

NGHIÊN CỨU VÀ ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN TRONG QUẢN LÝ VÀ XÁC MINH VĂN BẰNG CHỨNG CHỈ

Học viên: Cao Viết Thắng
Giảng viên hướng dẫn: TS. Nguyễn Đình Hưng
Trường: Đại học Nha Trang
Thời gian: 06/2023

I. Tóm tắt

Bài báo này tập trung vào nghiên cứu và ứng dụng công nghệ blockchain trong quản lý và xác minh văn bằng chứng chỉ. Nghiên cứu về một số mô hình quản lý không áp dụng công nghệ blockchain, chỉ ra các ưu, nhược điểm của từng mô hình, và từ đó khám phá khả năng của công nghệ blockchain trong việc ngăn chặn gian lận, cung cấp tính minh bạch và tăng cường hiệu quả trong quản lý văn bằng chứng chỉ.

Công nghệ blockchain được sử dụng để ghi lại thông tin văn bằng chứng chỉ một cách không thể thay đổi và công khai trên mạng. Điều này giúp ngăn chặn gian lận và việc chỉnh sửa thông tin về văn bằng. Bên cạnh đó, công nghệ này cũng cung cấp khả năng xác minh thông tin văn bằng chứng chỉ một cách dễ dàng và linh hoạt, giúp nhà tuyển dụng, trường đại học và sinh viên dễ dàng truy cập và xác minh thông tin.

Bài báo cũng trình bày về các lợi ích khác của công nghệ blockchain trong quản lý và xác minh văn bằng chứng chỉ, bao gồm bảo mật thông tin, chia sẻ thông tin linh hoạt, giúp các bên liên quan như nhà tuyển dụng, trường đại học và sinh viên có thể truy cập vào thông tin văn bằng chứng chỉ trên blockchain và xác minh tính hợp lệ của nó mà không cần sự tham gia của bên trung gian. Tuy nhiên, việc triển khai công nghệ blockchain trong lĩnh vực này còn đối mặt với một số thách thức, như kết nối thông tin từ các nguồn bên ngoài blockchain và đầu tư về hạ tầng và bảo mật.

Nhìn chung, việc áp dụng công nghệ blockchain trong quản lý và xác minh văn bằng chứng chỉ đã có được một số triển vọng và lợi ích đáng kể. Việc tiếp tục nghiên cứu và phát triển trong lĩnh vực này có thể mang lại sự cải thiện tốt hơn về tính hiệu quả và minh bạch trong quản lý văn bằng chứng chỉ.

II. Giới thiệu

Trong thời đại kỹ thuật số ngày nay, quản lý và xác minh tính hợp lệ của văn bằng chứng chỉ đóng vai trò quan trọng trong nhiều lĩnh vực, bao gồm giáo dục, tuyển dụng, và các quy trình chứng thực khác.

Thông thường, quy trình xác thực văn bằng chứng chỉ bao gồm 3 bước: Phát hành, Chia sẻ và Xác thực.

Trước khi có blockchain, để quản lý văn bằng chứng chỉ, cá tổ chức sẽ sử dụng một số mô hình như:

- Văn bằng chứng chỉ bằng giấy: Mô hình truyền thống sử dụng văn bằng chứng chỉ được in trên giấy. Điểm mạnh của mô hình này là dễ dàng trong việc cung cấp và lưu trữ. Tuy nhiên, nó dễ bị mất, giả mạo hoặc sửa đổi. Đồng thời, việc xác minh tính hợp lệ của văn bằng chứng chỉ bằng giấy có thể gặp khó khăn.
- Văn bằng chứng chỉ số (chưa áp dụng blockchain): Việc phát hành, duy trì và sử dụng văn bằng chứng chỉ số cần ít nguồn lực hơn, do VBCC số có thể được kiểm tra tính xác thực một chuẩn định dạng cụ thể, đồng thời đảm bảo tính bảo mật cao hơn do sử dụng các giao thức mật mã. Tuy nhiên, khi chưa áp dụng chữ ký số, việc giả mạo VBCC số là rất dễ dàng.

Sau khi Blockchain ra đời, Blockchain đã trở thành một công nghệ quan trọng và đột phá trong quản lý và xác minh các văn bằng chứng chỉ. Công nghệ này cung cấp một cách thức đáng tin cậy và minh bạch để lưu trữ, xác minh và chia sẻ thông tin văn bằng. Trong bối cảnh môi trường giáo dục đang ngày càng chuyển dịch sang hình thức trực tuyến, việc sử dụng blockchain trong quản lý văn bằng chứng chỉ mang lại nhiều lợi ích đáng kể.

Dựa vào các tìm hiểu và nghiên cứu công nghệ blockchain trong quản lý và xác minh văn bằng chứng chỉ. Chúng tôi giới thiệu một hệ thống sử dụng blockchain để lưu trữ và xác minh tính hợp lệ của văn bằng chứng chỉ.

Trong phần cơ sở lý thuyết, chúng tôi trình bày các khái niệm cơ bản về blockchain, bao gồm cơ chế băm (hashing), chuỗi khối (blockchain) và cơ chế chứng minh công việc (proof-of-work). Một số tính chất và kỹ thuật chính của Blockchain. Chúng tôi cũng xem xét các nghiên cứu liên quan đã được thực hiện trong lĩnh vực này và nhấn mạnh sự quan trọng của tính toàn vẹn và khả năng xác minh trong quản lý văn bằng chứng chỉ.

Tiếp theo, chúng tôi trình bày chi tiết về thiết kế hệ thống, trong đó chúng tôi mô tả cách thức triển khai công nghệ blockchain và cách tích hợp front-end, backend và cơ sở dữ

liệu vào hệ thống. Chúng tôi sử dụng Vue.js để xây dựng giao diện người dùng thân thiện và Express.js để xử lý các yêu cầu từ phía người dùng. Cơ sở dữ liệu MongoDB được sử dụng để lưu trữ thông tin văn bằng chứng chỉ.

