**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC NHA TRANG**



**CAO VIẾT THẮNG**

**NGHIÊN CỨU VÀ ỨNG DỤNG CÔNG NGHỆ**

**BLOCKCHAIN TRONG QUẢN LÝ VÀ XÁC MINH**

**VĂN BẰNG CHỨNG CHỈ**

**BÁO CÁO ĐỀ TÀI LUẬN VĂN THẠC SĨ**

**Ngành đào tạo: Công nghệ thông tin**

**Mã ngành: 8480201**

**KHÁNH HÒA - 2022**

# QUYẾT ĐỊNH GIAO ĐỀ TÀI

# CAM ĐOAN CỦA HỌC VIÊN

Tôi cam đoan rằng luận văn tốt nghiệp về “Nghiên cứu và ứng dụng công nghệ Blockchain trong quản lý và xác minh văn bằng chứng chỉ” là công trình nghiên cứu của chính tôi. Tất cả các tài liệu tham khảo được sử dụng trong luận văn đã được trình bày rõ ràng trong phần tài liệu tham khảo. Các kết quả và số liệu trình bày trong luận văn là hoàn toàn chính xác, nếu có sai sót, tôi sẽ chịu trách nhiệm và chấp nhận mọi hình thức kỷ luật từ bộ môn và nhà trường.

Khánh Hòa, ngày …… tháng ……… năm 2022

Sinh viên thực hiện

*Cao Viết Thắng*

# LỜI CẢM ƠN

Tôi muốn bày tỏ lòng biết ơn chân thành đến khoa Sau Đại học của Trường Đại học Nha Trang đã tạo điều kiện thuận lợi cho tôi hoàn thành đề tài luận văn tốt nghiệp này.

Ngoài ra, tôi cũng muốn gửi lời cảm ơn tới các thầy cô trong khoa Công nghệ Thông tin đã nhiệt tình dạy dỗ và trang bị cho tôi những kiến thức bổ ích trong những năm học qua, giúp tôi có nền tảng vững chắc để hoàn thành luận văn này. Đặc biệt, tôi muốn cảm ơn thầy TS. Nguyễn Đình Hưng - giảng viên khoa Công nghệ Thông tin đã hướng dẫn và đóng góp ý kiến nhiệt tình giúp tôi hoàn thành tốt luận văn tốt nghiệp.

Tuy nhiên, tôi nhận thức được rằng luận văn tốt nghiệp của tôi vẫn còn một số thiếu sót và hạn chế. Tôi rất mong nhận được sự thông cảm và góp ý tận tình từ quý thầy cô và các bạn để tôi có thể cải thiện hơn trong tương lai.

Một lần nữa, tôi xin chân thành cảm ơn!

# MỤC LỤC

Đề mục Trang

Trang bìa i

[QUYẾT ĐỊNH GIAO ĐỀ TÀI ii](#_Toc130032829)

[CAM ĐOAN CỦA HỌC VIÊN iii](#_Toc130032830)

[LỜI CẢM ƠN iv](#_Toc130032831)

[MỤC LỤC v](#_Toc130032832)

[DANH SÁCH HÌNH VẼ viii](#_Toc130032833)

[DANH SÁCH BẢNG BIỂU x](#_Toc130032834)

[DANH SÁCH CÁC TỪ VIẾT TẮT xi](#_Toc130032835)

[MỞ ĐẦU 12](#_Toc130032836)

[ Lý do chọn đề tài 12](#_Toc130032837)

[ Mục đích, đối tượng, chủ thể và phạm vi nghiên cứu 13](#_Toc130032838)

[ Phương pháp nghiên cứu 13](#_Toc130032839)

[ Ý nghĩa khoa học và thực tiễn của luận văn 13](#_Toc130032840)

[CHƯƠNG 1. GIỚI THIỆU CÔNG NGHỆ BLOCKCHAIN 14](#_Toc130032841)

[1.1. Giới thiệu BlockChain 14](#_Toc130032842)

[1.2. Nền tảng lý thuyết 15](#_Toc130032843)

[1.2.1. Hàm băm 15](#_Toc130032844)

[1.2.2. Chữ ký số 17](#_Toc130032845)

[1.3. Các kỹ thuật chính của BlockChain 18](#_Toc130032846)

[1.3.1. Cấu trúc phi tập trung 19](#_Toc130032847)

[1.3.2. Tính toán tin cậy 21](#_Toc130032848)

[1.3.3. Bằng chứng công việc 21](#_Toc130032849)

[1.4. Tính chất của Blockchain 21](#_Toc130032850)

[1.4.1. Cơ chế đồng thuận phân quyền (decentralized consensus) 21](#_Toc130032851)

[1.4.2. Bảo trì tập thể (collective maintenance) 21](#_Toc130032852)

[1.4.3. Tính bảo mật và độ tin cậy 22](#_Toc130032853)

[1.4.4. Mã nguồn mở 22](#_Toc130032854)

[1.5. Phân loại các hệ thống Blockchain 22](#_Toc130032855)

[1.6. Các ứng dụng điển hình của công nghệ Blockchain 23](#_Toc130032856)

[1.6.1. Ứng dụng Blockchain trong tiền số 23](#_Toc130032857)

[1.6.2. Ứng dụng Blockchain trong hợp đồng thông minh (Smart Contract) 23](#_Toc130032858)

[1.6.3. Một số ứng dụng nổi bật khác 24](#_Toc130032859)

[CHƯƠNG 2. TỔNG QUAN QUẢN LÝ VÀ XÁC MINH VĂN BẰNG, CHỨNG CHỈ 26](#_Toc130032860)

[2.1. Giới thiệu công tác quản lý và xác minh văn bằng, chứng chỉ 26](#_Toc130032861)

[2.1.1. Văn bằng, chứng chỉ là gì? 26](#_Toc130032862)

[2.1.2. Quy trình liên quan tới văn bằng, chứng chỉ 26](#_Toc130032863)

[2.1.3. Một số mô hình quản lý và xác minh văn bằng chứng chỉ không áp dụng công nghệ BlockChain 27](#_Toc130032864)

[2.1.4. Mô hình quản lý và xác minh văn bằng chứng chỉ sử dụng Blockchain 29](#_Toc130032865)

[2.2. Tình hình và các nghiên cứu liên quan 31](#_Toc130032866)

[2.2.1. Blockcerts 31](#_Toc130032867)

[2.2.2. BTCert 33](#_Toc130032868)

[CHƯƠNG 3. ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN TRONG QUẢN LÝ VÀ XÁC MINH VĂN BẰNG, CHỨNG CHỈ 34](#_Toc130032869)

[3.1. Thiết kế hệ thống CertsChain 34](#_Toc130032870)

[3.1.1. Định nghĩa bài toán 34](#_Toc130032871)

[3.1.2. Mô hình thực hiện 35](#_Toc130032872)

[3.1.3. Sơ đồ phân rã chức năng 36](#_Toc130032873)

[3.1.4. Cơ sở dữ liệu 42](#_Toc130032874)

[3.2. Xây dựng hệ thống CertsChain 43](#_Toc130032875)

[3.2.1. Môi trường triển khai và công cụ phát triển 43](#_Toc130032876)

[3.2.2. Xây dựng Blockchain của hệ thống 44](#_Toc130032877)

[3.2.3. Xây dựng hệ thống API 46](#_Toc130032878)

[3.3. Thực nghiệm hệ thống CertsChain 48](#_Toc130032879)

[3.3.1. Người dùng loại Issuer 49](#_Toc130032880)

[3.3.2. Người dùng loại Holder 55](#_Toc130032881)

[3.3.3. Người dùng loại Verifier 57](#_Toc130032882)

[3.3.4. Trang Verify Certificate 58](#_Toc130032883)

[CHƯƠNG 4. KẾT LUẬN VÀ KIẾN NGHỊ 60](#_Toc130032884)

[4.1. Kết quả đạt được 60](#_Toc130032885)

[4.2. Hạn chế của đề tài 60](#_Toc130032886)

[4.3. Hướng phát triển của đề tài 60](#_Toc130032887)

[4.4. Đề nghị ý kiến 60](#_Toc130032888)

[TÀI LIỆU THAM KHẢO 61](#_Toc130032889)

# DANH SÁCH HÌNH VẼ

[Hình 1. Mô hình thực hiện chữ ký số 17](#_Toc130026270)

[Hình 2. Cấu trúc dữ liệu của Blockchain 18](#_Toc130026271)

[Hình 3. Cấu trúc của block gốc trong Blockchain 19](#_Toc130026272)

[Hình 4. Mô hình thực hiện của hệ thống 35](#_Toc130026273)

[Hình 5. Sơ đồ phân rã chức năng Issuer 38](#_Toc130026274)

[Hình 6. Sơ đồ phân rã chức năng Holder 40](#_Toc130026275)

[Hình 7. Sơ đồ phân rã chức năng Verifier 41](#_Toc130026276)

[Hình 8. Cơ sở dữ liệu của hệ thống CertsChain 42](#_Toc130026277)

[Hình 9. Vue.js 43](#_Toc130026278)

[Hình 10. NodeJS - Express 44](#_Toc130026279)

[Hình 11. Trang chủ 48](#_Toc130026280)

[Hình 12. Trang đăng nhập 48](#_Toc130026281)

[Hình 13. Trang Profile của Issuer 49](#_Toc130026282)

[Hình 14. Trang Users của Issuer 49](#_Toc130026283)

[Hình 15. Popup tạo mới User 50](#_Toc130026284)

[Hình 16. Popup cập nhật User 50](#_Toc130026285)

[Hình 17. Popup Cập nhật danh sách danh sách Cources của User tham gia 50](#_Toc130026286)

[Hình 18. Trang Schools and Cources của Issuer 51](#_Toc130026287)

[Hình 19. Popup tạo mới School and Cource 51](#_Toc130026288)

[Hình 20. Popup cập nhật School and Cource 52](#_Toc130026289)

[Hình 21. Trang Certificates của Issuer 52](#_Toc130026290)

[Hình 22. Popup tạo mới Certificate 53](#_Toc130026291)

[Hình 23. Cấp phát VBCC cho học viên trong khóa học 53](#_Toc130026292)

[Hình 24. Mẫu văn bằng chứng chỉ của CertsChain 54](#_Toc130026293)

[Hình 25. Trang Certificate Requests của Issuer 54](#_Toc130026294)

[Hình 26. Trang Profile của Holder 55](#_Toc130026295)

[Hình 27. Trang danh sách Certificate của Holder 55](#_Toc130026296)

[Hình 28. Popup chia sẻ thông tin Certificate 56](#_Toc130026297)

[Hình 29. Trang Certificate Requests của Holder 56](#_Toc130026298)

[Hình 30. Popup tạo mới yêu cầu cấp phát VBCC 56](#_Toc130026299)

[Hình 31. Danh sách tất cả các User trong hệ thống 57](#_Toc130026300)

[Hình 32. Trang chi tiết User 57](#_Toc130026301)

[Hình 33. Danh sách tất cả các certificate trong hệ thống 58](#_Toc130026302)

[Hình 34. Trang xác minh VBCC 58](#_Toc130026303)

# DANH SÁCH BẢNG BIỂU

[Bảng 1. Các chức năng của Issuer 36](#_Toc130026304)

[Bảng 2. Các chức năng của Holder 39](#_Toc130026305)

[Bảng 3. Các chức năng của Verifier 41](#_Toc130026306)

[Bảng 4. Các API của hệ thống CertsChain 46](#_Toc130026307)

# DANH SÁCH CÁC TỪ VIẾT TẮT

**Từ viết tắt Giải thích**

VBCC Văn bằng, chứng chỉ

Certificate VBCC

Issuer Đơn vị phát hành VBCC

Holder Học viên hay Người nhận VBCC

Verifier Đơn vị cần xác minh VBCC

PDF Portable Document Format

App Application

API Application Programming Interface

URL Uniform Resource Locator

QR Mã QR

# MỞ ĐẦU

## Lý do chọn đề tài

Văn bằng được hiểu là những giấy tờ chứng nhận quá trình tốt nghiệp giữa các cấp học. Chứng chỉ là những bằng cấp, văn bằng chứng minh do cơ quan giáo dục cung cấp để công nhận một trình độ học vấn nhất định, có giá trị pháp lý trong thời gian dài. Văn bằng chứng chỉ là khái niệm rất quen thuộc trong ngành giáo dục hiện nay. Và với các ứng viên thì đây được xem là yếu tố quan trọng khi dựa vào đó để các bạn có thể nắm bắt cơ hội cho mình với việc làm hấp dẫn.

Tuy Inhiên, Ihiện Inay, Icác Ivăn Ibằng Ivà Ichứng Ichỉ Ichủ Iyếu Iđược Icấp Idưới Idạng Itài Iliệu Ivật Ilý I(giấy, Ipolymer, I...) Ibởi Icác Icơ Isở Iđào Itạo. ITuy Inhiên, Iphương Ithức Inày Igặp Inhiều Ibất Itiện Inhư Itốn Ikhông Igian Ilưu Itrữ, Idễ Imất Imát Ivà Ihư Ihỏng, Ivà Iđặc Ibiệt Ilà Idễ Ibị Ilàm Igiả. IViệc Ixác Iminh Ibằng Icấp Ivà Ichứng Ichỉ Icũng Irất Itốn Ithời Igian. IDo Iđó, Inếu Icó Icách Ixác Iminh Ibằng Icấp Ivà Ichứng Ichỉ Imột Icách Ichính Ixác Ivà Inhanh Ichóng, Ithì Ikhông Icòn Icơ Ihội Icho Ibằng Icấp Ivà Ichứng Ichỉ Igiả Itồn Itại.

Vào năm 2018, công nghệ Blockchain ra đời, và được ứng dụng rộng rãi vào các lĩnh vực trong đời sống. Đối với công tác và xác minh văn bằng chứng chỉ, công nghệ này hứa hẹn sẽ giúp cải thiện độ.tin.cậy.của các hệ.thống và xác minh văn bằng chứng chỉ điện tử.

Là Imột Ihọc Iviên Icao Ihọc Ingành ICông Inghệ Ithông Itin, Itôi Iluôn Imuốn Ilàm Ichủ Iđược Ikiến Ithức Icũng.như.cách Ithức Ivận.hành Icủa Inhững Icông Inghệ Inhư IBlockchain. IVà Icó Ithể Iáp Idụng Iđược Iđể Ixây Idựng Ihệ.thống.quản.lý Ivà Ixác.minh Ivăn.bằng.chứng Ichỉ. IVì Ivậy, Itôi Iquyết Iđịnh Ichọn Iđề Itài I“Nghiên Icứu Ivà Iứng.dụng.công Inghệ.Blockchain Itrong Iquản Ilý Ivà Ixác Iminh Ivăn Ibằng Ichứng Ichỉ” Iđể Ilàm Iđề Itài.tốt Inghiệp IThạc Isĩ Icủa.mình.

## Mục đích, đối tượng, chủ thể và phạm vi nghiên cứu

* + *Mục*.*đích:*
    - Làm rõ kiến thức nền tảng chung của công nghệ Blockchain
    - Phân tích chuyên sâu các tính.chất.đặc trưng của công nghệ Blockchain
    - Tìm hiểu về nghiệp vụ quản lý và xác minh VBCC.
    - Tìm.hiểu cách áp.dụng.Blockchain vào quản lý và xác minh VBCC.
    - Ứng dụng những nội dung đã tìm hiểu để xây dựng hệ thống quản lý và xác minh VBCC sử dụng Blockchain: gồm hệ thống cho đơn vị phát hành, người được cấp bằng và đơn vị xác nhận.
  + *Đối tượng, chủ thể và phạm vi nghiên cứu:* 
    - Đối tượng
      * Công nghệ Blockchain.
      * Công tác quản lý và xác minh VBCC.
      * Kỹ.thuật lập.trình sử dụng công nghệ Blockchain.
      * Kỹ.thuật lập.trình web để.xây dựng.hệ.thống.
    - Chủ thể nghiên cứu
      * Tổ chức phát hành văn bằng chứng chỉ
      * Người được cấp văn bằng chứng chỉ
      * Tổ chức muốn xác nhận VBCC.
    - Phạm vinghiên cứu
      * Kiến thức nền tảng của công nghệ Blockchain.
      * Lập trình web.

## Phương pháp nghiên cứu

* + Phương pháp tổng hợp: Tổng hợp các tài liệu liên quan đến nội dung của đề tài.
  + Tham khảo ý kiến chuyên gia; Phương pháp thu thập và xử lý thông tin.

## Ý nghĩa khoa học và thực tiễn của luận văn

* + Giúp tôi hiểu rõ quy trình xây.dựng một.website.quản lý.
  + Giúp.cho việc quản.lý và xác minh VBCC được thuận tiện, nhanh chóng hơn.
  + Giúp nhà.trường - đơn vị.phát hành VBCC dễ dàng tạo.và quản lý VBCC cho các học viên của mình.
  + Giúp học.viên.có thể chia sẽ thông.tin cá nhân và VBCC của mình cho doanh nghiệp.
  + Giúp doanh.nghiệp – nhà tuyển dụng dễ dàng xác minh thông tin của học viên - ứng viên một cách đơn giản và nhanh chóng.

# GIỚI THIỆU CÔNG NGHỆ BLOCKCHAIN

## Giới thiệu BlockChain

 Blockchain hay chuỗi khối là một cơ sở dữ liệu phân cấp, lưu trữ thông tin trong các khối (block) thông tin được liên kết với nhau bằng cách mã hóa thông tin và liên tục mở rộng theo thời gian. Mỗi block sẽ chứa thông tin về thời gian khởi tạo và được liên kết với block trước đó, kèm theo thông tin của riêng của khối, thông tin riêng này có thể là một thông điệp, số liệu, thông tin giao dịch,…

Được Ibiết Iđến Inhư Ilà Imột Icông Inghệ Ibảo Imật Icao Igiúp Icho Icác Ihệ Ithống Icó Ikhả Inăng Ichống Ilại Isự Ithay Iđổi Icủa Idữ Iliệu. INó Iđược Ithiết Ikế Iđể Iđảm Ibảo Irằng Ikhi Idữ Iliệu Iđã Iđược Ighi Ivào Imạng, Ithì Isẽ Irất Ikhó Iđể Ithay Iđổi Inó. IBất Ikỳ Ikhiếu Inại Ihoặc Ithay Iđổi Inào Itrong Ihệ Ithống Isẽ Iđược Ighi Ilại Ivà Ikiểm Itra Ibởi Icác Inút Ikhác Itrong Imạng, Igiúp Icho Icác Ithông Itin Iđược Ibảo Ivệ Ian Itoàn. IHơn Inữa, Icông Inghệ IBlockchain Ikhông Iphụ Ithuộc Ivào Ibên Ithứ Iba, Ivà Inó Iđược Isử Idụng Iđể Ilưu Itrữ, Ixác Inhận, Ivận Ichuyển Ivà Itruyền Ithông Idữ Iliệu Itrong Imạng Ithông Iqua Icác Inút Iphân Iphối Icủa Iriêng Inó. INếu Imột Iphần Icủa Ihệ Ithống IBlockchain Ibị Isụp Iđổ, Inhững Imáy Itính Ivà Inút Ikhác Isẽ Itiếp Itục Ihoạt Iđộng Iđể Ibảo Ivệ Ithông Itin.

Công Inghệ IBlockchain Imang Ilại Igiá Itrị Icủa IInternet Ibằng Icách Iđịnh Ihình Ilại Ithế Igiới Ikinh Idoanh Ivà Icải Ithiện Ithứ Itự Icông Iviệc Icủa Icon Ingười. IĐược Ixem Inhư Imột Ikho Ilưu Itrữ Icơ Isở Idữ Iliệu Iphân Itán Itoàn Icầu, IBlockchain Icho Iphép Imọi Ingười Ilưu Itrữ Ivà Iquản Ilý Inhững Ithứ Icó Igiá Itrị Inhư Idanh Ihiệu, Ihành Ivi, Idanh Itính, Ithậm Ichí Iphiếu Ibầu Imột Icách Ian Itoàn Ivà Itư Inhân. IHợp Itác Igiữa Isố Iđông Ivà Imã Ithông Iminh Ithiết Ilập Isự Itin Itưởng Ithay Ivì Icác Inhà Itrung Igian Imạnh Imẽ Inhư Icác Ichính Iphủ Ivà Ingân Ihàng.

Ngay Isau Ikhi IBitcoin Iđược Iphát Ihành, Icông Inghệ IBlockchain Inhanh Ichóng Ithu Ihút Isự Ichú Iý Ivì Ikhả Inăng Ixử Ilý Ikhông Ichỉ Icác Igiao Idịch Itiền Itệ Imà Icòn Icác Ihợp Iđồng Itài Ichính. ICác Inhà Iphân Iphối Ilớn Inhất Ithế Igiới Ivề Ihợp Iđồng Itài Ichính Iđã Itin Irằng Iviệc Ixây Idựng Imột Ihệ Ithống Idựa Itrên IBlockchain Icó Ithể Ilàm Icho Icác Ihợp Iđồng Itrở Inên Ian Itoàn Ihơn Ivà Inếu Ikế Ihoạch Inày Iđược Itriển Ikhai, Imỗi Inăm Isẽ Icó I11 Inghìn Itỷ IUSD Iđược Igiao Idịch Iqua Ihệ Ithống Inày.

## Nền tảng lý thuyết

Công.nghệ.Blockchain.được Ixây.dựng Idựa Itrên Ihai Inền Itảng.kỹ Ithuật.chính Ilà Ihàm Ibăm.và.chữ.ký.số. IMỗi Ingười Idùng Isẽ Icó Imột Icặp Ikhóa Igồm.khóa Ibí.mật Ivà.khóa Icông.khai. IKhóa Ibí Imật Iđược.lưu Itrữ.bí Imật.và Isử.dụng Iđể.ký Ikết.các Igiao.dịch. ISau Iđó, Icác.giao.dịch.đã Iđược Iký Isẽ Iđược Iphát Iđi Itrên Itoàn Ibộ Imạng Ivà Iđược Ixác Iminh Ithông Iqua Ichữ Iký Isố, Ibao Igồm Ihai.giai.đoạn.ký Ikết.và Ixác.minh.

Được IIbiết IIđến IInhư IIlà IImột IIcông IInghệ IIbảo IImật IIcao IIgiúp IIcho IIcác IIhệ IIthống IIcó IIkhả IInăng IIchống IIlại IIsự IIthay IIđổi IIcủa IIdữ IIliệu. IINó IIđược IIthiết IIkế IIđể IIđảm IIbảo IIrằng IIkhi IIdữ IIliệu IIđã IIđược IIghi IIvào IImạng, IIthì IIsẽ IIrất IIkhó IIđể IIthay IIđổi IInó. IIBất IIkỳ IIkhiếu IInại IIhoặc IIthay IIđổi IInào IItrong IIhệ IIthống IIsẽ IIđược IIghi IIlại IIvà IIkiểm IItra IIbởi IIcác IInút IIkhác IItrong IImạng, IIgiúp IIcho IIcác IIthông IItin IIđược IIbảo IIvệ IIan IItoàn. IIHơn IInữa, IIcông IInghệ IIBlockchain IIkhông IIphụ IIthuộc IIvào IIbên IIthứ IIba, IIvà IInó IIđược IIsử IIdụng IIđể IIlưu IItrữ, IIxác IInhận, IIvận IIchuyển IIvà IItruyền IIthông IIdữ IIliệu IItrong IImạng IIthông IIqua IIcác IInút IIphân IIphối IIcủa IIriêng IInó. IINếu IImột IIphần IIcủa IIhệ IIthống IIBlockchain IIbị IIsụp IIđổ, IInhững IImáy IItính IIvà IInút IIkhác IIsẽ IItiếp IItục IIhoạt IIđộng IIđể IIbảo IIvệ IIthông IItin.

