**Nghiên cứu mã định danh phi tập trung DID ứng dụng trong chứng thực mật mã khóa công khai.**

# **LỜI CẢM ƠN**

Trước hết, em xin gửi lời cảm ơn chân thành đến Ban Giám hiệu và các thầy cô trong khoa Công Nghệ Thông Tin, trường …, đã tạo điều kiện và hỗ trợ em trong suốt quá trình học tập và thực hiện đề tài này.

Em xin đặc biệt cảm ơn thầy/cô … đã tận tình hướng dẫn, chỉ bảo và động viên em trong suốt quá trình thực hiện đề tài “*Nghiên cứu mã định danh phi tập trung DID ứng dụng trong chứng thực mật mã khóa công khai*”. Sự hỗ trợ và góp ý quý báu của thầy/cô đã giúp em hoàn thành báo cáo với chất lượng tốt nhất.

Em cũng xin cảm ơn bạn bè và gia đình, những người đã luôn đồng hành và ủng hộ em, không chỉ trong học tập mà còn trong những lúc gặp khó khăn khi thực hiện đề tài.

Cuối cùng, em xin chân thành cảm ơn tất cả các tổ chức, cá nhân và nguồn tài liệu đã cung cấp thông tin, kiến thức bổ ích để em có thể hoàn thiện nghiên cứu này.

Mặc dù đã rất cố gắng, nhưng do thời gian và kiến thức còn hạn chế, báo cáo này chắc chắn không tránh khỏi những thiếu sót. Em rất mong nhận được sự đóng góp ý kiến của các thầy cô và các bạn để hoàn thiện hơn.

Xin chân thành cảm ơn!

MỤC LỤC

# **MỞ ĐẦU**

## **1. Lý do chọn đề tài**

Trong bối cảnh chuyển đổi số và sự phát triển không ngừng của các công nghệ số, việc quản lý danh tính số đang trở thành một yếu tố quan trọng trong hầu hết các lĩnh vực, từ thương mại điện tử, tài chính đến giáo dục và chăm sóc sức khỏe. Các phương pháp định danh truyền thống thường dựa trên các cơ sở dữ liệu tập trung, tiềm ẩn nhiều rủi ro về bảo mật và quyền riêng tư, như nguy cơ bị tấn công, giả mạo danh tính, hoặc lạm dụng dữ liệu cá nhân.

Mã định danh phi tập trung (Decentralized Identifier - DID) đã nổi lên như một giải pháp tiềm năng, tận dụng công nghệ blockchain và sổ cái phân tán để cung cấp một cách quản lý danh tính an toàn, minh bạch và không phụ thuộc vào bên thứ ba. Công nghệ DID không chỉ đảm bảo quyền kiểm soát danh tính thuộc về người dùng, mà còn giúp giảm thiểu các rủi ro bảo mật, đáp ứng tốt hơn yêu cầu của các hệ thống hiện đại.

Mặt khác, chứng thực mật mã khóa công khai đóng vai trò quan trọng trong việc bảo đảm tính bảo mật, toàn vẹn và xác thực trong giao tiếp số. Tuy nhiên, việc quản lý và phân phối khóa công khai trong các hệ thống hiện tại vẫn đối mặt với nhiều thách thức, đặc biệt là vấn đề tin cậy và tập trung.

Sự kết hợp giữa DID và chứng thực mật mã khóa công khai hứa hẹn mang lại một giải pháp tối ưu, không chỉ cải thiện tính bảo mật mà còn tăng cường quyền riêng tư và tính toàn vẹn cho các hệ thống định danh và chứng thực. Chính vì vậy, đề tài “*Nghiên cứu mã định danh phi tập trung DID ứng dụng trong chứng thực mật mã khóa công khai*” được lựa chọn nhằm nghiên cứu sâu hơn về ứng dụng thực tiễn của DID, đồng thời tìm hiểu các lợi ích, thách thức và khả năng mở rộng của công nghệ này trong việc xây dựng một hệ thống định danh số hiệu quả, an toàn và phi tập trung.

Việc nghiên cứu đề tài này không chỉ có ý nghĩa về mặt lý thuyết mà còn mở ra nhiều hướng ứng dụng trong các lĩnh vực khác nhau, góp phần giải quyết các vấn đề thực tế và thúc đẩy tiến bộ công nghệ trong thời đại số.

