

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC CẦN THƠ**

DƯƠNG TUẤN DŨNG

**XÂY DỰNG HỆ THỐNG QUẢN LÝ
VĂN BẢN CHỨNG CHỈ SỬ DỤNG
CÔNG NGHỆ BLOCKCHAIN**

**LUẬN VĂN THẠC SĨ
NGÀNH KHOA HỌC MÁY TÍNH
MÃ SỐ 8480101**

NĂM 2022

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC CẦN THƠ**

**DƯƠNG TUẤN DŨNG
MÃ SỐ HV: M3718005**

**XÂY DỰNG HỆ THỐNG QUẢN LÝ
VĂN BẢN CHỨNG CHỈ SỬ DỤNG
CÔNG NGHỆ BLOCKCHAIN**

**LUẬN VĂN THẠC SĨ
NGÀNH KHOA HỌC MÁY TÍNH
MÃ SỐ 8480101**

**NGƯỜI HƯỚNG DẪN
TS. NGUYỄN VĂN HÒA**

NĂM 2022

LỜI CẢM ƠN

Để hoàn thành luận văn này, tôi xin gửi lời cảm ơn chân thành đến:

Thầy hướng dẫn TS. Nguyễn Văn Hòa, thầy đã đồng hành và hướng dẫn tôi trong quá trình học tập cũng như trong việc hoàn thành luận văn.

Thầy, cô Khoa Công nghệ Thông tin và Truyền thông Trường Đại học Cần Thơ đã tận tình giảng dạy cho tôi trong thời gian học tập.

Xin cảm ơn Ban Giám hiệu Trường Đại học An Giang, Ban Giám đốc Trung tâm Tin học Trường Đại học An Giang đã tạo điều kiện thuận lợi trong suốt thời gian đi học và làm bài luận văn.

Xin cảm ơn đến gia đình, thầy, cô, anh, chị đồng nghiệp, bạn bè và anh chị học viên lớp KHMT-K25, những người đã luôn sẵn sàng chia sẻ và hỗ trợ nhau trong học tập và trong cuộc sống.

Do giới hạn kiến thức và khả năng của bản thân còn nhiều thiếu sót và hạn chế, kính mong sự chỉ dẫn và đóng góp của thầy, cô để bài luận văn của tôi được hoàn thiện hơn.

TÓM TẮT

Ứng dụng công nghệ thông tin vào quản lý văn bằng, chứng chỉ đã giúp tăng đáng kể hiệu quả công tác. Phần mềm quản lý giúp đơn vị quản lý, người có văn bằng, chứng chỉ trong việc tra cứu; các tổ chức có liên quan xác minh, công nhận văn bằng, chứng chỉ. Đồng thời thông tin cấp văn bằng, chứng chỉ được công khai, bảo đảm tính bảo mật thông tin cá nhân của người được cấp văn bằng, chứng chỉ.

Với mục đích đảm bảo tính an toàn, bảo mật thông tin và giải quyết vấn đề tồn tại khi đổi chiều thông tin thủ công, đề tài nghiên cứu xây dựng hệ thống quản lý văn bằng chứng chỉ sử dụng công nghệ blockchain. Mạng blockchain Hyperledger Fabric được dùng để triển khai mô hình thử nghiệm lưu trữ thông tin văn bằng chứng chỉ lên chuỗi khối sau đó xác minh hạn chế lộ thông tin của người xác minh với bên cần xác minh.

Hệ thống thử nghiệm trong đề tài thực hiện quá trình xác thực quyền truy cập thông qua máy chủ. Thông tin văn bằng chứng chỉ có thể được xác thực và tin cậy nhờ chữ ký số nội bộ của Hyperledger Fabric. Giao diện thử nghiệm được phát triển trên nền tảng web để người dùng có thể dễ dàng sử dụng. Dựa trên kết quả thử nghiệm, hệ thống quản lý đáp ứng được yêu cầu kỹ thuật bao gồm: cấp phát chứng chỉ, xác minh chứng chỉ hợp lệ theo cơ chế ít tiết lộ thông tin cá nhân.

ABSTRACT

Applying information technology to the management of diplomas and certificates has increased significantly in overall efficiency. The information management system helps the issuers, verifiers, the owners of diplomas and certificates in issuing, searching, verifying, and recognizing diplomas and certificates. At the same time, it ensures the confidentiality of the personal information of the diploma or certificate holders which is made public.

To ensure the privacy and confidentiality of the information and solve problems that exist when comparing information by hand, the research topic is the certificate management system based on blockchain technology. A Hyperledger Fabric blockchain network is used to deploy a proof of concept model that stores certificate information on the blockchain and then verifies it with limited disclosure of the owner's information to the party that needs to verify.

In the model, the authentication of access rights is performed through a server. Thanks to Hyperledger Fabric's internal digital signatures, certificate information can be authenticated and trusted. The model's interface is developed using a web platform so that users can easily use it. Based on the test results, the certificate management system meets the technical requirements including issuing certificates and verifying valid certificates through less personal information disclosure mechanism.

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn này được hoàn thành dựa trên sự nghiên cứu của tôi dưới sự hướng dẫn của giáo viên hướng dẫn, các tài liệu tham khảo, công trình nghiên cứu liên quan được trích dẫn đầy đủ trong luận văn.

Mọi vi phạm quy chế tôi xin hoàn toàn chịu trách nhiệm.

Cần Thơ, ngày ... tháng ... năm 2022

Người cam đoan

Dương Tuấn Dũng

MỤC LỤC

Tóm tắt	ii
Abstract	iii
Mục lục	vi
Chương 1: Mở đầu	1
1.1 Giới thiệu	1
1.2 Lý do chọn đề tài	2
1.3 Mục tiêu nghiên cứu	3
1.4 Đối tượng và phạm vi nghiên cứu	3
1.5 Phương pháp nghiên cứu	4
1.6 Ý nghĩa của đề tài	4
1.7 Tiểu kết chương 1	4
Chương 2: Cơ sở lý thuyết	5
2.1 Quản lý VBCC	5
2.1.1 Giới thiệu	5
2.1.2 Cấp phát chứng chỉ	7
2.1.3 Xác minh chứng chỉ	7
2.2 Kỹ thuật mật mã	8
2.2.1 Mật mã Khóa Đối xứng và mật mã Khóa Bất đối xứng	9
2.2.2 Hàm băm	10
2.2.3 Chữ ký số	11
2.2.4 Chứng thư số	12
2.3 Công nghệ Blockchain	13
2.4 Hyperledger Fabric	15
2.4.1 Giới thiệu	15
2.4.2 Các thành phần của Hyperledger Fabric	16
Chương 3: Xây dựng hệ thống	18
3.1 Tổng quan giải pháp	18
3.2 Kiến trúc phần mềm	18
3.3 Các thành phần tham gia	19
3.3.1 Mô tả usecase	22
3.3.2 Thiết kế cơ sở dữ liệu	22
3.3.3 Thiết kế mạng blockchain	22
Chương 4: Kết quả thực nghiệm	23
4.1 Môi trường thực nghiệm	23
4.1.1 Mạng blockchain	23
4.1.2 Môi trường ứng dụng web	24
4.1.3 Phần cứng	24
4.1.4 Phần mềm	24
4.2 Kết quả thực nghiệm	24
Chương 5: Kết luận	29

Tài liệu tham khảo	31
-------------------------------------	-----------

DANH SÁCH HÌNH VẼ

2.1	Sơ đồ hệ mật mã Khóa Đối xứng	9
2.2	Sơ đồ ký số và xác thực chữ ký số	11
2.3	Sơ đồ ký số và xác thực chữ ký số với hàm băm	12
2.4	Cấu trúc chứng thư số X.509 phiên bản 3	13
2.5	Mô tả một giao dịch blockchain	14
2.6	Mô tả cây mã hóa Merkle trong Bitcoin	14
2.7	Mô tả chuỗi Blockchain	15
2.8	Dự án Hyperledger	16
2.9	Kiến trúc mạng Hyperledger Fabric	17
3.1	Sơ đồ tổng quan giải pháp	19
3.2	Sơ đồ kiến trúc phần mềm	20
3.3	Quy trình hoạt động của hệ thống	21
4.1	Chương trình Visual Studio Code	23
4.2	Giao diện hệ thống	25
4.3	Màn hình cấp chứng chỉ cho sinh viên	25
4.4	Màn hình các chứng chỉ đã cấp	26
4.5	Màn hình đăng ký tài khoản sinh viên	26
4.6	Màn hình xem các chứng chỉ đã được cấp	27
4.7	Màn hình chia sẻ thông tin sinh viên	27
4.8	Màn hình hiển thị mã xác thực chứng chỉ	28
4.9	Màn hình nhập mã xác thực chứng chỉ	28

DANH MỤC TỪ VIẾT TẮT

VBCC	Văn bằng chứng chỉ
CSDL	Cơ sở dữ liệu
LTS	Long Term Support
PKI	Public Key Infrastructure
API	Application Programming Interface
CA	Certificate Authority
SDK	Software Development Kit

CHƯƠNG 1

MỞ ĐẦU

1.1 Giới thiệu

Đề tài nghiên cứu xây dựng hệ thống quản lý văn bằng, chứng chỉ sử dụng công nghệ blockchain. Ngày nay, các hệ thống ứng dụng công nghệ thông tin có vai trò ngày càng quan trọng. Trong lĩnh vực giáo dục, những hệ thống này giúp thu thập, quản lý thông tin, tạo ra các sản phẩm thông tin phục vụ nhu cầu học tập, giảng dạy và quản lý. Một trong những sản phẩm thông tin đó là văn bằng, chứng chỉ (VBCC). Điều 26 của Quy chế ban hành theo Thông tư số 21/2019/TT-BGDĐT có quy định công bố công khai thông tin về cấp VBCC trên cổng thông tin điện tử. Ngoài ra, VBCC là một chứng cứ học tập của người sở hữu và có vai trò cần thiết trong nghề nghiệp. Cá nhân được đào tạo và nhận chứng nhận trước khi có thể bắt đầu công việc của mình. Do đó, thông tin dữ liệu về VBCC cần được quan tâm, bảo đảm lưu trữ an toàn, tin cậy và sẵn sàng.

Công nghệ blockchain hay công nghệ chuỗi khối có những đặc tính rất hữu ích trong việc lưu trữ, xử lý và chuyển giao thông tin một cách an toàn, tin cậy có thể đáp ứng các điều kiện về an toàn thông tin. Công nghệ chuỗi khối là công nghệ mã hóa và lưu trữ thông tin thành các khối và liên kết lại với nhau. Mỗi khi thông tin hoặc giao dịch mới xảy ra, thông tin cũ sẽ không bị mất đi mà thay vào đó, thông tin mới sẽ được lưu vào một khối mới và lần lượt được nối vào khối cũ để tạo thành chuỗi. Hơn nữa, dữ liệu của chuỗi khối được lưu trữ phân tán trên các máy chủ kết nối trong hệ thống blockchain để mọi người có thể xem và xác minh các giao dịch. Điều này có thể ngăn chặn việc sửa đổi hoặc gian lận và đảm bảo tính minh bạch và an toàn thông tin.

Trong đề tài, công nghệ blockchain được ứng dụng vào quản lý VBCC trong việc lưu trữ thông tin VBCC trên chuỗi khối để đảm bảo thông tin an toàn, tin cậy, minh bạch và bền vững theo thời gian. Ngày nay, VBCC chủ yếu được quản lý dưới dạng hồ sơ giấy và việc cấp VBCC chưa được số hóa. Hồ sơ giấy là các hồ sơ gốc bao gồm VBCC được in lên mẫu phôi và các hồ sơ theo quy định. Hồ sơ gốc có chữ ký tay và được đóng dấu của đơn vị cấp VBCC theo quy định tại Điều 20 của Thông tư số 21/2019/TT-BGDĐT. Ứng dụng của blockchain để số hóa việc cấp VBCC và xác thực thông tin VBCC được khảo sát trên một số công nghệ blockchain khá phổ biến hiện nay như Hyperledger Fabric, Ethereum. Trong những công nghệ blockchain này, ứng dụng của hợp đồng thông minh sẽ thực hiện số hóa việc cấp VBCC, thông tin của VBCC được mã hóa và lưu trữ vào chuỗi khối.

Công nghệ blockchain là một xu hướng công nghệ ngày nay và được ứng dụng trong nhiều ngành, lĩnh vực khác nhau. Một số công trình nghiên cứu liên quan công nghệ blockchain như sau.

Trong lĩnh vực mật mã, nghiên cứu [1] của Ralph Charles Merkle về ứng dụng hệ

mật mã khóa công khai trong an toàn thông tin. Với các hệ mật mã chỉ dùng một khóa duy nhất trong mật mã và giải mật, khóa này được tạo ra và được mỗi bên giữ bí mật để bảo mật thông tin. Tuy nhiên, vấn đề trao đổi khóa gặp nhiều khó khăn trong thực tiễn. Ngoài ra, với một khóa duy nhất thì vai trò mỗi bên như nhau trong liên lạc. Với các hệ mật mã khóa công khai, mỗi bên tạo một cặp khóa. Trong đó, một khóa công bố công khai cho tất cả và một khóa riêng tư được mỗi bên giữ bí mật. Khóa công khai chỉ liên kết với khóa riêng tư, đảm bảo rất khó để người khác tạo ra khóa công khai mà không biết khóa cá nhân tương ứng. Bài giảng [2] có giải thích rằng các giải pháp mật mã với khóa công khai ra đời nhằm cá nhân hóa mật mã. Đó là các giải pháp Diffie-Hellman, ElGamal và RSA (viết tắt tên của 3 sinh viên trường Stanford: Rivest, Shamir và Adleman). Các giải pháp này vẫn còn nguyên giá trị đến ngày nay. Chữ ký số ra đời sau đó và được phát triển cùng với các giải pháp Băm (Hash) kết hợp với mật mã khóa công khai.

Trong lĩnh vực y tế

Trong lĩnh vực giáo dục

Trong lĩnh vực tiền ảo

Từ năm 2008, công nghệ chuỗi khối được hiện thực với đồng tiền ảo Bitcoin [3], đã đánh dấu sự ra đời cách thức lưu trữ và chuyển giao thông tin hoàn toàn mới.

Một thuộc tính của công nghệ chuỗi khối là sự đồng thuận giữa các thành phần không tin cậy - cùng tham gia vào một hệ thống mạng không tập trung. Công nghệ này đã được rất nhiều nghiên cứu [4, 5, 6, 7, 8] để hoàn thiện về cơ chế và ứng dụng trong các giải pháp xử lý, truyền tải an toàn thông tin.

Chuỗi khối (blockchain) sử dụng các kỹ thuật mật mã [2, 9, 1, 10] để ghi nhận các giao dịch xảy ra theo thời gian và để kiểm chứng nguồn gốc thông tin.

