**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 xin cam đoan luận văn tốt nghiệp “Nghiên cứu và ứng dụng công nghệ Blockchain trong quản lý và xác minh văn bằng chứng chỉ” là công trình nghiên cứu của bản thân. Những phần sử dụng tài liệu tham khảo trong luận văn đã được nêu rõ trong phần tài liệu tham khảo. Các số liệu, kết quả trình bày trong luận văn là hoàn toàn trung thực, nếu sai tôi xin chịu hoàn toàn trách nhiệm và chịu mọi kỷ luật của bộ môn và nhà trường đề ra.

Khánh Hòa, ngày …… tháng ……… năm 2022

Sinh viên thực hiện

*Cao Viết Thắng*

# LỜI CẢM ƠN

Tôi xin chân thành cảm ơn khoa Sau Đại học Trường Đại học Nha Trang đã tạo điều kiện tốt cho tôi thực hiện tốt đề tài luận văn tốt nghiệp này.

Ngoài ra, tôi xin chân thành cảm ơn quý thầy cô trong khoa Công nghệ Thông tin đã tận tình giảng dạy, trang bị cho tôi những kiến thức quý báu trong những năm học qua, giúp tôi có một nền tảng kiến thức vững chắc để hoàn thành luận văn này. Đặc biệt tôi xin chân thành cám ơn sự nhiệt tình hướng dẫn và đóng góp ý kiến của thầy TS. Nguyễn Đình Hưng - giảng viên khoa Công nghệ Thông tin đã giúp tôi hoàn thành tốt luận văn tốt nghiệp.

Mặc dù, tôi đã cố gắng hoàn thành luận văn tốt nghiệp trong phạm vi và khả năng cho phép nhưng chắc chắn vẫn không tránh khỏi những thiếu sót. Tôi kính mong nhận được sự thông cảm và tận tình đóng góp ý kiến của quý thầy cô và các bạn.

Tôi xin chân thành cảm ơn!

# MỤC LỤC

Đề mục Trang

Trang bìa i

[QUYẾT ĐỊNH GIAO ĐỀ TÀI ii](#_Toc111498851)

[CAM ĐOAN CỦA HỌC VIÊN iii](#_Toc111498852)

[LỜI CẢM ƠN iv](#_Toc111498853)

[MỤC LỤC v](#_Toc111498854)

[DANH SÁCH HÌNH VẼ viii](#_Toc111498855)

[DANH SÁCH BẢNG BIỂU x](#_Toc111498856)

[DANH SÁCH CÁC TỪ VIẾT TẮT xi](#_Toc111498857)

[MỞ ĐẦU 12](#_Toc111498858)

[ Lý do chọn đề tài 12](#_Toc111498859)

[ Mục đích, đối tượng, chủ thể và phạm vi nghiên cứu 13](#_Toc111498860)

[ Phương pháp nghiên cứu 13](#_Toc111498861)

[ Ý nghĩa khoa học và thực tiễn của luận văn 13](#_Toc111498862)

[CHƯƠNG 1. GIỚI THIỆU CÔNG NGHỆ BLOCKCHAIN 14](#_Toc111498863)

[1.1. Giới thiệu BlockChain 14](#_Toc111498864)

[1.2. Nền tảng lý thuyết 15](#_Toc111498865)

[1.2.1. Hàm băm 15](#_Toc111498866)

[1.2.2. Chữ ký số 17](#_Toc111498867)

[1.3. Các kỹ thuật chính của BlockChain 18](#_Toc111498868)

[1.3.1. Cấu trúc phi tập trung 19](#_Toc111498869)

[1.3.2. Tính toán tin cậy 21](#_Toc111498870)

[1.3.3. Bằng chứng công việc 21](#_Toc111498871)

[1.4. Tính chất của Blockchain 21](#_Toc111498872)

[1.4.1. Cơ chế đồng thuận phân quyền (decentralized consensus) 21](#_Toc111498873)

[1.4.2. Bảo trì tập thể (collective maintenance) 21](#_Toc111498874)

[1.4.3. Tính bảo mật và độ tin cậy 22](#_Toc111498875)

[1.4.4. Mã nguồn mở 22](#_Toc111498876)

[1.5. Phân loại các hệ thống Blockchain 22](#_Toc111498877)

[1.6. Các ứng dụng điển hình của công nghệ Blockchain 23](#_Toc111498878)

[1.6.1. Ứng dụng Blockchain trong tiền số 23](#_Toc111498879)

[1.6.2. Ứng dụng Blockchain trong hợp đồng thông minh (Smart Contract) 23](#_Toc111498880)

[1.6.3. Một số ứng dụng nổi bật khác 24](#_Toc111498881)

[CHƯƠNG 2. TỔNG QUAN QUẢN LÝ VÀ XÁC MINH VĂN BẰNG, CHỨNG CHỈ 26](#_Toc111498882)

[2.1. Giới thiệu công tác quản lý và xác minh văn bằng, chứng chỉ 26](#_Toc111498883)

[2.1.1. Văn bằng, chứng chỉ là gì? 26](#_Toc111498884)

[2.1.2. Quy trình liên quan tới văn bằng, chứng chỉ 26](#_Toc111498885)

[2.1.3. Một số mô hình quản lý và xác minh văn bằng chứng chỉ không sử dụng BlockChain 27](#_Toc111498886)

[2.1.4. Mô hình quản lý và xác minh văn bằng chứng chỉ sử dụng Blockchain 29](#_Toc111498887)

[2.2. Tình hình và các nghiên cứu liên quan 31](#_Toc111498888)

[2.2.1. Blockcerts 31](#_Toc111498889)

[2.2.2. BTCert 33](#_Toc111498890)

[CHƯƠNG 3. ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN TRONG QUẢN LÝ VÀ XÁC MINH VĂN BẰNG, CHỨNG CHỈ 34](#_Toc111498891)

[3.1. Thiết kế hệ thống CertsChain 34](#_Toc111498892)

[3.1.1. Định nghĩa bài toán 34](#_Toc111498893)

[3.1.2. Mô hình thực hiện 35](#_Toc111498894)

[3.1.3. Sơ đồ phân rã chức năng 36](#_Toc111498895)

[3.1.4. Cơ sở dữ liệu 41](#_Toc111498896)

[3.2. Xây dựng hệ thống CertsChain 42](#_Toc111498897)

[3.2.1. Môi trường triển khai và công cụ phát triển 42](#_Toc111498898)

[3.2.2. Xây dựng Blockchain của hệ thống 43](#_Toc111498899)

[3.2.3. Xây dựng hệ thống API 44](#_Toc111498900)

[3.3. Thực nghiệm hệ thống CertsChain 46](#_Toc111498901)

[3.3.1. Người dùng loại Issuer 47](#_Toc111498902)

[3.3.2. Người dùng loại holder 52](#_Toc111498903)

[3.3.3. Người dùng loại verifier 54](#_Toc111498904)

[3.3.4. Trang Verify Certificate 55](#_Toc111498905)

[3.4. Đánh giá kết quả **Error! Bookmark not defined.**](#_Toc111498906)

[CHƯƠNG 4. KẾT LUẬN VÀ KIẾN NGHỊ 57](#_Toc111498907)

[4.1. Kết quả đạt được 57](#_Toc111498908)

[4.2. Hạn chế của đề tài **Error! Bookmark not defined.**](#_Toc111498909)

[4.3. Hướng phát triển của đề tài 57](#_Toc111498910)

[4.4. Đề nghị ý kiến 57](#_Toc111498911)

[TÀI LIỆU THAM KHẢO 58](#_Toc111498912)

# DANH SÁCH HÌNH VẼ

[Hình 1. Mô hình thực hiện chữ ký số 17](#_Toc111498448)

[Hình 2. Cấu trúc dữ liệu của Blockchain 18](#_Toc111498449)

[Hình 3. Cấu trúc của block gốc trong Blockchain 19](#_Toc111498450)

[Hình 4. Mô hình thực hiện của hệ thống 35](#_Toc111498451)

[Hình 5. Sơ đồ phân rã chức năng Issuer 38](#_Toc111498452)

[Hình 6. Sơ đồ phân rã chức năng Holder 39](#_Toc111498453)

[Hình 7. Sơ đồ phân rã chức năng Verifier 40](#_Toc111498454)

[Hình 8. Cơ sở dữ liệu của hệ thống CertsChain 41](#_Toc111498455)

[Hình 9. Vue.js 42](#_Toc111498456)

[Hình 10. NodeJS - Express 43](#_Toc111498457)

[Hình 11. Trang chủ 46](#_Toc111498458)

[Hình 12. Trang đăng nhập 46](#_Toc111498459)

[Hình 13. Trang Profile của Issuer 47](#_Toc111498460)

[Hình 14. Trang Users của Issuer 47](#_Toc111498461)

[Hình 15. Popup tạo mới User 48](#_Toc111498462)

[Hình 16. Popup cập nhật User 48](#_Toc111498463)

[Hình 17. Trang Schools and Cources của Issuer 49](#_Toc111498464)

[Hình 18. Popup tạo mới School and Cource 49](#_Toc111498465)

[Hình 19. Popup cập nhật School and Cource 49](#_Toc111498466)

[Hình 20. Trang Certificates của Issuer 50](#_Toc111498467)

[Hình 21. Popup tạo mới Certificate 50](#_Toc111498468)

[Hình 22. Mẫu văn bằng chứng chỉ của CertsChain 50](#_Toc111498469)

[Hình 23. Trang Certificate Requests của Issuer 51](#_Toc111498470)

[Hình 24. Trang Profile của Holder 52](#_Toc111498471)

[Hình 25. Trang danh sách Certificate của Holder 52](#_Toc111498472)

[Hình 26. Popup chia sẻ thông tin Certificate 53](#_Toc111498473)

[Hình 27. Trang Certificate Requests của Holder 53](#_Toc111498474)

[Hình 28. Popup tạo mới yêu cầu cấp phát VBCC 53](#_Toc111498475)

[Hình 29. Danh sách tất cả các User trong hệ thống 54](#_Toc111498476)

[Hình 30. Trang chi tiết User 54](#_Toc111498477)

[Hình 31. Danh sách tất cả các certificate trong hệ thống 55](#_Toc111498478)

[Hình 32. Trang xác minh VBCC 55](#_Toc111498479)

# DANH SÁCH BẢNG BIỂU

[Bảng 1. Các chức năng của Issuer 36](#_Toc111498480)

[Bảng 2. Các chức năng của Holder 38](#_Toc111498481)

[Bảng 3. Các chức năng của Verifier 40](#_Toc111498482)

[Bảng 4. Các API của hệ thống CertsChain 44](#_Toc111498483)

# 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 nhiên, hiện nay, các văn bằng, chứng chỉ chủ yếu được các các cơ sở đào tạo cấp dạng vật lý (giấy, polymer,…) với nhiều bất cập như tốn không gian lưu trữ, khả năng mất mát, hư hỏng cao, và nhất là dễ bị làm giả. Công tác xác minh bằng cấp, chứng chỉ cũng hết sức mất thời gian. Vì vậy, nếu có cách xác minh chứng chỉ một cách chính xác, nhanh chóng thì bằng cấp, chứng chỉ giả không còn có cơ hội tồn tại.

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 một học viên cao học ngành Công nghệ thông tin, tôi luôn muốn làm chủ được kiến thức cũng như cách thức vận hành của những công nghệ như Blockchain. Và có thể áp dụng được để xây dựng hệ thống quản lý và xác minh văn bằng chứng chỉ. Vì vậy, tôi quyết định chọn đề tài “Nghiên cứu và ứng dụng công nghệ Blockchain trong quản lý và xác minh văn bằng chứng chỉ” để làm đề tài tốt nghiệp Thạc sĩ của 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 chứng chỉ dễ dàng tạo và quản lý chứng chỉ cho các học viên của mình.
  + Giúp học viên có thể chia sẽ thông tin cá nhân và chứng chỉ 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 biết đến là một công nghệ giúp các hệ thống có bảo mật cao. Blockchain được thiết kế để chống lại việc thay đổi của dữ liệu: Một khi dữ liệu đã được thay đổi trong mạng thì sẽ khó có thể thay đổi được. Nếu một phần của hệ thống Blockchain sụp đổ, những máy tính và nút khác sẽ tiếp tục hoạt động để bảo vệ thông tin.

Công nghệ Blockchain là một loại chương trình để lưu, xác nhận, vận chuyển và truyền thông dữ liệu trong mạng thông qua các nút phân phối của riêng nó mà không phụ thuộc vào bên thứ ba.

Một số trích dẫn đáng chú ý về công nghệ này được liệt kê dưới đây:

“Thế hệ đầu tiên của cuộc cách mạng kỹ thuật số mang lại cho chúng ta thông tin của Internet. Thế hệ thứ hai - được hỗ trợ bởi công nghệ Blockchain - mang lại cho chúng ta giá trị của Internet: một nền tảng mới để định hình lại thế giới kinh doanh và biến đổi thứ tự công việc của con người trở nên tốt hơn.”

“Blockchain là một kho lưu trữ, cơ sở dữ liệu phân tán toàn cầu, chạy trên hàng triệu thiết bị và mở cho mọi người, không chỉ đơn thuần là thông tin mà còn cả những thứ có giá trị, cả danh hiệu, hành vi, danh tính, thậm chí cả phiếu bầu - có thể được di chuyển, lưu trữ và quản lý một cách an toàn và tư nhân. Sự tin tưởng được thiết lập thông qua hợp tác giữa số đông và mã thông minh chứ không phải bởi các nhà trung gian mạnh mẽ như các chính phủ và ngân hàng.”

Không lâu sau khi Bitcoin được phát hành trên thế giới, nhiều người nhanh chóng nhận ra công nghệ đằng sau Bitcoin – Blockchain – có thể làm được nhiều hơn là xử lý các giao dịch tiền tệ. Nhà phân phối lớn nhất thế giới cho những hợp đồng tài chính cho rằng có thể làm cho các hợp đồng trở nên an toàn hơn bằng cách xây dựng một hệ thống dựa trên công nghệ Blockchain vào năm 2018. Nếu kế hoạch này đi vào hoạt động, mỗi năm sẽ có 11 nghìn tỷ USD được giao dịch qua hệ thống này.

## Nền tảng lý thuyết

Công nghệ Blockchain được phát triển dựa trên hai nền tảng kỹ thuật chính là hàm băm và chữ ký số. Mỗi người dùng sẽ sở hữu một cặp khóa gồm khóa bí mật và khóa công khai. Khóa bí mật được lưu trữ bí mật và sử dụng để ký kết các giao dịch. Các giao dịch đã ký dùng chữ ký số được phát đi trên toàn bộ mạng. Chữ ký số liên quan đến hai giai đoạn: giai đoạn ký kết và giai đoạn xác minh.

Ví dụ: người dùng A muốn gửi một thông báo cho người dùng B, trong giai đoạn ký, A mã hóa dữ liệu của mình bằng khóa bí mật và gửi cho B kết quả đã được mã hóa và dữ liệu gốc. Trong giai đoạn xác minh, B xác nhận giao dịch bằng khóa công khai của A. Bằng cách đó, B có thể dễ dàng kiểm tra xem dữ liệu có bị giả mạo hay không.

### Hàm băm

Hàm băm dùng để chuyển đổi từ một thông tin sang một đoạn mã. Bất kỳ nỗ lực gian lận nào để thay đổi bất kỳ phần nào của Blockchain sẽ bị phát hiện ngay lập tức vì giá trị băm mới sẽ không phù hợp với thông tin cũ trên Blockchain. Bằng cách này, ngành khoa học bảo mật thông tin (cần thiết cho việc mã hóa thông tin và mua sắm trực tuyến, ngân hàng) đã trở thành một công cụ hiệu quả để giao dịch mở.

#### Khái niệm hàm băm

**Hàm băm** (hash function) là thuật toán dùng để ánh xạ dữ liệu có kích thước bất kỳ sang một giá trị “băm” có kích thước cố định, giá trị băm còn được gọi là “đại diện thông điệp” hay “đại diện bản tin”.

Hàm băm là hàm một chiều, theo nghĩa giá trị của hàm băm là duy nhất, và từ giá trị băm này, **“khó”** có thể suy ngược lại được nội dung hay độ dài ban đầu của thông điệp gốc.

