**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**

[**LỜI CẢM ƠN** 2](#_Toc183950837)

[**CHƯƠNG 1. QUẢN LÝ DANH TÍNH SỐ** 6](#_Toc183950838)

[**1.1. Một số khái niệm** 6](#_Toc183950839)

[1.1.1. Thực thể 6](#_Toc183950840)

[1.1.2. Thuộc tính 6](#_Toc183950841)

[1.1.3. Danh tính 6](#_Toc183950842)

[1.1.4. Mã định danh 6](#_Toc183950843)

[1.1.5. Danh tính số 6](#_Toc183950844)

[**1.2. Tiến trình quản lý danh tính số** 7](#_Toc183950845)

[1.2.1. Định danh 7](#_Toc183950846)

[1.2.2. Xác thực 7](#_Toc183950847)

[1.2.3. Ủy quyền 7](#_Toc183950848)

[**1.3. Các pha trong quản lý danh tính** 7](#_Toc183950849)

[1.3.1. Đăng ký danh tính 7](#_Toc183950850)

[1.3.2. Xác thực danh tính 7](#_Toc183950851)

[1.3.3. Cấp phát và quản lý mã định danh 8](#_Toc183950852)

[1.3.4. Sử dụng danh tính 8](#_Toc183950853)

[1.3.5. Hủy bỏ danh tính 8](#_Toc183950854)

[**1.4. Mức đảm bảo trong quản lý danh tính** 8](#_Toc183950855)

[1.4.1. Identity Assurance Level (IAL) 8](#_Toc183950856)

[1.4.2. Authenticator Assuarance Level (AAL) 8](#_Toc183950857)

[1.4.3. Federation Assuarance Level (FAL) 8](#_Toc183950858)

[**1.5. Hệ thống quản lý danh tính số** 9](#_Toc183950859)

[1.5.1. Kiến trúc hệ thống 9](#_Toc183950860)

[1.5.2. Mô hình hoạt động 9](#_Toc183950861)

[**1.6. Mô hình quản lý danh tính số** 9](#_Toc183950862)

[1.6.1. Mô hình tập trung 9](#_Toc183950863)

[1.6.2. Mô hình liên hiệp 9](#_Toc183950864)

[1.6.3. Mô hình người dùng trung tâm 9](#_Toc183950865)

[1.6.4. Mô hình dựa trên định danh tự chủ 10](#_Toc183950866)

[**1.7. Ứng dụng quản lý danh tính số** 10](#_Toc183950867)

[**1.8. Một số tồn tại quản lý danh tính số** 10](#_Toc183950868)

[**Kết luận chương 1** 10](#_Toc183950869)

[**CHƯƠNG 2. MÃ ĐỊNH DANH PHI TẬP TRUNG (DID)** 11](#_Toc183950870)

[**2.1. Định danh tự chủ** 11](#_Toc183950871)

[2.1.1. Khái niệm 11](#_Toc183950872)

[2.1.2. Kiến trúc hệ thống danh tính tự chủ 11](#_Toc183950873)

[2.1.3. Các thành phần trong hệ thống danh tính tự chủ 11](#_Toc183950874)

[2.1.4. Các layer trong danh tính tự chủ 11](#_Toc183950875)

[**2.2. Mã định danh phi tập trung** 11](#_Toc183950876)

[2.2.1. Khái niệm, cú pháp mã định danh phi tập trung 11](#_Toc183950877)

[2.2.2. Kiến trúc mã định danh phi tập trung 12](#_Toc183950878)

[2.2.3. Ứng dụng DID trong thực tế 12](#_Toc183950879)

[**2.3. Ứng dụng của mã định danh phi tập trung trong VC và VP** 13](#_Toc183950880)

[2.3.1. Verifiable Credentials (VC) 13](#_Toc183950881)

[2.3.2. Verfiable Presentation (VP) 13](#_Toc183950882)

[**2.4. Hệ thống quản lý danh tính phi tập trung** 13](#_Toc183950883)

[2.4.1. Kiến trúc và thành phần hệ thống 13](#_Toc183950884)

[2.4.2. Quá trình quản lý và xác thực danh tính 14](#_Toc183950885)

[2.4.3. Cơ chế bảo mật trong hệ thống 14](#_Toc183950886)

[2.4.4. Ưu điểm và thách thức đối với hệ thống 14](#_Toc183950887)

[**Kết luận chương 2** 14](#_Toc183950888)

[**CHƯƠNG 3. TRIỂN KHAI HỆ THỐNG QUẢN LÝ MÃ ĐỊNH DANH PHI TẬP TRUNG** 14](#_Toc183950889)

[**3.1. Tổng quan hệ thống** 14](#_Toc183950890)

[3.1.1. Mô hình triển khai 14](#_Toc183950891)