Tuy nhiên, công nghệ chuỗi khối cũng có mặt hạn chế. Nghiên cứu [11] cho rằng công nghệ này chưa phù hợp để xử lý những giao dịch cần hiệu suất cao hoặc để thay thế cơ sở dữ liệu (database). Cơ chế lưu trữ của chuỗi khối cũng không dành để lưu dữ liệu lớn. Do đó cần có giải pháp linh hoạt kết hợp cơ chế lưu trữ ngoài chuỗi khối (off-chain) bên cạnh khả năng lưu dữ liệu và xử lý hạn chế của công nghệ.

1.2 Lý do chọn đề tài

Trung tâm Tin học Trường Đại học An Giang là đơn vị hoạt động về lĩnh vực đào tạo và có chức năng tổ chức thi và cấp chứng chỉ. Công tác quản lý về đào tạo, tổ chức thi và cấp chứng chỉ tại đơn vị đã được tin học hóa một số nghiệp vụ mang lại hiệu quả đáng kể như ghi danh học viên, quản lý hóa đơn, nhận hồ sơ dự thi, tra cứu điểm thi, và công khai thông tin VBCC do đơn vị cấp trên hệ thống website.

Sổ gốc cấp VBCC theo quy định tại Điều 19 thông tư số 21/2019/TT-BGDĐT yêu cầu ghi thông tin cấp phát VBCC cho người được cấp, đã thi đạt sau khi dự thi tại cơ sở tổ chức thi. Sổ gốc cấp VBCC phải được ghi chính xác, đánh số trang, đóng dấu giáp lai, không được tẩy xóa, đảm bảo quản lý chặt chẽ và lưu trữ vĩnh viễn. Tuy nhiên, việc cập nhật thông tin thay đổi vào sổ, theo dõi sổ gốc còn làm thủ công trong những trường hợp

như sau:

1. Nhân viên phát VBCC cho người nhận chứng chỉ đến trực tiếp và có giấy tờ khớp thông tin với sổ gốc thì nhân viên phát cho người đó và cập nhật sổ gốc. Ngược lại, nếu giấy tờ người nhận mang theo mà thông tin không khớp với sổ gốc thì nhân viên không phát cho người đó.

2. Nhân viên phát VBCC cho người nhận chứng chỉ có giấy ủy quyền đến trực tiếp và có giấy tờ ủy quyền khớp thông tin với sổ gốc thì nhân viên phát cho người đó và cập nhật sổ gốc. Ngược lại, nếu giấy tờ người nhận mang theo mà thông tin không khớp với sổ gốc thì nhân viên không phát cho người đó.

3. Văn bản, chứng chỉ chưa phát phải được quản lý, lưu trữ theo quy định.

Mặt khác những trường hợp 1, 2, dù không phát VBCC vẫn phải so khớp thông tin giấy tờ với sổ gốc, nên công việc chưa được hiệu quả. Thêm vào đó, xử lý trên hồ sơ giấy có thể gặp một số rủi ro như rách trang giấy, thất lạc,... làm ảnh hưởng đến công tác lưu trữ, bảo quản hồ sơ theo quy định.

Mục tiêu chính của đề tài là ứng dụng công nghệ Blockchain để lưu trữ thông tin VBCC. Ngoài việc tìm hiểu những khái niệm liên quan công nghệ chuỗi khối với các đặc tính công khai, an toàn, minh bạch, đề tài còn hướng đến nhu cầu dùng công nghệ chuỗi khối để kiểm chứng thông tin VBCC khi thông tin được truy vấn từ cơ sở dữ liệu VBCC bên ngoài chuỗi khối.

1.3 Mục tiêu nghiên cứu

Đề tài tập trung đề xuất mô hình ứng dụng công nghệ Blockchain trong quản lý VBCC nhằm hỗ trợ theo dõi việc cập nhật thông tin cho người sử dụng nhưng vẫn đảm bảo tính minh bạch, công khai và an toàn. Các mục tiêu cụ thể như sau:

1. Phân tích và xây dựng CSDL đáp ứng nghiệp vụ quản lý VBCC: cập nhật thông tin sổ gốc cấp VBCC; tra thông tin VBCC.

2. Xây dựng hệ thống website tương tác với người sử dụng, giao diện trực quan và phản hồi nhanh.

3. Xây dựng mạng Hyperledger Fabric và triển khai lưu trữ dữ liệu nhật ký về VBCC trên mạng này.

1.4 Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu:

- Lý thuyết mật mã có liên quan công nghệ chuỗi khối
- Mô hình mạng thử nghiệm Hyperledger Fabric
- Quy định pháp luật về quản lý VBCC

Phạm vi nghiên cứu:

- Quy trình cấp phát chứng chỉ của Trung tâm Tin học Trường Đại học An Giang
- Xây dựng hệ thống quản lý VBCC ứng dụng công nghệ blockchain.

1.5 Phương pháp nghiên cứu

- Tìm hiểu, phân tích và tổng hợp tài liệu về quản lý VBCC (quy định, biểu mẫu hiện hành) và các nền tảng kiến trúc, cơ chế hoạt động của mạng Blockchain.
- Xác định các quy trình nghiệp vụ, yêu cầu của hệ thống, cơ sở dữ liệu, thông tin được lưu trên chuỗi khối.
- Phương pháp thực nghiệm, ghi nhận kết quả và đánh giá kết quả đạt được.

1.6 Ý nghĩa của đề tài

Đề tài có tính ứng dụng cao, bên cạnh việc tìm hiểu kiến thức, những khái niệm liên quan công nghệ chuỗi khối. Ngoài việc triển khai với bài toán cụ thể tại Trung tâm Tin học Trường Đại học An Giang trong quản lý VBCC, nghiên cứu có thể ứng dụng ở các đơn vị khác có nghiệp vụ tương tự như các trường học, cơ sở đào tạo.

Công nghệ chuỗi khối có khả năng lưu trữ, xử lý và chia sẻ thông tin, dữ liệu minh bạch theo thời gian và có độ an toàn cao. Các nghiên cứu về công nghệ chuỗi khối có thể mở rộng ứng dụng trong nhiều lĩnh vực như nông nghiệp, y tế, ngân hàng, vận tải.

1.7 Tiểu kết chương 1

Chương 1 trình bày các mục tiêu của hệ thống cần đạt được trong quá trình nghiên cứu và thực hiện. Chương 2 sẽ tập trung giới thiệu cơ sở lý thuyết quản lý VBCC, đặc tính an toàn, bảo mật của công nghệ chuỗi khối, và mô hình mạng thử nghiệm Hyperledger Fabric.

CHƯƠNG 2

CƠ SỞ LÝ THUYẾT

2.1 Quản lý VBCC

2.1.1 Giới thiệu

Xã hội ngày càng phát triển nên nhu cầu học tập nâng cao trình độ đáp ứng cho các lĩnh vực lao động xã hội ngày càng tăng. Hàng năm có hàng nghìn các loại VBCC được cấp phát để công nhận trình độ, năng lực của các học viên đã qua một quá trình học tập và thi đạt. Ngoài ra, văn bằng được dùng trong tuyển dụng lao động và làm thủ tục hồ sơ liên quan khác, ảnh hưởng nhiều đến người sở hữu trong tương lai. Trong nhiều ngành nghề, chúng chỉ là điều kiện để thực hiện công việc, có tính quyết định và ảnh hưởng tới nhiều lĩnh vực khác. Do đó, quản lý VBCC đòi hỏi quy trình thực hiện nghiêm ngặt, tránh những trường hợp lợi dụng kẽ hở để thực hiện hành vi trái pháp luật.

Một số văn bản pháp luật được ban hành nhằm quy định việc quản lý VBCC, đảm bảo quyền lợi, trách nhiệm của các tổ chức và cá nhân như sau:

- Điều 12 Luật giáo dục 2019 quy định “Văn bằng của hệ thống giáo dục quốc dân được cấp cho người học sau khi tốt nghiệp cấp học hoặc sau khi hoàn thành chương trình giáo dục, đạt chuẩn đầu ra của trình độ tương ứng theo quy định của Luật giáo dục. Văn bằng của hệ thống giáo dục quốc dân gồm bằng tốt nghiệp trung học cơ sở, bằng tốt nghiệp trung học phổ thông, bằng tốt nghiệp trung cấp, bằng tốt nghiệp cao đẳng, bằng cử nhân, bằng thạc sĩ, bằng tiến sĩ và văn bằng trình độ tương đương. Chứng chỉ của hệ thống giáo dục quốc dân được cấp cho người học để xác nhận kết quả học tập sau khi được đào tạo, bồi dưỡng nâng cao trình độ học vấn, nghề nghiệp hoặc cấp cho người học dự thi lấy chứng chỉ theo quy định.”

- Điều 3 Thông tư 21/2019/TT-BGDĐT quy định về việc ban hành Quy chế quản lý VBCC của hệ thống giáo dục quốc dân, quy định việc phân cấp và giao quyền tự chủ, tự chịu trách nhiệm trong quản lý VBCC. Cơ sở giáo dục đại học, cơ sở đào tạo giáo viên tự chủ và tự chịu trách nhiệm trong việc quản lý, cấp phát VBCC theo quy định của pháp luật và quy định của Bộ trưởng Bộ Giáo dục và Đào tạo.

- Điều 5 Nghị định số 30/2020/NĐ-CP quy định về hoạt động văn thư lưu trữ, giá trị pháp lý về hồ sơ điện tử, văn bản điện tử được ký số bởi người có thẩm quyền và ký số của cơ quan, tổ chức theo quy định của pháp luật có giá trị pháp lý như bản gốc văn bản giấy.

- Nghị định Số 45/2020/NĐ-CP quy định thủ tục hành chính trên môi trường điện tử. Thủ tục hồ sơ điện tử rất tiết kiệm thời gian và thuận tiện hơn hình thức còn lại nên các giao dịch điện tử tăng nhanh trong những năm gần đây: thanh toán trực tuyến, nộp thuế qua mạng, hóa đơn điện tử, dịch vụ công trực tuyến.

Từ năm học 2020-2021, Bộ Giáo dục và Đào tạo đã triển khai ứng dụng công nghệ

để lưu trữ văn bằng quốc gia. Hệ thống ứng dụng công nghệ blockchain được triển khai bởi nhà phát triển công nghệ TomoChain. Hiệu quả của hệ thống được khẳng định là đảm bảo tính minh bạch, an toàn và tiết kiệm xã hội. Các đơn vị đào tạo thuộc Bộ Giáo dục và Đào tạo sẽ đưa dữ liệu văn bằng được cấp bởi các đơn vị vào hệ thống lưu trữ văn bằng quốc gia. Bên cạnh đó hệ thống còn đáp ứng những yêu cầu truy xuất cho các bên có nhu cầu và được xã hội hoá.

Học viện Công nghệ Bưu chính Viễn thông đang triển khai thí điểm Cổng thông tin xác thực VBCC trên môi trường số với nền tảng ứng dụng công nghệ Blockchain và chữ ký số. Hệ thống phần mềm đảm bảo tính công khai, minh bạch, tin cậy trong công tác tra cứu và xác thực VBCC; hướng tới việc cấp VBCC số trong tương lai đáp ứng theo Nghị định số 30/2020/NĐ-CP. Giải pháp có thể chống lại những hành vi làm giả chứng chỉ, hoặc cấp chứng chỉ không đúng quy định. Hệ thống giúp cho các cơ quan, tổ chức, cá nhân trong quá trình kiểm tra xác minh VBCC khi tuyển dụng giảm nhiều thời gian, sức lực so với cách truyền thống.

Trung tâm Tin học Trường Đại học An Giang (gọi tắt là Trung tâm) là đơn vị trực thuộc Trường Đại học An Giang. Từ năm 2017, Trung tâm thực hiện tổ chức thi và cấp chứng chỉ theo Quy chế tổ chức thi và cấp chứng chỉ ứng dụng công nghệ thông tin ban hành theo Quyết định 04/QĐ-TTTH ngày 27/2/2017 của Giám đốc Trung tâm Tin học (gọi tắt là Quy chế). Việc quản lý các dữ liệu chứng chỉ do đơn vị cấp cần phải đảm bảo tính chính xác. Hai hình thức giao dịch giữa các đơn vị trong và ngoài tổ chức; và giữa đơn vị với cá nhân bằng hồ sơ điện tử và hồ sơ giấy. Tuy nhiên, phạm vi nghiên cứu của đề tài chỉ tập trung vào hình thức hồ sơ giấy trong công tác tổ chức thi và cấp chứng chỉ như công văn, quyết định, phôi chứng chỉ và sổ gốc cấp chứng chỉ.

Theo đó, quản lý VBCC tại Trung tâm là triển khai các ban hành, phổ biến thông tin, tiếp nhận yêu cầu, thực hiện và lưu giữ hồ sơ được quy định tại Quy chế tổ chức thi và cấp chứng chỉ ứng dụng công nghệ thông tin ban hành theo Quyết định 04/QĐ-TTTH ngày 27/2/2017, bao gồm các nội dung như sau:

1. Kiểm tra thông tin học viên được cấp chứng chỉ
2. Gửi công văn đề nghị cấp phôi chứng chỉ
3. Tiếp nhận và quản lý phôi chứng chỉ
4. Lập sổ gốc
5. In chứng chỉ
6. Cấp phát chứng chỉ
7. Bảo quản chứng chỉ
8. Xác minh chứng chỉ
9. Cấp giấy xác nhận kết quả thi đạt
10. Thu hồi, hủy bỏ chứng chỉ

Trong phạm vi khả năng giới hạn, đề tài tập trung nghiên cứu vào việc lưu trữ thông tin VBCC dùng công nghệ blockchain để tăng tính bảo mật và chắc chắn cho việc cấp

phát các VBCC cho học viên sử dụng. Dữ liệu đầu vào của hệ thống được nhập vào từ chương trình quản lý học, quản lý thi. Những chương trình này được đã triển khai và đang đáp ứng tốt một số nghiệp vụ quản lý hiện nay. Đề tài nghiên cứu những nghiệp vụ như sau:

- Cấp phát chứng chỉ
- Xác minh chứng chỉ

2.1.2 Cấp phát chứng chỉ

Việc cấp phát chứng chỉ được quy định tại Điều 17 của Quy chế và Điều 19 Thông tư 21/2019/TT-BGDĐT. Sổ gốc cấp VBCC phải được ghi chính xác, đánh số trang, đóng dấu giáp lai, không được tẩy xóa, đảm bảo quản lý chặt chẽ và lưu trữ vĩnh viễn.