Sau đó, chúng tôi thực hiện thực nghiệm để kiểm tra hiệu suất và tính năng của hệ thống. Chúng tôi đánh giá khả năng xác minh và tính toàn vẹn của văn bằng chứng chỉ thông qua việc sử dụng blockchain. Kết quả thực nghiệm cho thấy hệ thống đáp ứng tốt yêu cầu và mang lại sự tin cậy và minh bạch trong quản lý văn bằng chứng chỉ.

Kết luận của chúng tôi là việc áp dụng công nghệ blockchain trong quản lý và xác minh văn bằng chứng chỉ mang lại nhiều lợi ích đáng kể. Hệ thống mà chúng tôi đã thiết kế và triển khai đáp ứng được yêu cầu về tính toàn vẹn, khả năng xác minh và bảo mật của văn bằng chứng chỉ. Công nghệ blockchain cung cấp một giải pháp đáng tin cậy và minh bạch để quản lý và chia sẻ thông tin văn bằng chứng chỉ trong lĩnh vực giáo dục.

III. Cơ sở lý thuyết

Trong phần cơ sở lý thuyết, chúng ta sẽ tìm hiểu về các khái niệm cơ bản của công nghệ blockchain và các kỹ thuật chính liên quan đến tính toàn vẹn và khả năng xác minh của blockchain.

A. Hàm băm (Hashing)

Hàm băm là một thuật toán mã hóa mật mã sử dụng để chuyển đổi dữ liệu đầu vào thành một chuỗi ký tự có độ dài cố định, gọi là mã hash. Đặc điểm quan trọng của hàm băm là bất kỳ thay đổi nhỏ nào trong dữ liệu đầu vào cũng sẽ dẫn đến một mã hash khác biệt. Hàm băm được sử dụng rộng rãi trong blockchain để bảo vệ tính toàn vẹn của dữ liệu.

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C

Hình 1. Ví dụ hàm băm

B. Chuỗi khối (Blockchain)

Chuỗi khối là một cấu trúc dữ liệu liên kết trong đó mỗi khối chứa thông tin và một mã hash duy nhất của khối trước đó. Việc liên kết các khối thông qua mã hash tạo thành một chuỗi không thể thay đổi. Bất kỳ sự thay đổi nào trong một khối sẽ làm thay đổi mã hash của nó và ảnh hưởng tới các khối kế tiếp. Điều này tạo ra tính toàn vẹn và an ninh cho dữ liệu trong chuỗi khối.

C. Cơ chế chứng minh công việc (Proof-of-Work)

Cơ chế chứng minh công việc là một phương pháp được sử dụng để xác minh và thêm các khối mới vào blockchain. Nó yêu cầu người tham gia mạng phải thực hiện một lượng công việc tính toán phức tạp để tìm ra một giá trị nonce (số ngẫu nhiên) sao cho mã hash của khối đáp ứng một yêu cầu nhất định, ví dụ như có một số lượng ký tự 0 ở đầu mã hash. Quá trình này tạo ra một khối mới được xác minh và thêm vào chuỗi khối.

D. Tính chất của blockchain:

Tính toàn vẹn (Integrity): Blockchain đảm bảo tính toàn vẹn của dữ liệu bằng cách sử dụng mã hash và chuỗi khối. Bất kỳ thay đổi nào trong dữ liệu cũng sẽ làm thay đổi mã hash và phá vỡ liên kết giữa các khối.

Khả năng xác minh (Verifiability): Mọi người dùng trong mạng có thể xác minh tính hợp lệ của dữ liệu được lưu trữ trong blockchain bằng cách so sánh mã hash và kiểm tra chuỗi khối.

Bảo mật (Security): Blockchain sử dụng mã hóa mật mã, mã hash và cơ chế chứng minh công việc để đảm bảo tính bảo mật của dữ liệu. Việc sử dụng mạng phân tán và cơ chế chứng minh công việc cũng làm cho blockchain khó bị tấn công và thay đổi dữ liệu.

Qua cơ sở lý thuyết này, chúng ta hiểu được cách các thành phần như hàm băm, chuỗi khối và cơ chế chứng minh công việc kết hợp lại để tạo nên tính toàn vẹn, khả năng xác minh và bảo mật của công nghệ blockchain.

IV. Nghiên cứu liên quan

Trong lĩnh vực quản lý và xác minh văn bằng chứng chỉ sử dụng công nghệ blockchain, đã có một số nghiên cứu đáng chú ý đã được tiến hành. Dưới đây là hai nghiên cứu liên quan:

A. Dự án BlockCerts

Blockcerts là một dự án nguồn mở, ra đời vào năm 2016 bởi một nhóm các nhà nghiên cứu tại MIT Media Lab - Hoa Kỳ. Nghiên cứu tập trung vào việc áp dụng công nghệ blockchain để tạo ra một hệ thống quản lý văn bằng chứng chỉ số an toàn và minh bạch. BlockCerts sử dụng Ethereum blockchain để lưu trữ dữ liệu văn bằng chứng chỉ và cung cấp khả năng xác minh công khai. Dự án này cũng giúp người dùng có quyền kiểm soát thông tin văn bằng của họ và chia sẻ nhanh chóng với các bên liên quan.

Điểm mạnh:

- Tích hợp công nghệ blockchain Ethereum để lưu trữ dữ liệu văn bằng chứng chỉ, đảm bảo tính toàn vẹn và bảo mật.
- Cung cấp khả năng xác minh công khai, cho phép người dùng và các bên liên quan kiểm tra tính hợp lệ của văn bằng chứng chỉ.
- Cho phép người dùng kiểm soát thông tin văn bằng của họ và chia sẻ nhanh chóng với các bên quan tâm.

Hạn chế:

- Sử dụng blockchain Ethereum có thể gây ra chi phí giao dịch cao và tốn thời gian xác minh.
- Phụ thuộc vào mạng lưới blockchain công cộng, có thể gặp phải các hạn chế về hiệu suất và khả năng mở rộng.

