

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NHA TRANG**



CAO VIỆT THẮNG

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

LUẬN VĂN THẠC SĨ

KHÁNH HÒA - 2023

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NHA TRANG



CAO VIỆT THẮNG

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

LUẬN VĂN THẠC SĨ

Ngành:	Công nghệ thông tin
Mã số:	8480201
Mã số học viên:	61CH097
Quyết định giao đề tài:	828/QĐ-ĐHNT ngày 15/07/2022
Quyết định thành lập hội đồng:	1290/QĐ-ĐHNT ngày 08/09/2023
Ngày bảo vệ:	01/10/2023
Người hướng dẫn khoa học:	
TS. Nguyễn Đình Hưng	
Chủ tịch Hội đồng	
TS. Nguyễn Đình Hưng	
Phòng DT Sau đại học:	
Hoàng Hà Giang	

KHÁNH HÒA - 2023

LỜI CAM ĐOAN

Tôi xin cam đoan mọi kết quả của đề tài: “*Nghiên cứu và ứng dụng công nghệ Blockchain trong quản lý và xác minh văn bằng chứng chỉ*” là công trình nghiên cứu của cá nhân tôi và chưa từng được công bố trong bất cứ công trình khoa học nào khác cho tới thời điểm này.

Khánh Hòa, ngày tháng năm 2023

Tác giả luận văn

(ký và ghi rõ họ tên)

Cao Viết Thắng

LỜI CẢM ƠN

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

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

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

Một lần nữa, tôi xin chân thành cảm ơn!

Khánh Hòa, ngày tháng năm 2023

Tác giả luận văn

(ký và ghi rõ họ tên)

Cao Viết Thắng

MỤC LỤC

LỜI CAM ĐOAN	i
LỜI CẢM ƠN	ii
MỤC LỤC	iii
DANH MỤC THUẬT NGỮ VIẾT TẮT	vi
DANH MỤC BẢNG	vii
DANH MỤC HÌNH	viii
TRÍCH YẾU LUẬN VĂN.....	x
TỔNG QUAN.....	1
➤ Lý do chọn đề tài	1
➤ Mục đích nghiên cứu	2
➤ Đối tượng, chủ thể và phạm vi nghiên cứu	2
➤ Phương pháp nghiên cứu	2
➤ Ý nghĩa khoa học và thực tiễn của luận văn.....	3
CHƯƠNG 1. GIỚI THIỆU CÔNG NGHỆ BLOCKCHAIN	4
1.1. Giới thiệu Blockchain	4
1.2. Nền tảng lý thuyết.....	5
1.2.1. Hàm băm.....	5
1.2.2. Chữ ký số	7
1.3. Các kỹ thuật chính của Blockchain.....	8
1.3.1. Cấu trúc phi tập trung	9
1.3.2. Tính toán tin cậy.....	11
1.3.3. Bằng chứng công việc.....	11
1.4. Tính chất của Blockchain.....	11
1.4.1. Cơ chế đồng thuận phân quyền (decentralized consensus).....	11
1.4.2. Bảo trì tập thể (collective maintenance)	12

1.4.3.	<i>Tính bảo mật và độ tin cậy</i>	12
1.4.4.	<i>Mã nguồn mở</i>	12
1.5.	<i>Phân loại các hệ thống Blockchain</i>	12
1.6.	<i>Các ứng dụng điển hình của công nghệ Blockchain</i>	12
1.6.1.	<i>Ứng dụng Blockchain trong tiền số</i>	13
1.6.2.	<i>Ứng dụng Blockchain trong hợp đồng thông minh (Smart contract)</i>	13
1.6.3.	<i>Một số ứng dụng nổi bật khác</i>	14
CHƯƠNG 2. TỔNG QUAN QUẢN LÝ VÀ XÁC MINH VĂN BẰNG, CHỨNG CHỈ		16
2.1.	<i>Giới thiệu công tác quản lý và xác minh văn bằng, chứng chỉ</i>	16
2.1.1.	<i>Văn bằng, chứng chỉ là gì?</i>	16
2.1.2.	<i>Quy trình liên quan tới văn bằng, chứng chỉ</i>	16
2.1.3.	<i>Một số mô hình quản lý và xác minh văn bằng chứng chỉ không áp dụng công nghệ Blockchain</i>	17
2.1.4.	<i>Mô hình quản lý và xác minh văn bằng chứng chỉ sử dụng Blockchain</i>	19
2.2.	<i>Tình hình và các nghiên cứu liên quan</i>	21
2.2.1.	<i>Blockcerts</i>	21
2.2.2.	<i>BTCert</i>	23
CHƯƠNG 3. ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN TRONG QUẢN LÝ VÀ XÁC MINH VĂN BẰNG, CHỨNG CHỈ		24
3.1.	<i>Thiết kế hệ thống CertsChain</i>	24
3.1.1.	<i>Định nghĩa bài toán</i>	24
3.1.2.	<i>Mô hình thực hiện</i>	25
3.1.3.	<i>Sơ đồ phân rã chức năng</i>	26
3.1.4.	<i>Cơ sở dữ liệu</i>	32
3.2.	<i>Xây dựng hệ thống CertsChain</i>	33

3.2.1. <i>Môi trường triển khai và công cụ phát triển</i>	33
3.2.2. <i>Xây dựng Blockchain của hệ thống</i>	35
3.2.3. <i>Xây dựng hệ thống API</i>	36
3.3. <i>Thực nghiệm hệ thống CertsChain</i>	38
3.3.1. <i>Người dùng loại Issuer</i>	39
3.3.2. <i>Người dùng loại Holder</i>	46
3.3.3. <i>Người dùng loại Verifier</i>	49
3.3.4. <i>Trang Verify Certificate</i>	50
CHƯƠNG 4. KẾT LUẬN VÀ KIẾN NGHỊ	52
4.1. <i>Kết quả đạt được</i>	52
4.2. <i>Hạn chế của đề tài</i>	53
4.3. <i>Hướng phát triển của đề tài</i>	54
4.4. <i>Đề nghị ý kiến</i>	54
TÀI LIỆU THAM KHẢO	55

DANH MỤC THUẬT NGỮ VIẾT TẮT

Thuật ngữ	Nghĩa tiếng Việt	Nghĩa tiếng Anh
API	Giao diện lập trình ứng dụng	Application Programming Interface
BackEnd	Những chức năng hỗ trợ hoạt động của một trang web hoặc ứng dụng mà người dùng không nhìn thấy được	Functions that support the operation of a website or application that are not visible to the user
CSDL	Cơ sở dữ liệu	Database
FrontEnd	Phần tương tác với người dùng trên một trang web hoặc ứng dụng	The user interaction part of a website or application
Holder	Học viên hay Người nhận VBCC	Holder unit
Issuer	Đơn vị phát hành VBCC	Issuer unit
PDF	File dạng PDF	Portable Document Format
QR	Mã vạch hai chiều	QR Code
Smart contract	Hợp đồng thông minh	Smart contract
URL	Liên kết URL	Uniform Resource Locator
VBCC	Văn bằng, chứng chỉ	Certificate
Verifier	Đơn vị cần xác minh VBCC	Verifier unit

DANH MỤC BẢNG

Bảng 3.1. Các chức năng của Issuer	26
Bảng 3.2. Các chức năng của Holder.....	29
Bảng 3.3. Các chức năng của Verifier	31
Bảng 3.4. Các API của hệ thống CertsChain.....	36

DANH MỤC HÌNH

Hình 1.1. Mô hình thực hiện chữ ký số	7
Hình 1.2. Cấu trúc dữ liệu của Blockchain.....	8
Hình 1.3. Cấu trúc của block gốc trong Blockchain.....	9
Hình 3.1. Mô hình thực hiện của hệ thống	25
Hình 3.2. Sơ đồ phân rã chức năng Issuer	28
Hình 3.3. Sơ đồ phân rã chức năng Holder.....	30
Hình 3.4. Sơ đồ phân rã chức năng Verifier	31
Hình 3.5. Cơ sở dữ liệu của hệ thống CertsChain	32
Hình 3.6. Vue.js	33
Hình 3.7. NodeJS - Express	34
Hình 3.8. Trang chủ	38
Hình 3.9. Trang đăng nhập	38
Hình 3.10. Trang Profile của Issuer.....	39
Hình 3.11. Trang Users của Issuer.....	39
Hình 3.12. Popup tạo mới User	40
Hình 3.13. Popup cập nhật User	40
Hình 3.14. Popup Cập nhật danh sách danh sách Courses của User tham gia	41
Hình 3.15. Trang Schools and Courses của Issuer	42
Hình 3.16. Popup tạo mới School and Course.....	42
Hình 3.17. Popup cập nhật School and Course	43
Hình 3.18. Trang Certificates của Issuer	43
Hình 3.19. Popup tạo mới Certificate	44
Hình 3.20. Cấp phát VBCC cho học viên trong khóa học.....	44
Hình 3.21. Mẫu văn bằng chứng chỉ của CertsChain	45
Hình 3.22. Trang Certificate Requests của Issuer	45
Hình 3.23. Trang Profile của Holder	46
Hình 3.24. Trang danh sách Certificate của Holder	46
Hình 3.25. Popup chia sẻ thông tin Certificate	47
Hình 3.26. Trang Certificate Requests của Holder.....	48
Hình 3.27. Popup tạo mới yêu cầu cấp phát VBCC	48

Hình 3.28. Danh sách tất cả các User trong hệ thống.....	49
Hình 3.29. Trang chi tiết User	49
Hình 3.30. Danh sách tất cả các certificate trong hệ thống	50
Hình 3.31. Trang xác minh VBCC	50

TRÍCH YẾU LUẬN VĂN

Tên đề tài: “*Nghiên cứu và ứng dụng công nghệ Blockchain trong quản lý và xác minh văn bằng chứng chỉ*”

Họ và tên học viên: Cao Viết Thắng

Mã học viên: 61CH097

Lớp: Công nghệ thông tin

Từ khóa: Blockchain, quản lý và xác minh văn bằng chứng chỉ.

Nội dung tóm tắt:

Luận văn thạc sĩ này tập trung vào nghiên cứu và ứng dụng công nghệ Blockchain trong việc quản lý và xác minh văn bằng, chứng chỉ. Để đạt được mục tiêu này, nghiên cứu đã được thực hiện theo các mục sau:

Đầu tiên, luận văn trình bày về bối cảnh, tình hình hiện tại của quản lý văn bằng, chứng chỉ, nhấn mạnh về các thách thức như gian lận, việc sao chép, giả mạo và sự thiếu minh bạch trong việc xác minh thông tin.

Sau đó, luận văn trình bày các khái niệm cơ bản về công nghệ Blockchain, bao gồm cách hoạt động của Blockchain và đặc điểm của một mạng Blockchain được sử dụng để quản lý các văn bằng, chứng chỉ.

Đánh giá một số công trình nghiên cứu liên quan và các vấn đề trong công tác quản lý và xác minh văn bằng chứng chỉ trong hệ thống hiện tại, bao gồm vấn đề về tính toàn vẹn, an ninh, bảo mật, sự phân cấp và tính cập nhật của dữ liệu.

Tiếp theo, luận văn trình bày cách sử dụng Blockchain để quản lý và xác minh văn bằng chứng chỉ. Xây dựng một mô hình Blockchain phù hợp để quản lý và xác minh văn bằng chứng chỉ. Mô hình này sử dụng một Blockchain riêng biệt để lưu trữ các thông tin về văn bằng chứng chỉ, bao gồm các thông tin của người dùng, của tổ chức giáo dục, thông tin văn bằng chứng chỉ được cấp và các thông điệp đã được mã hóa.

Cuối cùng, luận văn đánh giá các ưu điểm và hạn chế của việc sử dụng công nghệ Blockchain trong việc quản lý và xác minh văn bằng chứng chỉ và đề xuất các hướng nghiên cứu tiếp theo để nâng cao hiệu quả của hệ thống.

Tóm lại, luận văn thạc sĩ này là một nỗ lực để giải quyết một số vấn đề trong hệ thống quản lý văn bằng, chứng chỉ hiện tại, bao gồm việc giảm thiểu các rủi ro về tính

toàn vẹn và bảo mật, cải thiện tính cập nhật và tính nhất quán của dữ liệu và tăng tính minh bạch trong việc xác minh văn bằng chứng chỉ.

TỔNG QUAN

➤ Lý do chọn đề tài

Văn bằng là một loại giấy tờ chứng nhận quá trình tốt nghiệp giữa các cấp học, trong khi chứng chỉ là một loại bằng cấp hoặc văn bằng chứng minh được cung cấp bởi cơ quan giáo dục để công nhận một trình độ học vấn nhất định, có giá trị pháp lý trong thời gian dài. Hiện nay, trong ngành giáo dục, văn bằng chứng chỉ là một khái niệm rất quen thuộc và nó được xem là yếu tố quan trọng để ứng viên có thể nắm bắt cơ hội với các công việc hấp dẫn.

Tuy nhiên, phương thức cấp phát văn bằng và chứng chỉ hiện nay chủ yếu là dưới dạng tài liệu vật lý như giấy, polymer và vẫn gặp phải nhiều khó khăn như tốn không gian lưu trữ, dễ mất mát, hư hỏng và đặc biệt là dễ bị làm giả. Việc xác minh bằng cấp và chứng chỉ cũng rất tốn thời gian. Do đó, nếu có cách xác minh bằng cấp và chứng chỉ một cách chính xác và nhanh chóng thì sẽ không còn cơ hội cho các bằng cấp và chứng chỉ giả tồn tại.