1. Thí sinh thi đạt sẽ được cấp chứng chỉ. Sinh viên trực tiếp nhận và đem theo thẻ sinh viên hoặc chứng minh nhân dân, căn cước công dân hoặc giấy tờ có ảnh. Hoặc người được ủy quyền đến trực tiếp nhận và có đem theo giấy tờ tương tự.

2. Nhân viên dựa vào hệ thống quản lý và sổ gốc cấp chứng chỉ để kiểm tra thông tin chứng chỉ.

3. Nếu thông tin sinh viên trùng khớp trong sổ gốc cấp chứng chỉ thì nhân viên sẽ ghi lại thông tin người nhận vào sổ gốc cấp chứng chỉ.

4. Nhân viên phát chứng chỉ cho người nhận.

5. Sinh viên ký tên xác nhận thông tin đó.

2.1.3 Xác minh chứng chỉ

Việc xác minh VBCC là một trong những giai đoạn cần thực hiện để phát hành văn bản có hiệu lực. Quy trình xác minh VBCC là một dạng thủ tục hành chính, cơ sở đào tạo xác minh thông tin chứng chỉ với sổ gốc, kết quả thủ tục là đơn vị yêu cầu xác minh sẽ nhận được công văn trả lời kết quả xác minh (không phải là khẳng định chứng chỉ có giá trị hay không). Quy trình này trải qua 5 bước thực hiện chính như sau:

1. Đơn vị có nhu cầu xác minh các VBCC cần gửi công văn đến cơ sở đào tạo. Đơn vị có thể cử người có giấy giới thiệu đến trực tiếp phòng ban để bắt đầu làm thủ tục xác minh. Trong quá trình gửi công văn, đơn vị phải chịu trách nhiệm với hồ sơ được bàn giao.

2. Người phụ trách xác minh tại cơ sở tổ chức thi khi tiếp nhận hồ sơ gửi đến sẽ tiến hành kiểm tra lại hồ sơ, và thông tin trong sổ gốc được lập từ trước. Xác nhận người nhận chứng chỉ có trong danh sách thi, đã đạt kết quả và có thông tin chứng chỉ trong sổ gốc.

3. Người phụ trách kiểm tra xác nhận trong sổ gốc xong cần phải soạn công văn, và đề nghị lãnh đạo cơ quan chủ quản phê duyệt. Hồ sơ sẽ được lưu tại bên phụ trách kiểm tra, chờ cơ quan cấp trên cấp duyệt.

4. Viên chức tiếp nhận công văn của người phụ trách xác minh sẽ kiểm tra, quyết định ký duyệt và sau đó gửi lại cho bên phụ trách xác minh. Các công văn cần xác minh

của người yêu cầu đã được chấp nhận và được chuyển lại cho bên tổ chức thi.

5. Người phụ trách xác minh khi nhận được công văn đã ký duyệt của cấp trên sẽ tiến hành đóng dấu đỏ của cơ quan, hoàn tất thủ tục hành chính, xác minh văn bằng của người yêu cầu. Cuối cùng, người yêu cầu sẽ đến nhận lại công văn (hoặc có thể nhận qua thư hay email).

Hồ sơ VBCC, sổ gốc hay dữ liệu VBCC khi lưu trên máy tính cũng phải theo quy định để đảm bảo tính pháp lý. Theo quy định, nhân viên thực hiện kiểm tra, đối chiếu bản chính giấy tờ tùy thân, giấy tờ liên quan, thông tin sổ gốc nhằm tránh giả mạo người nhận. Chữ ký vào hồ sơ văn bản nhằm chứng minh cho sự hiện diện của người nhận và là một đặc điểm thể hiện dấu riêng của một người. Chữ ký số (hay chữ ký điện tử) là giải pháp được công nhận về tính pháp lý. Chữ ký số có các thuộc tính định danh, xác thực đúng nguồn gốc, đảm bảo được tính toàn vẹn của dữ liệu nhận được và chống thoái thác. Chữ ký số được xem như tương đương chữ ký tay trong giao dịch để đảm bảo tính pháp lý, tin cậy, tiết kiệm thời gian.

Nội dung tiếp theo sẽ giới thiệu về chữ ký số và các ứng dụng chữ ký số được nghiên cứu trong mật mã và blockchain.

2.2 Kỹ thuật mật mã

Kỹ thuật mật mã là ngành khoa học ứng dụng toán học vào việc biến đổi thông tin thành một dạng khác với mục đích che giấu nội dung, ý nghĩa thông tin cần mã hóa. Đây là một ngành quan trọng và có nhiều ứng dụng trong đời sống xã hội. Những ứng dụng của ngành Kỹ thuật mật mã không chỉ đơn thuần là mã hóa và giải mã thông tin mà còn mở rộng thêm bao gồm: chứng thực nguồn gốc nội dung thông tin (kỹ thuật chữ ký điện tử), chứng nhận tính xác thực về người sở hữu mã khóa, các quy trình giúp trao đổi thông tin và thực hiện giao dịch điện tử an toàn trên mạng.

Mục tiêu của Kỹ thuật mật mã là tạo ra các mô hình tin cậy đảm bảo đạt 4 tiêu chí của an toàn thông tin:

1. *Tính riêng tư hoặc tính bảo mật (confidentiality/privacy)*: tính chất này đảm bảo thông tin chỉ được hiểu bởi những người biết chìa khóa bí mật.

2. *Tính toàn vẹn thông tin (integrity)*: tính chất này đảm bảo thông tin không thể bị thay đổi mà không bị phát hiện, cung cấp bằng chứng xác nhận thông tin đã bị thay đổi.

3. *Tính xác thực một thực thể hay một định danh (authentication/identification)*: người gửi (hoặc người nhận) có thể chứng minh đúng họ. Phương pháp có thể dùng là mật khẩu, một thách đố dựa trên một thuật toán mã hóa hoặc một bí mật chia sẻ giữa hai người để xác thực. Sự xác thực này có thể thực hiện một chiều (one-way) hoặc hai chiều (mutual authentication).

4. *Tính không chối bỏ hay chống thoái thác trách nhiệm (non-repudiation)*: người gửi hoặc nhận sau này không thể chối bỏ việc đã gửi hoặc nhận thông tin. Thông thường

điều này được thực hiện thông qua chữ ký số (electronic signature).

2.2.1 Mật mã Khóa Đối xứng và mật mã Khóa Bất đối xứng

Theo Giáo trình lý thuyết mật mã [2], kỹ thuật mật mã có thể được biểu diễn bằng nguyên lý ánh xạ đơn ánh, như sau:

Nếu P là bản rõ là một phần tử của tập hợp X , còn bản mật C là phần tử của Y . Khi đó:

- Tạo mật mã với khóa $k \in K$ là ánh xạ đơn ánh có tham số $f_k : P \rightarrow C$
- Giải mật mã với khóa $k' \in K$ là ánh xạ ngược của f có tham số: $g_{k'} = f_{k'}^{-1} : C \rightarrow P$

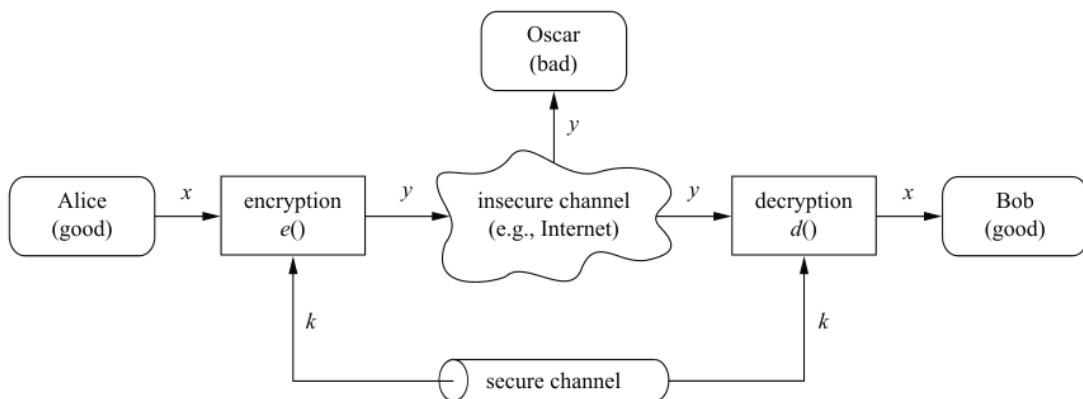
Phân loại mật mã

Có thể phân loại mật mã theo đặc điểm phụ thuộc vào loại khóa:

- Mật mã Khóa Đối xứng (Symmetric Key Cryptography) nếu $k = k'$
- Mật mã Khóa Bất đối xứng (Asymmetric Key Cryptography) nếu $k \neq k'$

Mật mã không phụ thuộc vào khóa: Hàm băm (Hash Function) là ánh xạ thu nhỏ một chiều (không có ánh xạ ngược).

Mật mã Khóa Đối xứng có chung một khóa khi mật mã và giải mã trong các thuật toán mật mã luồng và mật mã khối. Mật mã luồng xử lý từng ký tự một nhưng thường xuyên là từng bit một. Ngược lại, mật mã khối xử lý từng khối dữ liệu có độ dài chuẩn như nhau. Ưu điểm của mật mã Khóa Đối xứng là tốc độ xử lý nhanh. Thuộc tính khóa phải được chia sẻ an toàn cho người nhận để có thể giải mật dữ liệu. Các thuật toán mật mã Khóa Bất Đối xứng có thể dùng để chia sẻ khóa dùng chung một cách an toàn. Tên gọi khác của mật mã Khóa Đối xứng là: mật mã Khóa Bí mật (Secret Key Cryptosystems).



Hình 2.1: Sơ đồ hệ mật mã Khóa Đối xứng

Sơ đồ 2.1 minh họa một ứng dụng mật mã Khóa Đối xứng trong thực tế. Alice và Bob là 2 người bạn cần trao đổi thông tin bí mật bằng phương pháp sử dụng mật mã Khóa Đối xứng. Trong khi đó Oscar luôn tìm cách giải mật thông tin nghe được giữa Alice và Bob. Nhưng Alice và Bob có được khóa nên liên lạc được, chỉ Oscar thiếu duy nhất khóa để giải mật nên không thể hiểu thông tin.

Các ký hiệu trong sơ đồ 2.1:

- x là bản rõ
- y là bản mật
- k là khóa

Mật mã Khóa Bất đối xứng dùng hai khóa Cá nhân và khóa Công khai trong thuật toán tạo mật mã và giải mật, cặp khóa có liên hệ chặt chẽ nhau về toán học. Khóa Công khai được công bố cho cộng đồng sử dụng nên dễ bị lộ, còn khóa Cá nhân chỉ có cá nhân được sở hữu. Mặc khác khóa Công khai bị lộ thì cũng rất khó (sử dụng Phân tích mật mã) có thể tìm được khóa Cá nhân. Khóa cá nhân dùng để tạo mật mã và tạo chữ ký số. Khóa công khai dùng để giải mật mã và xác thực chữ ký số. Ví dụ: khi mật mã dùng một khóa công khai thì chỉ có khóa cá nhân của cặp khóa đó mới giải mã được; Tương tự, dùng một khóa cá nhân tạo chữ ký số thì chỉ có khóa công khai tương ứng mới xác thực chữ ký số đó.

2.2.2 Hàm băm

Hàm băm là phép biến đổi một chiều có đầu vào là thông điệp chiều dài bất kỳ thành một dãy bit có độ dài cố định (tùy thuộc vào thuật toán băm). Giá trị băm còn gọi là hash value (hay Digest) là đặc trưng cho thông điệp ban đầu.

Ví dụ: Với thông điệp ban đầu là Hello world sẽ có các giá trị băm tương ứng với một số hàm băm, như sau:

Adler32: 18ab043d

MD5: 3e25960a79dbc69b674cd4ec67a72c62

SHA-256: 64ec88ca00b268e5ba1a35678a1b5316d212f4f366b2477232...37f3c

Băm là một giải pháp tạo ra một đặc trưng cho một file dữ liệu. Tương tự như mỗi người có một dấu vân tay đặc trưng. Vì vậy Băm còn được gọi dấu vân tay (Fingerprint) của file dữ liệu.

Hàm băm (Hash Function) là một dạng mật mã tạo bản mật không cần giải mật mà đáp ứng yêu cầu kiểm tra tính toàn vẹn của một dữ liệu dựa trên đặc trưng vân tay của nó.

Hàm băm $H(x)$ có khả năng bảo mật tốt, nếu thỏa 3 tính chất: Một chiều (One Way), Tự do liên kết yếu (Weakly Collision Free) và Tự do liên kết mạnh (Strong Collision Free).

- *Tính chất Một chiều*: Cho trước giá trị băm y, rất khó tìm được x: $H(x) = y$. Điều này có nghĩa là nhận được giá trị băm y, rất khó tìm được dữ liệu gốc x thỏa: $H(x) = y$. Tính chất này đảm bảo rất ít tập dữ liệu x có $H(x) = y$.

- *Tính chất Tự do liên kết yếu*: cho trước tập dữ liệu x, rất khó tìm được tập dữ liệu $x' \neq x$: $H(x) = H(x')$. Nếu x là tập dữ liệu cần băm, thì hầu như không thể tìm được tập dữ liệu khác x' : $H(x') = H(x)$. Tính chất này đảm bảo tập dữ liệu x kèm $H(x)$ rất khó bị sửa thành x' có cùng $H(x)$.

- *Tính chất Tự do liên kết mạnh*: rất khó có thể tìm được 2 tập dữ liệu $x \neq x'$ có cùng giá trị băm $H(x) = H(x')$.