B. Dự án BTCert

Dự án BTCert được phát triển bởi một nhóm nghiên cứu thuộc Đại học Birmingham và thông tin chi tiết có thể được tìm thấy tại liên kết:

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

Nghiên cứu tập trung vào việc sử dụng công nghệ blockchain để quản lý và xác minh tính hợp lệ của văn bằng chứng chỉ trong lĩnh vực giáo dục. Hệ thống BTCert sử dụng Ethereum blockchain và cung cấp các tính năng như tạo văn bằng chứng chỉ số, chia sẻ văn bằng và xác minh công khai. Nghiên cứu này cũng tập trung vào việc xây dựng các cơ chế bảo mật và quyền riêng tư cho người dùng.

Điểm mạnh:

- Sử dụng công nghệ blockchain Ethereum để tạo và quản lý văn bằng chứng chỉ, đảm bảo tính toàn vẹn và khả năng xác minh.
- Cung cấp các tính năng như tạo văn bằng chứng chỉ số, chia sẻ văn bằng và xác minh công khai.
- Xây dựng cơ chế bảo mật và quyền riêng tư, đảm bảo rằng chỉ những người được ủy quyền có thể truy cập thông tin văn bằng.

Hạn chế:

- Cũng như Dự án BlockCerts, việc sử dụng blockchain Ethereum có thể gây ra chi phí giao dịch cao và tốn thời gian xác minh.
- Phụ thuộc vào mạng lưới blockchain công cộng, có thể gặp phải các hạn chế về hiệu suất và khả năng mở rộng.

Cả hai nghiên cứu trên đều khẳng định tiềm năng và lợi ích của việc sử dụng công nghệ blockchain trong việc quản lý và xác minh văn bằng chứng chỉ. Các dự án này đã cung cấp những phương pháp và kiến thức quan trọng để tiến xa hơn trong việc tạo ra một hệ thống quản lý văn bằng chứng chỉ an toàn, minh bạch và có khả năng xác minh.

V. Thiết kế hệ thống CertsChain

Trong phần 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 bài báo này, chúng tôi đặt tên cho hệ thống của mình là **CertsChain**.

A. Định nghĩa bài toán

Hiện nay, các tổ chức đào tạo tại Việt Nam thường thực hiện các bước quản lý chứng chỉ như sau:

Bước 1: Chọn và liệt kê danh sách học viên, sinh viên tốt nghiệp.

Bước 2: Tạo hồ sơ và gửi đến Bộ Giáo dục và Đào tạo để duyệt cấp phôi bằng.

Bước 3: Tiếp nhận và quản lý phôi bằng.

Bước 4: Xuất bản, in VBCC.

Bước 5: Xem xét và ký VBCC.

Bước 6: Cấp phát và xử lý các trường hợp VBCC bị hỏng.

Bước 7: Công bố thông tin về cấp phát VBCC trên trang web.

Bước 8: Quản lý VBCC.

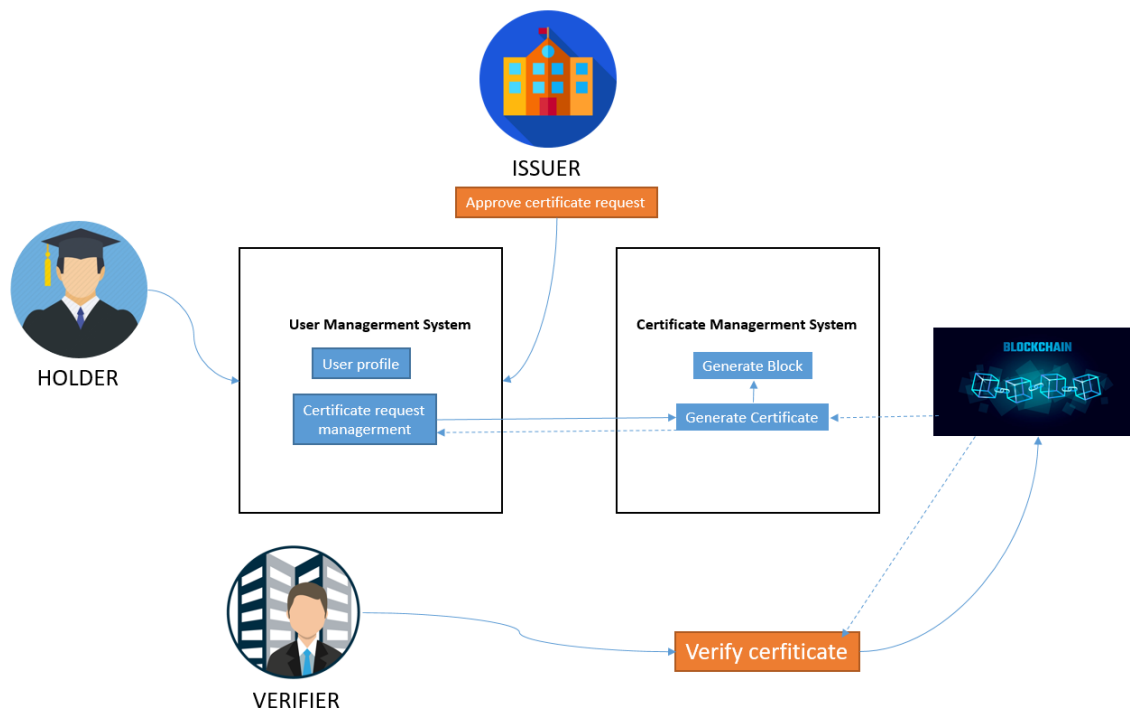
Sau khi nhận được VBCC, người sử dụng cần phải đem bản chứng chỉ gốc đến một cơ quan công chứng nếu muốn chia sẻ thông tin về chứng chỉ với một bên thứ 3. Để xác minh tính đúng đắn của VBCC, bên thứ 3 phải liên hệ với đơn vị phát hành, tuy nhiên việc này mất nhiều thời gian và tiền bạc.

