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 …
MÃ SỐ …

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 …
MÃ SỐ …

NGƯỜI HƯỚNG DẪN
TS. NGUYỄN VĂN HÒA

NĂM 2022

TRANG XÁC NHẬN CỦA HỘI ĐỒNG

Xác nhận của hội đồng

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, các 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

Tóm tắt tiếng việt

ABSTRACT

Abstract in english

LỜI CAM ĐOAN

Lời cam đoan

MỤC LỤC

DANH SÁCH BẢNG

DANH SÁCH HÌNH VẼ

DANH MỤC TỪ VIẾT TẮT

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

Hiện nay, hầu hết các cơ sở giáo dục rất quan tâm đến hệ thống thông tin quản lý, nhằm để tăng hiệu quả trong công việc quản lý chung. Bên cạnh những hệ thống thông tin quản lý đào tạo, quản lý thi, thì hệ thống tra cứu văn bằng chứng chỉ, bắt buộc công khai theo quy định tại Điều 2 thông tư số 21/2019/TT-BGDĐT. Một số yêu cầu của giải pháp tin học hóa nghiệp vụ, số hóa dữ liệu là đảm bảo nguyên tắc an toàn thông tin của các cá nhân, tổ chức tham gia theo quy định tại Điều 24 luật số 67/2006/QH11.

Tuy nhiên, trong thực tế phương tiện để chia sẻ thông tin là những mạng truyền thông như mạng internet, trạm thông tin di động, wifi. Những mạng này rất rủi ro cho an toàn thông tin bởi vì những người không được phép có thể dùng cách tấn công nghe lén để xâm phạm thông tin [1]. Ngoài ra, thông tin và các thành phần trong mạng là mục tiêu của các cuộc tấn công mạng [2].

Từ năm 2008, công nghệ chuỗi khối (blockchain technology) với Bitcoin [3] là một minh họa, 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. Nhờ đó, công nghệ này 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 [9, 10, 11, 12] để ghi nhận các giao dịch xảy ra theo thời gian và để kiểm chứng nguồn gốc thông tin. Theo đó, chuỗi khối như là một cấu trúc dữ liệu (cuốn sổ cái) ghi lại và mã hóa tất cả các giao dịch giữa các thành phần trong hệ thống để bảo đảm tính toàn vẹn thông tin giúp phát hiện rằng thông tin đã bị sửa đổi hay không (chống sửa đổi). Từ đó hệ thống giúp chống lại sự thoái thác trách nhiệm: một đối tác bất kỳ trong hệ thống không thể từ chối trách nhiệm về hành động mà mình đã thực hiện. Vì vậy, những đặc tính của công nghệ chuỗi khối rất hữu ích trong việc xử lý và chuyển giao thông tin.

Công nghệ chuỗi khối cũng có mặt hạn chế. Nghiên cứu [13] 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.

Mục đích chính của đề tài là ứng dụng công nghệ Blockchain để lưu trữ thông tin văn bằng, chứng chỉ. 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 văn bằng, chứng chỉ khi thông tin được

truy vấn từ cơ sở dữ liệu văn bằng, chứng chỉ bên ngoài chuỗi khối.

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 và có chức năng tổ chức thi và cấp chứng chỉ ứng dụng công nghệ thông tin. 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 văn bằng chứng chỉ do đơn vị cấp trên hệ thống website.

Sổ gốc cấp văn bằng, chứng chỉ theo quy định tại Điều 19 thông tư số 21/2019/TT-BGDĐT yêu cầu ghi thông tin cấp phát văn bằng, chứng chỉ cho người được cấp, đã thi đạt sau khi dự thi tại cơ sở tổ chức thi. Sổ gốc cấp văn bằng, chứng chỉ 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 văn bằng, chứng chỉ 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 văn bằng, chứng chỉ 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 văn bằng, chứng chỉ nhưng cần thiết phải so khớp thông tin giấy tờ với sổ gốc. Thêm vào đó, quá trình xử lý hồ sơ giấy còn gặp một số rủi ro như rách trang giấy, thất lạc,… ảnh hưởng đến công tác lưu trữ, bảo quản hồ sơ theo quy định.