2.2.3 Chữ ký số

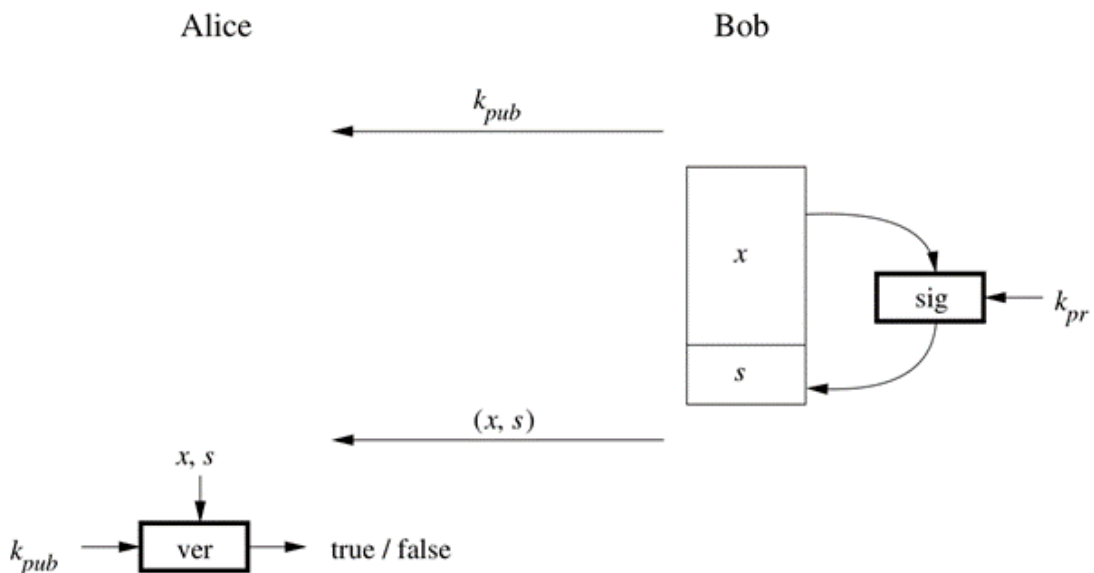
Chữ ký số được định nghĩa là một loại chữ ký điện tử, được tạo bằng sự chuyển đổi thông điệp dữ liệu sử dụng một hệ thống mật mã không đối xứng, theo đó người có được thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác.

a) Việc biến đổi nêu trên được tạo ra bằng đúng khóa bí mật tương ứng với khóa công khai trong cùng một cặp khóa;

b) Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.

Chữ ký số có chung mục tiêu như chữ ký tay trên văn bản. Đó là cách xác định một người bằng dấu vết riêng tác động lên văn bản và qua đó văn bản được ký là chứng cứ sự thật do người đó tạo lập nên. Chữ ký số là thành phần quan trọng trong những giải pháp ứng dụng mật mã, và được áp dụng rộng rãi trong thực tiễn cho đến nay. Chữ ký số cùng với cơ chế trao đổi khóa là cơ sở quan trọng trong hạ tầng khóa công khai. Tuy nhiên, chữ ký số chỉ có thể đảm bảo khi khóa bí mật không bị lộ. Khi khóa bí mật bị lộ thì người sở hữu chữ ký không thể ngăn chặn được việc bị giả mạo chữ ký.

Nguyên lý ký số và xác thực chữ ký số

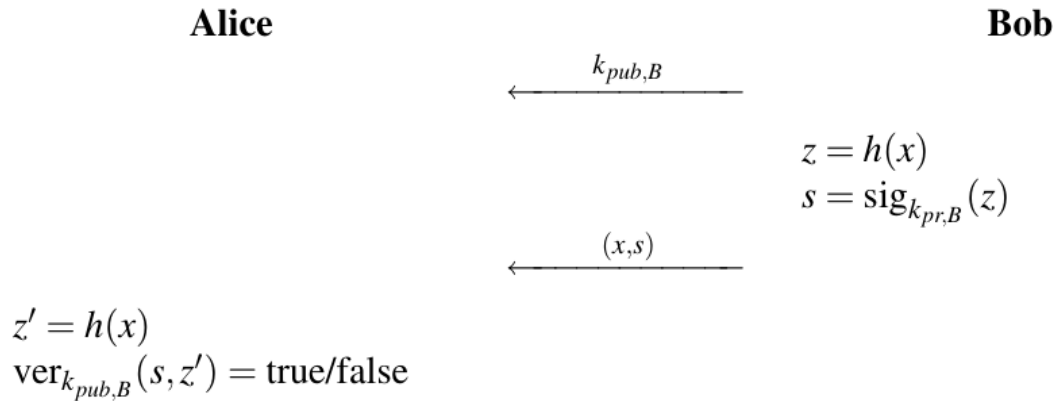


Hình 2.2: Sơ đồ ký số và xác thực chữ ký số

Quy trình bắt đầu khi Bob ký thông điệp x . Thuật toán ký số (sig) có tham số thứ nhất là khóa bí mật của Bob, k_{pr} . Khóa bí mật được Bob giữ và chỉ anh ta mới có thể ký số lên thông điệp x . Thông điệp x là tham số thứ hai của thuật toán ký số. Sau đó bản chữ ký s sẽ thêm vào thông điệp x tạo một cặp (x, s) gửi cho Alice.

Tiếp theo Alice xác minh chữ ký của hợp lệ hay không, hàm xác thực (ver) có 2 tham số (x,s) và k_{pub} của Bob. Nếu x do Bob ký số thì được kết quả true, ngược lại false. Sơ đồ nguyên lý ký số và xác thực chữ ký số được mô tả ở hình 2.2

Tuy nhiên, với thông điệp x rất lớn thì ký số sẽ chậm và chiếm dung lượng lớn. Như vậy, thay vì ký số lên thông điệp x , thì có thể ký số lên giá trị băm của $x = h(x)$, giá trị $h(x)$ nhỏ hơn thông điệp x , đồng nghĩa sẽ nhanh hơn.



Hình 2.3: Sơ đồ ký số và xác thực chữ ký số với hàm băm

Bob sẽ tính giá trị băm của thông điệp x và ký số lên giá trị băm $z = h(x)$ bằng khóa bí mật $K_{pr,B}$. Còn bên nhận, Alice sẽ tính giá trị băm z' của thông điệp x : $z' = h(x)$. Alice sẽ xác thực chữ ký s với khóa công khai $K_{pub,B}$ và z' . Sơ đồ mô tả nguyên lý ký số và xác thực chữ ký số với hàm băm ở hình 2.3

Chức năng của chữ ký số và tiêu chí an toàn thông tin

Chữ ký số đảm bảo 2 tiêu chí an toàn thông tin như sau:

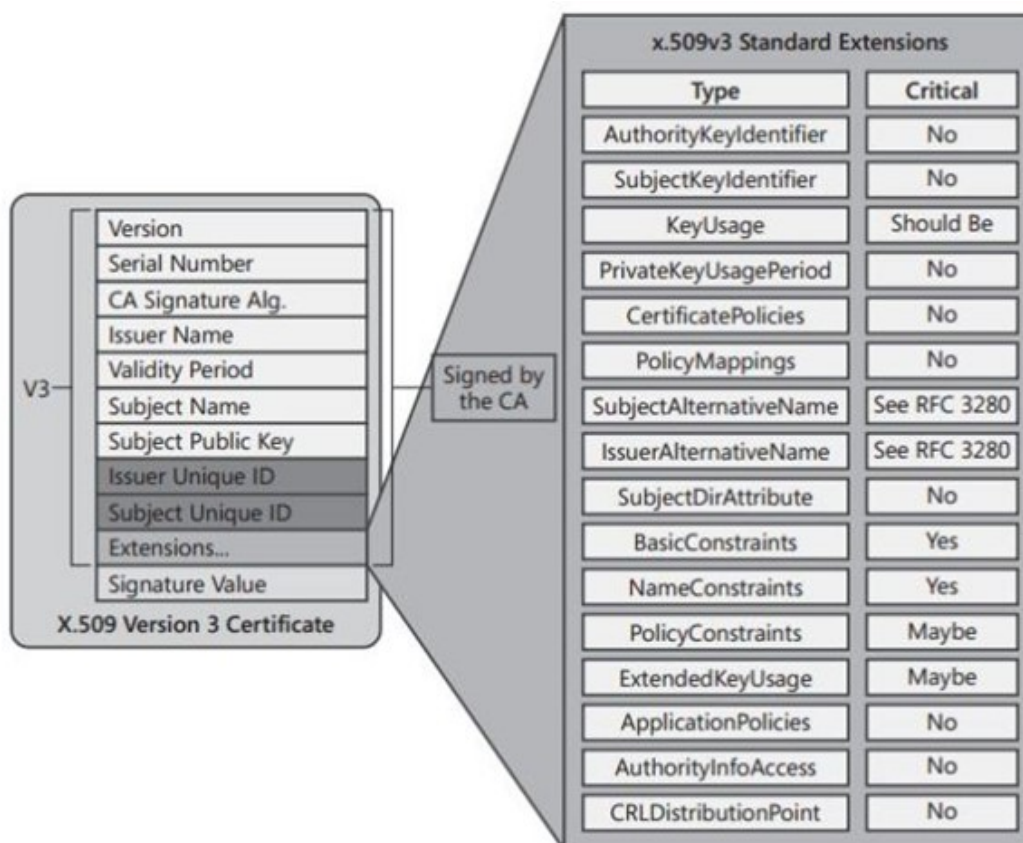
1. Tính toàn vẹn thông tin: khi có sự thay đổi bất kỳ lên thông điệp thì giá trị hàm băm sẽ bị thay đổi; nghĩa là thông điệp không toàn vẹn.
2. Tính không chối bỏ hay chống thoái thác trách nhiệm: vì chỉ có chủ thông điệp mới có khóa bí mật để ký lên thông điệp nên người ký không thể chối bỏ thông điệp của mình

2.2.4 Chứng thư số

Chứng thư số là một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số (Certification Authority) cấp nhằm cung cấp thông tin định danh cho khóa công khai của một cơ quan, tổ chức, cá nhân, từ đó xác nhận cơ quan, tổ chức, cá nhân là người ký chữ ký số bằng việc sử dụng khóa bí mật tương ứng.

Chứng thư X.509 phiên bản 3 có những thông tin sau:

- Chủ thể (subject) của chứng thư: thông tin về người dùng, máy tính, thiết bị mạng giữ khóa bí mật tương ứng với chứng thư được cấp phát.
- Tên dịch vụ chứng thực chữ ký số: thông tin về tổ chức cung cấp chứng thư.
- Khóa công khai tương ứng với khóa bí mật được liên kết với chứng thư.



Hình 2.4: Cấu trúc chứng thư số X.509 phiên bản 3

- Tên của các thuật toán để mã hóa và thuật toán tạo chữ ký số cho chứng thư.
- Trạng thái thu hồi (revocation) và tính hiệu lực của chứng thư (như ngày phát hành và ngày hết hạn).
- Các phần mở rộng (extension) cho loại chứng chỉ X.509 version 3.

2.3 Công nghệ Blockchain

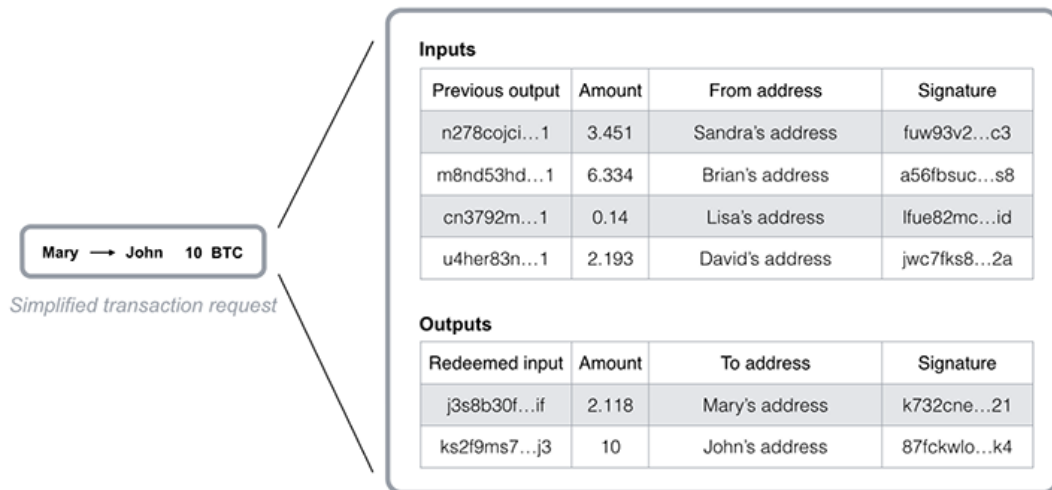
Giới thiệu các nền tảng blockchain như Bitcoin, ethereum, hyperledger fabric, bigchaindb.

Phân tích các ưu khuyết điểm của các nền tảng này.

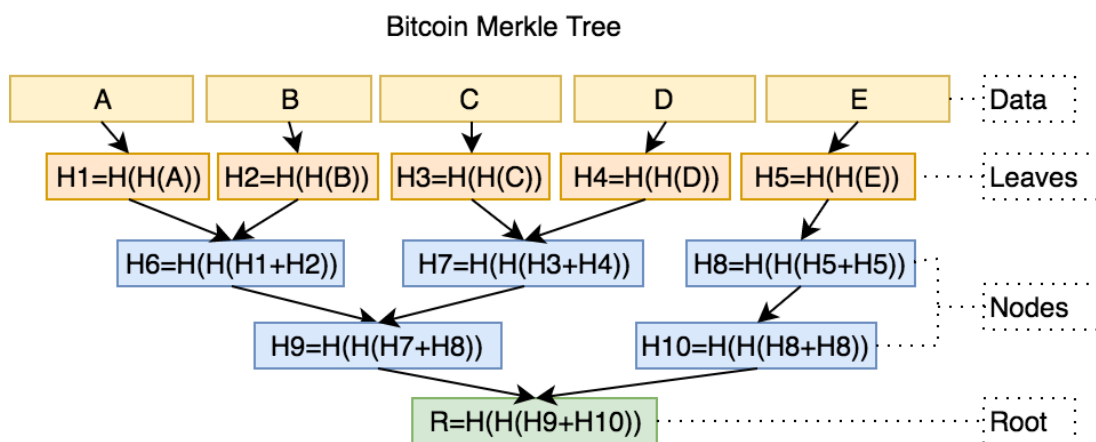
Công nghệ Blockchain được hình thành vào năm 2008 theo ý tưởng của Satoshi Nakamoto và trở thành cơ chế hoạt động của tiền điện tử Bitcoin [3]. Công nghệ này đóng vai trò như một quyển sổ cái ghi lại tất cả giao dịch công khai trên hệ thống máy tính ngang hàng theo phương thức mã hoá các giao dịch. Từ đó, các giao dịch phát sinh mà không cần các tổ chức trung gian, tạo ra giải pháp cho các ứng dụng cần sự minh bạch, tính trách nhiệm, bảo mật cao và giảm thiểu các quy trình thủ tục phức tạp. Công nghệ blockchain đang được nghiên cứu và ứng dụng vào nhiều lĩnh vực quan trọng trong giáo dục, dịch vụ công, y tế tại nhiều nước trên thế giới.

Công nghệ này mang đặc điểm của cơ sở dữ liệu phân tán. Tuy nhiên, mỗi khối gồm nhiều giao dịch được ký số bởi các bên tham gia như hình 2.5. Dữ liệu trong các khối

được liên kết với nhau bằng mã hóa (giá trị băm) như hình 2.6 và mở rộng theo thời gian. Mỗi khối được tạo ra đều chứa thông tin thời gian khởi tạo và liên kết với khối trước đó kèm một mã thời gian và thông tin giao dịch như hình 2.7. Vì thế, blockchain được thiết kế để chống lại sự thay đổi của dữ liệu. Khi dữ liệu đã lưu trữ trên mạng blockchain thì sẽ khó thay đổi được và nếu được cập nhật sẽ được lưu vết dưới dạng nhật ký.