Năm 2018 chứng kiến sự ra đời của công nghệ Blockchain, với ứng dụng rộng rãi vào nhiều lĩnh vực trong đời sống. Trong việc xác minh văn bằng chứng chỉ, công nghệ này hứa hẹn mang lại sự cải thiện đáng kể cho độ tin cậy của các hệ thống và văn bằng chứng chỉ điện tử.

Với tư cách là một học viên cao học ngành Công nghệ thông tin, tôi luôn quan tâm đến việc tiếp cận và hiểu biết sâu hơn về các công nghệ mới như Blockchain và cách sử dụng chúng trong quản lý và xác minh văn bằng chứng chỉ. Vì vậy, đề tài của tôi cho luận văn tốt nghiệp Thạc sĩ là “Nghiên cứu và ứng dụng công nghệ Blockchain trong quản lý và xác minh văn bằng chứng chỉ”. Tôi tin rằng đề tài này sẽ mang lại nhiều giá trị và hữu ích cho các hệ thống giáo dục cũng như các ứng viên trong việc xác minh văn bằng chứng chỉ.

➤ **Mục đích nghiên cứu**

Mục đích của nghiên cứu này là tập trung vào hiểu rõ công nghệ Blockchain và tìm hiểu cách áp dụng nó vào quản lý và xác minh Văn bằng chứng chỉ (VBCC). Nghiên cứu sẽ bắt đầu bằng việc tìm hiểu về kiến thức cơ bản về Blockchain, bao gồm cách hoạt động cơ bản và những khái niệm quan trọng liên quan đến nó. Sau đó, chúng tôi sẽ tiến hành phân tích sâu hơn để hiểu rõ các tính chất đặc trưng của công nghệ này, những đặc điểm làm cho nó trở thành một công nghệ đột phá.

Tiếp theo, ta sẽ áp dụng kiến thức đã thu thập vào việc quản lý và xác minh Văn bằng chứng chỉ (VBCC). Tôi sẽ tìm hiểu về các yêu cầu và quy trình liên quan đến VBCC, từ quá trình cấp phát cho đến quá trình xác nhận. Cuối cùng, chúng tôi sẽ xây dựng một hệ thống sử dụng công nghệ Blockchain để quản lý VBCC, phục vụ cho đơn vị phát hành, người được cấp bằng và đơn vị xác nhận, đảm bảo tính an toàn, bảo mật và minh bạch.

➤ **Đối tượng, chủ thể và phạm vi nghiên cứu**

Đối tượng: Nghiên cứu này tập trung vào các khía cạnh quan trọng liên quan đến công nghệ Blockchain và việc quản lý, xác minh văn bằng chứng chỉ (VBCC). Đối tượng nghiên cứu bao gồm: công nghệ Blockchain, các phương pháp quản lý và xác minh VBCC, cũng như kỹ thuật lập trình sử dụng công nghệ Blockchain và kỹ thuật lập trình web để xây dựng hệ thống.

Chủ thể: bao gồm tổ chức phát hành văn bằng chứng chỉ, những người nhận văn bằng chứng chỉ và các tổ chức mong muốn xác nhận tính hợp lệ của VBCC.

Phạm vi: tập trung vào việc hiểu rõ kiến thức nền tảng về công nghệ Blockchain và cách lập trình ứng dụng web liên quan đến hệ thống quản lý và xác minh VBCC.

➤ **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

Luận văn về quá trình xây dựng một trang web quản lý mang ý nghĩa hết sức quan trọng cả trong lĩnh vực khoa học và thực tiễn :

Đầu tiên, luận văn đem lại sự hiểu biết rõ ràng về quy trình xây dựng trang web quản lý, giúp người đọc dễ dàng tìm hiểu và áp dụng kiến thức trong thực tế.

Thứ hai, luận văn này đem lại lợi ích thực tiễn bằng cách tạo điều kiện thuận lợi cho việc quản lý và xác minh VBCC trong các tình huống khác nhau, từ phía nhà trường, đơn vị phát hành VBCC đến học viên và doanh nghiệp. Nhờ trang web này, nhà trường có khả năng tạo và quản lý VBCC cho học viên dễ dàng hơn, cùng việc học viên có thể chia sẻ thông tin cá nhân và VBCC của họ cho doanh nghiệp một cách tiện lợi.

Cuối cùng, doanh nghiệp và nhà tuyển dụng cũng được hưởng lợi bằng khả năng xác minh thông tin của học viên và ứng viên một cách đơn giản và nhanh chóng thông qua trang web quản lý này. Như vậy, luận văn này mang lại cả giá trị học thuật và ứng dụng thực tiễn đối với cộng đồng trong việc quản lý và sử dụng VBCC.

CHƯƠNG 1. GIỚI THIỆU CÔNG NGHỆ BLOCKCHAIN

1.1. 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. [6] 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 bảo mật tối cao, Blockchain giúp các hệ thống chống lại sự thay đổi dữ liệu. Nó được thiết kế để đảm bảo rằng dữ liệu ghi vào mạng sẽ rất khó bị thay đổi. Mọi khiếu nại hoặc thay đổi trong hệ thống sẽ được ghi lại và kiểm tra bởi các nút khác trong mạng, đảm bảo tính bảo mật của thông tin. Đặc biệt, công nghệ Blockchain không phụ thuộc vào bên thứ ba và được sử dụng để lưu trữ, xác nhận, vận chuyển và truyền tải dữ liệu trong mạng thông qua các nút phân phối của nó. Ngay cả khi một phần của hệ thống Blockchain gặp sự cố, những máy tính và nút khác sẽ tiếp tục hoạt động để bảo vệ thông tin.

Công nghệ Blockchain có giá trị đặc biệt trong lĩnh vực kinh doanh và thay đổi cách thức, quy trình làm việc của con người. Nó được coi như một kho dữ liệu được phân tán trên khắp thế giới, cho phép lưu trữ và quản lý thông tin của tất cả mọi thứ như tước vị, hành động, thậm chí có thể là phiếu bầu một cách an toàn và bảo mật. Công nghệ này còn kết hợp 2 yếu tố là đồng thuận số đông và mã thông minh để thiết lập sự tin tưởng, không cần phải qua các bước trung gian.

Ngay khi Bitcoin được ra mắt, công nghệ Blockchain đã nhanh chóng thu hút sự quan tâm của giới công nghệ vì khả năng xử lý không chỉ các giao dịch tiền tệ mà còn các giao dịch khác như hợp đồng tài chính. Các nhà phân phối lớn nhất thế giới trong lĩnh vực tài chính đã tin rằng việc xây dựng hệ thống dựa trên Blockchain có thể giúp tạo ra hợp đồng an toàn hơn và nếu triển khai thành công, sẽ có hàng nghìn giao dịch tài chính được trao đổi trên hệ thống này mỗi năm. [5]

1.2. Nền tảng lý thuyết

Công nghệ Blockchain dựa trên hai nền tảng kỹ thuật chính là *hàm băm* và *chữ ký số* để đảm bảo tính bảo mật của hệ thống. Mỗi người dùng có một cặp khóa bao gồm khóa bí mật và khóa công khai, trong đó khóa bí mật được giữ bí mật và được sử dụng để ký kết các giao dịch. Sau đó, các giao dịch được phát đi trên toàn bộ mạng và được xác minh bằng chữ ký số trong 2 bước: ký kết và xác thực.

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

1.2.1. Hàm băm

Hàm băm là một phương thức chuyển đổi thông tin thành một chuỗi mã hóa độc nhất và bất kỳ cố gắng nào để thay đổi bất kỳ phần nào của Blockchain đều sẽ được phát hiện ngay lập tức bởi giá trị băm mới không trùng khớp với thông tin cũ trên Blockchain. Vì vậy, ngành bảo mật thông tin đã trở thành một công cụ hiệu quả cho các giao dịch mở, cực kỳ cần thiết đối với một số lĩnh vực yêu cầu bảo mật cao như thương mại điện tử hay ngân hàng.

1.2.1.1. Khái niệm hàm băm

Hàm băm là một phương pháp mã hóa dữ liệu được sử dụng trong công nghệ thông tin. Hàm này có khả năng chuyển đổi dữ liệu có kích thước tùy ý thành một giá trị băm có độ dài không đổi, thường được biết đến như “đại diện thông điệp” hoặc “đại diện bản tin”. Hàm băm là một phép toán một chiều, được giải thích là: từ giá trị băm “khó” có thể suy ra được nội dung hoặc độ dài của thông điệp ban đầu.

Các hàm băm dòng MD, bao gồm MD2, MD4 và MD5, đã được phát triển bởi Rivest với kết quả đầu ra có độ dài 128 bit. Hàm băm MD4 được giới thiệu vào năm 1990 và một năm sau đó, MD5 ra đời và mạnh mẽ hơn.

Năm 1993, Hàm SHA được công bố bởi Hồ sơ Liên bang, phức tạp hơn hàm băm MD, với kết quả đầu ra có độ dài là 160 bit. Và ngay sau đó, hàm này đã được chấp nhận làm tiêu chuẩn bởi Viện Tiêu Chuẩn và Công nghệ Quốc Gia (NIST).

1.2.1.2. Đặc tính của hàm băm

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

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

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

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

- “Khó” để suy ra nội dung của bản tin gốc từ giá trị băm của nó. [4] Nghĩa là, với một thông điệp **x** bất kỳ, ta có thể tính được giá trị băm **z = h(x)**, nhưng việc tìm **x** từ **z** (thậm chí khi biết hàm băm **h**) là rất khó.

1.2.1.3. Ứng dụng của hàm băm

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

- Đảm bảo tính toàn vẹn dữ liệu: Khi Thắng muốn gửi tài liệu **Y** cho Vi, Thắng sẽ gửi giá trị băm của **Y** cùng với thuật toán băm. Khi nhận được tài liệu **Y**, Vi áp dụng thuật toán băm để tính ra giá trị **Y** và đối chiếu với giá trị băm mà Thắng gửi. Nếu không giống nhau, **Y** đã bị thay đổi bởi một người khác.
- Tương trợ cho công nghệ chữ ký số: tạo ra đại diện cho tài liệu, giúp cho công nghệ chữ ký số có thể ký lên đại diện này thay vì ký trực tiếp lên tài liệu ban đầu có dung lượng lớn. Điều này giúp thực hiện việc ký trực tuyến nhanh hơn nhiều lần.
- Tạo ra bảng băm: Bảng băm là một cấu trúc dữ liệu phép lưu giữ và truy vấn dữ liệu nhanh chóng.

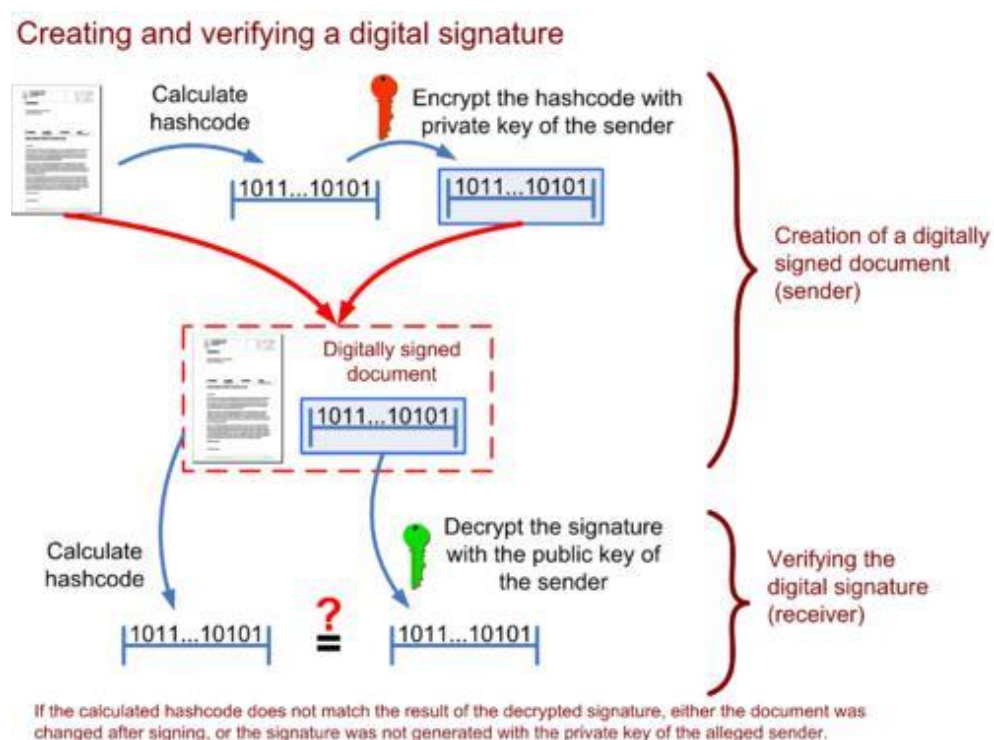
1.2.2. Chữ ký số

1.2.2.1. Khái niệm chữ ký số

Về phương diện kỹ thuật, chữ ký số là quá trình mã hóa tài liệu bằng một tài liệu khác, giúp xác minh người gửi. Để thực hiện việc ký và xác thực chữ ký, người gửi sử dụng hàm băm để chuyển đổi tài liệu ban đầu thành một bản “tóm tắt thông điệp” (Message Digest), như đã đề cập trong mục 1.2.1. Tiếp theo, người gửi mã hóa “tóm tắt thông điệp” bằng khóa bí mật của họ, sử dụng phần mềm bảo mật được cung cấp bởi cơ quan chứng thực, để tạo ra chữ ký số. Sau đó, người gửi gắn chữ ký số vào tài liệu ban đầu và gửi bản tài liệu đã ký kèm chữ ký số tương ứng đến người nhận. [1]