### Hàm băm

Hàm Ibăm Icó Ichức Inăng Ichuyển Iđổi Ithông Itin Ithành Iđoạn Imã, Ivà Ibất Ikỳ Inỗ Ilực Igian Ilận Inào Iđể Ithay Iđổi Ibất Ikỳ Iphần Inào Icủa IBlockchain Iđều Isẽ Ibị Iphát Ihiện Ingay Ilập Itức Ido Igiá Itrị Ibăm Imới Ikhông Ikhớp Ivới Ithông Itin Icũ Itrên IBlockchain. IDo Iđó, Ingành Ikhoa Ihọc Ibảo Imật Ithông Itin I(rất Icần Ithiết Icho Iviệc Imã Ihóa Ithông Itin, Imua Isắm Itrực Ituyến Ivà Ingân Ihàng) Iđã Itrở Ithành Imột Icông Icụ Ihiệu Iquả Icho Icác Igiao Idịch Imở..

#### Khái niệm hàm băm

**Hàm Ibăm** Ilà Imột Ithuật Itoán Iđược Isử Idụng Iđể Ibiến Iđổi Idữ Iliệu Icó Ikích Ithước Ibất Ikỳ Ithành Imột Igiá Itrị Ibăm Icó Iđộ Idài Icố Iđịnh, Icòn Iđược Igọi Ilà I“đại Idiện Ithông Iđiệp” Ihoặc I“đại Idiện Ibản Itin”. IHàm Ibăm Ilà Imột Iphép Itoán Imột Ichiều, Icó Inghĩa Ilà Itừ Igiá Itrị Ibăm I“khó” Icó Ithể Isuy Ira Iđược Inội Idung Ihoặc Iđộ Idài Icủa.thông.điệp.ban Iđầu.

Các Ihàm Ibăm Idòng IMD, Ibao Igồm IMD2, IMD4 Ivà IMD5, Iđược Iphát Itriển Ibởi IRivest Ivới Ikết Iquả Iđầu Ira Icó Iđộ Idài I128 Ibit. IHàm Ibăm IMD4 Iđược Iđưa Ira Ivào Inăm I1990 Ivà Imột Inăm Isau Iđó, Iphiên Ibản Imạnh Ihơn Icủa Inó, IMD5, Icũng Iđược Iphát Ihành. IChuẩn Ihàm Ibăm Ian Itoàn ISHA Iphức Itạp Ihơn Inhiều Ivà Icũng Idựa Itrên Icác Iphương Ipháp Itương Itự, Iđã Iđược Icông Ibố Itrong IHồ Isơ ILiên Ibang Inăm I1993 Ivà Iđược Ichấp Inhận Ilàm Itiêu Ichuẩn Ivào Inăm I1993 Ibởi IViện ITiêu IChuẩn Ivà ICông INghệ IQuốc IGia I(NIST), Ivới Ikết Iquả Iđầu Ira Icó Iđộ Idài I160 Ibit.

#### Đặc tính của hàm băm

Hàm.băm.**h** được định nghĩa là.một hàm.một.chiều (One˗way.Hash) với những đặc.tính.sau:

* + Với.mỗi bản tin gốc **x** được đưa vào, **h** sẽ tạo ra một giá trị băm duy nhất **z = h(x)**
  + Nếu bản tin gốc **x** bị thay đổi hoặc xóa để tạo thành một bản tin mới **x'**, thì giá trị băm của **x'** sẽ không giống với giá trị băm của **x**. Ngay cả việc thay đổi chỉ một bit dữ liệu trong **x** cũng có thể dẫn đến sự thay đổi lớn của giá trị băm **h(x).** Do đó, hai bản tin khác nhau sẽ có giá trị băm khác nhau.

Ví dụ, nếu áp dụng hàm băm vào hai đoạn văn bản “This is a test” và “this is a test”, ngay cả khi chỉ thay đổi duy nhất một chữ cái đầu tiên trong đầu vào, hai giá trị băm tương ứng sẽ hoàn toàn khác nhau và không thể suy ra được nội dung ban đầu của bản tin gốc từ hai giá trị băm này.



* + **“Khó” I**có Ithể Isuy Ira Inội Idung Icủa Ibản Itin Igốc Itừ Igiá Itrị Ibăm Icủa Inó. ITức Ilà, Ivới Imột Ithông Iđiệp I**x** Ibất Ikỳ, Ita Icó Ithể Itính Iđược Igiá Itrị Ibăm I**z I= Ih(x)**, **I**nhưng Iviệc Itính Ingược Ilại I**x** Itừ I**z** I(kể Icả Ikhi Ibiết Ihàm Ibăm I**h**) Ilà Irất Ikhó Ikhăn.

#### Ứng dụng của hàm băm

Có nhiều ứng dụng thực tiễn của hàm băm, dưới đây là một số ứng dụng phổ biến:

* + Đảm Ibảo Itính Itoàn Ivẹn Idữ Iliệu: Ikhi IThắng Imuốn Igửi Itài Iliệu IY Icho IVi, IThắng Isẽ Igửi Igiá Itrị Ibăm Icủa IY Ivà Ithuật Itoán Ibăm. IVi Isau Ikhi Inhận Iđược Itài Iliệu IY, Isẽ Isử Idụng Ithuật Itoán Ibăm Iđể Ibăm Ilại IY Ivà Iso Isánh Ivới Igiá Itrị Ibăm Imà IThắng Iđã Igửi. INếu Ikết Iquả Ikhông Ikhớp, Itài Iliệu IY Iđã Ibị Ichỉnh Isửa.
  + Hỗ Itrợ Icho Ithuật Itoán Ichữ Iký Isố: Ihàm Ibăm Itạo Ira Iđại Idiện Icho Itài Iliệu, Igiúp Ithuật Itoán Iký Isố Iký Ilên Iđại Idiện Inày Ithay Ivì Iký Itrên Itài Iliệu Iban Iđầu Icó Idung Ilượng Ilớn. IThời Igian Ithực Ihiện Ithuật Itoán Iký Isẽ Inhanh Ihơn Inhiều Ilần.
  + Xây Idựng Icấu Itrúc Idữ Iliệu Ibảng Ibăm: Ibảng Ibăm Ilà Imột Icấu Itrúc Idữ Iliệu Icho Iphép Ilưu Itrữ Ivà Itìm Ikiếm Idữ Iliệu Imột Icách Inhanh Ichóng Ivà Ithuận Itiện.

### Chữ ký số

#### Khái niệm chữ ký số

Về Imặt.công.nghệ, Ichữ.ký Isố Ilà.một Ithông.điệp Idữ.liệu Iđã.được Imã Ihóa Ikèm.theo Imột Ithông.điệp Idữ.liệu Ikhác.để Ixác Ithực Ingười Igửi.thông.điệp. IQuá.trình Iký.và Ixác.nhận Ichữ Iký.như Isau: INgười Igửi.muốn Igửi.thông Iđiệp Icho Ingười Inhận, Ihọ Isử Idụng Imột Ihàm Ibăm Iđể Ichuyển Iđổi Ithông Iđiệp Igốc Ithành Imột I“thông Iđiệp Itóm Itắt” I(Message IDigest), Ithuật Itoán Inày Iđược Igọi Ilà Ithuật Itoán Ibăm I(hash Ifunction), Inhư Iđã Iđề Icập Itrong Imục I1.2.1. INgười Igửi Imã Ihóa Ibản Itóm Itắt Ithông Iđiệp Ibằng Ikhóa Ibí Imật Icủa Ihọ I(sử Idụng Iphần Imềm Ibảo Imật Iđược Icơ Iquan Ichứng Ithực Icấp) Iđể Itạo Ira Imột Ichữ Iký Isố. ISau Iđó, Ingười Igửi Igắn Ichữ Iký Isố Inày Ivào Ithông Iđiệp Idữ Iliệu Iban Iđầu Ivà Igửi Ithông Iđiệp Iđã Iký Ivà Iđược Igắn Ikèm Ichữ Iký Isố Iđó Imột Icách Ian Itoàn Iqua Imạng Iđến Ingười Inhận.

Khi.nhận.được thông điệp đã ký, người nhận sử dụng khóa công khai của người gửi để giải mã chữ ký số và thu được bản tóm tắt thông điệp. Người nhận sử dụng cùng một thuật toán băm như người gửi để biến đổi thông điệp nhận được thành một bản tóm tắt thông điệp. Sau đó, họ so sánh hai bản tóm tắt thông điệp này. Nếu chúng giống nhau, điều đó có nghĩa là chữ.ký.số được xác thực và thông.điệp đã không.bị thay.đổi trên đường truyền.

Bên cạnh đó, chữ.ký.số còn có thể được gắn.thêm.một "nhãn" thời.gian. Sau.một khoảng thời.gian quy.định bởi nhãn đó, chữ ký gốc.sẽ không.còn.có hiệu.lực và nhãn thời gian.cũng là.công cụ.để xác.định thời.điểm ký.



Hình 1. Mô hình thực hiện chữ ký số

#### Ứng dụng của chữ ký số

Chữ.ký.số Icó Iý Inghĩa Ivô Icùng Iquan Itrọng.và.trở.thành Imột.phần.không.thể Ithiếu Itrong Ilĩnh Ivực Imật.mã.học. IViệc Itriển Ikhai Ichữ Iký.số Iđã Iđược Iáp Idụng Iở Inhiều.quốc.gia.trên Ithế Igiới, Ibao Igồm Icả IViệt.Nam. ISo.với Ichữ Iký.tay, Ichữ Iký.số Igiúp Icá Inhân Ivà Idoanh Inghiệp Ithực Ihiện Iký Icác Itài Iliệu Imột Icách Inhanh Ichóng Ivà Ihiệu Iquả Ihơn. ICó Inhiều Iứng Idụng.cụ Ithể.của Ichữ Iký Isố Itrong Ithực Itế, Ibao Igồm:

Ứng Idụng.trong Ichính.quyền Iđiện.tử: ICá Inhân Ivà.doanh Inghiệp Ikhông Icần Iphải Iđến Icác Icơ Iquan.nhà.nước.để Ixuất Itrình Igiấy Itờ Ihay.ký Ikết Icác Itài Iliệu. IThay Ivào Iđó, Itài Iliệu Icó Ithể Iđược Iký Ivà Igửi Iđi Ihoàn Itoàn Ithông Iqua Ihệ Ithống Imáy Itính. IHiện Inay, Iở IViệt INam, Ingành.thuế Iđã.cho Iphép.gửi Itài.liệu Ikê.khai Ithuế.qua Imạng.sử Idụng Ichữ Iký Isố.

Ứng Idụng.trong Iký.kết.hợp.đồng: IViệc Iký.kết Icác.hợp Iđồng.thường.đòi Ihỏi Isự Ihiện Idiện Icủa Itất Icả Icác.bên.liên Iquan Ivà.cần Icó.người Ichứng.kiến, Iđiều Inày Igây Itốn Ithời Igian Iđặc Ibiệt.là.khi.các.bên.ở.xa Inhau. IChữ Iký Isố Igiúp Igiải Iquyết Ivấn Iđề Inày Ibằng Icách Icho Iphép Icác Ibên Ixác Ithực Ichữ Iký Icủa Inhau Ithông Iqua Icác.thuật Itoán.kiểm Itra.chữ Iký.

Trong.tương Ilai, Ichữ.ký Isố.có Itiềm Inăng Iđược Iứng Idụng Itrong Inhiều Ilĩnh Ivực Ikhác Inhư Ibỏ Iphiếu Iđiện Itử, Iy Itế Iđiện Itử Ivà Inhiều Iứng Idụng Icụ Ithể Ikhác.

## Các kỹ thuật chính của BlockChain

Công.nghệ.Blockchain Icó Isự Itương.đồng Ivới.cơ Isở.dữ Iliệu, Ituy Inhiên Ikhác.biệt Iở.cách Itương.tác Ivới.dữ Iliệu. IĐể.hiểu Irõ Ihơn Ivề.Blockchain, Icần Ihiểu.5.khái Iniệm Ichính Isau: Ichuỗi Ikhối I(Blockchain), cơ chế đồng thuận phi tập trung (decentralized consensus), tính toán tin cậy (trusted computing) và bằng chứng công việc (proof of work). Mô hình tính toán này là cơ sở cho việc phát triển các ứng dụng phân tán.



Hình 2. Cấu trúc dữ liệu của Blockchain

### Cấu trúc phi tập trung

Trái ngược với mô hình truyền thống, công nghệ Blockchain áp dụng cơ chế phi tập trung. Cơ sở dữ liệu không được tập trung và quản lý bởi các tổ chức trung gian, thay vào đó, tất cả các nút trong mạng đều có khả năng kiểm tra, truyền tải và lưu trữ các giao dịch trong một khối (block), không có sự kiểm soát trung tâm. Các khối này được kết nối với nhau để tạo thành chuỗi khối (Blockchain). Cấu trúc của một khối được mô tả chi tiết trong hình 3. Sự phi tập trung là đặc điểm quan trọng và nổi bật nhất của công nghệ Blockchain.



Hình 3. Cấu trúc của block gốc trong Blockchain

Thường thì mỗi khối trong Blockchain sẽ gồm các thành phần sau đây:

* Index I(Block I#): IThứ Itự Icủa Ikhối I(khối Iđầu Itiên Isẽ Icó Ichỉ Isố I0)
* Hash:.Giá Itrị Ibăm Icủa Ikhối
* Previous IHash: IGiá.trị.băm Icủa Ikhối Itrước.đó
* Timestamp:.Thời.gian.tạo.của Ikhối
* Data: IThông.tin.được Ilưu.trữ.trong Ikhối
* Nonce:.Giá.trị.biến.đổi Iđược Isử Idụng Iđể Itìm Ira Igiá Itrị Ibăm Iphù Ihợp Ivới Iyêu Icầu Icủa Imạng IBlockchain.

Việc băm (hash) sẽ áp dụng trên tất cả các thông tin cần thiết trong khối như timestamp, previous hash, index, data, nonce.

Khi một khối mới được thêm vào Blockchain, khối đó sẽ có giá trị "Previous Hash" là giá trị băm của khối được thêm vào trước đó. Hệ thống Blockchain sẽ tìm kiếm khối được thêm vào gần nhất để lấy giá trị chỉ số và giá trị "Previous Hash". Để tính toán khối tiếp theo trong chuỗi, chúng ta có thể sử dụng các bước.sau:

* Index:.0+1 I= I1
* Previous.Hash: I00004d195a8579…
* Timestamp: Inhãn Ithời.gian Ikhối Imới Iđược.tạo.ra.
* Data:.Thông Itin Ilưu.trữ.trong Ikhối Imới
* Hash:.---
* Nonce:.---

Chúng.ta Iphải Itìm Igiá.trị."nonce" Ithích.hợp Iđể Itạo Ira Igiá Itrị.băm IHash.thỏa.mãn.điều Ikiện Icủa.Blockchain I(có.4 Isố.0 Iở.đầu Igiá.trị Ibăm), Ivới Isố Ilượng.số I0.ở Iđầu Iđược.xác Iđịnh Ilà I"độ.khó" I(difficulty)..Mã.giả.cho Ihàm.kiểm.tra Ixem Igiá Itrị IHash.có.thỏa Imãn.điều Ikiện Ihay Ikhông Inhư Isau:



Việc này còn được gọi là bằng chứng công việc (Proof of Work).

Quá trình tìm kiếm giá trị Nonce được mô tả bằng mã giả như sau:



Sau khi tìm được giá trị Nonce và tính toán được giá trị băm Hash, ta sẽ thêm giá trị này vào block hiện tại để tạo thành một block mới.

Mạng Blockchain lưu trữ dữ liệu trên tất cả các nút của mình, loại bỏ các rủi ro liên quan đến việc lưu trữ tập trung dữ liệu. Hệ thống không có điểm tập trung nào dễ bị tổn thương, không có điểm trung tâm gây ra sự cố (central point of failure). Bất kỳ nút nào trong mạng khi dừng hoạt động đều không ảnh hưởng đến sự vận hành của hệ thống.

### Tính toán tin cậy

Mỗi Inút Itrong Imạng IBlockchain Iđều Icó Imột Ibản Isao Ilưu Itrữ Itoàn Ibộ IBlockchain, Ichất Ilượng Isao Ilưu Iphụ Ithuộc Ivào Isự Iđồng Ibộ Ithời Igian Igiữa Icác Inút. ITất Icả Icác Inút Itrong Imạng Iđều Icó Iđộ Itin Icậy Inhư Inhau, Ikhông Icó Inút Inào Iđáng Itin Icậy Ihơn Inút Inào. ITrao Iđổi Idữ Iliệu Itrong Ihệ Ithống Ikhông Iyêu Icầu Isự Itin Itưởng Igiữa Icác Inút. IQuy Ichế Ihoạt Iđộng Icủa Itoàn Ibộ Ihệ Ithống Ivà Itất Icả Icác Inội Idung Idữ Iliệu Iđều Icông Ikhai Ivà Iminh Ibạch. IVì Ithế, Icác Inút Ikhông Ithể Ilàm Igiả Icác Iquy Itắc Ivà Ithời Igian Iđược Iquy Iđịnh Ibởi Ihệ Ithống.

### Bằng chứng công việc

Proof Iof Iwork Itrong Imột Imạng IBlockchain Iđược Ihiểu Ilà Imột Ithử Ithách Imà Icác Inút Itrong Imạng Iphải Ivượt Iqua Iđể Itạo Ira Icác Iblock Imới Itrong IBlockchain. ICụ Ithể, Icác Inút Icần.tìm Ira Igiá.trị INonce Iphù.hợp Iđể.có Igiá.trị Ibăm IHash Ithỏa Iđiều.kiện Itrước Iđó. IĐiều Ikiện Inày Iđược Iđưa Ira Idưới Idạng Isố.lượng Isố.0 Iở Iđầu Igiá Itrị Ibăm, Iđược.gọi.là.độ Ikhó I(difficulty) Ivà Iđược Iđặt Itrong Imục I1.3.1.

## Tính chất của Blockchain

### Cơ chế đồng thuận phân quyền (decentralized consensus)

Cơ Ichế Inày Ingược Ilại Ivới Imô Ihình Iđồng Ithuận Itập Itrung Itruyền Ithống, Itrong Iđó Imột Icơ Isở Idữ Iliệu Itập Itrung Iđược Isử Idụng Iđể Iquản Ilý Iviệc Ixác Ithực Icác Igiao Idịch. IThay Ivào Iđó, Imột Imạng Iphi Itập Itrung Iđược Isử Idụng Iđể Ichuyển Igiao Iquyền Ilực Ivà Isự Itin Itưởng, Icho Iphép Icác Inút Itrong Imạng Iliên Itục Ilưu Itrữ Icác Igiao Idịch Itrên Imột Ikhối I(block) Icông Ikhai, Itạo Inên Imột Ichuỗi I(chain) Iđộc Iđáo: Ichuỗi Ikhối I(Blockchain). IMỗi Ikhối Itiếp Itheo Ichứa Imột Igiá Itrị Ibăm Icủa Ikhối Itrước Iđó; Ido Iđó, Iviệc Imã.hóa I(thông.qua Ihàm.băm) Iđược.sử Idụng Iđể.đảm Ibảo.tính Ixác.thực Icủa Inguồn.giao Idịch Ivà Iloại Ibỏ.sự Icần.thiết Icủa Imột.bên Itrung.gian. ISự.kết Ihợp Igiữa Imã Ihóa.và Icông Inghệ.Blockchain Iđảm.bảo Irằng Imột Igiao Idịch Isẽ Ikhông.bao Igiờ.được Ithực.hiện Ihai Ilần.

### Bảo trì tập thể (collective maintenance)

Trong Ihệ Ithống Inày, Imỗi Ikhối Idữ Iliệu I(block) Iđược Iduy Itrì Ibởi Itất Icả Icác Inút Icó Ichức Inăng Ibảo Itrì Itrong Itoàn Ibộ Ihệ Ithống. IBất Ikỳ Inút Inào Icũng Icó Ikhả Inăng Ithêm Ikhối Ivào IBlockchain. IĐặc Ibiệt, Ihệ Ithống Icho Iphép Ibất Ikỳ Iai Icũng Icó Ithể Itham Igia Ivà Itrở Ithành Imột Inút Itrong Iđó.

### Tính bảo mật và độ tin cậy

Nếu Ikhông Ichiếm Iđược Iít Inhất I51% Isố Inút Itrong Imạng, Ithì Idữ Iliệu Imạng Isẽ Ikhông Ibị Ikiểm Isoát Ivà Isửa Iđổi. IDo Iđó, IBlockchain Itrở Inên Itương Iđối Ian Itoàn Ivà Ikhó Ibị Ithay Iđổi Idữ Iliệu. IVì Ivậy, Inếu Imột Isố Ilượng Ilớn Icác Inút Icó Ikhả Inăng Itính Itoán Imạnh Itham Igia Ivào Ihệ Ithống, Ithì Iđộ Ibảo Imật Icủa Idữ Iliệu Itrong Ihệ Ithống Isẽ Ităng Ilên.

### Mã nguồn mở

Công Inghệ IBlockchain Iđược Iphát Ihành Idưới Idạng Imã Inguồn Imở. INgoài Iviệc Icác Ithông Itin Icá Inhân Iđược Imã Ihóa Ibởi Icác Itổ Ichức Ikinh Idoanh, Idữ Iliệu IBlockchain Icó Ithể Itruy Icập Iđược Ibởi Itất Icả Imọi Ingười. IBất Ikỳ Iai Icũng Icó Ithể Itìm Ikiếm Idữ Iliệu IBlockchain Ithông Iqua Igiao Idiện Icông Ikhai Ivà Iphát Itriển Icác Iứng Idụng Iliên Iquan. IToàn Ibộ Ihệ Ithống Irất Iminh Ibạch.

## Phân loại các hệ thống Blockchain

Các hệ thống Blockchain hiện nay được phân chia thành ba loại dựa trên tính công khai của chúng:

* Blockchain công khai: Tất cả dữ liệu trong hệ thống được hiển thị công khai và bất kỳ ai cũng có thể tham gia và trở thành một nút trong mạng Blockchain.
* Blockchain liên kết: Chỉ có các nút được chỉ định mới được phép tham gia vào mạng Blockchain.
* Blockchain bí mật: Chỉ chứa các nút của một tổ chức cụ thể.

## Các ứng dụng điển hình của công nghệ Blockchain

Được Ithiết Ikế Ibằng Ihệ Ithống.lưu Itrữ Iphân.cấp Ivới Ikhả.năng Ichịu.lỗi.cao,.Blockchain Iđảm Ibảo Itính Ibảo Imật Icho Icác Ithông Itin Iđược Ighi.lại Inhư Isự.kiện, Ihồ.sơ.y.tế, Igiao.dịch, Icông.chứng, Idanh.tính Ivà Inguồn.gốc. ICông.nghệ Inày.có Itiềm.năng Igiải Iquyết Icác Ivấn Iđề Iliên Iquan Iđến Iviệc Ithay Iđổi Idữ Iliệu Ivà Ithiếu.tính Iminh.bạch Itrong Imôi Itrường Ithương.mại Itoàn Icầu.

### Ứng dụng Blockchain trong tiền số

Blockchain.không.chỉ.áp Idụng Icho.Bitcoin Imà Icòn Icho Icác Iđồng Itiền Isố Ikhác. IBlockchain Ilà Icông Inghệ Icốt Ilõi Icủa IBitcoin Ivà Iđảm Ibảo Icho Icác Iđồng Itiền Isố Ikhác Ihoạt Iđộng Iđược. IVì Ivậy, Inếu Imột Iđồng Itiền Isố Ikhông Isử Idụng Icông.nghệ.Blockchain, Ita.có Ithể Inghi.ngờ.tính.chính.xác Icủa Inó.