Các hàm băm dòng MD: MD2, MD4, MD5 được Rivest đưa ra có kết quả đầu ra với độ dài là 128 bit. Hàm băm MD4 đưa ra vào năm 1990. Một năm sau phiên bản mạnh MD5 cũng được đưa ra. Chuẩn hàm băm an toàn: SHA, phức tạp hơn nhiều cũng dựa trên các phương pháp tương tự, được công bố trong Hồ sơ Liên bang năm 1992 và được chấp nhận làm tiêu chuẩn vào năm 1993 do Viện Tiêu Chuẩn và Công Nghệ Quốc Gia (NIST), kết quả đầu ra có độ dài 160 bit.

#### Đặc tính của hàm băm

Hàm băm **h** là hàm một chiều (One-way Hash) với các đặc tính sau:

* Với thông điệp đầu vào (bản tin gốc) **x**, chỉ thu được giá trị duy nhất **z** = **h**(**x**).
* Nếu dữ liệu trong bản tin **x** bị thay đổi hay bị xóa để thành bản tin **x**’, thì giá trị băm **h**(**x**’) ≠ (**x**). Cho dù chỉ là một sự thay đổi nhỏ, ví dụ chỉ thay đổi 1 bit dữ liệu của bản tin gốc **x**, thì giá trị băm **h**(**x**) của nó cũng vẫn thay đổi. Điều này có nghĩa là: hai thông điệp khác nhau, thì giá trị băm của chúng cũng khác nhau.

Ví dụ: Ta áp dụng hàm hash vào 2 đoạn text: “This is a test” và “this is a test”, mặc dù bạn chỉ thay đổi duy nhất một chữ cái đầu tiên của đầu vào thì đầu ra đã gần như thay đổi hoàn toàn



* Nội dung của bản tin gốc “khó” thể suy ra từ giá trị hàm băm của nó. Nghĩa là: với thông điệp **x** thì “dễ” tính được **z** = **h**(**x**), nhưng lại “khó” tính ngược lại được **x** nếu chỉ biết giá trị băm **h**(**x**) (Kể cả khi biết hàm băm **h**).

#### Ứng dụng của hàm băm

Hàm băm được sử dụng trong nhiều ứng dụng thực tế, dưới đây là một số ứng dụng nổi bật của hàm băm được sử dụng phổ biến:

* Đảm bảo dữ liệu không bị sửa đổi: Khi Thắng muốn gửi tài liệu **X** cho Vi, Thắng gửi cả giá trị băm của **X** và thuật toán băm. Khi nhận được tài liệu **X**, Vi dùng thuật toán băm đó băm lại **X** và so sánh với giá trị băm Thắng đã gửi, nếu kết quả không trùng khớp chứng tỏ tài liệu **X** đã bị chỉnh sửa.
* Hỗ trợ các thuật toán chữ ký số: Hàm băm giúp tạo ra đại diện tài liệu, các thuật toán ký số thay vì ký trên tài liệu ban đầu có dung lượng lớn, sẽ ký lên đại diện của tài liệu đó. Thời gian thực hiện của thuật toán ký sẽ nhanh hơn nhiều lần.
* Xây dựng cấu trúc dữ liệu bảng băm: Bảng băm là một cấu trúc dữ liệu cho phép tổ chức lưu trữ và tìm kiếm dữ liệu một cách nhanh chóng và thuận tiện.

### Chữ ký số

#### Khái niệm chữ ký số

Về mặt công nghệ, chữ ký số là một thông điệp dữ liệu đã được mã hóa gắn kèm theo một thông điệp dữ liệu khác nhằm xác thực người gửi thông điệp đó. Quá trình ký và xác nhận chữ ký như sau: Người gửi muốn gửi thông điệp cho bên khác thì sẽ dùng một hàm băm, băm thông điệp gốc thành một “thông điệp tóm tắt” (Message Digest), thuật toán này được gọi là thuật toán băm (hash function) đã được trình bày trong mục 1.2.1. Người gửi mã hóa bản tóm tắt thông điệp bằng khóa bí mật của mình (sử dụng phần mềm bí mật được cơ quan chứng thực cấp) để tạo thành một chữ ký số. Sau đó, người gửi tiếp tục gắn kèm chữ ký số này với thông điệp dữ liệu ban đầu và gửi thông điệp đã gắn kèm với chữ ký một cách an toàn qua mạng cho người nhận.

Sau khi nhận được, người nhận sẽ dùng khóa công khai của người gửi để giải mã chữ ký số thành bản tóm tắt thông điệp. Người nhận cũng dùng hàm băm giống hệt như người gửi đã làm đối với thông điệp nhận được để biến đổi thông điệp nhận được thành một bản tóm tắt thông điệp. Người nhận so sánh hai bản tóm tắt thông điệp này, nếu chúng giống nhau tức là chữ ký số đó là xác thực và thông điệp đã không bị thay đổi trên đường truyền đi.

Ngoài ra, chữ ký số có thể được gắn thêm một “nhãn” thời gian: sau một thời gian nhất định quy định bởi nhãn đó, chữ ký gốc sẽ không còn hiệu lực, đồng thời 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 có ý nghĩa to lớn và trở thành một phần không thể thiếu đối với ngành mật mã học. Ứng dụng của chữ ký số đã được triển khai trên nhiều quốc gia trên thế giới, trong đó có Việt Nam. So với chữ ký tay, chữ ký số giúp các cá nhân, doanh nghiệp thực hiện việc ký các tài liệu được nhanh chóng, hiệu quả hơn. Một số ứng dụng cụ thể của chữ ký số trong thực tế có thể kể đến như sau:

Ứng dụng trong chính quyền điện tử: Các cá nhân và doanh nghiệp sẽ không cần đến các cơ quan nhà nước để xuất trình giấy tờ cũng như ký kết các giấy tờ. Thay vào đó, việc ký và gửi các tài liệu hoàn toàn thông qua hệ thống máy tính. Hiện nay ngành thuế ở Việt Nam đã cho phép gửi tài liệu kê khai thuế qua mạng sử dụng chữ ký số.

Ứng dụng trong ký kết hợp đồng: Việc ký kết các hợp đồng thường được thực hiện với sự có mặt của tất cả các bên liên quan và cần người chứng kiến, điều này gây tốn thời gian đặc biệt là khi các bên ở xa nhau về khoảng cách địa lý. Chữ ký số có thể cải thiện được việc này, các bên có thể xác thực được chữ ký của các bên liên quan khác thông qua các thuật toán kiểm tra chữ ký.

Trong tương lai, tiềm năng của chữ ký số chắc chắn sẽ còn tiến xa hơn nữa và có thể được ứng dụng trong nhiều ứng dụng cụ thể khác như bỏ phiếu điện tử, y tế điện tử, …

## Các kỹ thuật chính của BlockChain

Công nghệ Blockchain tương đồng với cơ sở dữ liệu, chỉ khác ở việc tương tác với cơ sở dữ liệu. Để hiểu Blockchain, cần nắm được năm định nghĩa sau: chuỗi khối (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 nền tảng của việc tạo ra các ứng dụng phân tán.



Hình 2. Cấu trúc dữ liệu của Blockchain

### Cấu trúc phi tập trung

Cơ chế này ngược lại với mô hình truyền thống – cơ sở dữ liệu được tập trung và được dùng để quản lý và xác thực giao dịch. Công nghệ Blockchain không dựa vào các tổ chức thứ ba để quản lý và xác thực, không có kiểm soát trung tâm, tất cả các nút nhận được thông tin tự kiểm tra, truyền tải, và quản lý, đặt sự tin tưởng vào các nút, cho phép các nút lưu trữ các giao dịch trong một khối (block). Các block được ghép nối với nhau tạo nên một chuỗi khối (Blockchain). Cấu trúc của một block được mô tả như hình 3. Cấu trúc phi tập trung là đặc điểm nổi bật và quan trọng nhất của Blockchain.



Hình 3. Cấu trúc của block gốc trong Blockchain

Mỗi block trong Blockchain thường bao gồm các thành phần sau:

* Index (Block #): Thứ tự của block (block gốc có thứ tự 0)
* Hash: Giá trị băm của block
* Previous Hash: Giá trị băm của block trước
* Timestamp: Thời gian tạo của block
* Data: Thông tin lưu trữ trong block
* Nonce: Giá trị biến thiên để tìm ra giá trị băm thỏa mãn yêu cầu của mỗi Blockchain.

Giá trị băm (Hash) sẽ băm toàn bộ các thông tin cần thiết như timestamp, previous hash, index, data, nonce.

Khi có một block mới được thêm vào, block mới sẽ có giá trị “Previous Hash” là giá trị băm của block được thêm trước nó. Blockchain tìm kiếm block được thêm vào gần nhất để lấy giá trị index và previous hash. Block tiếp theo của hình 3 sẽ được tính như sau:

* Index: 0+1 = 1
* Previous Hash: 0000018035a828da0…
* Timestamp: thời gian block được tạo ra
* Data: dữ liệu lưu trữ trong block
* Hash: **??**
* Nonce: **??**

Ta cần tìm giá trị “nonce” phù hợp để có giá trị băm Hash thỏa kiện của Blockchain (có 4 số 0 ở đầu giá trị băm). Với số lượng số 0 ở đầu là “difficulty”. Mã giả của hàm kiểm tra giá trị Hash có thỏa mãn hay không được viết như sau:



Công việc trên cũng được gọi là bằng chứng công việc (Proof of Work)

Quá trình tìm kiếm giá trị Nonce được thực hiện bằng mã giả sau:



Sau khi tìm được nonce và có được hash, dùng 2 giá trị này gắn vào block trên, ta sẽ hoàn thành việc tạo ra một block mới.

Bằng cách lưu trữ dữ liệu trên tất cả các nút của mình, mạng Blockchain loại bỏ các rủi ro đi kèm với dữ liệu được tổ chức lưu trữ tập trung. Trong mạng không có các điểm tập trung dễ bị tổn thương cho hệ thống, không có các điểm trung tâm làm cho hệ thống dừng hoạt động (central point of failure). Bất kỳ nút nào trong mạng khi dừng hoạt động sẽ không ảnh hưởng đến sự vận hành của hệ thống.

### Tính toán tin cậy

Mỗi nút trong mạng có một bản sao lưu trữ toàn bộ Blockchain, chất lượng phụ thuộc vào sự đồng bộ liên tục theo thời gian giữa các nút. Các nút trong mạng đều có độ tin cậy như nhau, không có nút nào đáng tin cậy hơn nút nào. Trao đổi dữ liệu trong hệ thống không yêu cầu các nút tin tưởng lẫn nhau. Quy chế hoạt động của toàn bộ hệ thống và tất cả các nội dung dữ liệu đều công khai và minh bạch. Vì vậy, các nút không thể giả mạo các quy tắc và thời gian do hệ thống chỉ định.

### Bằng chứng công việc

Bằng chứng công việc (proof of work) trong một mạng Blockchain được hiểu là một thử thách cho các nút trong mạng. Cụ thể là các nút cần tìm ra các block mới của Blockchain bằng cách tìm ra giá trị băm thỏa mãn điều kiện cho trước. Trong mục 1.3.1, điều kiện này là giá trị “difficulty” – số lượng số 0 đứng phía trước giá trị băm.

## Tính chất của Blockchain

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

Cơ chế này ngược lại với mô hình cổ điển về cơ chế đồng thuận tập trung – nghĩa là khi một cơ sở dữ liệu tập trung được dùng để quản lý việc xác thực giao dịch. Một sơ đồ phi tập trung chuyển giao quyền lực và sự tin tưởng cho một mạng lưới ảo phi tập trung và cho phép các nút của mạng lưới đó liên tục lưu trữ các giao dịch trên một khối (block) công khai, tạo nên một chuỗi (chain) độc nhất: chuỗi khối (Blockchain). Mỗi khối kế tiếp chứa một giá trị băm của khối trước nó; vì thế, mã hóa (thông qua hàm băm) được sử dụng để bảo đảm tính xác thực của nguồn giao dịch và loại bỏ sự cần thiết phải có một bên trung gian. Sự kết hợp của mã hóa và công nghệ Blockchain lại đảm bảo rằng sẽ không bao giờ một giao dịch được thực hiện hai lần.

### Bảo trì tập thể (collective maintenance)

Khối dữ liệu (block) trong hệ thống được duy trì bởi tất cả các nút với chức năng bảo trì trong toàn bộ hệ thống. Bất kỳ nút nào cũng có khả năng ghi block vào Blockchain. Hơn nữa, các nút trong hệ thống có thể được tham gia bởi bất cứ ai.

### Tính bảo mật và độ tin cậy

Khi không nắm được 51% số nút trong mạng, dữ liệu mạng không thể bị kiểm soát và sửa đổi. Do đó, bản thân Blockchain đã trở nên tương đối an toàn và có thể tránh việc sửa đổi dữ liệu. Vì thế, nếu một số lượng lớn các nút có khả năng tính toán mạnh được tham gia vào hệ thống thì dữ liệu trong hệ thống này sẽ có độ bảo mật cao hơn.

### Mã nguồn mở

Công nghệ Blockchain được phát hành theo mã nguồn mở. Ngoài thông tin cá nhân được mã hóa bởi các bên kinh doanh, dữ liệu Blockchain có thể truy cập được bởi tất cả mọi người. Bất cứ ai cũng có thể tìm kiếm dữ liệu Blockchain thông qua giao diện công khai, cũng như phát triển các ứng dụng có liên quan. Toàn bộ hệ thống rất minh bạch.

## Phân loại các hệ thống Blockchain

Phân chia theo tính công khai, các hệ thống Blockchain hiện tại được chia làm 3 loại:

* Blockchain công khai: tất cả các dữ liệu được hiển thị công khai và tất cả mọi người có thể tham gia và trở thành một nút vào trong mạng Blockchain.
* Blockchain liên kết: chỉ có các nút được chỉ định để tham gia vào mạng Blockchain.
* Blockchain bí mật: chỉ bao gồm các nút của một tổ chức cụ thể.

## Các ứng dụng điển hình của công nghệ Blockchain

Blockchain được đảm bảo nhờ cách thiết kế sử dụng hệ thống lưu trữ phân cấp với khả năng chịu lỗi cao. Vì vậy Blockchain phù hợp để ghi lại những sự kiện, hồ sơ y tế, xử lý giao dịch, công chứng, danh tính và chứng minh nguồn gốc,… Công nghệ này có tiềm năng giúp chống lại việc dữ liệu bị thay đổi, xử lý các vấn đề thiếu tính minh bạch trong bối cảnh thương mại toàn cầu.

### Ứng dụng Blockchain trong tiền số

Blockchain không chỉ dành riêng cho Bitcoin. Blockchain là công nghệ đằng sau, bảo đảm cho Bitcoin và những đồng tiền số (digital currency) khác hoạt động. Điều này có nghĩa là: Bất cứ đồng tiền nào chưa chứng minh được chúng sở hữu công nghệ Blockchain thì chúng ta đều có quyền nghi ngờ tính chính xác của của đồng tiền đó.

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

Smart Contract (Hợp đồng thông minh) là một thuật ngữ mô tả khả năng tự đưa ra các điều khoản và thực thi thỏa thuận của hệ thống máy tính bằng cách sử dụng công nghệ Blockchain. Toàn bộ quá trình hoạt động của Smart Contract là hoàn toàn tự động và không có sự can thiệp từ các yếu tố bên ngoài. Xe tự lái, hợp đồng thuê nhà dạng chìa khóa trao tay hay thu phí bảo hiểm,… chỉ là một số ví dụ về cách Smart Contract có thể chi phối hoạt động kinh doanh và đời sống của con người trong tương lai.

Smart Contract giúp đảm bảo việc thực thi hợp đồng hiệu quả hơn hợp đồng truyền thống và giảm thiểu những chi phí giao dịch gây lãng phí cho các bên. Các điều khoản của Smart Contract tương đương với một hợp đồng pháp lý và được ghi lại dưới dạng ngôn ngữ lập trình và không thể thay đổi. Mục tiêu chính của Smart Contract là cho phép hai bên không cần xác định danh tính có thể làm việc hay giao dịch với nhau trên Internet mà không cần thông qua trung gian.

