BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC CẦN THƠ

DƯƠNG TUẤN DŨNG

XÂY DỰNG HỆ THỐNG QUẢN LÝ VĂN BẰNG 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 BẰNG 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 đối chiếu 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 với tùy chọn chia sẻ thông tin cá nhân 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 với tùy chọn hạn chế 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 specific 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.

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

DANH SÁCH BẢNG

DANH SÁCH HÌNH VẼ

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
DLT	Decentralized Ledger Technology
ABCI	Application BlockChain Interface
HF	Hyperledger Fabric

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 được xem là dữ liệu gốc bao gồm các VBCC được in lên mẫu phôi và những 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, BigchainDB. Trong những công nghệ blockchain này, ứng dụng của hợp đồng thông minh trên nền tảng Hyperledger Fabric 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.

Lĩnh vực an toàn thông tin có các ứng dụng giúp dữ liệu trên blockchain được toàn

vẹn, chống làm giả. Nghiên cứu [1] của Ralphe Charles Merkle về ứng dụng hệ mật mã khóa công khai trong an toàn thông tin. Theo đó, 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. Còn trong các hệ mật mã khóa công khai, mỗi bên tham gia tạo một cặp khóa. Trong đó mỗi cặp khóa, có một khóa công bố công khai cho tất cả và một khóa riêng tư được mỗi bên giữ bí mật. Khóa công khai có liên kết về mặt toán học 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 Lý thuyết mật mã[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-Helmann, ElGamma 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 và chăm sóc sức khỏe, nghiên cứu [3] trình bày giải pháp ứng dụng công nghệ blockchain riêng tư trong quản lý và bảo vệ quyền sở hữu thông tin sức khỏe của bệnh nhân. Những thông tin này quan trọng đối với người bệnh, nhà thuốc, công ty bảo hiểm và nhà nghiên cứu. Do đó, thông tin này cần được quan tâm tránh rò rỉ khi chia sẻ thông tin người bệnh. Nghiên cứu chỉ ra rằng Hyperledger Fabric có thể đáp ứng về tính an toàn, dễ mở rộng, tuân thủ luật pháp và linh hoạt trong quản lý thông tin sức khỏe của bệnh nhân.

Trong lĩnh vực giáo dục, các nước trên thế giới và Việt Nam đang đẩy mạnh số hóa thông tin đào tạo. Trong đó, công nghệ blockchain được dùng để làm cơ sở dữ liệu bảo mật trong việc lưu trữ thông tin bằng cấp của sinh viên và thông tin quá trình đào tạo. Công nghệ blockchain giúp tránh tình trạng gian lận trong quá trình học tập của sinh viên. Phòng nghiên cứu truyền thông thuộc Viện Công nghệ Massachusetts, Hoa Kỳ nghiên cứu dự án Blockcerts để số hóa chứng nhận cho các học viên hoàn thành chương trình MIT trên nền tảng blockchain. Blockcerts cung cấp tiêu chuẩn mở để tạo, phát hành, xem và xác minh các chứng chỉ dựa trên blockchain.

1.2 Lý do chọn đề tài

Hiện nay, các hồ sơ dữ liệu liên quan VBCC được quản lý lưu trữ tập trung tại đơn vị cấp VBCC. Sinh viên nhận được VBCC dưới dạng bản in. Tuy nhiên, khi có yêu cầu xác thực thông tin VBCC, phải thông qua đơn vị quản lý VBCC tra cứu hồ sơ và thường tốn nhiều thời gian. Vì vậy, công nghệ blockchain có thể giải quyết vấn đề liên quan đến tra cứu, xác minh, công nhận VBCC. Thông tin VBCC được lưu trên blockchain có đặc tính chống làm giả và đảm bảo tính toàn vẹn dữ liệu.

Trung tâm Tin học Trường Đại học An Giang là đơn vị hoạt động về lĩnh vực đào 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 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 bằng, 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 đề 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 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, chứng 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 là hồ sơ điện tử và hồ sơ sơ giấy. Tuy nhiên, phạm vi nghiên cứu của đề tài chỉ tập trung vào các hồ sơ giấy trong quy trình 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 quy trình 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 hiện có. 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 dữ liệu gốc, đảm bảo được tính toàn vẹn của dữ liệu nhận được và chống thoái thác. Chữ ký số trong các giao dịch điện tử được xem như tương đương chữ ký tay, đảm bảo về tính pháp lý, tin cậy và tiết kiệm thời gian hơn so với cách xử lý các hồ sơ giấy

Phần 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

2.2.1 Giới thiệu

Kỹ thuật mật mã là một ngành khoa học ứng dụng. 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, việc biến đổi thông tin thành một dạng khác với mục đích che dấu nội dung, ý nghĩa thông tin cần mã hóa. Các ứng dụng còn mở rộng đa dạng 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 giao thức bảo đảm các mục tiêu an ninh mạng (tính bảo mật, tính toàn vẹn và tính khả dụng) [4].

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 (multual 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).

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

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

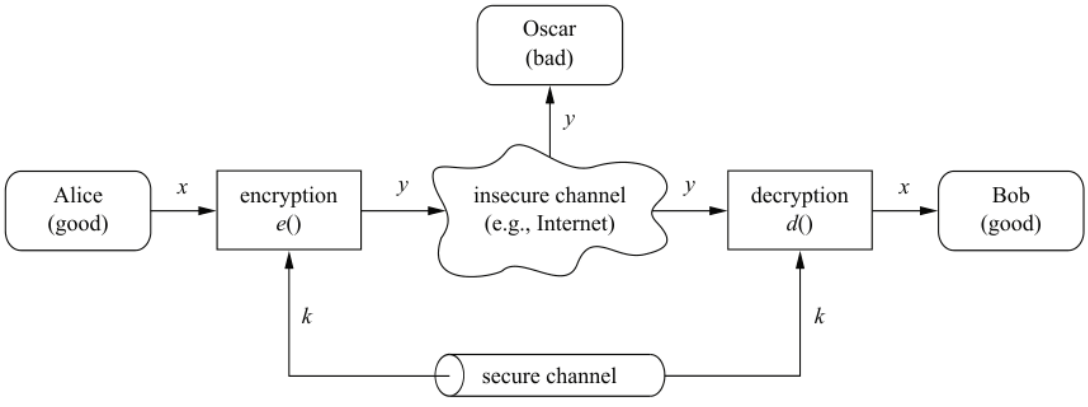
Phân loại mật mã

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 (Asymetric 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[5]. 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.

2.2.3 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.

Hàm băm là hàm một chiều, theo nghĩa từ giá trị của hàm băm rất khó để suy ngược lại nội dung hay độ dài ban đầu của thông điệp gốc.

Các hàm băm dòng MD: MD2, MD4, MD5 được Rivest đưa ra có kết quả đầu ra với độ dài là 128 bit. Chuẩn hàm băm an toàn: SHA, được Viện Tiêu Chuẩn và Công Nghệ Quốc Gia (NIST) công bố, SHA1 có kết quả đầu ra dài 160bit, SHA2: SHA-256, SHA-384, SHA-512 có kết quả đầu ra dài lần lượt là 256, 384, 512 bit [5].

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:

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 [6].

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'≠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 tệp 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 ≠ x' có cùng giá trị băm H(x) = H(x').

2.2.4 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. Chữ ký tay 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 môi trường điện tử đến hiện 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.

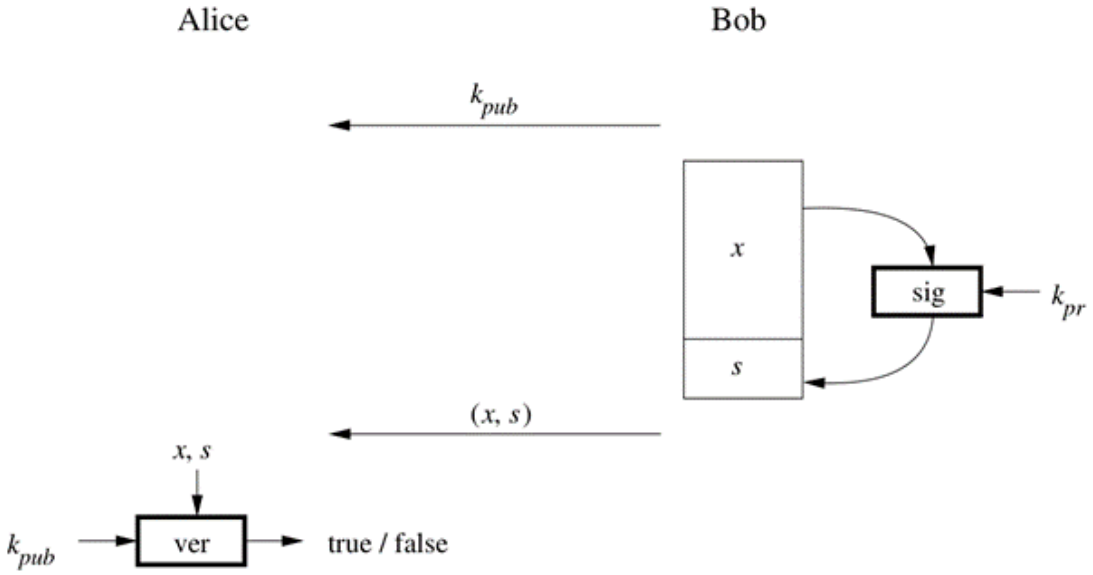
Công nghệ blockchain và chữ ký số cùng đảm bảo thông tin không bị thoái thác. Weidong Fang và cộng sự [7] nghiên cứu các sơ đồ chữ ký số điển hình trong blockchain gồm các chữ ký số hiện đại nhất được điều tra và so sánh về các lĩnh vực ứng dụng, phương pháp, bảo mật và hiệu suất. Tuy nhiên, sơ đồ chữ ký số phổ biến hiện nay là sơ đồ chữ ký RSA được Diffie-Hellman đề xuất vào năm 1976 và được Ronald Linn Rivest, Adi Shamir và Leonard Adleman thực hiện vào năm 1977. [5].

Sơ đồ chữ ký số bao gồm 3 thành phần: thuật toán tạo ra khóa, hàm tạo chữ ký và hàm kiểm tra chữ ký.

Hàm tạo ra chữ ký là hàm tính toán chữ ký trên cơ sở khóa mật và dữ liệu cần ký.

Hàm kiểm tra chữ ký là hàm kiểm tra xem chữ ký đã cho có đúng với khóa công cộng không. Khóa này mọi người có quyền truy cập cho nên mọi người đều có thể kiểm tra được chữ ký.

Nguyên lý ký số và xác thực chữ ký số

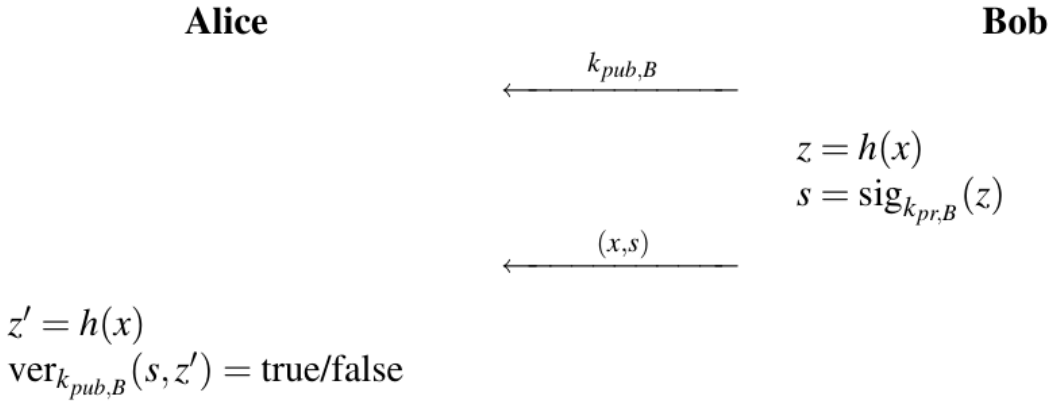


Hình 2.2: Sơ đồ ký số và xác thực chữ ký số

Sơ đồ nguyên lý ký số và xác thực chữ ký số[5] được mô tả ở hình 2.2. 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 điêp x tạo một cặp (x,s) gửi cho Alice.

Tiếp theo Alice xác minh chữ ký nhận được có 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.

Tuy nhiên, với thông điệp x rất lớn thì chữ ký số lớn và ký chậm. 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 và luôn có chiều dài cố định, đồng nghĩa sẽ nhanh hơn.



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

Sơ đồ 2.3 mô tả nguyên lý ký số và xác thực chữ ký số với hàm băm[5]. 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'.

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

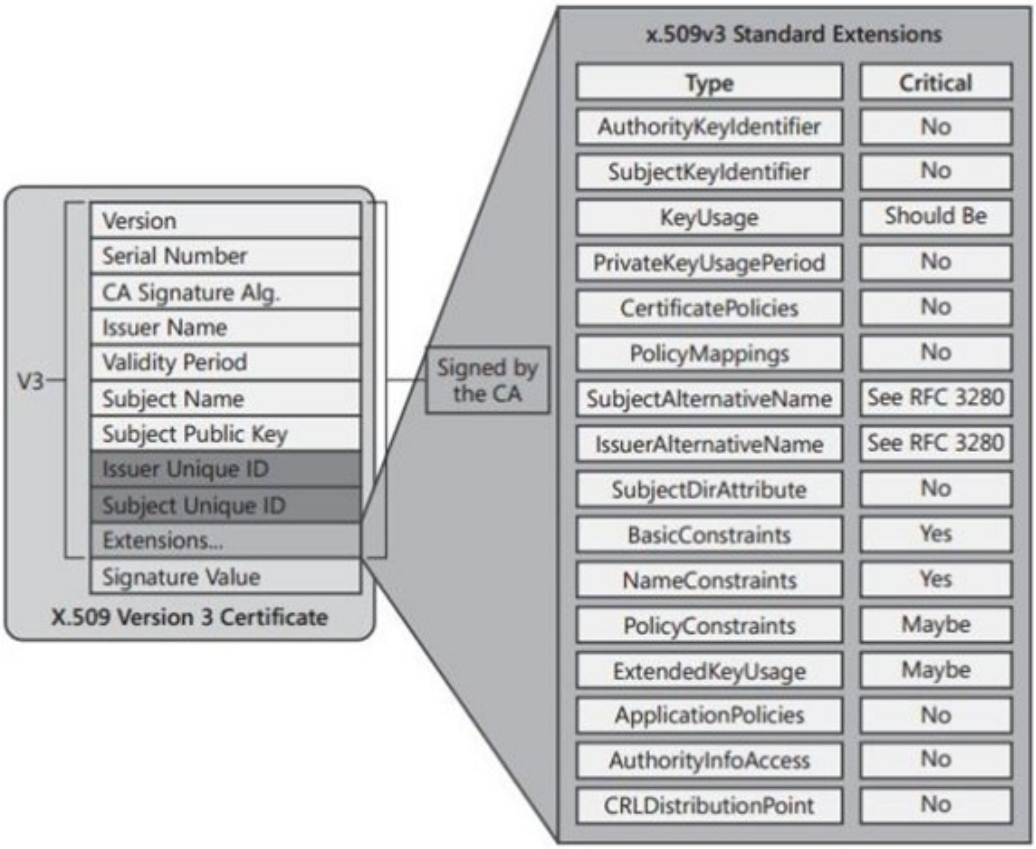
Chữ ký số đảm bảo 2 tiêu chí an toàn thông tin như sau:

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.