Để giải quyết vấn đề này, quản lý VBCC đào tạo có thể sử dụng công nghệ Blockchain, với các yêu cầu sau:

- Đảm bảo an toàn thông tin cho chứng chỉ khi được cấp phát.
- Tiết kiệm nguồn lực và chi phí trong việc thực hiện, quản lý và xác minh VBCC.
- Việc xác minh tính hợp lệ của chứng chỉ có thể được thực hiện một cách độc lập và không phụ thuộc vào đơn vị phát hành.

B. Mô hình thực hiện

Từ các module của dự án, mô hình sẽ được hình thành với cách thức hoạt động như sau:



Hình 2. Mô hình thực hiện của hệ thống

Để quản lý và xác minh VBCC, hệ thống sẽ thực hiện các bước sau đây:

1) Các đơn vị đào tạo (Issuer) sẽ có hệ thống quản lý thông tin học sinh, sinh viên hoặc Holder. Nếu Holder đủ điều kiện được cấp VBCC, Holder sẽ yêu cầu đơn vị đào tạo cấp VBCC cho mình thông qua hệ thống CertsChain.

2) Issuer sẽ xem xét yêu cầu cấp VBCC của Holder. Nếu đúng, hệ thống CertsChain sẽ tạo VBCC dưới dạng file PDF và tạo một block mới lưu thông tin VBCC, mã số VBCC và thông tin file PDF trên CertsChain Blockchain. Sau đó, hệ thống sẽ cập nhật để Holder có thể xem và chia sẻ VBCC.

3) Holder có thể truy cập vào hệ thống CertsChain để lấy file PDF, mã số VBCC và gửi cho một bên thứ 3 (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.

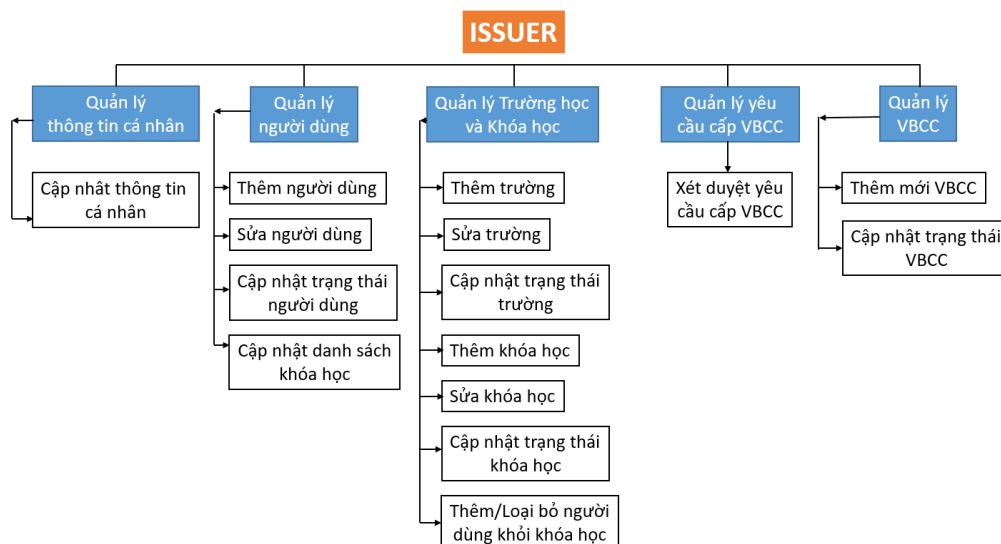
C. Các chức năng của hệ thống

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

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.

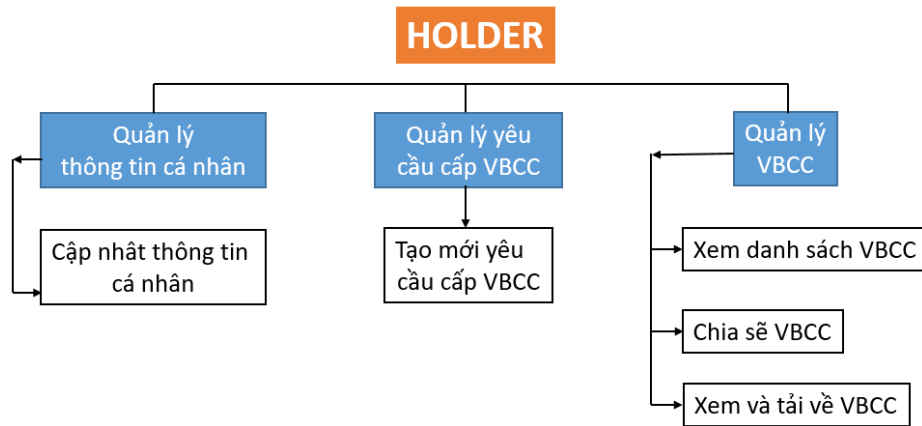
Sơ đồ phân rã chức năng Issuer



❖ **Người dùng loại 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.