* **Sự khác biệt giữa Truyền thống và hiện đại**

Hợp đồng truyền thống được tạo ra bởi các chuyên gia pháp lý với một lượng lớn tài liệu và cần bên thứ ba chứng thực. Điều này rất mất thời gian và trên thực tế vẫn thường xảy ra các trường hợp lừa đảo, làm giả. Nếu hợp đồng xảy ra sự cố thì cần dựa vào sự giải quyết của tư pháp, điều này dẫn đến tốn kém nhiều chi phí liên quan. Thậm chí trường hợp xấu xảy ra là mâu thuẫn.

Với Smart Contract được tạo ra bởi hệ thống máy tính bằng các ngôn ngữ lập trình. Trong đó đã nêu rõ các điều khoản và hình phạt tương đương giống như hợp đồng truyền thống đưa ra. Điều khác biệt là, Smart Contract không cần bất cứ sự can thiệp nào của con người, do vậy đảm bảo việc thực thi là chính xác và công bằng nhất. Toàn bộ đoạn mã của Smart Contract được thực hiện bởi hệ thống sổ cái phân tán của Blockchain.

Như vậy, dựa trên công nghệ Blockchain, ứng dụng Smart Contract tiếp tục cho chúng ta thấy mức độ tin cậy cao về mặt thỏa thuận và triển khai thực thi. Điều này giúp chúng ta liên tưởng tới việc ứng dụng Smart Contract sẽ làm thay đổi hoàn toàn suy nghĩ của con người trong các mối quan hệ có sự ràng buộc. Đặc biệt trong kinh doanh, điều này là vô cùng cần thiết.

### Một số ứng dụng nổi bật khác

* *Ngành vận tải biển*

Maersk là công ty vận tải biển lớn nhất thế giới vừa qua đã hoàn tất việc thử nghiệm ứng dụng Blockchain vào theo dõi hàng hóa. Bài kiểm tra không chỉ có Maersk mà còn bao gồm sự tham gia của đại diện Hải quan Hà Lan và Bộ An Ninh Nội Địa Hoa Kỳ. Công nghệ Blockchain đảm bảo độ tin cậy thông qua chữ ký điện tử giúp cho việc bỏ sót hoặc gian lận hàng hóa trong quá trình vận chuyển trở nên khó khăn hơn và giảm thời gian trung chuyển hàng hóa.

* *Ngành ngân hàng*

Bất chấp sự phức tạp đặc thù của mình, ngành ngân hàng vẫn bị ám ảnh bởi các hệ thống chậm chạp có thể mất hàng giờ hoặc vài ngày để xác nhận các giao dịch cơ bản như bán cổ phiếu hoặc chuyển tiền. Tuy nhiên, việc Barclays (một công ty của nước Anh chuyên điều hành dịch vụ tài chính trên toàn thế giới) tiến hành một giao dịch đột phá (liên quan đến xuất khẩu bơ) bằng việc sử dụng công nghệ Blockchain vào năm 2016 cho thấy điều này đang dần thay đổi. Các ngân hàng lớn thậm chí đang dự kiến sử dụng Blockchain để làm lại hệ thống SWIFT - được sử dụng trong các giao dịch liên ngân hàng toàn cầu.

* *Ngành tạp hóa*

Walmart là một trong những doanh nghiệp tiên phong sử dụng Blockchain, gã khổng lồ bán lẻ này đã sử dụng Blockchain từ năm 2016 để theo dõi nguồn lợn nhập từ Trung Quốc đến Mỹ. Trong tháng 8, một nhóm nông dân ở tiểu bang Arkansas đã in mã QR trên thùng đựng thịt gà để theo dõi giao dịch. Tất cả những ứng dụng này đều giúp nhà cung cấp giảm thiểu số lượng thực phẩm bị hư hỏng và ngăn chặn bệnh dịch tràn lan.

* *Ngành luật pháp*

Tất cả các bản thỏa thuận từ bán nhà cho đến hợp đồng lao động đều yêu cầu có sự tham gia của luật sư và tòa án. Hiện nay, nhiều công ty đang thử nghiệm sáng kiến hợp đồng thông minh - một ứng dụng của công nghệ Blockchain - để giảm thiểu thủ tục. Cụ thể, hệ thống sẽ là nơi tiếp tiếp nhận chìa khóa an toàn của người cho thuê nhà và tiền của người đi thuê nhà. Nếu thời hạn giao nhận chìa khóa và tiền không trùng khớp thì hợp đồng sẽ không được thực thi. Hiện nay, các luật sư có thể chưa lo lắng vì hợp đồng thông minh vẫn còn là một khái niệm mới lạ, nhưng điều này có thể thay đổi sớm, đặc biệt là khi các tiểu bang như Arizona của Hoa Kỳ thông qua luật xác nhận hợp đồng thông minh là hợp lệ.

* *Ngành quản trị nhân lực*

Trong lĩnh vực này, quản lý thông tin chính là chìa khóa để thành công. Tính xác thực của thông tin nguồn nhân lực đã trở thành yếu tố quan trọng ảnh hưởng đến chi phí và hiệu quả của việc quản lý nguồn nhân lực. Với sự phát triển nhanh chóng của các thiết bị di động và công nghệ Internet, các rủi ro nhân lực khác nhau gây ra bởi sự sai sót thông tin mang lại thiệt hại kinh tế đối với các doanh nghiệp. Dựa vào nghiên cứu của Blockchain, một số mô hình đã được đưa ra nhằm mục đích kết hợp công nghệ mã hóa truyền thống với công nghệ Internet để thiết lập một mô hình quản lý thông tin nhân sự, góp phần làm giảm chi phí quản lý thông tin cho các doanh nghiệp.

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

Chương này sẽ giới thiệu một số mô hình quản lý và xác minh VBCC hiện có tại Việt Nam cũng như trên thế giới, nêu ra một số ưu nhược điểm của các mô hình và từ đó giới thiệu và đánh giá mô hình quản lý và xác minh văn bằng, chứng chỉ sử dụng Blockchain.

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

### Văn bằng, chứng chỉ là gì?

Văn bằng là giấy chứng nhận tốt nghiệp hoặc chứng nhận học vị, bằng cấp.

Chứng chỉ là một văn bản được bên này cấp cho bên kia để xác nhận là một sự kiện nào đó là đúng. Trong lĩnh vực giáo dục, chứng chỉ được sử dụng trong một số tình huống chứng minh cho một số việc như sau:

* + Người học đã đạt được kết quả học tập
  + Năng lực của giáo viên
  + Người học vượt qua một quá trình học tập
  + Tổ chức giáo dục hoặc khóa học đạt được những tiêu chuẩn nhất định.
  + Một cơ quan được ủy quyền cấp VBCC.

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

Thông thường, VBCC gồm có 03 quy trình chính như sau:

* **Phát hành:** đây là quá trình ghi lại các thông tin vào VBCC. Thông thường, dữ liệu được ghi lại:
  + Trong cơ sở dữ liệu tập trung của đơn vị phát hành.
  + Trên VBCC cấp cho người dùng.
* **Chia sẻ:** Đây là quá trình người được cấp VBCC chia sẻ cho một bên thứ ba. Cũng có 3 cách chia sẻ VBCC:
  + Chuyển trực tiếp VBCC (hoặc một bản cop) cho bên thứ ba. Ví dụ: qua email, hoặc đưa trực tiếp cho bên thứ ba.
  + Lưu VBCC với người được ủy quyền chỉ chia sẻ với một số người theo yêu cầu của bạn (ví dụ trong trường hợp di chúc, công chứng viên chỉ được phép chia sẻ nội dung di chúc với người thụ hưởng, sau khi một người chết)
  + Đưa VBCC vào một kho dữ liệu công cộng nơi tất cả mọi người đều có thể tra cứu được.
* **Xác minh:** đây là quá trình một bên thứ 3 xác minh lại tính xác thực của VBCC. Có 3 mô hình thực hiện việc này:

Xác minh dựa vào các tính năng bảo mật được xây dựng ngay bên trong VBCC: việc này có thể bao gồm những biện pháp như kiểm tra tính xác thực của con dấu, giấy chuyên dụng, chữ ký, ….

* + Xác minh dựa vào đơn vị phát hành: bên thứ ba thực hiện liên hệ với đơn vị phát hành, hỏi về việc có thực sự phát hành ra VBCC hay không. Tại đó, các đơn vị phát hành sẽ kiểm tra thông tin trên cơ sở dữ liệu tập trung của họ hoặc kiểm tra chức năng bảo mật trong chính VBCC đó.
  + Xác minh dựa vào cơ sở dữ liệu tập trung. Với cách này, các nhà phát hành có thể cung cấp dữ liệu về các VBCC đã cấp phát cho một bên thứ ba cho phép mọi người truy vấn dữ liệu để xem các bản copy của các VBCC được phát hành và so sánh 2 cái với nhau.

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

Các chính phủ và các ngành công nghiệp đang nỗ lực để số hóa VBCC trên toàn thế giới. Tuy vậy, hầu hết VBCC vẫn được phát hành trên giấy hoặc các vật liệu vật lý khác. Ở nhiều quốc gia, VBCC lai được sử dụng như một sự kết hợp nơi mà VBCC giấy được sao lưu bởi các cơ sở dữ liệu của một bên thứ ba chuyên cung cấp dịch vụ truy vấn thông tin (Ví du: <https://hedd.ac.uk/>). Tuy nhiên, các giới hạn của mỗi hệ thống cho thấy rõ nhu cầu về sự cần thiết có một công nghệ quản lý và xác minh VBCC tốt hơn, mạnh mẽ hơn.

#### Văn bằng chứng chỉ giấy

* **Ưu điểm:**
* Thường được giữ trực tiếp bởi người nhận nên người nhận có toàn quyền kiểm soát VBCC.
* Tương đối dễ để giữ VBCC an toàn.
* Người được cấp có thể đưa ra ở bất kỳ nơi nào mà họ muốn.
* **Nhược điểm:**
* Khó tạo ra do tính năng bảo mật được tích hợp trong giấy làm VBCC.
* Vẫn có nguy cơ làm giả, người phát hành phải giữ một quyển sổ lưu trữ thông tin văn bằng đã cấp để làm nhiệm vụ xác minh thông tin khi cần.
* Quyển sổ lưu trữ thông tin văn bằng này là điểm chết. Nếu mất thông tin trên sổ này sẽ không thể xác thực được thông tin.
* Việc xác minh cần thực hiện thủ công => tốn nhân lực
* Để VBCC càng bảo mật, thì phụ thuộc hoàn toàn vào chất liệu làm VBCC. Chất liệu và công nghệ làm VBCC càng khó giả mạo thì chi phí càng cao.
* Không thể thu hồi VBCC đã ban hành nếu không được sự đồng ý của người được cấp.
* Bên thứ 3 cần xác minh VBCC họ phải đọc và xác minh bằng tay => tốn nguồn lực, thời gian.

#### Văn bằng chứng chỉ số (không sử dụng công nghệ Blockchain)

* **Ưu điểm:**

VBCC số có nhiều ưu điểm hơn VBCC giấy:

* + Cần ít nguồn lực hơn để phát hành, duy trì và sử dụng vì:
* Tính xác thực của các VBCC có thể tự động được kiểm tra mà không cần sự can thiệp thủ công nào.
* Khi bên thứ 3 cần sử dụng các VBCC, VBCC số có thể được tự động đối chiếu, xác minh thậm chí là tóm tắt nếu chúng được phát hành theo một chuẩn định dạng.
* Bảo mật vì nó bắt nguồn từ các giao thức mật mã, đảm bảo rằng chi phí phát hành VBCC rẻ nhưng để sao chép thì rất tốn kém trừ người phát hành.
  + Người phát hành có quyền thu hồi VBCC.
* **Nhược điểm:** 
  + Nếu không sử dụng chữ ký số, VBCC số rất dễ bị giả mạo.
  + Nếu sử dụng chữ ký số, nó yêu cầu phải có bên thứ 3 đảm bảo tính toàn vẹn của giao dịch – các bên thứ ba có quyền kiểm soát đáng kể mọi khía cạnh của quá trình chứng nhận và kiểm tra => dễ bị lợi dụng.
  + Tại nhiều quốc gia, không có một chuẩn mở cho chữ ký số, dẫn tới việc chứng thực chỉ có thể được kiểm tra trong một hệ sinh thái cụ thể nào đó.
  + Dễ dàng phá hủy các bản ghi điện tử, để đảm bảo an toàn dữ liệu cần có hệ thống sao lưu đa tầng và có khả năng chống lỗi.
  + Nếu nơi lưu trữ bị lỗi, VBCC số trở nên vô giá trị vì không thể xác minh được thông tin.
  + Có thể tấn công đơn vị đăng ký và lưu trữ VBCC dẫn tới một cuộc rò rỉ dữ liệu quy mô lớn.

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

Công nghệ Blockchain là một cơ sở hạ tầng mới về bảo mật, chia sẻ và xác minh thành tích trong học tập. Trong việc quản lý và xác minh VBCC, Blockchain có thể lưu trữ một danh sách các nhà phát hành và người nhận, cùng với đó là bảng băm của VBCC trong một database công khai (Blockchain) được lưu trữ trong hàng ngàn máy tính trên toàn cầu. VBCC số được bảo mật trên Blockchain có nhiều điểm lợi thế hơn VBCC số “thông thường” vì một số nguyên nhân như sau:

* + Không thể bị làm giả: có thể xác mình chắc chắn rằng VBCC ban đầu được cấp và được nhận bởi những người được chỉ định trong VBCC.
  + Bất kỳ ai cũng có thể xác minh được VBCC bằng cách sử dụng các phần mềm mã nguồn mở để truy cập vào Blockchain mà không cần bất kỳ một bên thứ ba nào.
  + Do không cần bất kỳ bên thứ ba nào tham gia vào quá trình xác minh VBCC nên VBCC vẫn có thể được xác minh ngay cả khi tổ chức phát hành không còn tồn tại.
  + Thông tin về VBCC chỉ bị mất khi hệ thống Blockchain trên thế giới bị sụp đổ. Nhưng đây là hệ thống phân tán vì vậy để đánh sập toàn bộ hệ thống là việc làm hết sức khó khăn.
  + Hàm băm được sử dụng để tạo liên kết với tài liệu gốc và được lưu trữ trên Blockchain. Như vậy, người dùng vẫn nắm giữ VBCC gốc đảm bảo tính riêng tư của tài liệu.

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

Blockchain đã giải quyết một số vấn đề đứng từ khía cạnh của người nhận:

* + Tính độc lập: Holder sở hữu VBCC và không cần đơn vị phát hành hay một bên thứ ba nào tham gia vào quá trình sau khi nhận được VBCC.
  + Tính sở hữu: Holder có thể chứng minh VBCC được sở hữu bởi họ chứ không phải bất kỳ ai khác.
  + Kiểm soát: Holder có toàn quyền kiểm soát VBCC của họ. Họ có thể chọn liên kết VBCC của mình với bản CV online của họ.
  + Có thể kiểm chứng: VBCC có thể kiểm chứng bởi một bên thứ ba như nhà tuyển dụng, hội đồng tuyển sinh hay các đơn vị xác minh.

#### Đơn vị phát hành (Issuer)

Đứng trên khía cạnh từ phía đơn vị phát hành, Blockchain đã giải quyết một số vấn đề như sau:

* + Đơn vị phát hành có thể chứng minh đâu là VBCC họ phát hành.
  + Đơn vị phát hành có thể đặt một thời hạn cho VBCC.
  + VBCC có thể được thu hồi bởi đơn vị phát hành.
  + Đảm bảo an toàn cho hệ thống quản lý và xác minh VBCC.

#### Đơn vị cần xác minh (Verifier)

Về phía đơn vị cần xác minh, Blockchain đã giải quyết một số vấn đề như sau:

* + Verifier có thể xác minh VBCC một cách nhanh chóng.
  + Nếu hệ thống có tích hợp hệ thống thông tin của ứng viên, Verifier có thể theo dõi trực tiếp profile của ứng viên.