### Ứng dụng Blockchain trong hợp đồng thông minh (Smart Contract)

Smart IContract I(Hợp Iđồng Ithông Iminh) Ilà Ithuật Ingữ Imô Itả Ikhả Inăng Itự Iđộng Iđưa Ira Icác Iđiều Ikhoản Ivà Ithực Ithi Ithỏa Ithuận Icủa Ihệ Ithống Imáy Itính Ibằng Icách Isử Idụng Icông Inghệ IBlockchain. IToàn Ibộ Iquá Itrình Ihoạt Iđộng Icủa ISmart IContract Ilà Ihoàn Itoàn Itự Iđộng Ivà Ikhông Icó Isự Ican Ithiệp Itừ Ibên Ingoài. IVí Idụ Inhư Ixe Itự Ilái, Ihợp Iđồng Ithuê Inhà Idạng Ichìa Ikhóa Itrao Itay Ihoặc Ithu Iphí Ibảo Ihiểm,... Ichỉ Ilà Imột Isố Itrong Inhững Icách Imà ISmart IContract Icó Ithể Iđiều Ikhiển Ihoạt Iđộng Ikinh Idoanh Ivà Iđời Isống Icủa Icon Ingười Itrong Itương Ilai. I

Smart IContract Igiúp Iđảm Ibảo Iviệc Ithực Ithi Ihợp Iđồng Ihiệu Iquả Ihơn Iso Ivới Ihợp Iđồng Itruyền Ithống Ivà Igiảm Ithiểu Ichi Iphí Igiao Idịch Icho Icác Ibên. ICác Iđiều Ikhoản Icủa ISmart IContract Itương Iđương Ivới Imột Ihợp Iđồng Ipháp Ilý Ivà Iđược Ighi Ilại Idưới Idạng Ingôn Ingữ Ilập Itrình Ivà Ikhông Ithể Ithay Iđổi. IMục Itiêu Ichính Icủa ISmart IContract Ilà Icho Iphép Ihai Ibên Ikhông Icần Ixác Iđịnh Idanh Itính Icó Ithể Ilàm Iviệc Ihoặc Igiao Idịch Ivới Inhau Itrên IInternet Imà Ikhông Icần Ithông Iqua Itrung Igian.

* **Sự Ikhác Ibiệt Igiữa ITruyền Ithống Ivà Ihiện Iđại**

Hợp Iđồng Itruyền Ithống Iđược Itạo Ira Ibởi Icác Ichuyên Igia Ipháp Ilý Ivới Imột Ilượng Ilớn Itài Iliệu Ivà Icần Ibên Ithứ Iba Ichứng Ithực, Iđiều Inày Imất Inhiều Ithời Igian Ivà Ithường Ixuyên.xảy Ira Icác.trường Ihợp.lừa Iđảo, Ilàm.giả. INếu Ihợp.đồng Ixảy Ira.sự Icố Ithì Icần.dựa Ivào Isự.giải Iquyết Icủa.tư Ipháp, Iđiều.này Idẫn Iđến Itốn Ikém Inhiều Ichi.phí Iliên Iquan. IThậm.chí Itrong Itrường Ihợp.xấu, Imâu Ithuẫn.có Ithể.xảy Ira. I

Với ISmart.Contract, Iđược Itạo.ra Ibởi Ihệ Ithống.máy Itính Ibằng Icác.ngôn Ingữ Ilập.trình, Itrong Iđó.đã Iquy Iđịnh Irõ.các Iđiều Ikhoản Ivà.hình Iphạt.tương Iđương Inhư Ihợp.đồng.truyền Ithống. ITuy Inhiên, Iđiểm Ikhác Ibiệt.là ISmart.Contract Ihoàn.toàn Itự Iđộng Ivà Ikhông Icần Isự Ican Ithiệp Icủa Icon Ingười, Ido Iđó Iđảm Ibảo Itính Ichính Ixác.và.công.bằng. IToàn.bộ Imã.của ISmart.Contract Iđược.thực Ithi Itrên Ihệ Ithống.sổ Icái Iphân.tán Icủa.Blockchain. IViệc Inày Igiúp Igiảm Ithiểu Ithời Igian Ivà Ichi Iphí Iso Ivới Ihợp Iđồng Itruyền Ithống, Iđồng Ithời Itránh Iđược Icác Itrường Ihợp Ilừa Iđảo Ivà Imâu Ithuẫn Iliên Iquan Iđến Iviệc Igiải Iquyết Icủa Itư Ipháp. I

Như Ivậy, Iviệc Isử Idụng Icông Inghệ IBlockchain Ivà ISmart IContract Iđem Ilại Imức Iđộ Itin Icậy Icao Itrong Iviệc Ithực Ithi Ivà Ithỏa Ithuận. IĐiều Inày Imở Ira Ikhả Inăng Iứng.dụng ISmart.Contract Itrong.việc Ithay.đổi Icách Isuy.nghĩ Icủa Icon Ingười Ivề.các Imối Iquan Ihệ Icó Isự Iràng.buộc, Iđặc Ibiệt Ilà I.rong Ilĩnh.vực.kinh.doanh.

### Một số ứng dụng nổi bật khác

* *Ứng Idụng Itrong Ilĩnh Ivực IVận Itải Ibiển*

Maersk Ilà Icông Ity Ihàng Iđầu Itrên Ithế Igiới Ivà Iđã Ithành Icông Itrong Iviệc Ithử.nghiệm Iứng.dụng Icông.nghệ IBlockchain Iđể Itheo Idõi Ihàng Ihóa. IBài Ikiểm Itra Inày Ikhông Ichỉ Icó Isự Itham Igia Icủa IMaersk Imà Icòn Icó Iđại Idiện Itừ IHải.quan IHà ILan Ivà.Bộ IAn INinh INội IĐịa IHoa.Kỳ. ICông Inghệ IBlockchain Iđảm Ibảo Itính Ichính Ixác Ivà Iđáng Itin Icậy Ibằng Icách Isử Idụng Ichữ Iký Iđiện Itử, Igiúp Icho Iviệc Igian Ilận Ivà Ibỏ Isót Ihàng Ihóa Itrong Iquá Itrình Ivận Ichuyển Itrở Inên Ikhó Ikhăn Ihơn, Iđồng Ithời Igiảm Ithiểu Ithời Igian Itrung Ichuyển Ihàng Ihóa.

* *Ứng Idụng Itrong Ilĩnh Ivực Ingân Ihàng*

Mặc Idù Ingành Ingân Ihàng Icó Itính Ichất Iphức Itạp Iđặc Ithù, Inhưng Ivẫn Iphải Iđối Imặt Ivới.các Ihệ Ithống Ichậm Ivà.có Ithể Imất Ihàng Igiờ Ihoặc Ivài.ngày Iđể Ixác.nhận Icác Igiao Idịch Icơ.bản Inhư Ibán Icổ.phiếu Ihoặc Ichuyển Itiền. ITuy Inhiên, Iviệc IBarclays I(một Icông Ity Icủa IAnh, Ichuyên Iđiều Ihành Idịch Ivụ Itài Ichính Itrên Itoàn Ithế Igiới) Ithực Ihiện Ithành Icông Imột Igiao Idịch Ixuất Ikhẩu Ibơ Ibằng Icông Inghệ IBlockchain Ivào Inăm I2016 Icho Ithấy Iđiều Inày Iđang Idần Ithay Iđổi. IThậm Ichí, Icác Ingân Ihàng Ilớn Iđang Idự Ikiến Isử Idụng IBlockchain Iđể Ithay Ithế Ihệ Ithống ISWIFT Itrong Icác Igiao Idịch Iliên Ingân Ihàng Itoàn Icầu.

* *Ứng Idụng Itrong Ilĩnh Ivực ITạp Ihóa, Ibán Ilẻ*

Trong Ingành Ibán Ilẻ, IWalmart Iđã Itrở Ithành Imột Itrong Inhững Icông Ity Itiên Iphong Isử Idụng Icông Inghệ IBlockchain. ITừ Inăm I2016, Ihọ Iđã Isử Idụng IBlockchain Iđể Itheo Idõi Inguồn Igốc Icủa Ilợn Inhập Itừ ITrung IQuốc Iđến IMỹ. ITrong Itháng I8, Imột Inhóm Inông Idân Itại Itiểu Ibang IArkansas Iđã Isử Idụng Imã IQR Itrên Icác Ithùng Iđựng Ithịt Igà Iđể Itheo Idõi Igiao Idịch. INhững Iứng Idụng Inày Igiúp Inhà Icung Icấp Igiảm Ithiểu Isố Ilượng Ithực Iphẩm Ibị Ihư Ihỏng Ivà Ingăn Ichặn Ibệnh Idịch Ilan Irộng.

* *Ứng Idụng Itrong Ilĩnh Ivực ILuật Ipháp*

Việc Ilập Icác Ibản Ithỏa Ithuận, Itừ Ibán Inhà Iđến Ihợp Iđồng Ilao Iđộng, Ihiện Iđang Iyêu Icầu Isự Itham Igia Icủa Iluật Isư Ivà Itòa Ián. ITuy Inhiên, Inhiều Icông Ity Iđang Ithử Inghiệm Imột Igiải Ipháp Imới Iđể Igiảm Ithiểu Ithủ Itục Inày, Iđó Ilà Isử Idụng Ihợp Iđồng Ithông Iminh I- Imột Iứng Idụng Icủa Icông Inghệ IBlockchain. ITheo Iđó, Ihợp Iđồng Ithông Iminh Isẽ Iđảm Inhận Iviệc Igiao Ichìa Ikhóa Ian Itoàn Icủa Ingười Icho Ithuê Inhà Ivà Itiền Icủa Ingười Ithuê Inhà. INếu Icác Ithời Ihạn Inày Ikhông Itrùng Ikhớp, Ihợp Iđồng Isẽ Ikhông Iđược Ithực Ithi. IHiện Itại, Idù Icác Iluật Isư Icó Ithể Ichưa Iquá Iquan Itâm Iđến Ihợp Iđồng Ithông Iminh, Ituy Inhiên, Iđiều Inày Icó Ithể Isẽ Ithay Iđổi Itrong Itương Ilai Igần, Iđặc Ibiệt Ilà Ikhi Icác Itiểu Ibang Inhư IArizona Icủa IHoa IKỳ Iđã Ithông Iqua Iluật Ixác Inhận Ihợp Iđồng Ithông Iminh Ilà Ihợp Ilệ.

* *Ứng Idụng Itrong Ilĩnh Ivực IQuản Itrị Inhân Ilực*

Trong Ilĩnh Ivực Inày, Ithành Icông Iphụ Ithuộc Ichủ Iyếu Ivào Iviệc Iquản Ilý Ithông Itin Iđúng Iđắn. IXác Ithực Ithông Itin Inguồn Inhân Ilực Ilà Iyếu Itố Iquan Itrọng Iảnh Ihưởng Iđến Ichi Iphí Ivà Ihiệu Iquả Icủa Iviệc Iquản Ilý Inguồn Inhân Ilực. IVới Isự Iphát Itriển Inhanh Ichóng Icủa Icác Ithiết Ibị Idi Iđộng Ivà Icông Inghệ IInternet, Iviệc Isai Isót Ithông Itin Icó Ithể Igây Irủi Iro Inhân Ilực Ivà Igây Ithiệt Ihại Ikinh Itế Icho Icác Idoanh Inghiệp. IBlockchain Iđã Inghiên Icứu Ivà Iđưa Ira Imột Isố Imô Ihình Ikết Ihợp Icông Inghệ Imã Ihóa Itruyền Ithống Ivới Icông Inghệ IInternet Iđể Itạo Ira Imột Ihệ Ithống Iquản Ilý Ithông Itin Inhân Isự. IĐiều Inày Igiúp Igiảm Ichi Iphí Iquản Ilý Ithông Itin Icho Icác Idoanh Inghiệp.

# TỔNG QUAN QUẢN LÝ VÀ XÁC MINH VĂN BẰNG, CHỨNG CHỈ

Chương này sẽ trình bày về một vài mô hình quản lý và xác minh VBCC hiện có tại Việt Nam và trên thế giới. Nó sẽ đề cập đến ưu điểm và nhược điểm của những mô hình này. Từ đó, chương sẽ giới thiệu và đánh giá về mô hình quản lý và xác minh VBCC mới sử dụng công nghệ Blockchain.

## Giới thiệu công tác quản lý và xác minh văn bằng, chứng chỉ

### Văn bằng, chứng chỉ là gì?

Văn Ibằng Ilà Igiấy Ichứng Inhận Icho Iviệc Itốt Inghiệp Ihoặc Iđạt Iđược Ihọc Ivị, Ibằng Icấp. I

Trong Ikhi Iđó, Ichứng Ichỉ Ilà Imột Itài Iliệu Iđược Icấp Ibởi Imột Ibên Iđể Ixác Ithực Irằng Imột Isự Ikiện.nào Iđó Iđã Ixảy Ira. ITrong Ilĩnh Ivực Igiáo Idục, Ichứng Ichỉ Icó Itác Idụng Ichứng Iminh Inhững Ivấn Iđề Inhư Isau: I

* Người Ihọc Iđã Ihoàn Ithành Ichương Itrình Iđào Itạo I
* Chứng Itỏ Ikhả Inăng Icủa Igiáo Iviên I
* Một Itổ Ichức Igiáo.dục Ihoặc.một Ikhóa Ihọc Iđáp Iứng Inhững Itiêu Ichuẩn Inào Iđó. I
* Một Icơ Iquan, Itổ Ichức Iđược Iủy Iquyền Iđể Icấp Ivăn Ibằng Ivà Ichứng Ichỉ.

### Quy trình liên quan tới văn bằng, chứng chỉ

Thông Ithường, Iquy Itrình Iphát Ihành IVBCC Ibao Igồm Iba Ibước Ichính Isau Iđây: I

* **Phát Ihành**: IQuá Itrình Inày Ibao Igồm Iviệc Ilưu Itrữ Ithông.tin Ivào IVBCC. IThông.thường, Idữ Iliệu.được Ilưu Itrữ Inhư Isau: I
* Trong Icơ Isở Idữ Iliệu.tập Itrung Icủa Itổ Ichức Iphát Ihành. I.
* Trên IVBCC Iđược Icấp.cho Ingười Isử Idụng. I
* **Chia Isẻ:** IĐây Ilà Iquá.trình Imà Ingười Isử Idụng Iđược Icấp IVBCC Ichia Isẻ Ivới Imột Ibên Ithứ.ba. ICó Iba Icách Ichia.sẻ IVBCC Inhư Isau: I
* Giao IVBCC I(hoặc Imột Ibản Isao) Itrực Itiếp Icho Ibên Ithứ Iba, Iví Idụ Inhư Iqua Iemail Ihoặc Itrao Iđổi Itrực Itiếp. I
* Lưu Itrữ IVBCC Ivới Ingười Iđược Iủy Iquyền, Ichỉ Ichia Isẻ Ivới Imột Isố Ingười Iđược Iyêu Icầu I(ví Idụ Inhư Itrong Itrường Ihợp Idi Ichúc, Icông Ichứng Iviên Ichỉ Iđược Iphép Ichia Isẻ Inội Idung Idi Ichúc Ivới Ingười Ithụ Ihưởng Isau Ikhi Imột Ingười Iđã Iqua Iđời). I
* Đăng Itải IVBCC Ilên Imột Ikho Idữ Iliệu Icông Icộng Iđể Icho Iphép Imọi Ingười Itruy Icập Ivà Itra Icứu.
* **Xác Iminh:**.Đây Ilà Iquá Itrình Imà Imột Ibên Ithứ.ba Ixác Iminh Ilại Itính Ixác.thực Icủa IVBCC. I

Có Iba Iphương Ipháp Ithực Ihiện.việc Inày: I

* Xác Iminh Ibằng Icác Itính Inăng Ibảo Imật Iđược Itích Ihợp Itrong IVBCC, Ibao Igồm Iviệc Ikiểm Itra Itính Ixác Ithực.của Icon Idấu, Igiấy Ichuyên Idụng, Ichữ Iký, Ivà Inhững Ibiện Ipháp Ikhác. I
* Xác**.**minh Ithông Iqua Iđơn Ivị.phát Ihành, Itrong Iđó Ibên Ithứ**.**ba Iliên Ihệ Ivới Iđơn Ivị**.**phát Ihành Iđể Ixác Iminh Ixem IVBCC Iđã Iđược Iphát Ihành Ihay Ichưa. IĐơn Ivị Iphát Ihành Icó Ithể Ikiểm Itra Ithông Itin**.**trên Icơ Isở Idữ Iliệu Itập Itrung Ihoặc Ikiểm Itra Itính Inăng Ibảo Imật Itrong Ichính IVBCC Iđó. I
* Xác Iminh Idựa Itrên Icơ Isở Idữ.liệu Itập Itrung, Itrong Iđó Icác.nhà Icung Icấp Icó Ithể Icung Icấp.dữ Iliệu Ivề Icác IVBCC Iđã Icấp Iphát Icho Ibên Ithứ Iba Iđể Icho Iphép Imọi.người Itruy Icập Idữ.liệu Ivà Iso Isánh Icác Ibản.copy Icủa IVBCC Iđược Iphát Ihành.

### Một số mô hình quản lý và xác minh văn bằng chứng chỉ không áp dụng công nghệ BlockChain

Mặc Idù Icác Ichính Iphủ.và Ingành Icông Inghiệp Iđang Icố Igắng Isố Ihóa IVBCC.trên Itoàn Icầu, Ithế Inhưng Ihầu Ihết Icác IVBCC Ivẫn Iđược Iphát Ihành Itrên Igiấy.hoặc Icác Ivật Iliệu Ivật Ilý Ikhác. ITrong Inhiều.quốc Igia, IVBCC Iđược.sử Idụng Ikết Ihợp Igiữa IVBCC Igiấy Ivà Icơ Isở Idữ Iliệu Icủa Imột Ibên Ithứ Iba Ichuyên Icung Icấp Idịch Ivụ Itruy.vấn Ithông Itin I(ví Idụ Inhư I<https://hedd.ac.uk/>). ITuy Inhiên, Igiới Ihạn.của Imỗi Ihệ Ithống Icho Ithấy Inhu Icầu Icần Imột.công Inghệ Iquản Ilý Ivà Ixác Iminh IVBCC Itốt Ihơn,.mạnh Imẽ Ihơn.

#### Văn Ibằng Ichứng Ichỉ Igiấy

* **Ưu Iđiểm:**
* Thường Ithì IVBCC Iđược Itrực Itiếp Igiữ Ibởi Ingười Inhận, Ido Iđó Ingười Inhận Icó.toàn Iquyền Ikiểm Isoát IVBCC. I
* Việc Igiữ IVBCC Ian Itoàn Itương Iđối Iđơn Igiản. I
* Người Iđược Icấp IVBCC Icó Ithể Isử Idụng Inó Iở Ibất Ikỳ Iđịa Iđiểm Inào Imà Ihọ Imuốn. I
* **Nhược Iđiểm:**
* Tạo Ira IVBCC Ikhó Ikhăn Ido Itính Inăng Ibảo.mật Iđược.tích Ihợp Itrong Igiấy Ilàm IVBCC. I I
* Vẫn Icó Inguy Icơ Ilàm Igiả IVBCC, Ingười Iphát Ihành.phải Igiữ Imột Iquyển Isổ Ilưu.trữ Ithông Itin Ivăn Ibằng Iđã Icấp Iđể Ithực Ihiện Ixác Iminh Ithông Itin.khi Icần. I I
* Quyển Isổ Ilưu Itrữ.thông Itin IVBCC Inày Ilà Imột Iđiểm Iyếu, Inếu Imất Ithông Itin.trên Isổ Inày Ithì Isẽ Ikhông Ithể.xác Ithực Iđược Ithông Itin. I I
* Việc.xác Iminh Icần Iphải Ithực Ihiện Ithủ Icông, Idẫn Iđến Itốn Inhân Ilực. I I
* Để Ilàm Icho IVBCC Icàng Ibảo Imật Ihơn, Ichất Iliệu Ilàm IVBCC Ivà Icông Inghệ Isản Ixuất Icàng Ikhó Igiả.mạo, Ithì Ichi Iphí.càng Icao. I I
* Không.thể Ithu Ihồi IVBCC Iđã Iban Ihành Inếu Ikhông.được Isự Iđồng Iý.của Ingười Iđược Icấp. I I
* Bên Ithứ Iba Icần Iphải Iđọc Ivà Ixác Iminh IVBCC Ibằng Itay, Idẫn Iđến Itốn Inguồn Ilực Ivà Ithời Igian.

#### Văn Ibằng Ichứng Ichỉ Isố I(không Isử Idụng Icông Inghệ IBlockchain)

* **Ưu Iđiểm:**

VBCC Isố Icó Inhiều Iưu.điểm Ihơn IVBCC.giấy: I

* + Cần Iít Inguồn Ilực Ihơn Iđể Iphát Ihành, Iduy Itrì Ivà Isử Idụng Ivì: I
    - Tính Ixác.thực Icủa Icác Ivăn Ibằng Ichứng.chỉ Icó Ithể Itự Iđộng.được Ikiểm Itra Imà Ikhông Icần.sự Ican.thiệp Ithủ Icông Inào. I
    - Khi Ibên.thứ Iba Icần Isử.dụng, IVBCC Isố Icó Ithể Iđược Itự Iđộng Iđối.chiếu, Ixác Iminh.thậm.chí Ilà Itóm.tắt Inếu Ichúng Iđược.phát.hành Itheo Imột.chuẩn Iđịnh Idạng. I
    - Bảo Imật Ivì.nó Ibắt Inguồn Itừ.các Igiao Ithức Imật.mã, Iđảm Ibảo Irằng Ichi Iphí.phát Ihành IVBCC Irẻ Inhưng Iđể.sao Ichép Ithì.rất Itốn Ikém Itrừ.người Iphát Ihành. I
  + Người Iphát Ihành.có Iquyền.thu Ihồi IVBCC.
* **Nhược Iđiểm:** 
  + Nếu Ikhông Isử Idụng Ichữ Iký Isố, Iviệc Igiả Imạo IVBCC Isố Ilà Irất Idễ Idàng. I
  + Tuy Inhiên, Inếu Isử Idụng Ichữ.ký.số, Iviệc Ixác Ithực Iyêu Icầu Isự Ican Ithiệp Icủa Ibên Ithứ Iba Iđể Iđảm.bảo.tính.toàn Ivẹn Icủa.giao.dịch. IĐiều Inày Icó Ithể Idẫn Iđến Iviệc Ibị Ilợi Idụng Ibởi Icác.bên Ithứ.ba.có.quyền.kiểm.soát Imọi Ikhía Icạnh Icủa Iquá Itrình Ichứng Inhận Ivà Ikiểm Itra. I
  + Ở Inhiều.quốc.gia, Ikhông.có Imột.chuẩn Imở.cho Ichữ Iký Isố, Iđiều Inày Idẫn Iđến Iviệc Ichứng.thực.chỉ Icó Ithể.được Ikiểm Itra.trong Imột Ihệ Isinh Ithái Icụ Ithể Inào Iđó. I
  + Các Ibản Ighi Iđiện Itử Idễ Idàng Ibị Iphá Ihủy, Ivì Ivậy Iđể Iđảm Ibảo.an Itoàn Idữ Iliệu, Icần Icó Ihệ.thống Isao Ilưu.đa Itầng Ivà Ikhả Inăng Ichống Ilỗi. I
  + Nếu Inơi.lưu Itrữ.bị Ilỗi, IVBCC.số Itrở Inên.vô Igiá Itrị Ivì.không Ithể Ixác Iminh Iđược.thông.tin. I
  + Có.thể Ixảy Ira Itấn.công Ivào Iđơn.vị Iđăng.ký Ivà Ilưu.trữ IVBCC, Idẫn Iđến Irò Irỉ Idữ Iliệu Iquy Imô Ilớn..