## **2. Mục tiêu nghiên cứu**

Mục tiêu chính của đề tài “*Nghiên cứu mã định danh phi tập trung DID ứng dụng trong chứng thực mật mã khóa công khai*” là tìm hiểu và đánh giá tiềm năng của mã định danh phi tập trung (Decentralized Identifier - DID) trong việc cải thiện tính bảo mật, minh bạch và hiệu quả của quá trình chứng thực danh tính và quản lý khóa công khai. Cụ thể, đề tài tập trung vào các mục tiêu sau:

* Tìm hiểu lý thuyết về mã định danh phi tập trung (DID): Tìm hiểu các khái niệm cơ bản, kiến trúc, và cơ chế hoạt động của DID. Phân tích các tiêu chuẩn quốc tế như W3C Decentralized Identifier Specification và DIDComm.
* Nghiên cứu mối quan hệ giữa DID và chứng thực mật mã khóa công khai: Tìm hiểu cách DID được tích hợp với mật mã khóa công khai để cải thiện quá trình quản lý và xác thực danh tính. Đánh giá vai trò của DID trong việc loại bỏ sự phụ thuộc vào các bên trung gian và tăng cường quyền kiểm soát danh tính của người dùng.
* Thiết kế và đề xuất mô hình ứng dụng DID: Xây dựng một mô hình thử nghiệm kết hợp DID và chứng thực mật mã khóa công khai trên nền tảng blockchain hoặc các sổ cái phân tán. Đề xuất quy trình tạo, quản lý và xác thực DID trong hệ thống.
* Phân tích ưu điểm và hạn chế của DID trong thực tiễn: Đánh giá hiệu quả của DID trong việc giải quyết các vấn đề bảo mật hiện tại, chẳng hạn như giả mạo danh tính, lộ lọt thông tin cá nhân và tập trung hóa quyền quản lý. Xác định những thách thức khi triển khai DID trong các hệ thống thực tế.
* Xây dựng cơ sở cho các nghiên cứu và ứng dụng tiếp theo: Đưa ra các đề xuất cho việc mở rộng ứng dụng của DID trong các lĩnh vực như thương mại điện tử, tài chính, giáo dục và chăm sóc sức khỏe. Đề xuất hướng nghiên cứu tương lai nhằm cải thiện và phát triển công nghệ DID.

## **3. Đối tượng nghiên cứu**

Đề tài “*Nghiên cứu mã định danh phi tập trung DID ứng dụng trong chứng thực mật mã khóa công khai*” tập trung vào các đối tượng nghiên cứu chính sau đây:

* Mã định danh phi tập trung (Decentralized Identifier - DID): Các khái niệm cơ bản và cấu trúc của DID, bao gồm:
  + Tài liệu DID (DID Document): Chứa thông tin liên quan đến DID, như khóa công khai, dịch vụ liên kết, và metadata.
  + Phương pháp DID (DID Method): Các cơ chế xác định cách DID được tạo, quản lý, và giải quyết.
* Các tiêu chuẩn và giao thức liên quan như W3C Decentralized Identifier Specification và DIDComm.
* Công nghệ blockchain và sổ cái phân tán: Vai trò của blockchain trong việc hỗ trợ DID hoạt động phi tập trung, an toàn và minh bạch. Các nền tảng hỗ trợ DID, ví dụ: Ethereum, Hyperledger, Sovrin.
* Chứng thực mật mã khóa công khai: Nguyên tắc hoạt động của mật mã khóa công khai và vai trò của nó trong việc đảm bảo tính bảo mật và xác thực trong các hệ thống số. Quy trình quản lý, trao đổi, và xác thực khóa công khai trong các hệ thống truyền thống.
* Sự kết hợp giữa DID và mật mã khóa công khai: Cách sử dụng DID để quản lý và xác thực danh tính thông qua khóa công khai. Cơ chế liên kết giữa DID và khóa công khai để loại bỏ sự phụ thuộc vào bên trung gian.
* Các hệ thống và ứng dụng tiềm năng của DID: Các lĩnh vực có thể ứng dụng DID, chẳng hạn như:
  + Quản lý danh tính số trong thương mại điện tử, tài chính, và chăm sóc sức khỏe.
  + Xác thực trong giao dịch số và quản lý thông tin cá nhân.

## **4. Phạm vi nghiên cứu**

Đề tài “*Nghiên cứu mã định danh phi tập trung DID ứng dụng trong chứng thực mật mã khóa công khai*” tập trung vào các khía cạnh lý thuyết và thực tiễn liên quan đến công nghệ DID và ứng dụng của nó trong lĩnh vực chứng thực danh tính. Phạm vi nghiên cứu cụ thể bao gồm:

* Phạm vi về nội dung: Nghiên cứu các khái niệm cơ bản, tiêu chuẩn, và phương pháp hoạt động của mã định danh phi tập trung (Decentralized Identifier - DID). Tìm hiểu và phân tích cách DID được tích hợp với các cơ chế mật mã khóa công khai nhằm cải thiện quá trình chứng thực danh tính. Đánh giá ưu điểm và hạn chế của DID so với các hệ thống định danh tập trung truyền thống. Tập trung vào việc sử dụng blockchain hoặc các sổ cái phân tán làm nền tảng cho DID.
* Phạm vi về công nghệ: Sử dụng nền tảng Hyperledger Indy để triển khai thử nghiệm DID.
* Phạm vi về thực nghiệm: Xây dựng một mô hình thử nghiệm minh họa cách DID hỗ trợ quản lý và chứng thực khóa công khai trong các giao dịch hoặc hệ thống quản lý danh tính số. Phân tích và đánh giá kết quả thực nghiệm dựa trên các tiêu chí như bảo mật và tính khả thi.
* Phạm vi về ứng dụng: Giới hạn phạm vi ứng dụng trong lĩnh vực chứng thực danh tính và bảo mật thông tin. Các tình huống nghiên cứu tập trung vào quản lý danh tính số trong các lĩnh vực như thương mại điện tử, tài chính, và giáo dục.
* Phạm vi địa lý và tài nguyên: Nghiên cứu chủ yếu dựa trên các tiêu chuẩn và công nghệ quốc tế, không ràng buộc bởi các yếu tố địa lý cụ thể. Sử dụng tài nguyên sẵn có như tài liệu khoa học, nền tảng blockchain mã nguồn mở, và các công cụ phát triển phần mềm.
* Phạm vi đánh giá: So sánh hiệu quả giữa hệ thống sử dụng DID và các hệ thống định danh tập trung truyền thống, đặc biệt trong việc quản lý và bảo mật thông tin danh tính. Đánh giá các thách thức, hạn chế và rủi ro khi triển khai DID, từ góc độ kỹ thuật.
* Phạm vi thời gian: Đề tài tập trung vào các nghiên cứu, công nghệ, và tiêu chuẩn đã được phát triển và công bố tính đến thời điểm hiện tại.

## **5. Phương pháp nghiên cứu**

Để đạt được mục tiêu nghiên cứu, đề tài *Nghiên cứu mã định danh phi tập trung DID ứng dụng trong chứng thực mật mã khóa công khai* sử dụng các phương pháp nghiên cứu sau:

* Phương pháp nghiên cứu tài liệu: Tìm hiểu cơ sở lý thuyết và các tiêu chuẩn liên quan đến mã định danh phi tập trung (DID) và mật mã khóa công khai. Thu thập và phân tích các tài liệu khoa học, báo cáo kỹ thuật, tiêu chuẩn quốc tế (W3C DID Specification, DIDComm). Nghiên cứu các nền tảng hỗ trợ DID như Hyperledger Indy. Tham khảo các tài liệu về blockchain, mật mã khóa công khai, và ứng dụng của chúng trong bảo mật danh tính. Hệ thống hóa các kiến thức cơ bản về DID và mật mã khóa công khai. Cung cấp cơ sở lý thuyết cho việc phân tích và đề xuất mô hình.
* Phương pháp nghiên cứu phân tích và so sánh: Đánh giá ưu điểm, nhược điểm của DID so với các phương pháp định danh tập trung truyền thống. Phân tích cơ chế hoạt động của DID trong việc quản lý danh tính và khóa công khai. So sánh các mô hình định danh tập trung và phi tập trung dựa trên các tiêu chí như bảo mật, quyền riêng tư, và hiệu quả. Xác định vai trò và lợi ích của DID trong việc cải thiện chứng thực danh tính.
* Phương pháp thiết kế và mô phỏng: Xây dựng mô hình thử nghiệm minh họa cách sử dụng DID để quản lý và chứng thực khóa công khai. Thiết kế một hệ thống thử nghiệm với DID trên nền tảng blockchain sử dụng Hyperledger Indy. Triển khai quy trình tạo, quản lý, và xác thực DID kết hợp với mật mã khóa công khai. Mô hình thử nghiệm minh họa cách hoạt động của DID trong thực tiễn. Cơ sở dữ liệu và giao thức thực nghiệm để đánh giá hiệu quả của hệ thống.
* Phương pháp thực nghiệm Đánh giá tính khả thi và hiệu quả của mô hình ứng dụng DID. Thực hiện các kịch bản thực nghiệm để kiểm tra khả năng quản lý và xác thực danh tính của DID. Thu thập và phân tích dữ liệu về độ tin cậy, và bảo mật của hệ thống. Đánh giá thực tiễn khả năng triển khai DID trong các hệ thống hiện đại.
* Phương pháp đánh giá và đề xuất: Đưa ra đánh giá toàn diện về hiệu quả và thách thức của DID. Tổng hợp kết quả nghiên cứu và thực nghiệm. Đề xuất các giải pháp cải tiến và hướng ứng dụng mở rộng của DID. Đánh giá khả năng ứng dụng DID trong các lĩnh vực như thương mại điện tử, tài chính, và giáo dục. Định hướng nghiên cứu và phát triển trong tương lai.