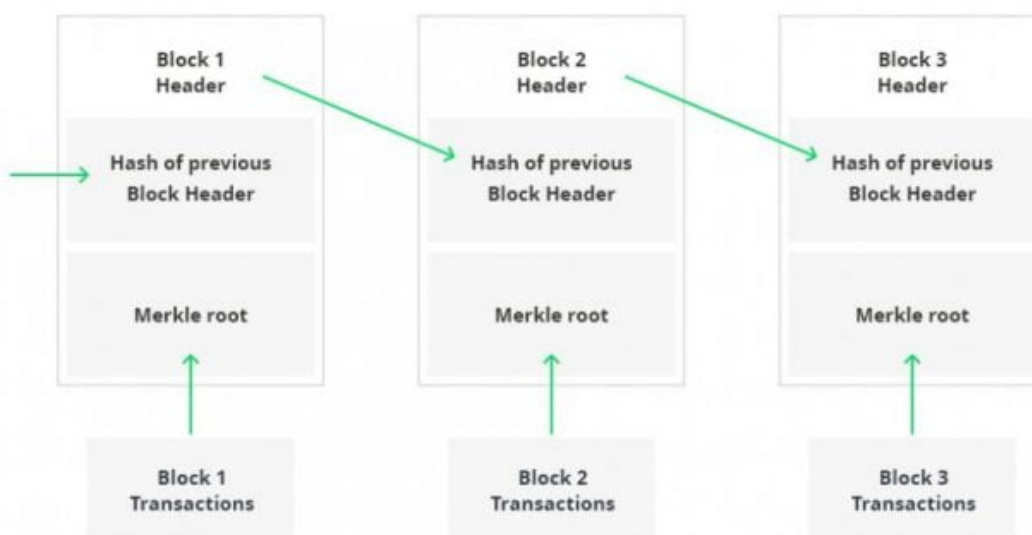
Hình 2.5: Mô tả một giao dịch blockchain



Hình 2.6: Mô tả cây mã hóa Merkle trong Bitcoin

Blockchain xác nhận giao dịch bằng hợp đồng thông minh. Hợp đồng thông minh là các chương trình chạy trên blockchain. Hợp đồng thông minh cũng giống như một hợp đồng kỹ thuật số bị bắt buộc thực hiện bởi một bộ quy tắc cụ thể. Các quy tắc này được lập trình trước và tất cả các nút (node) trong mạng đều phải sao chép và thực thi các quy tắc đó.

Hệ thống mạng blockchain có thể được chia làm 3 nhóm. (1) Nhóm hệ thống blockchain công cộng cho phép mọi người dùng có thể truy cập dữ liệu như Bitcoin, Ethereum,... (2) Nhóm hệ thống blockchain riêng tư do một tổ chức hoặc một cá nhân đầu tư và kiểm soát, thông tin được kiểm soát chặt chẽ và chỉ được phổ biến trong nội



Hình 2.7: Mô tả chuỗi Blockchain

bộ. (3) Nhóm còn lại là hệ thống blockchain cộng đồng là hiệp hội các tổ chức có thể xây dựng riêng mạng cho các thành viên của mình theo nguyên lý blockchain, cơ chế đồng thuận trong cộng đồng phát triển theo xu hướng tin cậy theo đa số trong cộng đồng. Mỗi hệ thống blockchain có những đặc điểm riêng và được ứng dụng trong từng lĩnh vực cụ thể.

2.4 Hyperledger Fabric

2.4.1 Giới thiệu

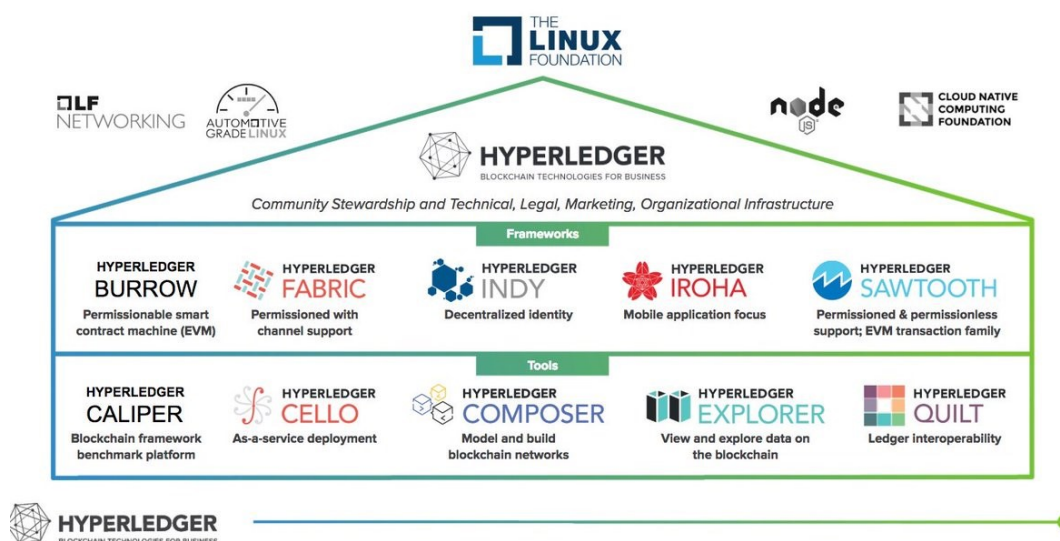
Hyperledger Fabric là một nền tảng blockchain trong dự án Hyperledger của tổ chức Linux Foundation gồm: Hyperledger Indy, Hyperledger Fabric, Hyperledger Iroha, Hyperledger Sawtooth, Hyperledger Burror. Hình 2.8 mô tả dự án Hyperledger.

Hyperledger Fabric thuộc nhóm phần mềm mã nguồn mở dưới sự cố vấn của công ty IBM. Mục đích thiết kế Hyperledger Fabric là cung cấp rộng rãi nền tảng ứng dụng blockchain cho các tổ chức, doanh nghiệp. Hyperledger Fabric có nhiều tính năng nổi trội so với các nền tảng blockchain phổ biến như Bitcoin, Ethereum. Hyperledger Fabric có kiến trúc mô-đun linh hoạt và tối ưu hoá cho nhiều ứng dụng trong các lĩnh vực như: tài chính, bảo hiểm, y tế, chuỗi cung ứng, hành chính công, ...

Nhờ vào thiết kế mô-đun linh hoạt và quản lý người tham gia nên Hyperledger Fabric trở thành nền tảng blockchain có tốc độ xử lý giao dịch nhanh và phù hợp với tổ chức muốn kiểm soát danh tính người tham gia, và xác minh các giao dịch với hợp đồng thông minh.

Phiên bản mới nhất của Hyperledger Fabric là 2.x. Hyperledger Fabric được cộng đồng hỗ trợ các vấn đề bảo mật, cập nhật. Hệ thống sẽ được cập nhật cho đến khi một phiên bản LTS mới được phát hành.

Trong phiên bản Fabric 2.x, các hợp đồng thông minh (smart contract) được cài đặt



Hình 2.8: Dự án Hyperledger

trên các peer tham gia chung channel và được đánh số các phiên bản. Các tổ chức thuộc kênh (channel) đồng ý các tham số của hợp đồng thông minh, chứng thực hợp đồng thông minh sau đó hợp đồng thông minh mới thực hiện tương tác với sổ cái (ledger).

Việc nâng cấp các hợp đồng thông minh (smart contract) sẽ được gắn với quá trình đồng thuận và được các nút mạng đồng ý. Khi đó các peer có đầy đủ các hợp đồng thông minh (chaincode được cài đặt). Việc thay đổi cơ chế nâng cấp hợp đồng thông minh trên phiên bản 2.x mang lại tính an toàn, đồng nhất dữ liệu so với phiên bản trước.

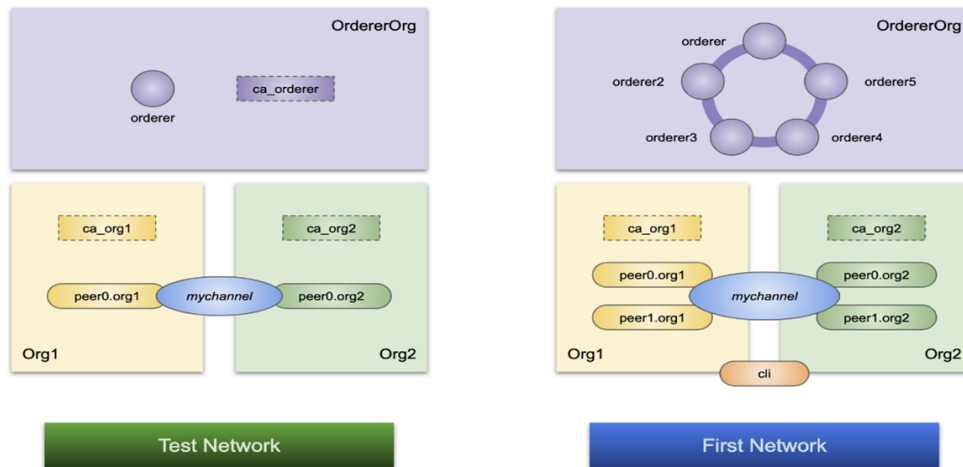
Dữ liệu riêng tư (Data Privacy) cho phép một phần dữ liệu được chia sẻ riêng tư giữa một số thành viên thuộc kênh thay vì tất cả thành viên đều có thể sở hữu. Thay vì tạo thêm một kênh để nhóm các thành viên và mất rất nhiều thời gian để cấu hình (kênh, chính sách, MSP,...)

Hyperledger Fabric 2.x có hiệu suất xử lý giao dịch đến hàng nghìn giao dịch mỗi giây. Một trong những điểm nổi bật của phiên bản Fabric 2.x là tối ưu hóa hiệu suất hoạt động của mạng Blockchain. Các giải thuật đồng thuận gồm có: Kafka, Raft. Các thực giao dịch được xử lý song song, xử lý khối bất động bộ, phân trang chaincode,....

2.4.2 Các thành phần của Hyperledger Fabric

Ledger: Một quyển sổ cái bao gồm 2 thành phần có liên quan nhau là “chuỗi khối” và “cơ sở dữ liệu trạng thái”. Các giao dịch thay đổi các tài sản (dữ liệu trong mạng blockchain) của mạng sẽ được “chuỗi khối” ghi nhận theo dạng nhật ký và không thể xóa hay chỉnh sửa. Ngược lại, “cơ sở dữ liệu trạng thái” (cơ sở dữ liệu LevelDB hoặc CouchDB) lưu trạng thái mới nhất của các tài sản hiện có trong mạng theo cặp khóa-giá trị (key-value). Toàn bộ ledger được lưu trên các Peer trong cùng Channel, và dữ liệu được đồng bộ khi có phát sinh giao dịch thông qua cơ chế đồng thuận.

Smart contract (Chaincode): Hợp đồng thông minh trong blockchain là các ứng



Hình 2.9: Kiến trúc mạng Hyperledger Fabric

dùng được lập trình bằng ngôn ngữ lập trình như: Javascript, Go, Java. Hợp đồng thông minh tương tác với mạng, quản lý tài sản. Trong Hyperledger Fabric, các hợp đồng thông minh còn được gọi là chaincode, được cài đặt trên các Peer.

Peer nodes: Là những nút cơ bản của mạng có chức năng lưu trữ bản sao của Ledgers và thực thi Hợp đồng thông minh. Các peer được quản lý và duy trì bởi các thành viên trong mạng. Peer được chia làm 2 dạng:

- **Endorsing peer:** thực thi các giao dịch trong chaincode và đề xuất giao dịch.
- **Committing peer:** có thể không cần cài đặt chaincode, lưu trữ sổ cái đầy đủ.

Ordering Service (Solo, Raft, Kafka): Là những nút chứa thuật toán đồng thuận và đảm nhận nhiệm vụ xác minh, bảo mật, kiểm định phân quyền, quản lý cấu hình Channel.

Channel: Kênh là một “mạng con” riêng kết nối giữa hai hoặc nhiều nút trong mạng blockchain. Mỗi kênh sẽ kết nối các nút như Orgs(tổ chức), Peer, Ordering service, MSP. Mỗi Peer có thể tham gia nhiều kênh và sẽ được cấp các định danh riêng với từng kênh bởi dịch vụ xác thực thành viên (MSP).

Fabric Certificate Authorities: Hyperledger Fabric CA là thành phần phát hành chứng thư số. Chứng thư số được cấp dựa trên hạ tầng khóa công khai PKI cho các nút trong mạng và người dùng. CA phát hành một chứng thư gốc (rootCert) cho mỗi thành viên và một chứng nhận đăng ký (ECert) cho mỗi người dùng được ủy quyền.

Membership Service Provider (MSP): MSP là dịch vụ xác minh các nút trong mạng, thông qua chứng thư số (cấp từ CA). Do đó HyperLedger Fabric có thể xác thực các thực thể kết nối với mạng thông qua danh tính (Identities) mà không cần khóa bí mật. Ngoài ra, nó còn có vai trò xác định quyền truy cập trong phạm vi mạng và kênh của một thành phần nào đó trong mạng.

Bổ túc kiến trúc

CHƯƠNG 3

XÂY DỰNG HỆ THỐNG

3.1 Tổng quan giải pháp

Problem Statement Every school/university around has its way of managing or maintaining its student records and transcripts. Of course, many of them usually do not share student information, such as transcripts for privacy reasons. Typically, in the case of international students, when one student tries for an admission in a foreign country, the student must get his transcripts evaluated by a third-party evaluator such as WES, an International evaluator.

For one reason, if somehow these transcripts are in a foreign language, there needs a translator and, most of the time requires to approach a third-party evaluator. When a person had started applying for a university in the United States, The university required him to first apply all the transcripts from his school and then had them evaluate through an external evaluator to match the grading system between the two countries, and it takes an average of 2-3 weeks to get the evaluation report. Table 1 is the third-party evaluator's cost summary. So, a cryptographic database solution for recording the academic certificates will help to solve all these issues. By making all the official and unofficial transcripts of the student store in a blockchain, which are accessible through all over the world and can share to any Employer or a University And the transcripts stored on a blockchain system are immutable, therefore preserves the integrity of data.

Objective of the Study To develop an application on a blockchain framework, which is a role-based access system, takes inputs and stores all the changes performed on it, which supports an authentication system and high scalability.