1.3 Mục đích nghiên cứu

Đề tài tập trung đề xuất mô hình ứng dụng công nghệ Blockchain trong quản lý văn bằng chứng chỉ 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 văn bằng chứng chỉ: cập nhật thông tin sổ gốc cấp văn bằng, chứng chỉ; tra thông tin văn bằng, chứng chỉ.
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 văn bằng chứng chỉ 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
- Ngôn ngữ lập trình PHP, JS, khung phát triển ứng dụng Web
- Quy định pháp luật về quản lý văn bằng, chứng chỉ

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 văn bằng chứng chỉ ứng dụng công nghệ blockchain.

1.5 Phương pháp nghiên cứu

- Tìm hiểu, phân tích và tổng hợp tài liệu về quản lý văn bằng chứng chỉ (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 văn bằng, chứng chỉ, 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 xử lý và chia sẻ thông tin, dữ liệu minh bạch theo thời gian 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 văn bằng chứng chỉ, 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 văn bằng chứng chỉ

2.1.1 Giới thiệu

Xã hội ngày càng phát triển, 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 văn bằng, chứng chỉ được cấp phát để công nhận trình độ, năng lực của các học viên đã đủ quá trình học tập và thi đạt. Ngoài ra, văn bằng còn dùng trong quá trình tuyển dụng 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 văn bằng chứng chỉ đòi hỏi quy trình thực hiện nghiêm ngặt, tránh những trường hợp lợi dụng kẽ hở để thực hiện hành vi trái phép.

Một số văn bản pháp luật được ban hành nhằm quy định việc quản lý văn bằng chứng chỉ, 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 văn bằng, chứng chỉ của hệ thống giáo dục quốc dân, quy định việc phân cấp và giao quyền tự chủ, tự chịu trách nhiệm trong quản lý văn bằng, chứng chỉ. 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 văn bằng, chứng chỉ 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 văn bằng chứng chỉ trên môi trường số với nền tảng ứng dụng công nghệ Blockchain và chữ ký số. Hệ thống phần mềm đảm bảo công khai, minh bạch, tin cậy trong công tác tra cứu và xác thực văn bằng, chứng chỉ; hướng tới việc cấp văn bằng, chứng chỉ 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 làm giả hồ sơ gốc. Hệ thống giúp cho các cơ quan, tổ chức, cá nhân trong quá trình kiểm tra xác minh văn bằng chứng chỉ khi tuyển dụng giảm nhiều thời gian, sức lực so với cách truyền thống.

Trung tâm Tin học Trường Đại học An Giang 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 (Quy chế). Việc quản lý các dữ liệu chứng chỉ do đơn vị cấp cần phải đảm bảo tính chính xác. Giao dịch giữa các đơn vị trong và ngoài tổ chức và giữa đơn vị với cá nhân phổ biến cả hai hình thức là hồ sơ điện tử và hồ sơ sơ giấy. Tuy nhiên, phạm vi nghiên cứu của đề tài chỉ tập trung vào hình thức hồ sơ giấy phục vụ 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 văn bằng chứng chỉ 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 văn bằng chứng chỉ dùng công nghệ blockchain để tăng tính bảo mật và chắc chắn cho việc cấp phát các văn bằng, chứng chỉ cho học viên sử dụng. Dữ liệu đầu vào của hệ thống được lấy từ chương trình quản lý học, quản lý thi đang đáp ứng tốt một số nghiệp vụ quản lý hiện nay. Những nghiệp vụ được nghiên cứu 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 văn bằng, chứng chỉ 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.
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 văn bằng, chứng chỉ là một trong những giai đoạn cần thực hiện để phát hành văn bản có hiệu lực. Quy trình xác minh văn bằng, chứng chỉ 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 văn bằng, chứng chỉ 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 và sử dụng trong mục đích cần thiết.