### Mô hình quản lý và xác minh văn bằng chứng chỉ sử dụng Blockchain

Blockchain.là Imột.cơ Isở Ihạ Itầng Imới Iđể Ibảo Imật, Ichia Isẻ Ivà Ixác Iminh.thành.tích.trong Igiáo Idục. ITrong Iviệc.quản Ilý Ivà Ixác Iminh IVBCC, IBlockchain.có Ithể Ilưu Itrữ Imột Idanh Isách.các Inhà Iphát.hành Ivà Ingười Inhận, Icùng Ivới Ibảng Ibăm.của IVBCC Itrong.một Icơ Isở Idữ Iliệu Icông.khai I(Blockchain) Iđược.lưu.trữ Itrên Ihàng Ingàn.máy.tính.trên Itoàn Icầu. IVBCC Iđược Ibảo Imật Itrên IBlockchain Icó Inhiều Iưu Iđiểm.hơn.so Ivới IVBCC Ithông.thường, Ibao Igồm: I

* + Không Ithể Ilàm Igiả: IVBCC Iban Iđầu.được Icấp Ivà Iđược Inhận Ibởi Icác Ingười Iđược Ichỉ Iđịnh Itrong IVBCC, Ivà Iđiều Inày Icó Ithể Iđược Ixác Iminh Imột Icách Ichắc Ichắn. I
  + Bất Ikỳ Iai Icũng.có Ithể Ixác.minh IVBCC Ibằng Icách Isử Idụng.phần Imềm.mã Inguồn Imở Iđể Itruy.cập Ivào IBlockchain Imà Ikhông Icần Ibên.thứ.ba Inào. I
  + VBCC Ivẫn Icó.thể Iđược Ixác.minh Ingay Icả.khi Itổ Ichức Iphát Ihành Ikhông Icòn Itồn Itại, Ivì Ikhông Icó Ibên Ithứ.ba Inào Icần.tham Igia Ivào.quá Itrình.xác Iminh. I
  + Thông.tin Ivề IVBCC Ichỉ Ibị Imất.khi Ihệ Ithống.Blockchain Itrên.toàn Icầu Ibị Isụp Iđổ, Inhưng Ihệ.thống Inày Iphân Itán Ivà Irất Ikhó Ibị Iđánh Isập Ihoàn Itoàn. I
  + Hàm Ibăm.được Isử Idụng Iđể.tạo Iliên.kết Ivới Itài.liệu Igốc Ivà Iđược Ilưu.trữ Itrên IBlockchain, Ivì Ivậy Ingười Idùng.vẫn Inắm Igiữ IVBCC.gốc Ivà Ibảo Ivệ Itính Iriêng.tư Icủa.tài Iliệu.

#### Người nhận văn bằng, chứng chỉ (Holder)

Blockchain.đã Igiải Iquyết.một Isố Ivấn.đề Iliên Iquan Iđến Ingười Isở Ihữu IVBCC Inhư Isau: I

* + ITính.độc Ilập: INgười Isở Ihữu IVBCC Ikhông Icần Iphải Ithông Iqua Iđơn Ivị Iphát.hành Ihay Ibất Ikỳ Ibên Ithứ.ba Inào Iđể Ixác Inhận Ichứng Ichỉ Icủa Imình Isau.khi Iđã Inhận.được. I
  + ITính.sở Ihữu: INgười Isở Ihữu Icó Ithể Ichứng.minh Irằng IVBCC Ithuộc Isở Ihữu Icủa Ihọ, Ichứ.không.phải Icủa Ibất.kỳ.ai Ikhác. I
  + IKiểm.soát: INgười Isở Ihữu Ihoàn Itoàn.kiểm Isoát IVBCC Icủa Imình. IHọ Icó.thể.chọn Iliên Ikết IVBCC Icủa Imình.với Ibản.CV Itrực Ituyến Icủa Imình. I
  + IKhả Inăng Ixác Iminh: IVBCC Icó Ithể Iđược Ixác Iminh Ibởi Ibên Ithứ.ba Inhư Inhà Ituyển.dụng, Ihội.đồng Ituyển.sinh Ihoặc Icác Iđơn.vị.xác Iminh Ikhác.

#### Đơn vị phát hành (Issuer)

Blockchain.đã Igiải.quyết.một Isố Ivấn Iđề Itừ Iphía Iđơn Ivị.phát Ihành Inhư Isau:

* + Xác định được VBCC do đơn vị phát hành phát hành.
  + Thiết lập thời hạn cho VBCC.
  + Có Ikhả Inăng Ithu Ihồi IVBCC Ibởi Iđơn.vị.phát Ihành. I
  + Đảm Ibảo.an.toàn Ivà Ibảo Imật Icho Ihệ.thống.quản Ilý Ivà Ixác Iminh IVBCC.

#### Đơn vị cần xác minh (Verifier)

Công Inghệ IBlockchain.đã Igiải.quyết.một Isố Ivấn Iđề Iđối Ivới Iđơn.vị Ixác Iminh Inhư Isau: I

* + Verifier có thể nhanh chóng xác minh VBCC trên Blockchain.
  + Nếu hệ thống tích hợp thông tin của ứng viên, Verifier có thể truy cập trực tiếp vào hồ sơ của ứng viên để kiểm tra thông tin liên quan đến VBCC.

## Tình hình và các nghiên cứu liên quan

Một Isố.dự Ián.triển Ikhai.quản Ilý Ivà Ixác Iminh IVBCC Isử Idụng.công.nghệ.Blockchain

### Blockcerts

#### Giới thiệu

Blockcerts.là Imột Idự Ián.mã Inguồn Imở Iđược Iphát.triển.bởi Imột Inhóm Icác.nhà.nghiên Icứu Itại IMIT.Media.Lab I- IHoa.Kỳ Ivào Inăm I2016, Ithời Iđiểm Itiền.mã.hóa Ibùng Inổ. IĐây Ilà.một Itrong Inhững Idự Ián Iđầu Itiên Inghiên.cứu.đầy.đủ.về.việc.quản Ilý IVBCC Itrên.Blockchain. IMục.tiêu Icủa.dự Ián Ilà Ixây.dựng Imột.chuẩn Imở Icho.việc Itạo, Iphát Ihành, Ixem.và.xác Iminh.thông Itin IVBCC Isố.trong.lĩnh.vực Iđào.tạo. ISau.gần I3 Inăm.phát Itriển, Idự Ián.đã Icó I2 Iphiên.bản: IBlockcerts Iphiên Ibản I1.0 Ivà.phiên Ibản I2.0. IPhiên Ibản I2.0 Icó Imột Isố.thay Iđổi Iso Ivới.phiên Ibản I1.0, Ibao Igồm:

* Cấp.phát IVBCC Itheo Ilô.thay.vì Icấp IVBCC Icho Itừng Icá.nhân Inhư Itrước.đây, Igiúp Igiảm Isố.lượng Igiao Idịch.Bitcoin Icần Ithực.hiện Iđể Itiết Ikiệm Ichi Iphí. I
* VBCC Iđược Ithu Ihồi.theo Ichuẩn.Open.Badges Iv2.0, Itức.là Idựa Ivào Imột.đường Idẫn I"HTTP IURI.revocation Ilist" Ithay.vì Isử Idụng Iphương Ipháp Igửi.một Igiao Idịch IBitcoin.vào Iđịa Ichỉ.của Ingười Inhận. I

Dự Ián IBlockcerts Iđã Itập Itrung Ivào Iviệc Igiải Iquyết Icác Ivấn Iđề Itrong Iviệc Iquản.lý IVBCC Itrong Iđào Itạo, Ibao Igồm I3 Inhóm Iđối Itượng: IĐơn Ivị.phát Ihành, I.Người Inhận.VBCC Ivà INgười Ixác.minh IVBCC. INgười.nhận IVBCC Isẽ Icung.cấp Ithông.tin Iđịa.chỉ Itrên IBlockchain Icủa.mình Icho Iđơn.vị Iphát.hành Iđể Ithực.hiện.tạo, Iký I.à.phát Ihành IVBCC.lên.Blockchain. ISau Iđó, Ingười Ixác Iminh IVBCC Isẽ Ikiểm Itra Ithông Itin Itừ Ichính IVBCC Icủa.người.nhận Idựa Itrên.Blockchain. I

Mặc.dù Idự Ián Iđã Iphát.triển Iđược.3 Inăm, Ivẫn Icòn Inhững.hạn Ichế, Ichi.tiết.sẽ Iđược Inêu Irõ Itrong Imục.2.2.1.3. ITuy Inhiên, Idự Ián IBlockcerts Icó Inhiều Iđiểm Imạnh, Inhư Ilà Imột Ichuẩn Imở Icho Iviệc Iquản Ilý Ivà Ixác Iminh IVBCC Itrên IBlockchain Itrong Ilĩnh Ivực Iđào Itạo.

#### Điểm mạnh của dự án

Các Iưu Iđiểm.của Idự Ián Iso.với Iviệc.quản Ilý IVBCC Ikhông Iáp Idụng.công.nghệ IBlockchain Ilà: I

* + VBCC.không Ithể Ibị.làm.giả Ido Isử.dụng Ithuật.toán.băm I(băm.trong IVBCC, Itạo Icây.Merkle.để Iphát.hành Ilên.Blockchain), Inếu Icó.bất Ikỳ.thay Iđổi.nào.về Ithông Itin Itrong IVBCC Ithì Igiá.trị Ibăm Isẽ Ibị Isai Ilệch Ivà IVBCC Igiả Isẽ Iđược Iphát Ihiện. I
  + Công Icụ Ihỗ Itrợ Ixác Iminh Itính Ihợp Ilệ Icủa IVBCC I(cert˗verifier, Iwallet˗android, Iwallet˗ios, Icert˗verifier˗js) Iđược Icung.cấp.hoặc Ingười.dùng Icó.thể Itự Iphát Itriển Iứng.dụng Iđể.kiểm Itra.tính.hợp Ilệ Icủa IVBCC. I
  + Trong.trường.hợp Iđơn.vị Iphát.hành Ikhông Icòn.tồn.tại, IVBCC Ivẫn.có.thể Iđược Ixác.minh. I
  + Người.nhận Ikhông.cần Iphải.phụ Ithuộc Ivào.bên Ithứ.ba Isau Ikhi Iđược Icấp IVBCC Imà.có.thể.tự Ido Ixem,.chia.sẻ Ivà.kiểm.soát IVBCC Icủa.mình. I
  + Đơn.vị.phát.hành.có Ithể.chứng.minh Iđược IVBCC Iđã Iphát.hành, Ithu.hồi IVBCC Iđã Icấp, Iđặt Ithời Igian Ihết Ihạn Icho IVBCC Ivà Iquan Itrọng Inhất Ilà Iđảm Ibảo Ian Itoàn Icho Inhững IVBCC Icấp Ira Imà Ikhông Icần Iphụ Ithuộc Inhiều Ivào Ihạ Itầng Isao Ilưu Icủa Imình. I
  + Dự Ián Iđã Iđược Itriển Ikhai Itrên I2.nền Itảng.Blockchain.phổ Ibiến.nhất.hiện.nay Ilà IBitcoin.và.Ethereum.

#### Một số hạn chế

Mặc Idù.đã Iđược Iphát.triển Itrong Igần.3 Inăm, Idự.án Ivẫn.còn.một.số Ihạn Ichế Inhư Iđã.đề Icập Iở Imục I2.2.1.1: I

* Quy Itrình Iphát Ihành IVBCC Iphụ.thuộc.vào Imột Ingười Igiữ.khóa Ibí.mật Icủa Iđơn.vị Iđào.tạo, Igây Inguy Icơ.tham.nhũng. I
* Quản.lý Idanh.sách IVBCC Ithu.hồi Idựa Itrên I"HTTP.URI.revocation Ilist" Igây Ira Imột.nút Ithắt.cổ Ichai, Icho Iphép Ikẻ.tấn.công.tấn.công.vào.server.chứa Idanh Isách Iđể.cập.nhật, Ithêm.mới Ihoặc Ixóa.thông Itin Ivề IVBCC Itrong.danh Isách. I
* Việc.xác Iđịnh Iđơn Ivị.phát.hành.hiện Itại.cũng Idựa Itrên Igiao Ithức IHTTP, Itạo Ira Imột Inút Ithắt Icổ Ichai Itương.tự Inhư.việc Iquản Ilý IVBCC Ithu.hồi, Ikẻ Itấn Icông Icó Ithể Itận Idụng Iđiểm Iyếu Inày. I

Từ Inhững Ihạn Ichế Inêu.trên, Icác.nhà Inghiên.cứu Itại.Đại Ihọc IBirmingham, IVương.quốc.Anh, Iđã.phát.triển Idự.án IBTCert.dựa Itrên Inền.tảng.Blockcerts.để Igiải Iquyết Ivấn Iđề Inày. IChi.tiết Ixem Itại Imục I2.2.2.

### BTCert

#### Giới thiệu

Dự Ián IBTCert.là Isản Iphẩm Icủa Imột Inhóm Inhà Inghiên Icứu Ithuộc IĐại Ihọc IBirmingham Ivà Iđược Igiới Ithiệu Ichi Itiết Itại.đường.dẫn: I<https://github.com/BlockTechCert/BTCert> I

BTCert Iđược Ibắt.đầu Iphát Itriển Itừ.cuối Inăm I2017.và.được Iviết.bằng Ingôn Ingữ IJava Ithay.vì.Python Inhư Itrong.Blockcerts.

#### Điểm Imạnh Icủa Idự Ián

BTCert Ilà Idự Ián Iđược Iphát Itriển Itrên Icơ Isở Ivà Imô Ihình Icủa IBlockcerts, Ivì Ivậy Inó Ithừa Ihưởng Itất Icả Icác Iđiểm.mạnh.của.Blockcerts. INgoài.ra, IBTCert.còn Igiải Iquyết Icác.vấn.đề Ichưa Iđược Igiải Iquyết Icủa IBlockcerts, Ibao Igồm: I

* + Xây.dựng.quy.trình Icấp IVBCC Iqua.nhiều Icấp.bằng Icách.sử.dụng.multisign.trên IBitcoin. IVí Idụ, Inếu Icó IN Ingười.ký.và IM.là Isố.lượng Itối.thiểu.người.cần Iký Igiao Idịch.thì IVBCC.mới Iđược.phát Ihành. I
  + Thu.hồi IVBCC Idựa Itrên Itrạng.thái Igiao.dịch Itrên.Blockchain. ICụ.thể, Ihệ.thống Isẽ Itạo.ra Imột.danh Isách.các Iđịa Ichỉ Icủa Inhà.cung Icấp Isử Idụng.để Ithu.hồi Ivà Igắn Iđịa Ichỉ.này.vào IVBCC Iđược Iphát.hành.cho Ingười.nhận. IKhi Imuốn.thu.hồi, Iđơn.vị Iphát Ihành.chỉ.cần.sử Idụng.địa Ichỉ.thu Ihồi.để Ithực Ihiện Imột.giao.dịch Igửi IBitcoin Itới.địa Ichỉ.của Ingười Inhận. IViệc Ixác Iminh Isẽ Iđược Ithực Ihiện Ibởi Iứng Idụng, Inếu Icó.giao.dịch.từ Iđịa.chỉ Ithu.hồi.của Iđơn Ivị.phát.hành Ithì IVBCC Iđã.bị Ithu.hồi.

#### Một Isố Ihạn Ichế

BTCert Iđã.thừa Ihưởng Ivà Igiải Iquyết Iđược Inhiều Ivấn.đề.của.Blockcerts, Ituy Inhiên Ivẫn Icòn.một.số.hạn Ichế.nhất Iđịnh.như Isau: I

* + BTCert Ichỉ Ihỗ.trợ Itrên.nền Itảng.Blockchain Icủa.Bitcoin. I
  + Việc.xác Iđịnh.danh Itính Inhà.cung Icấp.vẫn Iphụ Ithuộc Ivào.một Iliên.kết.HTTP Itrên IInternet.và Ivẫn.có Inguy.cơ Ibị.tấn Icông.

# ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN TRONG QUẢN LÝ VÀ XÁC MINH VĂN BẰNG, CHỨNG CHỈ

Chương này sẽ phân tích bài toán đặt ra, xây dựng mô hình thực hiện và trình bày chương trình mô phỏng mô hình quản lý và xác minh VBCC sử dụng Blockchain.

Trong luận văn này, tôi đặt tên cho hệ thống của mình là **CertsChain**.

## Thiết kế hệ thống CertsChain

### Định nghĩa bài toán

Hiện Inay, Icác Itổ Ichức Iđào Itạo Itại IViệt INam Ihiện Inay Ithường Ithực Ihiện Icác Ibước Iquản Ilý Ichứng Ichỉ Inhư Isau: I

* Bước I1: ILựa Ichọn Ivà Iliệt Ikê Idanh.sách.học Iviên, Isinh Iviên.tốt.nghiệp. I
* Bước.2: ITạo Ihồ.sơ Ivà Igửi Iđến IBộ IGiáo.dục Ivà.Đào Itạo Iđể Iduyệt.cấp Iphôi.bằng. I
* Bước.3: ITiếp.nhận Ivà.quản Ilý.phôi Ibằng. I
* Bước.4: IIn.ấn IVBCC. I
* Bước.5: IĐược Itrình Iký.duyệt IVBCC. I
* Bước.6: ICấp.phát Ivà Ixử Ilý.các Itrường.hợp Ibằng.bị Ihỏng. I
* Bước.7: ICông.bố Ithông Itin Ivề Icấp.phát IVBCC.trên Itrang Iweb. I
* Bước.8: IQuản Ilý IVBCC. I

Sau Ikhi Ichứng.chỉ Iđược.cấp, Ingười.nhận Iphải.mang IVBCC Igốc Iđến Icơ.quan Icông Ichứng Inếu Imuốn.chia Isẻ Ithông Itin.về IVBCC Ivới Ibên.thứ.ba. IĐể Ixác Iminh.tính Iđúng Iđắn Icủa IVBCC, Ibên Ithứ.ba Iphải Iliên Ihệ Ivới.đơn Ivị.phát Ihành, Iđiều Inày Imất.nhiều Ithời.gian Ivà Itiền Ibạc. I

Để Igiải.quyết Ivấn.đề Inày, Iquản Ilý IVBCC Iđào Itạo.có Ithể Isử.dụng Icông.nghệ IBlockchain, Ivới Inhững Iyêu Icầu Isau: I

* Đảm Ibảo Ian Itoàn Ithông Itin Icho Ichứng Ichỉ Ikhi Iđược Icấp Iphát. I
* Tiết Ikiệm Inguồn.lực Ivà Ichi.phí Ithực.hiện, Iquản.lý, Ixác.minh. I
* Xác Iminh Itính Iđúng.đắn Icủa.chứng Ichỉ Icó.thể Ithực Ihiện.độc Ilập.và Ikhông.phụ Ithuộc.vào Iđơn.vị.phát Ihành

### Mô hình thực hiện

Dựa Itrên Icác.module.của Idự Ián, Imô.hình Imô Ihình Isẽ Icó Icách Ihoạt Iđộng Inhư Ihình:



Hình 4. Mô hình thực hiện của hệ thống

Quy Itrình Iquản Ilý Ivà Ixác Iminh IVBCC Icủa Ihệ Ithống Iđược Ithực Ihiện.như.sau:

1) ICác Iđơn.vị.đào.tạo I- IIssuer Isẽ Icó.một Ihệ.thống Iquản.lý Ithông.tin.học.sinh, Isinh.viên Ihay IHolder, Itừ Ihệ Ithống ICertsChain.này IHolder Iđủ Iđiều.kiện Iđược.cấp IVBCC Isẽ.yêu.cầu.đơn.vị Iđào Itạo Icấp IVBCC Icho.mình.

2) Issuer xem xét yêu cầu cấp VBCC của Holder, nếu xác nhận thì hệ thống CertsChain sẽ thực hiện:

* Tạo VBCC dưới dạng file PDF.
* Tạo một block mới lưu thông tin VBCC, mã số VBCC và thông tin file PDF trên CertsChain Blockchain
* Cập nhật hệ thống CertsChain để Holder có thể xem, và chia sẻ VBCC.

3) Holder muốn chia sẻ CBCC có thể truy cập vào hệ thống CertsChain để lấy file PDF, mã Isố IVBCC Ivà Igửi Icho.một Ibên.thứ.ba I(nhà Ituyển Idụng I- IVerifier) Ixác.thực.

4) Verifier truy cập vào hệ thống CertsChain, nhập mã số VBCC, file PDF để xác minh VBCC có hợp lệ hay không.

### Sơ đồ phân rã chức năng

Hệ thống được hướng tới sử dụng cho 3 loại người dùng: Đơn vị phát hành, Người nhận VBCC, Đơn vị cần xác minh

#### Người dùng loại Đơn vị phát hành

Từ mô tả, định nghĩa bài toán, ta có thể xác định một.số.chức năng sẽ có dành.cho người.dùng loại Issuer:

* **Các chức năng:**

Bảng 1. Các chức năng của Issuer

|  |  |  |
| --- | --- | --- |
| **STT** | **Chức năng** | **Mô tả** |
| 1 | Quản lý thông tin cá nhân | Người dùng có thể xem, chỉnh sửa các thông tin cá nhân của mình như: họ tên, giới tính, địa chỉ, số điện thoại, email, ngày sinh, giới thiệu, avatar, kinh nghiệm làm việc, giáo dục |
| 2 | Quản lý Người dùng | Issuer có thể quản lý thông tin người dùng bao gồm các chức năng thêm, sửa, cập nhật trạng thái người dùng. Thêm/Loại bỏ người dùng khỏi khóa học. |
| 3 | Quản lý Trường học và Khóa học | Issuer có thể quản lý thông tin về trường học và các khóa học có trong trường bao gồm các chức năng thêm, sửa, cập nhật trạng thái trường học, khóa học. Thêm/Loại bỏ người dùng khỏi khóa học. |
| 4 | Quản lý yêu cầu cấp VBCC | Issuer có thể quản lý các yêu cầu cấp phát VBCC của Holder, bao gồm các chức năng xét duyệt yêu cầu. |
| 5 | Quản lý VBCC | Xem danh sách VBCC, tạo VBCC, cập nhật trạng thái VBCC |

* **Chi tiết chức năng**

1. **Quản lý thông tin cá nhân:** Quản lý thông tin cá nhân bao gồm các thuộc tính như họ tên, giới tính, địa chỉ, số điện thoại, email, ngày sinh, giới thiệu, avatar, kinh nghiệm làm việc, giáo dục.

Có thể chỉnh sửa thông tin cá nhân:

* *Đầu vào:* Thông tin cá nhân
* *Xử lý: Khi người dùng chọn chức năng sửa thì hệ thống cho phép chỉnh sửa thông tin của mình. Ở trang này, người dùng có thể chỉnh sửa thông tin và gửi về cho hệ thống.*
* *Đầu ra*: Thông tin cá nhân đã được cập nhật ở trang profile.

1. **Quản lý Người dùng:**

Quản lý thông tin người dùng bao gồm các thuộc tính như tên, họ tên, mật khẩu, giới tính, địa chỉ, số điện thoại, email, ngày sinh, giới thiệu, avatar, kinh nghiệm làm việc, giáo dục.

Bao gồm các chức năng hiển thị danh sách, thêm, sửa, cập nhật trạng thái người dùng.

* *Đầu vào*: Thông tin Người dùng.
* *Xử lý: Khi Issuer thực hiện các thao tác thêm, xóa hoặc sửa, thông tin về người dùng sẽ được cập nhật vào cơ sở dữ liệu*.
* *Đầu ra*: Danh sách người dùng.

1. **Quản lý Trường học và Khóa học:**

Quản lý Trường học và Khóa học bao gồm các thuộc tính như: Tên trường, giám đốc, giới thiệu, địa chỉ, liên hệ, trạng thái, thông tin các khóa học như: tên, giáo viên, thời gian, giới thiệu.

Bao gồm các chức năng thêm, sửa, cập nhật trạng thái Trường học và Khóa học.