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

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



Hình 1.1. Mô hình thực hiện chữ ký số

1.2.2.2. Ứng dụng của chữ ký số

Chữ ký số rất quan trọng trong lĩnh vực mật mã học. Một số quốc gia trên thế giới, bao gồm Việt Nam, đã triển khai sử dụng chữ ký số. Khác với chữ ký tay thì chữ ký số cho phép cá nhân hay doanh nghiệp ký các tài liệu một cách nhanh chóng và hiệu quả hơn trong thực tế đã rất nhiều ứng dụng của chữ ký số, ví dụ như:

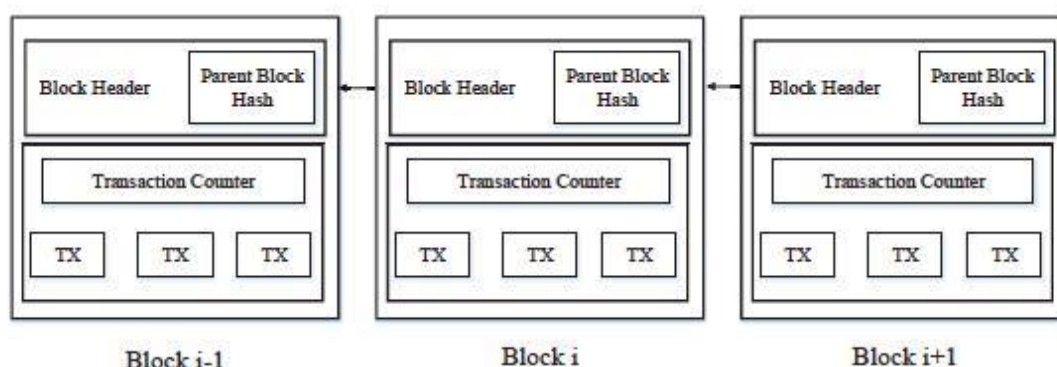
Chính phủ trực tuyến: để xuất trình giấy tờ hay ký các tài liệu, cá nhân hay doanh nghiệp không cần đến cơ quan nhà nước, mà có thể ký và gửi thông qua hệ thống máy tính. Ở Việt Nam, lĩnh vực thuế đã cho phép gửi hồ sơ khai thuế trực tuyến bằng cách sử dụng chữ ký số.

Ký kết hợp đồng trực tuyến: để ký kết hợp đồng thường đòi hỏi sự hiện diện của các bên liên quan và được chứng kiến bởi một ai đó, vì vậy sẽ gây tốn thời gian đặc biệt là khi các bên ở không gần nhau. Chữ ký số giúp giải quyết vấn đề này bằng cách cho phép các bên xác thực chữ ký của nhau thông qua các thuật toán kiểm tra chữ ký.

Trong những năm tới, chữ ký số còn có thể được ứng dụng trong nhiều lĩnh vực khác như bỏ phiếu điện tử, y tế điện tử và nhiều ứng dụng cụ thể khác.

1.3. Các kỹ thuật chính của Blockchain




Công nghệ Blockchain có sự giống nhau với một CSDL, tuy nhiên khác biệt ở cách tương tác với dữ liệu. Để hiểu sâu hơn về Blockchain, cần phải nắm rõ 3 khái niệm chính sau: cơ chế đồng thuận phi tập trung (decentralized consensus), tính toán tin cậy (trusted computing) và bằng chứng công việc (proof of work). Các khái niệm này đóng vai trò quan trọng trong việc phát triển các ứng dụng phân tán. [1]



Hình 1.2. Cấu trúc dữ liệu của Blockchain

1.3.1. Cấu trúc phi tập trung

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

 Genesis Block	
 Previous Hash	0
 Timestamp	Thu, 27 Jul 2017 02:30:00 GMT
 Data	Welcome to Blockchain CLI!
 Hash	0000018035a828da0...
 Nonce	56551

Hình 1.3. Cấu trúc của block gốc trong Blockchain

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

- Chỉ số Index: Đây là thứ tự của khối trong chuỗi (khối đầu tiên có chỉ số là 0).
- Giá trị băm (Hash): Đây là giá trị băm của khối.
- Giá trị băm trước đó (Previous Hash): Đây là giá trị băm của khối trước đó trong chuỗi.
- Thời gian (Timestamp): Đây là thời điểm mà khối được tạo ra.
- Dữ liệu (Data): Đây là thông tin được lưu trữ trong khối.
- Giá trị nonce (Nonce): Đây là giá trị biến đổi được sử dụng để tìm ra giá trị băm phù hợp với yêu cầu của mạng Blockchain.

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

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

- Index: $0+1 = 1$
- Previous Hash: 000004d195a8579...
- Timestamp: nhãn thời gian tạo ra khối mới.
- Data: Thông tin trong khối mới
- Hash: ---
- Nonce: ---

Để tạo giá trị băm đúng điều kiện trên Blockchain, cần tìm giá trị “nonce” phù hợp. Điều kiện đó là giá trị băm phải có 5 số 0 ở đầu, với số lượng số 0 này được gọi tên là “độ khó” (difficulty). Dưới đây là một đoạn mã kiểm tra giá trị băm có đáp ứng yêu cầu hay không:

```
function isValidHashDifficulty(hash, difficulty) {
  for (var i = 0, b = hash.length; i < b; i++) {
    if (hash[i] !== "0") {
      break;
    }
  }
  return i ≥ difficulty;
}
```

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

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

```
let nonce = 0;
let hash;
let input;
while (!isValidHashDifficulty(hash)) {
  nonce = nonce + 1;
  input = index + previousHash + timestamp + data + nonce;
  hash = CryptoJS.SHA256(input);
}
```

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

Mạng Blockchain lưu trữ dữ liệu trên tất cả các nút của mình, loại bỏ các rủi ro liên quan đến việc lưu trữ tập trung dữ liệu. Hệ thống không có điểm tập trung nào dễ bị tổn thương, không có điểm trung tâm gây ra sự cố. Một nút bất kỳ trong mạng ngừng hoạt động cũng không gây ảnh hưởng đến hoạt động của toàn bộ hệ thống.

1.3.2. Tính toán tin cậy

Mỗi đơn vị trong Blockchain đều giữ một bản sao của toàn bộ Blockchain. Chất lượng sao lưu phụ thuộc vào thời gian đồng bộ giữa các đơn vị. Tất cả các đơn vị trong mạng được xem là tin cậy và không có đơn vị nào được ưu tiên tin cậy hơn. Giao tiếp dữ liệu trong hệ thống không yêu cầu sự tin tưởng giữa các đơn vị. Quy chế hoạt động của toàn bộ hệ thống và các dữ liệu liên quan đều được công khai và minh bạch. Vì vậy, các đơn vị không thể giả mạo các quy định và thời gian được định nghĩa bởi hệ thống.

1.3.3. Bằng chứng công việc

Proof of work trong mạng Blockchain là một thử thách mà các nút trong mạng phải vượt qua để tạo ra các block mới. Cụ thể, các nút phải tìm ra giá trị “nonce” phù hợp để tạo ra giá trị băm thỏa mãn điều kiện trước đó. Cụ thể ở đây là số lượng số 0 ở đầu giá trị băm, còn được gọi là độ khó (difficulty) và được đặt trong mục 1.3.1.

1.4. Tính chất của Blockchain

1.4.1. Cơ chế đồng thuận phân quyền (decentralized consensus)

Cơ chế này ngược lại với mô hình đồng thuận tập trung truyền thống, trong đó một CSDL tập trung được sử dụng để quản lý việc xác thực các giao dịch. Thay vào đó, cơ chế này sử dụng một mạng phi tập trung để chuyển giao quyền lực và sự tin tưởng. Các nút trong mạng liên tục lưu trữ các giao dịch trên một khối công khai, tạo nên một chuỗi liên kết được gọi là Blockchain. Mỗi khối tiếp theo chứa một giá trị băm của khối trước đó để đảm bảo tính xác thực của giao dịch mà không cần một bên trung gian tham gia. Sự kết hợp giữa mã hóa và Blockchain đã đảm bảo rằng một giao dịch sẽ không thể bị trùng lặp hay được thực hiện hai lần.

1.4.2. Bảo trì tập thể (collective maintenance)

Hệ thống này cho phép mỗi khối dữ liệu (block) được duy trì bởi tất cả các nút có chức năng bảo trì trong toàn bộ hệ thống. Bất kỳ nút nào trong hệ thống cũng có khả năng thêm khối vào Blockchain. Điều đặc biệt là hệ thống cho phép bất kỳ ai cũng có thể tham gia và trở thành một nút trong đó.

1.4.3. Tính bảo mật và độ tin cậy

Nếu không chiếm được ít nhất 51% số nút trong mạng, dữ liệu mạng sẽ không bị kiểm soát và sửa đổi. Vì vậy, Blockchain trở nên tương đối an toàn và khó bị thay đổi dữ liệu. Nếu một số lượng lớn các nút có khả năng tính toán mạnh tham gia vào hệ thống, độ bảo mật của dữ liệu trong hệ thống sẽ tăng lên.

1.4.4. Mã nguồn mở

Công nghệ Blockchain được phát hành dưới dạng mã nguồn mở, do đó dữ liệu Blockchain có thể truy cập được bởi tất cả mọi người. Ngoài việc các thông tin cá nhân được mã hóa bởi các tổ chức kinh doanh, bất kỳ ai cũng có thể tìm kiếm dữ liệu Blockchain thông qua giao diện công khai và phát triển các ứng dụng liên quan. Tính minh bạch của toàn bộ hệ thống rất cao.

1.5. Phân loại các hệ thống Blockchain

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

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

1.6. Các ứng dụng điển hình của công nghệ Blockchain

Được xây dựng bằng một hệ thống lưu trữ phân tán với khả năng chịu lỗi cao, Blockchain đảm bảo tính bảo mật cho dữ liệu được lưu trữ bao gồm các thông tin về sự kiện, giao dịch, công chứng, danh tính và nguồn gốc. Công nghệ này có khả năng giải quyết các vấn đề liên quan đến việc thay đổi dữ liệu và thiếu tính rõ ràng và minh bạch trong môi trường thương mại quốc tế.

1.6.1. Ứng dụng Blockchain trong tiền số

Blockchain không chỉ áp dụng cho Bitcoin mà còn cho nhiều đồng tiền số khác. Công nghệ này là cốt lõi của Bitcoin và cũng đảm bảo hoạt động cho các đồng tiền số khác. Do đó, nếu một đồng tiền số không sử dụng công nghệ Blockchain, ta có thể nghi ngờ tính chính xác của nó.

1.6.2. Ứng dụng Blockchain trong hợp đồng thông minh (Smart contract)

Hợp đồng thông minh hay Smart contract là một thuật ngữ chỉ khả năng của hệ thống máy tính tự động xây dựng các điều khoản và thực hiện các thỏa thuận bằng cách sử dụng Blockchain. Hoạt động của hợp đồng thông minh hoàn toàn tự động mà không có sự can thiệp từ bên ngoài. Ví dụ: hợp đồng thuê nhà chìa khóa trao tay, phí bảo hiểm hoặc ô tô tự lái chỉ là một số cách hợp đồng thông minh sẽ kiểm soát doanh nghiệp và cuộc sống của mọi người trong tương lai.

Hợp đồng thông minh tạo điều kiện thực hiện hợp đồng hiệu quả hơn so với hợp đồng truyền thống và cắt giảm chi phí giao dịch cho người tham gia. Các điều khoản của Hợp đồng thông minh tương tự như hợp đồng pháp lý và được viết bằng ngôn ngữ lập trình, chúng không thể bị thay đổi. Mục đích chính của Hợp đồng thông minh là tạo điều kiện thuận lợi cho sự tương tác của hai bên ẩn danh qua internet mà không cần bên thứ ba.

➤ Sự khác biệt giữa truyền thống và hiện đại

Các hợp đồng truyền thống được soạn thảo bởi các chuyên gia pháp lý với khối lượng giấy tờ lớn và yêu cầu xác minh của bên thứ ba. Việc này tốn nhiều công sức và thường xuyên xảy ra các trường hợp làm giả hoặc lừa đảo. Nếu một hợp đồng có sai sót thì cách giải quyết thiết thực nhất là thông qua cơ quan tư pháp, điều này dẫn đến rất nhiều chi phí. Trong trường hợp nghiêm trọng nhất, tranh chấp có thể phát sinh.

Smart contract là một công nghệ được tạo ra bởi hệ thống máy tính sử dụng các ngôn ngữ lập trình, trong đó đã quy định rõ các điều khoản và hình phạt tương đương như hợp đồng truyền thống. Điểm khác biệt của Smart contract là nó hoàn toàn tự động và không cần sự can thiệp của con người, từ đó đảm bảo tính chính xác và công bằng. Toàn bộ mã của Smart contract được thực thi trên hệ thống sổ cái phân tán của Blockchain. Điều này giúp giảm thiểu thời gian và chi phí so với hợp đồng truyền thống, đồng thời tránh được các trường hợp lừa đảo và mâu thuẫn liên quan đến việc giải quyết tư pháp.

Vì vậy, việc sử dụng công nghệ Blockchain và Smart contract đem lại mức độ tin cậy cao trong việc thực thi và thỏa thuận. Điều này mở ra khả năng ứng dụng Smart contract trong việc thay đổi cách suy nghĩ của con người về các mối quan hệ có sự ràng buộc, đặc biệt là trong lĩnh vực kinh doanh.