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 dấu 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. Ngày nay, các ứng dụng mã hóa và bảo mật thông tin đang được sử dụng ngày càng phổ biến hơn trong nhiều lĩnh vực, từ lĩnh vực an ninh, quân sự, quốc phòng, cho đến các lĩnh vực dân sự như thương mại điện tử, ngân hàng.

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 quá trình bảo mật và mã hóa là tạo ra các mô hình tin cậy đảm bảo cho hệ thống đạt 4 tiêu chí của an toàn thông tin:

- 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.
- 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.
- 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 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).
- Tính không chối bỏ hay chống thoái thác (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

Mật mã luồng (Stream Ciphers) Mật mã khối (Block Ciphers) Các phương thức tính toán của mật mã khối

2.2.2 Mật mã Khóa bất đối xứng

RSA

2.2.3 Băm (Hash)

HASH

2.2.4 Chứng thư (Certificate)

X.509

2.2.5 Chữ ký số (Digital Signature)

2.2.6 Certificate Authority

2.2.7 Hạ tầng khóa công khai PKI (Public Key Infrastructure)

2.3 Công nghệ Blockchain

Công nghệ Blockchain có bản thiết kế đầu tiên vào năm 2008 bởi Satoshi Nakamoto và trở thành thành phần cốt lõi 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.

Trong những năm gần đây, 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 là một cơ sở dữ liệu phân cấp lưu trữ dữ liệu trong các khối thông tin được liên kết với nhau bằng mã hóa 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. 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. Hiện nay, công nghệ này đang thu hút nhiều nghiên cứu để xây dựng các mô hình mạng blockchain cho các qui trình đặc thù trong tài chính, bầu cử, nông nghiệp,…ngoài lĩnh vực tiên phong tiền mã hóa.

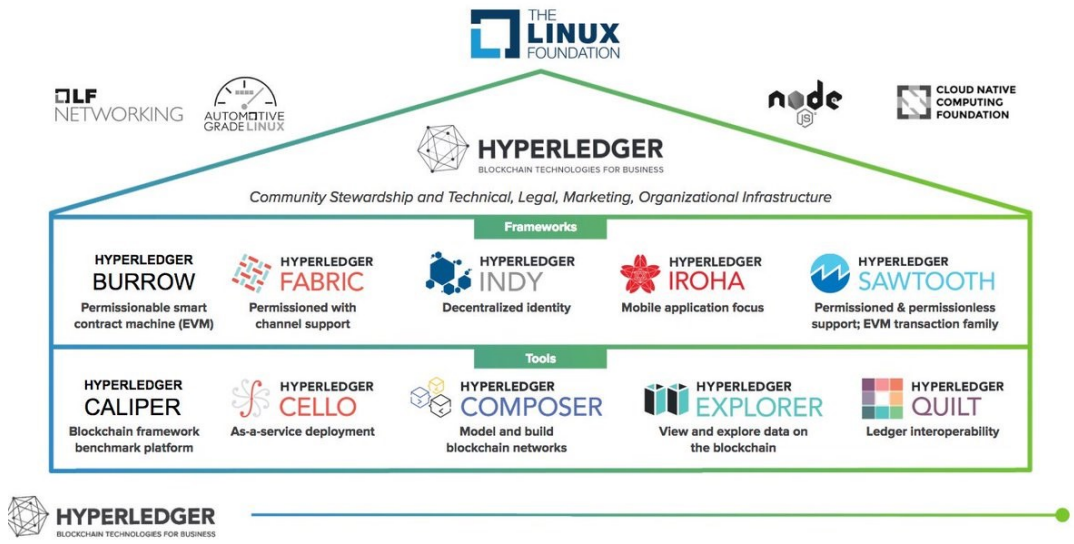
Hiện nay, hệ thống mạng blockchain được chia làm 3 nhóm. Nhóm hệ thống blockchain công cộng cho phép mọi người dùng có truy cập dữ liệu như Bitcoin, Ethereum. Nhóm hệ thống blockchain riêng tư do một tổ chức hoặc một cá nhân đầu tư và kiểm soát, thông tin được kiểm soát chặt chẽ và chỉ được phổ biến trong nội bộ. 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. Trong thực tế, công nghệ blockchain chỉ phù hợp với các dạng dữ liệu giao dịch.