2.2.5 Chứng thư số

Chứng thư số là một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực 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:



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

- 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.
- 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.

Phân loại chứng thư số

- *Chứng thư số tổ chức* là chứng thư số dùng để nhận diện các chủ thể là các tổ chức trên môi trường điện tử. Chữ ký số tạo bởi chứng thư số này có giá trị pháp lý như con dấu của tổ chức.
- *Chứng thư số cá nhân* là chứng thư số dùng để nhận diện các cá nhân trên môi trường điện tử. Chữ ký số tạo bởi từ chứng thư số cá nhân có giá trị pháp lý như chữ ký tay của cá nhân khi thực hiện các giao dịch. Chữ ký số tạo bởi từ chứng thư số này có giá trị pháp lý như chữ ký tay của cá nhân khi thực hiện các giao dịch điện tử
- *Chứng thư số cá nhân thuộc tổ chức* là chứng thư số dùng để nhận diện chủ thể là các cá nhân thuộc các tổ chức trên môi trường điện tử. Chữ ký số tạo bởi chứng thư số này có giá trị pháp lý như chữ ký tay của cá nhân trong tổ chức. Chứng thư số này thường gắn với các chức danh nội bộ của chủ thể như: Tổng giám đốc, Giám đốc, Trưởng phòng, kế toán trưởng…

2.2.6 Dịch vụ chứng thực số

Dịch vụ chứng thực số là một loại hình dịch vụ chứng thực chữ ký số, do tổ chức cung cấp dịch vụ chứng thực chữ ký số cung cấp cho thuê bao để xác thực việc thuê bao là người đã ký số trên thông điệp dữ liệu.

Dịch vụ chứng thực chữ ký số bao gồm:

- Tạo cặp khóa hoặc hỗ trợ tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao;
- Cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư số của thuê bao;
- Duy trì trực tuyến cơ sở dữ liệu về chứng thư số;
- Cung cấp thông tin cần thiết để giúp chứng thực chữ ký số của thuê bao đã ký số trên thông điệp dữ liệu.

2.2.7 Hạ tầng khóa công khai

Hạ tầng khóa công khai (Public Key Infrastructure) là một cơ chế để cho một bên thứ ba (thường là nhà cung cấp chứng thực số) cung cấp và xác thực danh tính các bên tham gia vào quá trình trao đổi thông tin. Cơ chế này cũng cho phép gán cho mỗi người sử dụng trong hệ thống một cặp khóa công khai/khóa riêng tư. Các quá trình này thường được thực hiện bởi một phần mềm đặt tại trung tâm và các phần mềm khác tại các địa điểm của người dùng. Khóa công khai thường được phân phối trong hạ tầng khóa công

khai.

Khái niệm hạ tầng khóa công khai PKI thường được dùng chỉ toàn bộ hệ thống bao gồm cả nhà cung cấp chứng thực số (CA) cùng các cơ chế liên quan đồng thời với toàn bộ việc sử dụng các thuật toán mã hóa công khai trong trao đổi thông tin. Tuy nhiên, các cơ chế trong PKI không nhất thiết sử dụng các thuật toán mã hóa công khai.

2.3 Công nghệ Blockchain

2.3.1 Giới thiệu

Blockchain là cuốn sổ cái kỹ thuật số chống giả mạo được triển khai theo mô hình phân tán (không có kho lưu trữ trung tâm), còn gọi là công nghệ sổ cái phân tán (Decentralized Ledger Technology). Khi người dùng phát sinh các giao dịch, sau khi được cộng đồng chấp nhận ghi vào sổ cái thì giao dịch đó không thể bị thay đổi. Công nghệ này được biết đến rộng rãi vào năm 2009 với sự ra đời của mạng Bitcoin [8], một trong những đồng tiền mã hóa hiện đại đầu tiên được bảo vệ bởi các cơ chế mật mã học thay vì nhờ vào bên chứng thực hoặc kho lưu trữ trung tâm.

Phân loại Blockchain

Mạng Blockchain có thể được phân loại thành: Blockchain công khai và Blockchain riêng tư [9]. Loại thứ nhất gồm Bitcoin, Ethereum, …, bất kỳ nút nào cũng có thể tham gia và rời khỏi mạng Blockchain, mô hình này phân tán hoàn toàn, mỗi nút có vai trò như nhau. Loại thứ hai gồm Hyperledger, BigchainDB,…, việc tham gia mạng Blockchain được kiểm soát chặt chẽ, xác định rõ danh tính của thành viên.

So sánh giữa các mạng Blockchain

Tien Tuan Anh Dinh và cộng sự [9] nghiên cứu và so sánh mạng Blockchain dựa trên 4 khái niệm chính của Blockchain: sổ cái phân tán, cơ chế đồng thuận (concensus), mô hình ứng dụng mật mã, hợp đồng thông minh (smart contract),

Sổ cái phân tán

Blockchain không dựa vào các tổ chức thứ ba để xử lý giao dịch, không có sự kiểm soát trung tâm. Tất cả thông tin được các nút kiểm tra, truyền tải và quản lý. Các nút lưu trữ bản sao của sổ cái, gồm các giao dịch trong từng khối ghép nối với nhau thành chuỗi. Cơ chế sổ cái phân tán là đặc điểm nổi bật và quan trọng nhất của Blockchain. Khái niệm sổ cái phân tán có 3 tiêu chí phân loại được mô tả ở bảng 2.1

Bảng 2.1: So sánh sổ cái phân tán

Dữ liệu mô tả	Số lượng sổ	Quyền kiểm soát	Ứng dụng
Tài khoản	1	Người quản trị	Sổ cái thông thường với hình thức lưu trữ tập trung ở những ngân hàng
Tài sản	Nhiều	Nhiều người	Sổ cái riêng của một tổ chức hoặc nhóm các tổ chức
Tiền hoặc tài khoản	1	Bất cứ người nào	Lĩnh vực tiền số: Bitcoin, Ethereum

Cơ chế đồng thuận

Trong Blockchain, sổ cái lưu trữ toàn bộ lịch sử các giao dịch và trạng thái dữ liệu hiện tại. Để sổ cái được lưu trữ, cập nhật dữ liệu giống nhau ở tất cả các nút thì cần có sự thống nhất giữa các bên tham gia. Ngược lại việc một tổ chức có đặc quyền cập nhật dữ liệu trong các ứng dụng CSDL truyền thống. Tuy nhiên, Blockchain không phụ thuộc vào độ tin cậy của một nút. Các nút không tin cậy như bài toán các vị tướng Byzantine. Do đó các nút sẽ yêu cầu thực hiện giải thuật đồng thuận để có chung một quyết định. Cơ chế đồng thuận hiện nay có thể chia thành ba loại [2]

(1) POW (Proof of Work) là cơ chế của Bitcoin: Cơ chế này yêu cầu các nút tính toán đề xuất khối mới và được đa số nút kiểm tra thành công tính tin cậy của các giao dịch phát sinh trong khối. Đối với Bitcoin, POW mật độ giao dịch (năm 2008) là 7 giao dịch/giây dẫn đến trung bình 10 phút xác thực thành công 1 khối.

(2) PBFT (Practical Byzantine Fault Tolerance): mỗi thành viên tạo khối mới của mình, kiểm tra xong thì chuyển cho thành viên khác kiểm tra, đồng thời nhận khối mới từ thành viên khác để kiểm tra. Khối nào được đa số chấp nhận thì được chọn đưa vào blockchain. Cơ chế này được dùng trong mạng Blockchain riêng tư bởi các nút đã xác định danh tính.

(3) POS (Proof of Stake): Mỗi thành viên tham gia mạng có một cổ phần (Stake) với một lượng lớn hay nhỏ tùy đầu tư ban đầu. Đầu tư càng cao thì trách nhiệm càng cao. Trách nhiệm càng cao thì khả năng kiểm tra một giao dịch đúng càng cao. Cơ chế này được dùng trong BigchainDB và Ethereum.

Mô hình ứng dụng mật mã

Blockchain ứng dụng mật mã khóa công khai. Khi giao dịch phát sinh, khóa công khai và chữ ký sẽ được dùng để kiểm tra danh tính. Khi thực hiện mã hóa giao dịch thì khóa công khai, chữ ký và thông tin người dùng của giao dịch trước đó phải khớp nhau.

Trong mạng Blockchain, thuộc tính khóa có vai trò quan trọng để xác định danh tính và xác minh giao dịch, nên cần được giữ an toàn. Trong những ứng dụng Blockchain vào tiền số, nếu xảy ra sự cố mất khóa thì gây thiệt hại thất thoát tiền, vì không thể khôi phục, xử lý dữ liệu của Blockchain. Ngược lại trong Blockchain riêng tư, thành phần quản lý cấp phép truy cập tách biệt với mã hóa giao dịch. Đối với Hyperledger, các dịch

vụ chứng thực số và dịch vụ thành viên (Membership Service Provider) sẽ cấp phép truy cập, nên một tài khoản quản lý thuộc tổ chức sẽ có quyền thiết lập cấp phép những dịch vụ, người dùng được truy cập vào mạng Blockchain.

Hợp đồng thông minh

Hợp đồng thông minh (Smart Contract) là chương trình máy tính giải quyết logic (hay trình tự) khi giao dịch phát sinh trong mạng Blockchain. Các trình tự trong Blockchain tiền số gồm có: đầu tiên kiểm tra tính hợp lệ của các địa chỉ, ký số trong giao dịch, kế tiếp kiểm tra số dư của các địa chỉ gửi và nhận trong giao dịch, cuối cùng là lưu lại các thay đổi các dữ liệu giao dịch. Hai thuộc tính phân biệt hợp đồng thông minh (HĐTM) là ngôn ngữ lập trình và môi trường thực thi HĐTM. Bảng 2.2 so sánh các Blockchain cùng thuộc tính của HĐTM. Hyperledger Fabric có khả năng chuyển dễ dàng giữa nhiều hệ điều hành, nhờ vào cơ chế hoạt động của container. Container tạo môi trường riêng để chương trình hoạt động và không ảnh hưởng tới phần còn lại của hệ điều hành.

Bảng 2.2: So sánh các Blockchain

Blockchain	Thực thi HĐTM	Ngôn ngữ HĐTM	Dữ liệu mô tả
Bitcoin	Thuộc ứng dụng	Go, C++	Giao dịch
Ethereum	EVM	Solidity, Serpent, LLL, C++	Giao dịch
Hyperledger Farbic v2.x	Docker	Go, Java, JavaScript	Khóa-Giá trị
BigchainDB	Thuộc ứng dụng	Python, Go, C++, Javascript	Giao dịch
Ripple	-	-	Tài khoản

2.3.2 Bitcoin

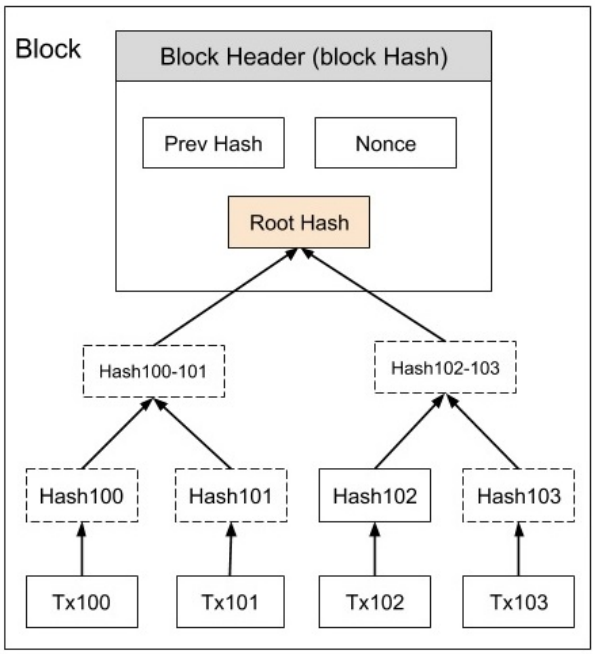
Mạng Bitcoin gồm có thành phần miner và Blockchain.

Miner là một node trên mạng kết nối với nhau theo giao thức mạng ngang hàng. Miner kết nối người dùng trong mạng và Blockchain. Bitcoin cho phép phát hành tiền mới thông qua cơ chế "phần thưởng" cho miner sau khi khối của mình tạo ra được xác thực hợp lệ. Cơ chế đồng thuận để duy trì và tự kiểm soát để đảm bảo rằng chỉ có các giao dịch và các khối hợp lệ mới được thêm vào Blockchain.