Hệ thống quản lý VBCC sử dụng công nghệ blockchain có các chức năng: cấp, quản lý và xác minh VBCC một cách an toàn, bảo mật. Giải pháp được thử nghiệm với nền tảng kỹ thuật số của IBM Blockchain Flatform, Hyperledger Fabric. VBCC có thể được xác thực với tùy chọn hạn chế tiết lộ thông tin và không cần sự can thiệp từ tổ chức cấp chứng chỉ (Trường/Trung tâm).

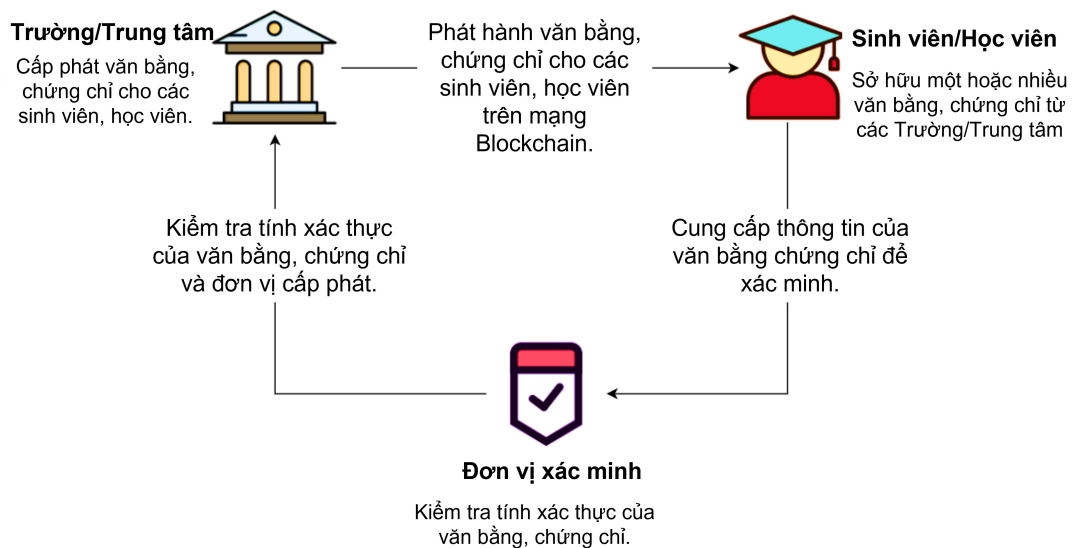
Những chức năng chính của hệ thống được mô tả như hình 3.1 bao gồm:

- Trường/Trung tâm: ký số và cấp VBCC.
- Sinh viên: xem và chia sẻ VBCC.
- Đơn vị xác minh: kiểm tra tính xác thực của các VBCC được chia sẻ.

3.2 Kiến trúc phần mềm

Kiến trúc phần mềm được mô tả như hình 3.2 bao gồm các thành phần:

1. Mạng Blockchain Hyperledger Fabric: IBM Blockchain Flatform và Docker container hỗ trợ xây dựng mạng blockchain Fabric, thực thi các hợp đồng thông minh (ngôn ngữ Javascript).



Hình 3.1: Sơ đồ tổng quan giải pháp

2. Fabric CA: được dùng để đăng ký và xác thực các thành phần trong mạng.
3. Webserver: sử dụng Node.js cung cấp giao diện Backend của ứng dụng web, kết hợp sử dụng Nodejs Express.
4. Cơ sở dữ liệu MongoDB: lưu trữ dữ liệu người dùng và chứng chỉ.
5. Giao diện Front-end của ứng dụng web: dùng các thư viện Bootstrap, jQuery.

3.3 Các thành phần tham gia

Các thành phần tham gia của hệ thống bao gồm: (1) Trường, Trung tâm, (2) Sinh viên (học viên) và (3) Bên xác minh chứng chỉ (Ví dụ: nhà tuyển dụng). Mỗi thành phần sẽ có các hành động như sau:

Trường, trung tâm

- Đăng ký tài khoản.
- Đăng nhập tài khoản.
- Cấp VBCC có xác nhận chứng thực và ký số VBCC.
- Xem VBCC đã cấp.

Sinh viên, học viên

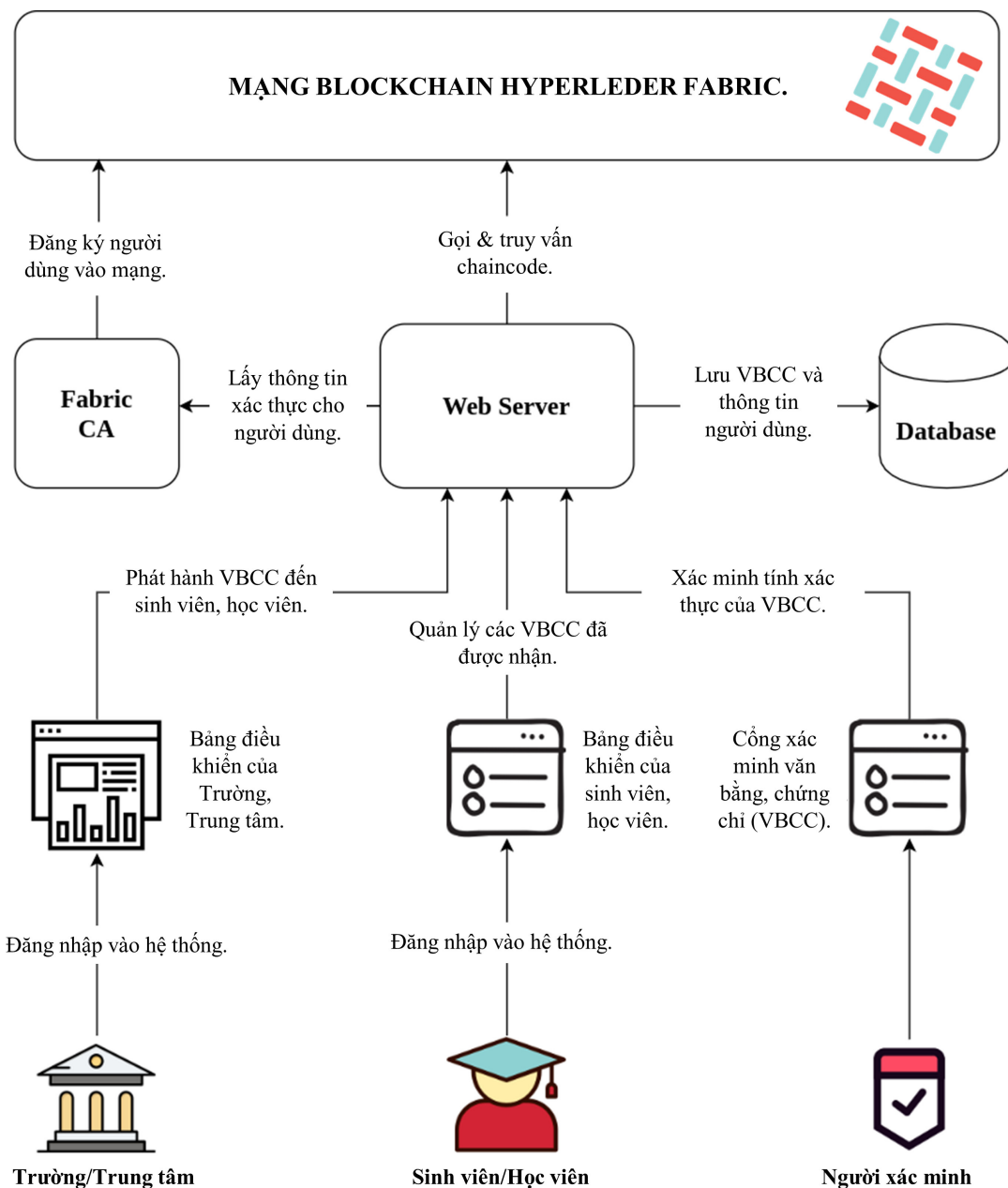
- Đăng ký tài khoản.
- Đăng nhập tài khoản.
- Xem VBCC đã nhận.
- Chia sẻ thông tin VBCC.
- Tiết lộ thông tin VBCC có chọn lọc nhằm hạn chế lộ thông tin.

Bên xác minh chứng chỉ

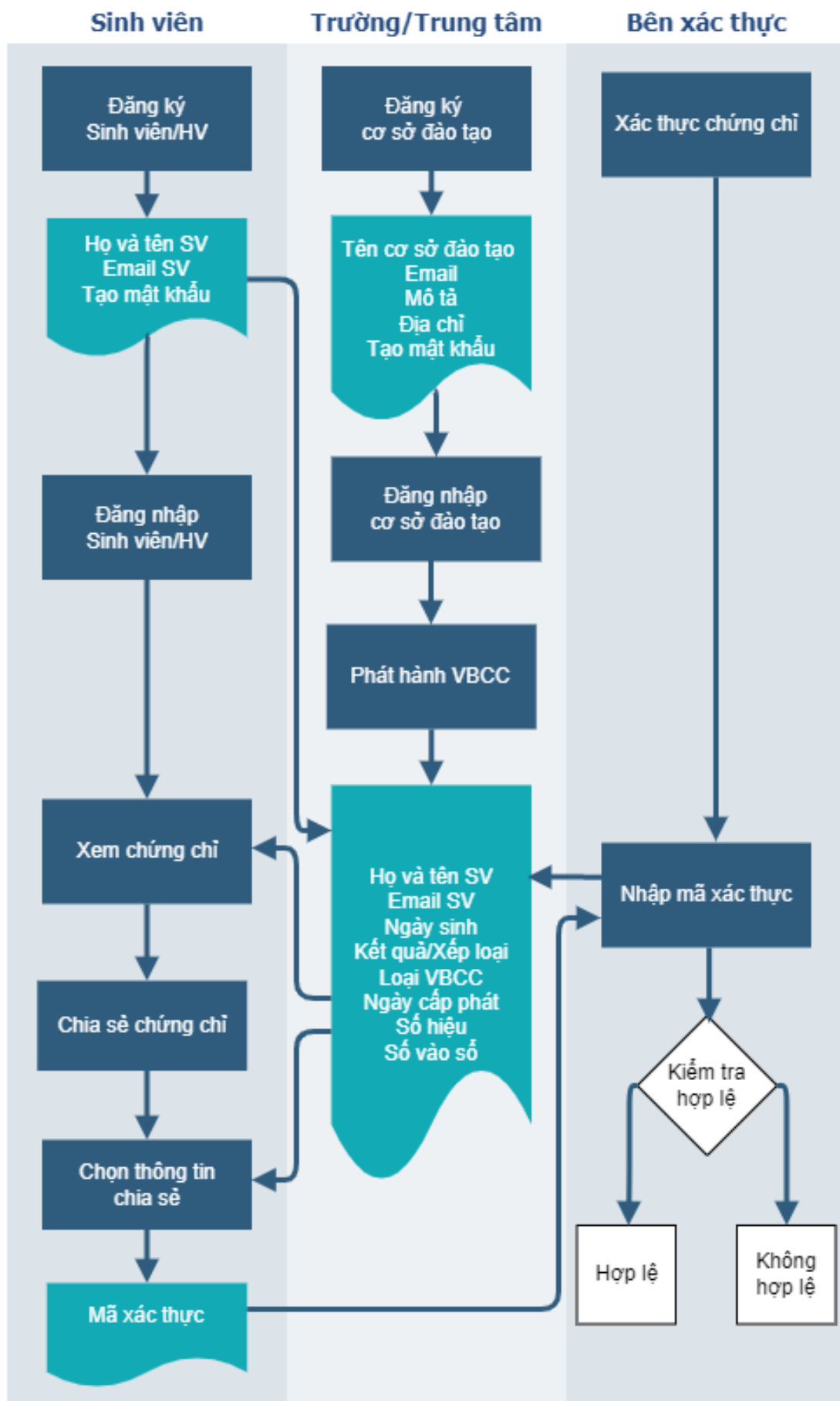
- Xác minh tính xác thực của VBCC với nền tảng blockchain.

Quy trình hoạt động của hệ thống được mô tả như hình 3.3

Mô tả quy trình hoạt động



Hình 3.2: Sơ đồ kiến trúc phần mềm



Hình 3.3: Quy trình hoạt động của hệ thống

3.3.1 Mô tả usecase

3.3.2 Thiết kế cơ sở dữ liệu

3.3.3 Thiết kế mạng blockchain

Mô tả các asset

Mô tả smartcontract

Mô tả cài mạng Hyperledger Fabric

CHƯƠNG 4

KẾT QUẢ THỰC NGHIỆM

4.1 Môi trường thực nghiệm

4.1.1 Mạng blockchain

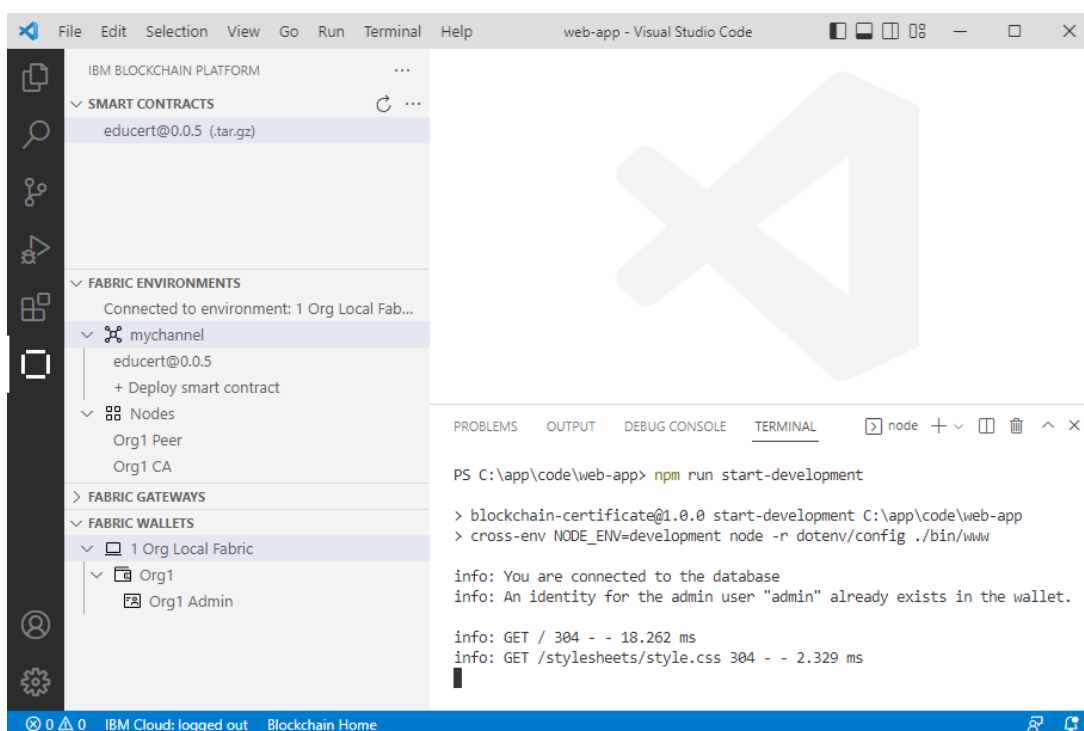
Cài môi trường phát triển hệ thống

Sơ đồ mạng blockchain gồm có 1 tổ chức Org1 trong đó có 1 peer, 1 CA, và 1 Order, 1 OrdererMSP, 1 Org1MSP

Môi trường thử nghiệm được thiết lập theo các bước sau:

1. Cài đặt môi trường phát triển hệ thống.
2. Mở Visual Studio Code và cài plugin IBM Blockchain Flatform, Fabric Enviroment.
3. Khởi tạo mạng eCert, chaincode của hệ thống được chạy trên mạng eCert, kênh an toàn trong tổ chức được khởi tạo, các peer tham gia vào kênh, đăng ký quyền Admin.
4. Khai báo thông số kết nối MongoDB với mạng Fabric trên máy tính.
5. Khởi động server Nodejs.