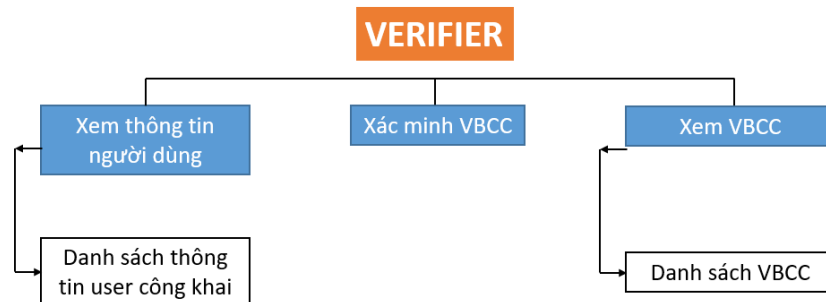
Sơ đồ phân rã chức năng Issuer



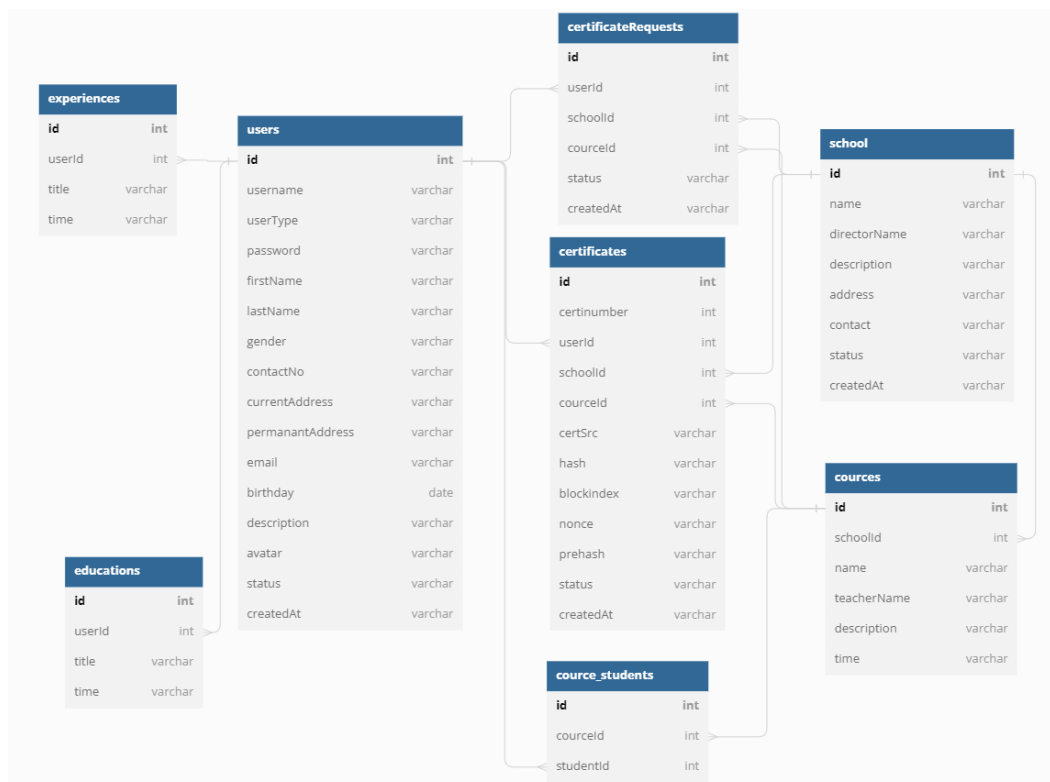
❖ Người dùng loại Verifier

STT	Chức năng	Mô tả
1	Xem thông tin của 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 trực tiếp trên hệ thống.

Sơ đồ phân rã chức năng Issuer



D. Cơ sở dữ liệu



VI. Xây dựng hệ thống CertsChain

A. 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: CSDL 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 chúng tôi quyết định xây dựng dưới dạng là một Web Application Single Page.

Front-end: 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.

Back-end: Backend chúng 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.

BlockChain: sẽ được chúng tôi tự xây dựng bằng NodeJS và chạy ở Backend.

Một số thư viện của NodeJS được chúng 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
- Pdkit: thư viện giúp sinh ra các file PDF, chúng tôi sử dụng để tạo ra các file VBCC dưới định dạng PDF.
- Qrcode: thư viện giúp tạo ra các mã QR code. Chúng 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.

B. 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, courseId, 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.

C. Xây dựng hệ thống API

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

Module	Api Method và URL	Mô tả - Chức năng
<i>Authentication</i>	/user/login	Người dùng loại Issuer hay Holder muốn dùng các chức năng của mình đăng nhập vào hệ thống, sử dụng API này.
<i>Users</i>	/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-courses	Lấy ra thông tin cần thiết để cập nhật danh sách khóa học của người dùng
	/user/update-courses	Cập nhật danh sách khóa học của người dùng có tham gia.
<i>Schools And Courses</i>	/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.
<i>Certificates</i>	/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 courseId.
	/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.
<i>Certificate Requests</i>	/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.

VII. Thực nghiệm hệ thống CertsChain

Dựa theo thiết kế, hệ thống sẽ bao gồm các chức năng theo mô tả.

Một số chức năng chính như:

- Xem thông tin người dùng.
- Cấp phát văn bằng chứng chỉ.
- Xem danh sách văn bằng chứng chỉ.
- Chia sẻ văn bằng chứng chỉ.
- Xác minh văn bằng chứng chỉ.

A. Chức năng xem thông tin người dùng

Bất kỳ ai khi truy cập tới hệ thống thì cũng có thể truy cập *trang Users* để có thể xem thông tin người dùng trên hệ thống.

Username	Name	Email	Created At	Status	Actions
usertest	User Test	wyhyq@mailinator.com	30/10/2022 - 02:19:12	Active	View Detail
pahebumi	Damian Long	havuwiz@mailinator.com	14/08/2022 - 09:13:27	Active	View Detail
vajoxibuke	Elliott Mayer	nirjoje@mailinator.com	13/08/2022 - 07:04:29	Active	View Detail
kyfimi	Alea Rhodes	kirowowy@mailinator.com	13/08/2022 - 07:04:05	Active	View Detail
dedulox	Kenneth Chapman	hivem@mailinator.com	13/08/2022 - 02:27:31	Active	View Detail
cvthang	Cao Thăng	cvthang56h2@gmail.com	13/08/2022 - 02:23:34	Active	View Detail
fayyhitit	Ignatius Finch	bikonone@mailinator.com	08/08/2022 - 10:03:00	Active	View Detail
farosi	Lilah Alexander	vymuzivufe@mailinator.com	08/08/2022 - 09:56:51	Active	View Detail
duzyte	Ima Tucker	xivi@mailinator.com	08/08/2022 - 09:56:47	Archived	View Detail

Danh sách tất cả các User trong hệ thống

Để xem chi tiết thông tin người dùng, click vào button *View Detail*.