1.6.3. Một số ứng dụng nổi bật khác

– Lĩnh vực Vận tải biển

Ứng dụng công nghệ Blockchain trong lĩnh vực Vận tải biển đã được Maersk, một trong những tập đoàn hàng đầu trên thế giới, hợp tác cùng Hải quan Hà Lan và Bộ An ninh Nội địa Hoa Kỳ, thử nghiệm thành công. Việc sử dụng công nghệ Blockchain đã giúp đảm bảo tính chính xác và đáng tin cậy trong việc theo dõi hàng hóa bằng cách sử dụng chữ ký điện tử, đồng thời làm cho việc gian lận và bỏ sót hàng hóa khi vận chuyển khó xảy ra hơn. Bên cạnh đó, việc sử dụng công nghệ này còn giúp giảm thiểu thời gian trung chuyển hàng hóa.

– Lĩnh vực ngân hàng

Mặc dù ngành ngân hàng có tính chất phức tạp đặc thù, nhưng hiện nay việc xác thực các giao dịch đơn giản như chuyển tiền hay bán cổ phiếu vẫn đang gặp phải vấn đề về hệ thống chậm và mất thời gian. Tuy vậy, Barclays, một công ty chuyên về dịch vụ tài chính trên toàn cầu, đã thành công trong việc thực hiện được giao dịch xuất khẩu bằng Blockchain trong năm 2016 và đã chứng minh được lợi ích của nó. Thậm chí, một số ngân hàng lớn cũng đang tích cực nghiên cứu và dự kiến áp dụng công nghệ Blockchain để thay thế hệ thống hiện tại trong các giao dịch liên ngân hàng quốc tế.

– Lĩnh vực Tạp hóa, bán lẻ

Trong lĩnh vực bán lẻ và tạp hóa, Walmart đã trở thành một trong những công ty tiên phong sử dụng công nghệ Blockchain. Từ năm 2016, họ đã áp dụng công nghệ này để theo dõi nguồn gốc của lợn nhập từ Trung Quốc đến Mỹ. Vào tháng 8, một nhóm nông dân ở Arkansas đã sử dụng mã QR trên hộp đựng gà để theo dõi các giao dịch. Những ứng dụng này giúp các nhà cung cấp giảm lượng thực phẩm hư hỏng và ngăn ngừa sự lây lan của dịch bệnh.

– Lĩnh vực Luật pháp

Sự tham gia của luật sư và tòa án hiện đang được yêu cầu để lập các bản thỏa thuận liên quan đến bán nhà và hợp đồng lao động. Tuy nhiên, một số công ty đang tiến hành

thử nghiệm giải pháp mới để giảm thiểu thủ tục phức tạp này bằng cách sử dụng hợp đồng thông minh - một ứng dụng của công nghệ Blockchain. Để đảm bảo việc giao chia khóa an toàn và thanh toán tiền của người thuê nhà, hợp đồng thông minh này sẽ được áp dụng và chỉ được thực thi khi các điều khoản không có sự trùng lặp. Hiện tại, các luật sư chưa đặc biệt quan tâm đến hợp đồng thông minh, nhưng điều này có thể thay đổi trong tương lai, đặc biệt là khi một số tiểu bang của Hoa Kỳ, chẳng hạn như Arizona, đã thông qua các quy định xác nhận tính hợp lệ của hợp đồng thông minh.

– *Lĩnh vực Quản trị nhân lực*

Trong lĩnh vực quản lý nhân sự, thành công phụ thuộc chủ yếu vào việc quản lý thông tin phải thật chính xác. Việc xác minh thông tin của nguồn nhân lực là yếu tố rất quan trọng, ảnh hưởng đến chi phí và hiệu quả của việc quản lý nguồn nhân lực. Tuy nhiên, với sự phát triển nhanh chóng của các thiết bị di động và công nghệ Internet, sai sót thông tin có thể gây rủi ro nhân lực và thiệt hại kinh tế cho các doanh nghiệp. Vì vậy, các mô hình kết hợp công nghệ mã hóa truyền thống và công nghệ Internet trên Blockchain đã được nghiên cứu và đưa ra nhằm tạo ra một hệ thống quản lý thông tin nhân sự. Điều này giúp giảm chi phí quản lý thông tin cho các doanh nghiệp.

CHƯƠNG 2. TỔNG QUAN QUẢN LÝ VÀ XÁC MINH VĂN BẰNG, CHỨNG CHỈ

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

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

2.1.1. Văn bằng, chứng chỉ là gì?

Văn bằng là giấy chứng nhận cho việc tốt nghiệp hoặc đạt được học vị, bằng cấp trong lĩnh vực giáo dục. Trong khi đó, chứng chỉ là một tài liệu được cấp bởi một bên để xác thực rằng một sự kiện nào đó đã xảy ra. [3] Trong ngành đào tạo, giáo dục, chứng chỉ có tác dụng chứng minh những vấn đề như sau:

- Người học đã hoàn thành chương trình đào tạo.
- Chứng tỏ khả năng của giáo viên.
- Một đơn vị đào tạo, giáo dục hoặc một khóa học đáp ứng những điều kiện nào đó của họ.
- Một tổ chức được cho phép ban hành VBCC.

2.1.2. Quy trình liên quan tới văn bằng, chứng chỉ

Quy trình phát hành VBCC thường bao gồm ba bước chính như sau:

Bước 1: Phát hành - quá trình này bao gồm việc lưu trữ thông tin vào VBCC. Dữ liệu sẽ được lưu trữ như sau:

- Trên CSDL tập trung của tổ chức phát hành.
- Trên VBCC được tạo ra cho người được cấp.

Bước 2: Chia sẻ - người được cấp VBCC chia sẻ với một bên thứ 3. Có ba cách chia sẻ VBCC như sau:

- Giao VBCC (hoặc một bản sao) cho bên thứ 3.
- Lưu trữ VBCC với người được ủy thác, chỉ cấp phép với một vài người được yêu cầu (ví dụ như trong trường hợp một người đã qua đời, công chứng viên chỉ được phép cho người thụ hưởng biết nội dung di chúc).
- Đăng tải VBCC lên một CSDL công cộng để cho phép bất kỳ ai cũng có thể truy cập và tra cứu.

Bước 3: Kiểm tra - bên thứ ba kiểm tra lại tính chính xác của VBCC. Dưới đây là 03 phương pháp để kiểm tra:

- Kiểm tra bằng các chức năng bảo mật được tích hợp trong VBCC, bao gồm việc xác minh tính chính xác chữ ký, của con dấu, giấy in, hay những biện pháp khác.
- Kiểm tra thông qua tổ chức phát hành, trong đó bên thứ 3 sẽ kết nối với tổ chức phát hành để xác nhận xem VBCC đã được phát hành hay chưa. Tổ chức phát hành có thể truy vấn thông tin trên CSDL tập trung và xác nhận tính bảo mật của VBCC.
- Kiểm tra dựa trên CSDL tập trung, trong đó nhà cung cấp sẽ cung cấp thông tin các VBCC đã cấp cho bên thứ 3 để bất kì ai cũng có thể truy cập dữ liệu và so sánh các bản sao chép của VBCC được cấp phát.

2.1.3. Một số mô hình quản lý và xác minh văn bằng chứng chỉ không áp dụng công nghệ Blockchain

Mặc dù, chính quyền và lĩnh vực công nghiệp đang cố gắng số hóa việc quản lý văn bằng, chủ yếu là văn bằng cao đẳng và đại học, trên toàn thế giới, tuy nhiên, phần lớn văn bằng vẫn được cấp trên VBCC giấy hoặc các chứng từ vật lý khác. Tại nhiều nước, việc sử dụng văn bằng được kết hợp giữa văn bằng trên giấy và một CSDL của một bên thứ 3 chuyên về truy vấn dữ liệu (như hedd.ac.uk). Tuy vậy, hệ thống hiện tại đã cho thấy giới hạn và có nhu cầu cần một công nghệ quản lý và xác thực văn bằng hiệu quả hơn và đáng tin cậy hơn.

2.1.3.1. Văn bằng chứng chỉ giấy

➤ Ưu điểm:

- Người nhận thường giữ VBCC, vì vậy họ có đầy đủ quyền kiểm soát và sử dụng VBCC một cách dễ dàng.
- Việc giữ VBCC an toàn tương đối đơn giản và tiện lợi.
- Người được cấp phát VBCC có thể sử dụng nó tại bất kỳ địa điểm nào mà họ mong muốn.

➤ **Nhược điểm:**

- VBCC được tích hợp với tính năng bảo mật khó khăn, điều này tạo ra nhiều khó khăn trong việc sản xuất và xác thực VBCC.
- VBCC có thể bị làm giả, do đó, người cấp phát cần giữ sổ cái để lưu giữ dữ liệu về VBCC đã cấp để thực hiện xác minh.
- Sổ cái lưu giữ dữ liệu về VBCC là một điểm yếu, nếu bị thất lạc, thông tin sẽ không thể xác minh được.
- Để xác minh cần phải đọc và kiểm tra thủ công, dẫn đến tốn nhân lực và thời gian. Cả người được cấp và bên thứ 3.
- Chi phí sản xuất VBCC và công nghệ sản xuất càng tinh xảo, khó làm giả thì càng đắt đỏ.
- Để huỷ bỏ VBCC đã cấp cần được sự chấp thuận của người được cấp.

2.1.3.2. *Văn bằng chứng chỉ số (không sử dụng công nghệ Blockchain)*

➤ **Ưu điểm:**

Có những ưu điểm của VBCC số so với VBCC giấy như sau:

- Việc phát hành, duy trì và sử dụng VBCC số cần ít nguồn lực hơn do VBCC số có thể được kiểm tra tính xác thực một cách tự động mà không cần sự can thiệp thủ công. Khi sử dụng, nó có thể tự động đối chiếu, xác minh và tóm tắt nếu được phát hành theo một chuẩn định dạng cụ thể, đồng thời đảm bảo tính bảo mật cao hơn do sử dụng các giao thức mật mã.
- Người phát hành có quyền thu hồi VBCC số.

➤ **Nhược điểm:**

- Nếu không áp dụng chữ ký số, việc giả mạo VBCC số là rất dễ dàng.
- Nếu áp dụng chữ ký số, việc xác thực cần sự can thiệp của bên thứ 3 để chắc chắn về tính toàn vẹn của giao dịch, dẫn đến khả năng bị lợi dụng bởi các bên thứ 3 có thể xem được mọi khía cạnh của quy trình xác thực.
- Ở nhiều nước việc xác thực chữ ký số chỉ có thể được thực hiện trong một hệ sinh thái cụ thể do chưa có một tiêu chuẩn nào về vấn đề này.
- Các bản ghi điện tử dễ dàng bị phá hủy, do đó cần có biện pháp chống lỗi và đảm bảo an toàn dữ liệu.

- Nếu nơi lưu giữ bị lỗi, VBCC sẽ bị mất giá trị vì không có cách nào để xác minh được thông tin.
- Có khả năng bị tấn công vào tổ chức đăng ký và lưu trữ VBCC, khiến dữ liệu bị rò rỉ ở quy mô lớn.

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

Blockchain là một cơ sở hạ tầng mới để bảo vệ, chia sẻ và xác thực thông tin trong giáo dục. Khi sử dụng Blockchain để quản lý và xác minh VBCC, thông tin của bên cung cấp và bên nhận VBCC cùng với giá trị băm của chúng sẽ được lưu trữ trong một CSDL công khai trên hàng ngàn máy tính trên toàn thế giới. VBCC được bảo vệ trên Blockchain mang lại nhiều lợi ích hơn so với việc sử dụng VBCC thông thường, gồm:

- Không thể giả mạo: khi phát hành VBCC, chỉ những người được nhất định trong VBCC được nhận và điều này có thể được xác minh một cách chắc chắn.
- Bất cứ ai cũng có thể xác thực được VBCC bằng cách kiểm tra trên Blockchain mà không cần sự can thiệp của bên thứ 3.
- Ngay cả khi tổ chức phát hành đã không còn tồn tại, VBCC vẫn có thể được xác minh mà không cần bên thứ ba tham gia vào quá trình này.
- Dữ liệu về VBCC chỉ bị thất lạc khi Blockchain trên toàn cầu bị sập, tuy nhiên, hệ thống là hệ thống được phân tán và rất khó bị tấn công hoàn toàn.
- Áp dụng hàm băm để liên kết tới nút gốc và được lưu giữ trên hệ thống Blockchain, do đó người dùng vẫn giữ được VBCC gốc và bảo vệ tính bảo mật của tài liệu.

2.1.4.1. Người nhận văn bằng, chứng chỉ (Holder)

Blockchain giúp khắc phục một vài trở ngại liên quan đến người sở hữu VBCC:

- Tính độc lập: Người sở hữu VBCC không phải thông qua tổ chức phát hành hoặc bất kỳ bên thứ 3 nào để xác nhận chứng chỉ của mình khi đã nhận được.
- Tính sở hữu: Người sở hữu có thể xác minh rằng VBCC là tài sản của mình, không thuộc về ai khác.
- Kiểm soát: để chia sẻ VBCC, người sở hữu có thể thêm 1 đường link của VBCC trên bản CV của mình.
- Khả năng xác minh: VBCC có thể được xác minh bởi bên thứ 3, ví dụ: doanh nghiệp, nhà trường hoặc các đơn vị xác thực khác.