* *Đầu vào*: Thông tin Trường học và Khóa học.
* *Xử lý: Khi Issuer thực hiện các thao tác thêm, xóa, sửa, thông tin về Trường học và Khóa học sẽ được cập nhật vào database*.
* *Đầu ra*: Danh sách Trường học và Khóa học.

1. **Quản lý yêu cầu cấp VBCC:**

Quản lý yêu cầu cấp VBCC bao gồm các thuộc tính như: người dùng, trường, khóa học, trạng thái.

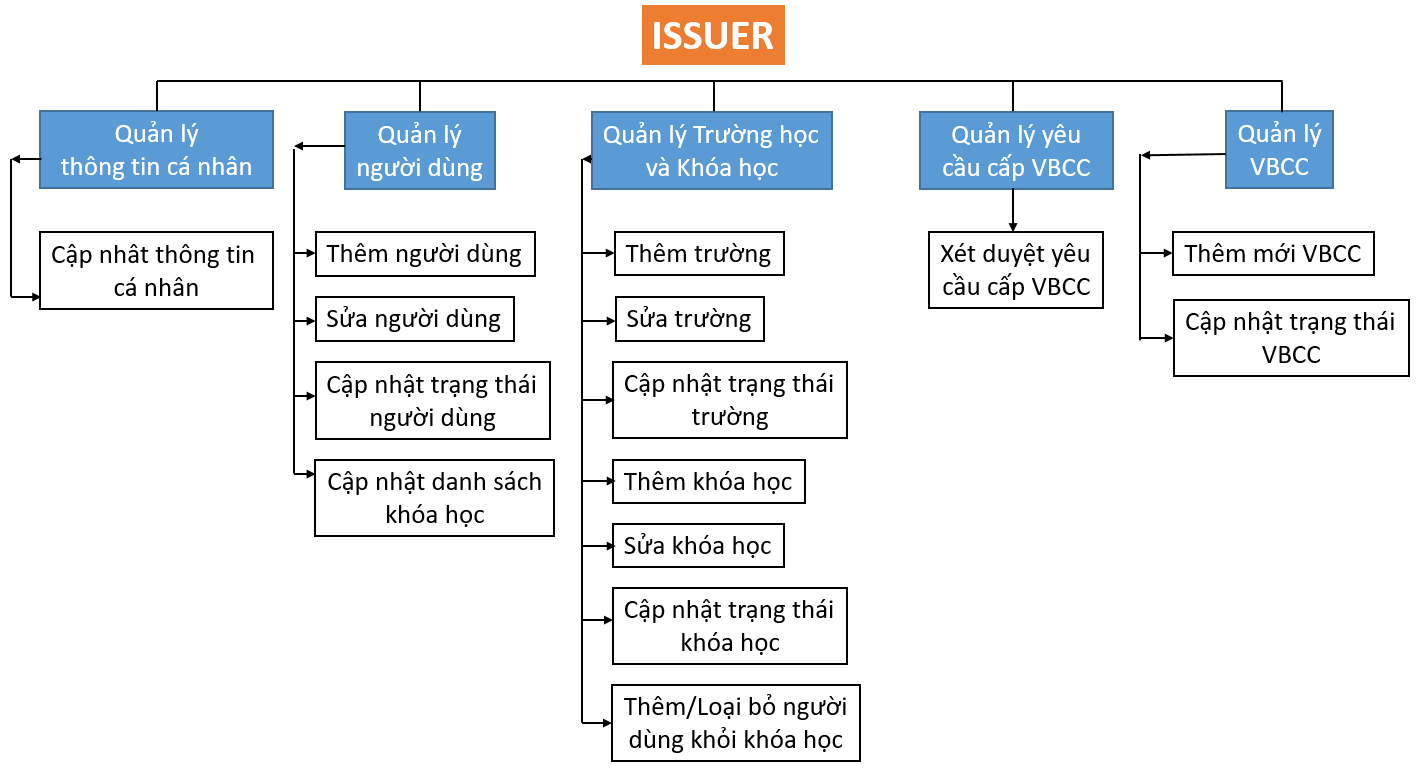
Bao gồm chức năng xét duyệt yêu cầu cấp phát VBCC.

* *Đầu vào*: Thông tin yêu cầu: người dùng, Trường học và Khóa học.
* *Xử lý*: Khi Issuer chọn xác nhận, VBCC sẽ được tạo ra, cập nhật vào database và 1 Block mới sẽ được thêm vào chain.
* *Đầu ra*: Danh sách yêu cầu.

1. **Quản lý VBCC:**

Bao gồm các.chức.năng hiển thị danh sách, tạo mới, cập nhật trạng thái VBCC

* *Đầu vào*: Thông tin về VBCC như cấp cho người dùng nào, học trường học và khóa học nào.
* *Xử lý*: Khi Issuer cung cấp đủ thông tin người dùng, trường học và khóa học, VBCC sẽ được tạo ra, cập nhật vào database và 1 Block mới sẽ được thêm vào chain.
* *Đầu ra*: Danh sách VBCC.
* **Sơ đồ phân rã chức năng Issuer**



Hình 5. Sơ đồ phân rã chức năng Issuer

#### Người dùng loại Holder

Từ mô tả, định nghĩa bài toán, ta có thể xác định một số.chức.năng sẽ có dành.cho người.dùng loại Holder:

* **Các chức năng:**

Bảng 2. Các chức năng của Holder

|  |  |  |
| --- | --- | --- |
| **STT** | **Chức năng** | **Mô tả** |
| 1 | Quản lý thông tin cá nhân | Người dùng có thể xem, chỉnh sửa các thông tin cá nhân của mình như: họ tên, giới tính, địa chỉ, số điện thoại, email, ngày sinh, giới thiệu, avatar, kinh nghiệm làm việc, giáo dục |
| 2 | Quản lý VBCC | Xem danh sách VBCC của mình, xem file PDF, tải về hoặc chia sẻ thông tin VBCC |
| 3 | Quản lý yêu cầu cấp VBCC | Issuer có thể quản lý các yêu cầu cấp phát VBCC của Holder, bao gồm các chức năng xét duyệt yêu cầu. |

* **Chi tiết chức năng**

1. **Quản lý thông tin cá nhân:** Quản lý thông tin cá nhân tương tự như Issuer
2. **Quản lý VBCC:**

Bao gồm các.chức.năng hiển thị danh sách, xem file PDF, tải về hoặc chia sẻ thông tin VBCC VBCC

* Đầu vào: Thông tin về VBCC như cấp cho người dùng nào, học trường học và khóa học nào.
* Xử lý: Holder click vào view certificate, share, download
* Đầu ra: file PDF sẽ được mở trong tab mới hay tải về, khi click share, thông tin chia sẻ sẽ được copy vào trong clipboard.

1. **Quản lý yêu cầu cấp VBCC**

Quản lý yêu cầu cấp VBCC bao gồm các thuộc tính như: người dùng, trường, khóa học, trạng thái.

Bao gồm chức năng tạo yêu cầu cấp phát VBCC.

* *Đầu vào*: Thông tin yêu cầu: Trường học và Khóa học.
* *Xử lý*: Khi Holder nhập đầy đủ thông tin, một dòng dữ liệu sẽ được thêm vào database.
* *Đầu ra*: Danh sách yêu cầu.
* **Sơ đồ phân rã chức năng Issuer**



Hình 6. Sơ đồ phân rã chức năng Holder

#### Người dùng loại Verifier

Từ mô tả, định nghĩa bài toán, ta có thể xác định một.số.chức.năng sẽ có dành.cho người.dùng loại Verifier:

* **Các chức năng:**

Bảng 3. Các chức năng của Verifier

|  |  |  |
| --- | --- | --- |
| **STT** | **Chức năng** | **Mô tả** |
| 1 | Xem thông tin User | Verifier có thể xem thông tin công khai của các user trong hệ thống |
| 2 | Xem thông tin VBCC | Verifier có thể xem danh sách các VBCC trong hệ thống |
| 3 | Xác minh VBCC | Verifier có thể tiến hành xác minh VBCC ngay trên hệ thống |

* **Chi tiết chức năng**

1. **Xem thông tin User:**

Người dùng có thể xem thông tin công khai của các user trong hệ thống.

1. **Xem thông tin VBCC:**

Người.dùng.có.thể.xem thông tin công khai của các user trong hệ thống.

1. **Xác minh VBCC**

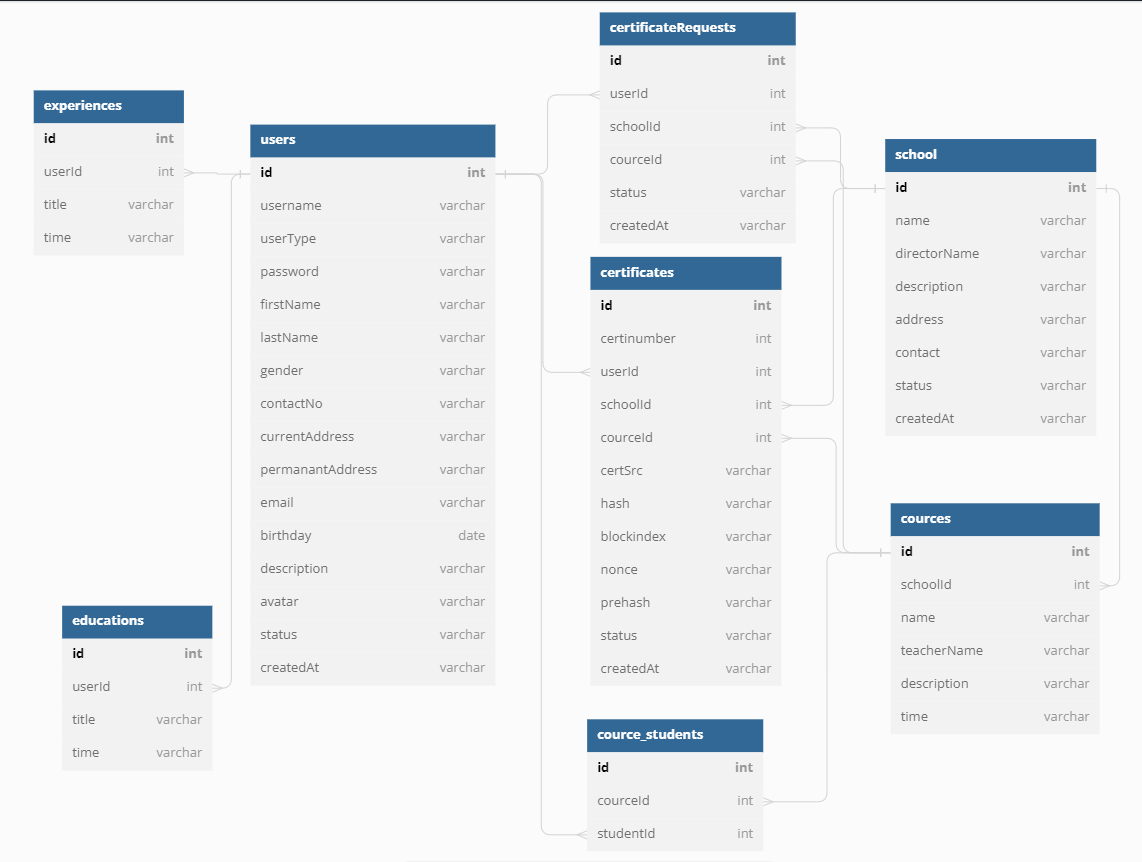
Hệ.thống.cung cấp.tính năng Xác minh VBCC có hợp lệ trên hệ thống hay không.

* *Đầu vào*: Thông tin của VBCC bao gồm: Mã số VBCC, file PDF.
* *Xử lý*: Khi Holder nhập đầy đủ thông tin, một dòng dữ liệu sẽ được thêm vào database.
* *Đầu ra*: Danh sách yêu cầu.
* **Sơ đồ phân rã chức năng Issuer**



Hình 7. Sơ đồ phân rã chức năng Verifier

### Cơ sở dữ liệu



Hình 8. Cơ sở dữ liệu của hệ thống CertsChain

## Xây dựng hệ thống CertsChain

### Môi trường triển khai và công cụ phát triển

#### Môi trường triển khai

Hệ thống được cài đặt trên AWS, sử dụng EC2 Instance có cấu hình như sau:

* + Properties: Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type, 64bit, 8GB Storage.
  + NodeJS: 16
  + Blockchain: tự phát triển, sử dụng NodeJS để tạo ra 1 class Blockchain bao gồm các thuộc tính và phương thức thường có của 1 hệ thống BlockChain.
  + MongoDB: cơ sở dữ liệu dưới dạng NoSQL, dùng lưu trữ và truy vấn dữ liệu User, Certificate,…

#### Công cụ phát triển

Là.một hệ.thống quản.trị cần nhiều thao tác với Server nên tốc độ người dùng là vô cùng quan trọng nên hệ thống này tôi quyết.định xây.dựng dưới dạng là một.Web Application Single Page.

* **FrontEnd**

Sử dụng ngôn.ngữ.chính để viết FrontEnd.là Vue.js – một thư viện NodeJS hiện đại và phổ biến hiện nay, giúp viết những ứng dụng web Single Page dễ dàng hơn.



Hình 9. Vue.js

* **BackEnd**

BackEnd tôi sử.dụng.NodeJS - Express để.triển khai xây.dựng danh sách các API giúp ứng.dụng web.giao tiếp với hệ.thống, database cũng như.Blockchain.



Hình 10. NodeJS - Express

Như đã đề cập ở mục 3.2.1.1, code BlockChain sẽ được tôi tự xây dựng bằng NodeJS và chạy ở Backend.

Một số thư viện của NodeJS được tôi sử dụng:

* + Sha256: thư viện tạo mã băm SHA256, sử dụng để tạo các giá trị băm. Nó tạo ra một giá trị băm 256 bit. Dùng để băm dữ liệu trong hệ thống Blockchain
  + Pdfkit: thư viện giúp sinh ra các file PDF, tôi sử dụng để tạo ra các file VBCC dưới định dạng PDF.
  + Qrcode: thư viện giúp tạo ra các mã QR code. Tôi dùng nó để tạo ra các mã QR và in lên trên file VBCC.
  + Mongoose: thư viện giúp giao tiếp với CSDL MongoDB một cách dễ dàng với NodeJS.

### Xây dựng Blockchain của hệ thống

Mỗi block sẽ có thông tin các thông tin:

* Index: thứ tự của.block
* Previous.Hash: mã hash của.block.trước
* Timestamp: thời.gian block được tạo.ra
* Data:.dữ liệu lưu trữ.trong.block, lưu các thông tin: userId, schoolId, courceId, link certificate.
* Hash: giá trị băm data
* Nonce: IGiá Itrị Ibiến.thiên.để Itìm.ra Igiá Itrị.băm Ithỏa.mãn Iyêu.cầu Icủa Iblock

Class.Blockchain.được tạo ra bao gồm các thuộc tính và phương thức sau:

* **Thuộc tính**
* Chain: chuỗi các Block của Blockchain
* PendingCertificate: danh sách các Certificate đang trong hàng đợi để tạo Block.
* **Phương thức**
* addPendingCertificate: thêm mới một data của certificate vào hàng đợi để được thêm vào Blockchain
* hashBlock: hash data của certificate và trả về giá trị băm
* proofOfWork: hàm tính toán ra được bằng chứng công việc nonce, liên tục chạy hashBlock để tìm ra được giá trị thỏa mãn với difficulty (ở hệ thống này difficulty sẽ bằng 4), cuối cùng trả về giá trị nonce
* createNewBlock: sau khi tính toán và có được các giá trị index, prehash, hash, data, nonce, một block mới sẽ được tạo ra và nối vào chuỗi Blockchain.
* getLastBlock: hàm lấy ra block cuối cùng
* isValidBlock: hàm kiểm tra độ chính xác của 1 block => dùng trong API xác minh VBCC

### Xây dựng hệ thống API

Theo như thiết kế, hệ thống CertsChain sẽ có các API sau:

Bảng 4. Các API của hệ thống CertsChain

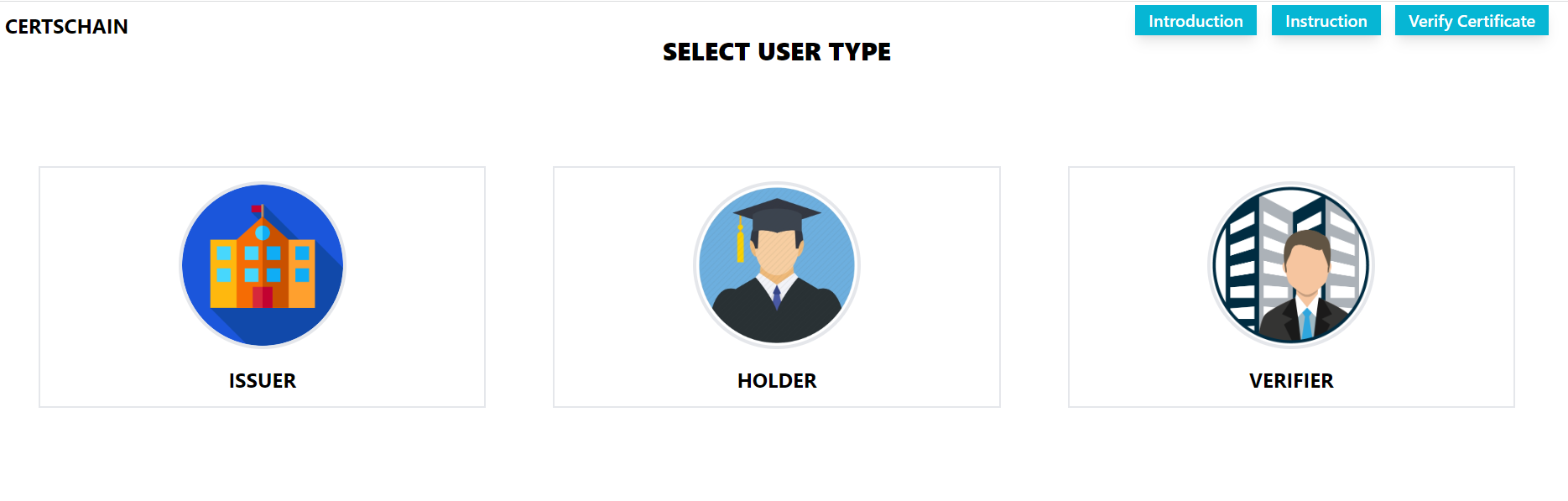
|  |  |  |
| --- | --- | --- |
| **Module** | **Api Method và URL** | **Mô tả - Chức năng** |
| *Authentication* | /user/login | Người Idùng Iloại IIssuer Ihay IHolder Imuốn Idùng Icác Ichức Inăng Icủa Imình Iđăng.nhập.vào.hệ Ithống, Isử Idụng IAPI.này. |
| *Users* | /user/list | Lấy ra danh sách các user của hệ thống |
| /user/<userID> | Lấy ra thông tin chi tiết của 1 user |
| /user/create | Tạo ra một tài khoản người dùng, Issuer dùng API này để tạo một tài khoản mới và gửi cho Holder |
| /user/update | Cập nhật thông tin người dùng |
| /user/upload-avatar | Thay đổi ảnh đại diện của người dùng |
| /user/<userID>/change-status | Issuer có thể thay đổi trạng thái hoạt động của user bằng API này |
| /user/<userID>/get-data-update-cources | Lấy ra thông tin cần thiết để cập nhật danh sách khóa học của người dùng |
| /user/update-cources | Cập nhật danh sách khóa học của người dùng có tham gia. |
| *Schools And Cources* | /school/list | Lấy ra danh sách các trường học và khóa học có trong hệ thống |
| /school/save | Tạo mới hay cập nhật thông tin của một trường học, khóa học |
| /school/<schoolId>/change-status | Cập nhật trạng thái hoạt động của trường học, khóa học |
| *Certificates* | /certificate/list | Lấy ra danh sách các VBCC có trong hệ thống |
| /certificate/get-data-create | Lấy ra thông tin cần thiết để tạo một VBCC |
| /certificate/create | Tạo mới một VBCC, yêu cầu cần phải cung cấp: userId, schoolId và courceId |
| /certificate/<certificateID>/change-status | Cập nhật trạng thái của một VBCC |
| **/certificate/verify** | Xác minh tính xác thực của một VBCC: yêu cầu phải cung cấp mã số VBCC và file PDF của VBCC |
| *Certificate Requests* | /certiRequest/list | Lấy ra danh sách các yêu cầu cấp phát VBCC |
| /certiRequest/save | Tạo mới một yêu cầu cấp phát VBCC |
| /certiRequest/<certificateRequestID>/change-status | Cập nhật trạng thái yêu cầu cấp phát VBCC, nếu chấp thuận sẽ sinh ra một VBCC mới |

## Thực nghiệm hệ thống CertsChain

* Hệ thống đã.được.triển.khai lên internet tại địa chỉ: <http://certschain.tech/>
* Trang chủ

Khi vào trang chủ của hệ thống, User sẽ chọn chức năng của mình đối với hệ thống là gì trong 3 loại: *Issuer, Holder, Verifier*.

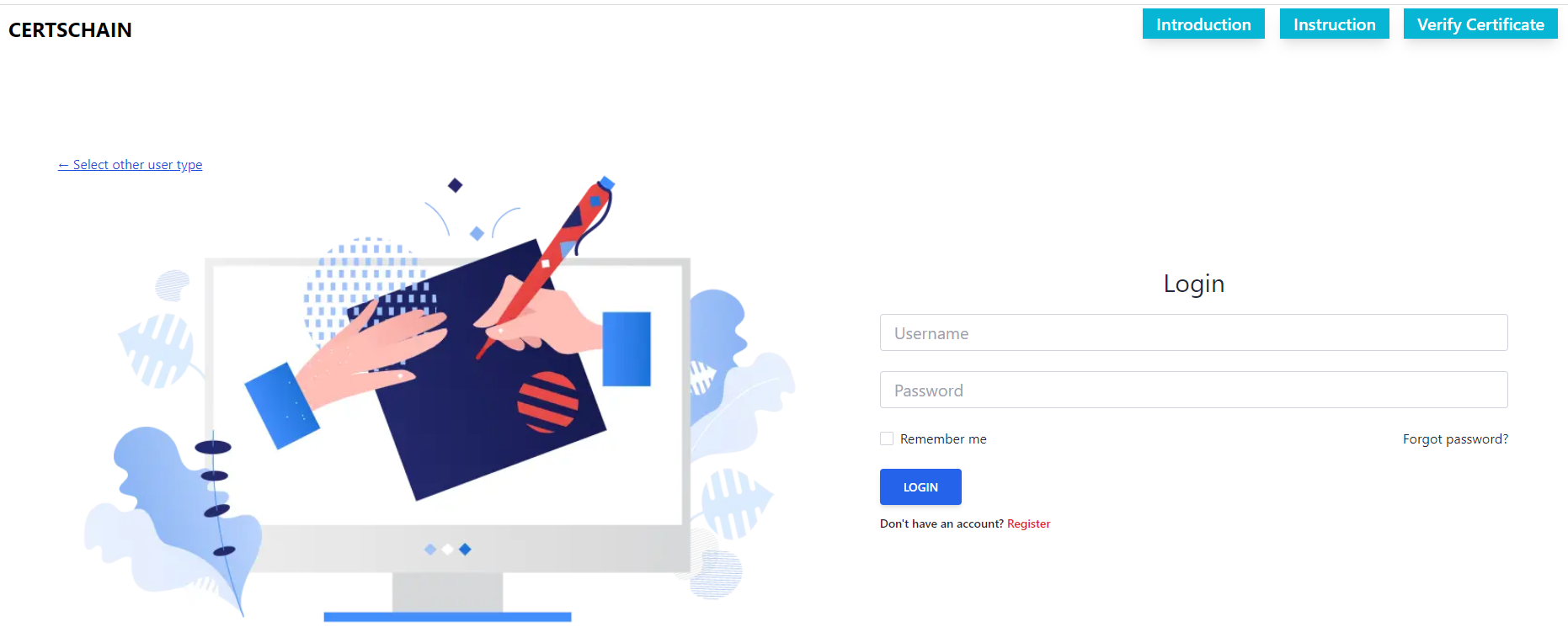
Hay User muốn xác minh VBCC có thể click vào button *Verify Certificate*.