## Tình hình và các nghiên cứu liên quan

Một số dự án triển khai quản lý và xác minh VBCC sử dụng công nghệ Blockchain

### Blockcerts

#### Giới thiệu

Blockcerts là một dự án mã nguồn mở được phát triển bởi một nhóm các nhà nghiên cứu thuộc MIT Media Lab – Hoa Kỳ. Dự án được bắt đầu phát triển năm 2016 thời điểm bùng nổ của các loại tiền mã hóa. Đây là một dự án sớm nhất nghiên cứu đầy đủ về việc quản lý VBCC trên Blockchain. Mục tiêu của dự án là xây dựng một chuẩn mở cho việc tạo, phát hành, xem và xác minh thông tin VBCC số trong lĩnh vực đào tạo. Sau gần 3 năm phát triển, dự án đã có 2 phiên bản: Blockcerts version 1.0 và Blockcerts version 2.0. Phiên bản 2.0 có một số thay đổi so với phiên bản 1.0 đó là:

* + Cấp phát VBCC theo lô thay vì cấp VBCC cho từng cá nhân như trước đây. Việc này giúp làm giảm số lượng giao dịch bitcoin cần phải thực hiện để tiết kiệm chi phí.
  + VBCC được thu hồi theo chuẩn Open Badges v2.0, tức là dựa vào một đường dẫn “HTTP URI revocation list” thay vì sử dụng phương pháp gửi một giao dịch bitcoin vào địa chỉ của người nhận.

Blockcert đã đi sâu vào xử lý các vấn đề trong việc quản lý VBCC trong đào tạo, cụ thể như sau:

* + Dự án thiết kế gồm 3 nhóm đối tượng: Đơn vị phát hành, Người nhận VBCC và người xác minh VBCC.
  + Người nhận VBCC sẽ cung cấp thông tin địa chỉ trên Blockchain của mình cho đơn vị phát hành thực hiện tạo, ký và phát hành VBCC lên Blockchain. Sau đó, người xác minh VBCC sẽ kiểm tra thông tin từ chính VBCC của người nhận dựa trên Blockchain.

Mặc dù, dự án đã phát triển được 3 năm nhưng dự án vẫn còn những hạn chế. Chi tiết sẽ được nêu ở mục 2.2.1.3, sau đây sẽ là các điểm mạnh của dự án

#### Điểm mạnh của dự án

Một số điểm mạnh của dự án so với việc quản lý VBCC không sử dụng công nghệ Blockchain:

* + VBCC không bị làm giả vì sử dụng thuật toán băm (băm trong VBCC, tạo cây merkle để phát hành lên Blockchain), khi có bất kỳ thay đổi nào về thông tin trong VBCC sẽ làm sai lệch giá trị băm và sẽ phát hiện ra VBCC giả.
  + Hỗ trợ công cụ xác minh VBCC có hợp lệ hay không (cert-verifier, wallet-android, wallet-ios, cert-verifier-js) hoặc người dùng có thể tự phát triển một ứng dụng riêng để kiểm tra tính hợp lệ của VBCC.
  + Trong trường hợp đơn vị phát hành không còn tồn tại, những VBCC của đơn vị này phát hành ra vẫn có thể được xác minh.
  + Người nhận không cần phụ thuộc vào một bên thứ ba sau khi VBCC được cấp mà có thể toàn quyền xem, chia sẻ và kiểm soát VBCC của mình.
  + Đơn vị phát hành có thể chứng minh được VBCC của họ phát hành, thu hồi VBCC đã cấp, đặt thời gian hết hạn cho VBCC và quan trọng nhất là đảm bảo an toàn cho những VBCC cấp ra mà không cần phụ thuộc nhiều vào hạ tầng sao lưu của mình.
  + Sẵn sàng trên 2 nền tảng Blockchain phổ biến nhất hiện nay là Bitcoin và Ethereum.

#### Một số hạn chế

Tuy vậy, như đã đề cập ở 2.2.1.1, mặc dù đã phát triển được gần 3 năm nhưng dự án vẫn còn tồn tại một số hạn chế như sau:

* + Quy trình để phát hành VBCC đang phụ thuộc vào duy nhất một người giữ khóa bí mật của đơn vị đào tạo. Điều này có thể dẫn tới các vấn đề liên quan tới tham nhũng.
  + Việc quản lý danh sách các VBCC thu hồi dựa vào “HTTP URI revocation list” tạo ra một nút thắt cổ chai. Kẻ tấn công có thể tấn công vào server chứa danh sách này để cập nhật, thêm mới, xóa thông tin các VBCC trong danh sách.
  + Việc định danh các đơn vị phát hành hiện tại cũng dựa vào một đường dẫn qua giao thức HTTP. Cũng tương tự như việc quản lý VBCC thu hồi, đây là một nút thắt cổ chai mà kẻ tấn công có thể lợi dụng.

Từ một số điểm bất cập nêu trên, các nhà nghiên cứu của đại học Birmingham của Vương quốc Anh đã phát triển dự án BTCert dựa trên nền tảng của Blockcerts để xử lý vấn đề. Chi tiết trong mục 2.2.2.

### BTCert

#### Giới thiệu

BTCert là dự án được phát triển bởi nhóm các nhà nghiên cứu thuộc Đại học Birmingham. Chi tiết dự án được mô tả trong đường dẫn:

<https://github.com/BlockTechCert/BTCert>

Dự án bắt đầu từ cuối năm 2017 và được viết bằng Java thay vì Python như Blockcerts.

#### Điểm mạnh của dự án

Do phát triển trên nền tảng và thừa kế mô hình của Blockcerts, vì thế BTCert mang đầy đủ những điểm mạnh của Blockcerts. Ngoài ra, BTCert còn xử lý các vấn đề còn tồn tại của Blockcerts như:

* + Xây dựng quy trình cấp VBCC qua nhiều cấp bằng cách sử dụng multisign trên Bitcoin. Giả sử, ta có N người ký và M là số lượng tối thiểu người cần ký giao dịch thì VBCC mới được phát hành.
  + Thu hồi VBCC dựa vào trạng thái giao dịch trên Blockchain. Cụ thể như sau: hệ thống sẽ sinh ra một danh sách các địa chỉ của nhà cung cấp sử dụng để thu hồi, gắn địa chỉ này vào VBCC phát hành cho người nhận. Khi muốn thu hồi, đơn vị phát hành chỉ cần sử dụng địa chỉ thu hồi thực hiện một giao dịch gửi bitcoin tới địa chỉ của người nhận. Việc còn lại là ứng dụng xác minh sẽ kiểm tra nếu có giao dịch từ địa chỉ thu hồi của đơn vị phát hành tức là VBCC đã bị thu hồi.

#### Một số hạn chế

Mặc dù kế thừa và xử lý được một số vấn đề của Blockcerts nhưng BTCert vẫn còn một số hạn chế nhất định như sau:

* + Chỉ hỗ trợ trên nền tảng Blockchain Bitcoin.
  + Việc xử lý định danh nhà phát hành vẫn dựa vào một liên kết HTTP trên Internet và vẫn có nguy cơ bị tấn công.

# 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 tại, hầu hết quy trình quản lý chứng chỉ của các tổ chức đào tạo tại Việt Nam sẽ như sau:

* Bước 1: Quyết định và danh sách học sinh, sinh viên tốt nghiệp
* Bước 2: Lập hồ sơ trình Bộ Giáo dục và Đào tạo duyệt cấp phôi bằng
* Bước 3: Tiếp nhận và Quản lý phôi bằng
* Bước 4: In ấn văn bằng chứng chỉ
* Bước 5: Trình ký duyệt văn bằng chứng chỉ
* Bước 6: Cấp phát và xử lý các bằng hỏng
* Bước 7: Công khai dữ liệu cấp phát văn bằng trên website
* Bước 8: Quản lý văn bằng

Sau khi chứng chỉ được cấp cho người nhận, người nhận phải mang chứng chỉ gốc đến các cơ quan có thẩm quyền công chứng nếu muốn chia sẻ thông tin về văn bằng với bên thứ ba.

Bên thứ ba khi muốn xác minh tính đúng đắn của chứng chỉ phải liên hệ với đơn vị phát hành để kiểm tra rất mất thời gian và tiền bạc để thực hiện.

Một giải pháp về quản lý chứng chỉ đào tạo sử dụng công nghệ Blockchain phải đảm bảo được các điều kiện như sau:

* Đảm bảo chứng chỉ khi được cấp phát ra phải đảm bảo an toàn về mặt thông tin.
* Cắt giảm nguồn lực và chi phí thực hiện, quản lý, xác minh.
* Việc xác minh tính đúng đắn của chứng chỉ có thể thực hiện độc lập và không phụ thuộc vào đơn vị phát hành.

### Mô hình thực hiện

Dựa trên các module của dự án, thực hiện mô hình thực hiện như sau:



Hình 4. Mô hình thực hiện của hệ thống

Quy trình thực hiện như sau:

1) Các đơn vị đào tạo - Issuer sẽ có một hệ thống quản lý thông tin học sinh sinh, viên hay Holder, từ hệ thống CertsChain này Holder đủ điều kiện được cấp VBCC sẽ yêu cầu đơn vị đào tạo cấp VBCC cho 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 sẽ VBCC.

3) Holder muốn chia sẽ CBCC có thể truy cập vào hệ thống CertsChain để lấy file PDF, mã số VBCC và gửi cho một bên thứ ba (nhà tuyển dụng - Verifier) xác 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. |
| 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. |
| 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 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 chọn các chức năng thêm, xóa, sửa thì thông tin về người dùng sẽ được cập nhật vào database.
* *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 chọn các chức năng thêm, xóa, sửa thì 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.

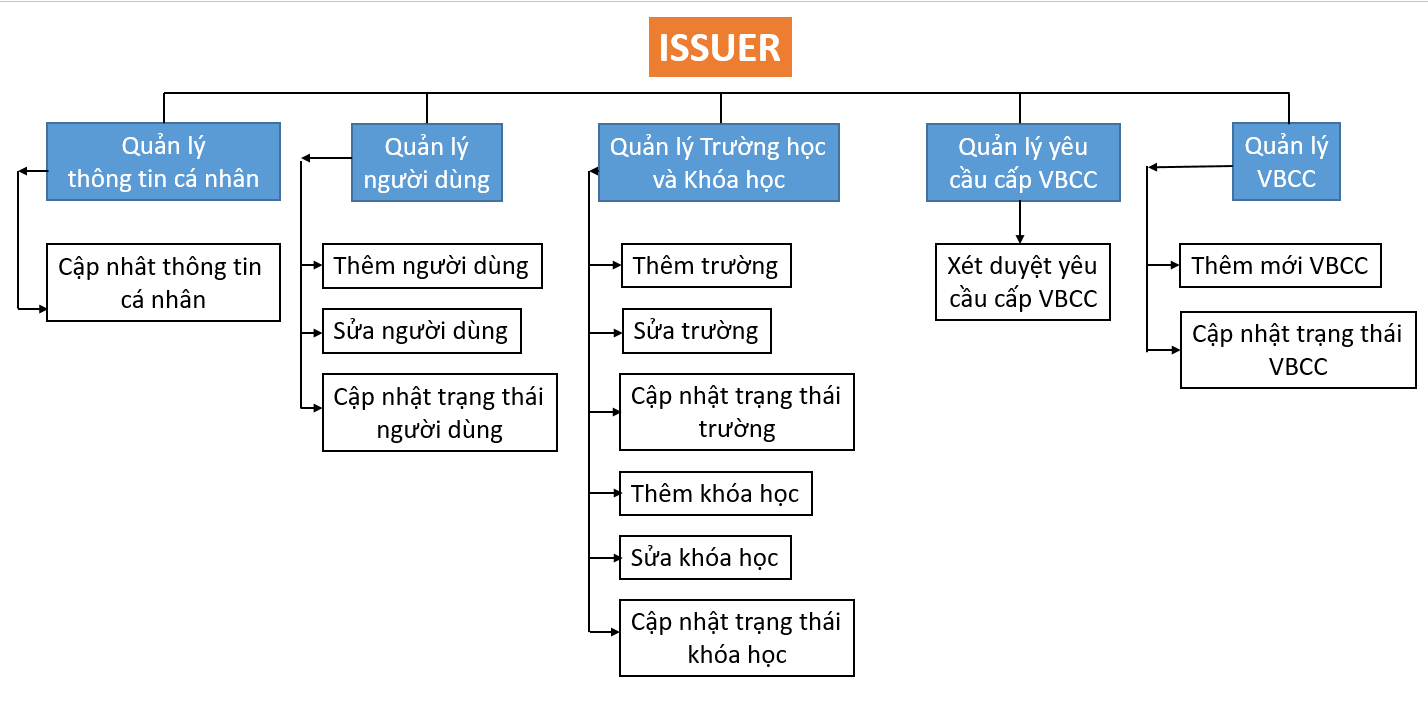
Bao gồm chức năng xét duyệt yêu cầu cấp phát VBCC.

* *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**

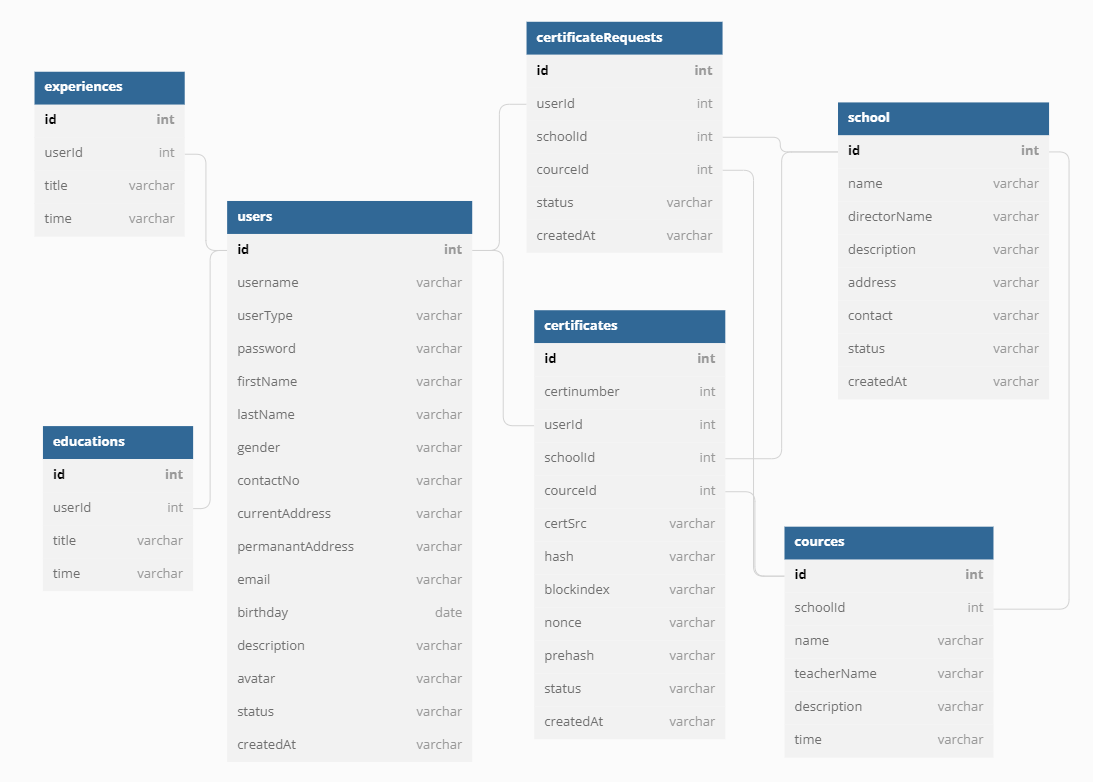
Hệ thống cung cấp tính năng Xác minh VBCC có hợp lệ trên hệ thống hay không.