## **6. Ý nghĩa khoa học và thực tiễn của đề tài**

Ý nghĩa khoa học:

* Cung cấp cơ sở lý thuyết về mã định danh phi tập trung (DID): Đề tài đóng góp vào việc nghiên cứu và hệ thống hóa các khái niệm liên quan đến DID, một công nghệ tiên tiến trong quản lý danh tính phi tập trung. Nó giúp làm rõ các tiêu chuẩn quốc tế như W3C Decentralized Identifier Specification và các giao thức liên quan như DIDComm.
* Kết hợp DID và mật mã khóa công khai: Đề tài làm sáng tỏ mối liên hệ và cơ chế tích hợp giữa DID và mật mã khóa công khai, tạo tiền đề cho các nghiên cứu mở rộng về bảo mật danh tính và giao dịch trong hệ thống số.
* Mở rộng hiểu biết về blockchain và ứng dụng bảo mật: Thông qua việc nghiên cứu và triển khai DID trên các nền tảng blockchain, đề tài góp phần vào sự phát triển và ứng dụng của blockchain trong lĩnh vực quản lý danh tính.

Ý nghĩa thực tiễn:

* Cải thiện bảo mật và quyền riêng tư: Đề tài đề xuất giải pháp sử dụng DID để tăng cường bảo mật và quyền riêng tư trong hệ thống chứng thực danh tính, giảm thiểu sự phụ thuộc vào các bên trung gian và nguy cơ tấn công mạng.
* Ứng dụng trong các lĩnh vực thực tế: DID có thể được triển khai trong nhiều lĩnh vực như:
  + Thương mại điện tử: Xác thực danh tính khách hàng mà không cần tiết lộ thông tin nhạy cảm.
  + Tài chính: Quản lý danh tính trong các giao dịch ngân hàng và tài sản kỹ thuật số.
  + Giáo dục: Định danh sinh viên và chứng thực bằng cấp.
  + Y tế: Quản lý hồ sơ bệnh nhân và đảm bảo tính riêng tư trong chia sẻ dữ liệu.
* Tạo cơ sở cho các hệ thống phi tập trung: DID mở ra khả năng xây dựng các hệ thống quản lý danh tính phi tập trung, linh hoạt hơn, phù hợp với xu hướng chuyển đổi số và phát triển công nghệ.
* Thúc đẩy đổi mới công nghệ: Kết quả của đề tài có thể là tiền đề cho việc nghiên cứu và phát triển các hệ thống định danh số hiện đại, đáp ứng nhu cầu ngày càng cao về bảo mật và quyền riêng tư trong kỷ nguyên số.

## **7. Cấu trúc báo cáo đồ án tốt nghiệp**

# **CHƯƠNG 1. TỔNG QUAN VỀ QUẢN LÝ DANH TÍNH**

## **1.1. Khái niệm về quản lý danh tính**

Quản lý danh tính (Identity Management - IdM) là một tập hợp các quy trình, chính sách, công nghệ và công cụ được sử dụng để quản lý thông tin danh tính số của các cá nhân, tổ chức hoặc thiết bị trong một hệ thống. Quản lý danh tính không chỉ liên quan đến việc lưu trữ và xác minh danh tính mà còn đảm bảo rằng danh tính này được sử dụng đúng cách trong các hoạt động tương tác, giao dịch hoặc truy cập hệ thống.

Cốt lõi của quản lý danh tính là việc xác định "ai" hoặc "cái gì" đang truy cập vào tài nguyên hoặc dịch vụ, và quản lý quyền truy cập này dựa trên danh tính đã được xác minh.

Quản lý danh tính đóng vai trò quan trọng trong việc đảm bảo bảo mật, tính minh bạch và hiệu quả của các hệ thống thông tin hiện đại. Những lợi ích và vai trò chính bao gồm:

* Bảo mật hệ thống và dữ liệu: Quản lý danh tính giúp xác định và xác thực người dùng hoặc thiết bị, từ đó ngăn chặn các truy cập trái phép và bảo vệ thông tin nhạy cảm.
* Tăng cường quyền riêng tư: Bằng cách quản lý danh tính đúng cách, thông tin cá nhân có thể được bảo vệ trước sự lạm dụng hoặc vi phạm.
* Hỗ trợ trải nghiệm người dùng: Các hệ thống quản lý danh tính tốt giúp người dùng truy cập dịch vụ một cách nhanh chóng, tiện lợi mà không làm mất đi tính bảo mật.
* Quản lý quyền truy cập: Quản lý danh tính không chỉ đảm bảo xác thực mà còn điều phối quyền truy cập tài nguyên hoặc dữ liệu dựa trên vai trò, quyền hạn, và chính sách đã thiết lập.
* Cần thiết cho các ứng dụng phân tán: Trong các hệ thống đa nền tảng hoặc dựa trên đám mây, quản lý danh tính là nền tảng để đảm bảo tính nhất quán và an toàn cho người dùng.