2.4 Hyperledger Fabric

2.4.1 Giới thiệu

Hyperledger Fabric là một trong năm framework về blockchain nằm trong chiến lược Hyperledger Umbrella của Linux Foundation gồm: Hyperledger Indy, Hyperledger Fabric, Hyperledger Iroha, Hyperledger Sawtooth, Hyperledger Burror.

Hyperledger Fabric là một nền tảng công nghệ mã nguồn mở dưới sự cố vấn của IBM, được thiết kế để sử dụng trong môi trường doanh nghiệp, cung cấp nhiều tính năng nổi trội với các nền tảng blockchain đang tồn tại. 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, chính phủ…



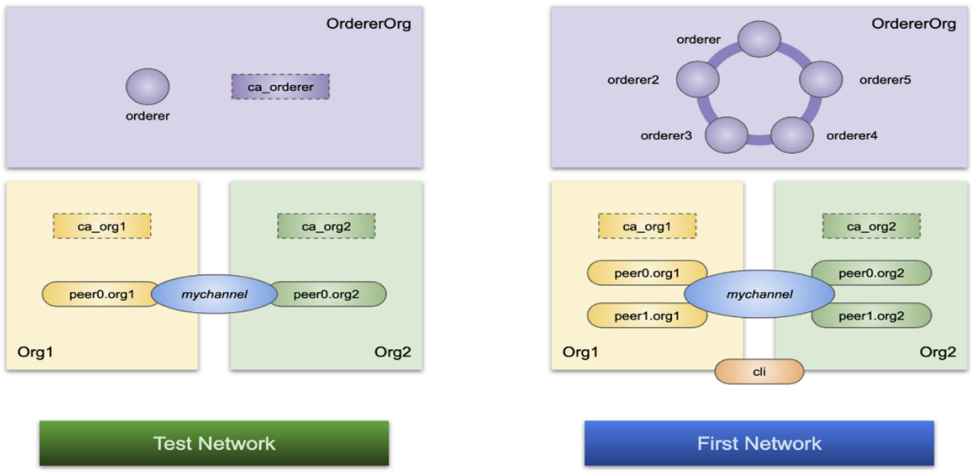
Hình 2.1: Chiến lược Hyperledger Umbrella

Nhờ vào thiết kế mô-đun linh hoạt, chính sách quyền hạn cho người tham gia đã giúp Hyperledger Fabric trở thành nền tảng blockchain hoạt động tốt về tốc độ xử lý giao dịch, độ trễ xác nhận giao dịch, cho phép bảo mật và xác minh các giao dịch với hợp đồng thông minh.

2.4.2 Những cải tiến của Hyperledger Fabric trong phiên bản 2.x

Những điểm mới trong phiên bản Hyperledger Fabric 2.x rất thích hợp cho hệ thống mạng blockchain mà đề tài đang hướng đến. Phiên bản mới Fabric 2.x được hỗ trợ dài hạn, điều đó có nghĩa rằng các vấn đề bảo mật, lỗi hệ thống sẽ sớm được công đồng và nhà phát triển cập nhật cho đến khi một phiên bản LTS mới được phát hành.

Trong phiên bản Fabric 2.x, các hợp đồng thông minh (chaincode) muốn được cài đặt trên peer và chạy trên channel cần phải thông qua một vòng đời mới. Các tổ chức thuộc kênh (channel) cần thống nhất (đồng ý thõa thuận) các tham số của hợp đồng như chính sách chứng thực hợp đồng trước khi hợp đồng được thực hiện tương tác với sổ cái (ledger).