* *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 máy local có cấu hình như sau:

* + Properties: Intel Core i5, 16GB RAM, Window 10 64bit.
  + 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: Giá trị biến thiên để tìm ra giá trị băm thỏa mãn yêu cầu của block

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

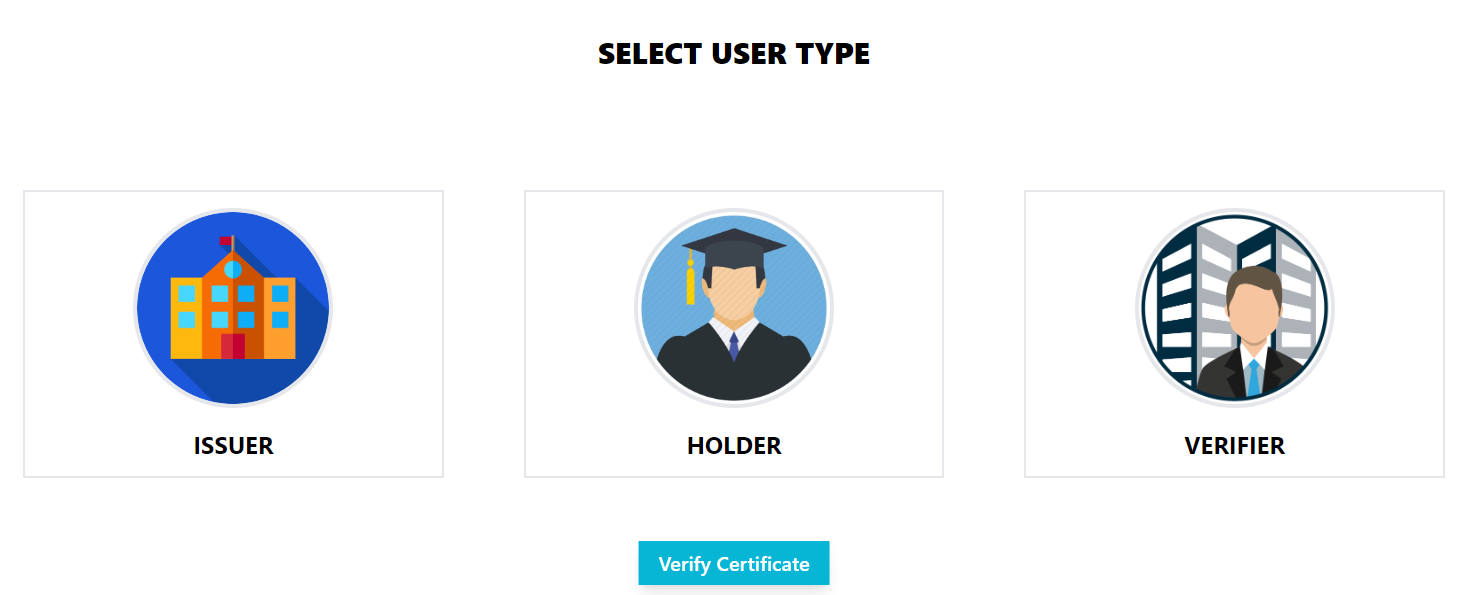
|  |  |  |
| --- | --- | --- |
| **Module** | **Api Method và URL** | **Mô tả - Chức năng** |
| *Authentication* | /user/login | Người dùng loại Issuer hay Holder muốn dùng các chức năng của mình đăng nhập vào hệ thống, sử dụng API này. |
| *Users* | /user/list | Lấy ra danh sách các user của hệ thống |
| /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 |
| *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 văn bằng chứng chỉ mới |

## Thực nghiệm hệ thống CertsChain

* 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*.

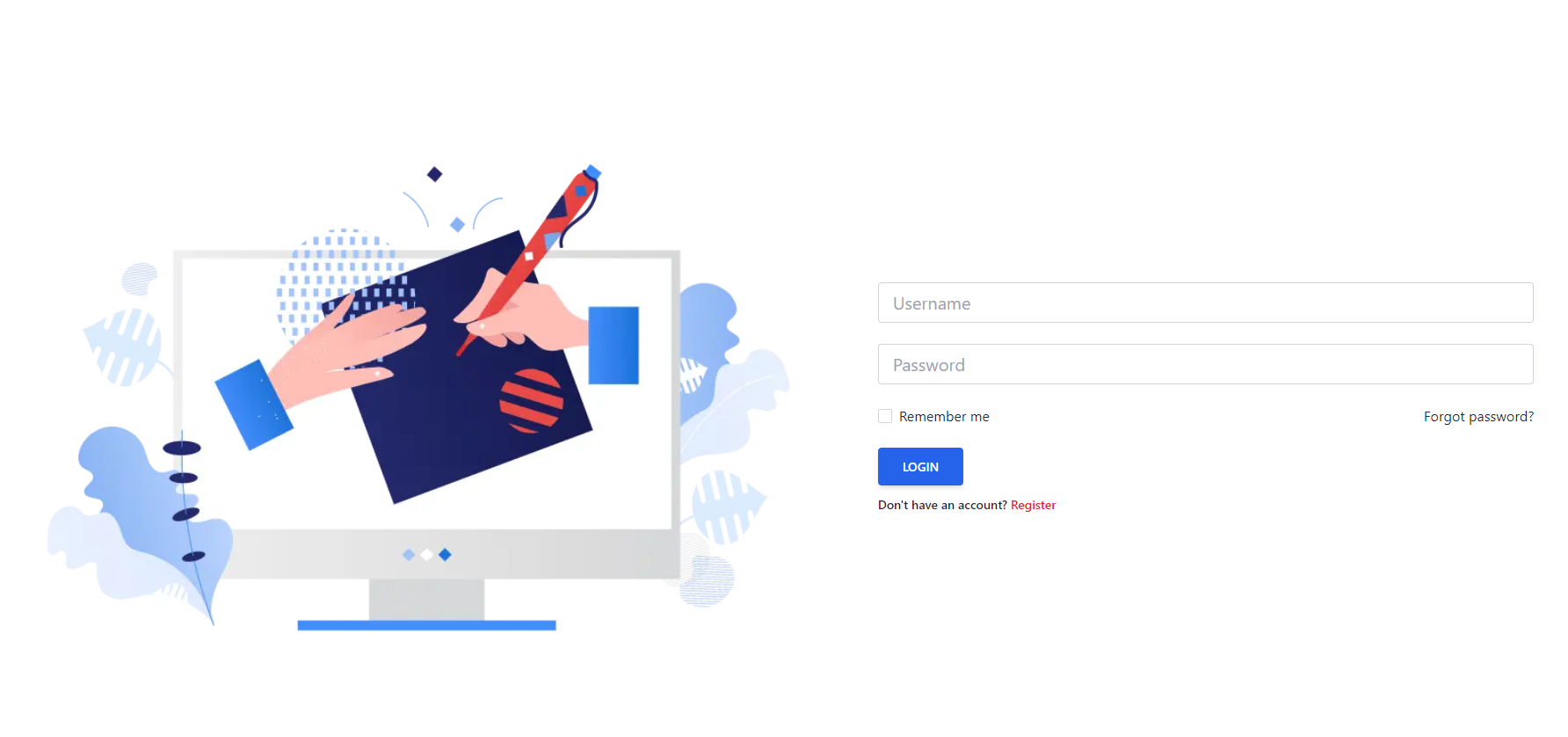
Hay User muốn xác minh VBCC có thể click vào button *Verify Certificate*.



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.

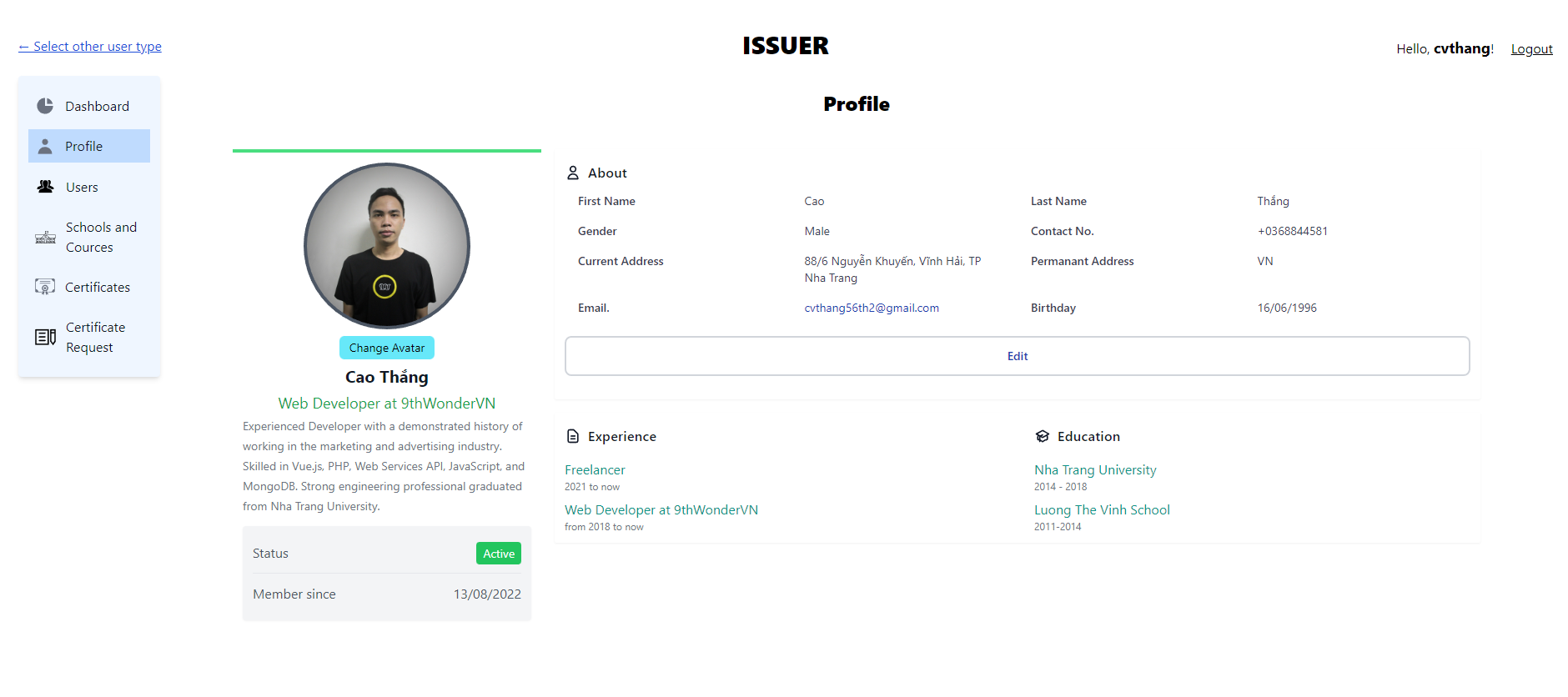


Hình 12. Trang đăng nhập

### Người dùng loại Issuer

#### Trang Profile

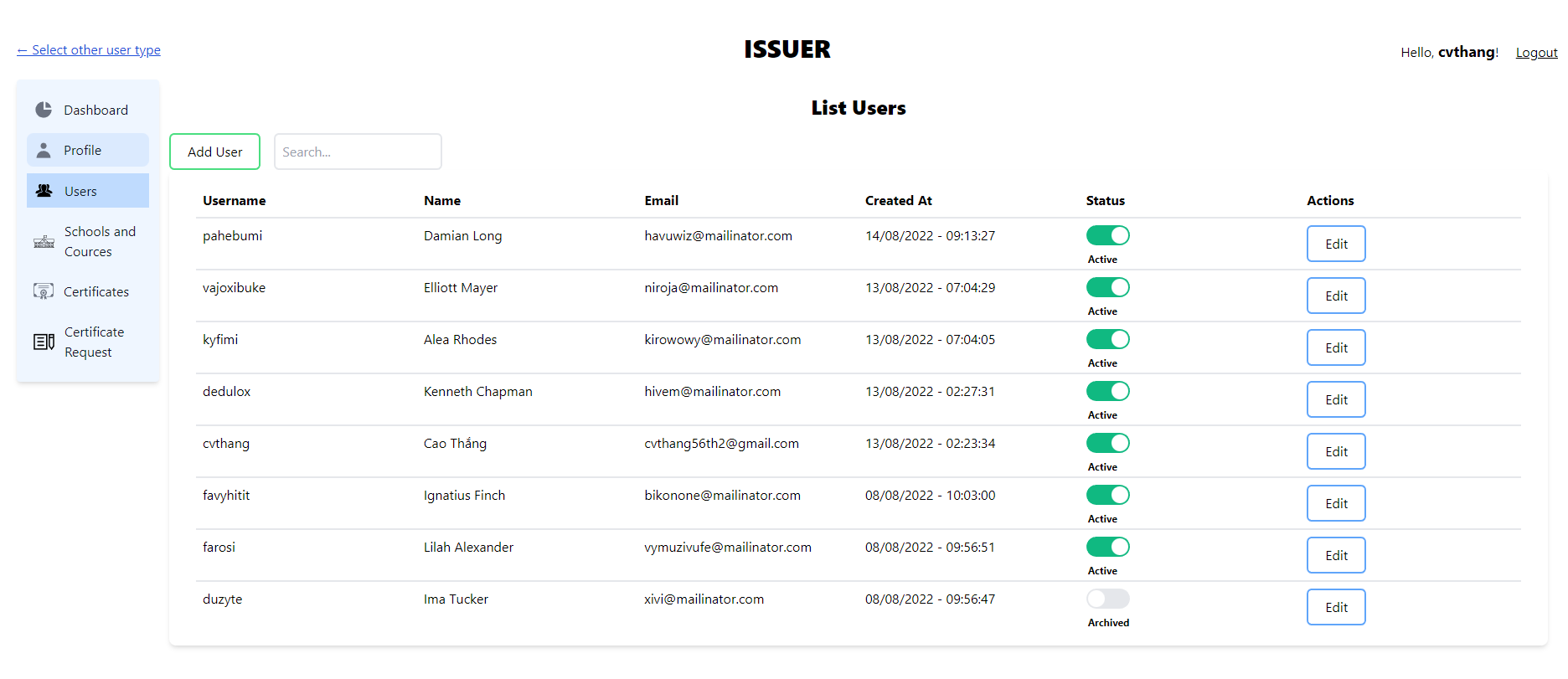
Đây là trang thông tin cá nhân của Issuer, có thể thực hiện chỉnh sửa các thông tin cá nhân của mình tại trang này bằng cách click vào button *Edit*.



Hình 13. Trang Profile của Issuer

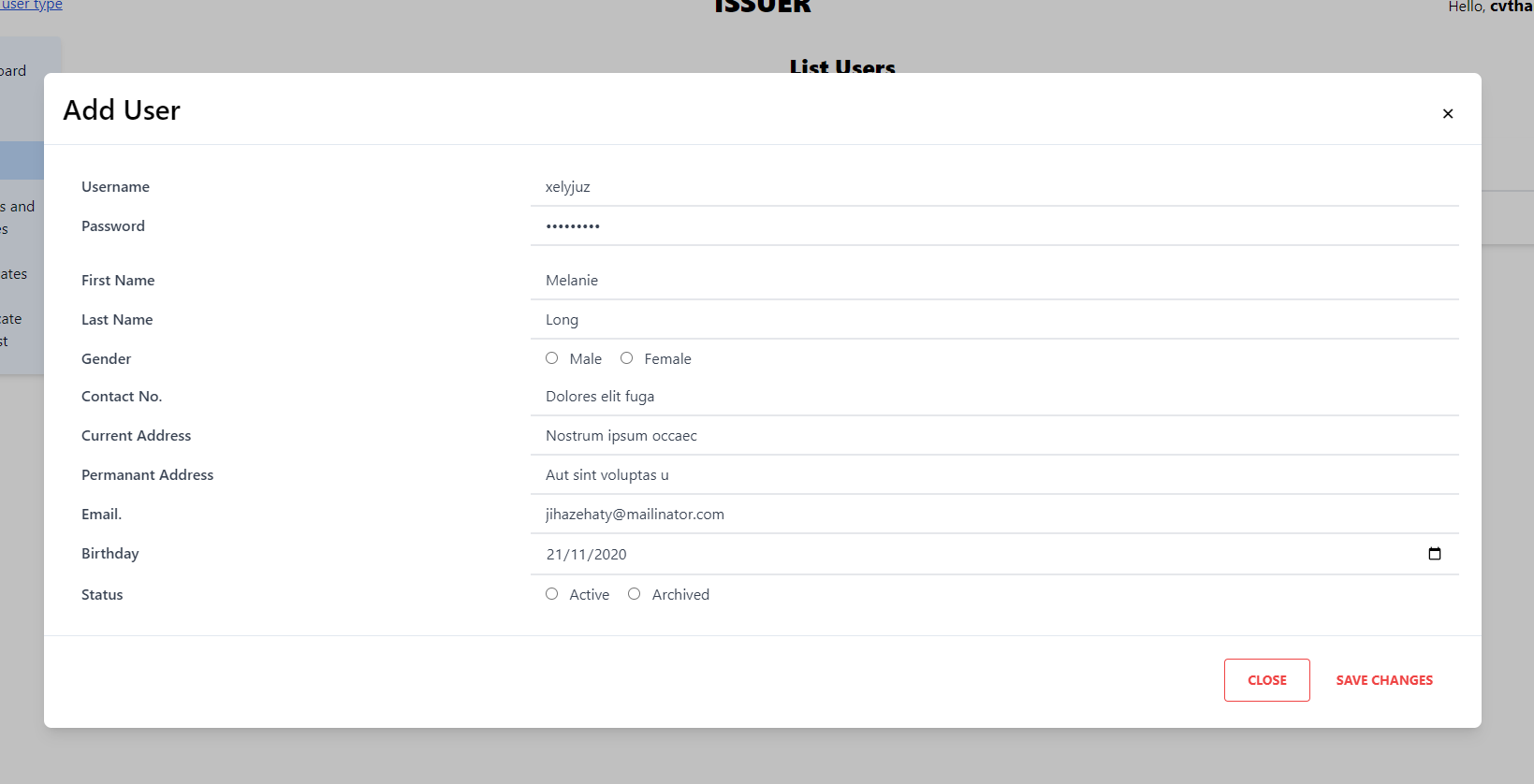
#### Trang Users

Giúp Issuer có thể quản lý User trong hệ thống:



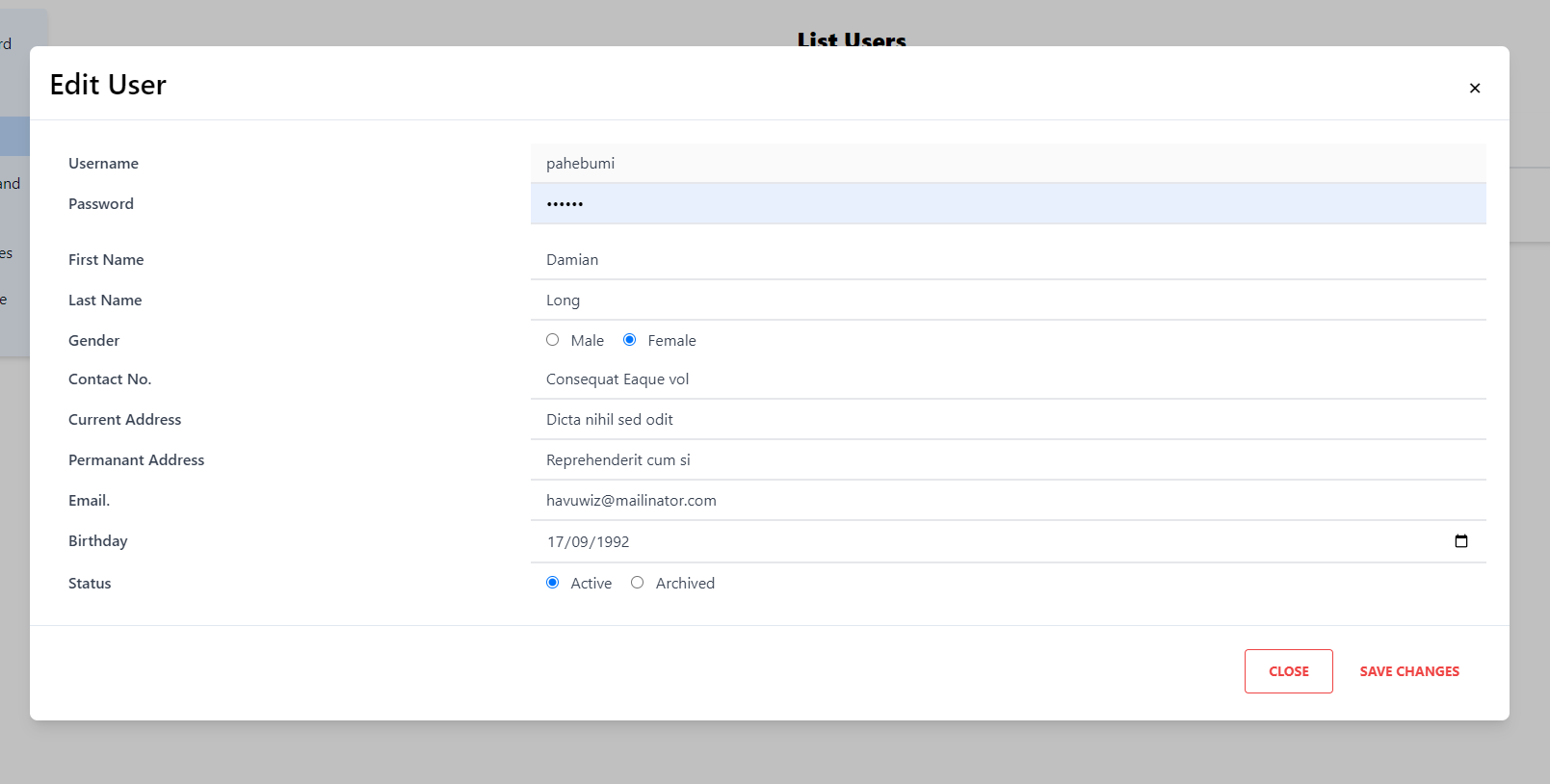
Hình 14. Trang Users của Issuer

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*:

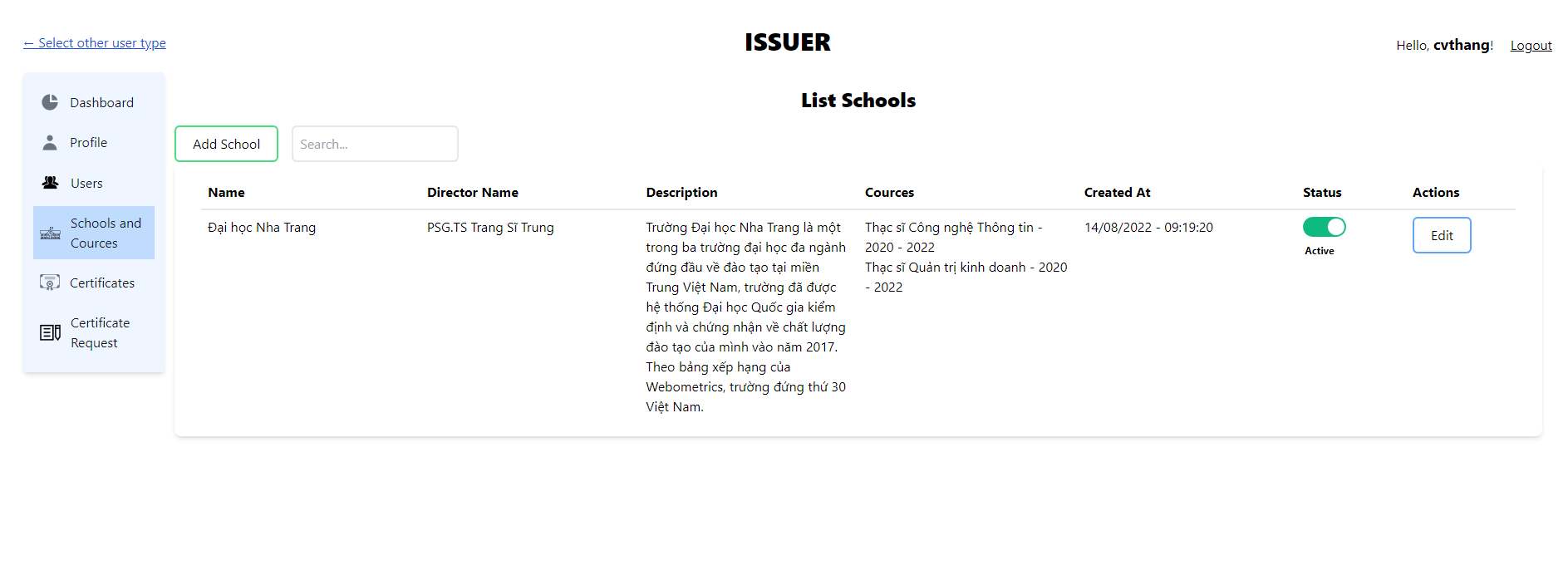


Hình 16. Popup cập nhật User

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

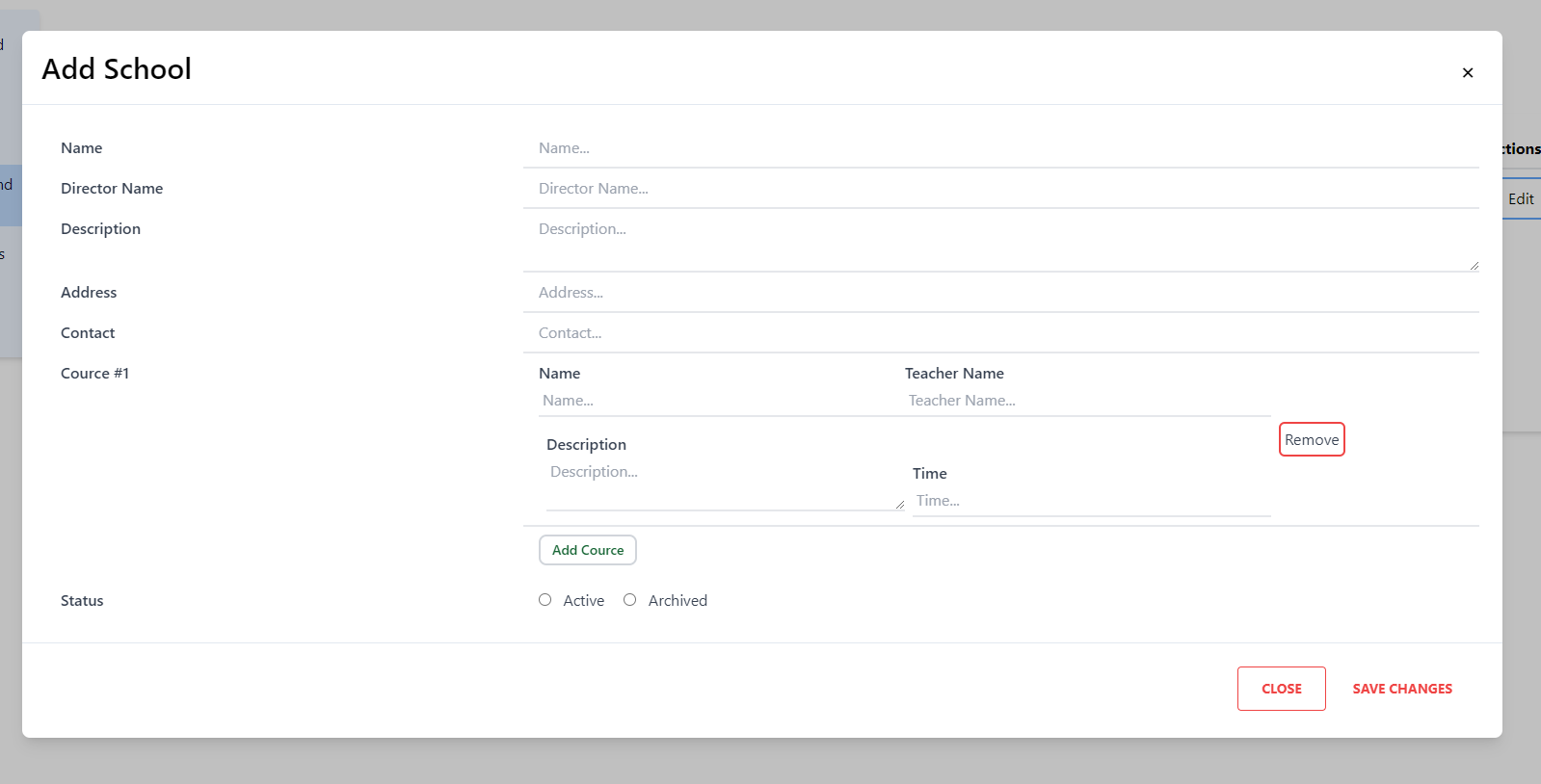
#### Trang Schools and Cources

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



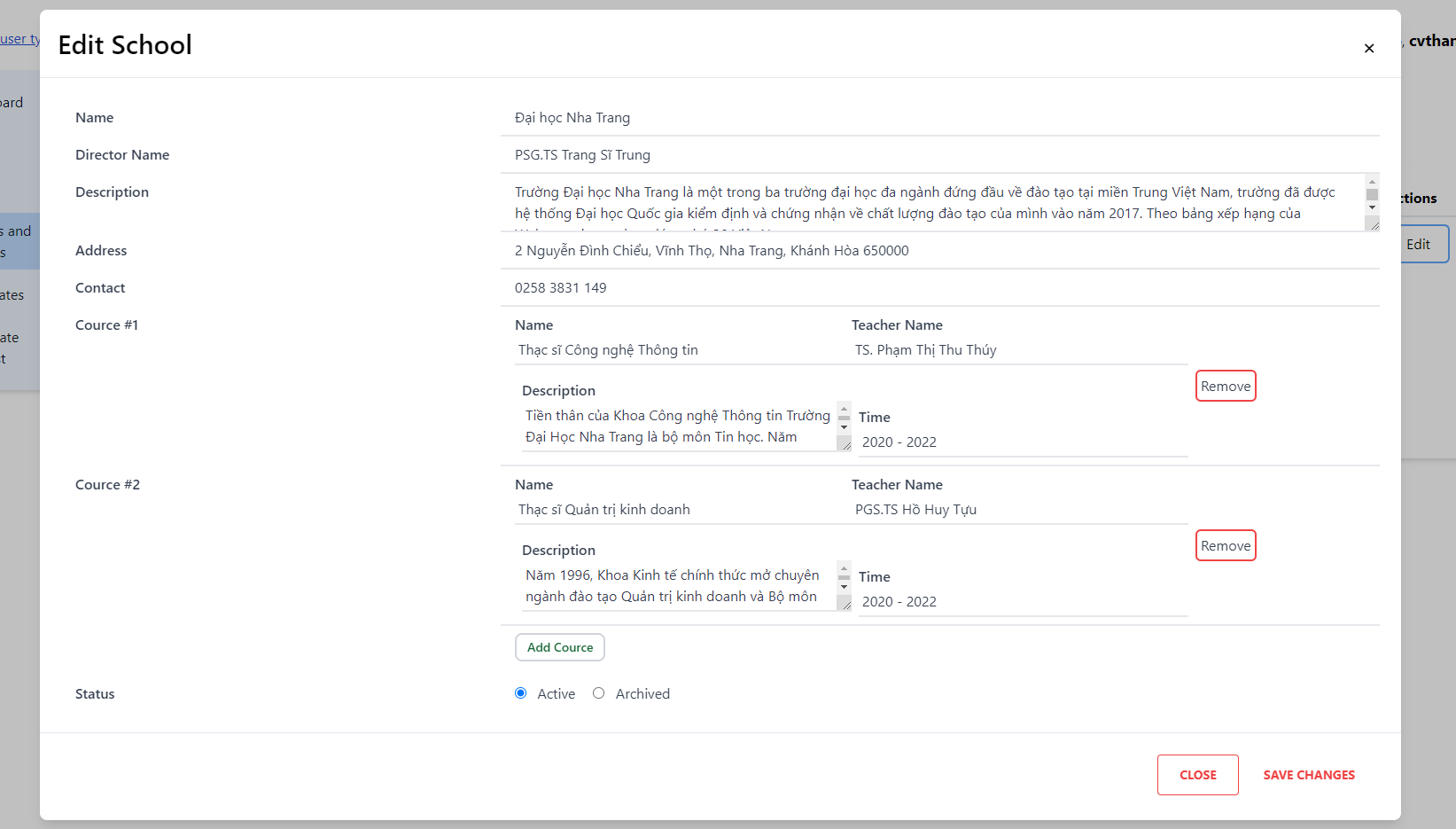
Hình 17. Trang Schools and Cources của Issuer