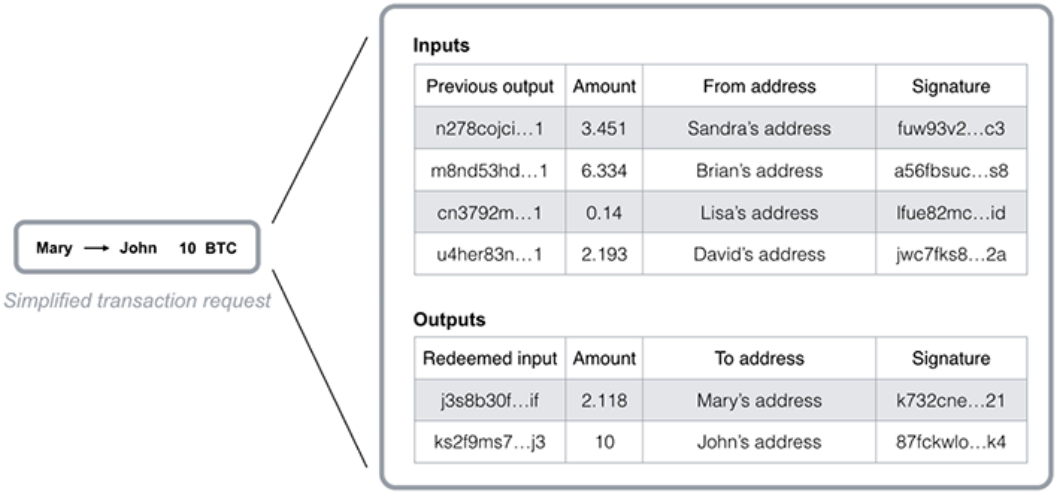
Blockchain là một hệ thống cơ sở dữ liệu phân tán lưu trữ các khối liên kết với nhau sau khi đã xác thực thành công bởi các miner. Hình 2.5 mô tả cấu trúc một khối bao gồm các thành phần: định danh khối (blockheader) và dữ liệu. Blockheader là giá trị băm của các thành phần gồm: Root hash của các dữ liệu giao dịch, giá trị blockheader của khối trước, số thứ tự khối, số nounce, nhãn thời gian.

Một dữ liệu giao dịch gồm có nhiều giao dịch được ký số bởi các bên tham gia như hình 2.6.

Mỗi dữ liệu giao dịch A, B, C, D, E được tính giá trị băm, sau đó gộp 2 khối dữ liệu

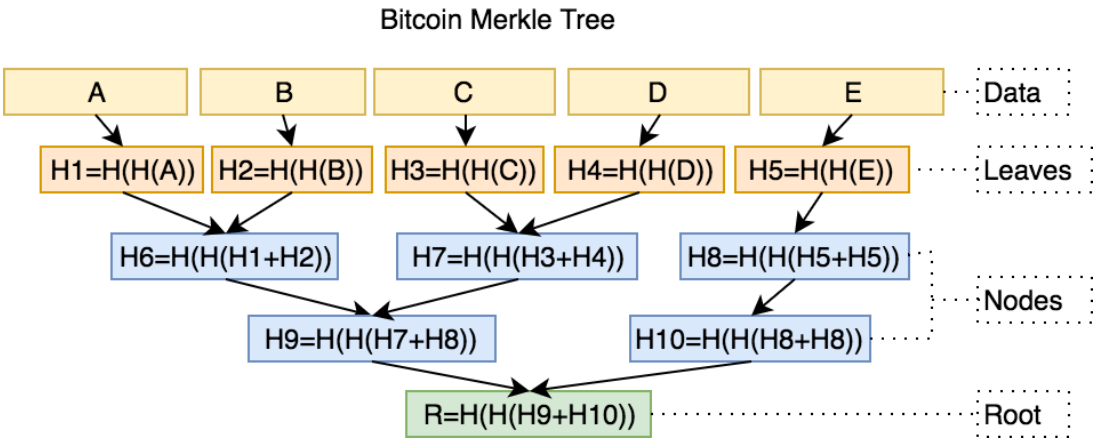


Hình 2.5: Mô tả cấu trúc một khối



Hình 2.6: Mô tả một giao dịch blockchain

thành từng cặp, tính giá trị băm trung gian, công việc này lặp lại cho đến khi tính được giá trị băm các giao dịch (Root Hash) được mô tả như hình 2.7.



Hình 2.7: Mô tả cây mã hóa Merkle trong Bitcoin

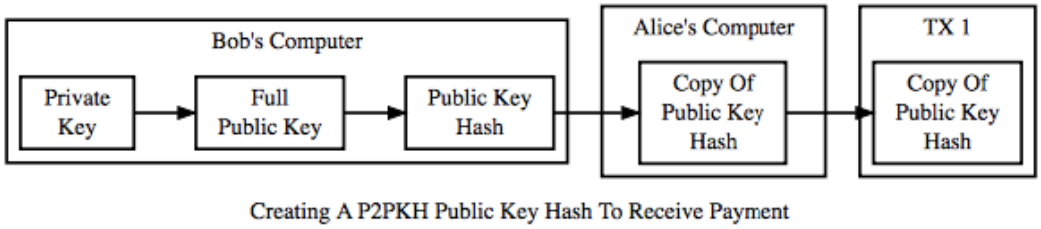
Giao dịch trong Blockchain có thể chia thành 3 loại: giao dịch thuộc về khối đầu tiên của Blockchain, giao dịch thưởng cho các miner và giao dịch thông thường.

• Giao dịch thuộc về khối đầu tiên của Blockchain sẽ được chèn vào trong mã nguồn của Blockchain tại khối đầu tiên của Blockchain. Các loại tiền số có quy định số lượng tiền giới hạn trong hệ thống.

• Giao dịch thưởng cho những người tạo ra khối mới: hệ thống Blockchain tự tạo tự động và sẽ chuyển tiền thưởng cho người tạo ra khối mới.

• Giao dịch thông thường là những giao dịch được tạo bởi những người dùng.

Ví Bitcoin



Hình 2.8: Tạo khóa để thực hiện giao dịch trong bitcoin

Mỗi người dùng Bitcoin cần tạo một ví Bitcoin để lưu trữ khóa bí mật để truy cập vào địa chỉ Bitcoin để có thể thực hiện các giao dịch. Theo hình 2.8, khi Alice muốn gửi tiền Bitcoin (BTC) cho Bob, Bob cần tạo ra cặp khóa gồm khóa bí mật và khóa công khai, Bitcoin sử dụng thuật toán chữ ký số đường cong Elliptic (ECDSA) [5] để thực hiện ký các giao dịch. Địa chỉ ví của Bob chính là giá trị băm của khóa công khai được mã hóa base58, Alice gửi BTC vào địa chỉ ví của Bob bằng cách giải mã base58 để lấy giá trị băm khóa công khai của Bob, Alice tạo các Outputs của các giao dịch cho phép bất cứ ai cũng có thể sở hữu các Output đó nếu chứng minh được họ có khóa bí mật của

Bob. Quá trình giao dịch như trên được gọi là thanh toán qua giá trị băm khóa công khai (P2PKH – Pay to Public Key Hash).

Mạng Bitcoin và các hệ thống Blockchain tương tự, việc chuyển thông tin kỹ thuật số với đại diện là tiền điện tử diễn ra trong một hệ thống phân tán. Người dùng Bitcoin ký chữ ký số và chuyển tài sản của mình sang người khác và Bitcoin ghi lại các giao dịch này công khai, cho phép những người tham gia mạng xác minh độc lập tính hợp lệ của giao dịch. Do đó, công nghệ blockchain được xem là giải pháp chung cho các đồng tiền mã hóa sau này.

2.3.3 Ethereum

Ethereum là mạng Blockchain của ứng dụng tiền số ETH. Ethereum cho phép mọi người xây dựng và sử dụng các ứng dụng phi tập trung dựa trên công nghệ Blockchain. Dự án Ethererum thuộc nhóm mã nguồn mở.

Trang chủ: https://ethereum.org/

Ethereum có một số đặc điểm sau:

- Là mạng Blockchain công cộng
- Sử dụng cơ chế đồng thuận bằng chứng công việc PoW
- Tích hợp sẵn tiền số ETH
- Hỗ trợ các ngôn ngữ như C++, Go và Python

2.3.4 BigchainDB

Giới thiệu

BigchainDB có mã nguồn mở. BigchainDB được thiết kế vừa có tính chất của CSDL và Blockchain như bảng 2.3.

Trang chủ: https://www.bigchaindb.com/

Bảng 2.3: Mục tiêu thiết kế BigchainDB 2.x

	Blockchain	CSDL	BigchainDB
Tính phi tập trung	có		có
Cơ chế đồng thuận BFT	có		có
Chống sửa đổi	có		có
Tốc độ giao dịch cao		có	có
Lập chỉ mục và truy vấn dữ liệu có cấu trúc		có	có

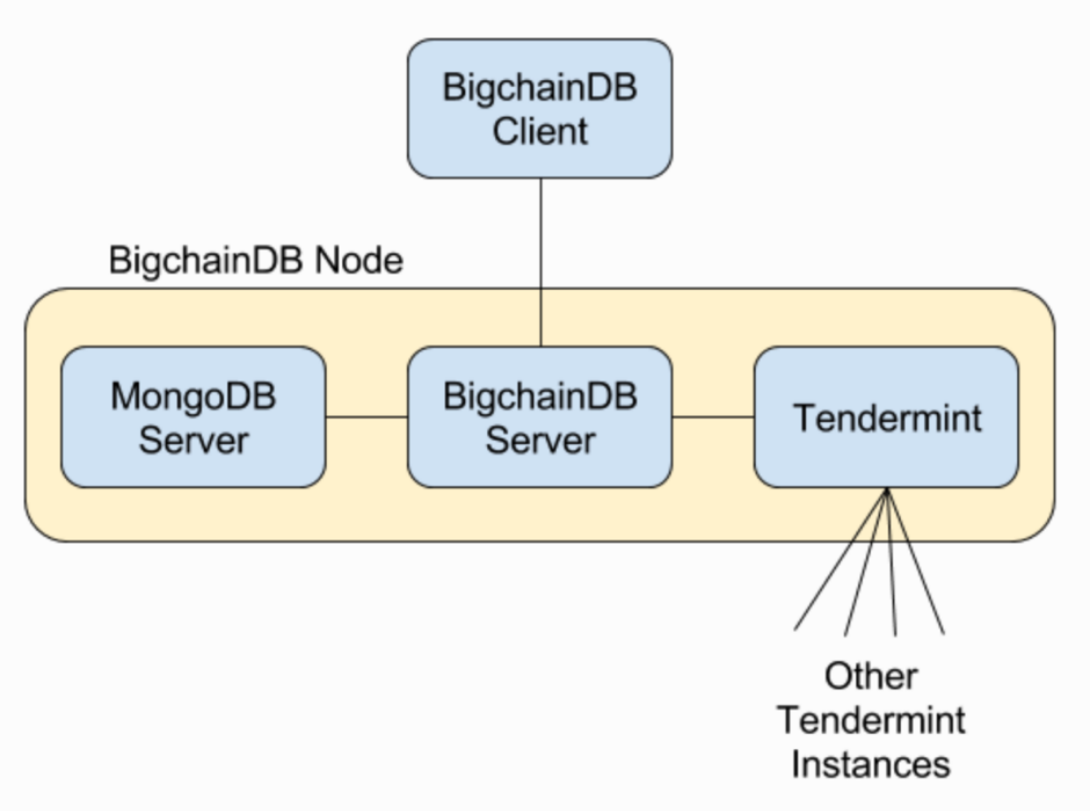
Kiến trúc của BigchanDB

Một node trong BigchainDB được mô tả như hình 2.9, mỗi thành phần có vai trò như sau:

• BigchainDB Server: Là phần giao tiếp giữa Tendermint và ứng dụng. Thực hiện giao tiếp với BigChainDB Client. Nhận các giao dịch và chuyển cho Tendermint. Nếu các giao dịch hợp lệ sẽ được lưu trữ vào MongoDB.

• Tendermint: Giao tiếp với các tendermint ở các node khác. Thực hiện xác thực giao dịch, nhận các giao dịch từ các node khác trong mạng. Lưu trữ giao dịch vào MongoDB nếu hợp lệ. Đảm nhiệm khi có bất kì một Tendermint ở node nào trong mạng gây lỗi (ví dụ như bị thay đổi giữ liệu) thì node sẽ bị cô lập.

• MongoDB Server: Lưu trữ giữ liệu trên hệ thống local của node đó. Dữ liệu sẽ được trao đổi giữa BigchainDB Server và Tendermint.



Hình 2.9: Các thành phần của một node BigchainDB

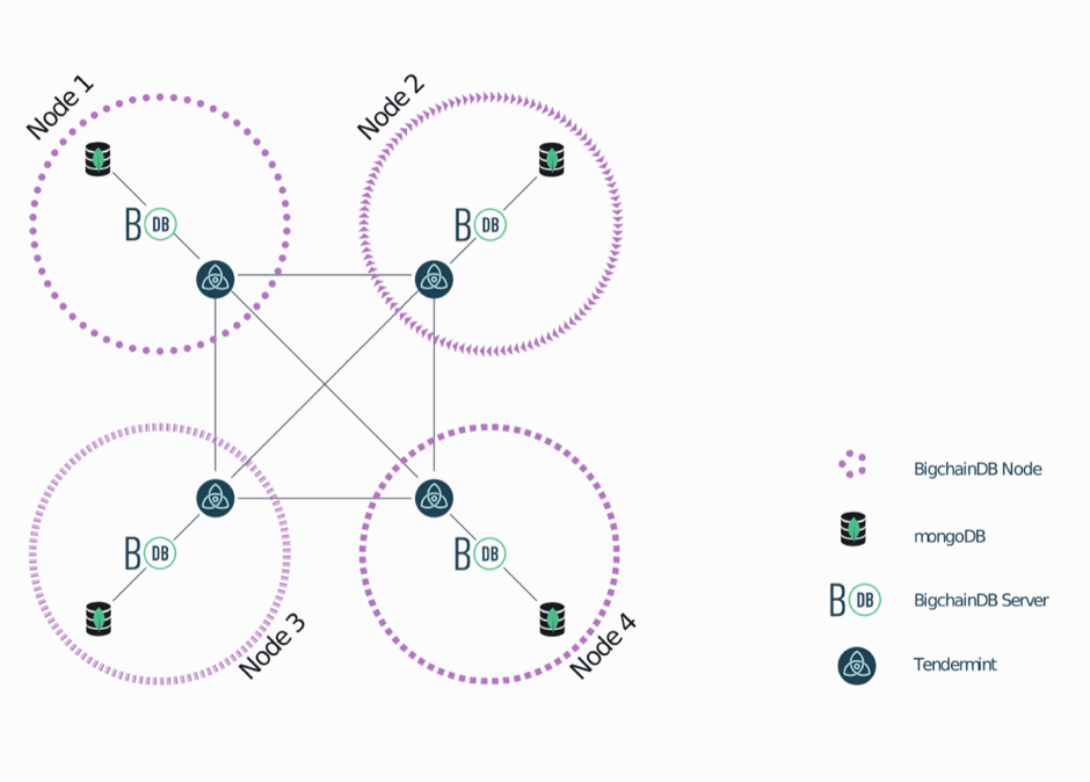
Mô hình vận hành mạng BigchainDB được mô tả như hình 2.10

Trong hình 2.10, giả sử Node 1 tạo dữ liệu giao dịch. BigchainDB server nhận giao dịch gửi cho Terdermint xác thực. Khi giao dịch hợp lệ nó sẽ được lưu tại cơ sở dữ liệu MongoDB trên node, đồng thời dữ liệu được gửi cho các Terdermint khác trong mạng kết nối. Các Terdermint khác nhận và thực hiện các xác thực liên quan sau đó lưu vào cơ sở dữ liệu MongoDB tại node đó.