CERTSCHAIN

[Back to Verifier Page](#)

Trang chi tiết User

B. Chức năng cấp phát văn bằng chứng chỉ

Đối với người dùng loại Issuer, sẽ có chức năng cấp phát văn bằng chứng chỉ.

Tại *trang Certificates* của Issuer, issuer có thể quản lý các VBCC trong hệ thống:

The screenshot shows the 'ISSUER' dashboard with a sidebar containing 'Certificate Requests', 'Users Management', 'Schools and Courses', 'Certificates Management' (highlighted), and 'Profile'. The main area displays a table titled 'List Certs' with columns: Certificate Number, User, School and Course, Created At, Link, and Status. There are three rows of certificates, each with a green 'Active' toggle switch. At the top right, there are buttons for 'Introduction', 'Instruction', and 'Verify Certificate', along with a user greeting 'Hello, cvthang!' and a 'Logout' link.

Certificate Number	User	School and Course	Created At	Link	Status
62421769	cvthang-Cao Thắng	Thạc sĩ Công nghệ Thông tin - 2020 - 2022	30/10/2022 - 09:30:55	certificate-Cao Thắng-Đại học Nha Trang-Thạc sĩ Công nghệ Thông tin-2020 - 2022-1667097055258.pdf	Active
56326986	usertest-User Test	Thạc sĩ Công nghệ Thông tin - 2020 - 2022	30/10/2022 - 09:30:52	certificate-User Test-Đại học Nha Trang-Thạc sĩ Công nghệ Thông tin-2020 - 2022-1667097051456.pdf	Active
32548546	farosi-Lilah Alexander	Thạc sĩ Công nghệ Thông tin - 2020 - 2022	30/10/2022 - 09:30:47	certificate-Lilah Alexander-Đại học Nha Trang-Thạc sĩ Công nghệ Thông tin-2020 - 2022-1667097045421.pdf	Active

Trang Certificates của Issuer

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

The 'Add Cert' popup form includes a toggle switch 'Is Generate for Course?' set to 'Yes'. Below this are three dropdown menus for 'User' (selected: Cao Thắng (cvthang)), 'School' (selected: Đại học Nha Trang), and 'Course' (selected: Thạc sĩ Quản trị kinh doanh - 2020 - 2022). At the bottom right, there are two buttons: 'CLOSE' and 'SAVE CHANGES'.

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 Course?*, chọn khóa học muốn cấp phát và click button *Save Changes*.

certificate-Cao Thang-

Add Cert

Is Generate for Course? ☒ No

School

Course

[CLOSE](#) [SAVE CHANGES](#)

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:

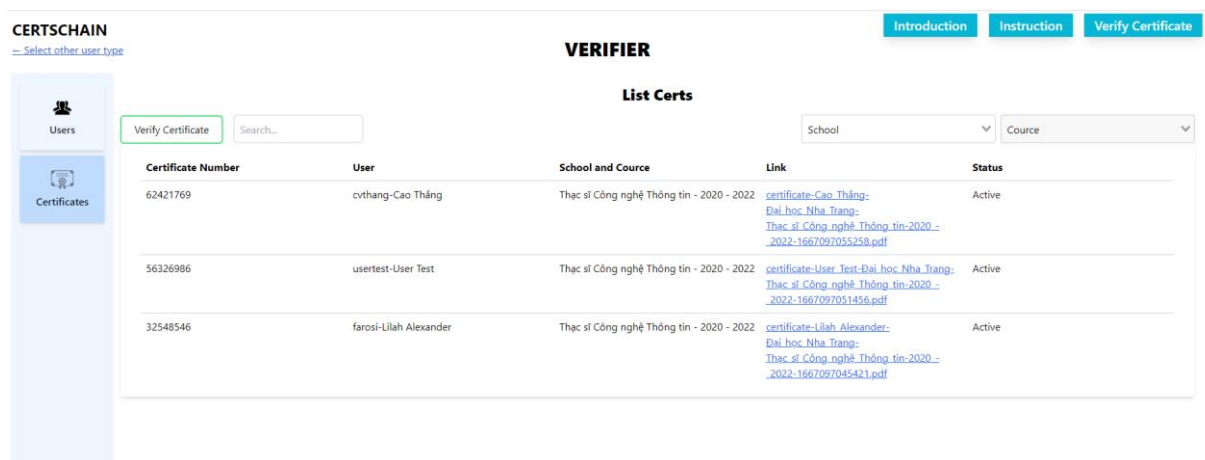


Mẫu văn bằng chứng chỉ của CertsChain

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

C. Chức năng xem danh sách văn bằng chứng chỉ

Trên hệ thống này, tất cả thông tin về văn bằng chứng chỉ đều sẽ được công khai, ai cũng có thể xem được danh sách văn bằng chứng chỉ tại *trang Certificates*:



The screenshot shows the 'VERIFIER' section of the CERTSCHAIN system. It includes a sidebar with 'Users' and 'Certificates' options. The main area is titled 'List Certs' and contains a table with columns: Certificate Number, User, School and Course, Link, and Status. There are also filters for School and Course, and a 'Verify Certificate' button with a search bar.