2.1.4.2. Đơn vị phát hành (Issuer)

Blockchain đã khắc phục một số vấn đề của tổ chức phát hành VBCC như sau:

- Giúp xác định VBCC được phát hành bởi đơn vị nào.
- Cho phép đơn vị phát hành thiết lập thời hạn cho VBCC.
- Có khả năng thu hồi VBCC từ người sở hữu bởi đơn vị phát hành.
- Đảm bảo an toàn và bảo mật cho hệ thống quản lý và xác minh VBCC.

2.1.4.3. Đơn vị cần xác minh (Verifier)

Công nghệ Blockchain đã khắc phục một số vấn đề đối với đơn vị xác minh sau:

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

2.2. Tình hình và các nghiên cứu liên quan

Một số startup, công trình nghiên cứu liên quan tới việc triển khai quản lý và xác minh VBCC áp dụng công nghệ Blockchain.

2.2.1. Blockcerts

2.2.1.1. Giới thiệu

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, trong thời điểm tiền mã hóa đang bùng nổ. Dự án này là một trong những dự án đầu tiên nghiên cứu toàn diện về việc quản lý VBCC trên Blockchain. Mục đích là tạo nên một tiêu chuẩn mở để quản lý và xác thực thông tin VBCC số trong ngành giáo dục. Sau gần 3 năm, dự án đã được cập nhật lên phiên bản 2.0, với một số thay đổi so với phiên bản 1.0, bao gồm:

- Không cấp VBCC cá nhân nữa mà cấp phát VBCC theo lô nên số lượng giao dịch Bitcoin ít đi, sẽ tiết kiệm chi phí hơn.
- Việc thu hồi VBCC dễ dàng hơn nhờ chuẩn Open Badges v2.0, áp dụng “HTTP URI revocation list” chứ không gửi giao dịch Bitcoin vào địa chỉ của người được cấp phát.

Dự án Blockcerts đã tập trung vào việc giải quyết các vấn đề trong việc quản lý VBCC trong đào tạo, bao gồm ba 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 để 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. [1]

2.2.1.2. Điểm mạnh của dự án

Dự án có những ưu điểm so với việc quản lý VBCC bình thường mà không sử dụng công nghệ Blockchain bao gồm:

- Việc sử dụng toán băm (tạo cây Merkle để lưu trữ VBCC trên Blockchain) giúp VBCC không bị giả mạo. Các thay đổi trong thông tin của VBCC sẽ gây ra sự sai lệch trong giá trị băm, từ đó giúp phát hiện và ngăn chặn VBCC giả mạo.
- Có thể sử dụng các công cụ hỗ trợ như wallet-android, cert-verifier, cert-verifier-js, wallet-ios để xác minh tính hợp lệ của VBCC, hoặc tự phát triển các ứng dụng để kiểm tra VBCC.
- VBCC vẫn có thể được xác minh ngay cả khi đơn vị phát hành không còn hoạt động nữa.
- Người nhận VBCC có thể kiểm soát, chia sẻ và xem thông tin của mình mà không cần phải phụ thuộc vào bên thứ 3.
- Đơn vị phát hành có thể chứng minh được VBCC đã phát hành, thu hồi VBCC, đặt thời gian hết hạn và đảm bảo an toàn cho VBCC mà không cần phụ thuộc vào hạ tầng sao lưu.
- Dự án đã được triển khai trên hai nền tảng Blockchain phổ biến nhất hiện nay là Bitcoin và Ethereum.

2.2.1.3. Một số hạn chế

Mặc dù đã được phát triển được khá lâu, dự án vẫn còn một số giới hạn như sau:

- Quy trình phát hành VBCC phụ thuộc vào một cá nhân giữ khóa bí mật của đơn vị đào tạo, gây nguy cơ tham nhũng.
- Danh sách VBCC thu hồi đang dựa trên “HTTP URI revocation list” có thể gây ra vấn đề về bảo mật, do kẻ tấn công có thể tấn công vào máy chủ chứa danh sách để thay đổi, thêm mới hoặc xóa thông tin về VBCC trong danh sách, gây ra một điểm yếu cho hệ thống. [1]
- Việc xác định tổ chức phát hành đang dựa trên giao thức HTTP, tạo ra một nút thắt cổ chai giống như việc quản lý VBCC thu hồi, kẻ tấn công có thể tận dụng điểm yếu này. [1]

Để khắc phục các hạn chế trên, nhóm nghiên cứu của trường Đại học Birmingham, Vương quốc Anh đã phát triển dự án BTCert, sử dụng nền tảng Blockcerts, nhằm giải quyết vấn đề này. Chi tiết xem tại phần 2.2.2.

2.2.2. BTCert

2.2.2.1. Giới thiệu

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>

BTCert được bắt đầu phát triển từ cuối năm 2017 và được lập trình bằng ngôn ngữ Java thay vì Python như trong Blockcerts.

2.2.2.2. Điểm mạnh của dự án

BTCert là một dự án được phát triển dựa trên mô hình của Blockcerts và vì thế nó cũng kế thừa tất cả các ưu điểm của Blockcerts. Ngoài ra, BTCert còn giải quyết những vấn đề mà Blockcerts chưa giải quyết được, bao gồm:

- Tạo ra một quy trình cấp VBCC theo nhiều cấp độ: sử dụng multisign trên Blockchain. Ví dụ, cần có N người ký và cần tối thiểu M người cần ký giao dịch thì VBCC mới được cấp phát.
- Để thu hồi VBCC, hệ thống sử dụng trạng thái giao dịch của VBCC trên Blockchain thay vì quản lý danh sách thu hồi dựa trên “HTTP URI revocation list”. Cụ thể, hệ thống sẽ tạo ra một loạt địa chỉ của nhà cung cấp được sử dụng để thu hồi và gắn địa chỉ này vào VBCC khi phát hành cho người nhận. Khi muốn thu hồi, đơn vị phát hành chỉ cần sử dụng địa chỉ thu hồi để thực hiện một giao dịch gửi Bitcoin tới địa chỉ của người nhận. Việc xác minh sẽ được thực hiện bởi ứng dụng, nếu có giao dịch từ địa chỉ thu hồi của đơn vị phát hành thì VBCC đã bị thu hồi.

2.2.2.3. Một số hạn chế

BTCert đã kế thừa và giải quyết nhiều vấn đề của Blockcerts, tuy nhiên, vẫn còn một số giới hạn nhất định, bao gồm:

- BTCert chỉ hỗ trợ trên nền tảng Blockchain của Bitcoin.
- Việc xác định nhà cung cấp vẫn phụ thuộc vào một liên kết HTTP trên Internet và dễ bị tấn công. [1]

CHƯƠNG 3. 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**.

3.1. Thiết kế hệ thống CertsChain

3.1.1. Định nghĩa bài toán

Hiện nay, các tổ chức đào tạo (Issuer) tại Việt Nam thường thực hiện các bước quản lý chứng chỉ như sau: [2]

- 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 được cấp VBCC (Holder) muốn sử dụng VBCC cần phải đem VBCC gốc đến một cơ quan công chứng nếu muốn chia sẻ thông tin về chứng chỉ với một bên thứ 3 hay đơn vị cần xác minh.

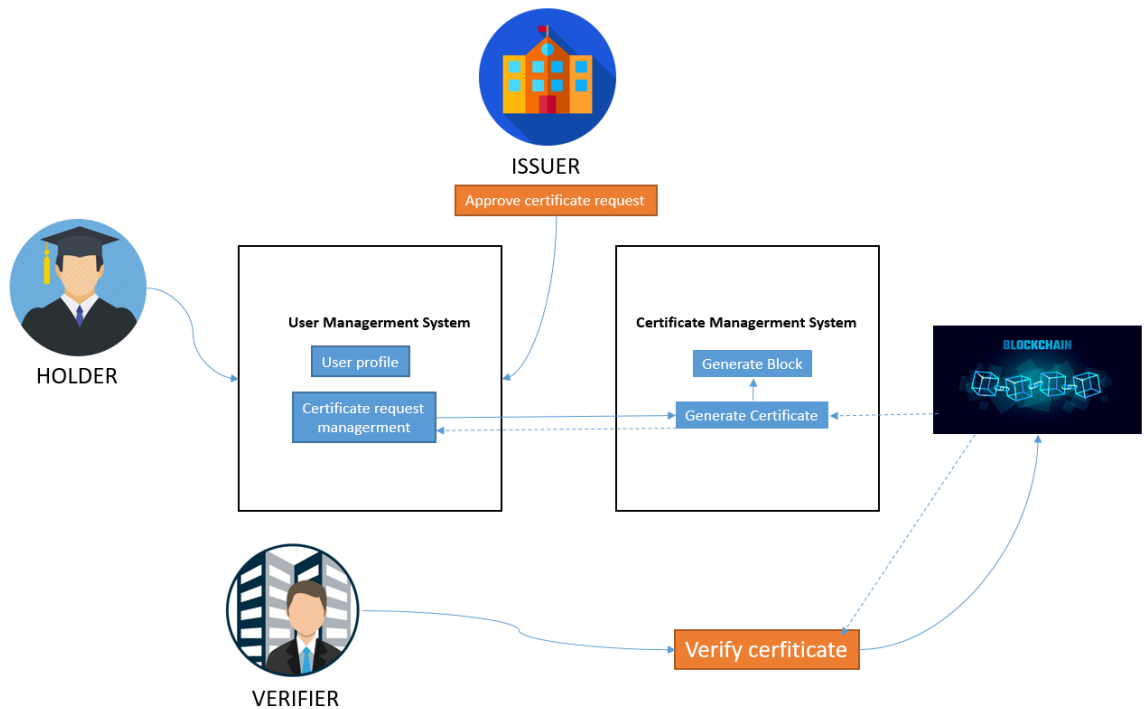
Để xác minh tính đúng đắn của VBCC, đơn vị cần xác minh (Verifier) cần phải liên hệ với đơn vị phát hành, tuy nhiên việc này mất nhiều thời gian và tiền bạc.

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.

3.1.2. Mô hình thực hiện

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



Hình 3.1. 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.

3.1.3. 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.

3.1.3.1. 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 3.1. Các chức năng của Issuer

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

➤ Chi tiết chức năng

1. Quản lý thông tin cá nhân:

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

Có thể chỉnh sửa thông tin cá nhân:

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

2. 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 mới, chỉnh sửa, cập nhật trạng thái người dùng.

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

3. Quản lý Trường học và Khóa học:

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

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

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

4. 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.

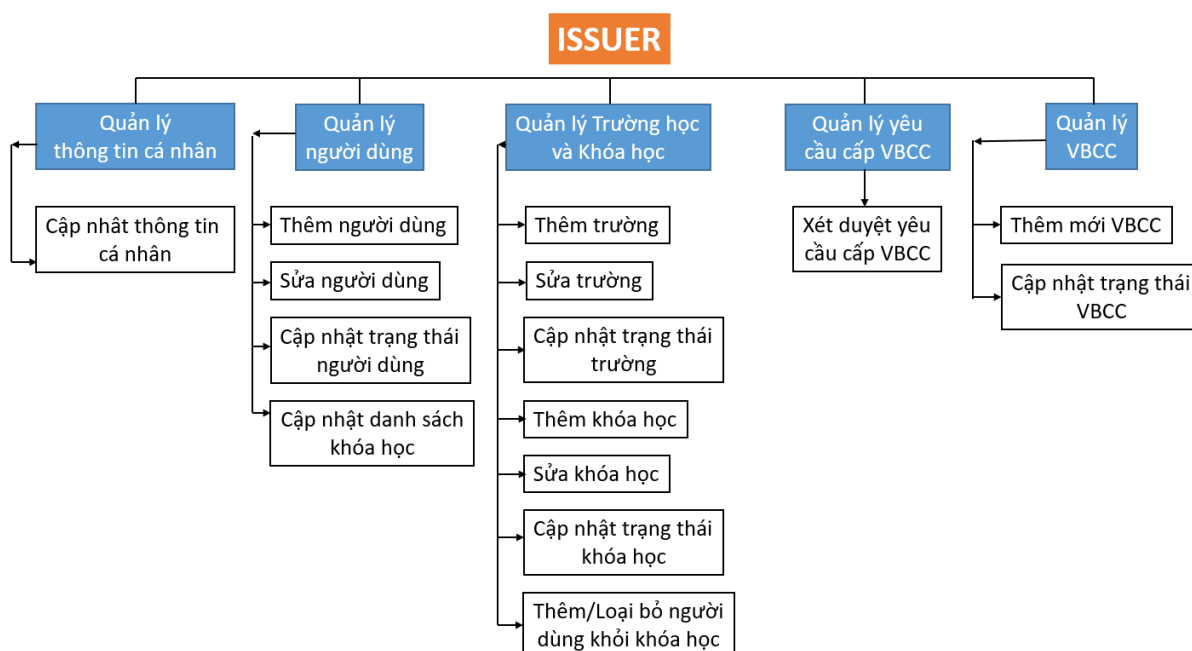
- Đầu vào: Thông tin yêu cầu: người dùng, Trường học và Khóa học.
- Xử lý: Khi Issuer chọn xác nhận, VBCC sẽ được tạo ra, cập nhật vào database và 1 Block mới sẽ được thêm vào chain.
- Đầu ra: Danh sách yêu cầu.

5. 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 mới vào chain.
- Đầu ra: Danh sách VBCC.

➤ Sơ đồ phân rã chức năng Issuer



Hình 3.2. Sơ đồ phân rã chức năng Issuer

3.1.3.2. 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 3.2. 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	Xem danh sách, tạo mới, chỉnh sửa các yêu cầu cấp phát VBCC của mình.

➤ 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:

- Đầu vào: Holder mở trang danh sách VBCC của mình.
- Xử lý: Lấy danh danh sách VBCC của Holder hiện tại, khi 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.