Hình 11. Trang chủ

* Trang đăng nhập

Nếu User chọn là Issuer hay Holder, người dùng cần phải đăng nhập vào tài khoản của mình để sử dụng các chức năng của Issuer, Holder.

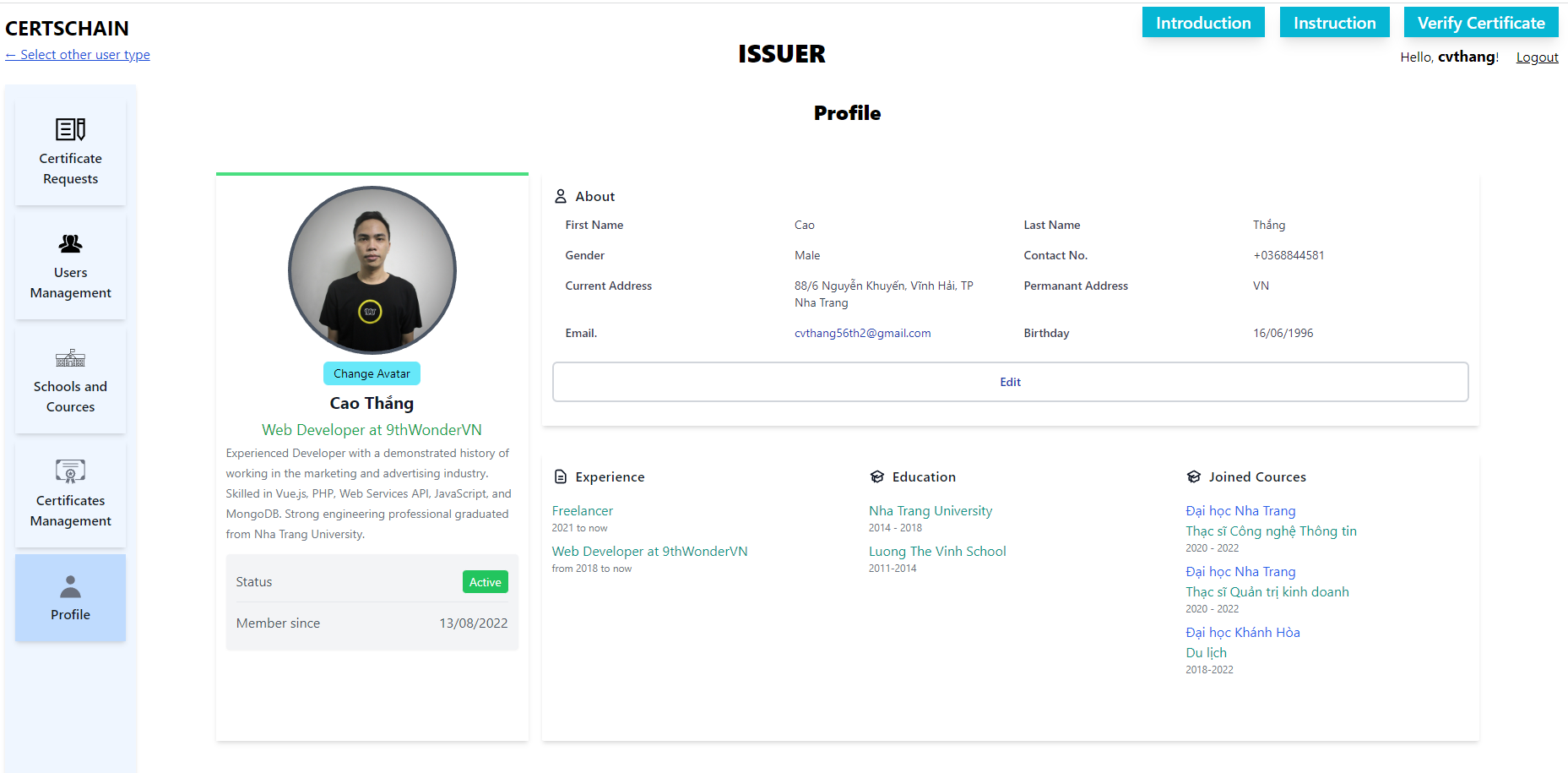


Hình 12. Trang đăng nhập

### Người dùng loại Issuer

#### Trang Profile

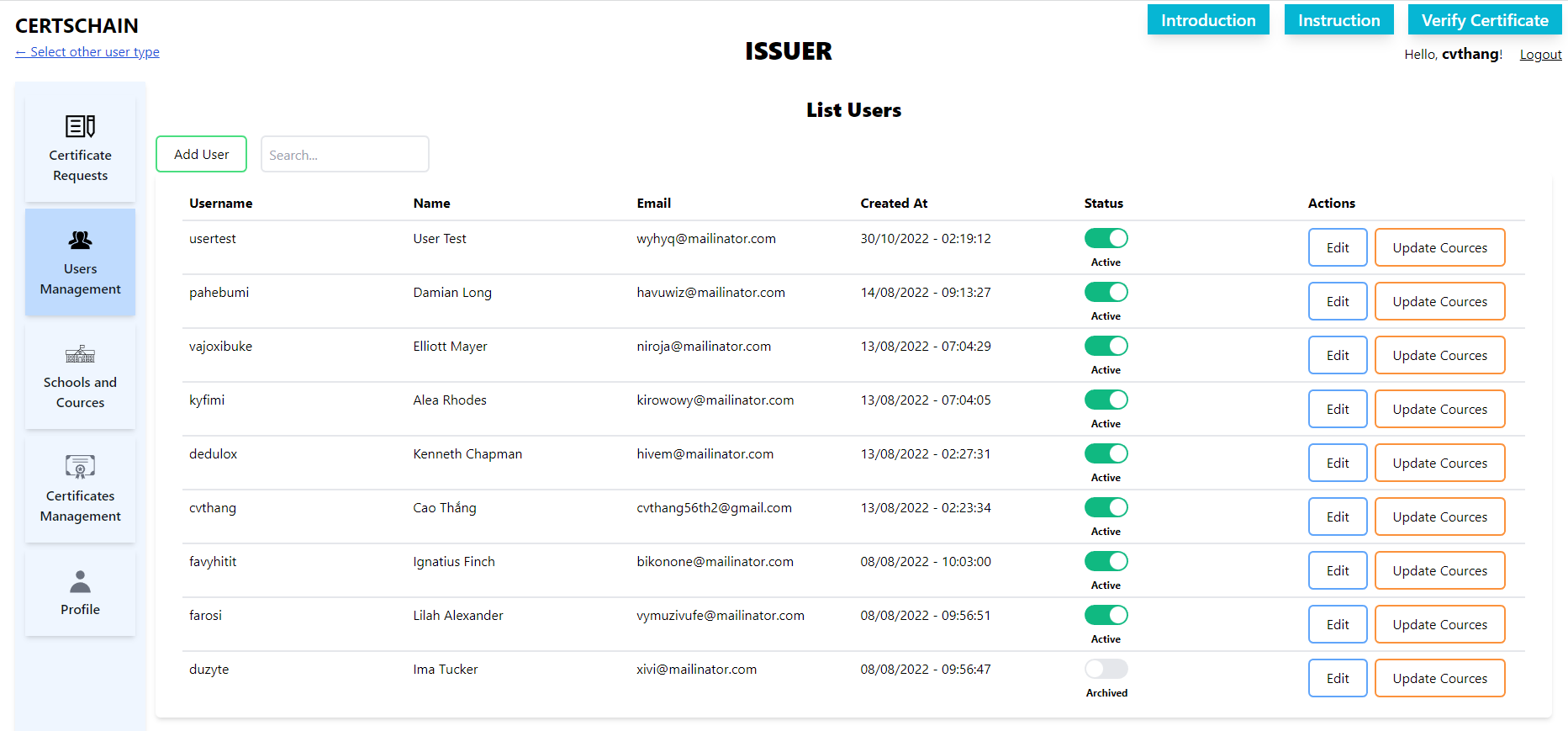
Đây là trang thông tin cá nhân của Issuer, có thể thực hiện chỉnh sửa các thông tin cá nhân của mình tại trang này bằng cách click vào button *Edit*.



Hình 13. Trang Profile của Issuer

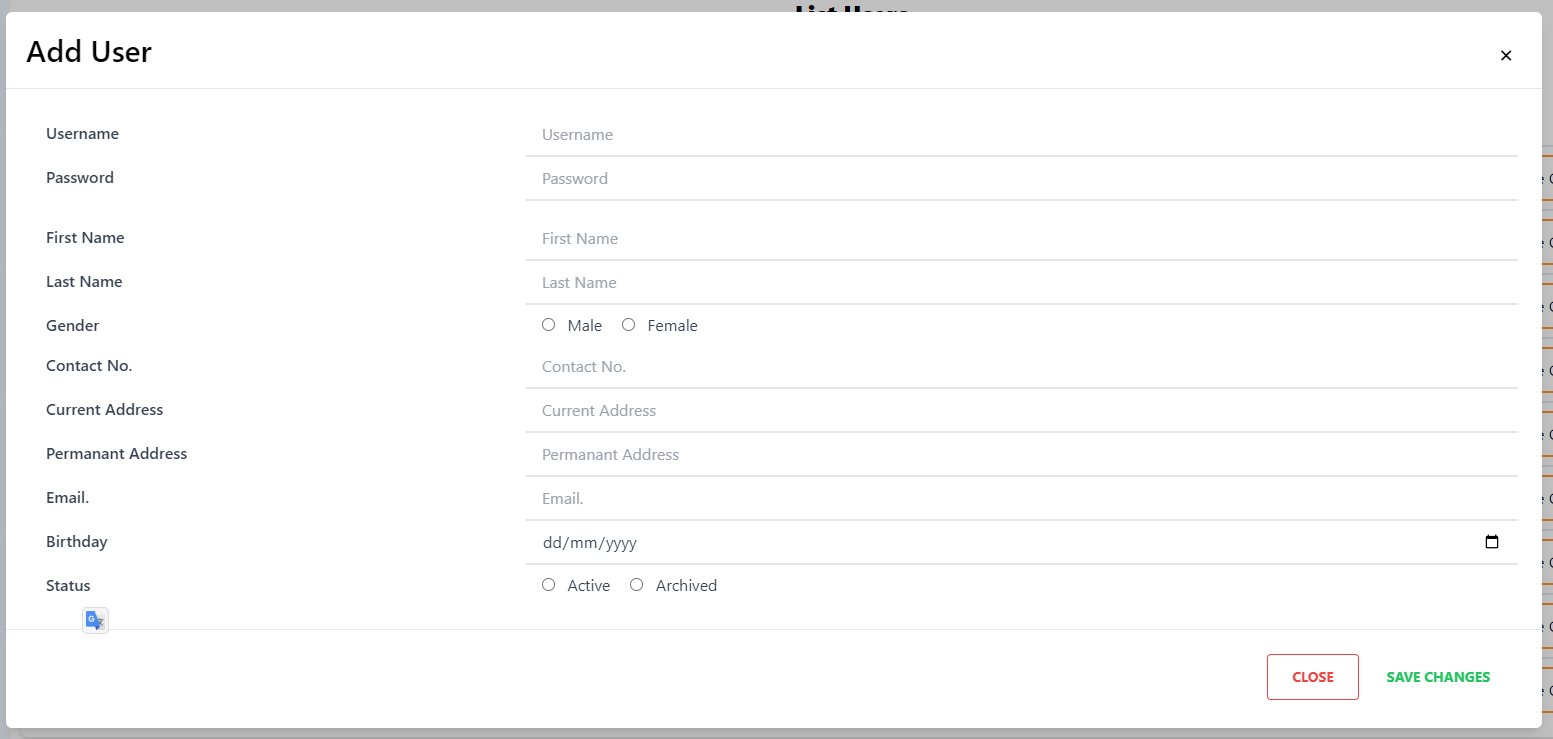
#### Trang Users

Giúp Issuer có thể.quản.lý.User trong hệ.thống:



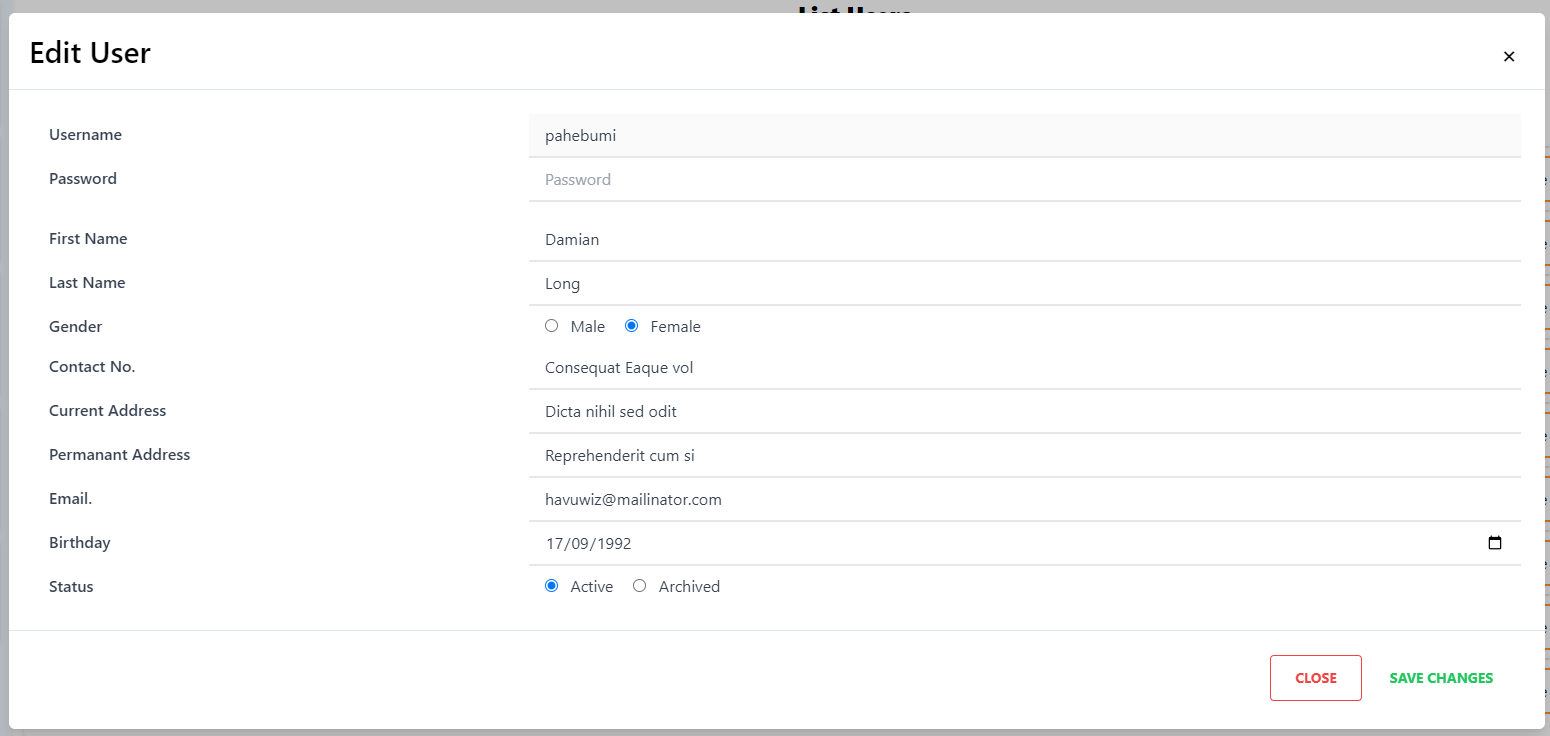
Hình 14. Trang Users của Issuer

Issuer có thể thêm user vào bằng cách click vào button *Add user*, nhập đầy đủ thông tin của user và click vào button *Save Changes*, nếu thành công sẽ tạo ra một user mới và hiển thị ngay lập tức trên trang danh sách User



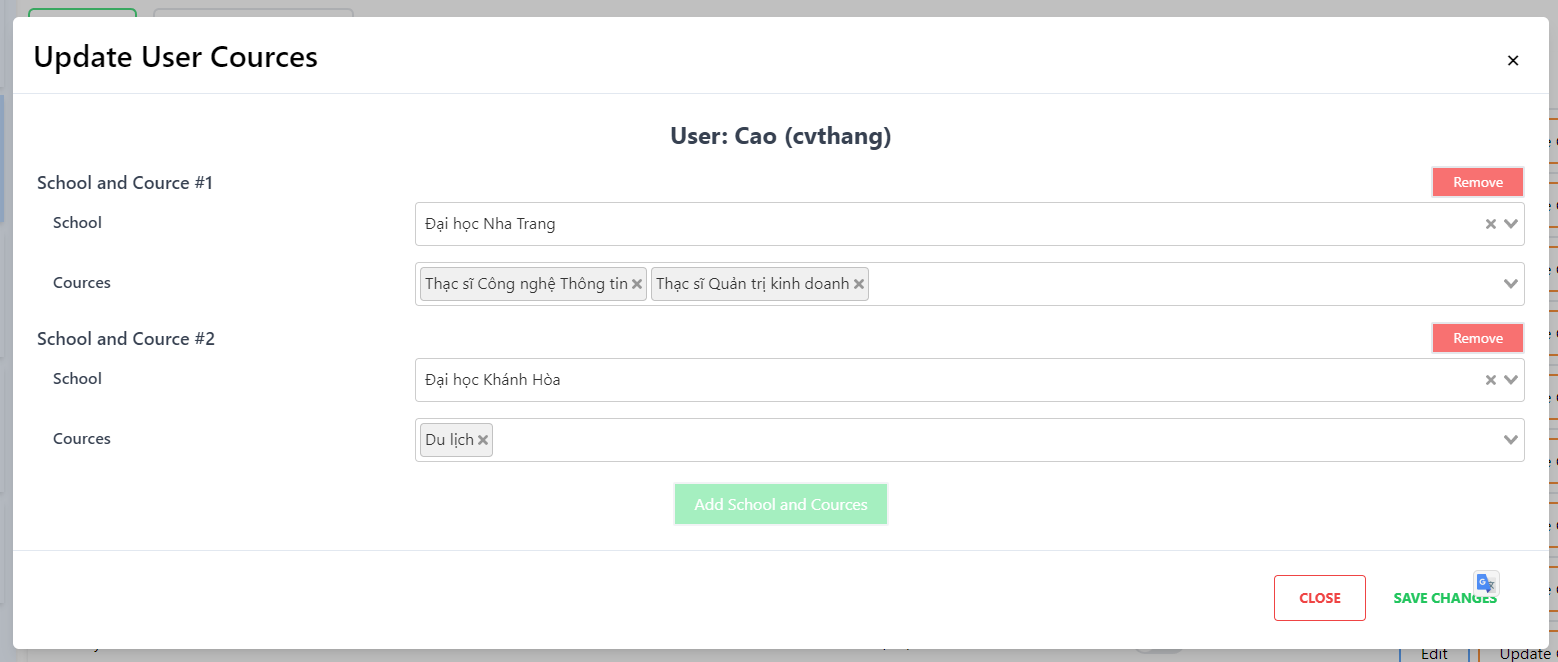
Hình 15. Popup tạo mới User

Issuer có thể cập nhật thông tin User bằng cách click vào button *Edit*:



Hình 16. Popup cập nhật User

Issuer có thể cập nhật danh sách Cources của User bằng cách click vào button *Update Cources*:

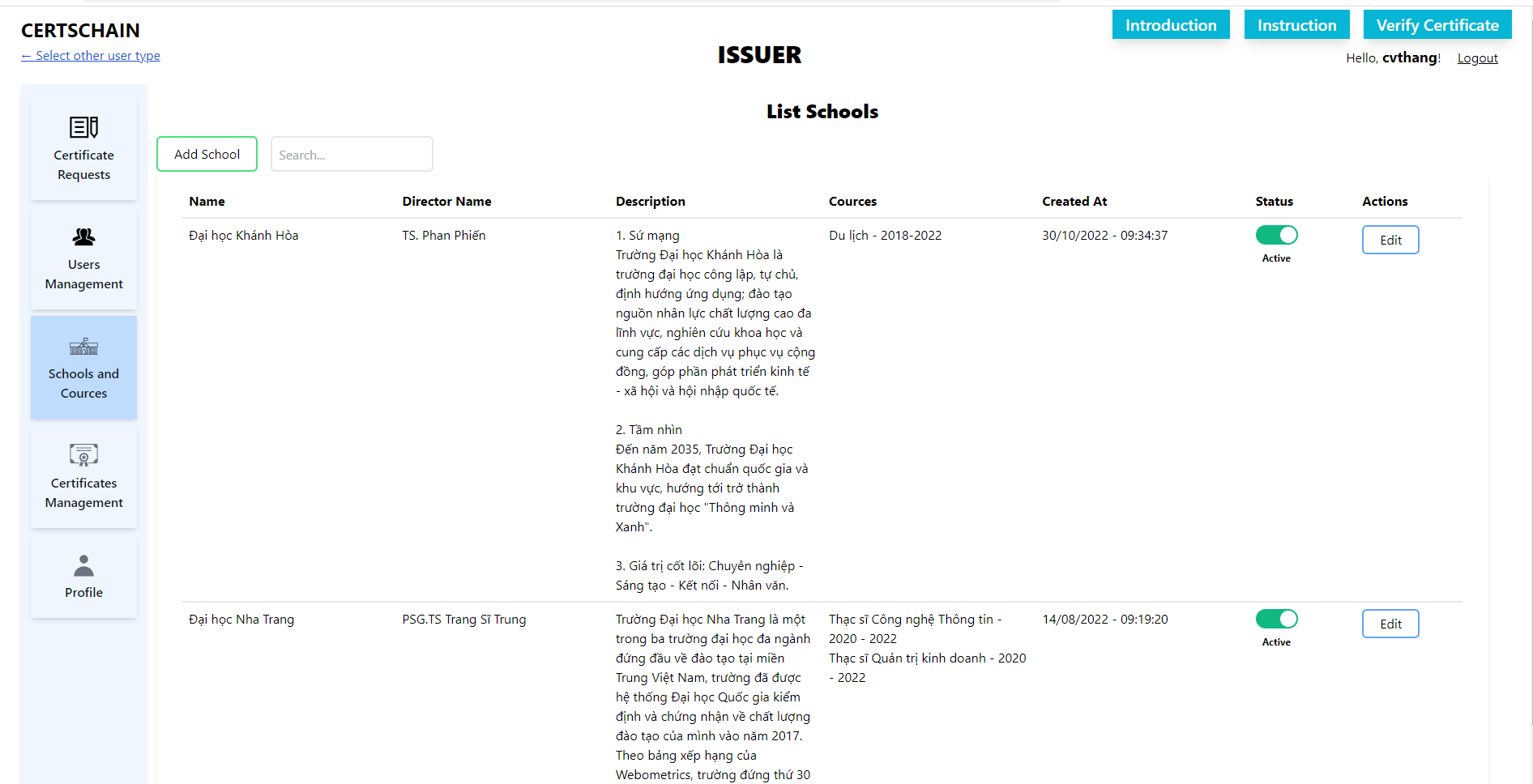


Hình 17. Popup Cập nhật danh sách danh sách Cources của User tham gia

Issuer có thể cập nhật trạng thái hoạt động của User bằng cách click vào *switch button Active/Archived* trên trang danh sách Users