BigchainDB dựa trên nền tảng Blockchain của Tendermint. BigchainDB bao gồm hai thành phần chính: Tendermint Core và môi trường ứng dụng (Application BlockChain Interface) (ABCI).

Tendermint Core được mô tả hoạt đông theo hai cơ chế: thứ nhất là dịch vụ điều phối hiệu suất cao cho các ứng dụng phân tán. Zookeeper, etcd và consul; thứ hai là cơ chế của blockchain bao gồm nền tảng tiền số và sổ cái phân tán.

Môi trường ứng dụng ABCI là lớp giao tiếp ở giữa ứng dụng và Tendermint. Ứng dụng có thể phát triển bằng nhiều ngôn ngữ lập trình Java, C++, Python, or Go. ABCI



Hình 2.10: Mô hình vận hành mạng BigchainDB

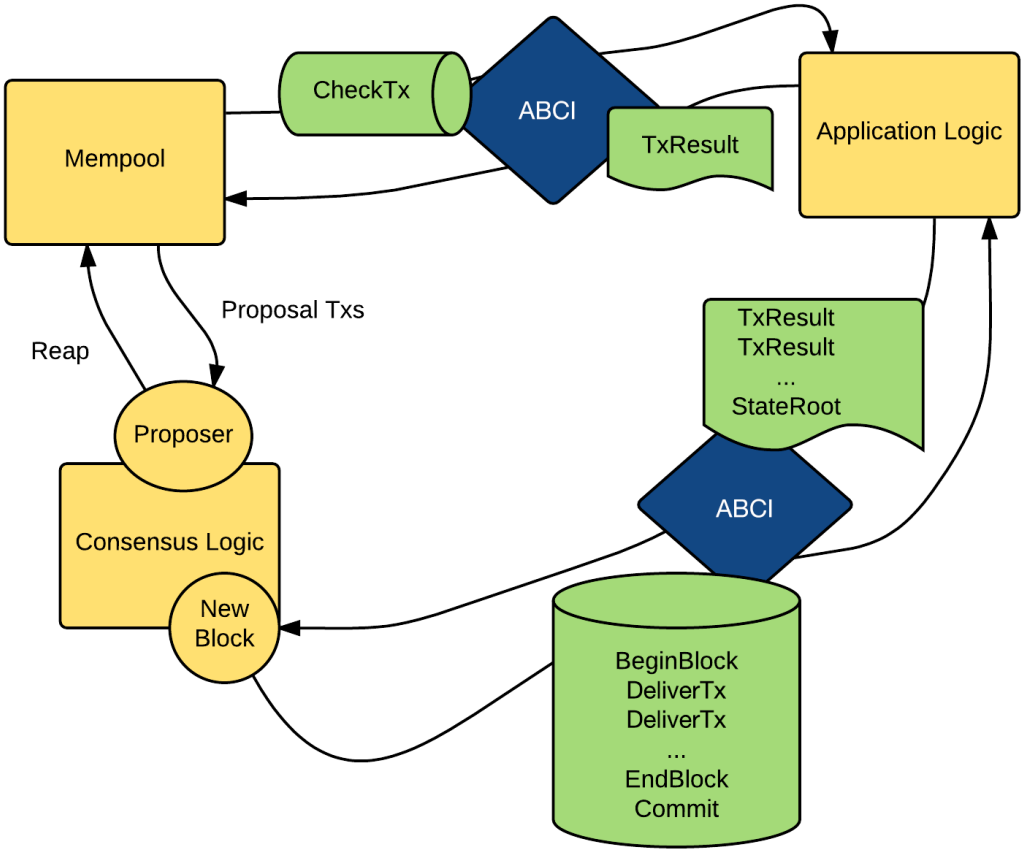
cung cấp ba thông điệp cơ bản giúp ứng dụng giao tiếp với Tendermint Core.

DeliverTx là mã công việc của ứng dụng. Mỗi giao dịch trong chuỗi khối được gửi kèm theo thông điệp này. Ứng dụng cần xác thực từng giao dịch nhận được với thông báo DeliverTx dựa trên trạng thái hiện tại, giao thức ứng dụng và thông tin đăng nhập mật mã của giao dịch. Sau đó, một giao dịch đã được xác thực cần cập nhật trạng thái ứng dụng - bằng cách ràng buộc một giá trị vào một kho lưu trữ các giá trị khóa, hoặc bằng cách cập nhật cơ sở dữ liệu UTXO chẳng hạn.

CheckTx tương tự như DeliverTx, nhưng nó chỉ để xác thực các giao dịch. Đầu tiên, mempool của Tendermint Core kiểm tra tính hợp lệ của một giao dịch với CheckTx và chỉ chuyển tiếp các giao dịch hợp lệ cho các giao dịch tương tự của nó. Ví dụ: một ứng dụng có thể kiểm tra số thứ tự tăng dần trong giao dịch và trả về lỗi khi CheckTx nếu số thứ tự cũ.

Commit được sử dụng để tính toán mật mã cho trạng thái ứng dụng hiện tại, được đặt vào tiêu đề khối tiếp theo. Điều này cũng đơn giản hóa việc phát triển các ứng dụng an toàn, vì các bằng chứng Merkle-hash có thể được xác minh bằng cách kiểm tra đối với hàm băm khối và rằng hàm băm khối được ký bởi một số thành viên.

Hình 2.11 mô tả đường đi của thông điệp trong ABCI.



Hình 2.11: Sơ đồ thông điệp trong ABCI

2.3.5 Hyperledger Fabric

Giới thiệu

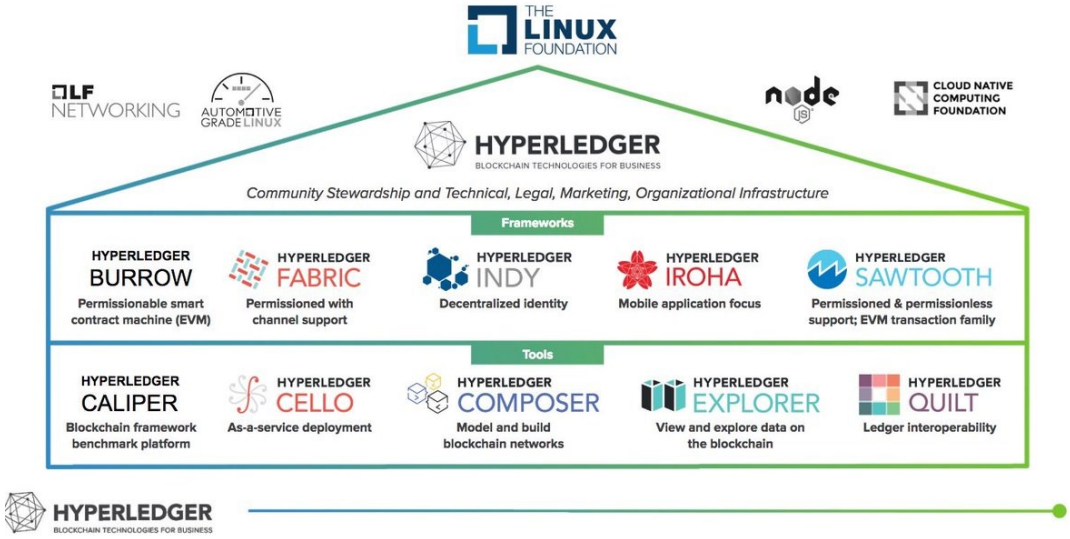
Hyperledger Fabric (HF) là một nền tảng blockchain riêng tư trong dự án Hyperledger của tổ chức Linux Foundation gồm: Hyperledger Indy, Hyperledger Fabric, Hyperledger Iroha, Hyperledger Sawtooth, Hyperledger Burror. Hình 2.12 mô tả các thành phần của dự án Hyperledger.

HF là phần mềm mã nguồn mở. Công ty IBM đề xuất phát triển dự án HF để làm nền tảng ứng dụng blockchain cho các tổ chức, doanh nghiệp. HF có nhiều tính năng nổi trội so với các nền tảng blockchain phổ biến như Bitcoin, Ethereum,…để đáp ứng nhu cầu cần thiết của môi trường tổ chức. Đó là nhu cầu định danh thành viên tham gia, mạng được cấp quyền truy cập và bảo mật thông tin riêng của tổ chức. HF có kiến trúc mô-đun linh hoạt và tối ưu hoá cho nhiều ứng dụng trong các lĩnh vực như: giáo dục, tài chính, bảo hiểm, y tế, chuỗi cung ứng, hành chính công,…

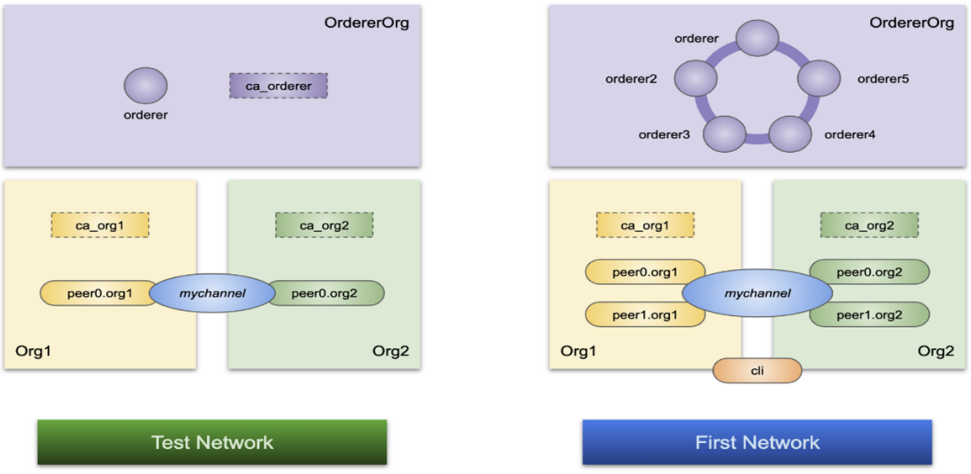
Hình 2.13 mô tả hai mô hình mạng cơ bản để thử nghiệm triển khai ứng dụng Blockchain trên nền tảng HF. Ngoài First Net, Test Net, mạng Blockchain có thể mở rộng thêm các thành phần, qui mô để phù hợp với yêu cầu của ứng dụng.

Kiến trúc của Hyperledger Fabric

Kiến trúc HF có các kênh bảo mật riêng kết nối trong mạng Blockchain, giúp các



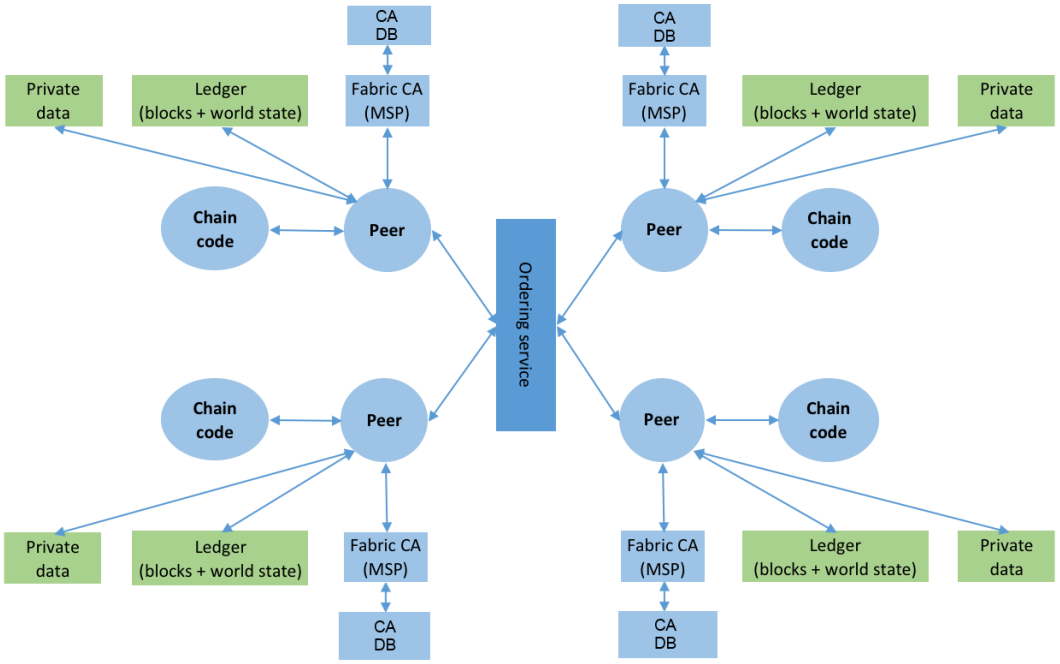
Hình 2.12: Dự án Hyperledger



Hình 2.13: Mô hình mạng thử nghiệm Hyperledger Fabric

sổ cái được chia sẻ thông qua nhiều kênh riêng. Mạng HF phù hợp với các ứng dụng Blockchain và không yêu cầu khái niệm đồng tiền số.