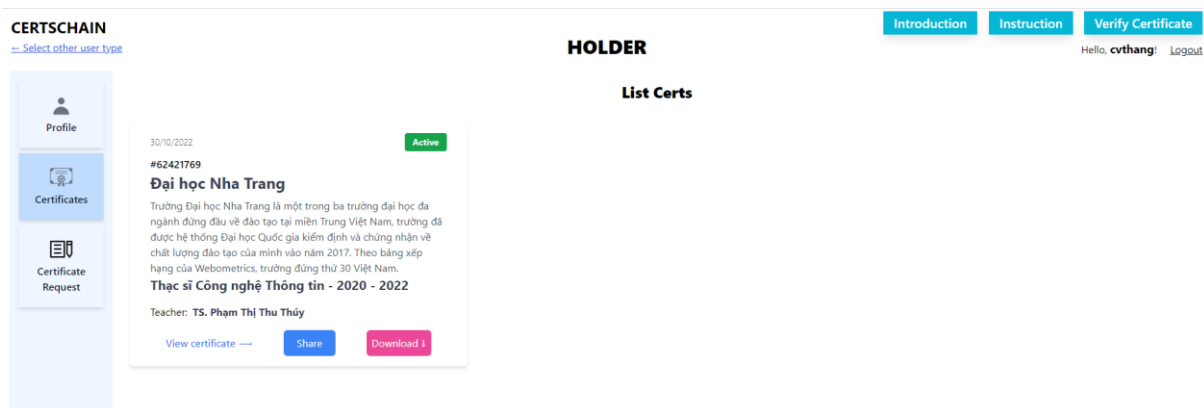
Certificate Number	User	School and Course	Link	Status
62421769	cvthang-Cao Thắng	Thạc sĩ Công nghệ Thông tin - 2020 - 2022	certificate-Cao Thắng-Đại học Nha Trang-Thạc sĩ Công nghệ Thông tin-2020 - 2022-1667097055258.pdf	Active
56326986	usertest-User Test	Thạc sĩ Công nghệ Thông tin - 2020 - 2022	certificate-User Test-Đại học Nha Trang-Thạc sĩ Công nghệ Thông tin-2020 - 2022-1667097051456.pdf	Active
32548546	farosi-Lilah Alexander	Thạc sĩ Công nghệ Thông tin - 2020 - 2022	certificate-Lilah Alexander-Đại học Nha Trang-Thạc sĩ Công nghệ Thông tin-2020 - 2022-1667097045421.pdf	Active

Danh sách tất cả các certificate trong hệ thống

D. Chức năng chia sẻ văn bằng chứng chỉ

Đối với người dùng loại Holder, sẽ có chức năng xem danh sách chứng chỉ mình có và chia sẻ thông tin văn bằng chứng chỉ của mình.

Tại trang Certificates của Holder sẽ hiển thị danh sách các VBCC của Holder:



The screenshot shows the 'HOLDER' section of the CERTSCHAIN system. It includes a sidebar with 'Profile', 'Certificates', and 'Certificate Request' options. The main area is titled 'List Certs' and displays a detailed view of a certificate. The certificate is for 'Đại học Nha Trang' and 'Thạc sĩ Công nghệ Thông tin - 2020 - 2022'. It includes the teacher's name 'TS. Phạm Thị Thu Thủy' and buttons for 'View certificate', 'Share', and 'Download'.

30/10/2022 Active

#62421769

Đại học Nha Trang

Trường Đại học Nha Trang là một trong ba trường đại học đa ngành đứng đầu về đào tạo tại miền Trung Việt Nam, trường đã được hệ thống Đại học Quốc gia kiểm định và chứng nhận về chất lượng đào tạo của mình vào năm 2017. Theo bảng xếp hạng của Webometrics, trường đứng thứ 30 Việt Nam.

Thạc sĩ Công nghệ Thông tin - 2020 - 2022

Teacher: TS. Phạm Thị Thu Thủy

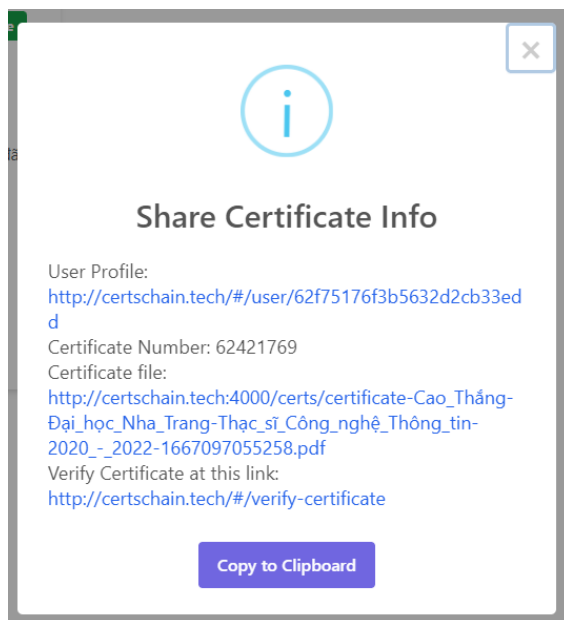
[View certificate](#) [Share](#) [Download](#)

Hình VII.1. 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 VII.2. Popup chia sẻ thông tin Certificate

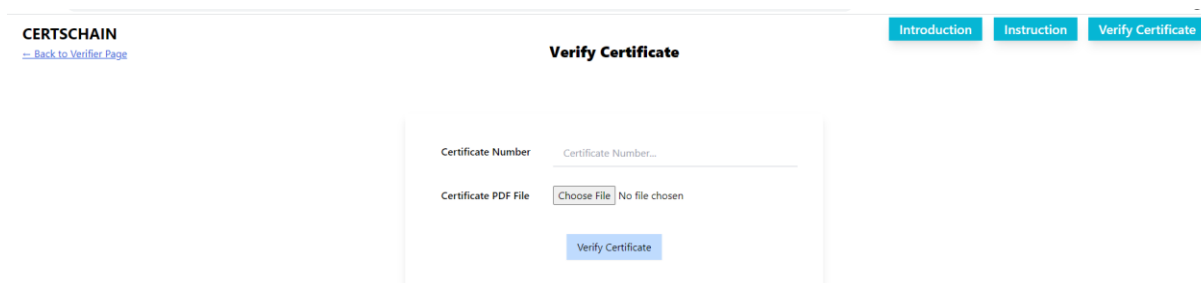
Tiếp đó, Holder có thể click vào button *Copy to Clipboard* để copy thông tin này và gửi đi.