Môi trường mạng hiển thị trong chương trình Visual Studio Code như hình 4.1



Hình 4.1: Chương trình Visual Studio Code

Mạng blockchain triển khai thử nghiệm

4.1.2 Môi trường ứng dụng web

4.1.3 Phần cứng

Hệ thống quản lý VBCC sử dụng công nghệ blockchain đã được triển khai thử nghiệm trên máy tính có cấu hình như sau:

- CPU: Intel(R) Core(TM) i3-10100F 3.00 GHz
- RAM: 16 GB
- Hard Disk: 120 GB NVME SSD

4.1.4 Phần mềm

- Hệ điều hành: Windows 10
- Docker Desktop: phiên bản 4.13.0
- Môi trường Nodejs: 12.22.12
- Trình soạn thảo: Visual Studio Code 1.71
- Các phần mở rộng của Visual Code: IBM Blockchain Platform
- Cơ sở dữ liệu MongoDB: 1.33.1
- Các phần mềm bổ sung: git, python, npm, ...

4.2 Kết quả thực nghiệm

Sau khi hệ thống quản lý VBCC được khởi động như hình 4.1. Giao diện chính có địa chỉ <http://localhost:3000/> như hình 4.2.

Trường, trung tâm có các màn hình chức năng như sau:

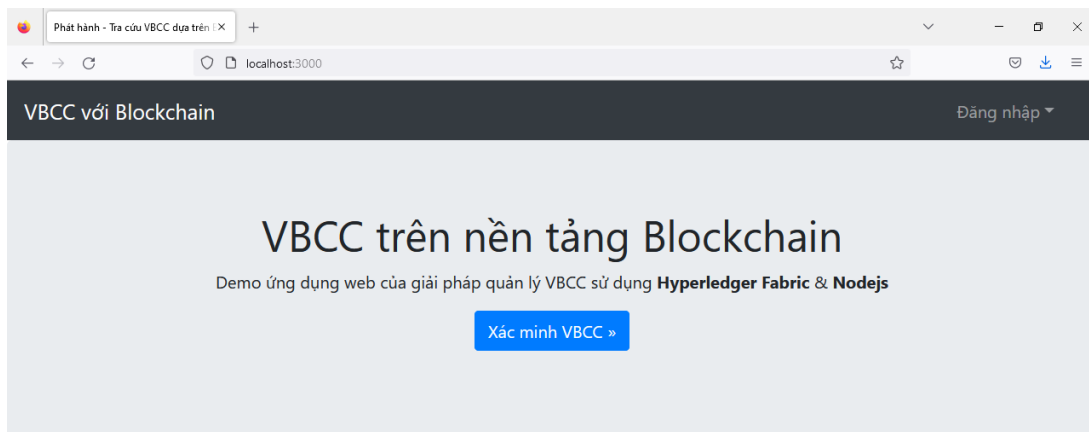
- Đăng ký tài khoản.
- Đăng nhập tài khoản.
- Cấp VBCC có xác nhận chứng thực và ký số VBCC, như hình 4.3
- Xem VBCC đã cấp, như hình 4.4

Sinh viên, học viên có các màn hình chức năng như sau:

- Đăng ký tài khoản, như hình 4.5
- Đăng nhập tài khoản.
- Xem VBCC đã nhận, như hình 4.6
- Chia sẻ thông tin VBCC, như hình 4.8
- Tiết lộ thông tin VBCC có chọn lọc nhằm hạn chế lộ thông tin, như hình 4.7

Bên xác minh chứng chỉ có màn hình chức năng như sau:

- Xác minh tính xác thực của VBCC với nền tảng blockchain, như hình



Sinh viên/Học viên

Sinh viên, học viên có thể sử dụng nền tảng này để quản lý và chia sẻ các VBCC của họ.

Đăng nhập »

Đăng ký »

Trường đại học/Trung tâm

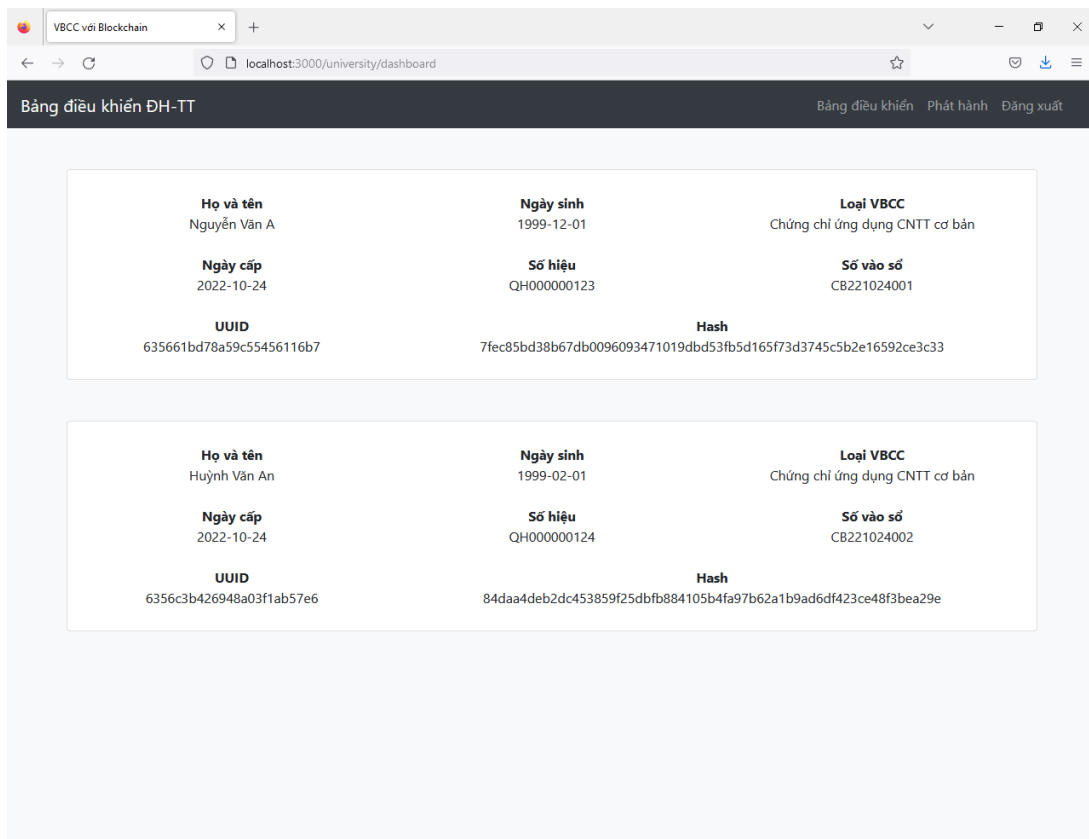
Các trường đại học và trung tâm có thể sử dụng nền tảng này để phát hành VBCC đến các sinh viên, học viên của họ.

Đăng nhập »

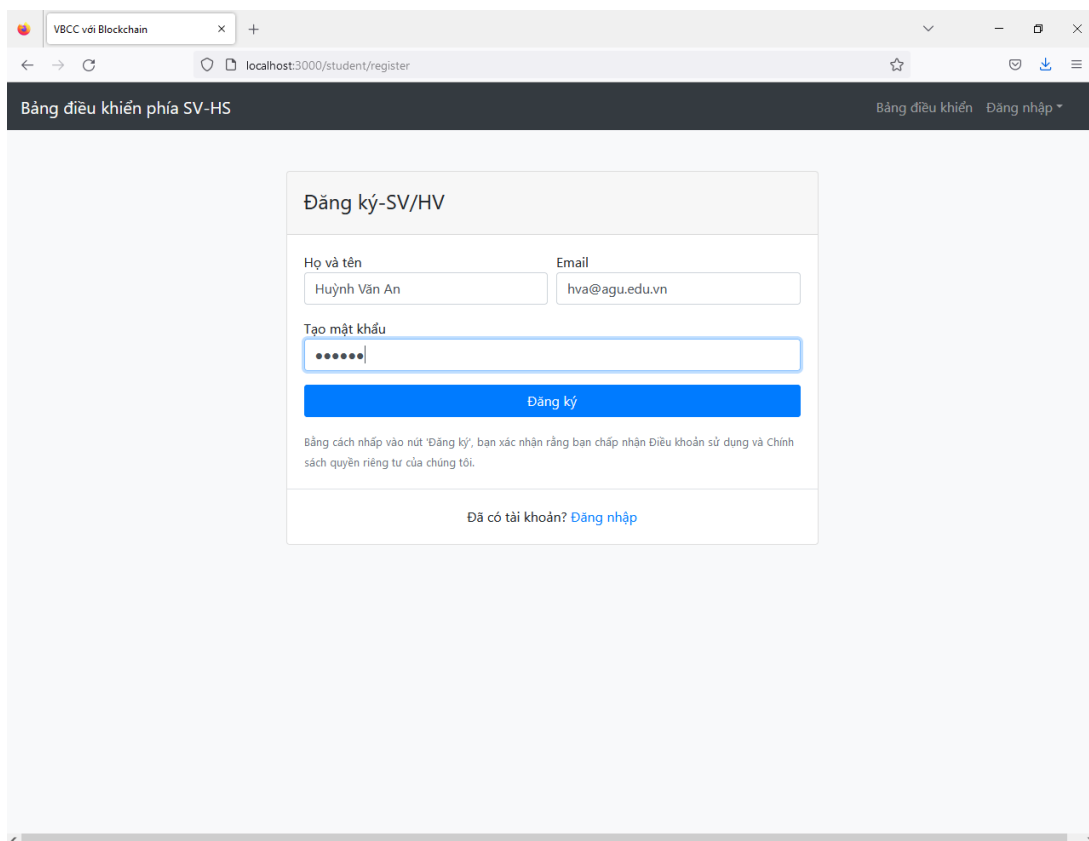
Đăng ký »

Hình 4.2: Giao diện hệ thống

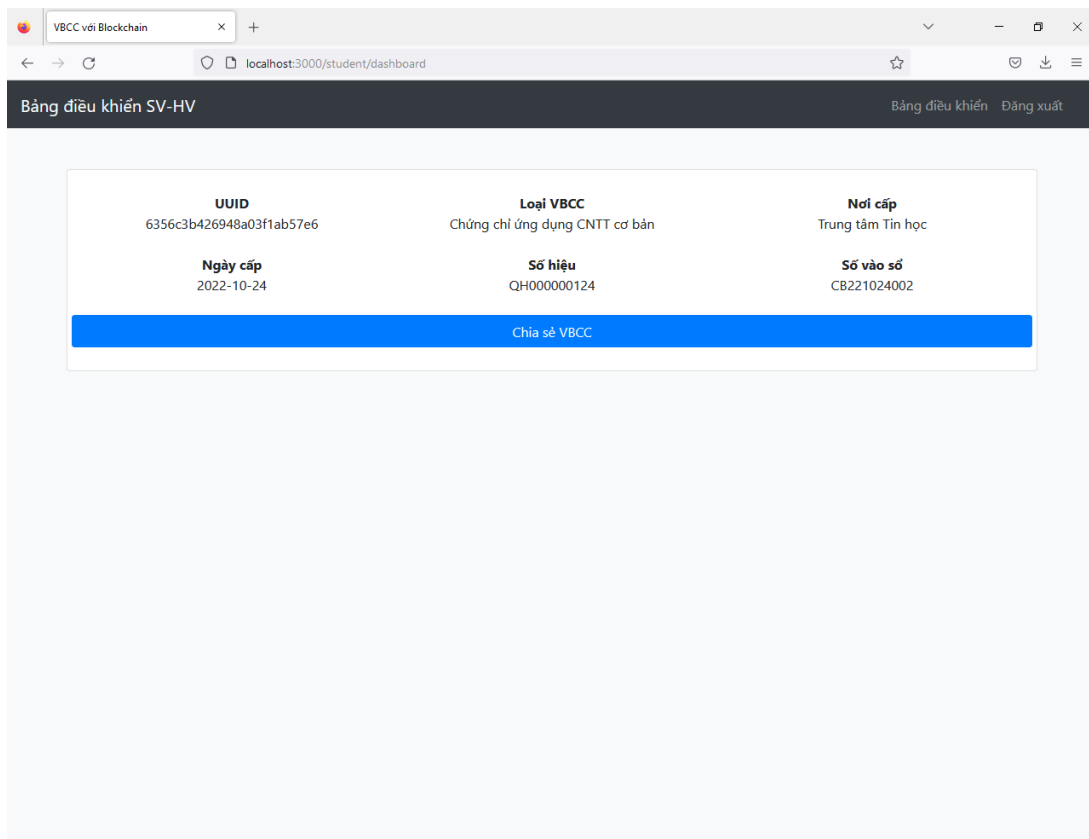
Hình 4.3: Màn hình cấp chứng chỉ cho sinh viên