Kiến trúc của HF gồm các thành phần chính như Dịch vụ chứng thực số và Dịch vụ thành viên (Membership service provider, Certificate Authority), Hợp đồng thông minh (Chaincode), các node thành viên (Peers, Nodes), Dịch vụ xử lý hàng đợi (ordering service), Kênh kết nối, Sổ cái (ledger), được mô tả ở hình 2.14



Hình 2.14: Kiến trúc mạng Hyperledger Fabric

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 được cài đặt trên các nút tham gia chung kênh an toàn và được đánh số các phiên bản. Các tổ chức trong mạng cùng thuộc kênh an toàn, 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.

Việc nâng cấp các hợp đồng thông minh sẽ được gắn với quá trình đồng thuận và được các nút mạng đồng ý. Khi đó các nút peer có đầy đủ các hợp đồng thông minh, gọi là chaincode. 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 sẽ riêng tư

giữa một số thành viên thuộc kênh thay vì tất cả thành viên đều có thể sở hữu. Tùy chọn này tối ưu hơn cách tạo thêm một kênh riêng mới cho một số thành viên, giảm được thời gian để cấu hình, thiết lập thông số 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,….

HF gồm các thành phần trong hình 2.14 được mô tả như sau:

Ledger: Quyển sổ cái bao gồm 2 thành phần có liên quan nhau là "chuỗi khối" và "cơ sở dữ liệu trạng thái". Khi các giao dịch làm thay đổi các tài sản trong mạng blockchai, dữ liệu sẽ đượcghi nhận tất cả lên "chuỗi khối" theo dạng nhật ký và không thể xóa hay chỉnh sửa. Đồng thời, "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 sổ cái được lưu trên các nút Peer trong cùng kênh, đồng thời sổ cái được đồng bộ khi có phát sinh giao dịch thông qua cơ chế đồng thuận.

Smart contract (hay chaincode): Hợp đồng thông minh trong blockchain là các ứng dụng được lập trình bằng ngôn ngữ lập trình như: Javascript, Go, Java. Hợp đồng thông minh tương tác với mạng, thực hiện logic (trình tự thực hiện) trong xử lý giao dịch. Trong HF, hợp đồng thông minh còn được gọi là chaincode, được cài đặt trên các nút Peer.

Peer nodes: Là những nút cơ bản của mạng có chức năng lưu trữ bản sao của Sổ cái và thực thi Hợp đồng thông minh. Các nút peer được quản lý và duy trì bởi các dịch vụ thành viên trong mạng. Nút Peer được chia làm hai 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 Kênh.

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 của tổ chức (các Orgs) như, Peer, Ordering service, MSP. Một nút 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 uỷ quyền.

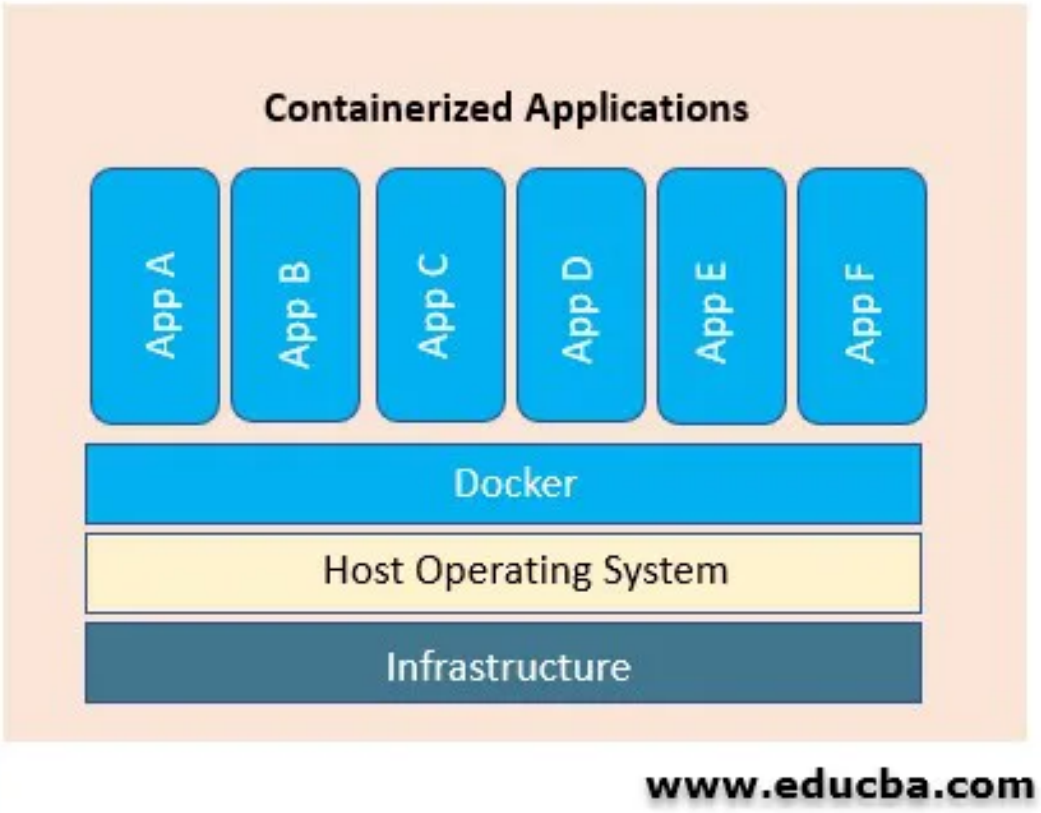
Membership Service Provider (MSP): MSP là dịch vụ xác minh các nút trong mạng, thông qua chứng thư số (cấp từ CA). Do đó HyperLedger Fabric có thể xác thực các thực thể kết nối với mạng thông qua danh tính mà không cần khóa bí mật. Ngoài ra, nó còn có vai trò xác định quyền truy cập trong phạm vi mạng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

Thiết lập mạng Hyperledger Fabric

Từ kiến trúc HF, các docker container giúp triển khai nhanh chóng mô hình mạng HF phân tán trên nhiều tổ chức. Mạng HF được thiết lập từ khung phần mềm HF, mã nguồn dự án, tài liệu HF: https://hyperledger-fabric.readthedocs.io/en/latest/

Docker container là môi trường riêng cho ứng dụng hoạt động gồm có các chương trình thực thi và các thư viện chương trình. Các docker container giảm thiểu yêu cầu sử dụng bộ nhớ máy và bộ nhớ trên đĩa. Docker container có thể hoạt động trên nhiều nền tảng Windows, Linux, Macos.

Docker Engine tạo các container hoạt động từ các file cấu hình Dockerfile. Một máy vật lý, máy ảo sẽ cần cài đặt Docker Engine. Sau đó các docker containers sẽ chạy trên Docker Engine. Các ứng dụng chạy trên Docker Engine được minh họa như hình 2.15,

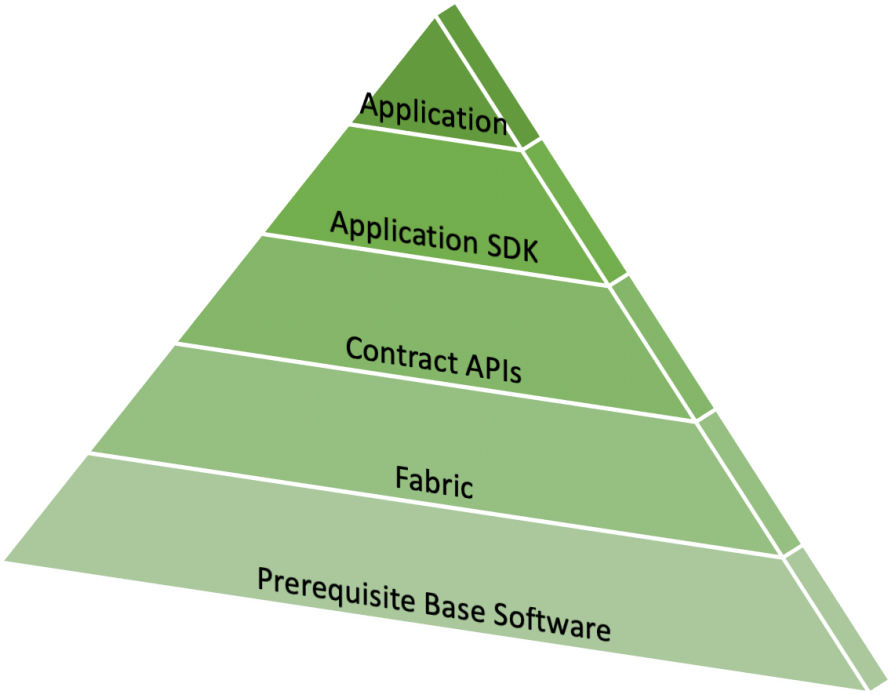


Hình 2.15: Docker container

Ứng dụng Blockchain HF sẽ chạy trong các docker container. Sơ đồ ứng dụng Blockchain được minh họa ở hình 2.16.

Tiện ích mở rộng IBM Blockchain Platform Extension trên VS Code

HF được hỗ trợ qua tiện ích mở rộng IBM Blockchain Platform Extension trên VS Code. Tiện ích mở rộng của IBM giúp tạo, phát triển kiểm tra và gỡ lỗi các hợp đồng thông minh, kết nối với môi trường Hyperledger Fabric và xây dựng các ứng dụng giao dịch trên mạng blockchain.



Hình 2.16: Sơ đồ ứng dụng blockchain Hyperledger Fabric

Quy trình phát triển hợp đồng thông minh

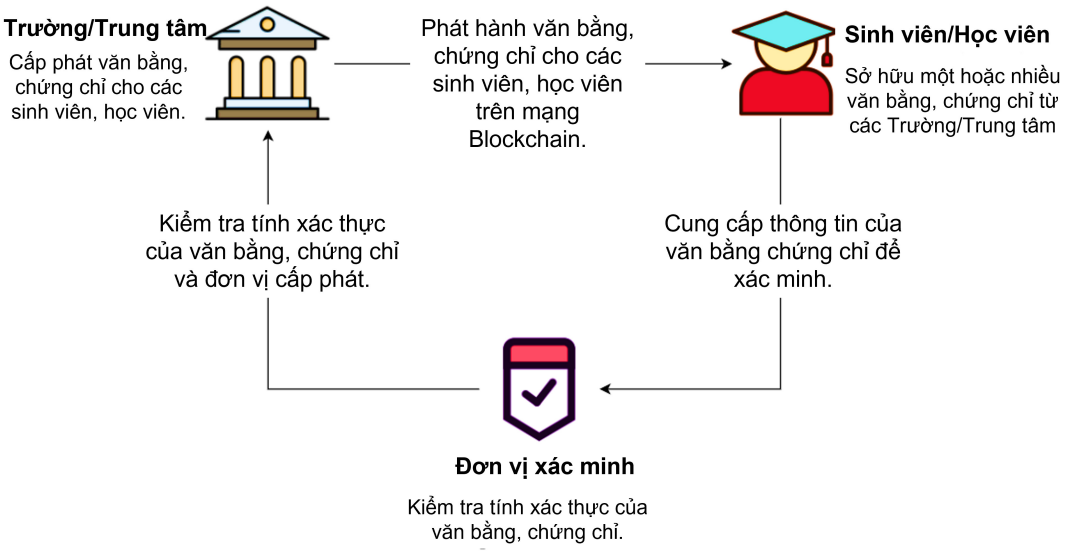
Môi trường phát triển là VS Code và tiện ích giúp hỗ trợ quy trình phát triển hợp đồng thông minh trên Blockchain, gồm các bước sau:

1. Tạo và đóng gói smart contract
2. Kết nối với mạng HF
3. Cài đặt chaincode
4. Gửi giao dịch, chạy kiểm tra smart contract

CHƯƠNG 3
XÂY DỰNG HỆ THỐNG

3.1 Mô tả bài toán

Bài toán đặt ra nhu cầu quản lý thông tin của người cấp, người được cấp và VBCC; số hóa các quy trình cấp VBCC, sở hữu VBCC, chia sẻ thông tin xác thực VBCC có liên quan đến thông tin cá nhân của người được cấp VBCC theo các quy định hiện hành về bảo vệ bí mật thông tin trong môi trường trực tuyến. Sơ đồ bài toán được minh họa như hình 3.1.