Danh tính (Identity): Danh tính là tập hợp các thuộc tính hoặc thông tin độc nhất dùng để nhận diện một cá nhân, tổ chức, hoặc thiết bị trong một hệ thống. Ví dụ: email, số điện thoại, mã nhân viên, hoặc các định danh số (Digital Identifier).

Xác thực (Authentication): Xác thực là quá trình kiểm tra và xác minh rằng một thực thể (người, tổ chức, hoặc thiết bị) thực sự là người/thiết bị mà họ tuyên bố. Các phương thức xác thực phổ biến bao gồm: mật khẩu, sinh trắc học (vân tay, khuôn mặt), hoặc mã OTP.

Ủy quyền (Authorization): Ủy quyền là quá trình xác định xem một thực thể được phép thực hiện những hành động hoặc truy cập vào các tài nguyên nào trong hệ thống. Ủy quyền thường xảy ra sau khi danh tính đã được xác thực thành công.

## **1.2. Tiến trình và vòng đời quản lý danh tính**

Quản lý danh tính bao gồm một chuỗi các hoạt động được thực hiện để đảm bảo rằng danh tính được thu thập, lưu trữ, sử dụng, và xóa bỏ một cách an toàn và có tổ chức. Các bước chính trong tiến trình này bao gồm:

* Thu thập và tạo danh tính: Giai đoạn này bao gồm việc đăng ký danh tính của người dùng, thiết bị hoặc tổ chức. Thông tin cần thiết như tên, địa chỉ email, số điện thoại hoặc các định danh khác được thu thập. Trong hệ thống số, quá trình này thường yêu cầu cung cấp thêm các phương tiện xác thực như mật khẩu hoặc dữ liệu sinh trắc học.
* Lưu trữ danh tính: Thông tin danh tính được lưu trữ trong cơ sở dữ liệu hoặc sổ cái phân tán (trong trường hợp sử dụng công nghệ blockchain). Yêu cầu lưu trữ phải đảm bảo tính toàn vẹn, an toàn, và khả năng bảo vệ trước các truy cập trái phép.
* Sử dụng danh tính: Danh tính được sử dụng trong các hoạt động như xác thực người dùng, ủy quyền truy cập tài nguyên, hoặc thực hiện các giao dịch. Việc sử dụng danh tính phải tuân theo các chính sách bảo mật để ngăn chặn lạm dụng hoặc vi phạm quyền riêng tư.
* Xóa danh tính: Khi danh tính không còn cần thiết, nó phải được xóa hoặc ẩn danh (anonymized) theo các quy định bảo mật, nhằm đảm bảo rằng dữ liệu cá nhân không bị lạm dụng.

Vòng đời của một danh tính mô tả toàn bộ các giai đoạn mà danh tính trải qua trong hệ thống, từ khi được tạo ra cho đến khi bị hủy bỏ. Các giai đoạn chính bao gồm:

* Đăng ký (Registration): Đây là bước đầu tiên trong vòng đời danh tính, nơi danh tính được tạo ra và đưa vào hệ thống thông qua quy trình đăng ký. Người dùng cung cấp thông tin cần thiết và có thể nhận được một định danh duy nhất.
* Kích hoạt (Activation): Sau khi đăng ký, danh tính được kích hoạt để bắt đầu sử dụng trong hệ thống. Quá trình kích hoạt có thể bao gồm xác minh danh tính, như nhập mã OTP hoặc xác nhận qua email.
* Sử dụng (Utilization): Giai đoạn này diễn ra khi danh tính được sử dụng để thực hiện các hoạt động như đăng nhập, xác thực, hoặc giao dịch. Quyền truy cập và hành động của danh tính được quản lý và kiểm soát theo các quy tắc đã định.
* Hủy bỏ (Deactivation/Deletion): Khi danh tính không còn cần thiết hoặc không hợp lệ (ví dụ: người dùng rời khỏi hệ thống), danh tính sẽ bị hủy bỏ. Quá trình này đảm bảo danh tính không còn tồn tại trong hệ thống hoặc bị sử dụng sai mục đích.

Tiến trình quản lý danh tính và vòng đời danh tính có mối quan hệ chặt chẽ, bổ trợ cho nhau trong việc quản lý danh tính hiệu quả:

* Sự tương tác: Các bước trong tiến trình quản lý danh tính (thu thập, lưu trữ, sử dụng, xóa bỏ) là các hoạt động cụ thể diễn ra ở từng giai đoạn trong vòng đời danh tính (đăng ký, kích hoạt, sử dụng, hủy bỏ). Ví dụ, "đăng ký" tương ứng với bước "thu thập và tạo danh tính", còn "hủy bỏ" gắn với "xóa danh tính".
* Quản lý liên tục: Tiến trình quản lý danh tính giúp theo dõi và duy trì vòng đời danh tính, đảm bảo rằng các danh tính luôn được kiểm soát chặt chẽ từ khi tạo đến khi hủy bỏ.
* Bảo mật và tuân thủ: Kết hợp tiến trình và vòng đời danh tính giúp duy trì bảo mật, tuân thủ các quy định pháp lý và chính sách quyền riêng tư trong toàn bộ vòng đời danh tính.