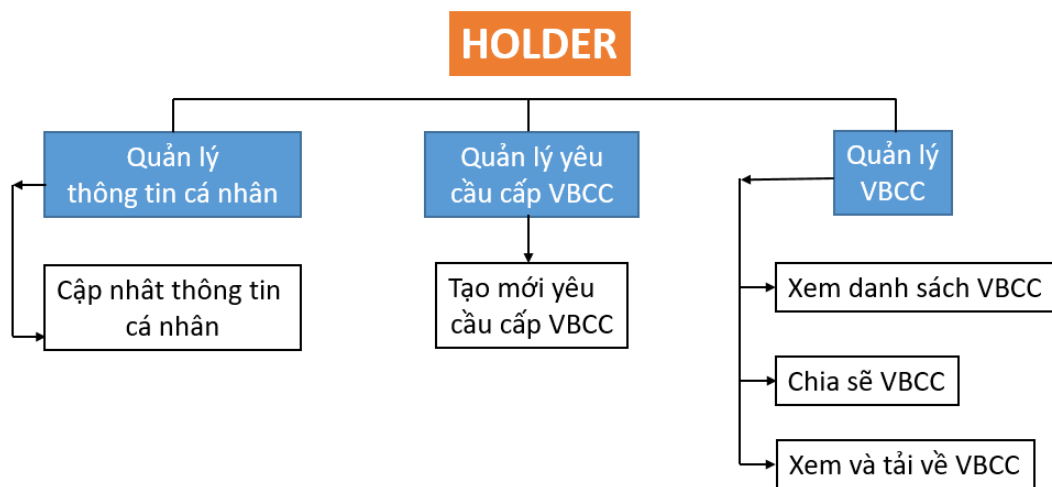
3. Quản lý yêu cầu cấp VBCC

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 cấp phát VBCC: Trường học và Khóa học.
- Xử lý: Khi Holder nhập đầy đủ thông tin yêu cầu và nhấn tạo mới, một dòng dữ liệu sẽ được thêm vào database.
- Đầu ra: Danh sách yêu cầu cấp VBCC.

➤ Sơ đồ phân rã chức năng Issuer



Hình 3.3. Sơ đồ phân rã chức năng Holder

3.1.3.3. 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 3.3. Các chức năng của 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.

➤ Chi tiết chức năng

1. Xem thông tin User:

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

2. Xem thông tin VBCC:

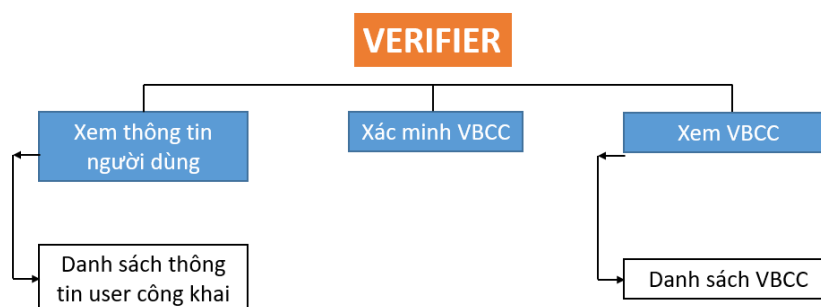
Người dùng có thể xem thông tin công khai của các user trong hệ thống.

3. Xác minh VBCC

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

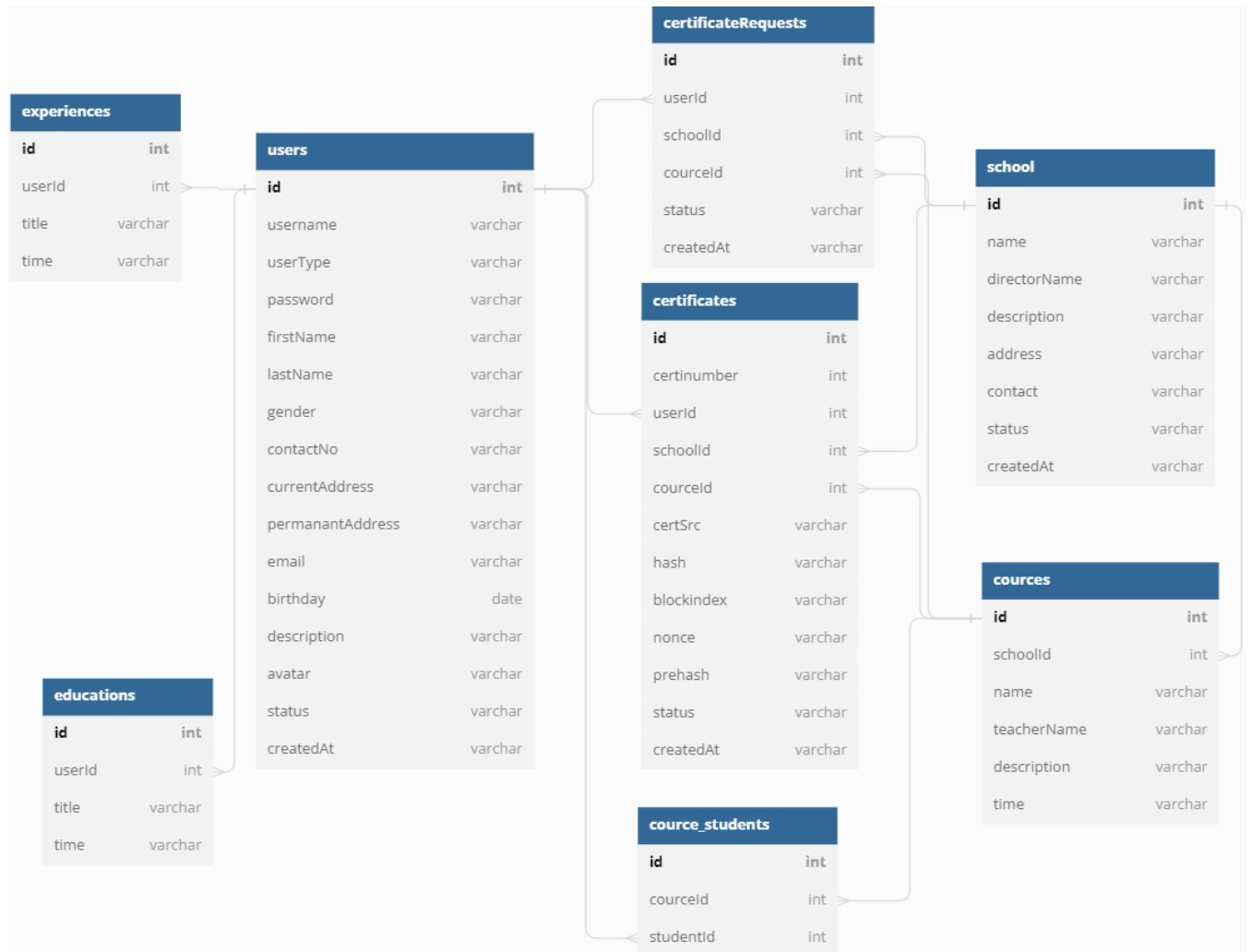
- Đầu vào: Thông tin của VBCC bao gồm: Mã số VBCC, file PDF.
- Xử lý: Khi nhập đầy đủ thông tin cho việc xác minh và nhấn xác minh, hệ thống sẽ lấy ra VBCC tương ứng với mã số được nhập và so sánh với file PDF.
- Đầu ra: Kết quả xác minh VBCC.

➤ Sơ đồ phân rã chức năng Issuer



Hình 3.4. Sơ đồ phân rã chức năng Verifier

3.1.4. Cơ sở dữ liệu



Hình 3.5. Cơ sở dữ liệu của hệ thống CertsChain

3.2. Xây dựng hệ thống CertsChain

3.2.1. Môi trường triển khai và công cụ phát triển

3.2.1.1. 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,...

3.2.1.2. 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 3.6. 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 3.7. 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.

3.2.2. 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 – sử dụng hàm băm SHA256 để băm dữ liệu.
- 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.

3.2.3. Xây dựng hệ thống API

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

Bảng 3.4. Các API của hệ thống CertsChain

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.

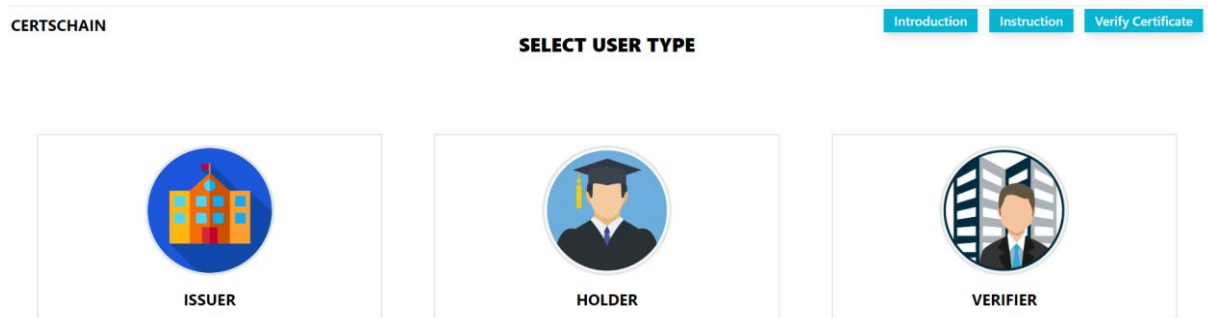
3.3. Thực nghiệm hệ thống CertsChain

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

– Trang chủ:

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

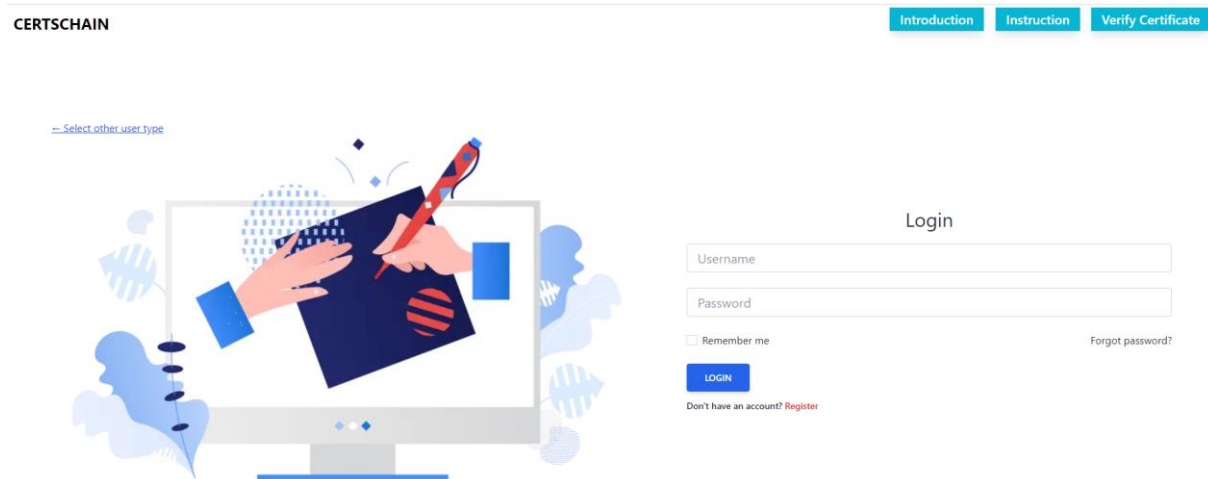
Hay User muốn xác minh VBCC có thể click vào button *Verify Certificate*.



Hình 3.8. 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 3.9. Trang đăng nhập

3.3.1. Người dùng loại Issuer

3.3.1.1. 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 3.10. Trang Profile của Issuer

3.3.1.2. Trang Users

Giúp Issuer có thể quản lý User trong hệ thống:

Hình 3.11. 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.

Add User x

Username	Username
Password	Password
First Name	First Name
Last Name	Last Name
Gender	<input type="radio"/> Male <input type="radio"/> Female
Contact No.	Contact No.
Current Address	Current Address
Permanent Address	Permanent Address
Email	Email
Birthday	dd/mm/yyyy 📅
Status	<input type="radio"/> Active <input type="radio"/> Archived

CLOSE SAVE CHANGES

Hình 3.12. Popup tạo mới User

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

Edit User x

Username	pahebumi
Password	Password
First Name	Damian
Last Name	Long
Gender	<input type="radio"/> Male <input checked="" type="radio"/> Female
Contact No.	Consequat Eaque vol
Current Address	Dicta nihil sed odit
Permanent Address	Reprehenderit cum si
Email	havuwiz@mailinator.com
Birthday	17/09/1992 📅
Status	<input checked="" type="radio"/> Active <input type="radio"/> Archived

CLOSE SAVE CHANGES

Hình 3.13. Popup cập nhật User

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

Update User Courses

User: Cao (cvthang)

School and Course #1

School

Đại học Nha Trang

Remove

Courses

Thạc sĩ Công nghệ Thông tin X Thạc sĩ Quản trị kinh doanh X

School and Course #2

School

Đại học Khánh Hòa

Remove

Courses

Du lịch X

Add School and Courses

CLOSE

SAVE CHANGES

Hình 3.14. Popup Cập nhật danh sách danh sách Courses của User tham gia

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

41

3.3.1.3. Trang Schools and Courses

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

CERTSCHAIN
-- Select other user type

ISSUER
Introduction Instruction Verify Certificate
Hello, cvthang! Logout

List Schools

Add School Search...