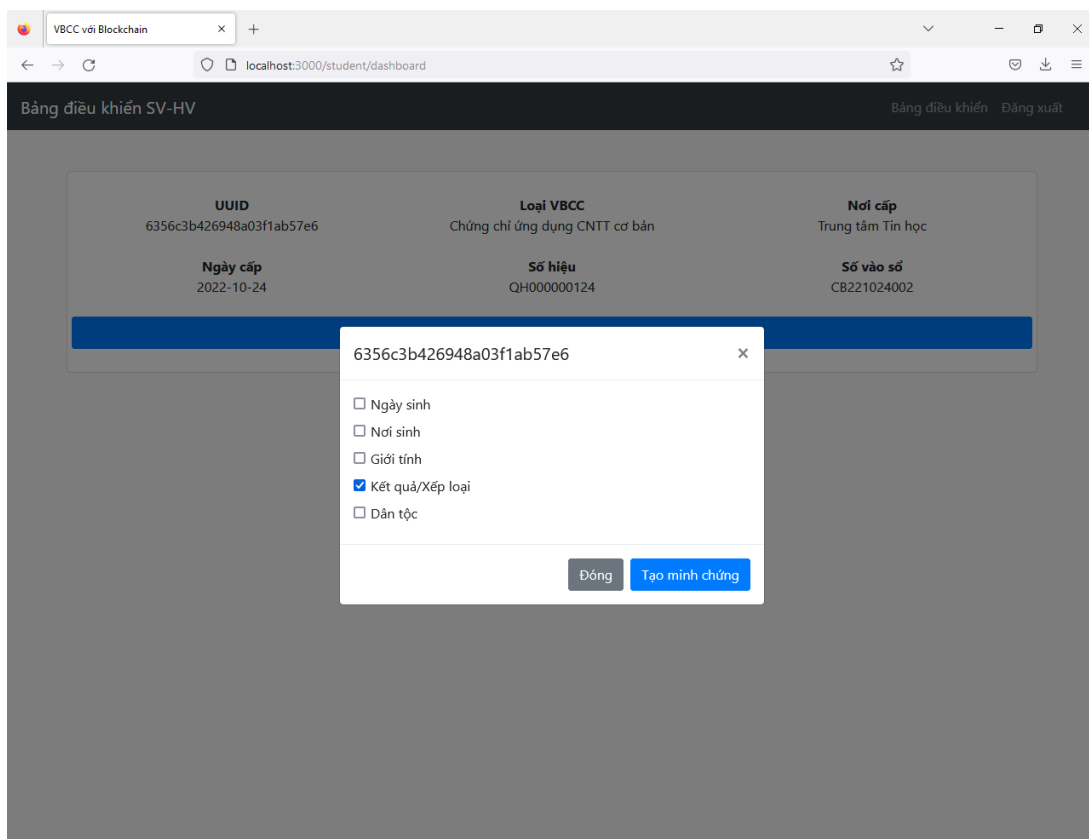
Hình 4.4: Màn hình các chứng chỉ đã cấp



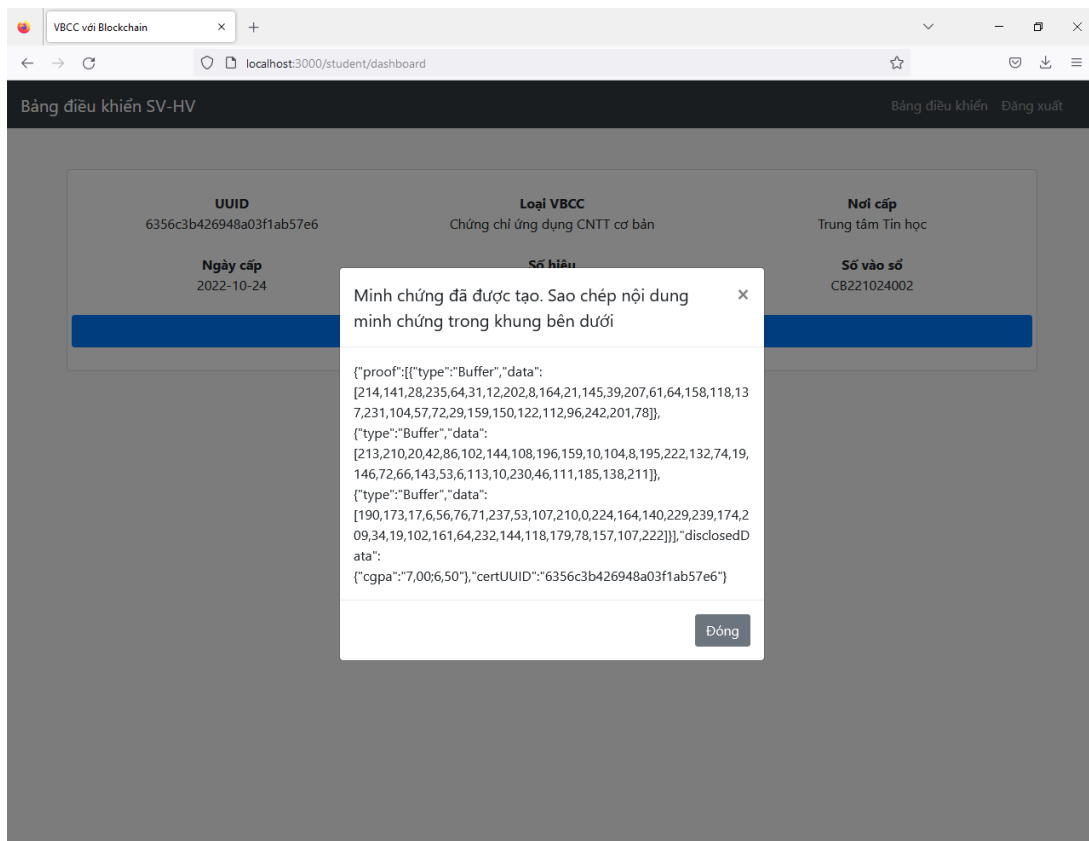
Hình 4.5: Màn hình đăng ký tài khoản sinh viên



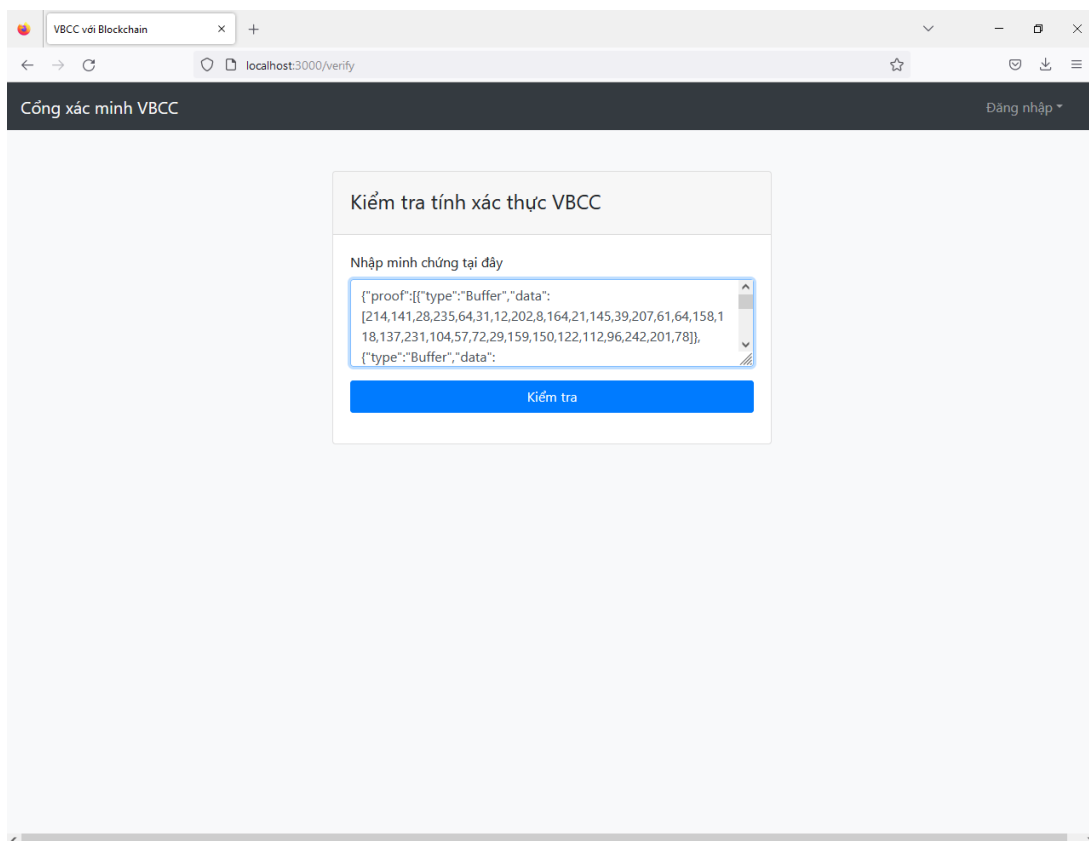
Hình 4.6: Màn hình xem các chứng chỉ đã được cấp



Hình 4.7: Màn hình chia sẻ thông tin sinh viên



Hình 4.8: Màn hình hiển thị mã xác thực chứng chỉ



Hình 4.9: Màn hình nhập mã xác thực chứng chỉ

CHƯƠNG 5

KẾT LUẬN

Qua quá trình nghiên cứu, cùng với sự giúp đỡ tận tình của giáo viên hướng dẫn, luận văn đã cơ bản hoàn thành được mục tiêu nghiên cứu, bao gồm một số kết quả sau đây:

1. Tìm hiểu nghiệp vụ quản lý và văn bản pháp lý về việc quản lý VBCC hiện hành theo quy định của pháp luật và tại Trung tâm Tin học Trường Đại học An Giang; Nghiên cứu tổng quan cơ sở lý thuyết mật mã, công nghệ blockchain và mô hình mạng Hyperledger Fabric.
2. Xây dựng website tương tác với người sử dụng trong việc cấp phát và xác thực chứng chỉ.
3. Xây dựng mạng Hyperledger Fabric để triển khai lưu trữ dữ liệu nhật ký về VBCC trên mạng này.

Hạn chế của đề tài

Hạn chế của đề tài là chỉ dùng chứng thư số nội bộ của Hyperledger Fabric. Phạm vi nghiên cứu giới hạn gồm 3 bên tham gia: đơn vị cấp, bên xác minh và sinh viên. Tuy nhiên, cài đặt máy chủ cấp chứng thư số ở ngoài thực tế là công việc phức tạp và liên quan nhiều vấn đề bảo mật an toàn thông tin cần được quan tâm kỹ lưỡng.

Ngoài ra, dữ liệu nhập vào chuỗi khối đòi hỏi thông tin chính xác và tin cậy. Do đó đề tài cần tiếp tục hoàn chỉnh nghiên cứu ứng dụng công nghệ blockchain trong quy trình tổ chức thi từ ban đầu đến khi cấp chứng chỉ. Thông tin cần được theo dõi khách quan, đảm bảo tin cậy cho người có VBCC, cơ quan quản lý và các tổ chức có liên quan.

Định hướng nghiên cứu tiếp theo

Ngoài những hạn chế trên, chắc chắn đề tài còn có nhiều thiếu sót. Do đó, đề tài sẽ tiếp tục việc nghiên cứu, cải tiến sau: (1) Nghiên cứu các thành phần của Hyperledger Fabric để ứng dụng nhiều tính năng hơn do nền tảng này cung cấp. (2) Nghiên cứu mở rộng các quy trình trong công tác tổ chức thi, liên quan đến cấp chứng chỉ. (3) Cải tiến giao diện người dùng giúp thuận tiện trong quản lý VBCC.

TÀI LIỆU THAM KHẢO

- [1] Ralph Charles Merkle (1979), “Secrecy, authentication, and public key systems”. Báo cáo kỹ thuật.
- [2] Lê Quyết Thắng (2016), *Bài giảng Lý thuyết mật mã* (ĐH Cần Thơ).
- [3] Satoshi Nakamoto (2008), “Bitcoin: A peer-to-peer electronic cash system”. *Decentralized Business Review*, tr. 21260.
- [4] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco và Jason Yellick (2018), “Hyperledger fabric: A distributed operating system for permissioned blockchains”. Trong “Proceedings of the Thirteenth EuroSys Conference”, EuroSys ’18 (Association for Computing Machinery, New York, NY, USA), ISBN 9781450355841, doi:10.1145/3190508.3190538, URL <https://doi.org/10.1145/3190508.3190538>.
- [5] McSeth Antwi, Asma Adnane, Farhan Ahmad, Rasheed Hussain, Muhammad Habib ur Rehman và Chaker Abdelaziz Kerrache (2021), “The case of hyperledger fabric as a blockchain solution for healthcare applications”. *Blockchain: Research and Applications*, tập 2, số 1, tr. 100.012, ISSN 2096-7209, doi:<https://doi.org/10.1016/j.b cra.2021.100012>, URL <https://www.sciencedirect.com/science/article/pii/S2096720921000075>.
- [6] Trương Minh Tuyên, Nguyễn Hoàng Tùng, Lê Hoàng Anh và Nguyễn Văn Hòa (2019 jun), “Giải pháp quản lý tài sản ngăn chặn bằng công nghệ blockchain”. Trong “Kỷ yếu Hội nghị Quốc gia lần thứ 12 về Nghiên cứu cơ bản và ứng dụng Công Nghệ thông tin (FAIR)”, .
- [7] T. Dinh, R. Liu, M. Zhang, G. Chen, B. Ooi và J. Wang (2018 jul), “Untangling blockchain: A data processing view of blockchain systems”. *IEEE Transactions on Knowledge and Data Engineering*, tập 30, số 07, tr. 1366–1385, ISSN 1558-2191, doi:10.1109/TKDE.2017.2781227.
- [8] Weidong Fang, Wei Chen, Wuxiong Zhang, Jun Pei, Weiwei Gao và Guohui Wang (2020 Mar), “Digital signature scheme for information

non-repudiation in blockchain: a state of the art review”. *EURASIP Journal on Wireless Communications and Networking*, tập 2020, số 1, tr. 56, ISSN 1687-1499, doi:10.1186/s13638-020-01665-w, URL <https://doi.org/10.1186/s13638-020-01665-w>.

- [9] Christof Paar (2015 apr), *Implementation of Cryptographic Schemes 1* (Ruhr University Bochum).
- [10] C. Shannon (1949 Oktober), “Communication theory of secrecy systems”. *Bell System Technical Journal*, Vol 28, pp. 656–715.
- [11] Jian Chen, Zhihan Lv và Houbing Song (2019), “Design of personnel big data management system based on blockchain”. *Future Generation Computer Systems*, tập 101, tr. 1122–1129, ISSN 0167-739X, doi:<https://doi.org/10.1016/j.future.2019.07.037>, URL <https://www.sciencedirect.com/science/article/pii/S0167739X19313354>.
- [12] H. Kopka và P. W. Daly, *A Guide to LaTeX* (Addison-Wesley, Reading, MA).
- [13] Phạm Nguyên Khang (2013), *Giáo trình An toàn và bảo mật thông tin* (ĐH Cần Thơ).
- [14] Đỗ Thanh Nghị (2018), *Bài giảng Phát hiện tấn công mạng* (ĐH Cần Thơ).
- [15] Christof Paar và Jan Pelzl (2009), *Understanding Cryptography: A Textbook for Students and Practitioners* (Springer Publishing Company, Incorporated), 1st edition, ISBN 3642041000.