## **1.3. Mức đảm bảo trong quản lý danh tính**

Mức đảm bảo (Level of Assurance - LoA) là thước đo mức độ tin cậy và an toàn của các quy trình quản lý danh tính trong việc xác định danh tính và cấp quyền truy cập. LoA giúp đánh giá khả năng một hệ thống quản lý danh tính có thể ngăn chặn giả mạo, bảo vệ thông tin cá nhân và đảm bảo chỉ những người dùng hợp lệ mới được truy cập tài nguyên.

LoA được xác định dựa trên các yếu tố như:

* Phương pháp xác thực được sử dụng (mật khẩu, OTP, sinh trắc học).
* Quy trình cấp và quản lý danh tính.
* Mức độ an toàn của thông tin lưu trữ và truyền tải.

Mức đảm bảo trong quản lý danh tính thường được phân thành nhiều cấp độ, phù hợp với mức độ nhạy cảm của tài nguyên và dữ liệu. Một số mô hình tiêu chuẩn như NIST SP 800-63 (Digital Identity Guidelines) chia LoA thành các cấp độ chính sau:

* LoA 1: Xác thực cơ bản (Basic Assurance): Đặc điểm là yêu cầu tối thiểu, thường sử dụng mật khẩu hoặc thông tin đăng nhập cơ bản. Không có biện pháp bảo vệ mạnh mẽ trước các mối đe dọa. Ứng dụng trong các hệ thống không đòi hỏi tính bảo mật cao, như diễn đàn hoặc trang web cộng đồng.
* LoA 2: Xác thực nâng cao (Moderate Assurance): Đặc điểm là sử dụng các phương pháp xác thực hai yếu tố (2FA) như OTP, email xác minh hoặc ứng dụng xác thực. Bảo vệ chống lại giả mạo ở mức trung bình. Ứng dụng trong các dịch vụ ngân hàng trực tuyến, tài khoản email.
* LoA 3: Xác thực mạnh (High Assurance): Đặc điểm là áp dụng các phương pháp xác thực sinh trắc học (vân tay, khuôn mặt) hoặc chứng chỉ kỹ thuật số. Đảm bảo mức bảo mật cao với các dữ liệu nhạy cảm. Ứng dụng trong hệ thống quản lý tài chính, y tế hoặc dữ liệu nhạy cảm.
* LoA 4: Xác thực rất cao (Very High Assurance): Đặc điểm là kết hợp nhiều yếu tố xác thực mạnh mẽ với khả năng chống giả mạo tối đa. Cơ chế bảo mật nâng cao, như sử dụng token phần cứng hoặc blockchain. Ứng dụng trong các hệ thống chính phủ, quân đội, hoặc cơ sở dữ liệu bảo mật cao.

Việc lựa chọn mức đảm bảo phù hợp phụ thuộc vào các tiêu chí sau:

* Mức độ nhạy cảm của dữ liệu: Dữ liệu càng nhạy cảm thì yêu cầu mức đảm bảo càng cao. Ví dụ: Dữ liệu cá nhân cơ bản cần LoA 2, trong khi dữ liệu tài chính yêu cầu LoA 3 hoặc 4.
* Mức độ rủi ro: Đánh giá khả năng xảy ra các mối đe dọa như tấn công mạng, giả mạo danh tính hoặc lạm dụng quyền truy cập. Rủi ro càng cao, hệ thống càng cần áp dụng các LoA cao hơn.
* Phương pháp xác thực: LoA được xác định bởi độ tin cậy của các phương pháp xác thực được sử dụng, từ mật khẩu cơ bản đến sinh trắc học và token phần cứng.
* Quy trình quản lý: Các quy trình cấp phát, lưu trữ và sử dụng danh tính phải tuân thủ các tiêu chuẩn bảo mật để đảm bảo tính toàn vẹn.
* Ứng dụng thực tiễn: Mức đảm bảo cần phù hợp với từng trường hợp sử dụng thực tế, tránh gây phiền hà không cần thiết cho người dùng. Ví dụ: Một hệ thống thương mại điện tử thông thường có thể chọn LoA 2, trong khi hệ thống giao dịch tiền số cần LoA 3 hoặc 4.