Name	Director Name	Description	Courses	Created At	Status	Actions
Đại học Khánh Hòa	TS. Phan Phiến	1. Sứ mạng Trường Đại học Khánh Hòa là trường đại học công lập, tự chủ, định hướng ứng dụng: đào tạo nguồn nhân lực chất lượng cao đa lĩnh vực, nghiên cứu khoa học và cung cấp các dịch vụ phục vụ cộng đồng, góp phần phát triển kinh tế - xã hội và hội nhập quốc tế. 2. Tầm nhìn Đến năm 2035, Trường Đại học Khánh Hòa đạt chuẩn quốc gia và khu vực, hướng tới trở thành trường đại học "Thông minh và Xanh". 3. Giá trị cốt lõi: Chuyên nghiệp - Sáng tạo - Kết nối - Nhân văn.	Du lịch - 2018-2022	30/10/2022 - 09:34:37	Active	Edit
Đại học Nha Trang	PGS.TS Trang Sĩ Trung	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	Thạc sĩ Công nghệ Thông tin - 2020 - 2022 Thạc sĩ Quản trị kinh doanh - 2020 - 2022	14/08/2022 - 09:19:20	Active	Edit

Hình 3.15. Trang Schools and Courses của Issuer

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

ISSUER
Hello, cvthang!

Add School

Name: Name...

Director Name: Director Name...

Description: Description...

Address: Address...

Contact: Contact...

Courses

Name	Teacher Name
Name...	Teacher Name...

Description: Description...

Time: Time...

Remove

Students: [Dropdown]

Add Course

Status: ☐ Active ☐ Archived

CLOSE SAVE CHANGES

Hình 3.16. Popup tạo mới School and Course

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

Edit School

Name: Đại học Nha Trang

Director Name: PGS.TS Trang Sĩ Trung

Description: 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

Address: 2 Nguyễn Đình Chiểu, Vĩnh Thọ, Nha Trang, Khánh Hòa 650000

Contact: 0258 3831 149

Course #1

Name: Thạc sĩ Công nghệ Thông tin

Teacher Name: TS. Phạm Thị Thu Thủy

Description: Tiền thân của Khoa Công nghệ Thông tin

Time: 2020 - 2022

Remove

Students: Alea Rhodes, Damian Long, Elliott Mayer, Kenneth Chapman, Cao Thắng, Ignatius Finch, Lilah Alexander, Ima Tucker, User Test

Course #2

Name: Thạc sĩ Quản trị kinh doanh

Teacher Name: PGS.TS Hồ Huy Tựu

Description: Năm 100% Khoa Kinh tế chính thức mở chuyên

Time

CLOSE SAVE CHANGES

Hình 3.17. Popup cập nhật School and Course

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 Courses.

3.3.1.4. Trang Certificates

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

CERTSCHAIN

— Select other user type

ISSUER

Introduction Instruction Verify Certificate

Hello, cvthang! Logout

List Certs

Add Cert Search...

School Course

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

Certificate Requests

Users Management

Schools and Courses

Certificates Management

Profile

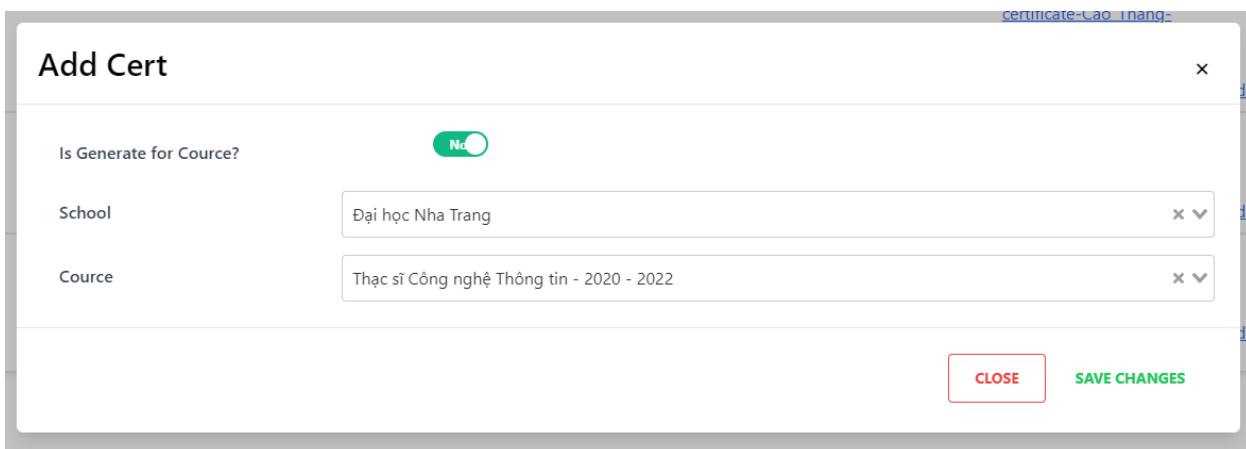
Hình 3.18. Trang Certificates của Issuer

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



Hình 3.19. 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*.



Hình 3.20. Cấp phát VBCC cho học viên trong khóa học

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

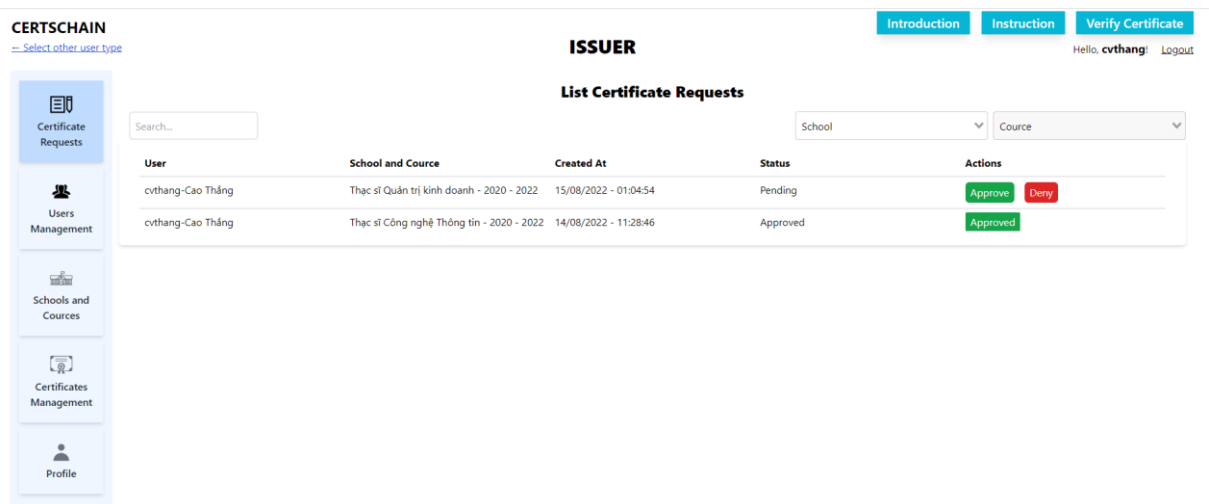


Hình 3.21. Mẫu văn bằng chứng chỉ của CertsChain

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

3.3.1.5. Trang Certificate Requests

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



Hình 3.22. Trang Certificate Requests của Issuer

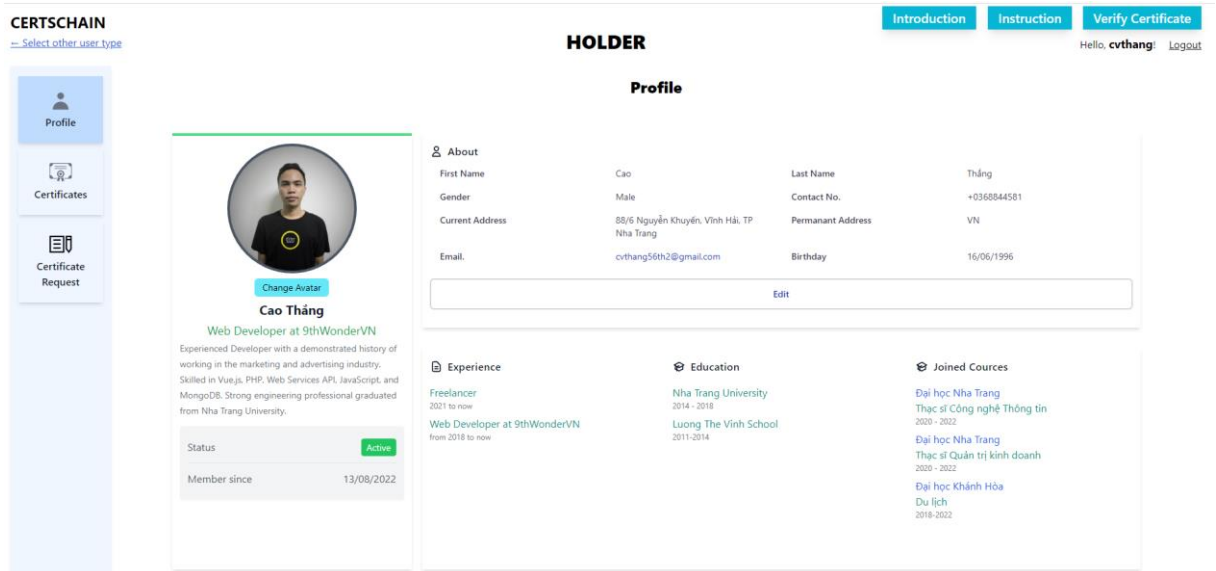
Sau khi xét duyệt yêu cầu cấp phát VBCC, Issuer sẽ click vào button *Approve* nếu chấp thuận, *Deny* nếu từ chối yêu cầu cấp phát.

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

3.3.2. Người dùng loại Holder

3.3.2.1. Trang Profile

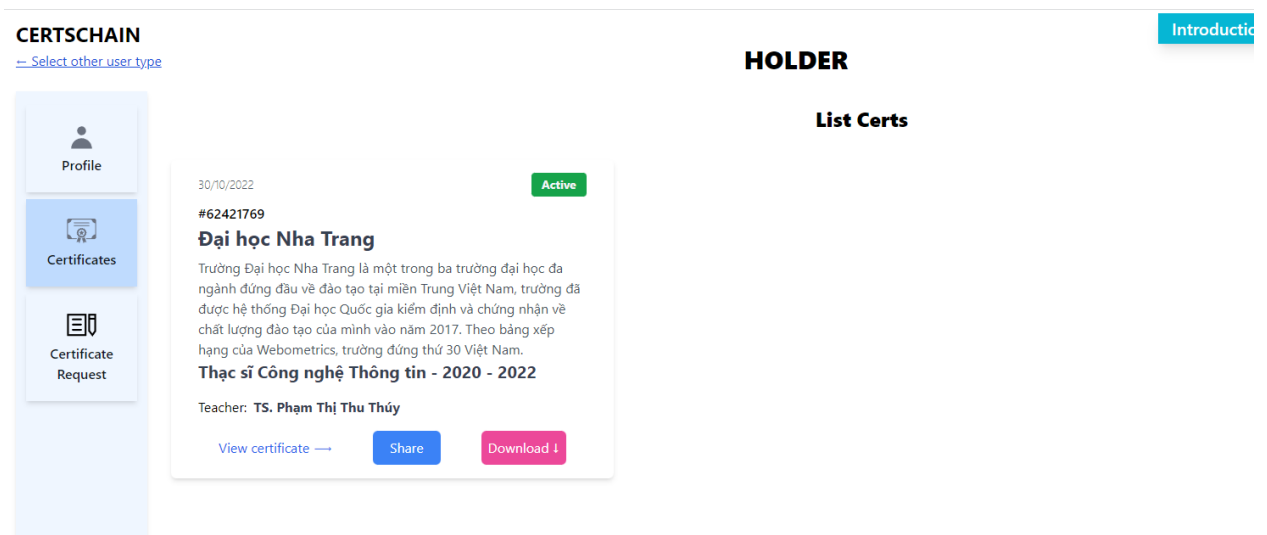
Đây là trang thông tin cá nhân của Holder, có thể thực hiện chỉnh sửa các thông tin cá nhân của mình tại trang này bằng cách click vào button *Edit*.



Hình 3.23. Trang Profile của Holder

3.3.2.2. Trang Certificates

Hiển thị danh sách các VBCC của Holder:

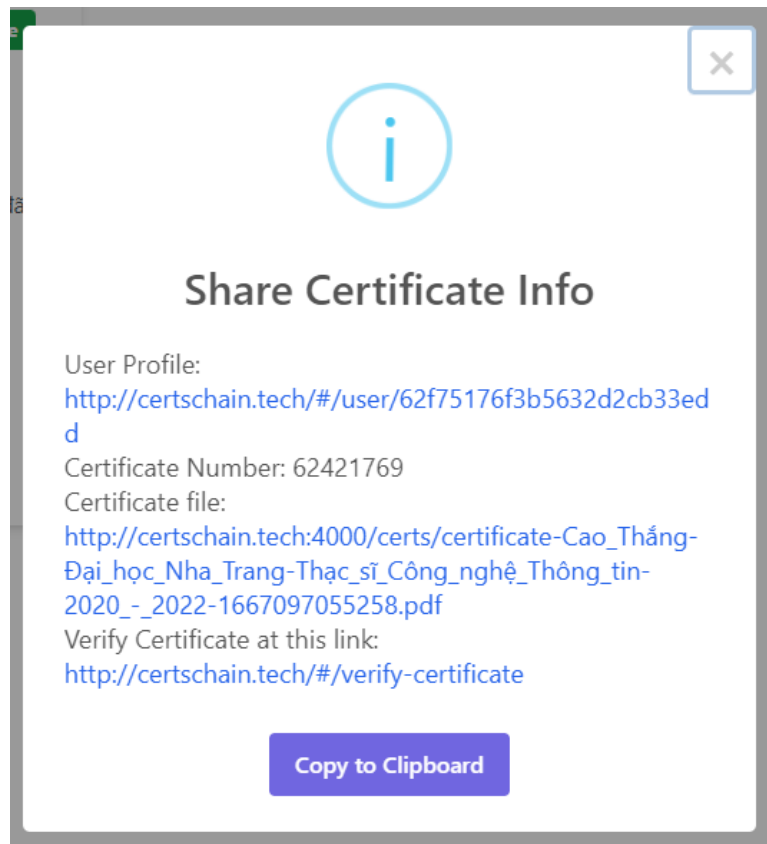


Hình 3.24. Trang danh sách Certificate của Holder

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 từng VBCC, thông tin chia sẻ của VBCC sẽ được hiển thị lên trong dialog như dưới:



Hình 3.25. Popup chia sẻ thông tin Certificate

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

3.3.2.3. Trang Certificate Requests

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

CERTSCHAIN
-- Select other user type

HOLDER

Introduction Instruction Verify Certificate
Hello, cvthang Logout

List Certificate Requests

New Certificate Request Search...