Hình 3.1: Sơ đồ bài toán quản lý VBCC

3.2 Tổng quan giải pháp

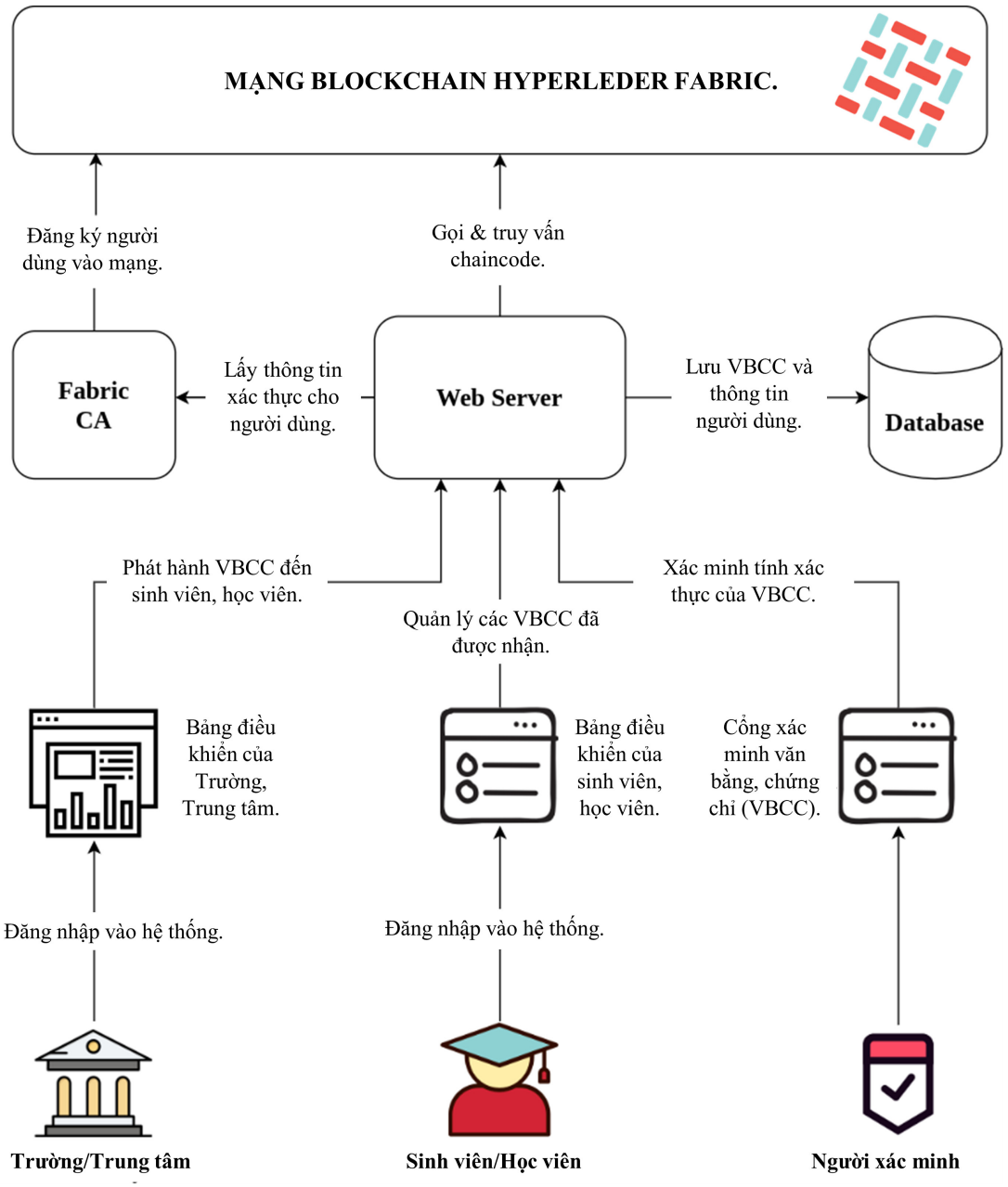
Nghiên cứu đề xuất một mô hình thử nghiệm ứng dụng Blockchain để đảm bảo tính an toàn thông tin VBCC và tính bí mật thông tin của người được cấp VBCC. Hệ thống thực hiện việc ký số khi cấp VBCC, lưu VBCC đã cấp vào blockchain và truy vấn dữ liệu blockchain để xác thực VBCC. Kiến trúc hệ thống được mô tả như hình 3.2.

Quy trình hoạt động của hệ thống được minh họa như hình 3.3.

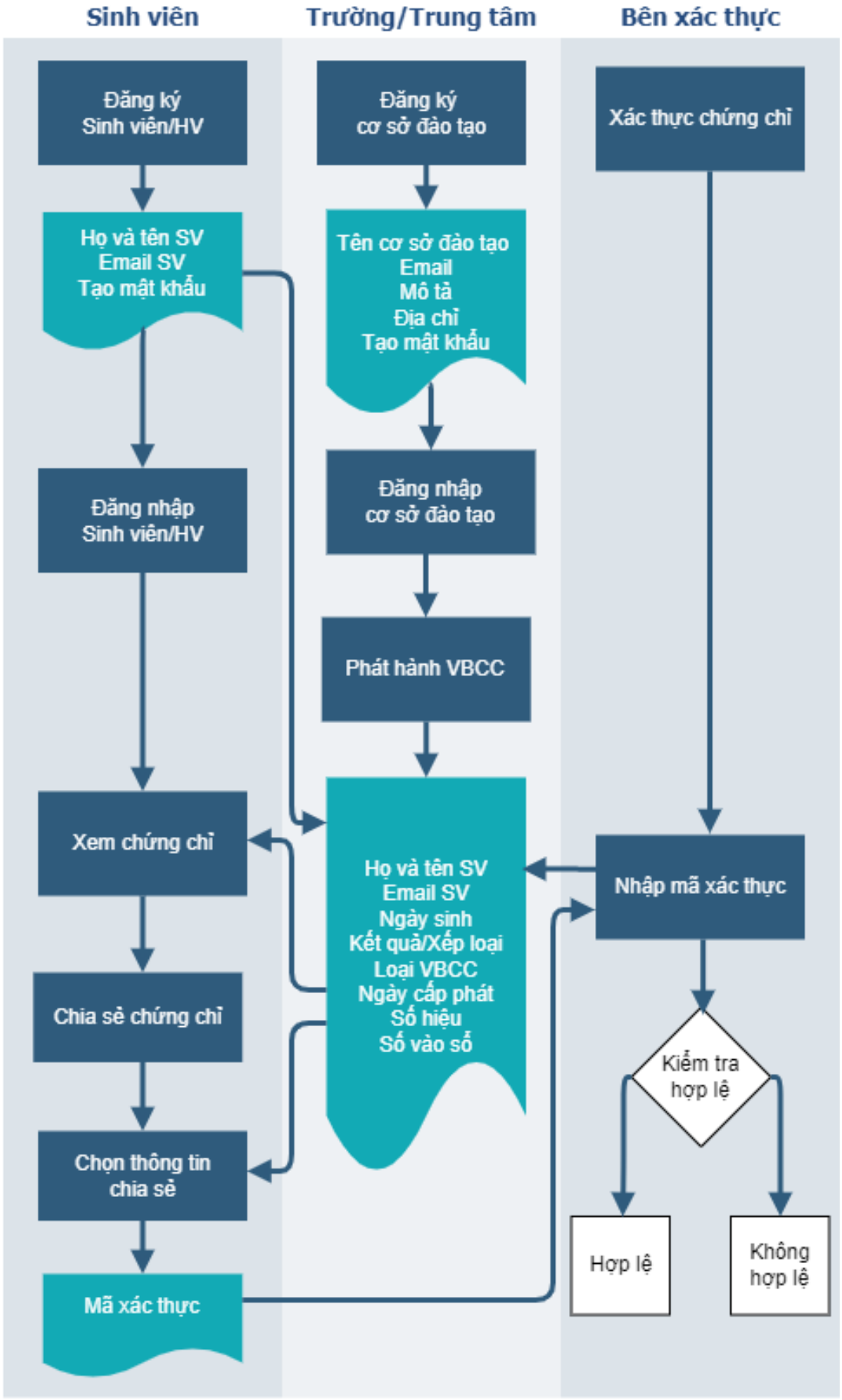
3.2.1 Danh sách tác nhân

Bảng 3.1: Danh sách tác nhân

ID	Tên actor	Mô tả
A1	Sinh viên	là sinh viên/học viên nhận VBCC
A2	Trường học	Trường/Đơn vị có quyền cấp VBCC
A3	Người xác minh	Người/Đơn vị có nhu cầu xác minh VBCC



Hình 3.2: Sơ đồ kiến trúc hệ thống



Hình 3.3: Quy trình hoạt động của hệ thống

3.2.2 Danh sách chức năng

Bảng 3.2: Danh sách chức năng

STT	ID	Tên Use Case	Mô tả	Yêu cầu nghiệp vụ
1	U1	Đăng nhập	Đăng nhập vào hệ thống để xác thực người dùng	Được mở rộng bởi tất cả
2	U2	Đăng ký	Đăng ký tài khoản vào hệ thống	Được mở rộng bởi tất cả
3	U3	Cấp VBCC	Cấp VBCC có xác nhận chứng thực và ký số VBCC	
4	U4	Xem VBCC đã cấp	Xem các VBCC Trường cấp	
5	U5	Xem VBCC đã nhận	Xem VBCC sinh viên đã nhận	
6	U6	Chia sẻ thông tin VBCC	Chia sẻ thông tin VBCC	
7	U7	Xác thực VBCC	Xác minh tính xác thực của VBCC với nền tảng blockchain	

3.2.3 Mô tả chức năng hệ thống

1. Chức năng Đăng ký tài khoản

• Mô tả: chức năng này cho phép người dùng đăng ký tài khoản để đăng nhập vào hệ thống, để sử dụng các chức năng yêu cầu bắt buộc đăng nhập.

• Tác nhân: sinh viên, trường cấp VBCC

• Yêu cầu: người dùng đã truy cập vào hệ thống

2. Chức năng Đăng nhập

• Mô tả: chức năng để người sử dụng đăng nhập vào hệ thống

• Tác nhân: sinh viên, trường cấp VBCC

• Yêu cầu: người dùng đã truy cập vào cập hệ thống

3. Chức năng Cấp VBCC

• Mô tả: chức năng cho phép Trường thêm mới một VBCC

• Tác nhân: Trường cấp VBCC

• Yêu cầu: người dùng đã đăng nhập vào hệ thống; người dùng chọn chức năng cấp VBCC

4. Chức năng Xem VBCC đã cấp

• Mô tả: chức năng cho phép người dùng xem VBCC đã cấp

• Tác nhân: Trường cấp VBCC

• Yêu cầu: người dùng đã đăng nhập vào hệ thống; người dùng chọn chức năng xem VBCC

5. Chức năng Xem VBCC đã nhận

• Mô tả: chức năng cho phép người dùng xem VBCC

• Tác nhân: sinh viên

• Yêu cầu: người dùng đã đăng nhập vào hệ thống; người dùng chọn chức năng xem VBCC

6. Chức năng Chia sẻ thông tin VBCC

• Mô tả: chức năng cho phép người dùng chia sẽ thông tin VBCC

• Tác nhân: sinh viên

• Yêu cầu: người dùng đã đăng nhập vào hệ thống; người dùng chọn chức năng chia sẽ VBCC

7. Chức năng Xác thực VBCC

• Mô tả: chức năng cho phép người dùng xác thực VBCC

• Tác nhân: người xác minh, sinh viên, trường

• Yêu cầu: người dùng truy cập vào hệ thống; người dùng chọn chức năng xác thực VBCC

3.2.4 Thiết kế CSDL

Danh sách cấu trúc dữ liệu trong hệ thống

Bảng 3.3: Danh sách cấu trúc dữ liệu trong hệ thống

STT	Tên cấu trúc	Diễn giải
1	certificate	Cấu trúc thông tin VBCC
2	student	Cấu trúc thông tin sinh viên
3	university	Cấu trúc thông tin trường/trung tâm

Thuộc tính của các cấu trúc dữ liệu

Bảng 3.4: Bảng mô tả các thuộc tính của cấu trúc certificate

STT	Tên trường	Kiểu dữ liệu	Diễn giải	Ràng buộc
1	studentName	String	Họ tên	not null
2	studentEmail	String	Email	not null
3	studentID	String	Mã số	
4	birthday	String	Ngày sinh	
5	place	String	Nơi sinh	
6	gender	String	Giới tính	
7	ethnic	String	Dân tộc	
8	universityName	String	Tên trường cấp VBCC	not null
9	universityEmail	String	Email trường cấp VBCC	
10	major	String	Khóa học	not null
11	number	String	Số hiệu VBCC	not null
12	regNo	String	Số vào sổ gốc	not null
13	departmentName	String	Tên khoa	
14	cgpa	String	Kết quả	not null
15	dateOfIssuing	String	Ngày cấp	

Bảng 3.5: Bảng mô tả các thuộc tính của cấu trúc student

STT	Tên trường	Kiểu dữ liệu	Diễn giải	Ràng buộc
1	email	String	Email	not null
2	name	String	Họ tên	not null
3	password	String	Mật khẩu	
4	publicKey	String	Khóa công khai	

Bảng 3.6: Bảng mô tả các thuộc tính của cấu trúc university

STT	Tên trường	Kiểu dữ liệu	Diễn giải	Ràng buộc
1	email	String	Email	not null
2	name	String	Tên trường	not null
3	location	String	Địa chỉ	
4	password	String	Mật khẩu	
5	publicKey	String	Khóa công khai	

3.2.5 Thiết kế blockchain

1. Danh sách các đối tượng trong hệ thống

Bảng 3.7: Danh sách các đối tượng trong hệ thống

STT	Tên cấu trúc	Diễn giải
1	certificate	Chứng chỉ
2	schema	Loại VBCC
3	university	Trường cấp VBCC

Bảng 3.8: Bảng mô tả các thuộc tính của đối tượng certificate

STT	Tên trường	Kiểu dữ liệu	Diễn giải	Ràng buộc
1	certHash	String	Lưu giá trị băm của VBCC	not null
2	universitySignature	String	Chữ ký số lên certHash dùng khóa cá nhân của Trường cấp VBCC	not null
3	studentSignature	String	Chữ ký số lên certHash dùng khóa cá nhân của sinh viên nhận VBCC	
4	dateOfIssuing	String	Ngày cấp	
5	certNumber	String	Số hiệu VBCC	
6	certRegNo	String	Số vào sổ gốc	
7	certNumber	String	Số hiệu VBCC	
8	certUUID	String	Mã số VBCC	
9	universityPK	String	Khóa công khai của Trường cấp VBCC	
10	studentPK	String	Khóa công khai của sinh viên nhận VBCC	

Bảng 3.9: Bảng mô tả các thuộc tính của đối tượng schema

STT	Tên trường	Kiểu dữ liệu	Diễn giải	Ràng buộc
1	certificateType	String	Loại VBCC	not null
2	id	String	Mã loại	not null
3	ordering	String		

Bảng 3.10: Bảng mô tả các thuộc tính của đối tượng university

STT	Tên trường	Kiểu dữ liệu	Diễn giải	Ràng buộc
1	name	String	Tên Trường cấp VBCC	not null
2	publicKey	String	Khóa công khai của Trường cấp VBCC	not null
3	location	String	Địa điểm	
4	description	String	Thông tin mô tả	