[3.1.2. Giới thiệu về công cụ Hyperledger Indy và Hyperledger Aries 14](#_Toc183950892)

[3.1.3. Giới thiệu mạng phi tập trung quản lý danh tính dựa trên Hyperledger Indy 15](#_Toc183950893)

[3.1.4. Giới thiệu ứng dụng Dapp quản lý mã định danh phi tập trung 15](#_Toc183950894)

[**3.2. Triển khai hệ thống quản lý mã định danh phi tập trung dựa trên Hyperledger Indy** 15](#_Toc183950895)

[3.2.1. Cài đặt và cấu hình Hyperledger Indy 15](#_Toc183950896)

[3.2.2. Tạo và quản lý danh tính trên Hyperledger Indy 15](#_Toc183950897)

[3.2.3. Triển khai mạng lên môi trường production 15](#_Toc183950898)

# **CHƯƠNG 1. QUẢN LÝ DANH TÍNH SỐ**

## **1.1. Một số khái niệm**

### **1.1.1. Thực thể**

### **1.1.2. Thuộc tính**

### **1.1.3. Danh tính**

### **1.1.4. Mã định danh**

### **1.1.5. Danh tính số**

## **1.2. Tiến trình quản lý danh tính số**

### **1.2.1. Định danh**

### **1.2.2. Xác thực**

### **1.2.3. Ủy quyền**

## **1.3. Các pha trong quản lý danh tính**

### **1.3.1. Đăng ký danh tính**

### **1.3.2. Xác thực danh tính**

### **1.3.3. Cấp phát và quản lý mã định danh**

### **1.3.4. Sử dụng danh tính**

### **1.3.5. Hủy bỏ danh tính**

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

### **1.4.1. Identity Assurance Level (IAL)**

### **1.4.2. Authenticator Assuarance Level (AAL)**

### **1.4.3. Federation Assuarance Level (FAL)**

## **1.5. Hệ thống quản lý danh tính số**

### **1.5.1. Kiến trúc hệ thống**

### **1.5.2. Mô hình hoạt động**

## **1.6. Mô hình quản lý danh tính số**

### **1.6.1. Mô hình tập trung**

### **1.6.2. Mô hình liên hiệp**

### **1.6.3. Mô hình người dùng trung tâm**

### **1.6.4. Mô hình dựa trên định danh tự chủ**

## **1.7. Ứng dụng quản lý danh tính số**

## **1.8. Một số tồn tại quản lý danh tính số**

## **Kết luận chương 1**

# **CHƯƠNG 2. MÃ ĐỊNH DANH PHI TẬP TRUNG (DID)**

## **2.1. Định danh tự chủ**

### **2.1.1. Khái niệm**

### **2.1.2. Kiến trúc hệ thống danh tính tự chủ**

### **2.1.3. Các thành phần trong hệ thống danh tính tự chủ**

### **2.1.4. Các layer trong danh tính tự chủ**

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

### **2.2.1. Khái niệm, cú pháp mã định danh phi tập trung**

### **2.2.2. Kiến trúc mã định danh phi tập trung**

*2.2.2.1. DID Document*

*2.2.2.2. DID Actions*

*2.2.2.3. VERIFIABLE DATA REGISTRY*

### **2.2.3. Ứng dụng DID trong thực tế**

## **2.3. Ứng dụng của mã định danh phi tập trung trong VC và VP**

### **2.3.1. Verifiable Credentials (VC)**

*2.3.1.1. Khái niệm*

*2.3.1.2. Các thành phần*

*2.3.1.3. Mô hình hoạt động*

### **2.3.2. Verfiable Presentation (VP)**

*2.3.2.1. Khái niệm*

*2.3.2.2. Các thành phần*

*2.3.2.3. Mô hình hoạt động*

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

### **2.4.1. Kiến trúc và thành phần hệ thống**

### **2.4.2. Quá trình quản lý và xác thực danh tính**

### **2.4.3. Cơ chế bảo mật trong hệ thống**

### **2.4.4. Ưu điểm và thách thức đối với hệ thống**

## **Kết luận chương 2**

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

## **3.1. Tổng quan hệ thống**

### **3.1.1. Mô hình triển khai**

### **3.1.2. Giới thiệu về công cụ Hyperledger Indy và Hyperledger Aries**

### **3.1.3. Giới thiệu mạng phi tập trung quản lý danh tính dựa trên Hyperledger Indy**

### **3.1.4. Giới thiệu ứng dụng Dapp quản lý mã định danh phi tập trung**

## **3.2. Triển khai hệ thống quản lý mã định danh phi tập trung dựa trên Hyperledger Indy**

### **3.2.1. Cài đặt và cấu hình Hyperledger Indy**

### **3.2.2. Tạo và quản lý danh tính trên Hyperledger Indy**

### **3.2.3. Triển khai mạng lên môi trường production**