School Course

User	School and Course	Created At	Status
cvthang-Cao Thắng	Thạc sĩ Quản trị kinh doanh - 2020 - 2022	15/08/2022 - 01:04:54	Pending
cvthang-Cao Thắng	Thạc sĩ Công nghệ Thông tin - 2020 - 2022	14/08/2022 - 11:28:46	Approved

Hình 3.26. 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.

New Certificate Request ×

School Đại học Nha Trang × ▾

Course Thạc sĩ Quản trị kinh doanh - 2020 - 2022 × ▾

CLOSE SAVE CHANGES

Hình 3.27. Popup tạo mới yêu cầu cấp phát VBCC

3.3.3. Người dùng loại Verifier

3.3.3.1. Trang Users

Hiển thị ra tất cả các Users có trong hệ thống:

CERTSCHAIN

[-- Select other user type](#)

Users

Certificates

VERIFIER

IntroductionInstructionVerify Certificate

List Users

Search...

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	niroja@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 Thắng	cvthang56th2@gmail.com	13/08/2022 - 02:23:34	Active	View Detail
favyhitit	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

Hình 3.28. Danh sách tất cả các User trong hệ thống


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

CERTSCHAIN

[-- Back to Verifier Page](#)

Profile

IntroductionInstructionVerify Certificate



Cao Thắng
Web Developer at 9thWonderVN
Experienced Developer with a demonstrated history of working in the marketing and advertising industry. Skilled in Vue.js, PHP, Web Services API, JavaScript, and MongoDB. Strong engineering professional graduated from Nha Trang University.

Status

Active

Member since

13/08/2022

About

First Name	Cao	Last Name	Thắng
Gender	Male	Contact No.	+0368844581
Current Address	85/6 Nguyễn Khuyến, Vĩnh Hải, TP Nha Trang		
Permanant Address	VN		
Email	cvthang56th2@gmail.com	Birthday	16/06/1996

Experience

Freelancer

2021 to now

Web Developer at 9thWonderVN

from 2018 to now

Education

Nha Trang University

2014 - 2018

Luong The Vinh School

2011-2014

Joined Courses

Đại học Nha Trang

Thạc sĩ Công nghệ Thông tin

2020 - 2022

Đại học Nha Trang

Thạc sĩ Quản trị kinh doanh

2020 - 2022

Đại học Khánh Hòa

Du lịch

2018-2022

Hình 3.29. Trang chi tiết User

3.3.3.2. Trang Certificates

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

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

Hình 3.30. Danh sách tất cả các certificate trong hệ thống

3.3.4. Trang Verify Certificate

Trang này dùng để User có thể xác minh VBCC:

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

CERTSCHAIN
[Back to Verifier Page](#)

Verify Certificate

Introduction

Certificate Number:

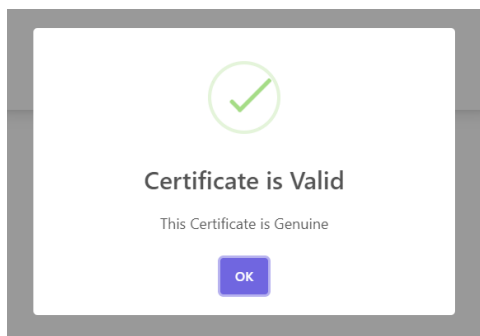
Certificate PDF File: No file chosen

Hình 3.31. 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***

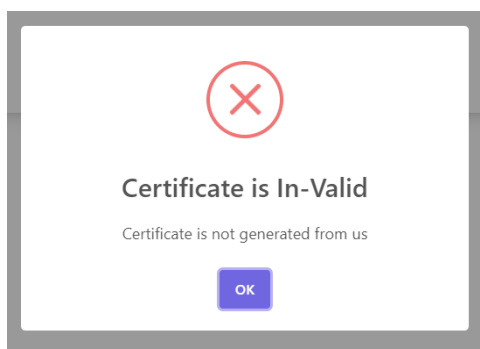
Hệ thống sẽ thông báo như sau:



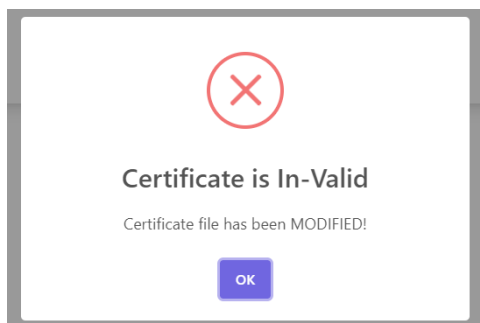
➤ ***Nếu VBCC không hợp lệ***

Hệ thống sẽ hiển thị một số lỗi như sau:

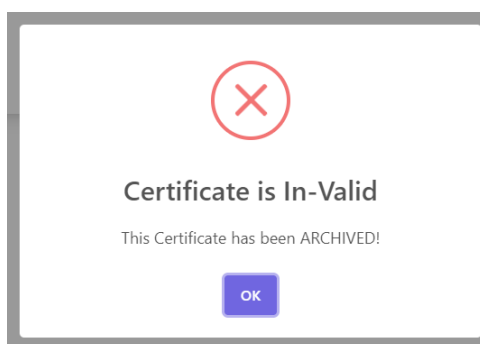
- VBCC không được cấp phát bởi hệ thống.



- VBCC đã bị sửa chữa.



- VBCC không còn hiệu lực.



CHƯƠNG 4. KẾT LUẬN VÀ KIẾN NGHỊ

4.1. Kết quả đạt được

Sau thời gian nghiên cứu và thực hiện đề tài, tôi đã đạt được các kết quả quan trọng như sau:

Hiểu rõ về Blockchain: nắm vững khái niệm, tính chất đặc trưng và cách hoạt động của Blockchain, các kỹ thuật quan trọng của công nghệ này.

Nghiên cứu về quản lý và xác minh VBCC: đã thực hiện nghiên cứu về quá trình quản lý và xác minh VBCC, đồng thời hiểu rõ ưu điểm và nhược điểm của các mô hình quản lý VBCC khác nhau.

Xây dựng hệ thống CertsChain: đã ứng dụng kiến thức đã học để xây dựng thành công CertsChain, một ứng dụng web sử dụng công nghệ Blockchain để quản lý và xác minh VBCC. Ứng dụng này đã đáp ứng một loạt yêu cầu về quản lý và xác minh VBCC: 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 được công khai, minh bạch từ đó sẽ thuận tiện cho mục đích tuyển dụng, chứng minh năng lực.

Cải tiến về mặt bảo mật so với BlockCerts và BTCert: như đã đề cập tới các hạn chế của BTCert và BlockCerts, 2 hệ thống này đang quản lý danh sách các VBCC bị thu hồi thông qua HTTP URI revocation list, có nhược điểm tiềm ẩn. Việc này đã được khắc phục trong hệ thống CertsChain bằng cách kiểm tra VBCC đã bị thu hồi hay chưa dựa theo một giá trị được lưu trữ trên CSDL thay vì dựa vào HTTP URI revocation list.

Mã nguồn công khai: Mã nguồn của CertsChain đã được công khai trên GitHub để chia sẻ và hỗ trợ cộng đồng (<https://github.com/cvthang56th2/CertsChain>).

Tóm lại, kết quả của đề tài này không chỉ giúp tôi hiểu rõ hơn về Blockchain và quản lý VBCC mà còn tạo ra một ứng dụng thực tế giúp cải thiện quy trình quản lý VBCC và tiết kiệm thời gian cho các đơn vị liên quan. Mã nguồn công khai cũng đóng góp vào việc chia sẻ kiến thức và công nghệ với cộng đồng.

4.2. Hạn chế của đề tài

Tuy đề tài đã đạt được nhiều thành tựu quan trọng, nhưng vẫn còn một số hạn chế cần xem xét:

Thiếu ứng dụng thực tế: Mặc dù tôi đã xây dựng một ứng dụng quản lý và xác minh VBCC, nhưng hệ thống chưa được triển khai hoặc áp dụng trong bất kỳ cơ sở đào tạo cụ thể nào. Điều này làm mất đi giá trị thực tế và ứng dụng của đề tài. Thông thường, việc thử nghiệm và áp dụng thực tế trong môi trường thực tế giúp xác minh tính khả thi và hiệu quả của một giải pháp.

Chưa có phản hồi thực tế: Việc không áp dụng ứng dụng trong một môi trường thực tế cũng đồng nghĩa rằng chưa có cơ hội thu thập phản hồi từ người dùng thực sự hoặc các cơ sở đào tạo. Phản hồi từ người dùng và sử dụng thực tế có thể là nguồn thông tin quý báu để cải tiến và điều chỉnh ứng dụng.

Hiệu suất và bảo mật: Trong môi trường thực tế, hiệu suất và bảo mật của hệ thống là một vấn đề quan trọng. Đề tài này chưa nêu rõ về cách hệ thống CertsChain xử lý các vấn đề này trong trường hợp áp dụng thực tế.

Hạn chế về sự phổ cập: Việc áp dụng công nghệ Blockchain và ứng dụng CertsChain có thể gặp khó khăn trong việc thuyết phục các cơ sở đào tạo sử dụng nó. Nếu công nghệ này đòi hỏi sự đầu tư lớn hoặc không phù hợp với cơ sở hạ tầng hiện có, việc thúc đẩy sự áp dụng có thể khó khăn.

Có thể cần điều chỉnh và cải tiến: Việc phát triển một ứng dụng không phải lúc nào cũng đảm bảo hoàn hảo từ đầu. Sự cải tiến liên tục và phản hồi là quan trọng để đảm bảo rằng ứng dụng phù hợp với nhu cầu và yêu cầu thay đổi của cơ sở đào tạo và người dùng cuối.

Có thể thấy, đề tài có tiềm năng nhưng chưa có sự áp dụng thực tế và thu thập phản hồi từ người dùng. Điều này tạo ra một số hạn chế quan trọng trong việc đảm bảo tính thực tế và hiệu quả của giải pháp CertsChain trong môi trường giáo dục.

4.3. Hướng phát triển của đề tài

Một số hướng phát triển tiềm năng cho đề tài CertsChain:

Triển khai thực tế: Như đã đề cập ở trên, để đảm bảo tính ứng dụng thực tế của CertsChain, cần nghiên cứu và hợp tác với một số cơ sở đào tạo để triển khai và thử nghiệm ứng dụng trong môi trường thực tế. Thu thập phản hồi từ người dùng và cơ sở đào tạo để điều chỉnh và cải tiến ứng dụng.

Mở rộng tính năng: Bổ sung thêm tính năng và khả năng cho CertsChain để làm cho nó hấp dẫn hơn cho các cơ sở đào tạo. Các tính năng có thể bao gồm khả năng tùy chỉnh, tích hợp với hệ thống quản lý học tập, bảo mật cao hơn và quản lý báo cáo chi tiết.

Nghiên cứu bảo mật và hiệu suất: Tăng cường bảo mật và hiệu suất của hệ thống CertsChain là một hướng phát triển quan trọng. Điều này bao gồm việc nghiên cứu và triển khai các biện pháp bảo mật mạnh mẽ và cải tiến hiệu suất để đảm bảo sự ổn định và đáng tin cậy.

Nghiên cứu và tích hợp công nghệ mới: Công nghệ Blockchain và quản lý VBCC là lĩnh vực đang phát triển. Tìm hiểu và tích hợp các cải tiến công nghệ mới, như hợp đồng thông minh (Smart contract) hoặc cải tiến liên quan đến bảo mật có thể cải thiện tính năng của CertsChain.

4.4. 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

Tài liệu tiếng Việt

- [1]. 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
- [2]. 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

Các trang web

- [3]. ACCGroup, Văn bằng chứng chỉ là gì? Trích từ: <https://accgroup.vn/van-bang-chung-chi-la-gi>
- [4]. TEK4, Hashing (hàm băm) cơ chế đằng sau sự toàn vẹn của Blockchain. Trích từ: <https://tek4.vn/hashing-ham-bam-co-che-dang-sau-su-toan-ven-cua-blockchain>
- [5]. AWS, What is Blockchain Technology? Trích từ <https://aws.amazon.com/what-is/blockchain>
- [6]. Wikipedia, Blockchain. Trích từ <https://en.wikipedia.org/wiki/Blockchain>