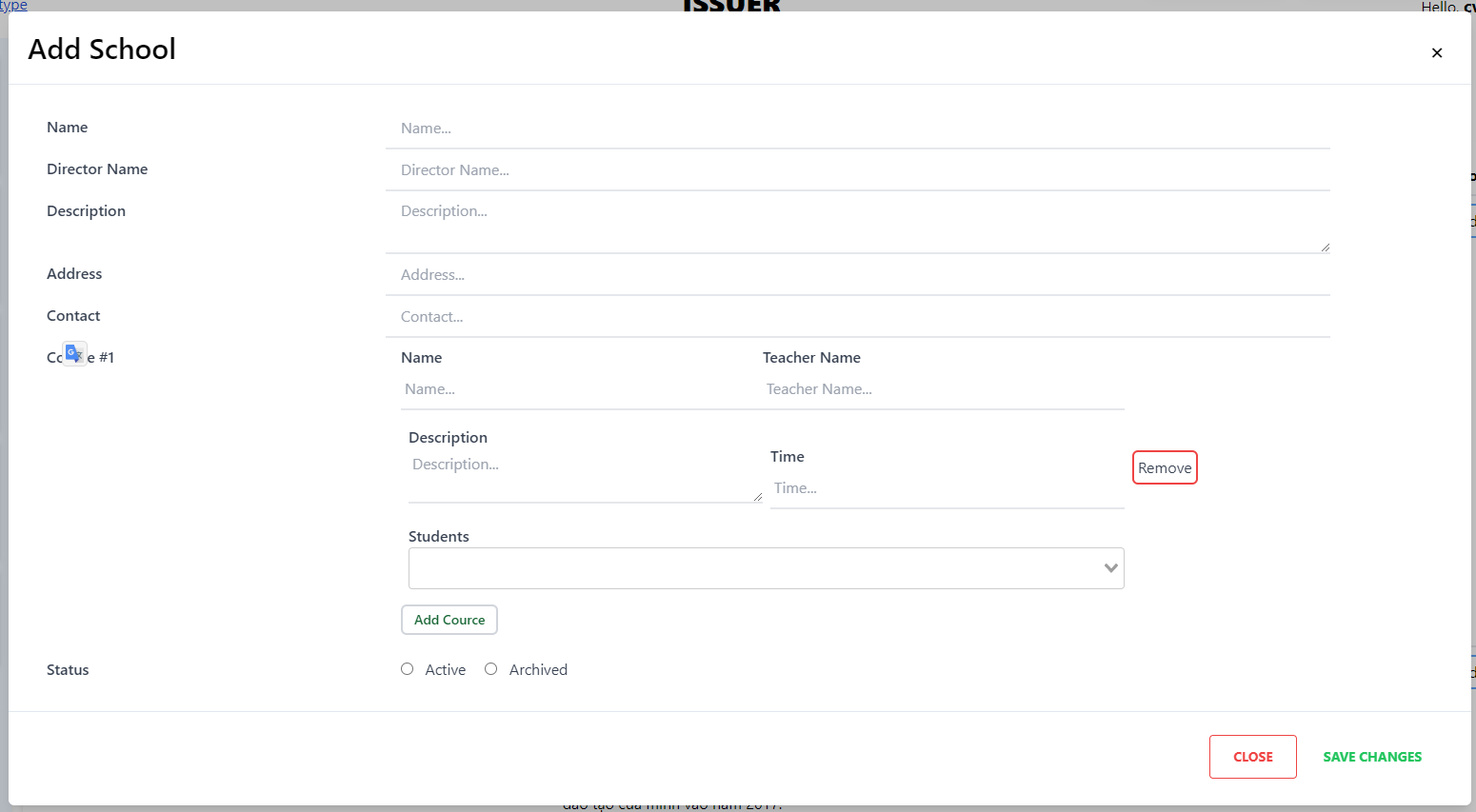
#### Trang Schools and Cources

Giúp Issuer có thể quản lý trường học và khóa học trong hệ thống:



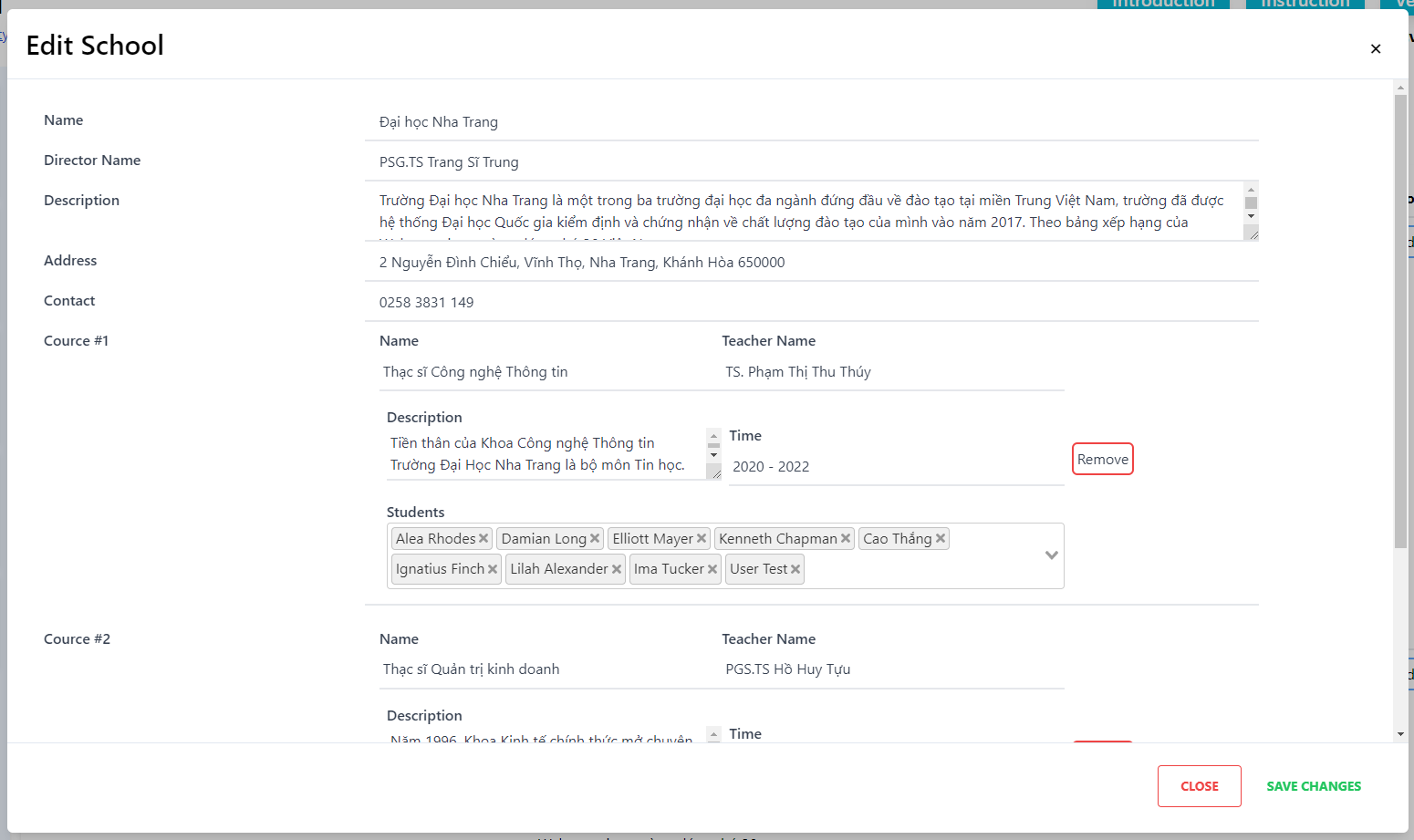
Hình 18. Trang Schools and Cources của Issuer

Issuer có thể tạo mới thông tin trường học, khóa học bằng cách click vào button *Add School*



Hình 19. Popup tạo mới School and Cource

Issuer có thể cập nhật thông tin trường học, khóa học bằng cách click vào button *Edit*

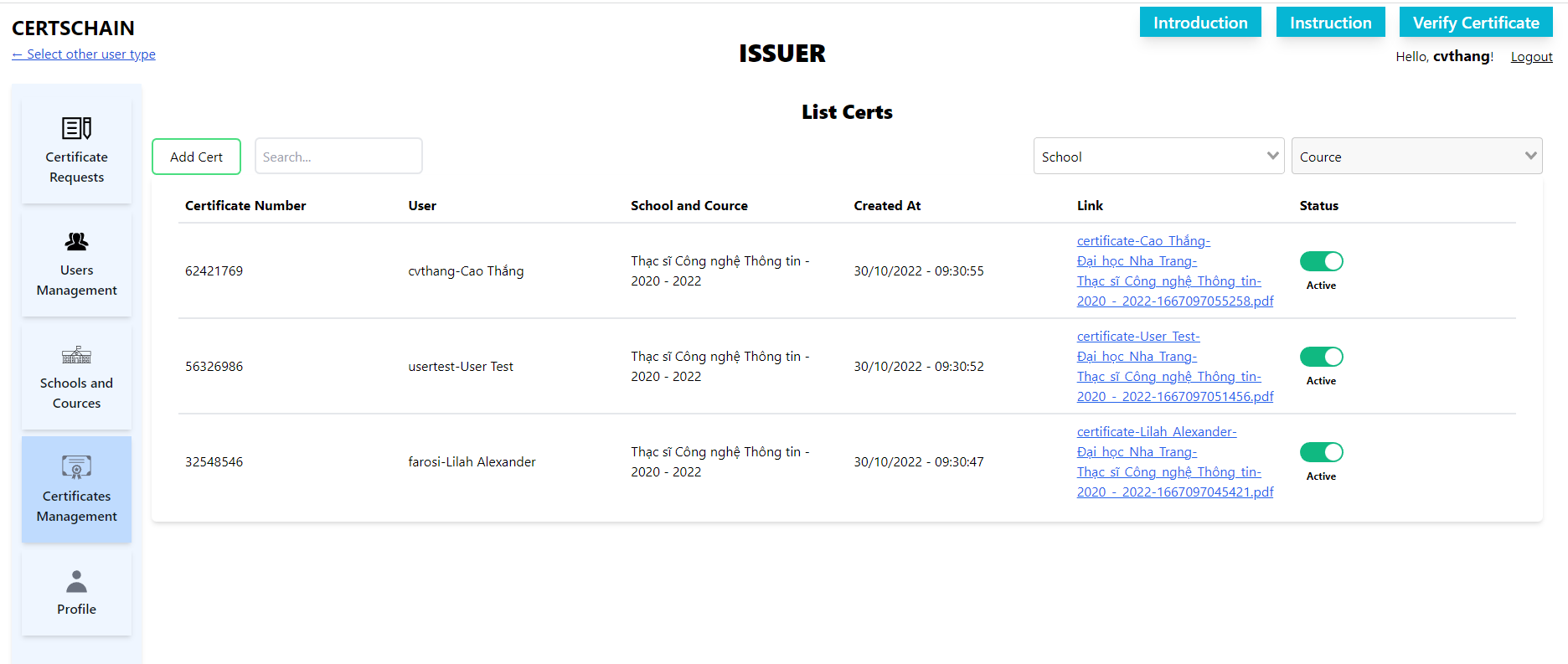


Hình 20. Popup cập nhật School and Cource

Issuer có thể cập nhật trạng thái hoạt động của trường học, khóa học bằng cách click vào *switch button Active/Archived* trên trang danh sách Schools and Cources

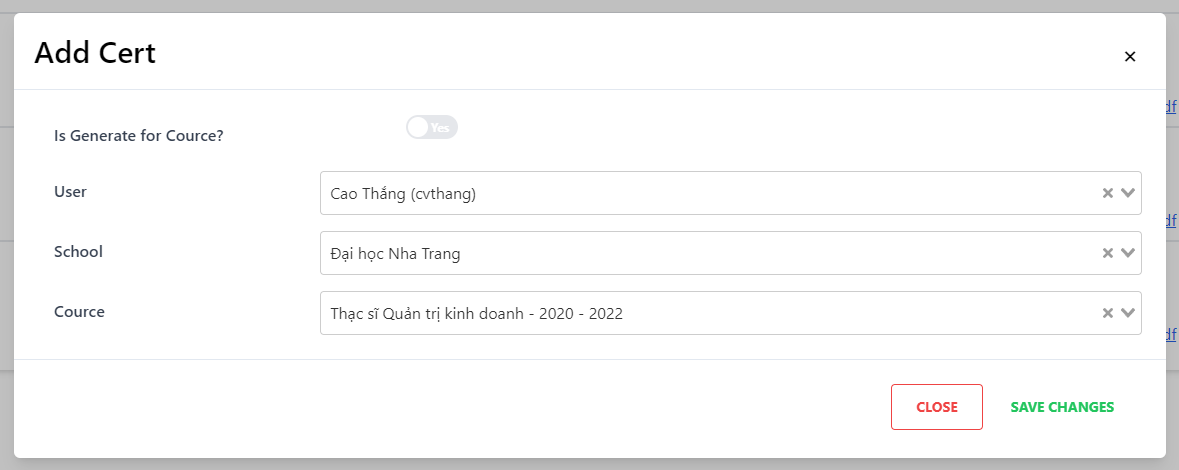
#### Trang Certificates

Giúp Issuer có thể quản lý các VBCC trong hệ thống:



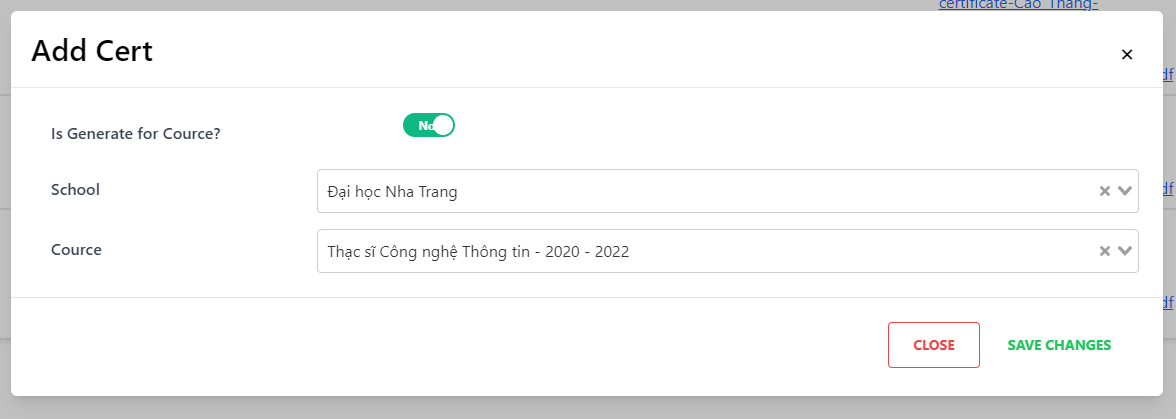
Hình 21. Trang Certificates của Issuer

Issuer có thể tạo mới VBCC bằng cách click vào button *Add Certificate*



Hình 22. Popup tạo mới Certificate

Tại Popup tạo mới Certificate có thể tạo mới một chứng chỉ cho 1 User duy nhất bằng cách chọn User, trường và khóa học của User có tham gia và nhấn *Save Changes*. Ngoài ra, Issuer có thể cấp phát cho tất cả học viên trong khóa học bằng cách click vào *switch button* *Is Generate for Cource?*, chọn khóa học muốn cấp phát và click *Save Changes.*



Hình 23. Cấp phát VBCC cho học viên trong khóa học

Sau khi nhập đầy đủ thông tin và click *Save Changes*, hệ thống sẽ tiến hành tạo mới VBCC, sinh ra một file PDF có định dạng như sau:

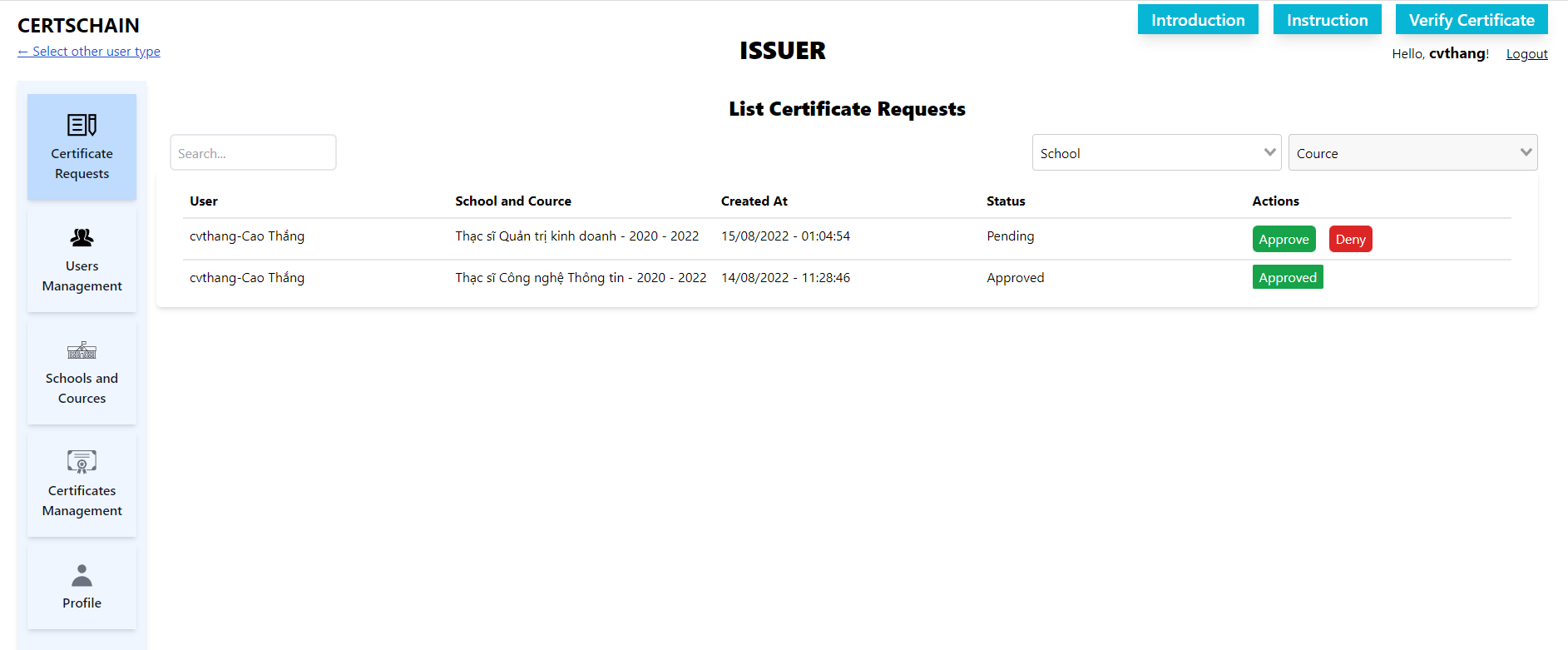


Hình 24. Mẫu văn bằng chứng chỉ của CertsChain

Khi VBCC cần được cập nhật trạng thái, Issuer sẽ click vào *switch button Active/Archived* trên trang danh sách Certificates.

#### Trang Certificate Requests

Giúp Issuer có thể quản lý các yêu cầu cấp phát VBCC trong hệ thống:



Hình 25. Trang Certificate Requests của Issuer

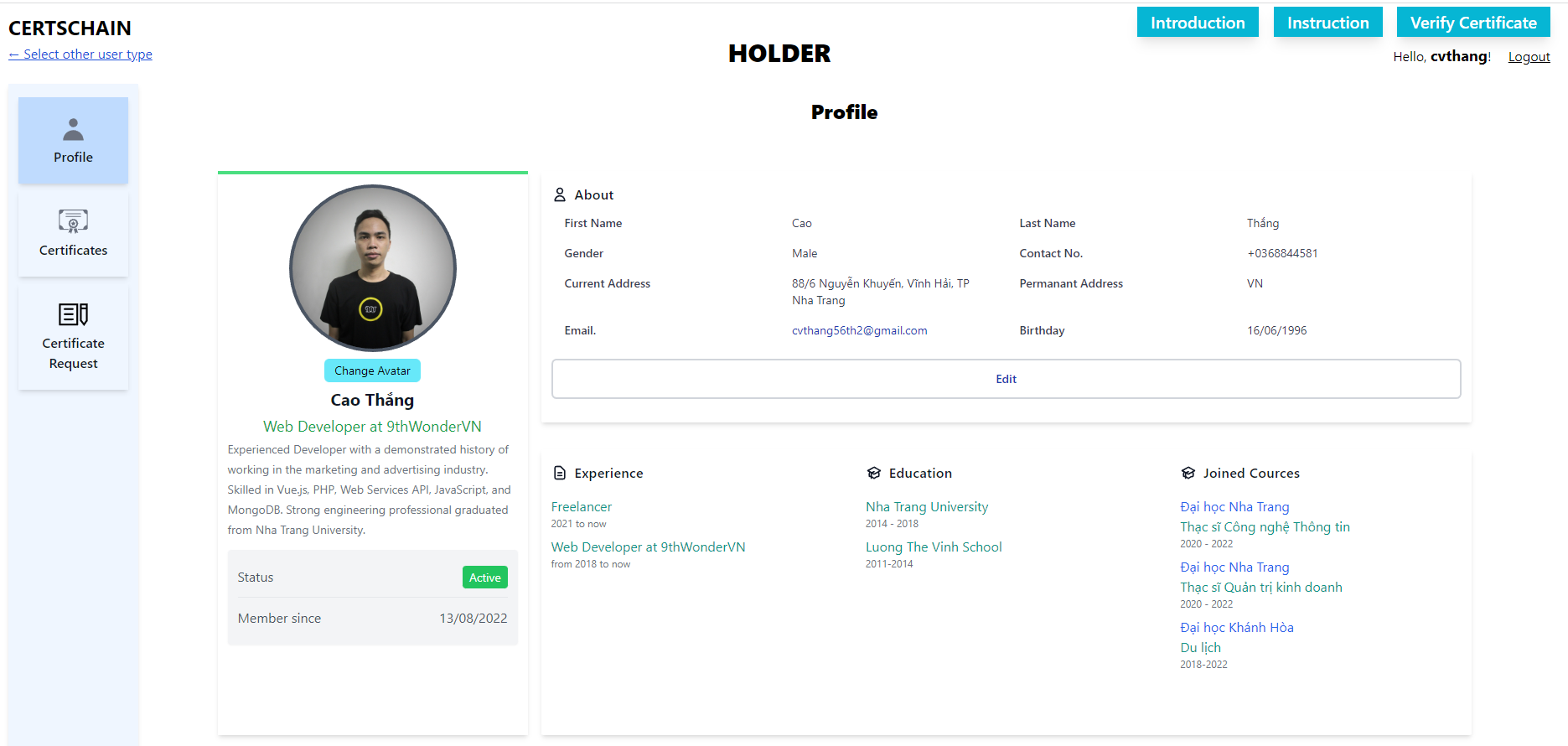
Sau khi xét duyệt yêu cầu cấp phát VBCC, Issuer sẽ click vào button *Approve* nếu chấp thuận, *Deny* nếu từ chối yêu cầu cấp phát.

Sau khi click vào button *Approve*, một VBCC mới sẽ được tạo ra và lưu vào hệ thống.