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



Hình 18. Popup tạo mới School and Cource

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

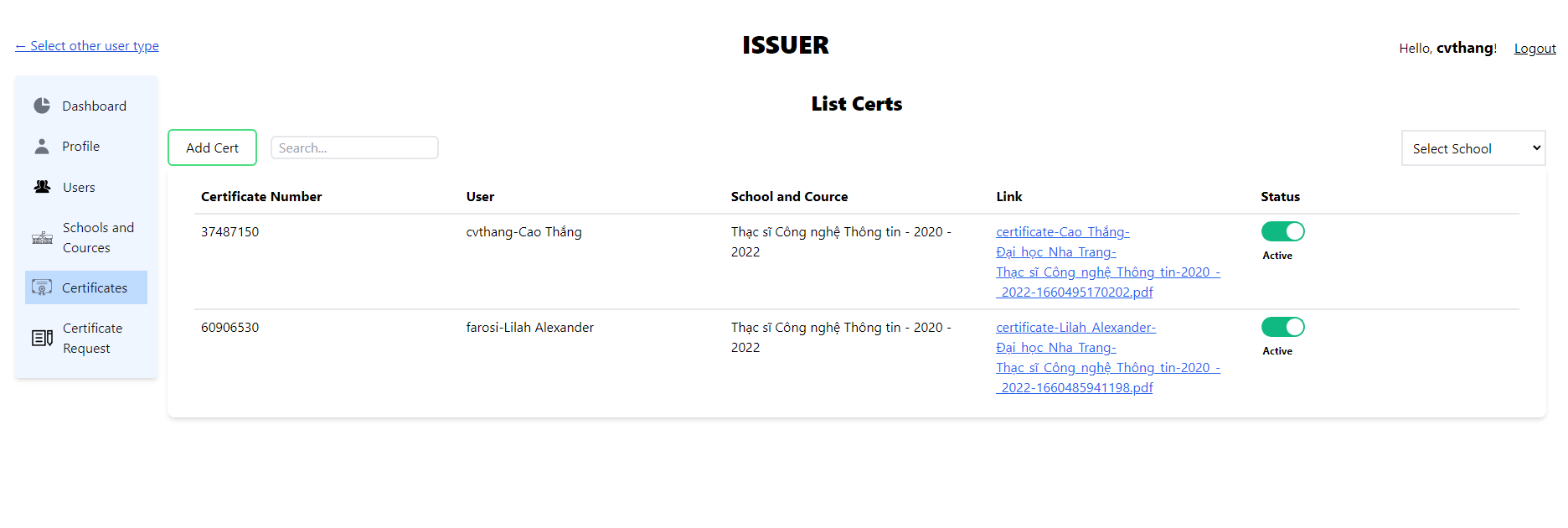


Hình 19. Popup cập nhật School and Cource

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

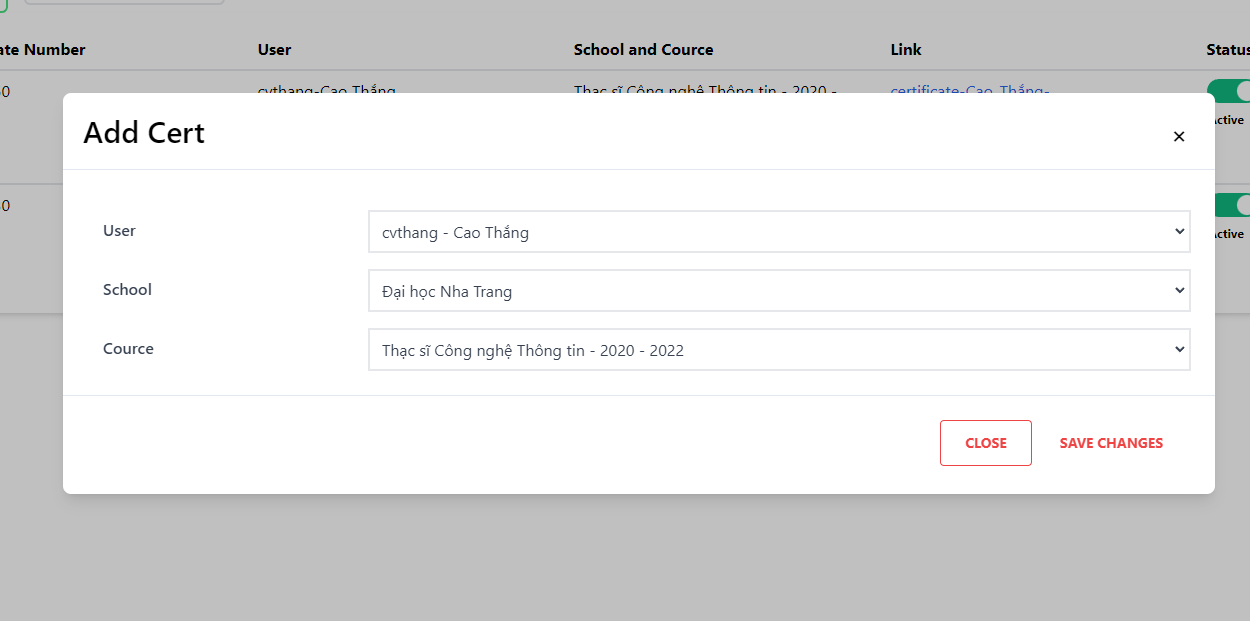
#### Trang Certiciates

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



Hình 20. Trang Certificates của Issuer

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



Hình 21. Popup tạo mới Certificate

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

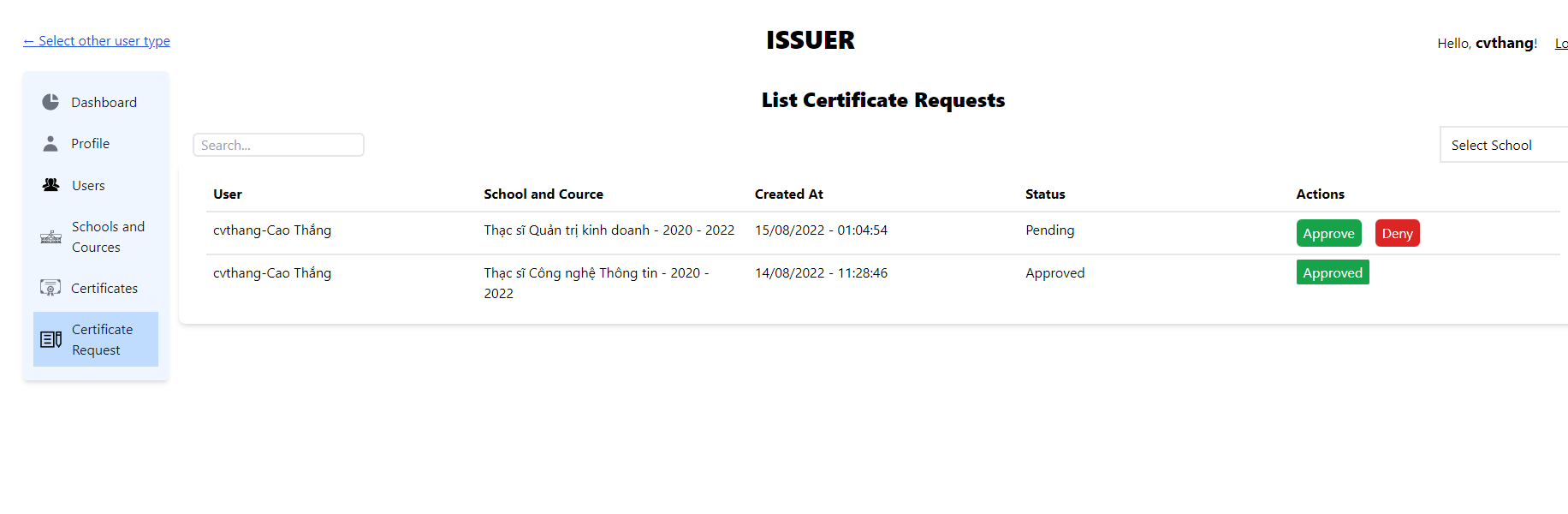


Hình 22. Mẫu văn bằng chứng chỉ của CertsChain

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 23. Trang Certificate Requests của Issuer

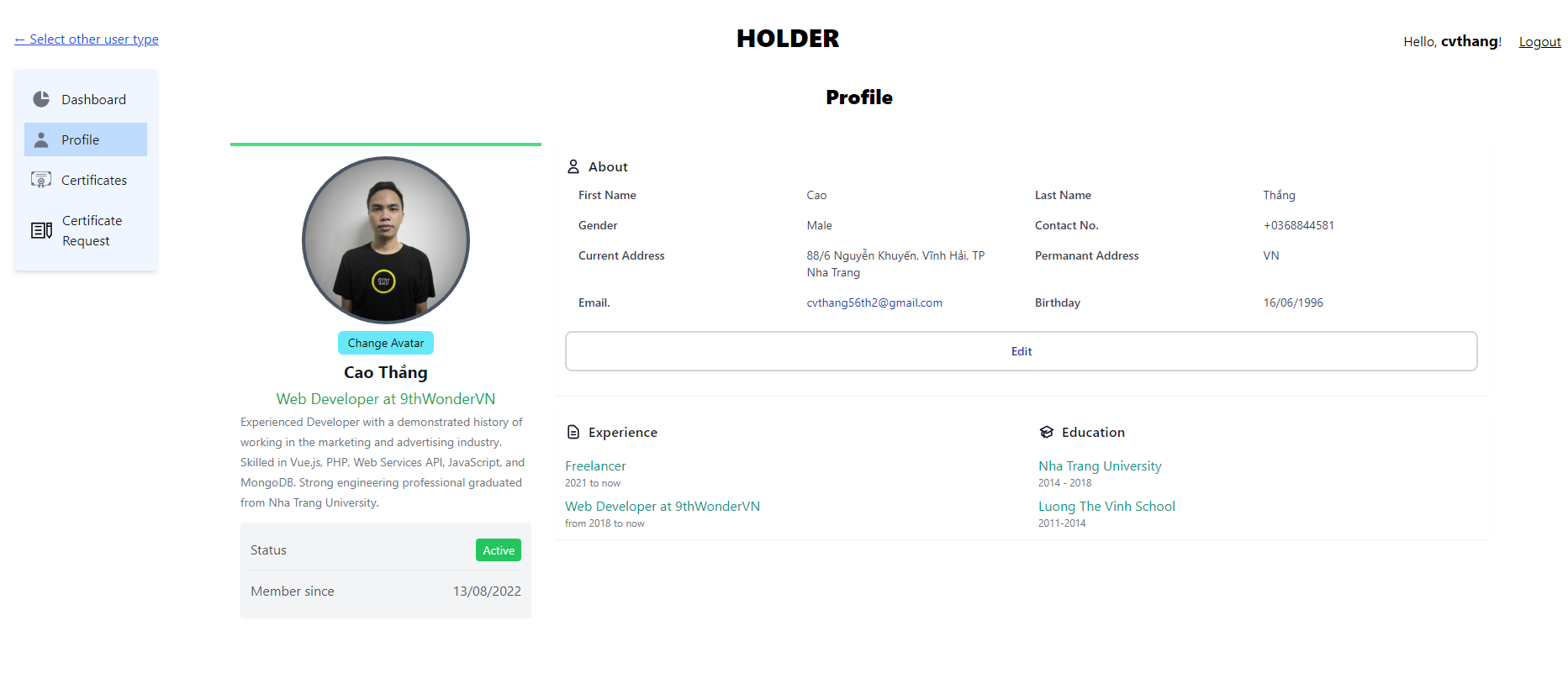
Sau khi xét duyệt yêu cầu cấp phát VBCC, Issuer sẽ click vào button *Approve* nếu chấp thuận, *Deny* nếu từ chối yêu cầu cấp phát.

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

### Người dùng loại holder

#### Trang Profile

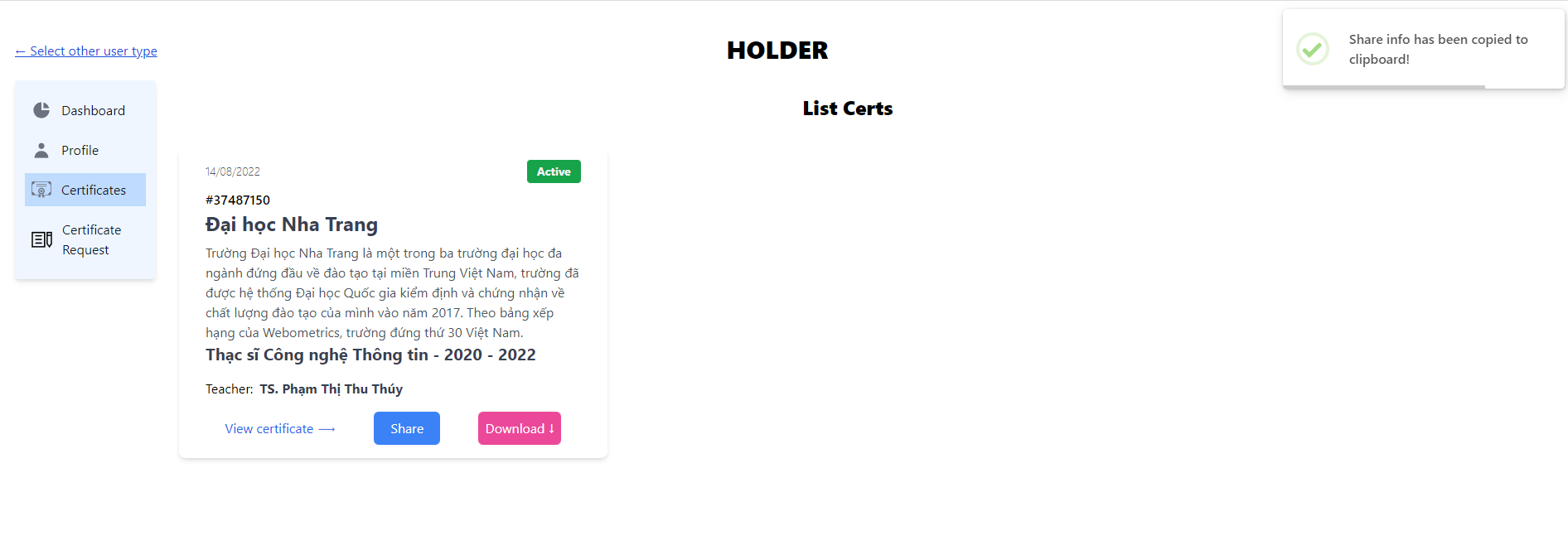
Đây là trang thông tin cá nhân của Holder, có thể thực hiện chỉnh sửa các thông tin cá nhân của mình tại trang này bằng cách click vào button *Edit*.