E. Chức năng xác minh văn bằng chứng chỉ

Bất kỳ ai khi truy cập tới hệ thống thì cũng có thể truy cập *trang Verify Certificate* để có thể xác minh văn bằng chứng chỉ.

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.

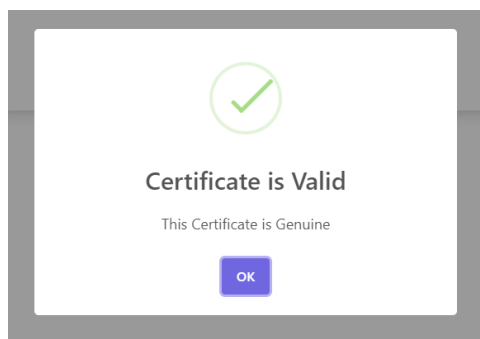


Trang xác minh VBCC

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***

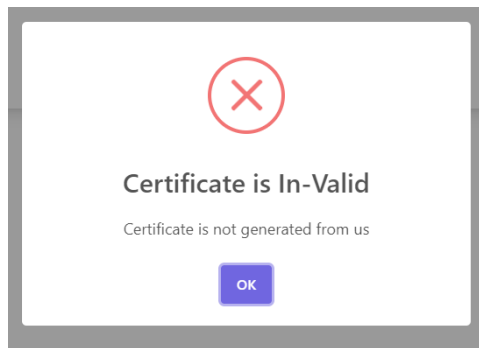
Hệ thống sẽ thông báo như sau:



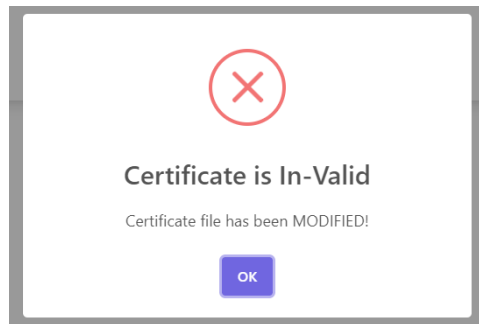
➤ ***Nếu VBCC không hợp lệ***

Hệ thống sẽ hiển thị một số lỗi như sau:

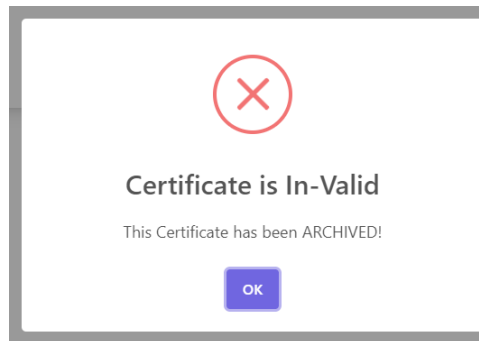
- VBCC không được cấp phát bởi hệ thống.



- VBCC đã bị sửa chữa.



- VBCC không còn hiệu lực.



VIII. KẾT LUẬN

A. Kết quả đạt được:

Nghiên cứu đã thành công trong việc áp dụng công nghệ Blockchain vào quản lý và xác minh văn bằng chứng chỉ.

Hệ thống đã được triển khai và kiểm tra trong một môi trường thực tế, và đã chứng minh tính khả thi và hiệu quả của việc sử dụng Blockchain trong lĩnh vực này.

Hệ thống cho phép người dùng tạo, xem và xác minh văn bằng chứng chỉ một cách tin cậy, minh bạch và không thể sửa đổi.

Đã triển khai lên internet tại địa chỉ: <http://certschain.tech/>

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

B. Đóng góp của nghiên cứu:

Nghiên cứu đã đưa ra một phương pháp mới và hiệu quả để quản lý và xác minh văn bằng chứng chỉ bằng cách sử dụng công nghệ Blockchain.

Hệ thống đã giúp cải thiện tính toàn vẹn và tin cậy của thông tin văn bằng, ngăn chặn việc sửa đổi trái phép và giả mạo văn bằng.

Đồng thời, việc sử dụng Blockchain cũng mang lại tính minh bạch, cho phép các bên liên quan kiểm tra và xác minh tính hợp lệ của văn bằng chứng chỉ một cách dễ dàng.

C. Hạn chế và hướng phát triển tiếp theo:

Mặc dù nghiên cứu đã đạt được kết quả tích cực, vẫn còn một số hạn chế cần được cải thiện. Ví dụ, hệ thống hiện tại chưa có tính năng rà soát ngang hàng (peer-to-peer) và vẫn phụ thuộc vào một máy chủ trung gian.

Hướng phát triển tiếp theo có thể tập trung vào nâng cao tính bảo mật và hiệu suất của hệ thống, bao gồm việc xây dựng mạng ngang hàng (peer-to-peer network) để đảm bảo tính phân tán và khả năng chịu lỗi cao hơn.

Nghiên cứu cũng có thể mở rộng để áp dụng công nghệ Blockchain vào các lĩnh vực quản lý thông tin khác, như quản lý tài liệu, chứng chỉ nghề nghiệp, hoặc giấy tờ chứng minh quyền sở hữu.

Tổng kết lại, việc nghiên cứu và ứng dụng công nghệ Blockchain trong quản lý và xác minh văn bằng chứng chỉ đã mang lại những kết quả tích cực và có tiềm năng ứng dụng

rộng rãi trong lĩnh vực này. Điều này đóng góp vào sự phát triển của công nghệ và giúp tạo ra một môi trường quản lý văn bằng chứng chỉ an toàn, minh bạch và tin cậy hơn trong tương lai.

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

[9]. Ali Alammery, 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>

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

<https://youtu.be/r20hCF9NbTo>