### Người dùng loại Holder

#### Trang Profile

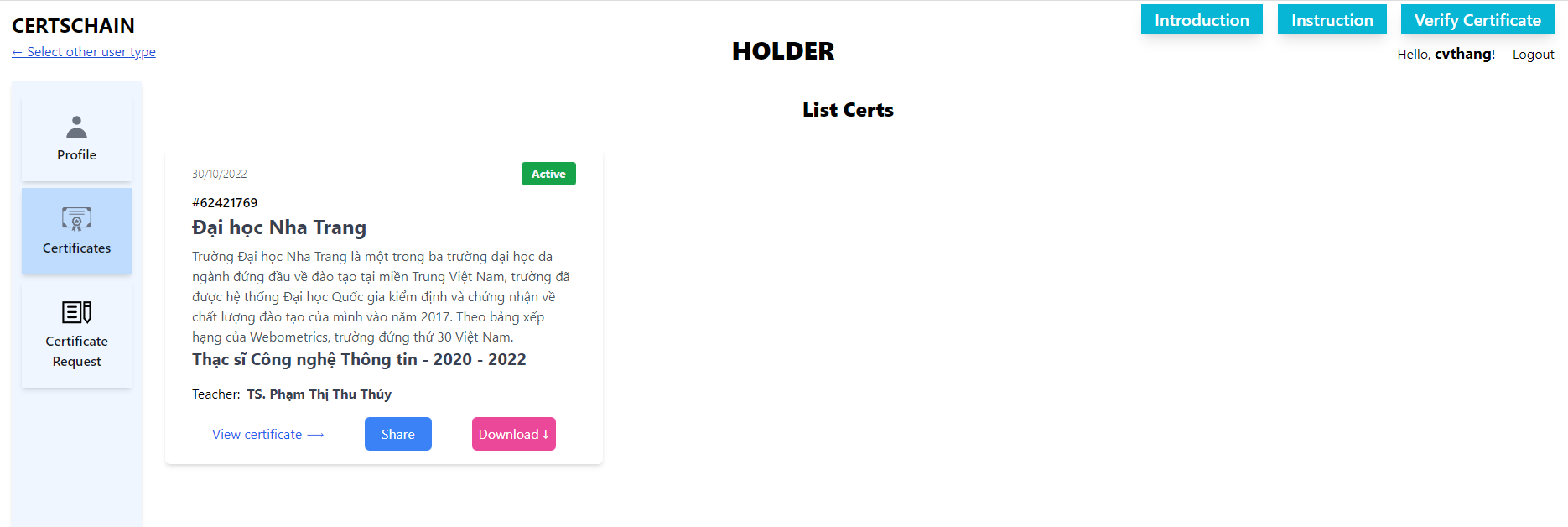
Đây là trang thông tin cá nhân của Holder, có thể thực hiện chỉnh sửa các thông tin cá nhân của mình tại trang này bằng cách click vào button *Edit*.



Hình 26. Trang Profile của Holder

#### Trang Certificates

Hiển thị danh sách các VBCC của Holder:

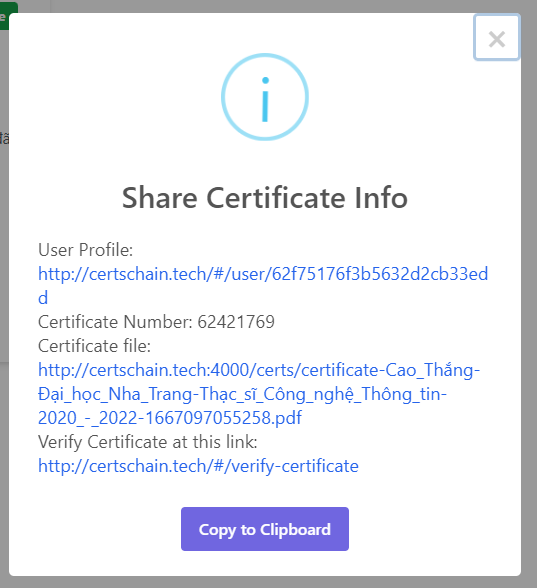


Hình 27. Trang danh sách Certificate của Holder

Holder có thể tải xuống hoặc xem trực tiếp file chứng chỉ bằng cách click vào button *View Certificate* hay *Download*

Ngoài ra, Holder có thể lấy VBCC này chia sẻ cho nhà tuyển dụng hay bất kỳ ai bằng cách gửi mã số VBCC và file PDF cho Verifier.

Hoặc click vào button *Share* ở certificate, thông tin chia sẻ của VBCC sẽ được hiển thị lên trong dialog như dưới:



Hình 28. Popup chia sẻ thông tin Certificate

Tiếp đó, Holder có thể click vào button *Copy to Clipboard* để copy và gửi đi.

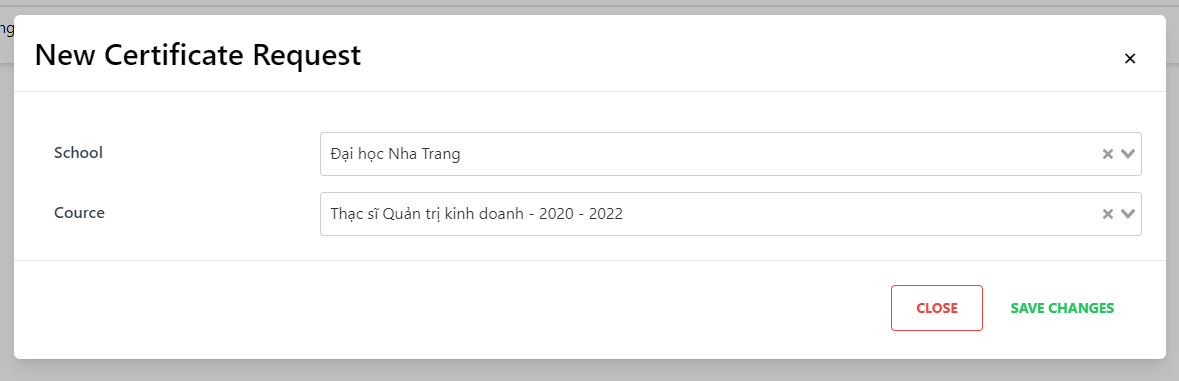
#### Trang Certificate Requests

Hiển thị danh sách các yêu cầu cấp phát VBCC của Holder:



Hình 29. Trang Certificate Requests của Holder

Để tạo mới một yêu cầu cấp phát VBCC, Holder sẽ click vào button *New Certificate* Request, chọn Trường và khóa học sau đó gửi đi và đợi Issuer xử lý yêu cầu của mình.

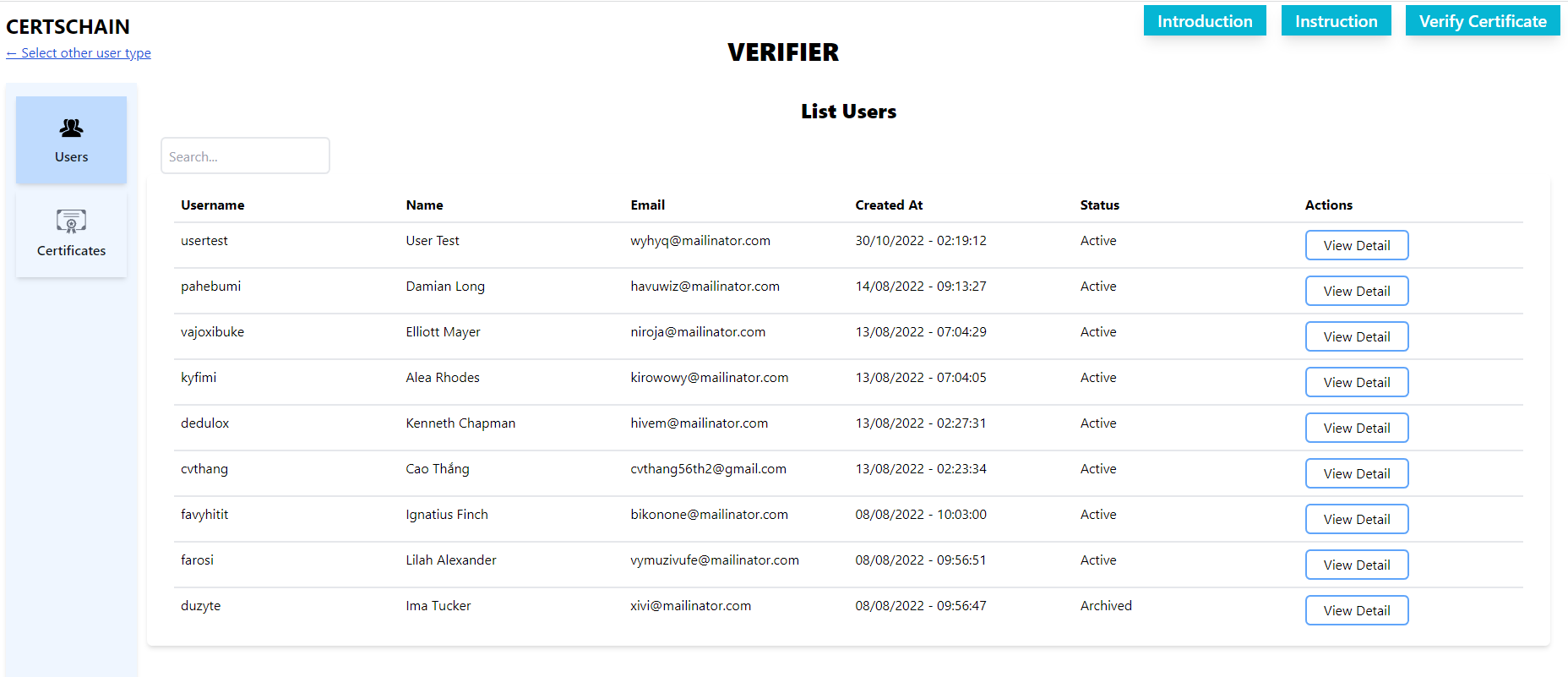


Hình 30. Popup tạo mới yêu cầu cấp phát VBCC

### Người dùng loại Verifier

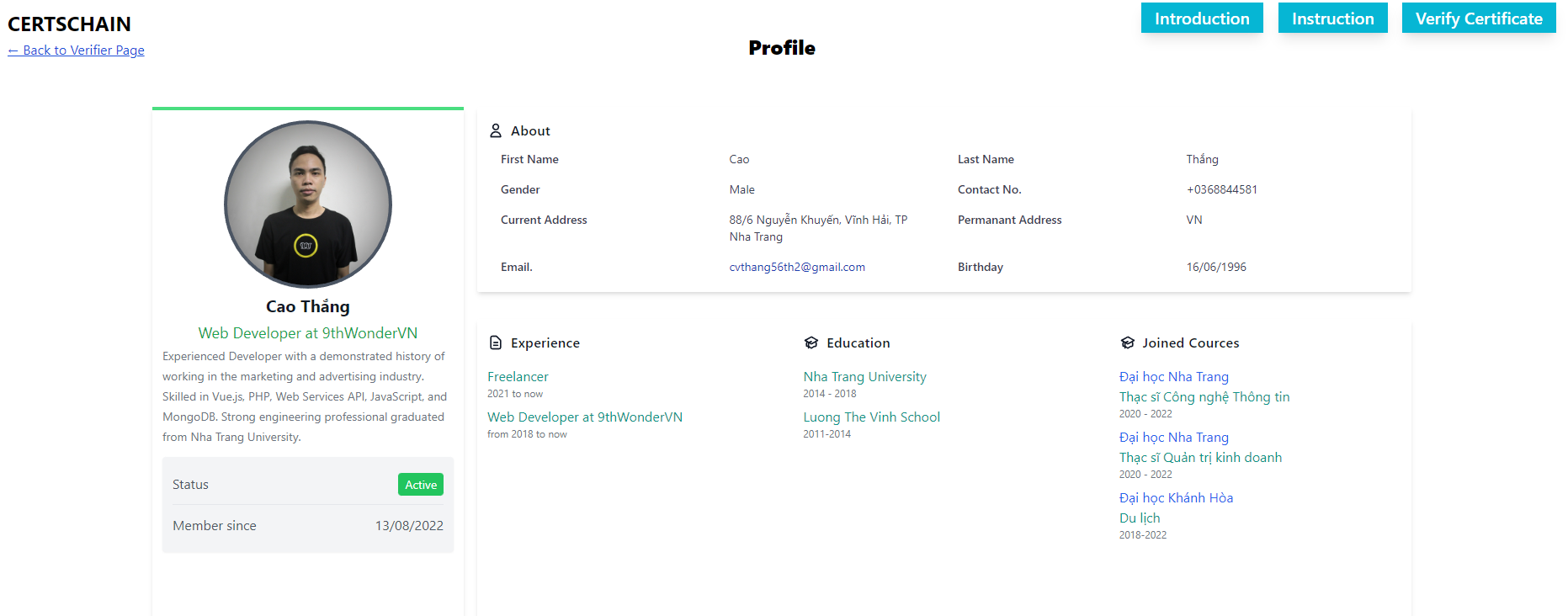
#### Trang Users

Hiển thị ra tất cả các Users có trong hệ thống



Hình 31. Danh sách tất cả các User trong hệ thống

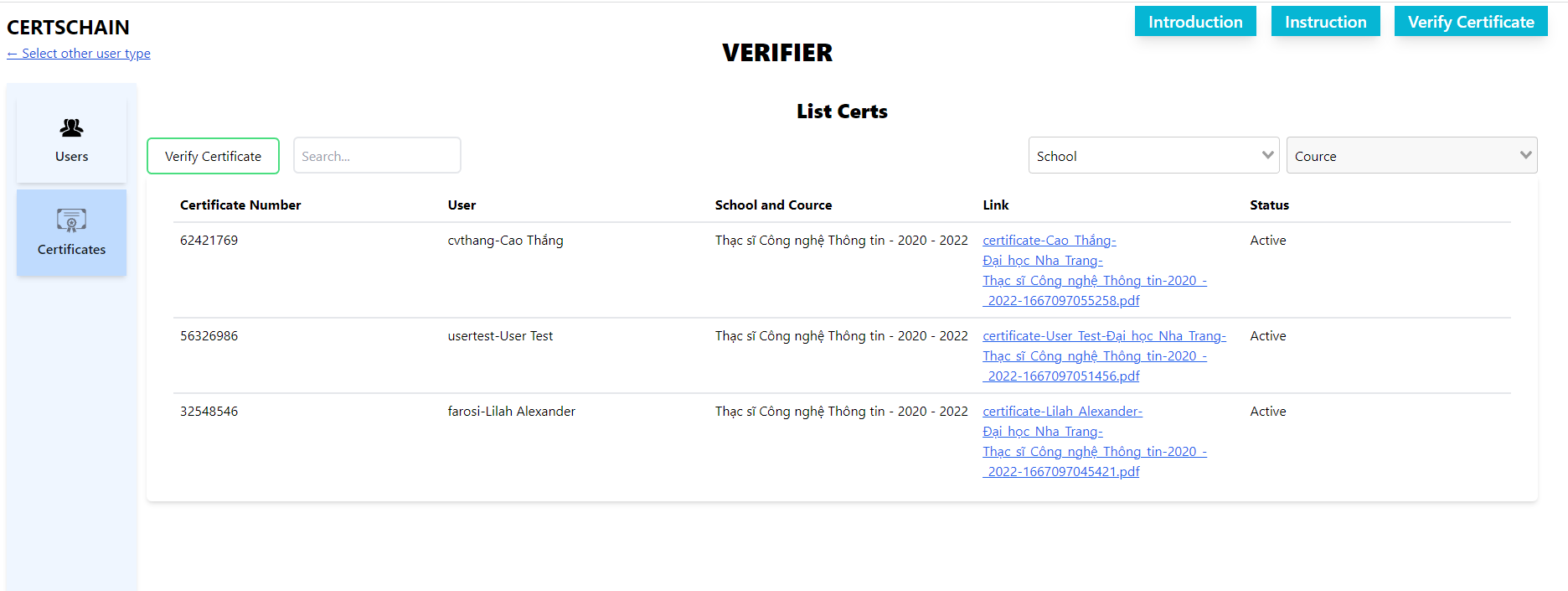
Bất kỳ ai cũng có thể xem chi tiết thông tin công khai của user trong hệ thống. Bằng cách click vào button *View Detail*.



Hình 32. Trang chi tiết User

#### Trang Certificates

Hiển thị tất cả các certificate có trong hệ thống, bất kỳ ai cũng có thể xem danh sách này.

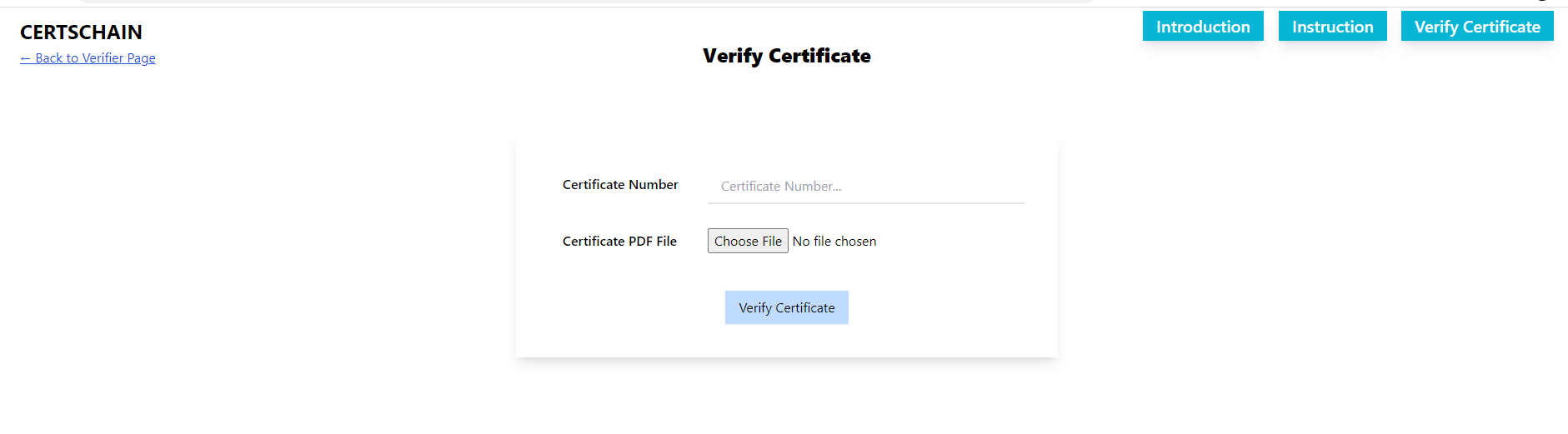


Hình 33. Danh sách tất cả các certificate trong hệ thống

### Trang Verify Certificate

Trang này dùng để User có thể xác minh VBCC

* + Có được cấp phát bởi hệ thống hay không .
  + Có bị thay đổi gì không.
  + Có còn đang được công nhận hay đang còn hiệu lực hay không.



Hình 34. Trang xác minh VBCC

User truy cập vào trang, nhập mã số, chọn file PDF của VBCC và click Verify Certificate để xác minh tính xác thực của VBCC.

* *Nếu đây là một VBCC hợp lệ*

Hệ thống sẽ thông báo như sau



* *Nếu VBCC không hợp lệ*

Hệ thống sẽ hiển thị một số lỗi như sau:

* + VBCC không được cấp phát bởi hệ thống



* + VBCC đã bị sửa chữa



* + VBCC không còn hiệu lực



# KẾT LUẬN VÀ KIẾN NGHỊ

## Kết quả đạt được

Sau thời gian thực hiện đề tài, hệ thống đã hoàn thành và tôi đã đạt được một số kết quả sau:

* + Hiểu và nắm rõ được khái niệm, các tính chất đặc trưng, cách.thức.hoạt.động của Blockchain.
  + Hiểu được.nghiệp.vụ quản lý và xác minh VBCC, các ưu nhược điểm của các mô hình quản lý VBCC.
  + Ứng dụng.kiến.thức.đã tìm hiểu, xây.dựng thành công web app CertsChain – hệ thống quản lý và xác minh VBCC sử dụng công nghệ Blockchain, đáp ứng được yêu cầu của bài toán quản lý và xác minh VBCC đưa ra.
  + Đã cố gắng tối ưu nhất có thể về mặt giao diện của web app thân thiện, dễ sử dụng.
  + Hệ thống đã giúp các đơn vị phát hành - người nhận - đơn vị cần xác minh VBCC tiết kiệm thời gian, công sức để có thể phát hành - chia sẻ - xác minh VBCC. Dễ dàng quản lý thông tin chi tiết người dùng, các thông tin về VBCC từ đó sẽ thuận tiện cho mục đích tuyển dụng, chứng minh năng lực,...
  + Thực hiện kiểm thử phần mềm ở mức độ lập trình.
  + Đã triển khai lên internet tại địa chỉ: <http://certschain.tech/>
  + Mã nguồn đã được công khai trên git: <https://github.com/cvthang56th2/CertsChain>

## Hạn chế của đề tài

* + Chưa áp.dụng.cho bất kỳ cơ sở đào tạo nào.

## Hướng phát triển của đề tài

* + Áp dụng vào một số cơ sở cụ thể ví dụ như trường đại học, cơ sở đào tạo tiếng anh, lập trình,…
  + Nâng cao hiệu suất của web hơn nữa.

## Đề nghị ý kiến

Trong thời gian thực hiện đề tài này, tôi không thể tránh khỏi những thiếu sót, rất mong nhận được ý kiến đóng góp từ phía quý thầy cô và các bạn để tôi hoàn thiện hơn hệ Ithống Iquản.lý.văn.bằng Ichứng.chỉ Isử Idụng.công.nghệ.Blockchain.này.

# TÀI LIỆU THAM KHẢO

[1]. Wikipedia, Blockchain

<https://vi.wikipedia.org/wiki/Blockchain>

[2]. PGS. TS. Huỳnh Tường Nguyên, Ứng dụng công nghệ Blockchain trong việc cấp phát và quản lý văn bằng, chứng chỉ Đại học Bách Khoa TP Hồ Chí Minh – 2020

[3]. Trần Tuấn Linh, luận văn thạc sĩ Áp dụng công nghệ Blockchain trong việc quản lý chứng chỉ đào tạo, Đại học Công Nghệ - Đại học Quốc Gia Hà Nội, năm 2019

[4]. Nguyễn Đức Duy, Nghiên cứu ứng dụng Blockchain cho bài toán thanh toán phi tiền mặt trong lĩnh vực tài chính ngân hàng, Học viện Bưu chính Viễn thông, Hà Nội, năm 2020

[5]. Đoàn Ngọc Sơn, luận văn thạc sĩ Nghiên cứu, ứng dụng công nghệ Blockchain trong thanh toán di động, Đại học Công Nghệ - Đại học Quốc Gia Hà Nội, năm 2017

[6]. Nguyen Van Hien, Tản mạn về các ứng dụng của Blockchain

<https://viblo.asia/p/tan-man-ve-cac-ung-dung-cua-blockchain-XL6lAXANZek>

[7]. Vân Anh, Ứng dụng Blockchain và chữ ký số giải bài toán xác thực văn bằng, chứng chỉ

<https://ictnews.vietnamnet.vn/cuoc-song-so/>

[8]. Ninoslav Marina, Pavel Taskov: Blockchain-Based Application for Certification Management - University of Information Science and Technology "St. Paul the Apostle", Partizanska bb, 6000 Ohrid, North Macedonia.

[9]. Preeti Bhaskar, Chandan Kumar Tiwari, Amit Joshi: Blockchain in education management: present and future applications - Interactive Technology and Smart Education - ISSN: 1741-5659 Article publication date: 16 November 2020

[10]. Grigore Albeanu: Blockchain technology and education - The 12th International Conference on Virtual Learning ICVL 2017

[11]. Ali Alammary, Samah Alhazmi, Marwah Almasri and Saira Gillani: Blockchain-Based Applications in Education: A Systematic Review - Applied Sciences. 2019; 9(12):2400. https://doi.org/10.3390/app9122400

[12]. Channel Youtube Microsoft Mechanics: Verifiable Credentials Using Blockchain | Digital Identity | Microsoft Ignite 2020

<https://youtu.be/r20hCF9NbTo>

[13]. Channel Youtube Blockchain Council: Blockchain Use Case #3 | Education Industry | Blockchain Council

<https://youtu.be/0w6ii3HFmYo>