CHƯƠNG 4
KẾT QUẢ THỰC NGHIỆM

4.1 Mạng blockchain

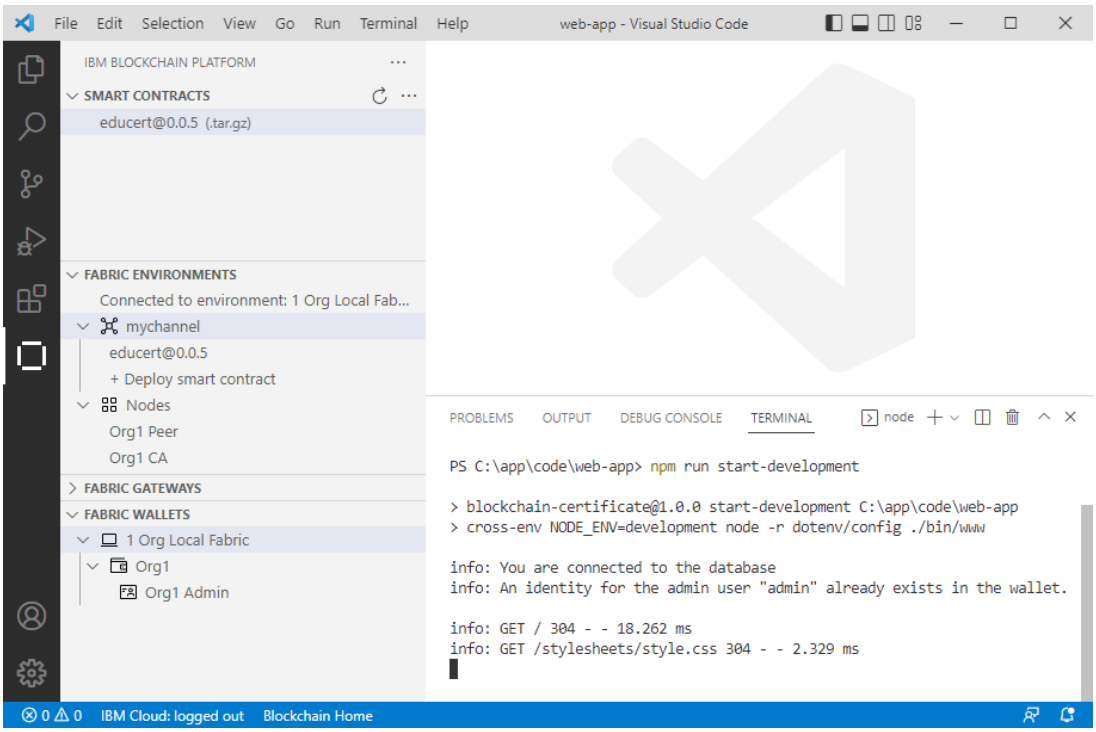
Mạng Blockchain được cài đặt trên máy tính cá nhân có cấu hình như sau:

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

Máy tính được thiết lập theo các bước sau:

1. Mở Visual Studio Code
2. Tìm extension IBM Blockchain Flatform, chọn cài đặt.

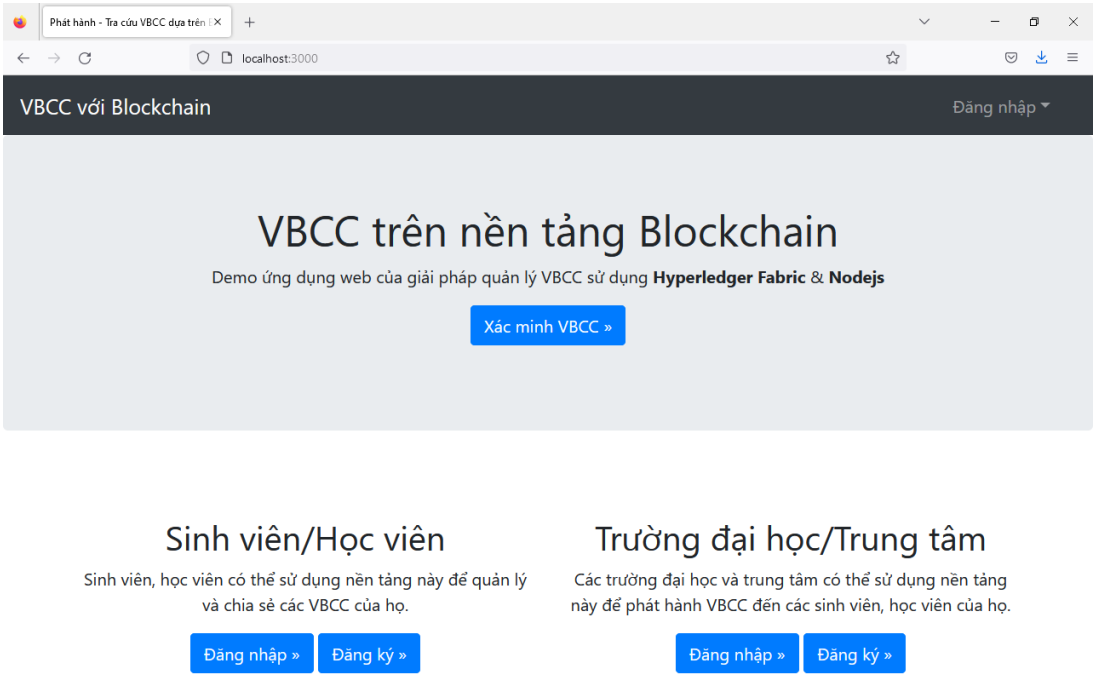
Mạng Blockchain Fabric hoạt động như hình 4.1, blockchain thử nghiệm chaincode gồm có tổ chức Org1, peer, CA, Order, OrdererMSP, Org1MSP



Hình 4.1: Chương trình Visual Studio Code

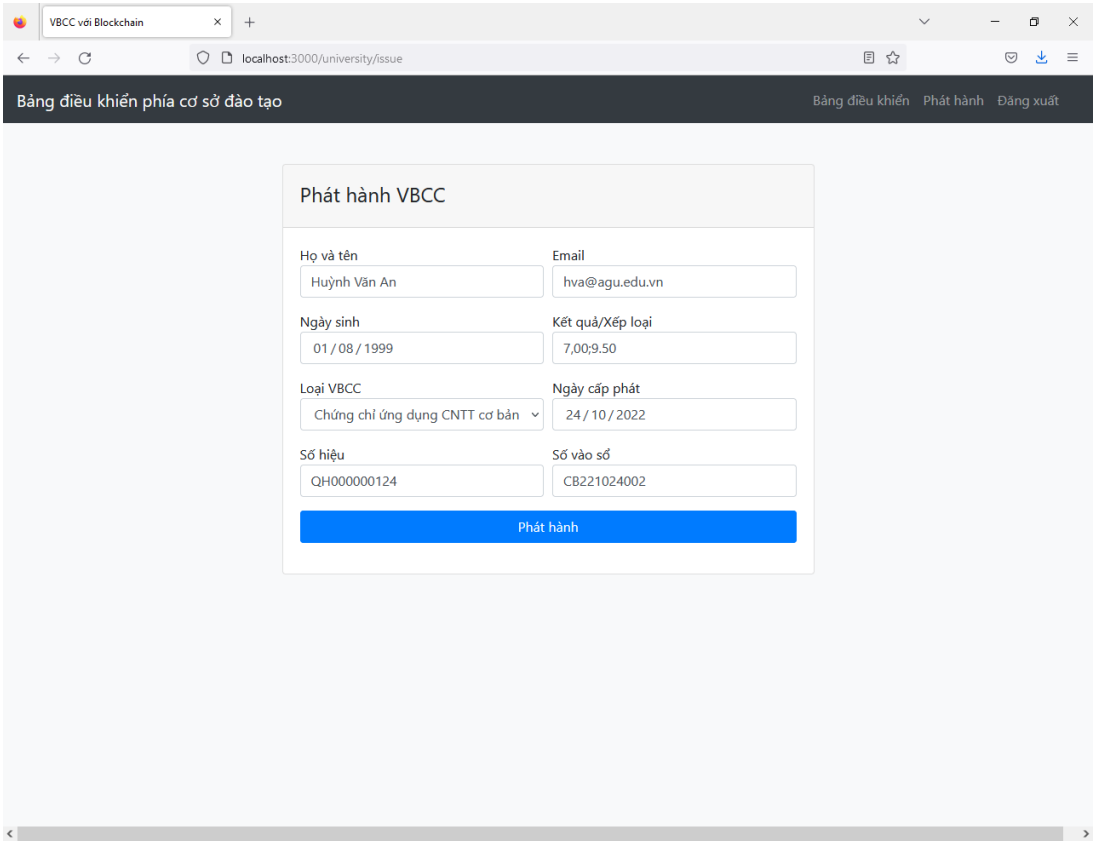
4.2 Ứng dụng Web

Giao diện ứng dụng web hoạt động tại địa chỉ http://localhost:3000/ như hình 4.2.