Hình 24. Trang Profile của Holder

#### Trang Certificates

Hiển thị danh sách các VBCC của Holder:

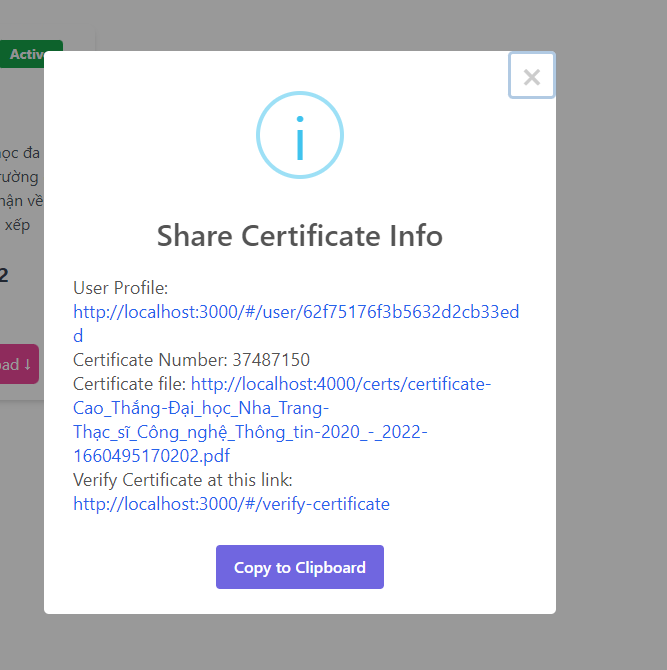


Hình 25. Trang danh sách Certificate của Holder

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 kì 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:

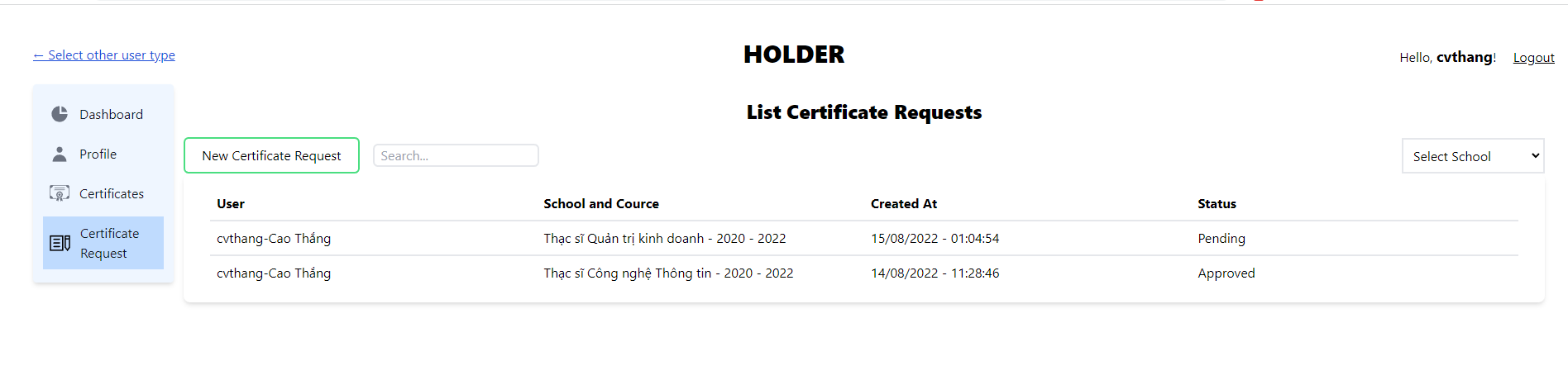


Hình 26. Popup chia sẻ thông tin Certificate

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

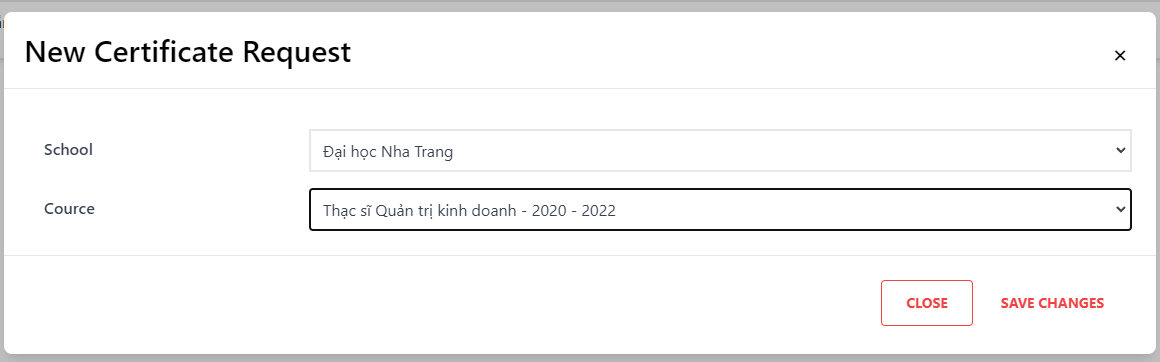
#### Trang Certificate Requests

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



Hình 27. 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.

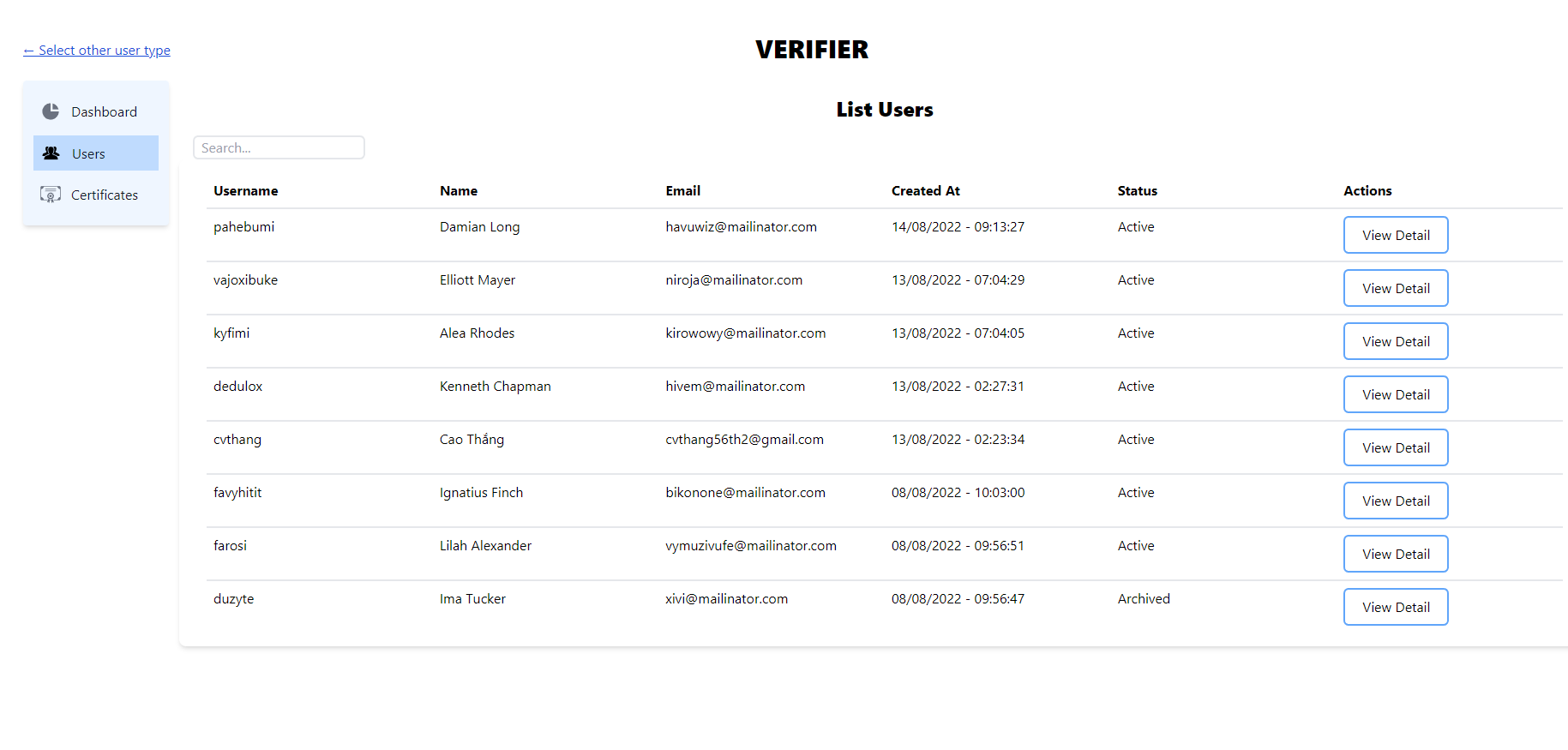


Hình 28. Popup tạo mới yêu cầu cấp phát VBCC

### Người dùng loại verifier

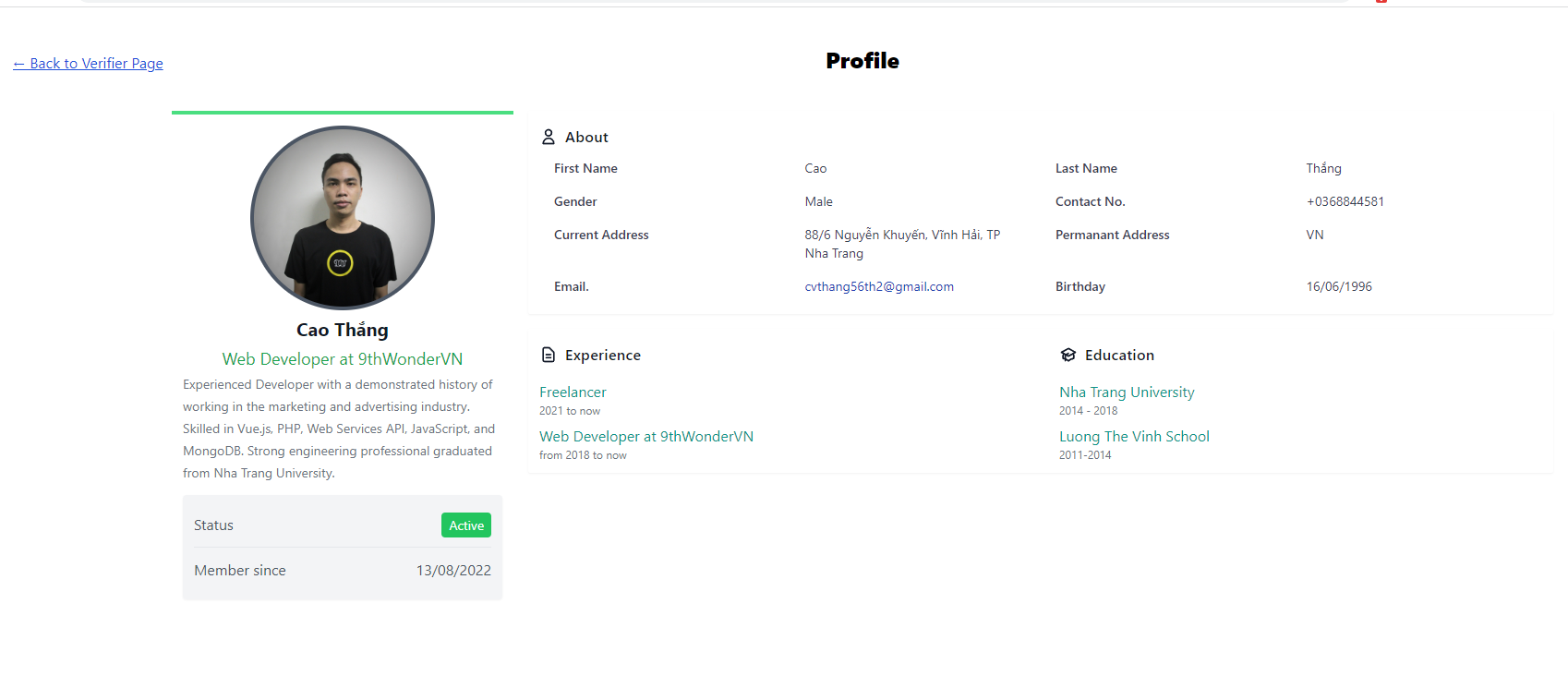
#### Trang Users

Hiển thị ra tất cả các Users có trong hệ thống



Hình 29. Danh sách tất cả các User trong hệ thống

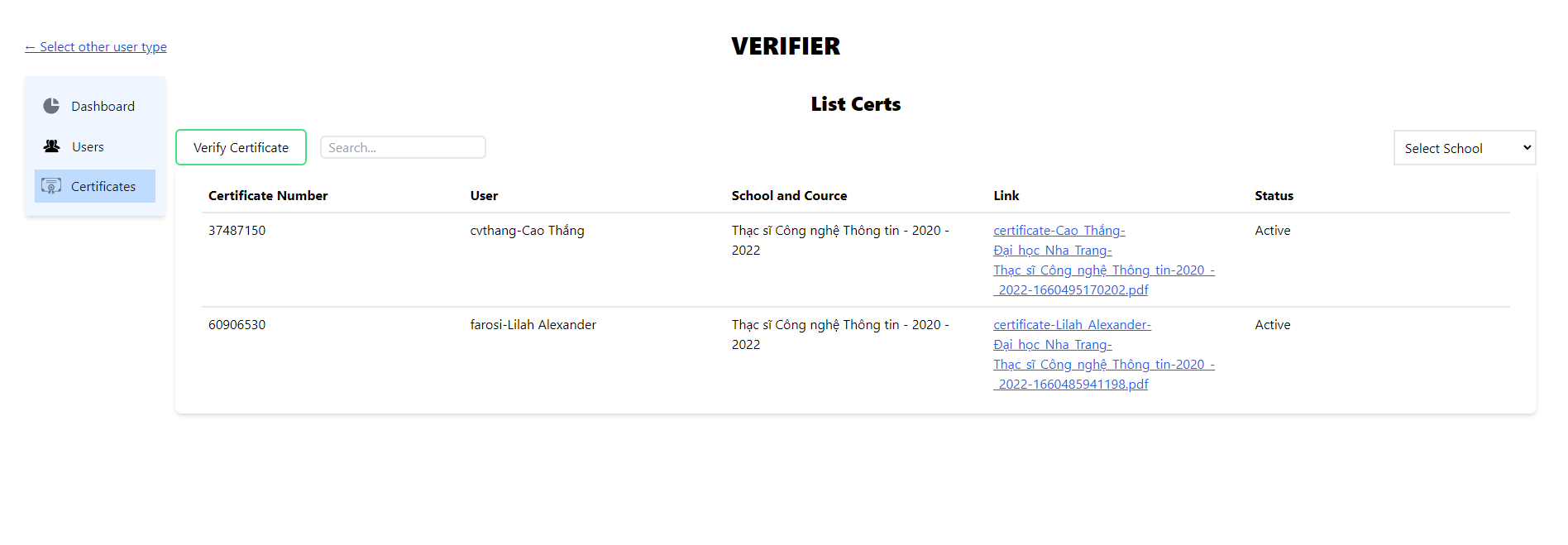
Bất kì ai cũng có thể xem chi tiết thông tin công khai của user trong hệ thống. Bằng cách click vào button *View Detail*.



Hình 30. Trang chi tiết User

#### Trang Certiciates

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

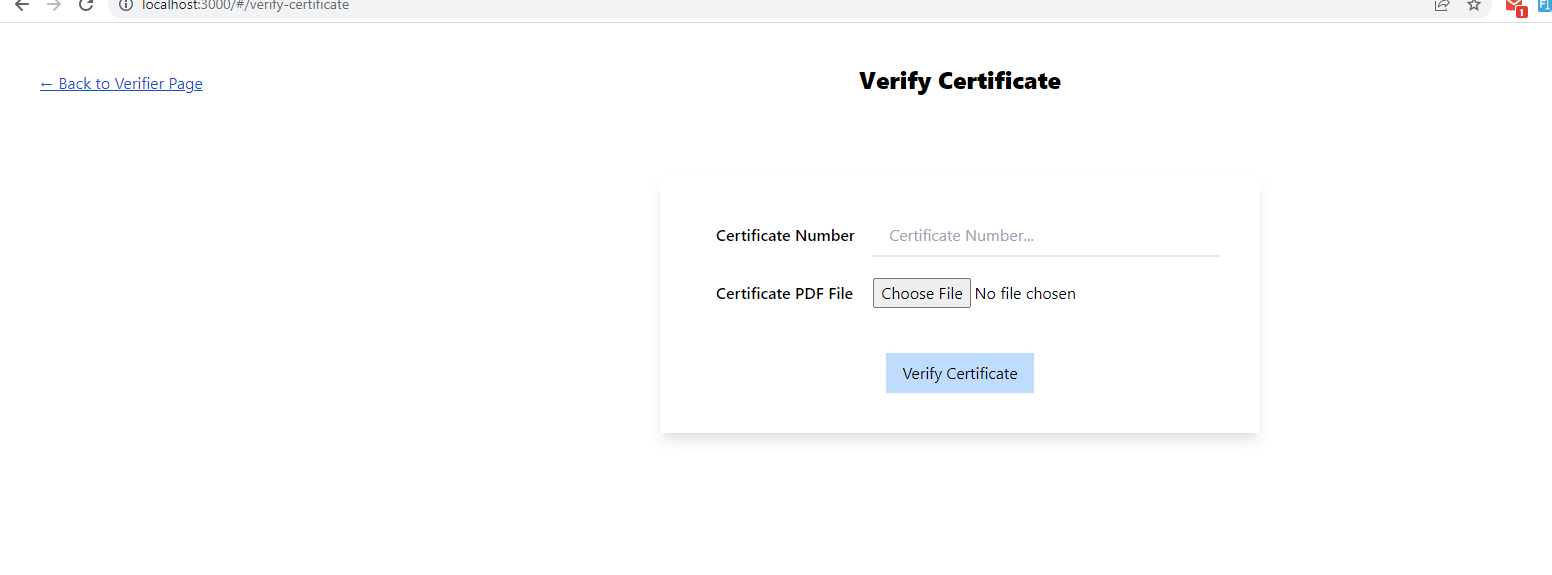


Hình 31. Danh sách tất cả các certificate trong hệ thống

### 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 lựu hay không.



Hình 32. 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.
  + Mã nguồn đã được công khai trên git: <https://github.com/cvthang56th2/CertsChain>

## Hạn chế của đề tài

* + Chưa triển khai lên server trên internet.

## 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 thống quản lý văn bằng chứng chỉ sử dụng 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>