Áp dụng mức đảm bảo (LoA):

* Việc áp dụng LoA cần cân nhắc giữa yếu tố bảo mật và trải nghiệm người dùng. Hệ thống phải đáp ứng các yêu cầu bảo mật mà không làm phức tạp quá trình đăng nhập hoặc truy cập.
* LoA không chỉ áp dụng cho các tổ chức lớn mà còn hữu ích cho các doanh nghiệp nhỏ và vừa, nơi các mức bảo mật cơ bản hoặc nâng cao có thể bảo vệ tài nguyên hiệu quả.

## **1.4. Các mô hình và ứng dụng quản lý danh tính**

Mô hình quản lý danh tính tập trung:

* Khái niệm:
  + Trong mô hình này, danh tính của người dùng được quản lý bởi một hệ thống hoặc tổ chức trung tâm. Tất cả thông tin danh tính như tên người dùng, mật khẩu, và các dữ liệu liên quan được lưu trữ trong cơ sở dữ liệu tập trung.
* Đặc điểm:
  + Dữ liệu dễ dàng truy cập và quản lý từ một nguồn duy nhất.
  + Đòi hỏi một hệ thống bảo mật mạnh mẽ để ngăn ngừa các cuộc tấn công hoặc rò rỉ dữ liệu.
* Ưu điểm:
  + Dễ dàng triển khai và quản lý.
  + Thích hợp cho các tổ chức hoặc doanh nghiệp nhỏ.
* Nhược điểm:
  + Rủi ro cao khi hệ thống bị tấn công (single point of failure).
  + Quyền kiểm soát danh tính thuộc về tổ chức, không phải người dùng.

Mô hình quản lý danh tính phân tán:

* Khái niệm:
  + Trong mô hình này, thông tin danh tính được quản lý trên các hệ thống phi tập trung, thường dựa trên công nghệ blockchain hoặc sổ cái phân tán.
* Đặc điểm:
  + Người dùng tự kiểm soát danh tính của mình thông qua các mã định danh phi tập trung (Decentralized Identifiers - DID).
  + Không cần phụ thuộc vào một cơ quan trung tâm.
* Ưu điểm:
  + Tăng cường bảo mật và quyền riêng tư.
  + Khó bị tấn công hoặc giả mạo do thông tin được phân tán.
* Nhược điểm:
  + Cần công nghệ phức tạp để triển khai.
  + Khả năng tương thích với các hệ thống hiện tại còn hạn chế.

Mô hình liên minh danh tính (Federated Identity):

* Khái niệm:
  + Mô hình liên minh danh tính cho phép người dùng sử dụng cùng một danh tính để truy cập nhiều hệ thống hoặc dịch vụ khác nhau, thường qua các nhà cung cấp danh tính (Identity Providers - IdPs).
* Đặc điểm:
  + Người dùng có thể đăng nhập vào các dịch vụ khác nhau bằng một bộ thông tin đăng nhập duy nhất.
  + Một số giao thức phổ biến: OAuth, OpenID Connect, SAML.
* Ưu điểm:
  + Cải thiện trải nghiệm người dùng nhờ khả năng đăng nhập một lần (Single Sign-On - SSO).
  + Giảm gánh nặng quản lý danh tính cho từng hệ thống riêng lẻ.
* Nhược điểm:
  + Nếu nhà cung cấp danh tính bị tấn công, toàn bộ hệ thống liên minh có thể bị ảnh hưởng.
  + Phụ thuộc vào bên thứ ba để cung cấp dịch vụ danh tính.

Ứng dụng quản lý danh tính trong thực tế: Quản lý danh tính có nhiều ứng dụng trong các lĩnh vực khác nhau, đóng vai trò quan trọng trong việc bảo mật và tối ưu hóa trải nghiệm người dùng:

Ngân hàng và tài chính:

* + Xác thực người dùng khi truy cập dịch vụ ngân hàng trực tuyến hoặc ví điện tử.
  + Bảo mật giao dịch thông qua các hệ thống xác thực mạnh mẽ như sinh trắc học hoặc token phần cứng.
  + Quản lý danh tính khách hàng trong các hệ thống KYC (Know Your Customer).

Giáo dục:

* + Quản lý danh tính sinh viên để truy cập các hệ thống học trực tuyến hoặc hệ thống quản lý học vụ.
  + Cấp phát và xác thực bằng cấp, chứng chỉ kỹ thuật số thông qua các giải pháp DID.

Y tế:

* + Quản lý hồ sơ bệnh nhân trong các hệ thống y tế.
  + Cung cấp quyền truy cập an toàn cho các bác sĩ, y tá và bệnh nhân vào dữ liệu y tế.
  + Tăng cường quyền riêng tư và bảo mật khi chia sẻ thông tin nhạy cảm.

Thương mại điện tử:

* + Xác thực danh tính người dùng khi thực hiện giao dịch trực tuyến.
  + Quản lý thông tin tài khoản khách hàng trong các hệ thống loyalty programs (chương trình khách hàng thân thiết).

