kêu gọi tất cả các bên liên quan tham gia cùng chúng tôi trong 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 một mô hình cho các hệ thống danh tính số trên toàn thế giới.

---

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. Chứng minh không biết 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 thực tiễn tốt nhất về bảo mật Blockchain
    - Liên kết đến Tài nguyên

---

14. Phụ lục

A. Từ điển

- Blockchain: Một sổ cái phân tán của tất cả các giao dịch trên một mạng ngang hàng.
- Định danh phi tập trung (DID): Một định danh duy nhất toàn cầu không yêu cầu cơ quan đăng ký tập trung.
- Chứng minh không biết (ZKP): Một phương pháp mật mã trong đó một bên có thể chứng minh cho bên kia rằng một tuyên bố là đúng mà không tiết lộ bất kỳ thông tin nào ngoài tính hợp lệ của tuyên bố đó.
- Chứng minh quyền hạn (PoA): Một cơ chế đồng thuận trong đó các giao dịch được xác thực bởi các tài khoản được phê duyệt được gọi là các nút xác thực.
- Blockchain có quyền truy cập: Một mạng blockchain trong đó quyền truy cập và tham gia được kiểm soát.
- Nút xác thực: Một nút chịu trách nhiệm xác thực các giao dịch và duy trì sổ cái blockchain.
- Hyperledger Besu: Một khách hàng Ethereum mã nguồn mở được thiết kế cho mục đích doanh nghiệp.
- Chứng chỉ có thể xác minh (VC): Một chứng chỉ có thể phát hiện sự giả mạo và có thể được xác minh bằng mật mã.

B. Thông số giao thức chi tiết

B.1 Các chức năng hợp đồng thông minh của đăng ký DID

- registerDID(address did, DIDDocument doc):
    - Đăng ký một DID mới và liên kết nó với một Tài liệu DID.
    - Kiểm soát truy cập: Chỉ các thực thể được ủy quyền mới có thể gọi chức năng này.
- updateDID(address did, DIDDocument doc):
    - Cập nhật Tài liệu DID liên kết với một DID hiện có.
    - Xác thực: Đảm bảo rằng người gọi có quyền thực hiện các thay đổi.
- revokeDID(address did):
    - Thu hồi một DID hiện có, đánh dấu nó là không hoạt động.
    - Tác động: Ngăn chặn các 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 'Người xác thực', 'Người phát hành', và 'Người dùng'.
    - Gán quyền dựa trên các vai trò.

C. Định nghĩa và Thuật toán Toán học

C.1 Chứng minh Không biết (zk-SNARKs)

- Định nghĩa:
    - Một bộ `(G, P, V)` nơi:
        - $G(1^\lambda) \rightarrow (pp, vk)$: Tạo ra các tham số công khai và khóa xác thực.
        - `P(pp, x, w) → π`: Người chứng minh sử dụng các tham số công khai, tuyên bố `x`, và nhân chứng `w` để tạo ra chứng minh `π`.
        - $V(vk, x, \pi) \rightarrow \{0,1\}$: Người xác thực sử dụng khóa xác thực, tuyên bố, và chứng minh để chấp nhận hoặc từ chối.
- Các thuộc tính:
    - Tính đầy đủ: Nếu `w` là một nhân chứng hợp lệ cho `x`, thì `V(vk, x, π) = 1`.
    - Tính hợp lệ: Nếu `V(vk, x, π) = 1`, thì tồn tại một `w` mà `P` có thể đã tạo ra `π`.
    - Không biết: `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. Đối với hai nút xác thực trung thực bất kỳ `vi` và `vj`, các blockchain của họ `Bi` và `Bj` đồng ý về tất cả các khối cho đến khối đã xác nhận mới nhất.
- Tính sống động:
    1. Các giao dịch được gửi bởi các 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 xác minh `B_h` để đảm bảo tính chính xác.
    3. Cam kết:
        - Nếu hợp lệ, các nút xác thực thêm `B_h` vào blockchain cục bộ của họ.

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 tải khác nhau.
- Quan sát:
    - TPS vẫn ổn định lên 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.
- Quan sát:
    - 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 ở 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