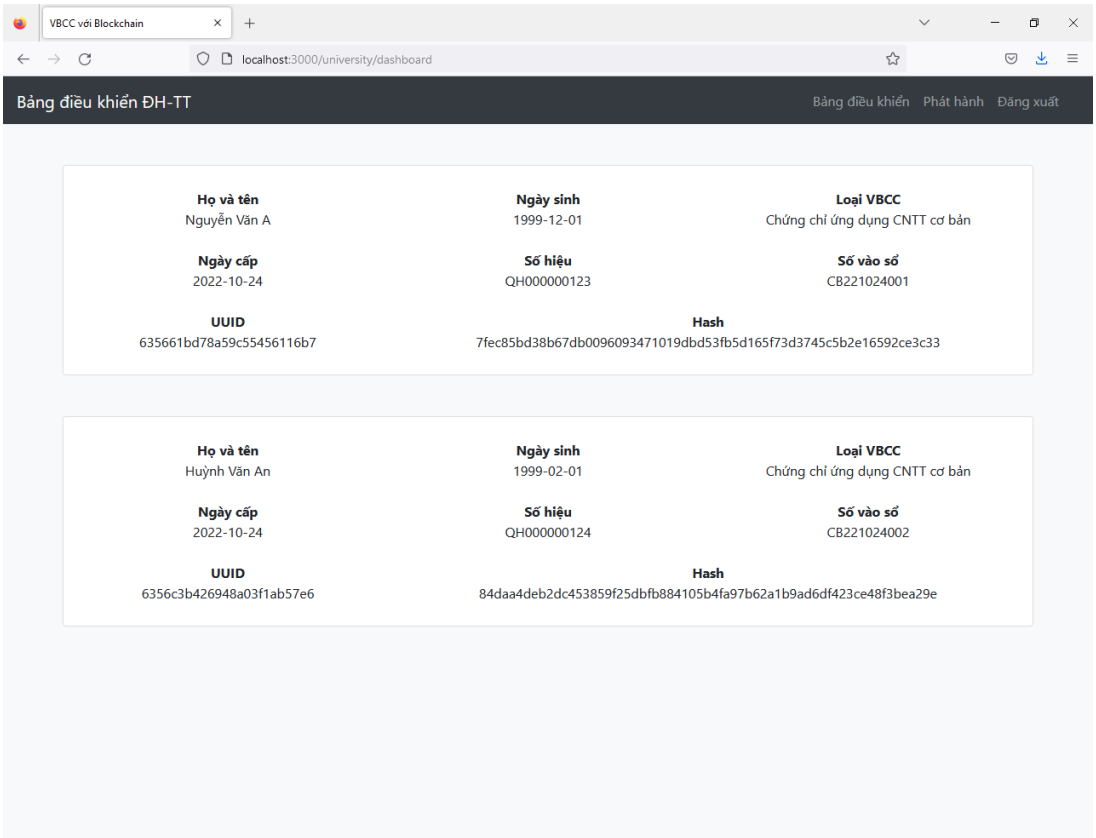


Hình 4.2: Giao diện hệ thống

Trường, trung tâm có chức năng

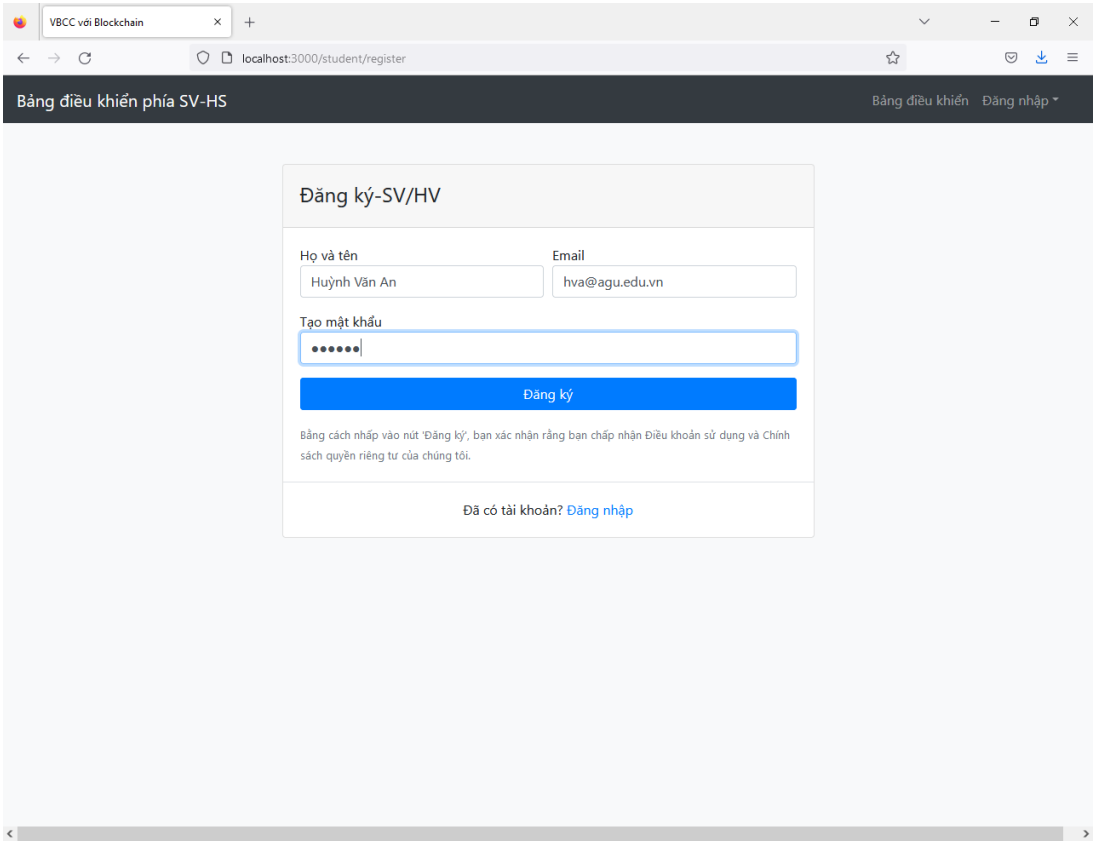


Hình 4.3: Màn hình cấp VBCC cho sinh viên

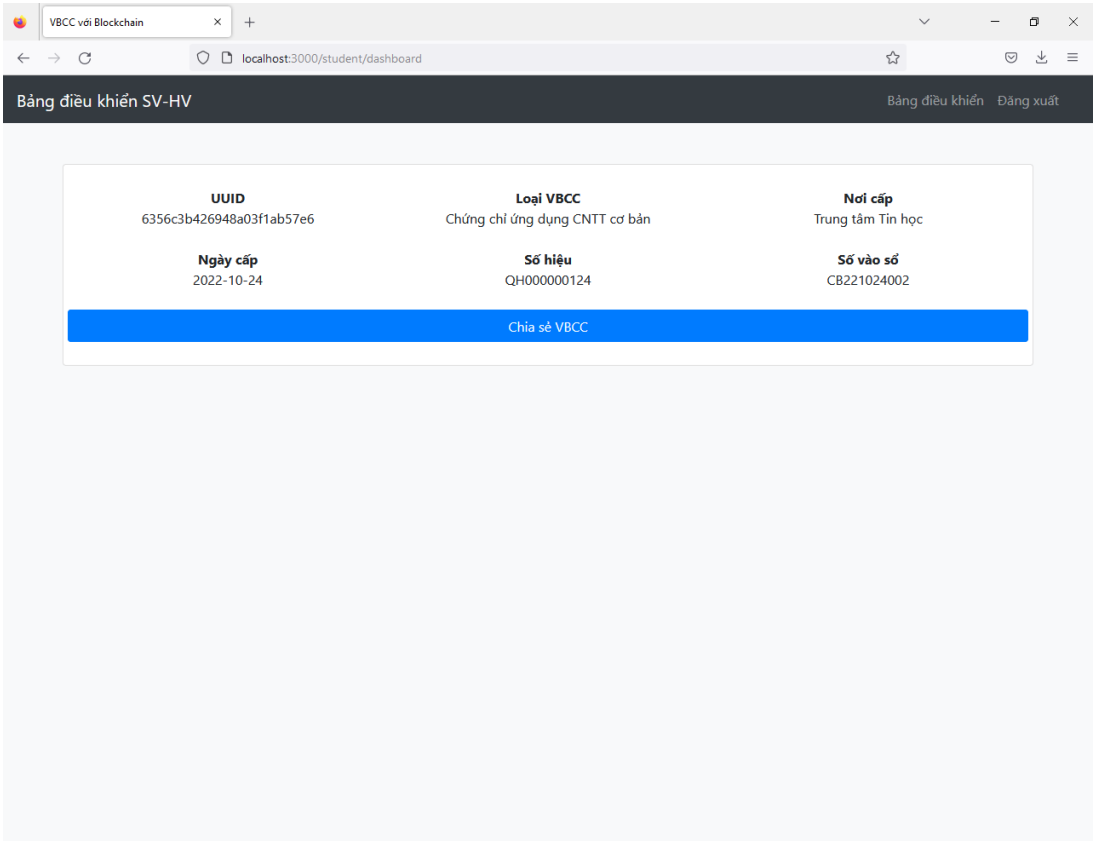


Hình 4.4: Màn hình xem các VBCC đã cấp

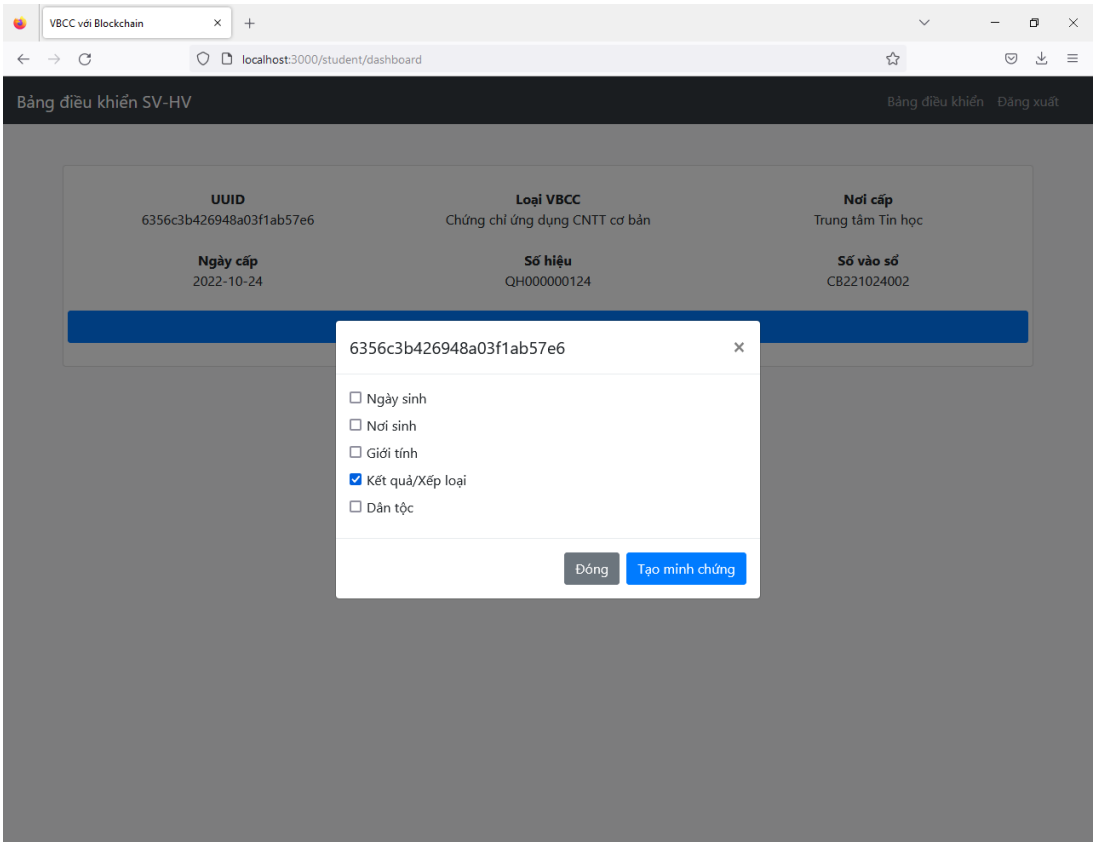
Sinh viên, học viên có chức năng



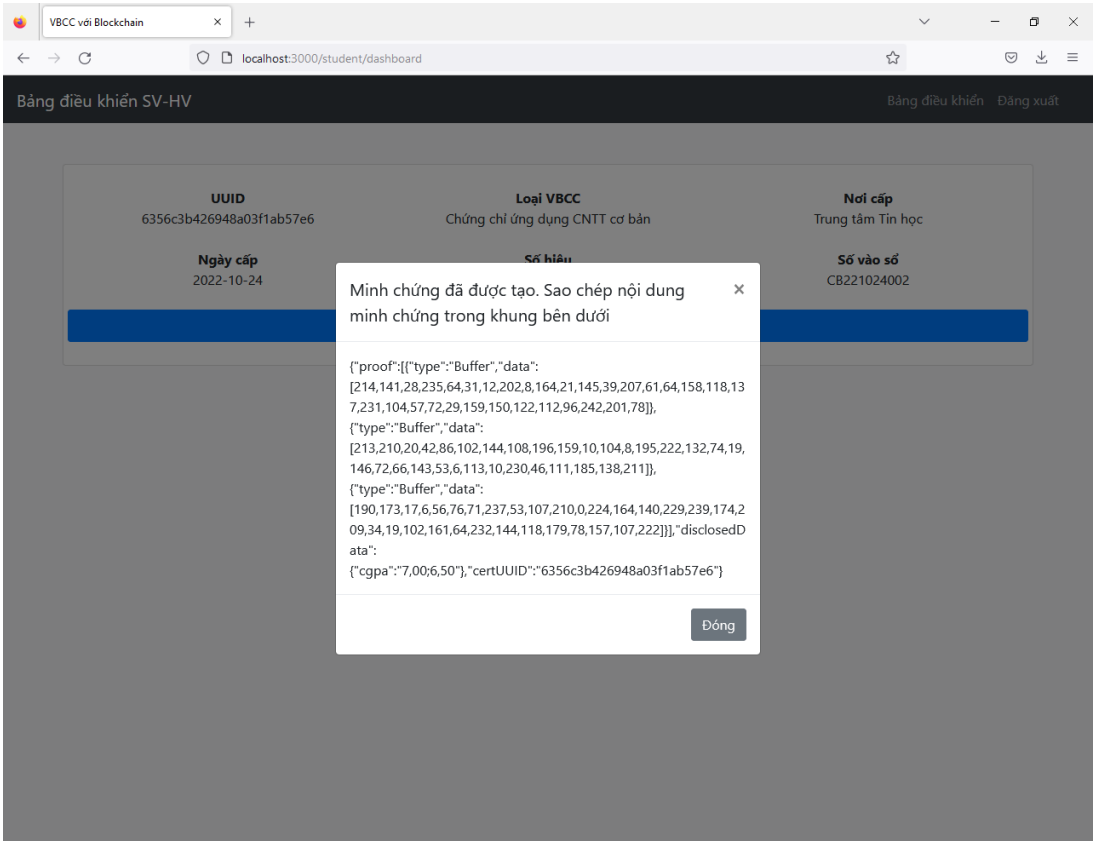
Hình 4.5: Màn hình đăng ký tài khoản



Hình 4.6: Màn hình xem các VBCC đã nhận

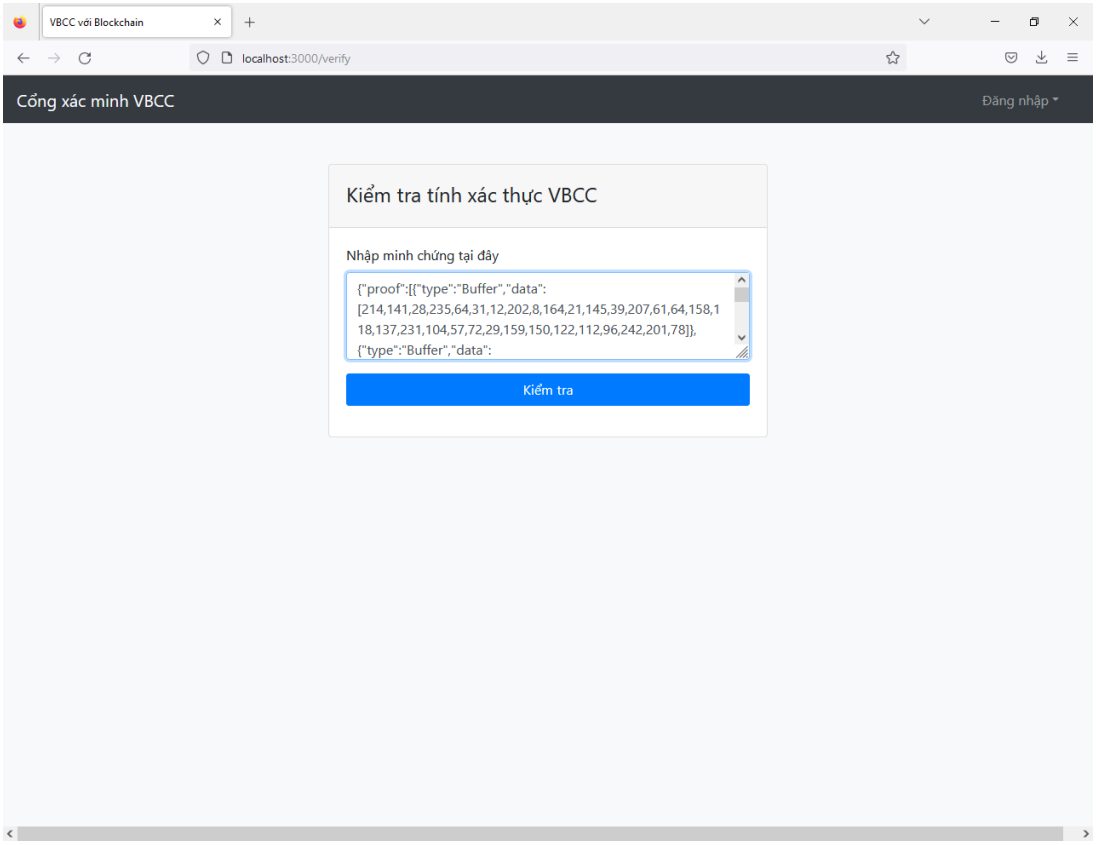


Hình 4.7: Màn hình chia sẻ thông tin VBCC



Hình 4.8: Màn hình hiển thị mã xác thực VBCC

Đơn vị xác minh chứng chỉ có chức năng



Hình 4.9: Màn hình nhập mã xác thực VBCC

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.

Hạn chế của đề tài

Hạn chế của đề tài là chỉ dùng dịch vụ chứng thư số của Hyperledger Fabric và chứng thư số tự cấp trong hệ thống. 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 hạ tầng khóa công khai và dịch vụ 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 tính chính xác và tin cậy. Do đó đề tài cần tiếp tục nghiên cứu ứng dụng công nghệ blockchain trong quy trình tổ chức thi để có thông tin chính xác 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] 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.bcra.2021.100012, URL `https://www.sciencedirect.com/science/article/pii/S2096720921000075`.

[4] Đỗ Thanh Nghị (2018), *Bài giảng Phát hiện tấn công mạng* (ĐH Cần Thơ).

[5] Christof Paar và Jan Pelzl (2009), *Understanding Cryptography: A Textbook for Students and Practitioners* (Springer Publishing Company, Incorporated), 1st edition, ISBN 3642041000.

[6] Phạm Nguyên Khang (2013), *Giáo trình An toàn và bảo mật thông tin* (ĐH Cần Thơ).

[7] 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`.

[8] Satoshi Nakamoto (2008), "Bitcoin: A peer-to-peer electronic cash system". *Decentralized Business Review*, tr. 21260.

[9] 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.

[10] 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.

[11] 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.

[12] C. Shannon (1949 Oktober), "Communication theory of secrecy systems". *Bell System Technical Journal, Vol 28, pp. 656–715*.