Chính phủ điện tử:

* + Xác thực danh tính công dân để truy cập các dịch vụ công như khai thuế, cấp giấy phép, hoặc bỏ phiếu điện tử.
  + Sử dụng quản lý danh tính số để giảm thiểu gian lận và tăng hiệu quả xử lý hồ sơ.

## **1.5. Tồn tại và thách thức trong quản lý danh tính số**

Các vấn đề về bảo mật và quyền riêng tư

* Nguy cơ tấn công mạng: Hệ thống quản lý danh tính số là mục tiêu của các cuộc tấn công như đánh cắp thông tin cá nhân, giả mạo danh tính, và tấn công từ chối dịch vụ (DDoS). Nếu dữ liệu danh tính bị lộ, kẻ xấu có thể sử dụng thông tin này để thực hiện các hành vi gian lận hoặc gây tổn hại.
* Rủi ro tập trung hóa: Trong các mô hình quản lý danh tính tập trung, việc lưu trữ toàn bộ thông tin người dùng trong một cơ sở dữ liệu duy nhất dễ dẫn đến các vấn đề về bảo mật nếu hệ thống bị xâm nhập.
* Mất quyền kiểm soát của người dùng: Người dùng không có toàn quyền quản lý hoặc quyết định cách sử dụng danh tính của mình trong các hệ thống tập trung hoặc liên minh danh tính.
* Quyền riêng tư không được đảm bảo: Một số hệ thống quản lý danh tính thu thập quá nhiều thông tin cá nhân không cần thiết, gây lo ngại về lạm dụng dữ liệu và vi phạm quyền riêng tư của người dùng.

Khó khăn trong việc triển khai ở môi trường đa nền tảng

* Không đồng bộ về công nghệ: Mỗi nền tảng hoặc hệ thống sử dụng các giao thức và chuẩn quản lý danh tính khác nhau, dẫn đến khó khăn trong việc tích hợp và tương thích giữa các hệ thống. Ví dụ: OAuth, SAML, và OpenID Connect đều có các cấu trúc khác nhau, gây phức tạp trong việc áp dụng trên diện rộng.
* Chi phí triển khai: Việc áp dụng các mô hình quản lý danh tính tiên tiến như DID hoặc liên minh danh tính đòi hỏi đầu tư lớn về hạ tầng công nghệ và nhân lực.
* Thiếu tiêu chuẩn chung: Hiện nay, chưa có một tiêu chuẩn duy nhất được áp dụng toàn cầu cho quản lý danh tính số, khiến việc triển khai gặp nhiều khó khăn và không nhất quán.
* Thách thức về trải nghiệm người dùng: Các hệ thống bảo mật phức tạp như xác thực nhiều yếu tố (MFA) có thể làm giảm sự tiện lợi, dẫn đến việc người dùng bỏ qua hoặc tìm cách đơn giản hóa quy trình, làm giảm hiệu quả bảo mật.

Những rủi ro khi danh tính số bị lạm dụng:

* Giả mạo danh tính: Kẻ xấu có thể sử dụng danh tính số bị đánh cắp để giả mạo người dùng thực hiện các hành vi gian lận như giao dịch tài chính trái phép hoặc chiếm đoạt tài sản.
* Gian lận và lạm dụng dịch vụ: Trong các hệ thống thương mại điện tử hoặc dịch vụ trực tuyến, danh tính số bị lạm dụng có thể dẫn đến tổn thất lớn về tài chính và uy tín cho cả người dùng và tổ chức.
* Rủi ro về pháp lý: Khi danh tính số bị sử dụng cho các mục đích phi pháp, người dùng thật có thể gặp rắc rối với pháp luật nếu không chứng minh được sự liên quan.
* Tác động dài hạn: Một khi danh tính số bị lộ, rất khó để khắc phục hoàn toàn hậu quả. Thông tin cá nhân bị đánh cắp có thể được sử dụng lâu dài, gây ảnh hưởng đến tài chính, uy tín, và sự an toàn của người dùng.

# **CHƯƠNG 2. MÃ ĐỊNH DANH DID**

## **2.1. Danh tính tự chủ**

## **2.2. Mã định danh phi tập trung**

## **2.3. Ứng dụng của mã định danh phi tập trung**

## **2.4. Hệ thống quản lý mã danh tính phi tập trung**

# **CHƯƠNG 3. TRIỂN KHAI HỆ THỐNG QUẢN LÝ MÃ ĐỊNH DANH PHI TẬP TRUNG**

## **3.1. Tổng quan hệ thống**

## **3.2. Triển khai mạng ứng dụng server trên Hyperledger Indy**

## **3.3. Triển khai ứng dụng client trên Hyperledger Aries**

## **3.4. Vận hành hệ thống**

## **3.5. Đánh giá kết quả**

# **KẾT LUẬN**

# **TÀI LIỆU THAM KHẢO**

# **PHỤ LỤC 1**