Hình 2.2: Cấu trúc mạng đề xuất của hai phiên bản 1.4 và 2.x

Việc nâng cấp các hợp đồng thông minh (chaincode) sẽ được gắn với quá trình đồng thuận và chỉ hoàn thành khi đạt được ngưỡng cho phép của các thành viện thuộc kênh. Điều đó có nghĩa tất cả thành viên thuộc kênh luôn giữ đầy đủ các hợp đồng (được cài đặt chaincode) cùng nhau thay vì có thể từ chối như phiên bản 1.4. Việc thay đổi cơ chế nâng cấp giao dịch của 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. Thay vì tạo thêm một kênh để nhóm các thành viên và mất rất nhiều thời gian để cấu hình (kênh, chính sách, MSP,…)

Một trong những điểm nổi bật của phiên bản Fabric 2.x là tối ưu hóa hiệu suất hoạt động của mạng Blockchain. Bằng cách thay thế giải thuật Rafka thành giải thuật Raft, thêm một bộ nhớ đệm mới vào các peer để tìm nạp dữ liệu nhanh hơn khi sử dụng CouchDB bên ngoài, xác thực giao dịch song song, xử lý khối bất động bộ, phân trang chaincode,…Điều đó cho phép Hyperledger Fabric 2.x đảm bảo hiệu suất có thể xử lý hàng nghìn giao dịch mỗi giây.

2.4.3 Các thành phần của mạng Hyperledger Fabric

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

Smart contract (Chaincode): Hợp đồng thông minh – một ứng dụng được viết bằng các ngôn ngữ lập trình như: Javascript, Go, Java dùng để tương tác với mạng, quản lý tài sản. Trong Hyperledger Fabric, các hợp đồng thông minh được gọi là chaincode,

được cài đặt trên các Peer.

Peer nodes: Là thành phần cơ bản của mạng, lưu trữ bản sao của Ledgers và thực thi Smart contract. 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 thành phần chứa thuật toán đồng thuận và đảm nhận nhiệm vụ xác minh, bảo mật, kiểm định chính sách, quản lý cấu hình Channel.

Channel: Kênh là một "mạng con" riêng kết nối giữa hai hoặc nhiều thành viên trong mạng. Cấu hình một kênh gồm các Orgs(tổ chức), Peer, Ledger, Chaincode, Ordering service. Mỗi Peer có thể tham gia nhiều kênh và sẽ được cấp các định danh riêng với từng kênh bởi nhà cung cấp dịch vụ thành viên (MSP).

Fabric Certificate Authorities: Hyperledger Fabric CA là thành phần phát hành chứng chỉ mặc định, cung cấp chứng chỉ dựa trên PKI cho các tổ chức thành viên mạng và người dùng. CA phát hành một chứng chỉ gốc (rootCert) cho mỗi thành viên và một chứng nhận đăng ký (ECert) cho mỗi người dùng được uỷ quyền.

Membership Service Provider (MSP): Trong cơ sở hạ tầng của mạng Hyperledger Fabric, MSP là một tập hợp các thư mục được thêm vào cấu hình của mạng Fabric nhằm xác minh một tổ chức. Đây là một tập hợp các thư mục chứa các chứng chỉ số (cấp từ CA), giúp mạng 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 thực đặc quyền truy cập trong phạm vi mạng và kênh của một thành phần nào đó trong mạng.

TÀI LIỆU THAM KHẢO

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

[2] Đỗ Thanh Nghị (2018), *Bài giảng Phát hiện tấn công mạng* (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.bcra.2021.100012, URL `https://www.sciencedirect.com/science/article/pii/S2096720921000075`.

[6] Trương Minh Tuyền, 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] Lê Quyết Thắng (2016), *Bài giảng Lý thuyết mật mã* (ĐH Cần Thơ).

[10] Christof Paar (2015 apr), *Implementation of Cryptographic Schemes 1* (Ruhr University Bochum).

[11] Ralph Charles Merkle (1979), "Secrecy, authentication, and public key systems". Báo cáo kỹ thuật.

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

[13] 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.

[14] H. Kopka và P. W. Daly, *A Guide to LaTeX* (Addison-Wesley, Reading, MA).